ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse75852019.pdf
https://doi.org/10.30534/ijatcse/2019/75852019

Medical Data Framework Using Blockchain Technology

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

ABSTRACT

The biggest advantage of introducing blockchain is that it can deliver data to members while maintaining the security of medical data sensitive to personal privacy. That is, by using a blockchain in the ecosystem of medical information, it is possible to connect the insurer, the health care organization, and the patient. The blockchain provides health data efficiently and increases accuracy and efficiency when changing patient data through the health system. In addition, it improves the efficiency and control of patients' personal health data and increases the price transparency of pharmaceuticals and health services. So far, the healthcare industry has had strict regulations and policies to limit data security and personal privacy. Therefore, this paper has suggested the framework with functions to support clinical decision making more efficiently using blockchain technology and FHIR data standards. Basically, this framework is built on the FHIR, which is designed to be provided to patients. In addition, it complements and uses open key encryption technology and meets the key requirements required in interoperability functions, such as user identification/authentication, secure data exchange, and authorized data. In particular, it provides further secure data exchange method aiming access guarantee, consistent data format and system modularity.
These instructions give you guidelines for preparing papers for

Key words : Blockchain, Framework, Medical Data, medical.

1. INTRODUCTION

There are many changes in the field of current medical information and the application of various advanced technologies is attempted[1, 2]. In particular, the application of technologies that can be specialized in the medical field, such as blockchains, is being studied. In other words, multiple peers validate and store each other's data over the network[3, 4]. Therefore, it is a storage platform designed to make it difficult for other people to manipulate their data. One block that makes up this blockchain consists of a Header and a Body[5].

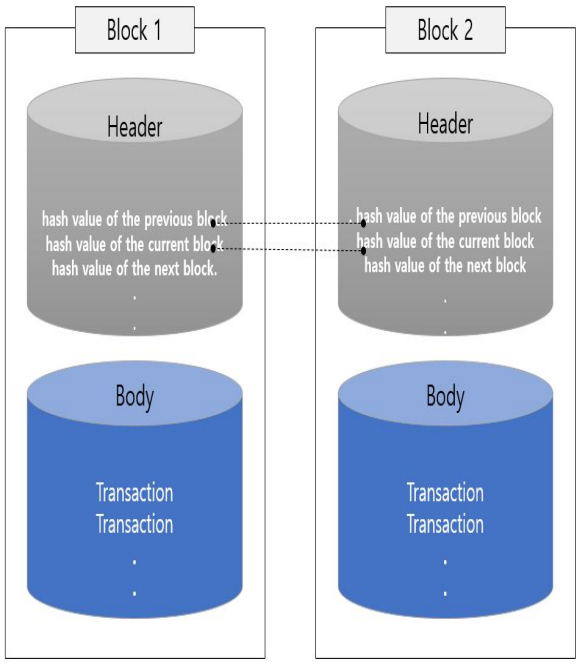

Figure 1 : Structure of Blockchain

Where the header consists of the Hash value that connects the previous block to the next block and Nonce, a random number, associated with encryption. The body also records transactions by trade, and peers in the blockchain can verify the data using the hash values here. This is named blockchain because of the structural shape in which the blocks are linked between the previous block's hash value and the current block's hash value[6, 7].

When comparing these blockchain technology with the past method, it is as follow. The existing method is a form of delivering transaction information by collecting data from "Trusted Third Party" called "Center". However, the blockchain technology is a technology that transfers information based on a decentralized peer network and members have record and manage transaction information in common. In particular, blockchain technology can be applied efficiently in the medical field as well. In particular, blockchain technology can be applied efficiently in the medical field as well That is, blockchain technology can be used to effectively manage human DNA and deliver sensitive DNA information to hospitals or laboratories without an intermediate trading agency[8, 9].

In this paper, we suggest a framework that is specialized in the medical fields that can manage medical data and improve patient care by designating peers on blockchain and creating a medical IT ecosystem connected to trusted peers.

