ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse84862019.pdf
https://doi.org/10.30534/ijatcse/2019/84862019

PHR System using Blockchain Technology

Sang Young Lee[1]
[1]Namseoul University, South Korea, sylee@nsu.ac.kr

ABSTRACT

PHR is easy to check patients' health condition, which is suitable for the customized medical service. However, the EMR systems were made of different type in each medical institute, thereby being difficult to integrate the information into PHR. A Cloud is an appropriate alternative because it has easy environment where the integrated PHR is easily built and processed while keeping the system under various EMR systems. The concept of the current medical paradigm has been changing from treatment to management. For the management, it is important to know current health condition, but the existing diseases and their treatment processes. The environment of medical information is shifting from recording and to saving into PHR which is an integrated record of EMR information and subsidiary patients' health information. PHR is very easy to check patients' health condition, which is suitable for the customized medical service. This study provided how to apply blockchain technology to the medical field and utilize it for PHR applications. For these applications, it suggested an architecture for gateway application of healthcare date to control and share PHR data more easily and securely.

Key words : PHR, Blockchain , Healthcare, Framework.

1. INTRODUCTION

With constant advance in IT technology, there have been various healthcare devices and services. A number of companies have provided the new healthcare value to doctors and patients using state-of-art technology such as sensor, smartphone, wireless communication, etc. In this trend, there have been growing efforts to take care of oneself and prevent disease by using smart IT devices, including smartphone, health device, and others, not only for patients but for the healthy people. In other words, interest in and usage of Personal Health Record (PHR) are growing more and more[1, 2].

PHR is for all information relating to personal health. Also, it is a concept that includes personal healthcare services, health information, healthcare platforms. Its previous systems were Electronic Medical Record (EMR) and Electronic Health Record (EHR) that are medical information systems. While EMR is created and utilized in a single medical institution, HER is utilized in several medical institutions that comply with national standards for interoperability[3, 4]. Private medical information stored on EMR and HER is an important part of PHR. PHR has been evolved from the initial model that checks and share the integrated personal information scattered across a wide range of institutions and devices. And now, it has been developed as a model to provide useful services such as disease prevention and follow-up management connected with self-care, medical institution, and insurance company[5, 6, 7].

In general, PHR is a "tool which provides a function to keep and manage entire health information of individuals or families throughout their lifetime. Google Health is a web platform to provide a free service developed by Google. With the platform centrally managed PHR, a patient is able to retrieve medical information and share it with his/her doctor. In addition, the patient can edit and store medicine information, insurance-related information, medical records, etc. with the computer at his home. To be specific, it can be used to input user's PHR, provide health information relating to PHR (symptoms, causes and treatments), upload PHR information via medical institutes, check drug interactions, search doctors/hospitals and so on[8, 9, 10].

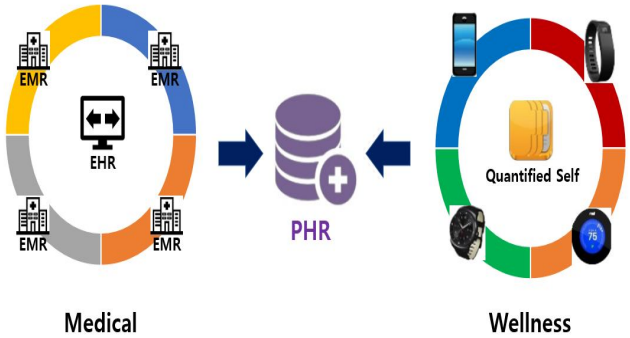

Figure 1 : Structures of PHR

The modern paradigm for healthcare has been changing from treatment to management. For the management, it is important to record information not only about diseases and their treatment processes but about routine and periodic health conditions. The environment of medical information is shifting from recording and saving into EMR system to saving into PHR. PHR is very easy to check patients' health condition, which is suitable for the customized medical service. However, the EMR systems were made of different type in each medical institute, thereby being difficult to integrate the information into PHR[11, 12]. A Cloud is an appropriate alternative because it has easy environment where the integrated PHR is easily built and processed while keeping the system under various EMR systems. Also, medical information is one of the sensitive information, and its security/safety problems can be resolved by the blockchain. If PHR is built in the Cloud using the blockchain, the medical system can be maintained, and the medical information can be widely applied. Moreover, the algorithm for data distribution processing using blockchain was applied for the high cost of managing data for each individual under the Cloud environment. This method minimizes the cost that are passed on to each person. In doing so, the medical information system is constructed, which will help provide a positive impact on medical world and suitable medical services[13, 14].

