Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 5858-5864

Research Article

Efficient Distributed Consensus Algorithm in BIoT Environment

Ph.D.Young-Bok Cho [a]

[a]Assistant Professor of Information Security, Deajeon University

Abstract: Currently, the importance of telemedicine is emerging in the era of Untect. In this paper, the proposed algorithm guarantees its transparency and reliability based on a blockchain-based lightweight distributed consensus algorithm that supports accurate diagnosis and reading by consensus of distributed image-reading experts in a telemedicine environment. However, since the blockchain consensus algorithm requires high-specification computing power or generates network traffic, its use in relatively low-performance Internet-of-Things (IoT) devices is very limited. Therefore, in this paper, we proposed a distributed consensus algorithm for reading medical images based on a blockchain suitable for IoT telemedicine environments and showed its more efficient performance than the existing blockchain consensus algorithm. The proposed algorithm has a fast computing transaction speed of about 3 s and reduces the memory usage by 38.5%. In addition, it provides a secure remote environment by solving security vulnerabilities in the IoT environment.

Keywords: Internet of Things, Bio, Medical Image, Energy efficient, Blockchain

1. Introduction

In recent years, the importance of telemedicine has emerged in society as we enter the era of Untect. In Korea's telemedicine, after the revision of the Medical Act in 2002, various pilot projects have been conducted for the public to address medical blind spots due to distance problems, as in the case of islands and mountainous areas. However, the condition that facilities and equipment for telemedicine (i.e., sphygmomanometer, blood glucose meter, electrocardiogram, blood analyzer, patient monitoring system (PMS), chemical analyzer, X-ray, ultrasound) stipulated in Article 34(2) of the domestic medical law must be equipped. There is a condition that data required for remote medical treatment must be processed by safely transmitting patient data measured from medical equipment to remote doctors **(Kim,J.Y& Lee,K.I.2020, Kumar,R.B, Goren,N.D, Stark,D.E, Wall,D.P & Longhurst,C.A 2016)**. However, collision and communication problems may occur among medical devices, due to difference in the protocol of data processing and interfaces built for each equipment by the manufacturer. Blockchain is a technology consisting of generated information in the form of blocks that are then interconnected over time, making it difficult to forge or alter information **(Li,X.2020)**.

Blockchains are classified into two types, public and private blockchains, and the validity of transactions is verified using a consensus algorithm according to each situation. It is important to provide a stable environment for the speed and performance of transactions even when the number of users increases while ensuring the integrity of transactions. In order to create a block used in the blockchain, an algorithm that all participants in the blockchain network can agree on is required, but the consensus algorithm requires high-specification computing power or generates network traffic. Therefore, in 2008, Satoshi Nakamoto proposed a Proof-of-Work consensus algorithm based on the amount of CPU computation, and in 2015, Vitalik Buterin published in a white paper various consensus algorithms with contents such as stake **(Cho,Y.B.2020, Tang,W.2019)**. However, these consensus algorithms have a disadvantage as blocking information branching, making the Practical Byzantine Fault Tolerance (PBFT) announced in 1999 to receive attention again. PBFT is a consensus algorithm in which a valid block is generated when a vote between nodes is conducted before block generation and a vote rate of 75% or more is achieved. Over time, several improved PBFT algorithms have been proposed, but the vulnerability that arises is a problem. Therefore, in this paper, we proposed a consensus algorithm that can be used in low-specification Internet-of-Things (IoT) devices based on the PBFT algorithm and used it for telemedicine for diagnosis and prediction **(Qadri,Y.A, Nauman,A., Zikria,Y.B, Vasilakos,A.V & Kim,S.W.2020, Lao,L, Dai,X, Xiao,B & Guo,S.2020)**

