Survey On Use Of Blockchain Technology In Cloud Storage for The Security Of Healthcare Systems

Etikala Aruna [a], Dr. Arun Sahayadhas [b]

[a] Research Scholar of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai
[b] Professor of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai

[a]arunae.phd@velsuniv.ac.in, [b]arun.se@velsuniv.ac.in.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: The security has been the need of the hour in health care systems with so much of electronic health records. The cloud not assured to provide security as it is involved the parallel processing and is in distributed nature. The Blockchain (BC) has been introduced in the cloud for some applications like smart healthcare systems since they are highly susceptible on some security violations and several attacks, such as forgery, tampering, privacy leakage, etc. to provide the protection and security for the medical data. Thus a survey on use of Blockchain (BC) technology in cloud storage for the security of healthcare systems is presented in this paper. At first the security measures provided by the traditional cloud storage system are discussed along with its limitations. Then a brief introduction of Blockchain technology in cloud storage with its background work is presented. Finally survey of different works focused on blockchain technology in the healthcare systems is presented as a promising solution for the security issues to provide tightened and enhanced security levels over the health care systems. A potential solution can be provided by this survey with the use of blockchain technology for the protection of healthcare data outsourced over the cloud. By evaluating and comparing the simulation experiments of presented Blockchain technology focused works, it can be prove that a verification of integrity with cloud storage and medical data, data sharing with less computing complexity, and security and privacy protection are achieved.

Keywords: Blockchain technology, Cloud network, Health care systems, Security measures.

I. INTRODUCTION

Since health caring is the most significant part for every people, the health care data such as prescriptions, previous health records, etc. have become essential to secure them for diagnosing the patients also for the future reference purpose. Initially, this health care data was used to record manually on the paper. There were many chances to get modify and damage the data in this method. Storing of the healthcare data electronically is therefore essential one. But there is possibility of permanent tampering or deleting of healthcare databases so in this also facing the challenges of information blocking. This information blocking incurred when the medical data, that should not have to see without concern of the patients or hospitals, accessed by entity such as a person with or without intention of accessing. Whether in improving the quality or in solving the problems of resource allocation in addition to the information blocking, a very important role can be played by the technology. It is involved with the time especially in the sharing technology of healthcare data through cloud [1]. Cloud computing technology also has an increasing privacy and security challenges even though it enjoy all the success with its available services. Therefore, deploying of security policies and procedures for the cloud environment has been focused by the various multinational companies in prior of using it for their business solutions [2]. Hence, constant sustaining of trust from the clients about the data security along with its privacy outsourced over the cloud environment became most essential for the cloud service providers. The distributed and decentralized security policy requirement is underlined in the cloud environment as of its limitations. Therefore the Blockchain (BC) technology is taken as a best system for the security to delpoy in the cloud architecture due to its nature of distributed network and great interconnectivity with the cloud [3]. Furthermore, popularity of the blockchain technology can be reinforced as a most suitable system in a security point of view for a cloud environment because of fact that it can communicate at a faster rate and can utilize very less number of computational resources. In the security of this blockchain technology, the distributed data ledger can't be updated or deleted once the details of transaction entered in it and updated. Even though this distributed data ledger is shared over cloud environment among the all nodes a high immutability and the best security of data can promoted. The data privacy is preserved probably within a better way in the blockchain as the blocks contain it utilize the cryptographic techniques. Such aspects make the blockchain as a best candidate in providing data security for deployment in cloud environment. In this paper a survey on this blockchain technology over the cloud environment for the secure healthcare data sharing is presented.

II. CLOUD SECURITY SYSTEMS

In building the smart hospitals, it has been became a more priority every time to accurately record the medical data regarding the diseases of patients or the previous medical records and to store as well as share the medical data securely for the protection patient's privacy data. A secure access policy is designed and implemented in the conventional data access control policy along with a server that absolutely reliable makes difficult to adapt the distributed network environment in this modern days. Blockchain given a new idea to the people as the end-to-end reliable communication, encryption algorithm, consensus mechanism and distributed data storage because it well known for decentralization and security. Attribute based Encryption (ABE) has become a significant technology over the recent days for the security requirements in the cloud environment. Moreover, the access control policy of ABE under the cloud environment has also been extensively studied [4]. A mechanism that links users to the cipher texts via attributes should necessary in attribute base encryption mechanism since it uses a public key as an attribute. It significantly improves the security of data storage under the cloud by its flexible encryption and access control schemes. For the meantime, it became an important access control scheme for securing the cloud data storage in addition it achieves fine grained access. The conventional ABE however does not fully guarantee about the privacy of data, effective prevention from collision attack or assurance of attribute revocation-based forward and the backward security also has caused huge computing costs by the revocation. Thus, employing the blockchain technology and implementing its security mechanism to the cloud environment would become an important part of research to improve the data storage security and cloud computing performance. The inconsistency between the data privacy and the data sharing can be solved by integrating the blockchain and cloud computing as well as an adequate security strategy [5].