.

2. RELATED WORKS

Blockchain technology is a technology standard that enables personalized health in health care systems and has the potential to address the problem of interoperability that enable health providers and medical researchers to securely share health data electronically[10, 11]. Meantime, several studies have been carried out in this respect. These studies have been proposed to solve the ownership problem of individual medical and health information by using the blockchain technology[12]. In particular, block - chain technology has been recognized as one of the various ICT technologies for the transition of medical environment paradigm to personal customized health care. That is, the blockchain technology is being used as an effective alternative to protect the patient's data in the medical field. In addition, several researchers have studying to be used to support the data management in various medical applications. Figure 2 shows the blockchain in this medical environment.

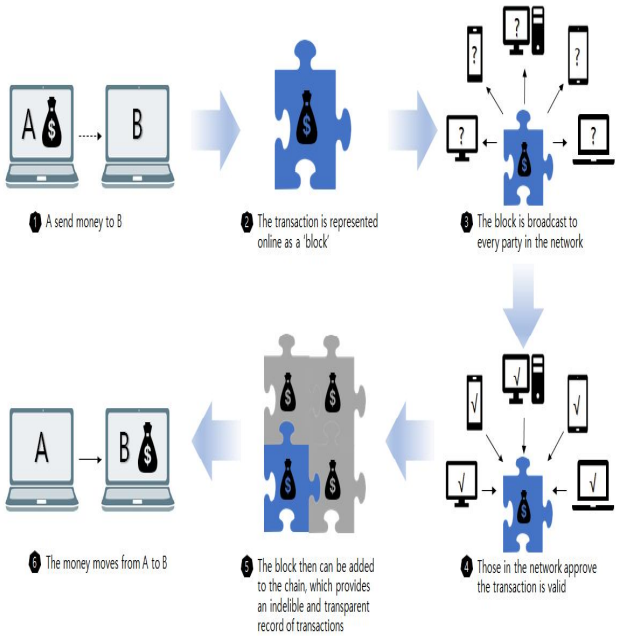

Figure 2 : Blockchain of Medical Environment.

Blockchain also enables users to secure ownership on recording, storing, distributing not only medical field data related to person's health, such as personal care information, medication information, medical staff and health care organization information, physical/biomechanical information, and genetic information but also all date related to personal health such as diet, exercise, sleep, distance, and driving status[13, 14].

These blockchain-based systems are expected to provide a realistic solution that minimizes medical cost billing-related imposture. That is, by automating most of the billing judgement and payment processing activities, the block-chain system can help eliminate the need for verification or coordination steps and reduce the administrative cost and time of suppliers and payers. In addition, this blockchain can be used as an important means to improve the logistics information of large-capacity pharmaceuticals and medical devices that track the obstacles of Reliability-Centered Maintenance[15].

3. APPLICATION OF FAST HEALTHCARE INTEROPERABILITY RESOURCES

The blockchain technology suggested in this paper basically has the following six characteristics;

First, Distributed (distributed across all subjects who participate in the network; Second, Decentralized (decentralization with a copy of the blockchain on all the entire nodes; Third, Pubic (Publicness that all attendants of blockchain transaction is hidden, but allows everyone to see all transactions); Forth, Time-stamped (transparency that records the date and time of all transactions); Fifth, Persistent (persistency that cannot be damaged by fire or flooding due to the nature of consent and digital recording); Sixth, Non-reputation (Non-repudiation that cannot deny the fact of data transmission sent by a specific sender). In particular, the FHIR (Fast Healthcare Interoperability Resources), an interoperability standard, is designed in purpose to exchange records in electronic formats, and it is a standard describing data formats and elements while providing publicly accessible application programming interfaces (APIs).

