"BLOCKCHAIN BASED PRIVACY PRESERVATION IN HEALTHCARE: A RECENT TRENDS AND CHALLENGES"

Nidhi Raghav

Ph.D. Scholar, CSE, AIM & ACT, Banasthali Vidyapith,Rajasthan, India Email: raghav.nidhi@gmail.com

Anoop Bhola

Assistant professor CSE, AIM & ACT, Banasthali Vidyapith, Rajasthan, India Email: anupbhola@banasthali.in

ABSTRACT:

Healthcare is changing fast with better and efficient services for patient care. Electronic health records are electronic saved information related to health in digitally format. With EHR the healthcare data can be easily shared across the different healthcare settings.EHR enhances the Patient care by providing the accuracy and precision of medical records where security and privacy preservation are challenging in the system. In recent years, Blockchain has become viable technology which has invaded different domains. Blockchain has enormous potentialin healthcare because of demand of patient centric system and to connect different systems together. Blockchain is a promising solution for security and preservation of privacy in a healthcare sector. In this paper we have provide a comprehensive review of healthcare systems which are based on blockchain. The main objective of this paper is to reveal about blockchain technology in privacy preservation, security of healthcare and its future research directions. We have recognized and analyze latest research papers and literature to present a challenges and comparison between various published work in the domain of blockchain for healthcare.

Keywords:

blockchain, healthcare, distributed systems, privacy preservation, security, smart contract, Ethereum

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

INTRODUCTION

Healthcare and Health data are vital in our lives. The health data traditionally were kept on papers which is vulnerable to modification and damage.so, it was essential for healthcare data to be store electronically to reduce the barriers of data sharing and data protection between different healthcare providers. With the rapid increase in digitization in healthcare there is huge generation of electronic health records. Such growth of EHR requires unmatched data protection in healthcare. Interoperability is also one of the essential requirements of healthcare industry. Interoperability is the data and information sharing between entities either between humans or machines, consistently and efficiently. For sharing the data throughout the environment and to be distributed among different hospital systems interoperability provides a platform for exchange the EHR and health related information among different healthcare providers. Since, the sources of medical data are very diverse. Interoperability enables to share medical data despite of healthcare provider location and trust between them. Diagnostic accuracy may boost up in healthcare sector by sharing the patient data among different health care providers but centralized health data repository can be vulnerable to single point of failure and to cyberattacks also.

This raises the concerns about confidentiality and privacy of patient health data. Therefore, data security is important aspect in healthcare and play very important role in protective sensitive information of patients [15][20]. The traditional methods used for security and privacy are not enough in securing the healthcare application data. Sharing and accessing medical records are vital for receiving more advanced and intelligent medical services, patients should be given more priority and they should have control of their data because every data cannot be made public because of security and privacy. The Blockchain Technology and smart contract emergence are providing promising solutions to solve the challenges in the health care sector. This Technology transparent mechanism has the potential to cater the issues of integrity, data privacy and security [18][19]. To enhance the patient outcomes, increase compliance, patient data management and to optimize the business processes blockchain technology is definitely affecting positive consequences on companies and stakeholders in healthcare.

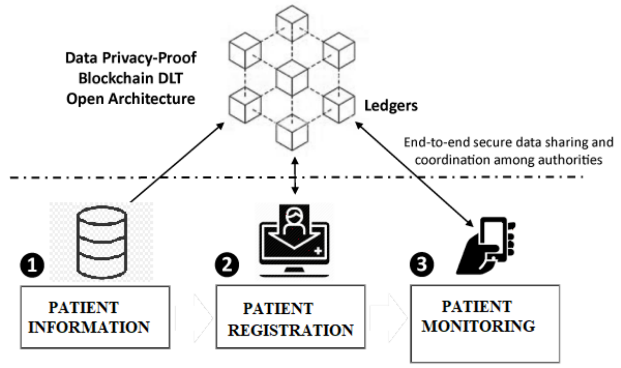

Figure 1: Blockchain and Healthcare

Blockchain is a distributed ledger technology for P2P(peer to peer) network allowing data to stored and shared publicly or privately to users in distributed manner with reliable and verifiable plan [23]. It uses advanced cryptosystem techniques to secure applications. It provides transparencyand remove the need of third party or intermediaries by relying on miners that validate the transactions in a decentralized manner. This is attained through a consensus mechanism and cryptography techniques among multiple parties that are distributed in peer-to-peer network. On blockchain, Smart contract is a program and legal binding rules that contains the agreement under which different entities of the system agrees to interact with each other. The purpose of Smart Contract is to make trade simple between parties without the intermediaries. To make healthcare smarter and to enhance the quality of healthcare, it is essential to share the health data without risking the user privacy and security [11][14]. The goal of this paper is to present a review on the privacy preserving model of healthcare based on blockchain and their current challenges.

