Advanced Industrial SCIence
Vol. 3, No. 1, pp. 30-36, 2024
ISSN 2951-2476
https://doi.org/10.23153/AI-Science.2024.3.1.030

IoT 환경을 위한 블록체인 기반의 중요 정보 관리 기법

정윤수
목원대학교 게임소프트웨어공학과 교수

Blockchain-based Important Information Management Techniques for IoT Environment

Yoon-Su Jeong
Department of Game Software Engineering, Mokwon University

요 약 최근 다양한 산업 분야에 적용되고 있는 사물인터넷(IoT)은 자동화와 디지털화하는 과정에서 끊임없이 진화하고 있다. 그러나, IoT 장치가 구축된 네트워크에서는 중간 노드 간의 IoT 중요 정보 관련 데이터의 공유, 개인정보보호 및 데이터 무결성 등의 연구가 아직도 활발하게 연구되고 있다. 본 연구에서는 IoT가 구축된 네트워크 환경에서 중간 노드에 부담을 주지 않으면서 구현이 쉬운 블록체인 기반의 IoT 중요 정보 관리 기법을 제안한다. 제안 기법은 중간 노드에 도착한 IoT 중요 정보에 대해서 임의 크기의 무작위 값을 할당하여 탈중앙화된 P2P 블록체인이 되도록 관리한다. 또한, 제안 기법은 IoT 중요 정보의 가중치 조건에 따라 시간제한, 장치 제한 등의 라이선스를 만들어 IoT 중요 데이터 관리가 수월하여지도록 한다. 성능평가, 제안 기법은 지연시간 및 처리시간이 기존 기법보다 평균 7.6%, 10.1%가 향상되었다.

주제어 : IoT, 블록체인, 탈중앙화, 정보 관리, 머신러닝

Abstract Recently, the Internet of Things (IoT), which has been applied to various industrial fields, is constantly evolving in the process of automation and digitization. However, in the network where IoT devices are built, research on IoT critical information-related data sharing, personal information protection, and data integrity among intermediate nodes is still being actively studied. In this study, we propose a blockchain-based IoT critical information management technique that is easy to implement without burdening the intermediate node in the network environment where IoT is built. The proposed technique allocates a random value of a random size to the IoT critical information arriving at the intermediate node and manages it to become a decentralized P2P blockchain. In addition, the proposed technique makes it easier to manage IoT critical data by creating licenses such as time limit and device limitation according to the weight condition of IoT critical information. Performance evaluation and proposed techniques have improved delay time and processing time by 7.6% and 10.1% on average compared to existing techniques.

Key Words : IoT, Blockchain, Decentralization, Information Management, Machine Learning

*Corresponding Author : Yoon-Su Jeong(bukmunro@mokwon.ac.kr)
Received February 20, 2024
Revised March 5, 2024
Accepted March 20, 2024
Published March 30, 2024

1. 서론

최근 다양한 산업 분야에 적용되고 있는 사물인터넷(IoT)은 자동화 및 디지털화 과정에서 끊임없이 진화하고 있다[1, 2]. 특히, IoT 기반 기술은 효율적인 데이터 관리를 수행하기 위해서 무선 장치를 활용하고 있다. 그러나, IoT를 활용하고 있는 산업 분야는 사이버 공격 중 단일 장애 지점과 사이버 공격 가능성이 크다.

사물인터넷 보안을 연구하는 연구자들은 네트워크 보안을 강화하려고 다양한 시도를 하고 있다[3]. 네트워크 환경에서는 관리자가 개인적으로 데이터베이스에 저장된 데이터에 접근할 수도 있고, 데이터를 안전하게 기록할 수도 있으므로 이를 안전하게 제공하기 위한 보안 솔루션이 요구되고 있다. 이를 해결하는 방안으로써, 사물인터넷은 대용량의 데이터를 효율적으로 관리하기 위해서 머신러닝과 통합하는 추세이다[4].

IoT 데이터 관리를 위해 IoT와 머신러닝(Machine Learning, ML)을 활용하는 동안 다양한 분야에서 사이버 범죄자들의 보안 공격에 직면하게 되었다[5,6]. 산업 분야서는 안전한 블록체인 기술을 활용하여 데이터 관리를 개선할 필요가 있다.

