**ISSN** 1816-6075 (Print), 1818-0523 (Online)
**Journal of System and Management Sciences**
Vol. 10 (2020) No.4, pp. 125-136
DOI:10.33168/JSMS.2020.0408

# A Fast Healthcare Interoperability Resources based Blockchain Framework for Medical Data Management

Sang Young Lee
Department of Public Health Administration, Namseoul University, South Korea
*sylee@nsu.ac.kr*

**Abstract.** The 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 medical environment paradigm and health services. This paper suggested the framework with functions to support clinical decision making more efficiently using blockchain technology and Fast Healthcare Interoperability Resources (FHIR) data standards. This framework is built on 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.

**Keywords:** FHIR, blockchain, framework, Medical Data.

# 1. Introduction

Blockchain technology has received considerable attention because it has some benefits in terms of security. It is not possible to use the technology separately, but it is suitable to manage the safely dispersed database in a field that has to be operated centrally (Zapata, 2018). Thus, blockchain has been used in diverse fields such as healthcare industry which requires a safe database. In short, blockchain is typically managed by the distributed authorization or a manager. It is a digital ledger that has a signature provided in a record list form which is a block in peer-to-peer (P2P) networks for continuous expansion. And, it automatically checks its own validity in its own network. Also, blockchain offers a continuous upgrade service (Imtiaz, 2017; Elhoseny, 2018).

In particular, the volume of data to be collected and analyzed has been on a rapid increase owing to the growth of Internet of Things (IoT) environment. In the transition of the existing Hadoop, an analytical platform on centralized bigdata induced considerable load and latency in the network. Moreover, the concerns regarding accessibility and availability have been mounting since the platform has functioned by Single Point of Failure (SPoF). Blockchain technology has highly been spotlighted as a solution of overcoming the issues and it has been utilized in a variety of application areas(Puthal, 2018; Ma, 2013).

Blockchain is based on a system of P2P distributed network while blocks of trade information are created by verification and agreement of network participants. Blockchain, utilized by distribution storage and code technique, consists of two core procedures. The first step is ‘Mining’ to create an effective individual-block by collecting trade information or record, which can avoid double payment. Some of the miners among the participants in the network use substantial computing power to find Nonce values, fitted in the conditions of block creation in Hash function. When Node finds an appropriate Nonce value at first, the block is transmitted to the corresponding network. The pertinence of the Nonce value and trade is verified by each Node. Then the corresponding block is approved with time stamp and connected to the next to the preceding block. In this process, if any information has been changed or modified, it will be captured and deleted by the verification step. The small incentive will be provided for the miners who complete the new block, which finds the optimum values in the given condition (Panarello, 2018; Neudecker,2018).

In fact, medical data for blockchain should be standardized for a successful application. Currently, research on standardization of medical information have been accomplished, on the other hand, an appropriately applied medical institution is hardly found within the country. It suggests a necessity of considering appropriacy of the technology in the medical system. Especially, at this point of time when genomic data has expanded to the clinical area, an accurate study should

be supported by discovering a strategy of standardization. Clinical Document Architect (CDA) of HL7 is an essential parameter of distribution of clinical data. It enables us to share and exchange medical information between medical institutions regardless of a type of medical institution (Jae, 2015; Tanuja, 2016)

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 (Hyoung-Keun, 2019). 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 (Sang, 2019)

## 2. Related Works

Blockchain technology has been applied in various applications for management of distribution of data. The technology could be applicable to diverse areas including financial service. Especially, it shows excellent performance in the inspection of data efficiency and confirmation of any changes in records. Recently, a variety of blockchain technology has been developed in diverse applications. The following figure shows the description of system (Siwoo, 2019; Manmohan, 2017)