The remainder of this paper is organized as follows. In Section 2, background information about blockchain and its concepts for healthcare is presented. The literature survey and review about privacy preservation with blockchain in healthcare is discussed in section 3. The Section 4 provides the comparison between different privacy preservation blockchain models in healthcare and their challenges. The paper is summed up in section 5 in which conclusion is drawn.

1. Blockchain Overview

Blockchain is a distributed digital ledger that’s help in sharing of data among the peer network in a decentralized way. It was proposed by Nakamoto et al as a decentralized cryptocurrency. Blockchain is a chain of blocks that are linked together using cryptographic hashes with a timestamping. Each block is transparent, searchable, secure and immutable. The chain of blocks constantly grows by appending a block to the end whereas every new block has a hash value of content of previous block stored in it.Every node has two keys associated with it that is public and private key. So, the concept of asymmetric key is used in blockchain network [12][13]. The blocks are connected with each other with the help of hash. The hashes are generated with the help of cryptographic hash functions like SHA-256.This makes certain of immutability and anonymity of blocks. Before the transaction is broadcasted in a peer-to-peer network, it is digitally signed by using a private key. It provides authentication and integrity of transactions. The transaction then broadcasted into the network and validated transactions by the miners are packed into time stamped blocks. The specific consensus method like proof of work or proof of stake etc. is used in the network for agreement in a distributed network. The blocks are broadcasted in a network where it is validated and then added into chain of blocks. Blockchain provides trust in a peer-to-peer network. The main component of blockchain technology is cryptography, consensus and distributed ledger.

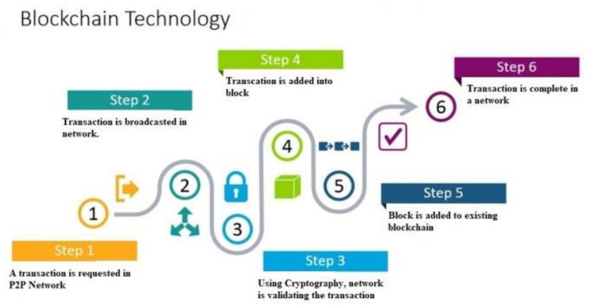
Blockchain Technology
Step 1
A transaction is requested in P2P Network
Step 2
Transaction is broadcasted in network.
Step 3
Using Cryptography, network is validating the transaction
Step 4
Transcation is added into block
Step 5
Block is added to existing blockchain
Step 6
Transaction is complete in a network
1
2
3
4
5
6

Figure 2: Blockchain Roadmap

The single block in a blockchain consists of Blockheader, blocksize, transaction data and transaction counter. The all-important information about the block and transaction is stated in blockheader.The integrity of blocks is maintained with the use of hash. The blockheader contains the block version, previous block hash, Merkle root, timestamp, Nonce and difficulty target. The value of these fields is encrypted together to called as Block hash. The First block of blockchain is called as Genesis block. This structure makes it immutable and secure in nature.

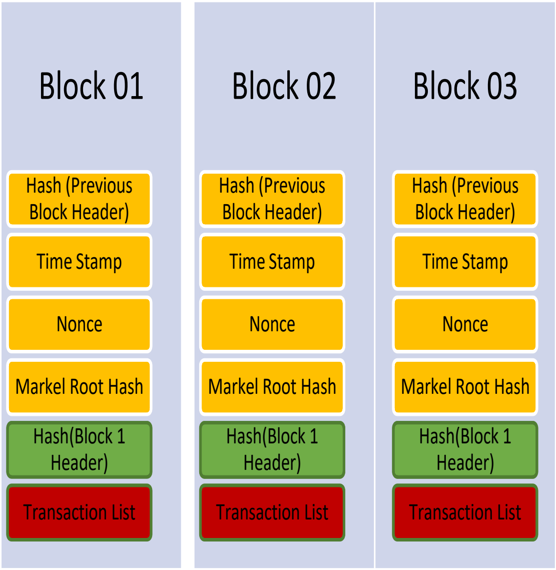

Figure 3: Block chain Blocks

Blockchain Architectures for healthcare system

Blockchain architectures are defined according to entitlement given to users to read and write on the distributed ledger. It provides public/private access of ledgers or permissioned or permission less access of ledgers. Mainly three blockchain architectures are defined:

1) Public permissionless blockchain or public blockchain: The data in this type of blockchain is accessible and visible to public. Anyone can participate in the consensus and can join the network without permission. With some anonymity transaction is visible to all nodes. This type of architecture is used in cryptocurrency networks such as Bitcoin and Ethereum but it is subjected to privacy issues.

2) Public permissioned or consortium blockchain: This blockchain is visible in public for use but selected or permissioned nodes can participate in the consensus

mechanism. Only these selected nodes can write in the distributed ledger. Between one or several industries this type of architecture can be used where use is opened for public but some part still have partial centralized trust.

3) Private or permissioned Blockchain: In this type of architecture only selected nodes or permissioned node can join the network. To participate in consensus or perform operations on the ledger a permission is needed. They are generally run by single organization and its use is private for their purposes. Hyperledger and Ripple are one of the examples of private blockchains.

Blockchain based health system is trending topic. Blockchain can connect the different entities of healthcare system and increase the efficiency in storing and sharing of health records [21][22]. All the health data that is generated should be verifiable and tamperproof, this is provided by blockchain [16][17]. Patients can control their own sensitive data by privacy preservation feature of blockchains.

RELATED WORK

Blockchain Technology has the potential to solve the critical issues like securing data, transaction and storage in healthcare in robust and effective manner. This technology enables secure sharing process for healthcare data [23]. This paper presents a systematic review and latest research depicting the state-of-the-art blockchain technology in the privacy preservation in healthcare systems.

In 2019, Mubarakali et al. [1] implemented an effective and secure health record transaction utilizing a block chain (SEHRTB) algorithm to resolve medical records regarding the knowledge transactions between doctors, patients, organizations and content providers in such a privacy-preserving manner. Research has supported the healthcare industry with block chain technologies. While evaluating health care, the individual became far more inclined to access and exchange their health information in a safe way through cloud services without any loss of privacy. This work further offered an efficient path for securing the private data of patient in intellectual health care scheme. Without contravene the privacy, this paper builds the system in a decentralized computing structure for ensuring trusted third party in order to conduct the calculation over patient data. On the basis of simulation outcome, the SEHRTB algorithm has achieved the reduced latency of 2.05, an execution time of 1.08, and the enhanced throughput of 30.5% as compare with the existing approaches.

In 2019, Omar et al. [2] stated the emerging interest of healthcare data in cloud for the cyber attackers. The healthcare organizations have suffered annihilating consequences by these attacks on healthcare data. The impact of attacks has been minimized by the Decentralization of the cloud data. Computing on confidential private health information processed and managed by data decentralization of the peer-to-peer (P2P) system. Blockchain technology has maintained transparency and openness by exploiting decentralized or shared properties. Although the attacks impact has been controlled by proposing diverse solutions based on decentralized approach, these solutions have failed on ensuring the complete privacy of patient centric systems. Such research study has therefore identified a patient-centric healthcare data processing framework focused on blockchain technologies as a database mechanism that seeks to ensure anonymity. Cryptographic methods have been used to encrypt medical details and to guarantee pseudonymity. As a result, study of the data processing processes and the cost-effectiveness of both the smart contracts have also been carried out.

In 2019, Cao et al. [3] has introduced a safe cloud-assisted eHealth to secure outsourced EHRs against illicit reform dependent on blockchain technologies (blockchain-related currencies, e.g., Ethereum). Key terminology was that the privatization of the EHRs was carried out by authorized parties and outsourcing process of the

EHRs was integrated as a transaction inside the public blockchain. The EHRs could not make any modifications until the subsequent transaction was registered in the database, while the block chain-based currency provided a tamper-testing route for payments without the need for a central authority. Thus, any party can verify its legitimacy by checking the resulting transaction of the privatised EHRs. Performance analysis and safety review described the proposed framework with robust protection testing including increased efficiency.