2.Related Works

2.1.Telemedicine

The concept of telemedicine does not have a unified definition for each country, but it is collectively referred to as "*all medical services performed between doctors and patients*" in a non-face-to-face manner using information and communication technology **(Park,H.S, Kim,K, Soh,J.Y, Hyun,Y.H, Lee,B.E, Lee,J.H & Kim,H.S.2020)**. In

addition, telemedicine is defined as "*the act of a doctor treating a patient remotely*" as a concept with a narrower scope than telemedicine **(Qadri,Y.A, Nauman,A, Zikria,Y.B, Vasilakos,A.V & Kim,S.W.2020, Cho,Y.B & Woo,S.H.2018).** In almost all countries with non-face-to-face care, non-face-to-face care is targeted at patients. The Health Resources and Services Administration (HRSA) defines telehealth as "*use of electronic information and telecommunication technologies to support long-distance clinical healthcare, patient and professional health-related education, public health, and health administration*".

Telemedicine is largely classified into three types as follows.

- Telemedicine-Medical personnel diagnose the patient's condition remotely by replacing face-to-face treatment, and treatment such as issuing prescriptions,
- Remote monitoring-Medical personnel continuously monitor the patient's disease condition and manage counseling and education,
- Remote Consultation-A remote medical doctor advises on knowledge or skills about the medical process of a medical professional from a distance.

It is important to secure the number of patients through non-face-to-face medical care while the number of patients for in-person visits has decreased significantly in a pendemic situation such as Corona 19.

The importance of telemedicine, which has emerged as a "New Normal" after the coronavirus, is being debated because of its advantages as cost reduction, improved accessibility to medical institutions, and patient convenience compared to existing face-to-face medical services. Currently, we have various medical equipment for telemedicine including electrocardiogram, blood analyzer, PMS, chemical analyzer, and expensive X-ray and ultrasonic measuring devices. In addition, in telemedicine, the results from medical devices are stored and image information from endoscopy, X-ray, CR, CT, and MRI examinations are transmitted using an image codec. Then, a local doctor checks the transmitted data, conducts remote imaging treatment, diagnoses it, and issues a prescription. This system is based on secured communication. However, as previously mentioned, since manufacturers' medical devices provide each data processing protocol, collision and communication problems among medical devices are very important problems. In addition, the biggest problem in telemedicine is the risk of misdiagnosis and unverified safety problems. The possibility of misdiagnosis is high because the patient is diagnosed during an online interview rather than face-to-face during treatment.

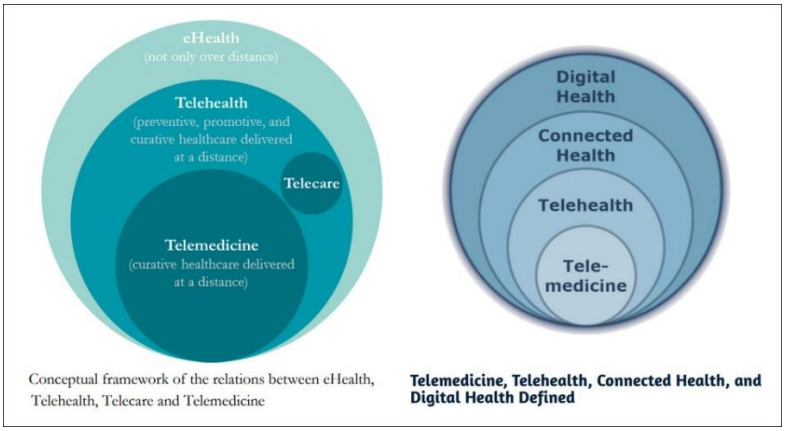

Figure. 1 telemedicine means 'telemedicine' in a narrow sense. if interpreted more broadly, it is sometimes used as 'telehealth'. In a broader sense, it is also interpreted as 'digital health' and 'connected health'.

To address these misdiagnosis and safety problems, telemedicine targets are being operated to follow up for lesions that have occurred especially in chronically ill patients. Thus, it is necessary to utilize a medical-image-reading system that is widely used in medical treatment, which will aid in follow up observation. In addition, telemedicine involves experts in each field in a distributed environment to whom the medical images and diagnostic results of patients for diagnosis are shared, which can solve its limitation on reliability.