Accordingly, this paper suggested a framework that is able to complete PHR system, using blockchain technology. This paper consists of the following contents. At first, there are relevant researches in Chapter 2. Chapter 3 is about standards for PHR. Chapter 4 contains PHR that uses blockchain technology. Finally, the goal of Chapter 5 is to provide a conclusion.

2. RELATED WORKS

Blockchain is a data structure, which is composed of block lists connected with chains. Such blockchain is distributed through peer to peer (P2P) networks with the latest version of all nodes. The block is a record of transaction data. Blockchain based on Bitcoin is one of distributed ledger technologies, which is a distributed, shared, and encrypted-database that serves as an "irreversible and incorruptible repository of information". The block includes header and body[15, 16].

- Version of Block: It represents validation rules that are based on a series of blocks.
- Parent Block Hash: It is 256-bit hash speed.
- Merkle Tree Root Hash: Hash of all the hashed of all the transactions.
- Timestamp: Currently, it represents the value for every second.
- nBits: it consists of simple target hash.
- Nonce: It is a 4-byte field, which starts at 0 and is incremented for each hash.

Figure 2 shows structures and elements of blockchain.

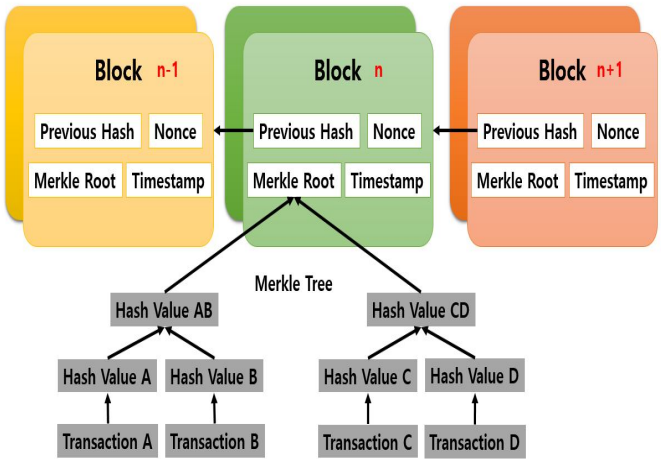

Figure 2 : Structures and Elements of Blockchain

In the health-related fields, one of the typical applications of blockchain is the electronic medical record. This area is categorized into three different types: electronic record-centered EMR, interchange-centered HER and private health record-centered PHR. In these fields, main researches have been conducted to manage private medical or health-related data for generation and storage of electronic documents. In practice, for blockchain in EMR, there have been various case studies carried out mainly on decentralization and immutability of blockchain, data source, reliability, rigidity, contract, and security and privacy. This study focused on how to easily share patient-centered data in studies on blockchain application in diverse medical services to store and manage patients' EMR. Especially, studies have been conducted to build medical platform that is able to control patients' method and to share, process, and utilize the data[17, 18, 19, 20].

In particular, for the application to manage healthcare data, blockchain has been introduced to apply the perfect technology in order to design a medical system. For easy and safe control to share data, this study suggested an architecture for gateway applications of the healthcare data. In short, it was to suggest the blockchain technology using the multi-step authentication which may protect and share medical data between different objects[21. 22, 23]. Also, it suggested research scenarios relating to biometric and biomedical systems for security of medical data. In this study, Ethereum-based smart contract system was proposed to intelligently protect private medical records

3. PHR AND STANDARDS

The PHR-related standards are categorized into three types of exchanges via Personal Health Device (PHD), medical information device, and Internet of Things (IoT) device. Firstly, the PHD standard was established in Institute of Electrical and Electronics Engineers (IEEE) 11073. It has been the ISO international standard in accordance with Standard Harmonization between International Organization for Standardization (ISO) and IEEE. ISO/IEEE 11073 PHD Group is continually enacted the device standard for individual's health based on ISO/IEEE 11073-20601 which is a standard protocol to measure and transmit personal biometric information.

PHR-based medical information exchange is required to transmit private health information such as medical records, test results, etc. It is classified as shown in the following figure.