2.1 Limitations of existing cloud security systems

It can be observed from the previous section that the distributed nature is not there in majority of the security system adopted for the cloud environment. However, the cloud computing has inherently a distributed nature then consecutively the data flow also distributed nature over this cloud environment. This makes it very critical in order to deploy the existing security schemes over cloud computing environment. Those security schemes in addition have a less transparency. Data is mutable through this existing security schemes at a large extent which means that each participating node can easily change the data. Existing security schemes simultaneously require a lot of resources and are very expensive.

2.2 Block chain

Since from the few recent years, blockchain technology has been researched comprehensively. This blockchain technology was introduce as a supporting mechanism for the digital crypto-currency called as Bitcoin [6]. A basis for collaboration between the strange and undependable things can be provided through the basic model of the blockchain technology as similar to the present cloud computing and it can also support a widespread features of mobile or smart health devices without any requirement of central security and authentication authority. This underlying technology is based on the data record called as an immutable "public-ledger" that shared by all of the participants. A block of data associated with the usage of cryptographic hash key is contained in this public-ledger record. This process of consensus or process of linking is known as Proof of Work (PoW). For the manipulation of data both consensus and ledger are inherently unaffected. Since earlier block hashes in blockchain are cancelled also consensus between the nodes is violated by the block data, it can't be changed post-fact.

2.3 Blockchain Background study

This Blockchain has been not just being limited to the financial sector but also extend further than bitcoin and up to the public healthcare and many of other applications. One of the promising subjects that have been focusing recently is the blockchain technology based medical systems. The total medical data created should be reliable must necessary to verifiable and must not be tampered. There should be a requirement of ability to verity the correctness of data by the researcher or patient of patient's relatives or any of the other users who needs it. In order to share the data with a specific security various researchers tried to integrating the blockchain technology with the other different technologies. Several number of researchers integrated the various technologies with the block chain, one of such used technology application is the identification of radio frequency with blockchain in the agro food supply chain monitoring field [7]. Some of such other applications are blockchain together with IoT, blockchain in vehicular ecosystem, blockchain in smart contracts, etc. Following figure (1) shows the typical diagram of block chain.

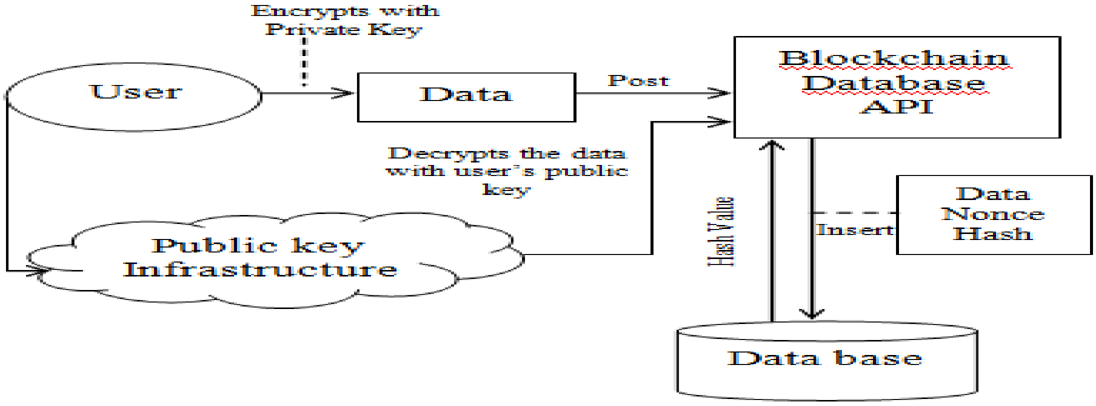

Encrypts with Private Key
User
Data
Post
Blockchain Database API
Decrypts the data with user's public key
Public key Infrastructure
Hash Value
Insert
Data Nonce Hash
Data base