2.2.Blockchain

Blockchain refers to a "distributed and shared database" that checks and records various transaction details in electronic transactions between multiple network participants over the Internet without the help of intermediaries. Distributed here does not mean that a part of the large-capacity data is divided and stored for each network participant (node), but it means that all network participants (nodes) store the same data in duplicate (**Kim.H.Y**,**Yun**.**J**,**Goh**.**Y**,**Chung**.**J**.**M**,**2020**)

In blockchain, transaction records are organized in block units, are connected by time, and have a distributed ledger structure. Blockchain does not limit network participants (nodes) and has no access restrictions by administrators, so anyone can participate. It can be divided into a public blockchain that has the right, a private blockchain that can only participate with permission from a service provider (organization), and a consortium blockchain that only certain network participants (nodes) have the authority to participate. Since blockchain maintains a distributed ledger, it is possible to trust the integrity of the ledger among participants. The ledger is accessed by sharing the ledger that connects authentication and authorization using Hyperledger Fabric. In addition, blockchain connects nodes through a distributed network and performs a technology that enables each node to manage the same data in the same order in the environment through a consensus algorithm, resulting to transparent sharing and managing of data. Representative consensus algorithms for public blockchains are Proof of Work (PoW) and Proof of Stake (PoS), and representative consensus algorithms for private blockchains are Paxos, PBFT, and Raft.

PoW of the public blockchain is a universal consensus algorithm that calculates a hash value of a specific difficulty using excessive computing power and calculates and verifies a nonce value by inversely hashing the value. PoS was developed to solve the problem of wasted computing power of PoW, and it grants authority based on the assets held by each node, draws consensus, and distributes rewards.

Paxos of the private blockchain is a method that determines the leader among the connected nodes and achieves consensus through a majority agreement. It has a very simple core compared to the public blockchain, but is not widely applied due to the complexity of operations such as the formula for the leader selection and consensus processes.

PBFT, on the other hand, achieves consensus by using a three-step protocol based on a voting mechanism to improve the uncertainty about the finality of the consensus, which is highlighted as a disadvantage of PoW and PoS, and to supplement the performance of the consensus process. PBFT was adopted and used by Hyperledger Fabric and Eris, which were initially disclosed for reasons such as the efficiency of the consensus process. However, PBFT can guarantee the optimism of consensus compared to public blockchains, but duplicate broadcasts are provided. As all nodes are consensus through the network, the communication cost of the network is high and the burden on the network gradually increases due to the increase in communication volume that is caused by the increase in the number of nodes.

In addition, Raft is a complementary form of Paxos, which has a complex computational process, and is characterized by simplified selection of leaders and candidates through voting and timeout. Raft is operated so that one leader node handles the client’s request and the updated log is reflected to other replicas. If the leader has a problem, a new leader can be quickly selected

3.Efficient and Lightweight Distributed Consensus Algorithm for IoT Environment Telemedicine System

Unlike PoW and PoS, the PBFT blockchain consensus algorithm has the advantage of not generating a block chain after making a decision by majority vote. Therefore, the finality can be secured because the block once confirmed is not changed. In addition, it operates at very high speed because it does not have to repeat calculations until conditions are satisfied, such as PoW.

Even if you want to use fraud, you have to get a majority, and if all participants monitor the leader's movements and judge that it is a lie, even if privacy lies, you can apply for a leader replacement with a majority vote. Therefore, it can be said to be an algorithm with very strong resistance to disability. However, since it is always necessary to communicate with all participants, when the number of participants increases, the amount of communication increases. This means that the throughput is eventually lowered. Therefore, PoW or PoS can create thousands of nodes, but PBFT is limited to dozens of nodes.