This includes standards of terms, code system, protocol and medical documents in the health and medical information field. For the term and code system, there are various kinds of standards: SNOMED-CT and UMLS are for the definition of terms, LOINC for test code, ICD for diagnostic code, and RxNorm for medicine code. For the protocol, there are standards: V2 and V3 of HL7, message standards, are for exchange of medical information, DICOM for sending medical images, CCD of HL7 and Consolidated CDA for medical documents. For IoT, the standardization that is related to healthcare, including PHR, is on the way. OIC created the Healthcare Task Group and started to develop a standard of healthcare applications and services in IoT environment. In 2018, oneM2M held an operation showcase by interlocking IoT standard platform and existing healthcare standard. Recently, with the development of various IoT devices, including wearable devices such as activity tracker, heart rate measurement, etc., sleep monitoring device, smart home device and so on, it is expected that there would be active discussions on establishment of PHR-related healthcare standard for the future IoT.

Unlike the current system that uses the provider-centered EHR for management, PHR is a patient-centered application program that is managed and used by the patient. The real owner of the information accesses and manages his own health information. The ultimate goal of PHR is to help patients securely and conveniently collect, track, and control their perfect health conditions. Also, the information provider manages hospital visit data, vaccination records, prescription records, physical activity data collected from the smartphone devices. From the PHR, patients can use their own health information and control how to share the information. They can keep accuracy of their own health record and prevent potential errors of the data. Existing companies, such as Apple and Microsoft, have been trying the centralized management through solutions like Apple Health and Microsoft HealthVault. However, such approaches do not solve the problem to share key data, so they would also face similar obstacle of the heterogeneous EHR system. On the other hand, blockchain is possible to distribute the controlled data. This study uses an algorithm agreed by various participants. For the participants, it guarantees widespread access and secure data distribution. Additionally, the patients can manage health data with a personal smart device via a service that is connected to the existing health system. Medical professionals have the following advantages:

- they control data access;
- they know the source of data;
- they'll let the patient know when the provider accesses to the data;
- its data log always transparent to the patient; and,
- the patient can search his own health information anytime or anywhere.

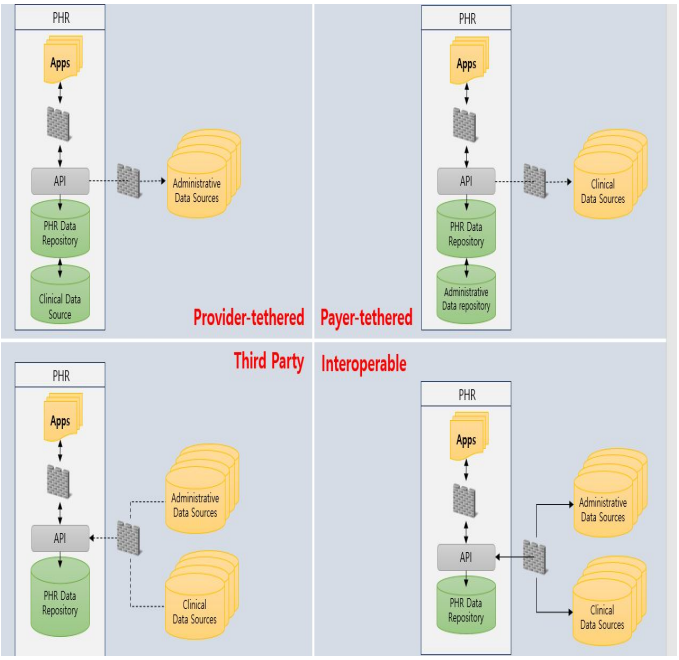

Figure 3 : Elements of Blockchain

PHR is defined as an internet-based tool that allows a person access to his own health information all his life, for the people who need specific information. PHR will improve the quality of medical care because medical service users can make a better decision, it enables easier access to the required information, and it makes patients and medical teams communicate more effectively.

4. PHR USING BLOCKCHAIN

Blockchain is a form of "distributed ledger, which stores a copy of trade in a computer system where different individual or corporate has controlled". In other words, ledger, storing trade information, is saved in a digitalized unit of 'block'.

Block consists of body and header for storing trade information and cryptic code, respectively. Such blocks are distributed to the computer node of network participants, which is all block system. It functions as a mechanism of chain that if any new trade or changes in an existing trade, a new block is created and connected to the existing block system. An operational structure of the distributed ledger is determined and operated by a pre-established consensus algorithm.

In the blockchain system, blocks with a form of information are connected to each other according to chronological order. The information input is not only saved in the corresponding block, but also uploaded in all network of P2P where the user wants to create a block. Once such information was verified by all users, the block is connected. The information of the created blocks is shared with the corresponding users. All types of information have been shared with all users. So, if someone wants to modify any codes in the blocks with a bad aim, it is not possible to change it without the permission of others. As a result, information gets more perfect structure along with the algorithm.