Fig. 1: TYPICAL BLOCKCHAIN DIAGRAM

III. SURVEY ON BLOCKCHAIN SECURITY IN HEALTH CARE SYSTEMS

3.1 Blockchain and smart healthcare

This work focused on the blockchain technology application in the smart healthcare systems. From the few recent decades, the serious concern has been there in the healthcare service systems about the cyber attacks. There is an ultimate challenge on the privacy and security about the medical data of the patients due to the failure of existed infrastructure in providing security against such data violations. Another gap is opened by the currently implemented smart healthcare record models into a difficult situation, i.e. data of the patients being in the supervision of health organizations, putting the information of patients into risk and making the data transfer regarding the healthcare of patients inefficient. For an instant, chance of delay in treatment to due to the only reason of more time taken by the transfer of patient's health information from one service provider to other service provider. Blockchain technology can be useful to overcome these limitations in EHR which has them practically. Several private, government and public private partner projects have adopted this blockchain technology over the recent days. When this blockchain technology was focused by the United States Food and Drug Administration (FDA) as well as IBM Watson Health to for protecting of the oncology related data, its potential advantages in the healthcare field were became apparent.

This blockchain allows for the collection of data from a variety of sources and a transaction audit log is used to save this data. This transaction audit log can eventually help to keep track of data ownership and transparency of data during the data exchange period. From the FDA and IBM it can be believed that the blockchain does have an ability to support the exchange of data for which various sources are considered for collection of data with patients consent and mutually agreed terms. The models currently implemented are based on passwords consisting of secret data which must be exchanged also stored in the cloud is unreliable and less secured. Handling of the accessing the healthcare data with precautions is also has a huge importance. In the similar way, ensuring the data integrity has also required a certain standardized auditing. The data integrity, privacy, and secured storage and reduced chances of data violations are provided with the block chain. In addition, since this blockchain technology stores data in a distributed nature, single-point-of-failure is also mitigated.

3.2 Blockchain integrated with cloud computing in healthcare

A blockchain integrated with the cloud computing based distributed healthcare data privacy protection scheme is focused in this paper with the aim of addressing indefinite question carried by smart hospitals for the secure sharing of health data and privacy protection of patient's healthcare information. In other words the introduced scheme is a cloud computing model along with the distributed blockchain based data management architecture more specifically for the smart hospitals guaranteeing the efficient blockchain operation and reduction in the computing load on the user side by using the consortium chain on the blockchain in it. The definite access control schemes can be provided to the users by using the proxy re-encryption and ABE technologies in addition to address the very complex computing incurred with encryption. Exchange of patient's healthcare information securely among each physician can provide by the each status and attribute based user access. The total health care data is encrypted at the side of response. At the request side, nodes in the cloud process the transferred healthcare data to receive and sent back the final cipher text. In other words, proxy re-encryption and data sharing with the rules for privacy protection by the participation of service side of cloud environment is designed in this work that solved the challenges of secured data storage and sharing of information among smart hospitals largely.

3.3 Blockchain based EMR, EHR, or PHR eco system

This paper focused on working of blockchain based Electronic Medical Records (EMR), Electronic healthcare Records (EHR), or Personal Health Record (PHR) ecosystem. Recently, there has been an interest in using the blockchain technology which was popularly known from the successful Bitcoin to provide the secure management of healthcare data. Blockchain is generally a technology that allows building of an online database with an open-ended and distributed nature consisting of a data block such as the list of data structures that are linked with one and each other that means a block is pointed by the previous block following one, thus named as block chain. Over the different nodes in infrastructure, such blocks are in distributed and not stored centrally. The transaction information, timestamp of block production and previous block's hash are contained in the every block along with the healthcare data of patients as well as information of healthcare provider in our perspective. This blockchain based EMR, EHR or PHR conceptual ecosystem is described from the following figure (2). A new block is generated and distributed among the all end-nodes in a patient network including patients, their relatives and their doctors especially once new created a healthcare data regarding the particular patient. This new block will be added to the chain after approving by the most of its end nodes, which allows obtaining a verifiable, lasting, and efficient way of medical history of patients in a comprehensive view. The chain creates a fork when not reached the agreement and the block is not belonging to the main chain called as an orphan. There is no chance of changing the data in one block when a new block is added to the chain without changing of all consequent blocks. On other hand change can be easily recognized. Before the data presenting in to block, healthcare data must necessary being protected since the contents of block is accessible publicly. Conceptually, blockchain is inherently secure and offers the ability to achieve decentralized consensus and consistency, as well as resistance to deliberate and / or unintended attacks.