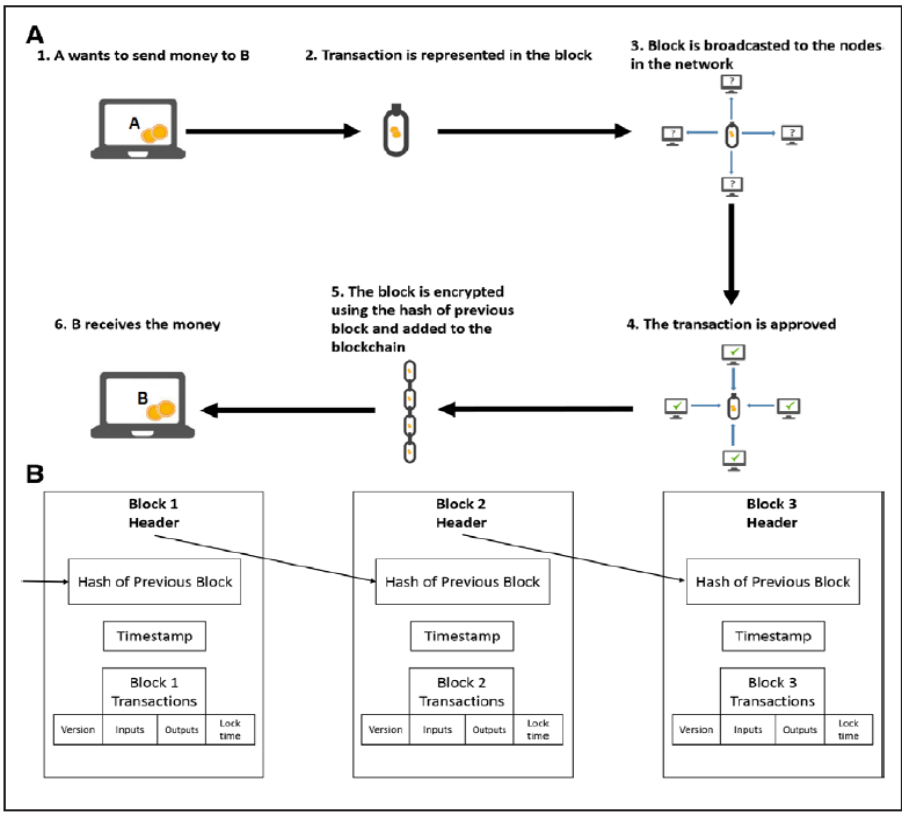


Fig. 1: The execution of a transaction in blockchain

Several problems are still presented in Blockchain technology. Since Bitcoin is the most popular application currently, the related issues are mostly discussed as follows.

- Expandability and latency: Block files are grown infinitely and should be copied in all nodes of P2P network, resulting in issues of expandability and latency.
- Reliability: Integrity is determined by hashpower, not the number of nodes in the network. Thus, an entity with powerful computational resources possibly re-creates Genesis Block (the first block of blockchain) by accumulating hashpower.
- The numbers processed: In the case of Bitcoin, 1 MB has been created every 10 minutes which is relatively small capacity compared to the process of transactional information in Visa card, showing 56,000 cases processed per second. Due to the fact that the capacity of block is correlated to the time required for verification and approval of trades, difficulties exist in expanding capacity blindly.
- Encryption: Basically, the content of blockchain, transaction, and record itself are not encoded.
- Mistake or misuse: Blockchain is an unchangeable record storage. Goof-up or fraudulent dealings could exist in the system. Despite quick detection, it is difficult to prevent.

Blockchain technology is a 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(Krishn, 2016; Kumar, 2016). 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. In particular, blockchain 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 (Ho-Kyung,2018; Debabrata, 2015; Sang, 2019)

# 3. Healthcare Interoperability

Blockchain technology is a 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. In particular, blockchain 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.

A principle of operation of blockchain is to record and store the related data into an entry of each distributed node when the trade has been created. It is processed by comparing and verifying consistency between the data and record in the corresponding node. Since comparison and conformation of data are processed for all participants, it guarantees stability and reliability of data. According to the characteristics of participants and accessible scopes of system, the encrypted currency has been issued in such Bitcoin or Ethereum. In addition, various types of blockchain are existed, for instance, public blockchain to anyone, private blockchain like NASDAQ link allowed to licensed users, and Consortium blockchain, accessible to specific participants in consortium such as R2CEV

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.