본 연구에서는 IoT 네트워크를 구성하는 구성 요소 중 중간 노드(게이트웨이 등)에 부담을 주지 않으면서 구현이 수월한 블록체인 기반의 IoT 중요 정보 관리 기법을 제안한다. 제안 기법은 중간 노드에 도착한 IoT 중요 정보에 대해서 임의 크기의 무작위 값을 할당하여 P2P 블록체인이 관리되도록 함으로써 비용 절감 및 시간 감소 효과를 얻는다. 제안 기법은 IoT 환경에서 블록체인을 사용함을써 서비스 추적성을 향상시켜 IoT 환경의 효율성과 가시성을 개선시킨다. 또한, 제안 기법은 IoT 중요 정보마다 가중치 정보를 부여한 후 가중치 조건에 따라 시간 제한, 장치 제한 등의 라이선스를 만들어 IoT 중요 데이터 관리가 수월하게 한다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 보안 관련 기존 연구에 관해서 설명한다. 3장에서는 블록체인 기반 IoT 중요 정보 관리 기법을 제안하고, 4장에서는 제안 기법의 실험환경을 구축하여 성능평가를 수행한다. 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

2.1 IoT 보안 위협

최근 IoT 관련 해킹 사고는 과거에 비해 빠른 속도로 증가하고 있다. 특히, 사물인터넷 악성코드(IoT Malware) 공격과 사물인터넷 기기 공격이 증가하는 경향을 보이고 있다. 최근 IoT 공격을 분석해보면 대부분이 사토리(Satory), 미라이(Mirai) 악성코드에 의해 발생하였다. IoT 보안 공격은 더욱 다양해 질다양해질 전망이며, 산업시설 등에 확대 가능성이 매우 크다. Table 1은 한국인터넷진흥원(KISA)이 IoT 제품 유형별 주요 보안 위협에 분석한 내용으로써, 물리적 보안 취약점 및 접근통제 부재, 인증 메커니즘 부재 등으로 인해 보안 위협이 발생하였다.

Table 1. Major security threats by IoT product type

Type	Key products	Key security threats	Key security threat causes
Multimedia products	Smart TVs, smart refrigerators, etc	·All abuse in a PC environment ·Intrusive privacy when built-in cameras/microphones	·No authentication mechanism ·Weak password ·Firmware update vulnerability ·Physical security vulnerabilities
Household appliances	Vacuum cleaners, artificial intelligence robots, etc	·Known operating system vulnerabilities and internet-based hacking threats ·Monitoring the user's privacy through a camera built into the robot vacuum cleaner	·No authentication mechanism ·Firmware update vulnerability ·Physical security vulnerabilities
Network Products	Homecam, network camera, etc	·Send dictionaries and videos to the attacker's server and email ·Infringement of privacy such as arbitrary shooting by remotely controlling home cameras connected to the network	·Lack of access control ·Transmission data protection member ·Physical security vulnerabilities
Control Products	Digital door lock, gas valve, etc	·Any opening and closing of the door lock by deodorizing the control function	·No authentication mechanism ·Weak password ·Lack of access control ·Physical security vulnerabilities
	Mobile apps (web), etc	·Deception of IoT product control function by exposing application source code	·Store certification information plaintext ·Transmission data protection member
Sensor products	Temperature/humidity sensor, etc	·Send incorrect or altered temperature and humidity information	·Transmission data protection member ·No data integrity ·Physical security vulnerabilities

2.2 이전 연구

S. Rahhimi et al. 은 산업 제어 환경에서 VPN 구성에 보안 위반 및 프로토콜 결함에 있어 일부 기능이 제한되어 있는 것을 증명하였다[7]. S. Surendran et al. 은 Brutforce 공격과 암호 분석에 적합한 민감한 데이터를 처리하는 데 적합한 DES 메커니즘 방식을 제안하였다[8]. Choi et al. 은 112bit 및 168bit 크기의 키를 동시에 사용하는 3DES(Triple Data Encryption Standards)가 기존 DES보다 상대적으로 더 강력하지만, 충돌 공격에 취약한 것을 증명하였다[9]. 4. M. Sookhak et al은 허가 유·무에 따른 블록체인을 고려하여 헬스케어에서 EHR 접근통제를 위한 스마트 계약에 초점을 맞춘 연구를 하였다[10]. 헬스케어 분야에서 블록체인 기술을 활용함으로써, 데이터 프라이버시 및 보안을 유지하면서 의료 데이터의 처리 및 공유를 허용함으로써 정보 보안을 강화할 수 있다[11-13]. 이 연구들은 헬스케어 영역의 다양한 블록체인 구현을 조사하고, 응급상황 및 원격 환자 모니터링 시 정확한 진단, 사이버 범죄 보호, 환자 케어보살핌 강화 등 헬스케어의 잠재적 연구 방향과 동향이 제시되어있다.