These standards are prepared and managed by Health Level Seven International (HL7), i.e. by the Health Standards Organization. The FHIR is licensed without restrictions or royalty requirements, which serves to promote broader adoption. In particular, FHIR users provide the improved mobile and cloud-based application utilization, integration of medical devices, and flexible/customized opportunities for healthcare workers. Using the FHIR can separate HER data elements. It also has two kinds of resource types; identifiers (suppliers and patients) and general clinical activities. These partitioned resource configuration of this FHIR facilitates the transmission of EHR data in appropriate. In addition, the FHIR resource follows the Representational State Transfer (ReST) principle and allows for verification of the structural suitability of the standard and can be added by an additional conformity declaration called a profile.

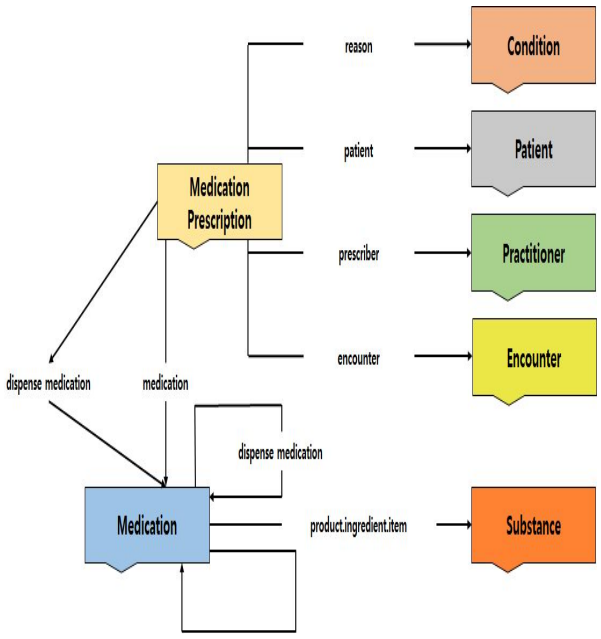

Figure 3 : References Between FHIR Resources

In particular, FHIR is a standard framework that defines common methods for addressing problem of healthcare information sharing and defines resources that can be used in various environments. In other words, it was developed to support paths that could interact with existing standard transmission models.

FHIR provides improved functions compared to v2, v3, and CDA which are existing standard transport models. These improved functions include: First, since FHIR is focused on implementation, the developers can use it easily and simple. Second, the FHIR supports an execution library and numerous available cases to speed up development. Third, FHIR utilizes resource-based interoperability. For example, for the management of patients with hypertension, a chronic disease, only three resources are available for exchange and treatment: blood pressure measurement information (Observation), patient information (Patient), and blood pressure system information (Device). Fourth, since they are doing mapping work with the data types of the existing reference standard HL7 v2 and the reference information model, they can coexist in the same environment. Fifth, it expresses the clinical documents received by the medical worker to facilitate understand through summary of patient information. And the resources of the FHIR are available at any time as an open source. The environment for sharing and exchanging health information is extensive, including Social Media on Mobile phones, Cloud Communications, Electronic Health Record System, and Personal Health records. Social Media can identify patients by external identification and patients' records connections or logins through Google, Facebook and open IDs, and logins restrict access to security and patient records through standardized authentication methods. One general method to integrate medical information from various resources is to create space to store patient records.

The FHIR defines the context and concepts used in a variety of medical information as a data set called 'Resources', and it is a data processing platform specification designed allow to manage resources individually or to collect the complex document. Resources defined by these specifications are treated as XML or JSON structures on locations expressed as URLs through the HTTP protocol, and are designed to represent data as much as possible using open Internet standards.

The blockchain-based framework in this paper is the API provided based on these FHIR standards. In other words, it is proposed that patient data can be used in research projects with trusted application and service developers through API Developer Preview Service. According to the PHR scenario of the HL7 FHIR, the electronic medical record system is to access the medical records owned by users via mobile applications or Web portals, a third medical information system. It also made a disclosure of and uses the FHIR server, which supports searching, reading, and working of resources, and provides a useful API for an efficient approach.