Blockchain utilized by Bit Coin or Ethereum was a form of permissionless type, but currently, permissioned blockchain has also proposed. A type of permissionless creates blocks by proof of work and mining process with no limitation of users. On the other hand, the permission form is operated by only authorized users without the mining process. The use of permissionless blockchain not only requires more time to upload block, but also manages the network users. Regarding construction of medical information system, permissioned blockchain is the most optimum configuration with advanced technologies for information integrity.

Blockchain technology has a lot of potentials to change Trust model in various industrial areas and business processes innovatively. However, technologies of blockchain have been restricted in reality. For instances, manufacturing industry does not want to share their independent technologies with other companies and the financial industry does not want to leak out customer's information. On the other hand, the industries in distribution, insurance and medical areas have expected to introduce blockchain technology into their business. If blockchain technology is introduced to distribution business, loss or damage of products could be minimized due to the trackable delivery routes. The origin of the product is also identified clearly. In the case of the insurance industry, new product fitted to the individual is designed on the basis of an accident rate of individual, incidence of diseases, and lifestyle, resulting in a decrease of unnecessary loss of cost.

In the field of medical business, accurate treatment has been made by managing detailed information such as, medical history, history of the accident, constitution, and medical history, providing better medical care. Moreover, the cost for unnecessary tests could be minimized through this management system, which reduces the patient's financial burden and increases the confidence of medical treatment. It is expected that blockchain technology brings innovative changes in diverse areas such as health care, distribution, insurance and medical field.

A construction method of PHR system, based on blockchain, is indicated as followings. A function of PHR should be implemented due to the fact that security is the most important parameter. In this study, it has been operated by an authorized author in Cloud-based system exclusively for users (medical institutions and patients). They are able to be provided a private key for individually secured login. The system enables users to process the data by creating API (application program interface), resulting in user's flexible data size. Cloud consists of a few layers, such as 'Layer 1' for patient's information, 'Layer 2' for individual medical history with a form of blockchain, and 'Layer 3' for storing database based on standardized HL7 and KOSTOM in the individual patient. Layer 1 has public key to identify patients who can find the location of patient within the Cloud.

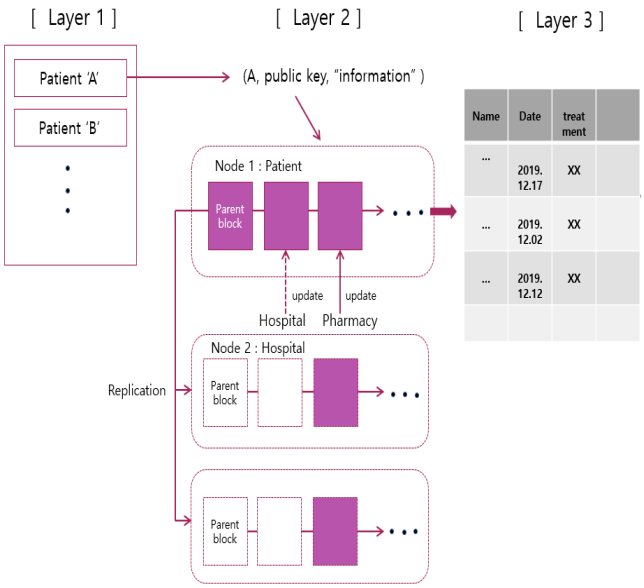

Figure 4 : PHR Layer

Layer 2 is composed of several nodes, designated by an individual user for instance, patient, medical institution and pharmacy. When individual user updates block, in fact, patient's information, another node will be created and connected to each other in the form of a chain. Due to the complex node configuration, it enables to construct a perfectly secured system. Layer 3 is useful in verifying PHR and utilizing study materials by applying HL7 and KOSTOM for the construction of the standard database.