3. 블록체인 기반 IoT 중요 정보 관리 기법

3.1 개요

IoT는 다양한 환경에서 인터넷에 연결된 내장 센서를 사용하여 자료를 수집하고, 때에 따라 그것에 맞게 반응한다. IoT는 난방과 조명을 자동으로 조절하는 스마트 홈기기부터 산업 장비를 감시하여 문제를 찾은 후 고장 예방을 위해 자동으로 해결하는 지능형 공장에 이르기까지 다양한 분야에 응용되고 있다. 하지만, 이러한 뛰어난 편리성과 가능성에도 불구하고, IoT는 모든 것이 연결된 만큼 해킹 위협도 증가하고 있다.

이 절에서는 클라우드 네트워크 환경에서 중간 노드의 부담을 줄이면서 IoT 장치 구현이 가능한 블록체인 기반의 IoT 중요 정보 관리 기법을 제안한다. 제안 기법은 IoT 네트워크를 구성하는 중간 노드의 안정성 및 효율성을 향상하기 위해서 IoT 중요 정보를 임의 크기로 할당하여 할당된 크기에 임시 값을 부여하여 탈중앙화된 P2P 블록체인 네트워크에서 수행한다. 이때, IoT 중요 정보는 가중치를 부여하여 부여된 가중치 조건에 따라 시간제한, 장치 제한 등의 라이선스를 생성함으로써, IoT 중요 정보의 무결성 및 정확성을 향상한다.

Fig.1은 블록체인 기반으로 IoT 중요 정보 처리 과정을 을 보여주고 있으며, IoT 장치에서 생성된 IoT 중요 정보를 실시간으로 감시하여 업데이트된 IoT 중요 정보를 사전 처리 및 계산 작업을 수행할 수 있도록 한다.블록체인 네트워크는 IoT 중요 정보를 안전하게 처리하기 위해서 트랜잭션(즉, 로컬 및 글로벌 업데이트) 단위로 기록하고 전송할 수 있도록 분산 원장을 제공한다.

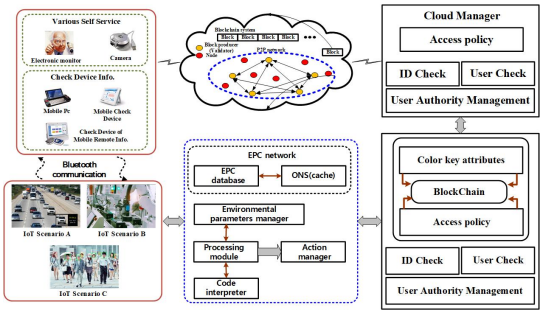


Fig. 1. Proposal scheme based on Blockchain

3.2 IoT 중요 정보의 블록체인 연결 관리

제안 기법은 클라우드 네트워크가 평균적으로 특정 시간마다 블록체인 관리자(Blockchain Manager, 이후 BM이라고 함)에게 IoT 중요데이터에 대한 새로운 블록을 부가한다. 또한, IoT 중요 데이터 처리 시간을 'BM 블록 기간'으로 정의하고, 그에 대응하는 시간 지속 시간을 'BM 체크 포크'라고 정의한다. 추가적으로, BM 체크 포크를 순서 인덱스 n(n=0, 1,…)으로, 블록체인 관리자 블록을 B^n로 나타내고, BM^n 체크 포크에 의해 BM을 업데이트한다. 이 프로세스는 식 (1)과 같이 처리한다.

$$BM^n = BM^{n-1} \,||\, B^n \tag{1}$$

BM 체크 포크가 시작되면 각 노드의 BM은 BM^{n-1}이 되고 새로운 블록을 찾으려고 시도하는 노드는 새로운 블록을 계산한다. 새로운 블록을 성공적으로 계산한 첫 번째 관리자 블록(B^n)은 BM 네트워크에 공지한다. 다른 노드들은 유효성을 확인한 후 B^n에 BM^n을 추가하여 자신의 BM(모두 BM^n과 같은 것으로 가정)를 BM^n에 업데이트하여 공지된 블록 B^n에 대한 합의를 한다, 제안 기법은 BM 에포크는 R^n_{BM}이 되고, 광부가 트랜잭션 t^n_1, …, $t^n_{c^n}$을 수집하여 BM에 기록하고, h^{n-1}은