The APIs provided describe the regulations of FHIR resources so that individual resources can be collected and managed in a particular type of server. Since these functions search user requirements independently, they enable faster data processing than traditional standard documentation methods. In particular, these frameworks immediately perform requests/response from HTTP (Hypert ext Transfer Protocol) on server resources during transactions. The electronic medical records system can add the functions to allow the caregiver to access patient records to allow patient information updates, medication history, and observations. The electronic medical record system uses secure event resources to allow patient access, where APIs must be logged in to these resources. The FHIR document allows resources to be added through expansion and supports allow to express specific resources only, such as Lego block.

The document is largely composed of three parts: expansion, text, and standard data contents. Extension functions include Modifier Extensions, Exchanging Extensions, Control of Extensions, and Defining Extensions. Since it may happen the cases that extend to different resources between application programs which exchange the information in healthcare situations, the FHIR specification provides basic rules. Extension controls are defined by classifying content items through extensions to maintain briefness, and simplicity of the resource structure rather than using all content items in a single resource area. The extension element is available on URI basis and HL7 supports publicly accessible test registers.

Definition extensions can use resources and element types. This further defines the profile of the resource to be expanded or apply constraints on the type of element. However, only the elements defined in the FHIR specification can be used. Text summarizes and indicates the contents of the resource and can be defined to be legible. Expressions of text can be described in narrative or XHTML (eXtensible Hypertext Language). The contents of XHTML do not include head and can be configured with body elements, external style sheet references, font, frame, entity, or event-related properties. The FHIR run library defines the text type as Narrative. In narrative, XHTML can be designated as CSS (Cascading Style Sheets) external and internal. External styles are used through the id properties of the XHTML element, and internal styles use the style properties directly in the XHTML element.

The blockchain technology applied in this paper can be used as an alternative to meet the requirements of existing standards, while supplementing rather than replacing the FHIR system. Because blockchain is not yet sufficient to store and distribute all medical and health-related information. Because it is difficult to store large image information, such as X-rays and MRIs directly, and it is also dangerous if Personal Identification Information (PII) is publicly exposed. In order to address these problems, two types of information storage methods are used: 'On-Chain' data that stores information directly in the blockchain and 'Off-Chain' data that uses links stored in the blockchain as a pointer for information stored in a separate traditional database.

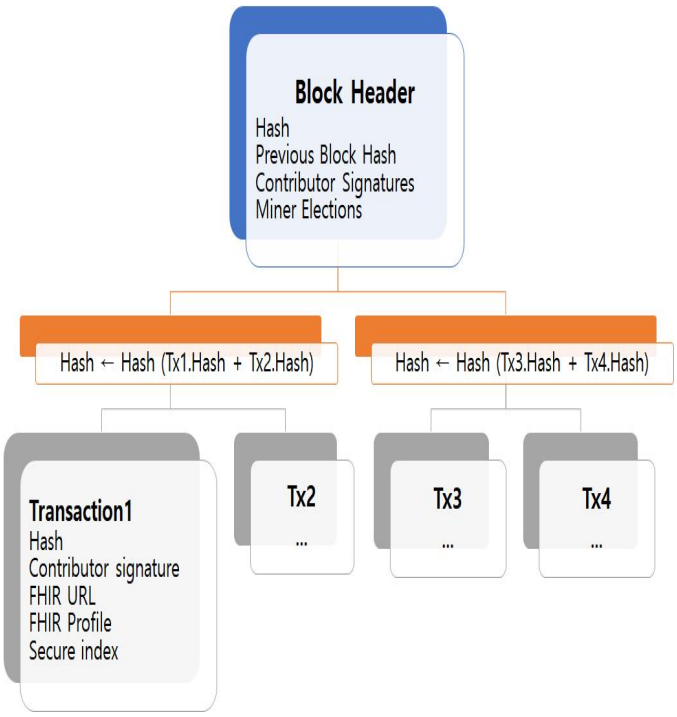

Figure 4 : Example of a Healthcare Blockchain Structure Reflecting FHIR

4. BLOCKCHAIN-BASED ARCHITECTURE FOR CLINICAL DATA SHARING

In this paper, it presents a blockchain-based architecture designed to meet the requirements for safe and extendable sharing of medical data. And it provides a reason for presenting this architecture and a solution to the problems faced by blockchain technology that addresses the needs of the medical sector.