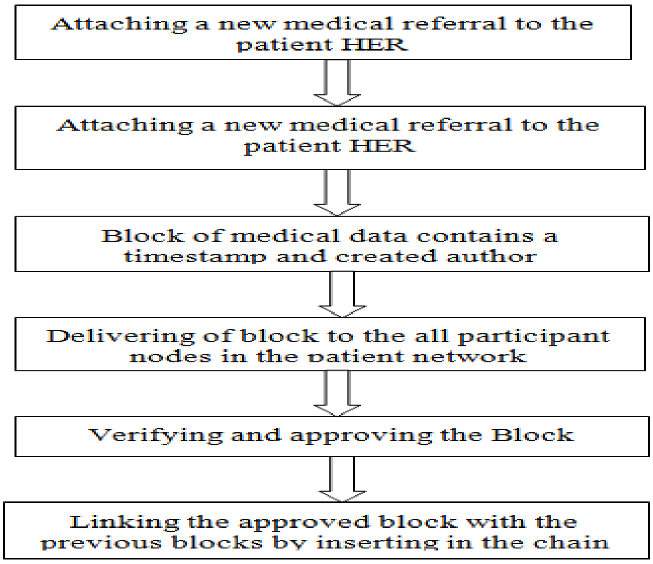

Attaching a new medical referral to the patient HER
Attaching a new medical referral to the patient HER
Block of medical data contains a timestamp and created author
Delivering of block to the all participant nodes in the patient network
Verifying and approving the Block
Linking the approved block with the previous blocks by inserting in the chain

Fig. 2: blockchain based EMR, EHR or PHR conceptual ecosystem

The main advantages of implementing this type of blockchain approach avoiding of the blockage performance and a single-point-of-failure as the agreement reached without the involvement of a trusted mediator, controlling on the data by patients, a complete, accurate, timely, consistent and easy distributed of healthcare information as blockchain data, changes in blockchain are noticeable to the total members of the patient network, and all data insertions are immutable.

IV. RESULTS

The performance of the blockchain method is evaluated using a set of data collection. Similar dataset is used for each work to acquire accurate and common results with verifying the time consumption for accessing the EHR and time complexity in terms of processing time. The dataset considered for the experiment has a collection of EHRs consisting information regarding treatment and medicines of different patients that should not to share. The privacy data of patients such as medicinal, treatment and financial information can be misused by the other healthcare institutes, insurance companies and other competitors as they available from the place where they fetched. According this dataset, the processing time and time complexity are verified and compared for all the technologies of cloud, cloud with authentication schemes, blockchain and cloud integrated with blockchain technologies.

The time consumption attained by the different technologies presented in this survey paper is compared as shown in figure (3). As seen from figure (3) it can be notice that the blockchain technology and cloud integrated with blockchain technology has acquired low time consumption with the increasing of file size for processing of EHR data compared to the traditional cloud computing and cloud with authentication technologies. That means it can be said that blockchain technology offers better performance than others.