최신 블록 B^{n-1}의 해시값으로 식 (2) 처럼 정의한다.

$$H(h^{n-1}||t_1^n||...||t_{c^n}^n||r) \in C_{BM} \quad (2)$$

여기서 H는 암호 해시 함수 SHA-256, c^n는 B^n에서 수집할 트랜잭션 수, C_{BM}은 조건을 의미한다. 제안 기법은 식 (2) 에서 왼쪽 항이 오른쪽에 쓰인 조건을 '만족' 한다는 것을 나타내기 위해 '∈'라는 표기법을 사용한다. C_{BM}조건은 BM의 합의 알고리즘에 의해 부과된다. 예를 들어, '작업 증명' 합의 알고리즘을 사용한다면, 조건 C_{BM}은 식 (2) 의 해시값이 고정된 작은 수보다 작아야 한다. 블록(B^n)의 해시값은 식 (3) 처럼 정의된다.

$$h^n = H(h^{n-1} || t_1^n || ... || t_{c^n}^n || r^n) \quad (3)$$

여기서, r^n은 난수를 의미한다.

3.3 IoT 중요 정보 알고리즘

3.3.1 IoT 중요 정보 추가 알고리즘

제안 기법은 중간 노드가 IoT 중요 정보를 교환하기 전에 토큰을 사용하여 데이터 교환의 목적으로 요청 메시지(request message)를 받게 된다. 정보를 교환하고자 하는 IoT 장치는 자신이 인증해야 IoT 중요 정보를 교환할 수 있다. IoT 장치가 P2P 블록 네트워크를 이탈할 경우, 권한 있는 IoT 장치와 동기화해야 한다. Table 2는 IoT 장치를 P2P 블록 네트워크에 추가하는 알고리즘이다. Table 2에서 authorized_node() 함수는 IoT 장치의 MAC 주소를 검증함으로써 non-IoT 장치들이 P2P 블록 네트워크 가입을 허용하는 데 사용된다.

Table 2. IoT Device Addition Algorithm in P2P Block Network

```
Input e New IoT Connection Information Value
Output : Personal information connection status or absence
1: Begin
2:      if(Personal Info. is not Auth.) then
3:        throw
4:      else
5:        if(New Connection Information Value already exists)
then
6:          return false;
7:        else
8:          authorised_node[add new Connection Information
Value]
9:      end if
10: End
```

3.3.2 토큰 알고리즘

Table 3은 제안 기법에서 토큰 추가 관련 알고리즘을 보여주고 있다. 제안 기법은 IoT 장치 간의 추가 통신을 위해 P2P 블록 네트워크에서 성공적인 링크가 이루어질 경우, 토큰을 매핑하여 IoT 장치에 인증서를 교환한다. 만약 non-IoT 장치가 이미 존재한다면, P2P 블록 네트워크 관리자는 요청을 무시한다.

Table 3. Adding Token of IoT Device in P2P Block Network

```
Input: key, trans_id, token
Output: Boolean Value (True/False)
Begin
   while(!(IoT_Device is exist)){
     if (req.sender is not_Auth), then
        throw;
     end if
     mapping token to Non_IoT_Device(tran_id, key) to the
token collection
     return true;
   }
End
```

3.3.3 IoT 중요 정보 교환 알고리즘

중간 노드들은 트랜잭션 수행 시 업데이트되며, P2P 블록 네트워크의 IoT 장치 간에 교환되는 IoT 중요 정보를 쉽게 추적하는 데 도움이 된다. Table 4는 IoT 장치 간 데이터 교환에서, 송신자 IoT 장치와 수신자 IoT 장치 중 어느 하나는 데이터를 교환하기 전에 인증된다.