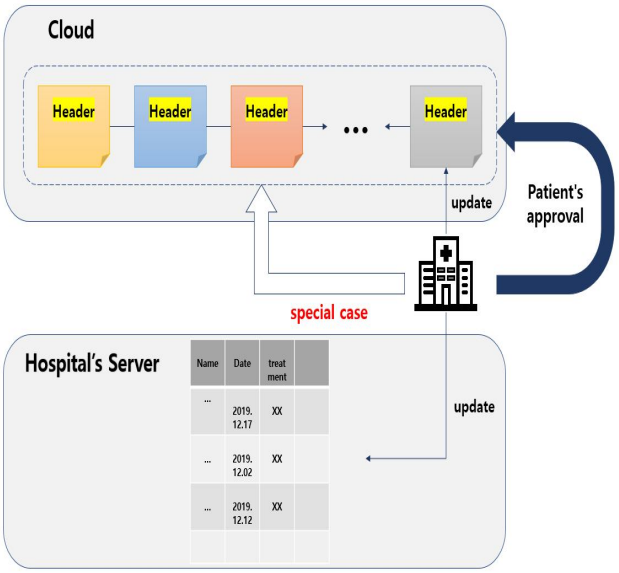

Figure 5 : Cloud based PHR

The users authorized to update patient's medical information, save the data in both cloud and pre-existing servers simultaneously when they upload the corresponding block (patient information). The user is able to update patient's information in cloud. However, they can't track patient's PHR since the coded address was recorded in Header (information of block). Sometimes, patient's PHR should be confirmed depending the specific situation. In this case, you should ask for patient's consent. Patient's information in cloud DB can be used as a purpose of research. For this occasion, new DB should be created by utilizing API and anonymizing the process of DB within cloud. The researchers registered as authorized users are able to access the corresponding DB for purpose of the study and the history is recorded in DB.

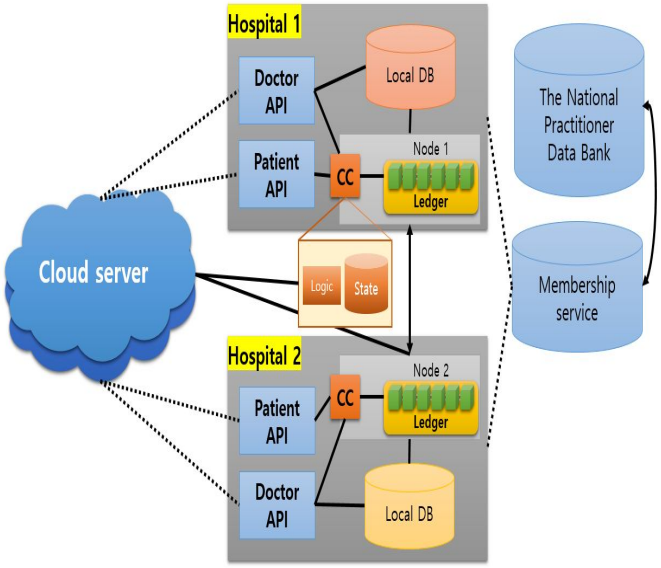

Figure 6 : PHR System Framework

5. CONCLUSION

The concept of the current medical paradigm has been changing from treatment to management. For the management, it is important to know current health condition, but the existing diseases and their treatment processes. The environment of medical information is shifting from recording and to saving into PHR which is an integrated record of EMR information and subsidiary patients' health information. PHR is very easy to check patients' health condition, which is suitable for the customized medical service.

Since blockchain technology was introduced, it has been easy to apply to general-purpose technologies in diverse industrial fields, including health-related areas. To apply the technologies on healthcare areas and leverage the latest ones, specific examinations and processes mapping with the relevant fields would be required.

This paper provided how to apply blockchain technology to the medical field and utilize it for PHR applications. For these applications, it suggested an architecture for gateway application of healthcare date to control and share PHR data more easily and securely.

ACKNOWLEDGEMENT

Funding for this paper was provided by Namseoul university

REFERENCES

1. Krystsina S..,**doptation of blockchain technologyu in supplychain and logistics**, Bachelor of Business Logistics, 2017.
2. Zhen, H., Zehua, W., Wei, C., and Victor, C.M., Lenug, **Blockchain-Empowered Fair Computational Resource Sharing System in the D2D Network**, Future Internet, 2017, 85; doi:10.3390/fi9040085
3. Yue X,Wang H, Jin D, Li M, and Jiang, W. **Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control**. Journal of Medical Systems, 40(10):218, 2016. https://doi.org/10.1007/s10916-016-0574-6
4. Jenkins J, Kopf J, Tran BQ, Frenchi C, and Szu H. **Bio-mining for biomarkers with a multi-resolution blockchain. In SPIE Sensing Technology+Applications**, International Society for Optics and Photonics, 2015. https://doi.org/10.1117/12.2180648
5. Beninger P and Ibara MA. Pharma, **covigilance and biomedical informatics: a model for future development**. Clinical Therapeutics, 2016. https://doi.org/10.1016/j.clinthera.2016.11.006
6. M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. Lou, **Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption**, IEEE Transactions on Parallel and Distributed Systems, vol. 24(1), pp. 131-143, 2013