3.1.Proposal System Overview

In this paper, we proposed a distributed consensus algorithm that can be used to read medical images in remote medical systems in IoT environments. To ensure the reliability of the telemedicine environment, we proposed an efficient algorithm that can be used in the IoT environment by solving the computing power problem based on the blockchain consensus algorithm and by considering security vulnerabilities. In the proposed algorithm, a private blockchain of experts is built for reading medical images of blockchain consensus. Since the private blockchain is in a state of knowing the information about the participants in advance, a person with a high social reputation or verified among them is selected and authorized for block generation. The algorithm started from the belief that the authority will manage the blockchain network, take charge of the transmission and creation of blocks, and thoroughly verify the blocks to protect social reputation. If verification fails, the authority will lose social reputation.

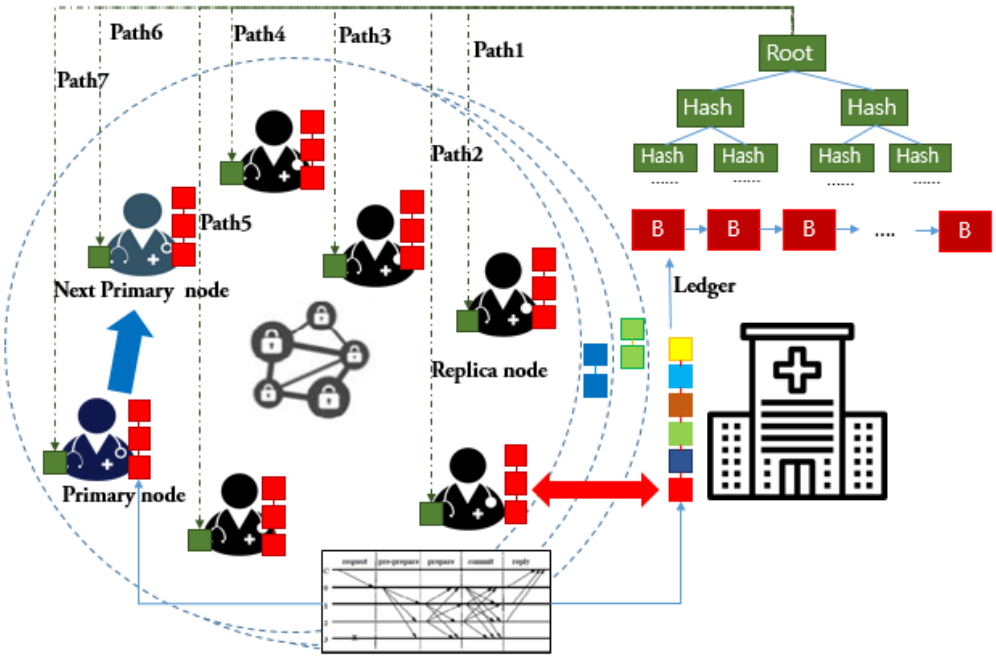

Figure. 1 proposed system overview

Also, since the proposed system considers a distributed environment for consensus on reading medical images based on the PBFT algorithm. Medical imaging experts in each field are distributed in each region, and after registering as image-reading experts through a pre-consortium, the system provides a pool list (Figure 1). The lightweight distributed consensus algorithm proposed herein improves the asynchronous network PBFT consensus algorithm to secure the safety of the distributed consensus medical-image-reading system. In general, reading of medical images is uploaded, and the final diagnosis is decided by agreement for a certain period of time and delivered to the patient. Thus, the proposed system can be used for accurate diagnosis through a number of agreements among experts using asynchronous consensus algorithm.