Table 4. Data Exchange in P2P Block Network

```
Input: key, trans_id, token, data
Output: Boolean Value (True/False)
Begin
   if (req. sender is not_Auth) then
      throw;
   end if
   if (req.receiver is not_Auth) then
      throw;
   end if
   if (Non_IoT_Device is available) then
      Send_data[key,trans_id,token,payload_data];
      return true;
   else
      return false;
   end if
End
```

3.3.4 해시 블록 갱신 및 검증 알고리즘

해시 블록 갱신 및 블록 검증 절차를 수반하는 알고리즘인 SHA-256 암호 해시 메커니즘을 사용한다. 분산형 네트워킹 IoT 장치들 사이에서 데이터를 교환하는 모든 트랜잭션을 갱신한다. 이전 블록의 해시값은 블록의 현재 해시값을 평가한다. 제안 기법에서 해싱은 블록체인 기술에서 새로운 트랜잭션을 생성하고, 트랜잭션을 타임스탬프하고, 결국 이전 블록에 해당 트랜잭션에 대한 참조를 포함하기 위해 광범위하게 사용된다. 새로운 트랜잭션 블록이 블록체인에 추가될 때마다, 그리고 유효하고 관련된 원장 버전을 보장하는 서로 다른 연결된 IoT 장치 간 합의가 업데이트될 때마다, 하나의 방향성 있는 방식의 해싱으로 트랜잭션을 변경하거나 되돌리기가 더 어려워질 것이고, 블록체인을 변경하기 위해서는 막대한 컴퓨팅 자원이 필요하다. 따라서, 해싱은 네트워크에서 블록체인의 암호학적 무결성을 보장하기 위해서이다.

Table 5. Hash block Verification

```
Input: Transaction value for verification
Output: Status of hash verification
Begin
   if(transaction is valid), then
      if (Block.prev_block_hash != prev_Block_Hash) then
         return false;
      else
         return true;
      if(Prev_Block_Hash = Block.Prev_Block_Hash)
         Update BlockiHash;
      end if
   else
      return false;
End
```

4. 평가

제안 기법은 다양한 매개 변수를 고려하여 기존 접근 방식과 비교하여 평가한다. 제안 기법의 무결성은 50개, 100개, 150개, 200개의 블록 P2P 네트워킹 내 중간 노드를 통해 평가되고 있다. 제안 기법은 Table 6처럼 블록체인 네트워크가 트랜잭션을 실행하는 데 걸리는 실행 타임스탬프는 최소, 평균 및 최대 시간으로 구분한다.

Table 6. Represents the execution time for the node registration

No. of Devices	20	100	150	200
Minimum Time (ms)	184	190	198	207
Average Time (ms)	192.5	199.5	206	213.5
Maximum	201	208	214	220

Table 6처럼 교환되는 IoT 중요데이터는 수신되는 각각의 데이터 패킷과 트랜잭션 정보를 처리하는 데 추가적인 시간이 소모되는 각 중간 노드에서 분석, 처리 및 전달이 필요하므로 P2P 블록 네트워킹의 IoT 장치의 증가로 인하여 네트워크 지연시간이 약간 증가하는 것을 알 수 있다. 네트워크 내의 인접 중간 노드의 정보는 경로 추정이 쉽고 더 빠른 데이터 교환을 위해 라우팅 테이블을 업데이트하기 위해 인접 IoT 장치 간에 공유된다.

제안 기법의 시간 지연은 Table 7처럼 네트워킹 IoT 장치 간 IoT 중요 정보의 블록체인 기반 암호화로 인해 발생하는 지연을 보여주고 있다. Table 7에서 얻어진 값들은 SHA-256 기반의 암호화 방식이 경량이고, 네트워크는 IoT 장치 수와 관계없이 동작 지연이 같은 성능을 수행했다.

Table 7. Represents the time delay for sharing the records

Number of Records	50	100	150	200
Time Delay (ms)	82	173	241	357

Table 8은 블록 P2P 네트워크에서 블록체인에 SHA-256을 반영한 결괏값을 나타낸다. 성능은 블록 P2P 네트워크의 가변 개수의 IoT 장치에 대해 128bit 길이의 문자열과 비교하여 평가된다. 처리량은 블록체인 기반 암호화를 통합하여 근사화한다. 암호화 및 원장 업데이트의 중요한 작업은 클러스터 헤드 역할을 수행하는 중간 노드에서 담당하였다,

Table 8. The complexity represents the Delay, Hash Rate, Throughput for the IoT device

Number of Nodes	50	100	150	200
Processing Delay(ms)	60.47	56.12	51.59	47.24
Hash Rate(Mhash/s)	17.34	16.85	16.04	15.57
Throughput(Mbps)	1447	1324	1269	1132