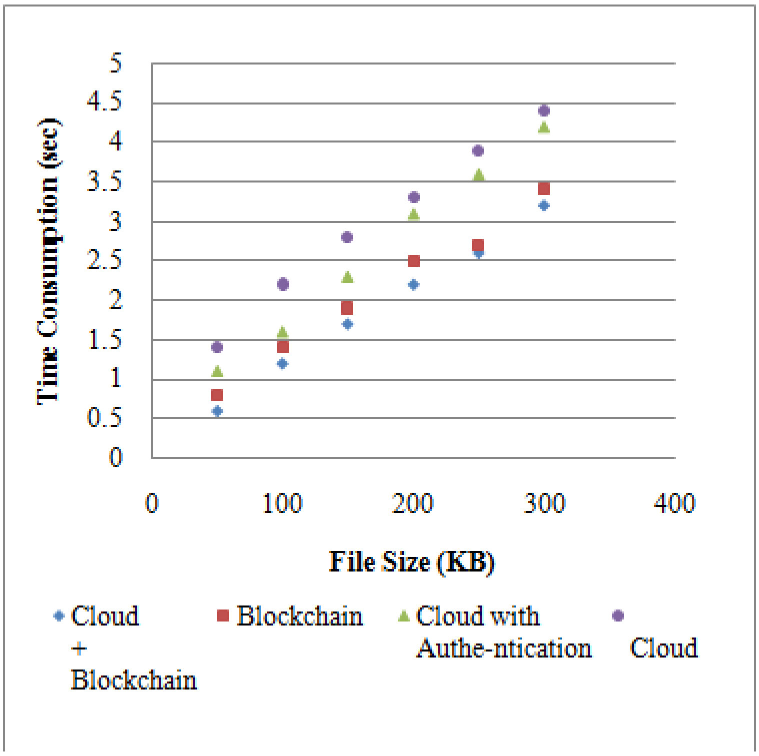


Fig. 3: Time consumption for electronic health records access

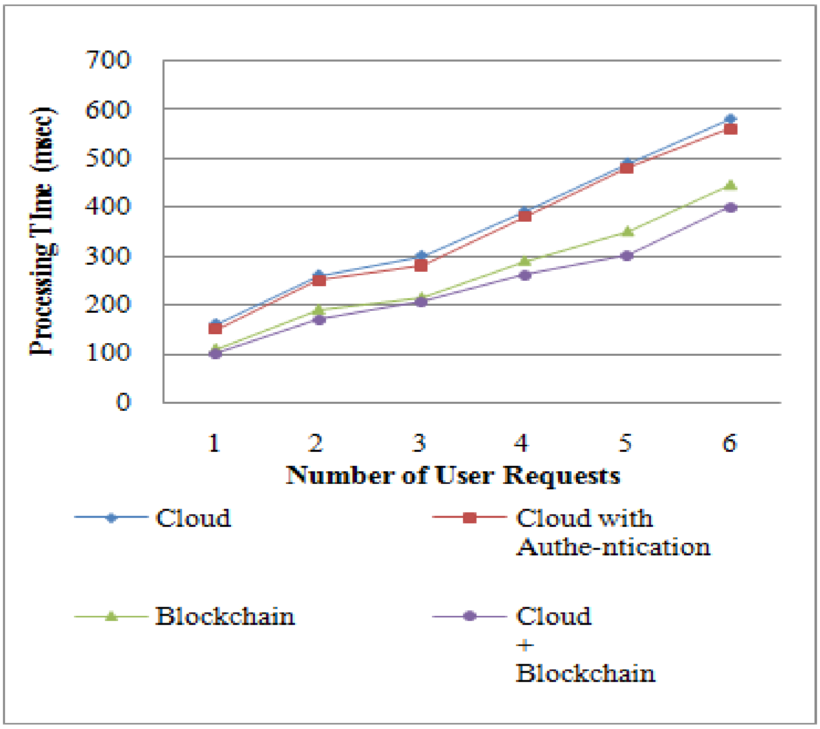
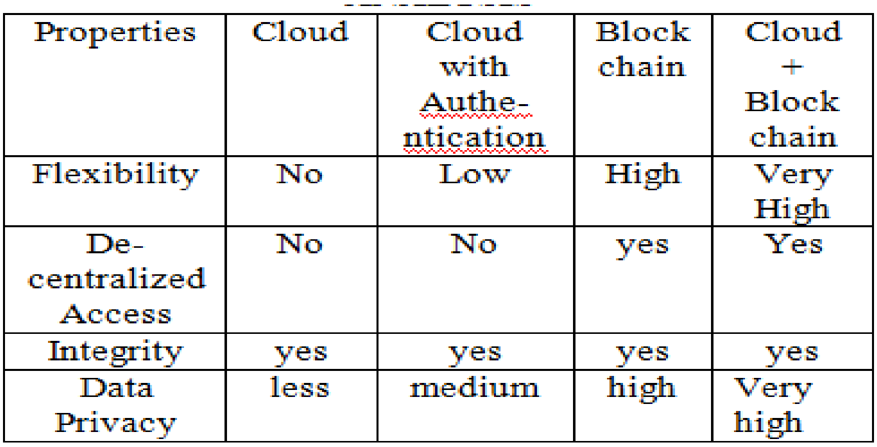


Fig. 4: Time complexity COMPARISION GRAPHS with respect to processing time

Similarly, Figure (4) shows the comparison of time complexity attained by the different technologies with respect to the processing time. A less time complexity is achieved for the blockchain technology and cloud integrated with blockchain technology than the other two traditional cloud based technologies.