3.2.Lightweight Distributed Consensus Algorithm

In this paper, we proposed a lightweight distributed sum algorithm suitable for IoT environments. The proposed algorithm improved the basic blockchain PBFT consensus algorithm. In the PBFT consensus algorithm, the primary node does not have a large weight and simply propagates the message received from the client to other nodes. Therefore, this is a burden on the amount of computation in that it is necessary to verify whether the client's message is the correct message to other nodes including the primary node. It is also difficult for the client to check whether the message has been correctly delivered to the node and if the vote received from the node is the correct vote for the correct block. Figure 2 shows the flow chart of the proposed lightweight distributed consensus algorithm, which consists of the following steps: a request to create a new block, a preprepare step to digitally sign a received message and deliver it to other nodes, and a prepare step to confirm message delivery. The steps involved in the proposed algorithm are each described as follows:

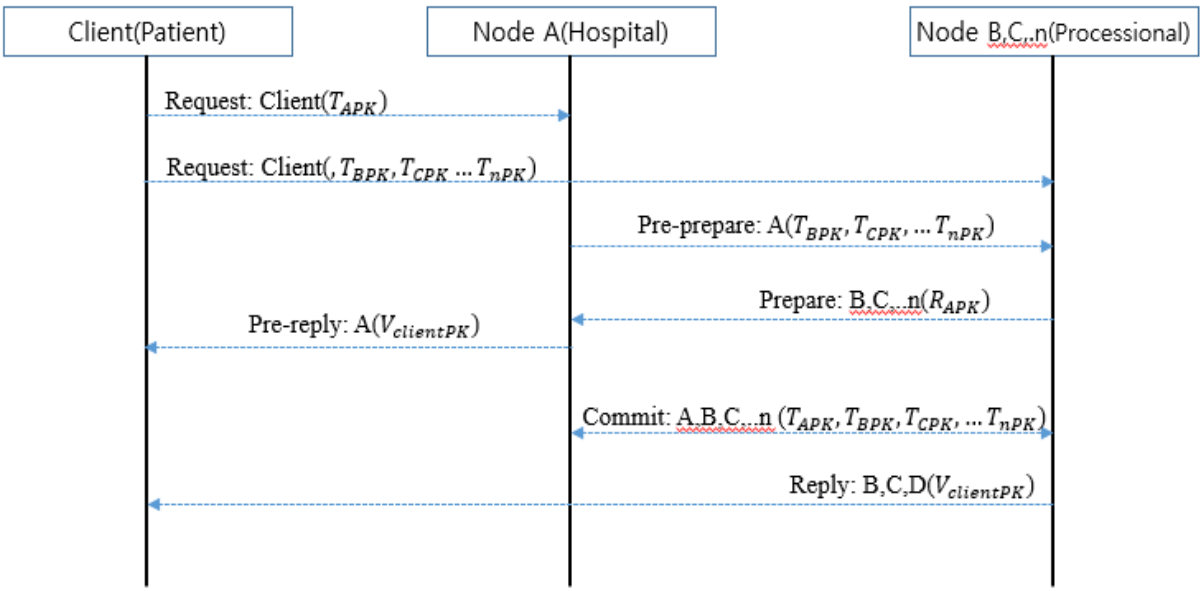

Figure. 2 the proposed lightweight distributed consensus algorithm

- Request step: To create a new block, the client sends an electronically signed message to nodes to check the validity of the block and receive the result. If the client sends a message only to the primary node, in the request step in the proposed algorithm, the client transmits the message T to all other nodes including the primary node.
- Pre-prepare step: The primary node digitally signs the message delivered to the client and propagates it to other nodes. In this process, other nodes compare the message received from the client with the message received from the primary node to see if the primary node delivered the correct message.
- Prepare step. All nodes inform other nodes whether or not they have received a message from the primary node. If the value received from the client and the value received from the primary node are different, it is regarded that an incorrect value is delivered.
- Pre-reply step: The primary node sends its vote value for the validity of the block to the client. The client temporarily stores this value and then compares it with the value sent by the primary node in the upcoming reply process to verify that it has received more than *3/4* of the votes. Through this process, the client can check whether the value sent by the primary node matches the value sent by other nodes in the reply process to be followed. Through this process, it is possible to improve sequential processing, which is a disadvantage of PBFT. If the number of nodes participating in the blockchain network is small, there is no significant difference. However, as the number of nodes increases, the number of packets in the network increases by $2N^2$ in the case of the existing PBFT consensus algorithm. Therefore, the larger the number of participating nodes, the more load is caused to the network. Therefore, the proposed method can suppress the increase in the corresponding index through the pre-reply process. The packet reduction effect of the network occurs by comparing the value transmitted by the primary node first and the value transmitted in the reply process.
- Commit step: All nodes transmit the voted value for the validity of the block to other nodes. Through this process, nonrepudiation can be made. For example, if node *D* votes that the block is invalid for malicious purposes and later changes its position to be valid, verification of *D's* vote value is not possible because different nodes have received *B's* decision during the Commit process.
- Reply step: Nodes other than the primary node transmit the result value to the client. In the existing PBFT consensus algorithm, if the result value for the validity of the block exceeds *3/4* during this process, it is recognized as a correct block and added to the existing blockchain, but in the proposed method, it is compared with the value sent by the primary node in the pre-reply process.