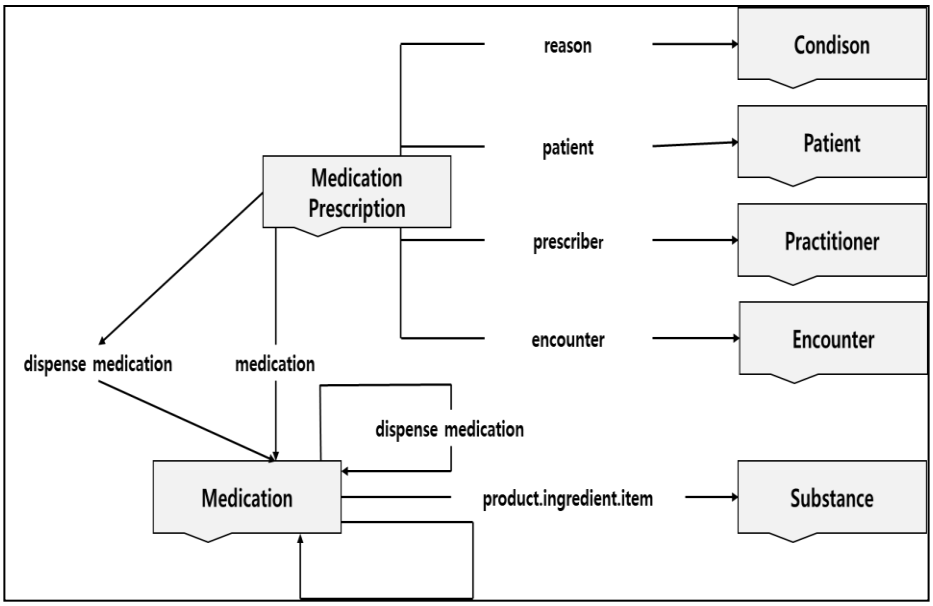



Fig. 2: References between FHIR resources

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.

These standards are prepared and managed by Health Level Seven International (HL7 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 configurations of 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.

In this paper, blockchain technology applied 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.

## 4. Blockchain-based Architecture for Clinical Data Sharing

Currently, blockchain technology is still very much in an early stage in the steps of technical development. A variety of essential issues are existed in a slow rate of

trade, limited storage of data, incompatibility with old block system after an upgrade, and instability of program, suggesting a necessity of resolving the problems. Moreover, it has a tendency to seek autonomy of blockchain rather than efficiency. In this case, it is not suitable to apply in the business area, which requires quick trade. Under this circumstance, diverse technologies have been introduced to overcome the technical obstacles. Along with new concept of Data Lake, an attempt has been introduced by dividing on-chain data stored in block and off-chain data saving results of hash values.

In the case of the public blockchain, most of them are a type of decentralized App having no their own blockchain technology while a few cases retain their own blockchain network such as, Ethereum, and Quantum. In fact, issues in the decentralized application have been indicated for unexchangeable data communication between the blockchain. The problems are based on a lack of standardization of terminological system, different program system, and none of the protocol for data exchange. Regardless of forms of blockchain, it should be resolved for all blockchain technology. To apply the technology in industrial areas successfully, it is required to develop technology for efficient algorism as well as protocol for intervention. A consortium in the bank and financial areas has been founded to construct a platform of blockchain and to plan expandable application for payment of financial products and real-time financial transactions (Sang, 2019).