The following figure 5 shows the architecture presented to address the needs of the medical sector. This architecture enables application in a wide range of health IT systems. In addition, it can be applied to distributed mobile systems that support decision making on joint treatment (cooperative treatment) in remote health care.

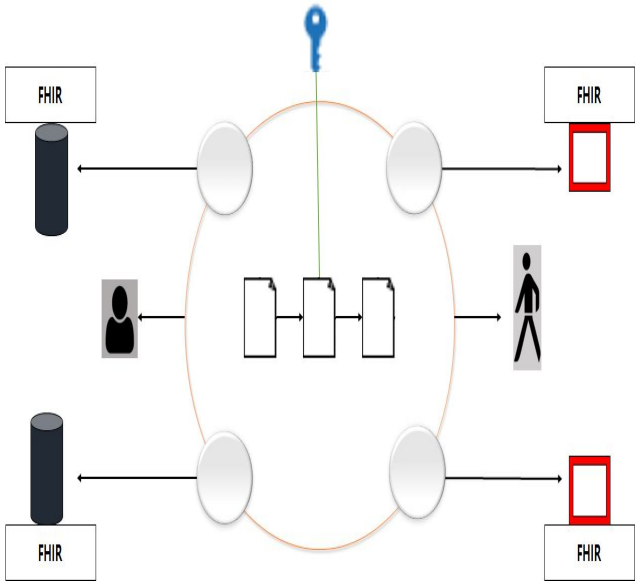

Figure 5 : Architectural Components in Healthcare Blockchain

In Figure 5, the central ellipse represents a blockchain that supports data sharing among collaborative health care professionals. Clinical data used here can be linked and operated with different types of databases. The architecture also utilizes the FHIR standard and use the common structure that shared data has. In this structure, a secure database connector is connected to the blockchain. Here, it has a blocked data source that only authorized entities can be obtained. And the secure tokens are recorded in the smart contract document (display as linked document) for distributed access and traceability. This smart access allows to store/exchanges secure access tokens and maintain transaction logs of events that use tokens. These logs record specific information about what access right was granted to the user, which token was used to access the resource, and so on. In other words, this architecture ensures that all shared data is approved by authorized clinicians and health care organization only to ensure the validity of all shared data.

This architecture has the following technical requirements:

First, it is the requirements for authenticating. In here, the verifying identity and all peer's contexts are authenticated. That is, the blockchain provides an anonymous personal account (an open address consisting of random hash values) for the user to process the cryptogram. However, these unique IDs do not address all peer's identifiability or requirements for authenticating. Basically, the blockchain can be accessed by anyone who can access to the Internet. Since users can have multiple blockchain accounts, minimizing the identifiability of the account owner. However, these requirements should be able to identify all health care person concerned and require traceable users that are completely different from the unique ID of the blockchain. That is, these functions define the identity of the medical user involved in the sharing of clinical data and protect important personal information in the blockchain. Second, it is the requirements for storing and exchainging. In here, data is stored and exchanged safely. The key function provided by blockchain is that it also supports transactions between parties that do not have trust relationships. Since the blockchains are peer-to-peer in nature, they support the ubiquitousness of digital assets traded. Third, it has access right. It is a right that is accessible to data source context. Data references are performed by blockchains for access of multiple paths. However, access rights should only be granted to providers authorized to view data.