In 2019, Nguyen et al. [4] has suggested a narrative framework for exchanging EHRs on such a mobile cloud network that incorporates blockchain as well as a shared interplanetary file system (IPFS). Specifically, a secure access management system has already been developed on the basis of blockchain technology to ensure protected EHR sharing between different patients and health care providers. In addition, a conceptual implementation on a smartphone device using Ethereum blockchain was introduced in a specific data exchange feature with Amazon cloud computing. The proactive results have shown that this research has offered an efficient approach to virtual clouds for reliable data sharing in the protection of critical health details against future threats. Security research and device optimization have demonstrated increased efficiency in lightweight network access architecture.

In 2020, Uddin et al. [5] has introduced Blockchain Integrated eHealth Infrastructure through three layers: 1) The Sensing Layer of Body Field Sensor Networks that contains medical sensors typical of a patient in or on a body that transmits data through a smartphone. 2) The Close computing layer of Edge Networks comprising of data sensing equipment of IoT equipment at a single jump. 3) The FAR application system of Core Networks includes cloud or other large storage facilities. The Patient Agent (PA) program distributed medical data on three layers to ensure safe, confidential and effective contact. The performance review of the unified eHealth model was analysed to demonstrate the feasibility of the structure in the collection and storing of RPM information.

In 2016, Yue et al. [6] has proposed a Software called Healthcare Data Gateway (HGD) blockchain-based infrastructure to enable patients to possess, exchange and monitor their data safely and conveniently without breaching privacy, providing an innovative way to improve the intelligence of healthcare facilities where private patient data remains. In this Model it has been ensured patients own and have full control of their healthcare data in a simple manner by using a simple unified Indicator- Centric Schema (ICS). New purpose-centric control paradigms have established that the individual manages and regulates the health data; a basic centralized Indicator-Centric Schema (ICS) allows it easy to coordinate effectively and conveniently all sorts of personal health data. It also found out that MPC (Secure Multi-Party Computing) was one of the exciting approaches for allowing untrusted third parties to participate in computing the patient data without violating privacy.

In 2020, Islam and Shin [7] have introduced a block chain-based, safe healthcare system whereby health data (HD) was obtained by users via the closest storage portal as well as the unmanned aerial vehicle (UAV). UAV first formed a partnership with either the body sensor hives (BSHs) with a token and exchanged key of BSHs to allow small-power safe communication. Since extracting the HD, the UAV decrypts that encrypted HD (BSH authenticated) by using a two-phase authentication method. After positive validation, the UAV transferred HD to the closest server to safely preserve it in blockchain. A safety review was explored to prove the viability of the new healthcare system. At last, the performance of both the conceptual system was examined via analysis and implementation. The protection and efficiency review have indicated that the new scheme promotes stronger BSH assistance although retaining stability.

In 2019, Chen et al. [8] have implemented a publicly accessible security system focused on blockchain for EHRs. The EHR database was built using complicated logic expressions and placed in the blockchain such that the data consumer could use expressions to scan the dataset. As only the database has been moved to the blockchain to allow dissemination, data holders have complete power of who will access their EHR details. The usage of blockchain technologies guaranteed the credibility, anti-tampering and quality control of the EHR database. Eventually, the design of the suggested system was measured on two factors, namely the overhead for the retrieval of record IDs from EHRs as well as the complexity for the operation of smart contract operations in Ethereum.

In 2019, Roehrs et al. [9] presented the introduction and assessment of a PHR model, which implemented public health information leveraging blockchain technologies and the transparent EHR interoperability framework. The Omni PHR architecture paradigm was adopted, defining an environment that facilitates the application of a centralized system interoperable PHR. This approach involved the creation of a prototype as well as the assessment of the synchronization and output of medical documents from various production sources. In addition to assessing the consolidated view of data, the assessment criterion often centered on non-functional capacity specifications, such as reaction time, CPU use, memory use, disk use and network use. In addition, research model was tested using a data collection of more than 40 thousand adult patients anonymized through two hospital repositories. Instantaneously, this results in an overall answer time of less than 500 ms. The blockchain deployed in this test was accomplished with such an availability of 98%.