5. 결론

최근 IoT 기술은 다양한 분야에서 사용되고 있다. 그러나 IoT 장치는 다양한 분야에서 송·수신되는 정보가 노출되는 문제점을 가지고 있다. 본 연구에서는 IoT가 구축된 네트워크 환경에서 중간 노드에 부담을 주지 않는 블록체인 기반의 IoT 중요 정보 관리 기법을 제안하였다. 특히, 제안 기법은 중간 노드에 임의 무작위 값을 생성하여 IoT 중요 정보에 적용하였으며, P2P 블록체인이 되도록 중간 노드에서 IoT 중요 정보를 관리한다. 그리고, IoT 중요 정보의 가중치 조건에 따라 IoT 중요 정보의 라이선스를 만들어 IoT 중요데이터의 안전성을 향상시켰다. 성능평가, 제안 기법은 지연시간 및 처리시간이 기존 기법보다 평균 7.6%, 10.1%가 향상되었다. 향후 연구에서는 기존 연구 결과를 기반으로 다양한 IoT 환경에 적용하여 연구를 지속해서 수행할 계획이다.

REFERENCES

[1] Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors, 19(10)*, 2228, 1-26.
DOI : 10.3390/s19102228

[2] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR), 52(3),* 1-34.
DOI : 10.1145/3316481

[3] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematicliterature review of blockchain cyber security. *Digital Communications and Networks, 6(2),* 147-156.

[4] Roh, Y., Heo, G., & Whang, S. E. (2019). A survey on data collection for machine learning: a big data-ai integration perspective. *IEEE Transactions on Knowledge and Data Engineering*, 1328-1347.
DOI : 10.1109/TKDE.2019.2946162

[5] Food & Drug Administration. (2019). Proposed regulatory framework for modifications to artificialintelligence/machine learning(AI/ML)-based software as a medical device (SaMD). 2019.

[6] Lim, D. J., & Kwon, K. S. (2021). Research on The Implementation of Smart Factories through Bottleneck improvement on extrusion production sites using NFC. *Journal of the Korea Academia-Industrial cooperation Society*, 22(2), 104-112.
DOI : 10.5762/KAIS.2021.22.2.104

[7] Rahimi, S., & Zargham, M. (2011). Security analysis of VPN configurations in industrial control environments. In Critical Infrastructure Protection V: 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, ICCIP 2011, Hanover, NH, USA, March 23-25, 2011, Revised Selected Papers 5 (pp. 73-88). Springer Berlin Heidelberg.

[8] S. Surendran, A. Nassef & B. D. Beheshti. (2018). A survey of cryptographic algorithms for IoT devices. *Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale*, 1-8.
DOI : 10.1109/LISAT.2018.8378034

[9] Choi, J., Kim, J., Sung, J., Lee, S., & Lim, J. (2005). Related-key and meet-in-the-middle attacks on triple-DES and DES-EXE. *Computer Vision: Springer Science and Business Media: Berlin/Heidelberg, Germany, 2005,* 3481, 567-576.

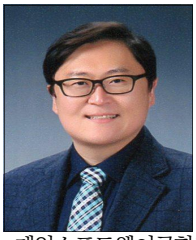
[10] Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. *(2021).* Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, 179, 102950.
DOI : 10.1016/j.jnca.2020.102950

[11] Tandon, A., Dhir, A., Islam, A. N., & Mäntymäki, M. (2020). Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. *Computers in Industry, 122, 103290,* 1-22.
DOI : 10.1016/j.compind.2020.103290

[12] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: a comprehensive review and directions for future research. *applied sciences, 9(9),* 1736.
DOI : 10.3390/app9091736

[13] Avdoshin, S., & Pesotskaya, E. (2019). Blockchain revolution in the healthcare industry. In: Arai K, Bhatia R, Kapoor S, eds. *Proceedings of the Future Technologies Conference (FTC) 2018,* 626-639.
DOI :10.1007/978-3-030-02686-8_47

정 윤 수(Yoon-Su Jeong) [종신회원]



· 1998년 2월 : 청주대학교 전자계산학과 학사
· 2000년 2월 : 충북대학교 전자계산학과 석사
· 2008년 2월 : 충북대학교 전자계산학과 박사
· 2012년 3월 ~ 현재 : 목원대학교 게임소프트웨어공학과 조교수
· 관심분야 : 유·무선 통신 보안, 정보보호, 바이오인포매틱, 헬스케어, 빅 데이터, 클라우드 컴퓨팅
· E-Mail : bukmunro@mokwon.ac.kr