- Calculate step: The client checks whether the value sent by the primary node in the pre-reply process and the value sent by other nodes in the reply process are the same. If the value sent by the primary node and the value sent by other nodes do not satisfy *3/4*, it returns to the request process. If the value sent by the primary node and the value sent by other nodes are the same, a block is added to the live server. Through this process, the reliability of the primary node can be verified. If the wrong value is continuously transmitted to other nodes or the value received in the pre-reply process and the value received in the reply process do not satisfy *3/4*, the client determines that the existing node is not eligible as the primary node, and a new primary node is selected.

4.Experiment and Evaluation

Consensus medical-image-reading system. Based on the security advantages of the existing PBFT consensus algorithm, we compared and analyzed whether a more secure and efficient PBFT consensus algorithm is proposed. In the existing PBFT consensus algorithm, Gatcoin's proposed method increases the block generation speed through parallel processing of blocks by adding a prepare process prior to the preprepare process, and Tendermint uses a locking mechanism to utilize PBFT and DPoS. In the Gatcoin consensus algorithm, by adding a prepare process, blocks are processed in parallel, which can increase the block generation speed. However, as the number of nodes participating in the PBFT consensus algorithm increases, the generation speed rather decreases. In the existing PBFT consensus algorithm, if the total amount of communication is $2N^2$, in the case of Gatcoin, the amount of communication as much as $2N^2 \times N^2$ occurs. Therefore, if the number of nodes is not properly managed, the block processing speed is rather reduced compared to the existing method. Therefore, in this paper, it is possible to maintain a high speed even if many nodes participate by reducing the communication volume of the blockchain network rather than the block generation speed. To this end, by adding a pre-reply process, the reliability of the primary node is improved so that the client can predict the value of the next block to some extent only by communicating with the primary node.

4.1.Confidentiality

In all processes, packet delivery uses asymmetric encryption using the key of RSA bit. The client, the primary node, and other nodes encrypt the packet using their own private key to authenticate that they sent it and encrypt the packet using the public key of the receiving node so that only the relevant node can open it. Since the electronic envelope concept of such asymmetric encryption is used, it is difficult for an attacker to find the original value in the communication among nodes.

4.2.Integrity

In order for a block to be applied to the live server, it must have a hash function that includes the value and transaction details of the last block. In order for an attacker to alter this, he must find a problem with the hash algorithm used in *SHA-2* and find a free image value that satisfies the same value as the existing hash. For the *SHA-2* hash function, it is very difficult to find two different values that are satisfied.

4.3.Availability

The PBFT consensus algorithm only participates in the network by verified users, so nodes participating in the blockchain network can check the contents of the block at any time. This is related to the maximization of Liveness, a characteristic of the blockchain network.

4.4.Efficacy Analysis

The PBFT consensus algorithm determines that a block voted by more than 75% of nodes is a correct block when there are $3N + 1$ nodes. This is a common phenomenon in BFT series algorithms. Therefore, when adding a node, the number of $3N + 1$ must always be satisfied.