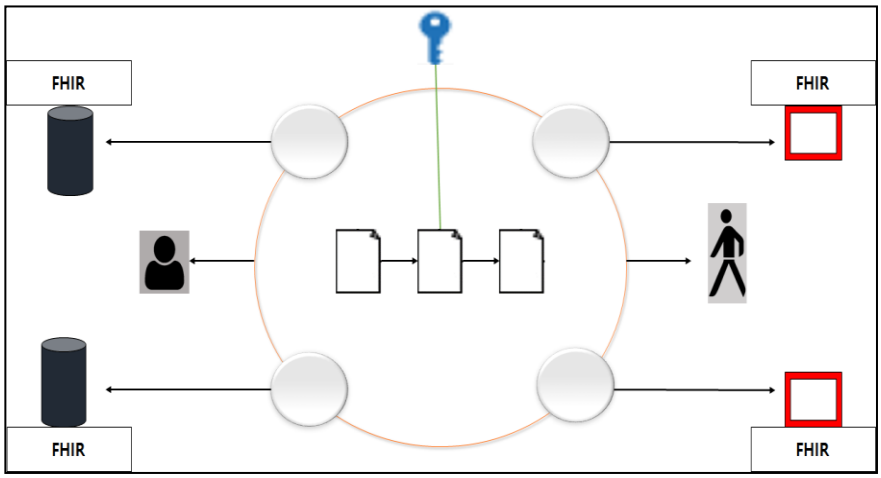



Fig. 3: Architectural Components in Healthcare Blockchain

Figure 3 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.

In Figure 3, 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 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.

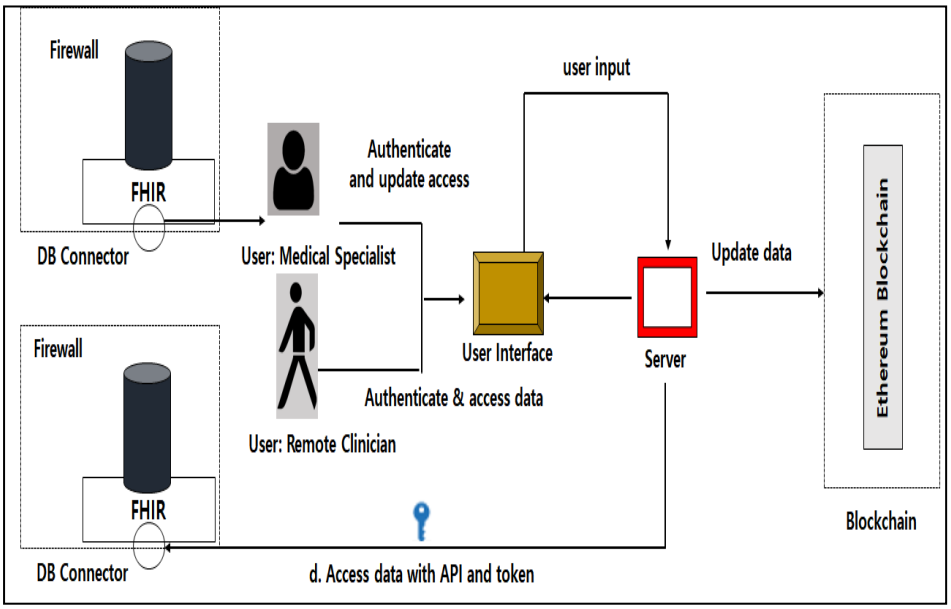
Second, it is the requirements for storing and exchanging. In here, data is stored and exchanged safely. The key function provided by blockchain is that it also supports transactions between parties that do not have trust relationships. Since the blockchains are peer-to-peer in nature, they support the ubiquitous 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 to multiple paths. However, access rights should only be granted to providers authorized to view 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 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 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.

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 4 shows the form of this extended framework (Sang, 2019).

Fig. 4: Extended Framework.

Blockchain technology has been expected to apply in diverse industries including

manufacture, public, education and media. Especially, it will affect the medical industry considerably. In detail, blockchain technology potentially resolves the issues, such as ① asymmetry of medical information between hospital and patient, ② inefficiency and insufficiency of insurance claim • evaluation and monitoring system, ③ inadequacy of monitoring system for the circulation of medical supplies, and ④ security risks of collected personal information.

First, an integrated platform of medical information is constructed by applying blockchain technology in Personal Health Record (PHR) management system, potentially resolving the asymmetry of medical information.

Second, efficiencies of claim and inspection are enhanced by an automated system for insurance claim • evaluation based on blockchain technology. It prevents ethical issues in overcharges and underpayment.

Third, the originality of medicine is guaranteed by implementing the collected information on all processes of distribution, preventing forgery through censoring.