Assume that the provider initiates the sharing of patient data to another supplier. In this architecture, they make a digital sign on the sharing content. And encrypt the document with the provider's private signature key and the public encryption key. And then, after obtaining an encrypted token, make a smart contract for access to the document. This digital signature process ensures that the provider actually shares the resources and does not tamper. It protects documents from unauthorized access. These authorities can be implemented by connecting in the same way as a traditional centralized system. In this case, a meta-encryption key pair is created for the properties and stored securely in the system database. Users who meet certain authority criteria allow to use the key when accessing data while protecting users from non-critical details.

Forth, it is a consistent data formats/context. Clinical data may exist in a various formats and structures, but may or may not be meaningful when shared with other providers. Fifth, it is a maintenance of module method. In here, design patterns apply to MVC (Model-View-Controller) model.

MVC patterns divide the system into three components: (1) Models: Manage the behavior and data of the system and respond to requests (2) View: Information on status and status change instructions, (3) Controller: Manage information displays, and deliver user input to view or model.

This architecture applies these MVC patterns to individual context. (1) Allow to store the required metadata through a model in the form of non-changeable blockchain components. (2) Views provide a front-end user interface that accepts user input and provides data. (3) The controller facilitates interaction with the data between the user interface and the blockchain components. (4) The Controller Call Data Connector Service is used to verify the implementation of the FHIR standard and to create a reference pointer for the data source upon request from the server.

In this architecture, the update work for data access carries out in four steps.

- Users can authenticate through the User Interface (UI) and enter the request for data access authority into the system once they have been successfully authenticated.
- The UI delivers user requests to the server.
- The server records authorized or revoked access in block chain components (BC).
- The server updates the UI with an appropriate response and notifies the user.

Similarly, the work to access a data source carried out with the following a-e.

a) Users are authenticated through the UI and successfully authenticated data access requests can be entered into the system.

b) UI forwards user requests to the server.

c) The server queries the BC for the access token of the current user.

d) If the privilege is valid, the server uses the correct key provided by the user to decode the access token and obtain the actual data from the DB connector to the appropriate database using the decrypted reference pointer.

e) When retrieving data from a data source through a DB connector, the server updates the UI and displays the data in a readable format.

This architecture separates the rest parts of the system and the data store by storing healthcare-related information in smart contracts. This decoupling has the advantage of enabling future upgrades to other components without losing access right to existing users or authority information. Figure 6 shows the form of this extended framework.

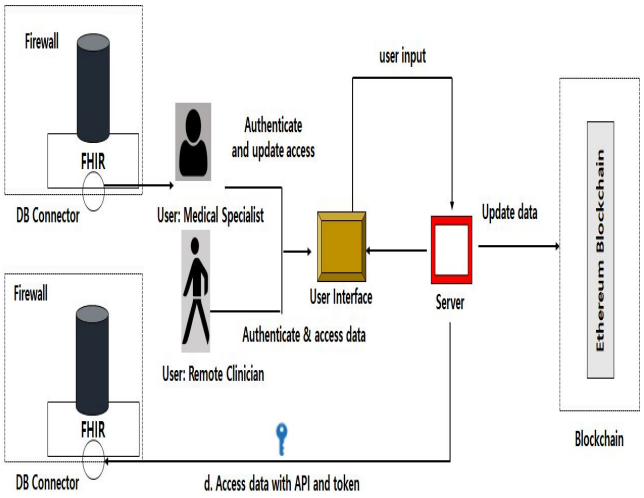

Figure 6 : Extended Framework.

5. CONCLUSION

When blockchain technology is applied to medical field, personal information can be protected from malicious hacking by storing personal information on blockchain. It also makes it possible to build a patient-centered integrated healthcare information platform based on the high security, reliability, transparency, interoperability and accessibility of blockchain technology. It can also address information asymmetry problems that existing centralized systems has. In addition, the using the blockchain can realizing innovation in the medical industry by effectively recording and managing medical information while by making impossible the tamper and reducing the possibility of leakage of personal information.