https://doi.org/10.1109/TPDS.2012.97

7. Y. Zheng**, Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption**, Master's thesis, Worcester Polytechnic Inst., 2011.
8. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, **Secure Attribute-Based Systems**, J. Computer Security, vol. 18, no. 5, pp. 799-837, 2010.
https://doi.org/10.3233/JCS-2009-0383
9. Tang PC, Ash JS, Bates DW, Over hage JM, Sands DZ, **Personal Health Records: definitions, benefits, and strategies for overcoming barriers to adoption**, JAMIA, vol. 13, no.2, pp. 121-126, 2006.
https://doi.org/10.1197/jamia.M2025
10. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren , Wenjing Lou, **Scalable and secure sharing Personal Health Records in cloud computing using attribute based encryption**, IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp.131-143, 2013.
https://doi.org/10.1109/TPDS.2012.97
11. Ming Li, Shuncheng Yu, Kui Ren, Wenjing Lou, **Securing Personal Health Records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings, Security and Privacy in Communication Networks**, Lecturer notes of the institute for computer science, vol. 50, pp. 89-106, 2010.
https://doi.org/10.1007/978-3-642-16161-2_6
12. Zhiguo Wan, Jun ' e Liu, Deng R H, **HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing**, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012.
https://doi.org/10.1109/TIFS.2011.2172209
13. R.S. Mans1, M.H. Schonenberg, M. Song1, W.M.P. van der Aalst,,and P.J.M. Bakker, **Application of Process Mining in Healthcare – A Case Study in a Dutch Hospital**, A. Fred, J. Filipe, and H. Gamboa (Eds.): BIOSTEC 2008, CCIS 25, pp. 425–438, 2008., springer 2008.
14. Raja, J., & Praveen, G., **Blockchain for IoT Security and Privacy: The Case Study of a Smart Home**, Conference: IEEE Percom workshop on security privacy and trust in the internet of thing, 2017
15. Michael, C., Nachiappan, S.V., and Vignesh, K., **Blockchain Technology, Sutardja Center for Entrepreneurship & Technology** , Technical Report 2015.
16. Asaph, A., Ariel, E., Thiago, V., and Andrew, L., **MedRec: Using Blockchain for Medical Data Access and Permission Management**, 2nd International Conference on Open and Big Data, 2016.
17. Steve, H., Rituparna, B., Martin, W., Natalia, B., **Internet of Things, Blockchain and Shared Economy Applications**, Procedia Computer Science, Volume 98, 2016.
https://doi.org/10.1016/j.procs.2016.09.074
18. Marlon, D., Marcello, L. R., Jan, M., and Hajo, A. R., **Fundamentals of Business Process Management.** Second Edition. Springer, 2018.
19. Tien Tuan, A.D.,, Ji, W., Gang, C., Rui, L., Beng, C.O, Kian-Lee, T. , **BLOCKBENCH: A Framework for Analyzing Bitfury grou**p ,Digital Assets on Public Blockchains, 2016 Private Blockchains, SIGMOD'17, Chicago, USA 2017.
20. Zibin, Z., Shaoan, X., Hongning, D., Xiangping, C., and Huaimin, W., **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**, IEEE 6th International Congress on Big Data, 2017.
21. Monica Thomas and Dr. Varghese S Chooralil, **Security and Privacy via Optimised Blockchain**, International Journal of Advanced Trends in Computer Science and Engineering , Vol 8(3), pp.415-418, 2019.
https://doi.org/10.30534/ijatcse/2019/14832019
22. Mark Renier M. Bailon and Lawrence Materum, **International Roaming Services Optimization Using Private Blockchain and Smart Contracts**, International Journal of Advanced Trends in Computer Science and Engineering , Vol 8(3), pp.544-550, 2019
https://doi.org/10.30534/ijatcse/2019/32832019
23. Enrique G. Abad, Dr. Ariel M. Sison and Dr. Ruji P. Medina, **Security Evaluation of the Enhanced Key Generation Algorithm of Hashing Message Authentication Code**, International Journal of Advanced Trends in Computer Science and Engineering , Vol 8(4), pp.1254-1259, 2019.
https://doi.org/10.30534/ijatcse/2019/35842019