Table. 1. Comparison of consensus algorithm

Division	Gatcoin	Tendermint	Proposed
Block generation speed	High	Low	Middle
Network traffic	Low	Middle	High
Primary node reliability	Low	Middle	High

5.Conclusion

In this paper, an improved PBFT consensus algorithm is proposed to solve the problems of the existing PBFT consensus algorithm. As the number of nodes participating in the blockchain network increases, the traffic volume of the entire network also increases, and it was proposed that the burden on the client and the network can be reduced by adding a pre-reply process to reduce the traffic volume. By reinforcing the verification of the reliability of the primary node, even if a node with a malicious purpose participates in the blockchain network, it can be easily

verified. There is a problem that the existing PBFT consensus algorithm is not suitable for large-scale networks. Therefore, in order to improve this, the method described herein adopts a pre-reply process to reduce the number of packets transmitted in the blockchain network and proposes a method that can reduce the amount of communication from $2N^2$ up to $(N-1)^2$ if the value is correct. In addition, compared with other improved PBFT consensus algorithms proposed today, the problem of sequential processing of blocks, which is an existing problem, has been improved by increasing primary trust through the pre-reply process. The advantage of no branching of blocks is that it can be used in fields where accurate records are to be recorded. Since multiple transaction details do not occur, there is no possibility of block branching, and only verified participants exist in the network. Thus, when a problem occurs, it is possible to quickly resolve it. In addition, since the speed of block generation is fast, it will be able to be used in various fields that require real-time transactions.

References

A. Kim,J.Y & Lee,K.I.(2020). Advantages and Necessities of Telehealth Care Service. Journal of the Korean Association of Internal Medicine, 95(4), 217-227.
B. Kumar,R.B, Goren,N.D, Stark,D.E, Wall,D.P & Longhurst,C.A.(2016). Automated Integration of Continuous Glucose Monitor Data in the Electronic Health Record using Consumer Technology. Journal of the American Medical Informatics Association, 23(3), 532-537.
C. Li,X, Jiang,P, Chen,T, Luo,X, & Wen,Q.(2020). A survey on the security of blockchain systems. Journal of the Future Generation Computer Systems, 107, 841-853.
D. Cho,Y.B.(2020). Blockchain based Medical Image Sharing Protocol, Journal of TEST Engineering &Management, 83(1),13059-13068.
E. Tong,W, Dong,X & Zheng,J.(2019). Trust-PBFT: a PeerTrust-based Practical Byzantine Consensus Algorithm. In 2019 International Conference on Networking and Network Applications (NaNA). 344-349.
F. Kim,H, Yun,J, Goh,Y & Chung,J.M (2020). Adaptive Consensus Bound PBFT Algorithm Design for Eliminating Interface Factors of Blockchain Consensus. Journal of Internet Computing and Services, 21(1), 17-31.
G. Qadri,Y.A, Nauman,A, Zikria,Y.B, Vasilakos,A.V & Kim,S.W.(2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communications Surveys & Tutorials, 22(2), 1121-1167.
H. Lao,L, Dai,X, Xiao,B & Guo,S.(2020). G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications. In 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), 664-673.
I. Park,H.S, Kim,K, Soh,J.Y, Hyun,Y.H, Lee,B.E, Lee,J.H & Kim,H.S.(2020). Development and Operation of a Video Teleconsultation System Using Integrated Medical Equipment Gateway: a National Project for Workers in Underserved Areas. Journal of Medical Systems, 44(11), 1-14.
J. Korea Legislation Research Institute. Article 34 of the Medical Service Act. https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=40970&type=abc&key=MEDICAL%20SERVICE%20ACT&param=M Accessed February 27, 2020.
K. Cho,Y.B & Woo,S.H.(2018). Algorithm for Extract Region of Interest Using Fast Binary Image Processing. Journal of the Korea Institute of Information and Communication Engineering, 22(4), 634-640.
L. Lee, J.G, Jun,S, Cho,Y.W, Lee,H, Kim,G.B, Seo,J.B & Kim N.(2017). Deep learning in medical imaging: general overview. Korean journal of radiology, 18(4), 570-584.