Therefore, this paper has suggested the framework with functions to support clinical decision making more efficiently using blockchain technology and FHIR data standards. Basically, this framework is built on the FHIR, which is designed to be provided to patients. In addition, it complements and uses open key encryption technology and meets the key requirements required in interoperability functions, such as user identification/authentication, secure data exchange, and authorized data. In particular, it provides further secure data exchange method aiming access guarantee, consistent data format and system modularity.

ACKNOWLEDGEMENT

Funding for this paper was provided by Namseoul university

REFERENCES

1. Zapata, B. C., Fernández-alemán, J. L., Toval, A., and Idri, A., **Reusable software usability specifications for mHealth applications**. J. Med. Syst. Vol.42, No. 1, 2018. https://doi.org/10.1007/s10916-018-0902-0
2. Imtiaz, S. A., Krishnaiah, S., Yadav, S. K., Bharath, B., and Ramani, R. V., **Benefits of an android based tablet application in primary screening for eye diseases in a rural population**, India J. Med. Syst. Vol. 41(4), pp. 49-56, 2017. https://doi.org/10.1007/s10916-017-0695-6
3. Elhoseny, M., Abdelaziz, A., Salama, A. S., Riad, A. M., Muhammad, K., and Sangaiah, A. K., **A hybrid model of internet of things and cloud computing to manage big data in health services applications**. Future Generation Computer System, 2018. https://doi.org/10.1016/j.future.2018.03.005
4. Puthal, D.,Malik, N.,Mohanty, S. P., Kougianos, E., and Yang, C., **The blockchain as a decentralized security framework**. IEEE Consumer Electronics Magazine, Vol. 7(2), pp.18–21, 2018. https://doi.org/10.1109/MCE.2017.2776459
5. Ma, Y., and Sharbaf, M. S., **Investigation of static and dynamic android anti-virus strategies**. In: 10th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, 2013.
6. A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, **Blockchain and iot integration: A systematic survey**, Sensors, Vol. 18, no. 8, pp. 2575, 2018. https://doi.org/10.3390/s18082575
7. K. Christidis and M. Devetsikiotis, **Blockchains and smart contracts for the internet of things**, IEEE Access, Vol. 4, pp. 2292–2303, 2016.
8. T. Neudecker and H. Hartenstein, **Network layer aspects of permissionless blockchains,** IEEE Communications Surveys & Tutorials, 2018. https://doi.org/10.1109/COMST.2018.2852480
9. W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, **Decentralized applications: The blockchain-empowered software system**, IEEE Access, 2018.
10. S. Banerjee, P. K. Singh, and J. Bajpai, **A comparative study on decisionmaking capability between human and artificial intelligence**, in Nature Inspired Computing. Springer, pp. 203–210, 2018. https://doi.org/10.1007/978-981-10-6747-1_23
11. S. Janson, D. Merkle, and M. Middendorf, **A decentralization approach for swarm intelligence algorithms in networks applied to multi swarm pso**, International Journal of intelligent computing and cybernetics, Vol. 1, No. 1, pp. 25–45, 2008.
12. D. Magazzeni, P. McBurney, andW. Nash, **Validation and verification of smart contracts: A research agenda**, Computer, Vol. 50, No. 9, pp. 50–57, 2017. https://doi.org/10.1109/MC.2017.3571045
13. B.Manoj, K.V.K.Sasikanth, M.V.Subbarao and V Jyothi Prakash, **Analysis of Data Science with the use of Big Data**, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 7, No.6, 2018. https://doi.org/10.30534/ijatcse/2018/02762018
14. Munisha Devi and Nasib Singh Gill, **Performance Evaluation of Dynamic Source Routing Protocol in Smart Environment**, International Journal of Advanced Trends in Computer Science and Engineering , Vol. 8, No.2, 2019.
15. Prasad TV, S. K Kumar, Ajay Kumar, Ch Uma Devi and B Nanda Kishore, **A Novel Approach of De duplication of Records using Febrl Algorithm and Data Mining**, Advanced Trends in Computer Science and Engineering, , Vol. 7, No.6, 2018. https://doi.org/10.30534/ijatcse/2018/22762018