Fourth, data can be protected from malicious hacking by saving the collected personal medical information through the censoring process.

So far, limitations of blockchain are clearly presented in ever-changing medical or personal information in the aspects of expandability and security. Nevertheless, it is expected that the blockchain system provides innovation to the medical industry since the issues have not addressed by other approaches as well.

## 5. Conclusion

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.

A core of futuristic medical care is to realize customized and predictive medical systems on the basis of data. The open system should be constructed by reading and circulation of personal medical information. On the other hand, a considerable level of reliability and security is required since medical data has dealt with sensitive information on personals. In the aspect of data, it is difficult to guarantee both openness and safety. To resolve the ambilateral aspects, blockchain has been received tremendous attention in the medical profession. The use of blockchain enables to record and manage medical information efficiently which lowers the possibility of personal information leakage and contributes realization of medical innovation.

This paper has suggested the framework with functions to support clinical

decision making more efficiently using blockchain technology and FHIR data standards. 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.

## Acknowledgements

Funding for this paper was provided by Namseoul university References

## References

Debabrata S.R.B. and Sudipta S., (2015). An enhanced cloud network load balancing approach using hierarchical search optimization technique. *International Journal of Hybrid Information Technology*, 8(3), 9-20.

Elhoseny, M., Abdelaziz, A., Salama, A. S., Riad, A. M., Muhammad, K., and Sangaiah, A. K., (2018), A hybrid model of internet of things and cloud computing to manage big data in health services applications. *Future Generation Computer Systems.*

Hari K.T., (2016). Role of kernel in operating system survey. *International Journal of Private Cloud Computing Environment and Management*. 3(1), 17-20.

Ho-Kyung, Y., Hyun-Jong C., You-Jin S., (2018). Efficient identifier management using the blockchain. *International Journal of Software Engineering for Smart Device*, 5(2), 13-18.

Hyoung-Keun P., (2019), A study on relationship recognition and analysis through IoT-Based infant activity monitoring, *International Journal of Advanced Science and Technology*, 130, 59-68.

Imtiaz, S. A., Krishnaiah, S., Yadav, S. K., Bharath, B., and Ramani, R. V., (2017). Benefits of an android based tablet application in primary screening for eye diseases in a rural population. *India J. Med. Syst*. 41(4), 49.

Jae, Y. L., Lahari, K., (2015). Security based network for health care system. *Asia-pacific Journal of Convergent Research Interchange*, 1(1), 1-6.

Kumar K.P., (2016). Efficient approach for query based search in data mining. *International Journal of Private Cloud Computing Environment and Management*, 3(2), 1-6.

Ma, Y., and Sharbaf, M. S., (2013). Investigation of static and dynamic android anti-virus strategies. *In: 10th International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, Nevada, 398–403.

Manmohan S., and Tripathi, B.K., (2017). On the efficient machine learning of the fundamental complex-Valued neurons. *International Journal of Neural Systems Engineering*, 1(1).

Neudecker, T. and Hartenstein, H., (2018). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., and Yang, C., (2018). The blockchain as a decentralized security framework. *IEEE Consumer Electronics Magazine*, 7(2), 18–21.

Panarello, A., Tapas N., Merlino, G., Longo, F., and Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, 18(8), 2575.

Siwoo B., (2019). Sensor data transmission control using selective dynamic compression for mobile IoT devices, *International Journal of Control and Automation*, 12(8), 87-96.

Sang Y. L., (2019), Blockchain-based framework for medical data management, *International Journal of Advanced Research in Big Data Management System*, 3(2), 29-34.

Tanuja, Patgar P. and Shankaraiah, (2016). The impact of hybrid data fusion based on probabilistic detection identification model for Intelligent Rail Communication Highway. *International Journal of Sensor and Its Applications for Control Systems*, 4(2), 9-20.

Zapata, B. C., Fernández-alemán, J. L., Toval, A., and Idri, A., (2018). Reusable software usability specifications for mHealth applications. *J. Med. Syst*. 42, 1–9.