Table 1: Comparison of Performance analysis



Properties	Cloud	Cloud with Authe-ntication	Block chain	Cloud + Block chain
Flexibility	No	Low	High	Very High
De-centralized Access	No	No	yes	Yes
Integrity	yes	yes	yes	yes
Data Privacy	less	medium	high	Very high

Furthermore, the overall performance of such four technologies are evaluated and compared with respect to their data accessing and security features as depicted in table (1).

V. CONCLUSION

Now a day, smart healthcare systems have facing many critical security and privacy challenges. So it is necessary to understand the security requirements of those systems in order to minimize such challenges. Also, there was a concern on information blocking. Some works that focused on healthcare data security based on blockchain technology are reviewed in this paper with an appropriate study. The privacy and storage security issues in the cloud environment are additionally focused in this paper. Then from the total experiment results, it was concluded that the blockchain technology offers an efficient and effective security performances than the traditional technologies.

REFERENCES

[1] Yongfeng Qian, Kai Hwang, Min Chen, Shiwen Mao, Long Hu and Jing Chen, “Privacy Protection and Intrusion Avoidance for Cloudlet-Based Medical Data Sharing”, IEEE Trans., on Cloud Computing, Vol: 8, Issue: 4, 2020.

[2] Udaya Tupakula and Vijay Varadharaj, “Securing Services in Networked cloud Infrastructures”, IEEE Trans., on cloud Computing, Vol: 6, Issue: 4, 2018.

[3] Mingtao Ni, Bo Zhao and Peiru Fan, “Mchain: A Blockchain-Based VM Measurements Secure Storage Approach in IaaS Cloud With Enhanced Integrity and Controllability”, IEEE Access, Vol: 6, 2018.

[4] Zhenfu Cao, Lifei Wei, Jianting Ning, and Xiaolei Dong, “White-Box Traceable CP ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively”, IEEE Trans., Depe., & Sec., Comp., Vol: 15, Issue: 5, 2018.

[5] Emmanuel Boateng Sifah, Xiaojiang Du, Mohsen Guizani, Qi Xia, Jianbin Gao and Kwame Omono Asamoah, “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Block chain”, IEEE Access, Vol: 5, 2017.

[6] Kouichi Sakurai, Sushmita Ruj and Samiran Bag, “Bitcoin Block Withholding Attack: Analysis and Mitigation”, IEEE Trans., Infor., Fore., & Secu.,, Vol: 12, Issue: 8, 2017.

[7] Sk Md Mizanur Rahman, Hadeal Abdulaziz Al Hamid, Atif Alamri, M. Shamim Hossain and Ahmad Almogren, “A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography”, IEEE Access, Vol: 5, 2017.

[8], Tianyi Xu, Ruiguo Yu, Jie Gao, Jianrong Wang, Yongli An, Mei Yu, and Gong Zhang, “Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network”, IEEE Access, Vol: 5, 2017

[9] Ning Ye, Tianhe Gong, Yi Dou Ruchuan Wang and Haiping Huang, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System", IEEE Trans., on Ind., Info.,, Vol: 13, Issue: 3, 2017

[10] Ing Ray Chen and Hamid Al-Hamadi, "Trust-Based Decision Making for Health IoT Systems", IEEE Internet of Things Journal, Volume: 4, Issue: 5, 2017

[11] F. Tian, "An Agri-Food Supply Chain Traceability System for China Based on RFID & Blockchain Technology", Kunming, China, IEEE, 2016.

[12] Arsalan Mohsen Nia, Susmita Sur-Kolay, Anand Raghunathan and Niraj K. Jha, "hysiological Information Leakage: A New Frontier in Health Information Security", IEEE Transactions on Emerging Topics in Computing, Volume: 4, Issue: 3, 2016

[13] Vijay Varadharajan, Lan Zhou and K. Gopinath, "Secure Role-Based Cloud Storage System For Encrypted Patient-Centric Health Records", The Computer Journal, Volume: 59, Issue: 11, 2016

[14] Ximeng Liu, Rongxing Lu, Jianfeng Ma, Le Chen, Baodong Qin, "Privacy-Preserving Patient-Centric Clinical Decision Support System on Naïve Bayesian Classification", IEEE Journal of Biomedical and Health Informatics, Vol: 20, Issue: 2, 2016

[15] Marcos A. Simplicio, Leonardo H. Iwaya, Bruno M. Barros, Tereza C. M. B. Carvalho, and Mats Näslund, "Secour Health: A Delay-Tolerant Securiy Framework for Mobile Health Data Collection", IEEE Journal of Biomedical and health Informatics, Volume: 19, Issue: 2, 2015.