In 2019, Tripathi et al. [10] described the rise of the healthcare sector being one of the most favored applications of IoT and its associated technology. The universal use, though, was only a vague sight. The main explanation for this was the confidentiality and protection of the data and the people concerned. To resolve this, blockchain technology has evolved as a practical way of enhancing encryption and privacy of data. In addition to smart healthcare systems (SHS), there will be various problems and concerns connected to the stability, accessibility and privacy of data and users. Research work examined the technical and social obstacles to the implementation of SHS through a study of traditional method, expert opinions and consumer expectations. It also introduced a blockchain-based SHS platform to maintain the system's intrinsic protection and legitimacy. At last, the potential directions for study and the usage of blockchain cases throughout the healthcare sector have already been addressed.

2. Comparison of different Blockchain based models and their challenges

Author [citation]	Methodology	Features	Challenges
Mubarakali et al. [1]	SEHRTB	Reduced latency Increased throughput	Intended to estimate the feasibility of the system
Omar et al. [2]	MediBchain protocol	Improved time consumption Satisfies all requirements	Need to explore interoperability between different entities of healthcare processes
Cao et al. [3]	TP-EHR	Safe against diverse existing attacks Pose practical and efficient communication and computation overhead	Further investigation needed to utilize the blockchain technology to enhance eHealth systems
Nguyen et al. [4]	Blockchain and IPFS	The sharing of medical data is exploited in reliable and quick manner	Further efficient management of e-health records on mobile clouds is needed in future
Uddin et al. [5]	Blockchain leveraged decentralized eHealth architecture	Ensure secure communication channel	Need to develop a dynamic storage selection algorithm
Yue et al. [6]	HGD architecture	Patients are aware of who is accessing their data Simple regulatory decisions about storing, and collecting sharing patient data	Further optimization concepts are needed for the effective management of data
Islam and Shin [7]	Blockchain-based secure healthcare scheme	Very much secure Lower power transmission Light security mechanisms	Need consideration in the privacy issue of HD

Table 1: Challenges and features of the models based on block chain for privacy preservation in healthcare system

Table I explains the features and challenges of the state-of-the-art models regarding the privacy preservation in healthcare system. More research works are exploited regarding this concept and the methodologies related with their works are explained with their pros and cons are explained as follows: SEHRTB [1] has reduced latency with increased throughput. Future work intends to estimate the feasibility of the system. MediBchain protocol [2] improves the time consumption and satisfies all requirements. However, need to explore interoperability between different entities of healthcare processes. TP-EHR [3] is safe against diverse existing attacks and poses practical and efficient communication and computation overhead. Further investigation needed to utilize the blockchain technology to enhance eHealth systems. Blockchain and IPFS [4] exploits the sharing of medical data in reliable and quick manner, yet further efficient management of e-health records on mobile clouds is needed in future. Blockchain leveraged decentralized eHealth architecture [5] Ensure secure communication channel and still Need to develop a dynamic storage selection algorithm. HGD architecture is the used methods in [6], in which the patients are aware of who is accessing their data and acquire Regulatory decisions about collecting, storing and sharing patient data become simpler. However, further optimization concepts are needed for the effective management of data. Blockchain-based secure healthcare scheme [7] is Very much secure with Lower power transmission and Light security mechanisms. But this model doesn't consider the privacy issue of the HD. Blockchain based searchable encryption scheme [8] is feasible and effective and is able to achieve a reliable and confidential search scheme. But it needs to evaluate it in a real-world environment.

CONCLUSION

In Conclusion, Challenges of Healthcare industry can be tackled with the Blockchain Technology. Its features decentralization, integrity, security, authentication principles and availability help Blockchain to solve the problems of healthcare systems. With the growing internet enabled technological advancements in healthcare like IoT, cloud, smart and sensing Devices to connect with world to serve the patients more efficiently risk of data breaches makes data sharing between hospitals difficult. Based on the survey in this paper, it is clear that blockchain has a tremendous potential to address a number of challenges of health industry. Blockchain can play very important role in privacy preservation due to its features of immutability. Patients can have ownership of their own data with the help of Blockchain Technology. In this paper we have also discussed potential research challenges like scalability, key management, security and research is to be carried out for real-life datasets. It is very much clear that blockchain has enormous potential for secure data sharing and privacy preservation.

REFERENCES

[1] AzathMubarakali, Subash Chandra Bose, Karthick Srinivasan, AmriaElsir& Omer Elsier," Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain", Journal of Ambient Intelligence and Humanized Computing, 2019.

[2] Abdullah Al Omar, Md ZakirulAlam Bhuiyan, Anirban Basu, ShinsakuKiyomoto, Mohammad Shahriar Rahman," Privacy-friendly platform for healthcare data in cloud based on blockchain environment", Future Generation Computer Systems, vol. 95, pp. 511-521, June 2019.

[3] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, Ferrante Neri," Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain", Information Sciences, vol. 485, pp. 427-440, June 2019.

[4] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019.

[5] Md. Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, Venki Balasubramanian," Blockchain leveraged decentralized IoT eHealth framework", Internet of Things, vol. 9, March 2020, Article 100159.

[6] Xiao Yue, Huiju Wang, DaweiJin, Mingqiang Li & Wei Jiang," Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, vol.40, Article number: 218, 2016.

[7] Anik Islam, Soo Young Shin,” A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things”, Computers & Electrical Engineering, vol. 84, June 2020, Article 106627.

[8] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, Nan Zhang,” Blockchain based searchable encryption for electronic health record sharing”, Future Generation Computer Systems, vol. 95, pp. 420-429, June 2019.

[9] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, Douglas C. Schmidt,” Analyzing the performance of a blockchain-based personal health record implementation”, Journal of Biomedical Informatics, vol. 92, April 2019, Article 103140.

[10] Gautami Tripathi, Mohd Abdul Ahad, Sara Paiva,” S2HS- A blockchain based approach for smart healthcare system”, HealthcareIn press, corrected proof, Available online 19 November 2019, Article 100391.

[11] Ado Adamou Abba Ari, Olga KengniNgangmo, ChafiqTitouna, Ousmane Thiare, Abdelhak Mourad Gueroui,” Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges”, Applied Computing and Informatics, In press, corrected proof, Available online 22 November 2019.

[12] Tiago C. S. Xavier, Igor L. Santos, Flavia C. Delicato, Paulo F. Pires, Claudio L. Amorim,” Collaborative resource allocation for Cloud of Things systems”, Journal of Network and Computer Applications, vol. 1591 June 2020, Article 102592.

[13] Antonio Celesti, Davide Mulfari, Antonino Galletta, Maria Fazio, Massimo Villari,” A study on container virtualization for guarantee quality of service in Cloud-of-Things”, Future Generation Computer Systems, vol. 99, pp. 356-364, October 2019.

[14] G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarné,” Using trust and local reputation for group formation in the Cloud of Things”, Future Generation Computer Systems, vol. 89, pp. 804-815, December 2018.

[15] Yuan Tian, Mariya M. Kaleemullah, Mznah A. Rodhaan, Biao Song, Tinghuai Ma,” A privacy preserving location service for cloud-of-things system”, Journal of Parallel and Distributed Computing, vol. 123, pp. 215-222, January 2019.

[16] Xiaolong Xu, Shucun Fu, Lianyong Qi, Xuyun Zhang, Shancang Li,” An IoT-Oriented data placement method with privacy preservation in cloud environment”, Journal of Network and Computer Applications, vol. 124, pp. 148-157, 15 December 2018.

[17] Abdu Gumaei, Rachid Sammouda, Abdul Malik S. Al-Salman, Ahmed Alsanad,” Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation”, Journal of Parallel and Distributed Computing, vol. 124, pp. 27-40, February 2019.

[18] Pan Jun Sun,” Security and privacy protection in cloud computing: Discussions and challenges”, Journal of Network and Computer Applications, In press, journal pre-proof, Available online 4 April 2020, Article 102642.

[19] Hui Tian, Fulin Nan, Chin-Chen Chang, Yongfeng Huang, Yongqian Du,”

Privacy-preserving public auditing for secure data storage in fog-to-cloud computing", Journal of Network and Computer Applications, vol. 127, pp. 59-69, 1 February 2019.

[20] NureniAyofe Azeez, Charles Van der Vyver," Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", Egyptian Informatics Journal, vol. 20, no. 2, pp. 97-108, July 2019.

[21] Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen," Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", Future Generation Computer Systems, vol. 97, pp. 512-529, August 2019.

[22] Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H. Deng," A blockchain-based location privacy-preserving crowdsensing system", Future Generation Computer Systems, vol. 94, pp. 408-418, May 2019.

[23] Qi Feng, Debiao He, SheraliZeadally, Muhammad Khurram Khan, Neeraj Kumar," A survey on privacy protection in blockchain system", Journal of Network and Computer Applications vol. 126, pp. 45-58, 15 January 2019.