Check for updates

Journal of KIIT. Vol. 19, No. 1, pp. 131-138, Jan. 31, 2021. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2021.19.1.131

블록체인 기반의 물품 반출입 관리 메커니즘

김진수*, 김상춘**, 박남제***

Blockchain-based Product Carry-in/out Management Mechanism

Jinsu Kim*, Sangchoon Kim**, and Namje Park***

이 논문은 2020년도 제주대학교 연구교수 기간에 연구되었음

요 약

일반적으로 사용되고 있는 물품 반출입 기록 관리 시스템은 주로 자산의 관리가 요구되는 조직에서 사용되며, RFID에 기반하여 각 RFID에 기록되어있는 고유한 ID를 서버상에 장치로서 등록하여 관리하게 된다. 이와 같은 방식은 단일 서버의 에러 및 외부의 공격에 의하여 기록되어있는 물품 기록의 무결성이 훼손될 가능성을 가지고 있다. 이러한 문제에 대하여 블록체인은 중심이 되는 서버가 아닌 망구성에 참여하는 다수의 노드를 이용하는 P2P(Peer-to-Peer) 방식을 적용하며, 이는 단일 서버에 의존하는 일반적인 방식에 비하여 데이터의 무결성을 강화할 수 있다. 또한 단일 서버에 의존한 서비스 제공이 아니기 때문에 한 노드의 에러가 전반적인 시스템에 큰 영향을 끼치지 않는다는 장점을 가진다. 본 논문에서는 분산 네트워크 방식의 블록체인을 물품 반출입 기록 관리 시스템에 적용함으로서 단일 서버 방식으로 구성된 물류 관리 시스템의 무결성을 강화하고, 분산화된 컴퓨팅 환경을 통해 관리 시스템의 서비스 가용성을 높일 수 있는 방안을 제안한다.

Abstract

The commodity carry-in/out records management system, which is commonly used, is mainly used in organizations requiring asset management, and based on RFID, the unique ID recorded in each RFID is registered and managed as a device on the server. This method has the potential to damage the integrity of the records of goods recorded by errors and external attacks on a single server. In response to these problems, the block chain applies a peer-to-peer (P2P) approach that uses a large number of nodes participating in the network rather than the central server, which can enhance the integrity of the data compared to the usual way of relying on a single server. It also has the advantage that errors on a node do not have a significant impact on the overall system because it is not a single server dependent service delivery. In this paper, by applying the distributed network-style block chain to the commodity carry in/out record management system, we propose measures to enhance the integrity of the logistics management system composed of single server-style, and to increase the service availability of the management system through distributed computing environment.

Keywords

RFID, block network, carry-in/out record management, block chain

* 제주대학교 융합정보보안학협동과정 박사과정
- ORCID ID: https://orcid.org/0000-0003-1009-3928
** 강원대학교 정보통신공학전공 교수
- ORCID ID:https://orcid.org/0000-0001-9401-4232
*** 제주대학교 초등교육학과 교수(교신저자)
- ORCID ID: https://orcid.org/0000-0003-4434-8933

· Received: Sep. 07, 2020, Revised: Nov. 11, 2020, Accepted: Nov. 14, 2020

· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

물품 반출입 기록 관리 시스템은 일반적으로 조직에서 보유하고 있는 물적 자산에 대해 전반적인 상태의 파악과 효과적으로 자산을 관리하기 위해 다양한 현장에서 적용되는 기록관리 시스템이다. 특히 물적 자산의 관리를 보다 효율적으로 진행하기 위해 원거리 통신태그인 RFID(Radio-Frequency IDentification)를 적용하여 원거리에서도 물적 자산을 파악할 수 있다는 점에서 장점을 가진다. 이와 같은 RFID는 식품, 의료, 산업과 같은 다양한 분야에서 대상에 대한 추적과 감시를 진행하기 위한 하나의 기술로서 적용되고 있다. RFID를 이용하여 사용되는 물품 관리 시스템은 각 물적 자산에 부착되어있는 태크의 식별번호를 사용하여 서버상에서 해당 식별번호를 관리하는 방식을 적용한다[1-2].

단일 서버방식으로 구성된 시스템은 분산형에 비해 단순한 구조를 가지기 때문에 관리가 수월하고, 서버가 단일 방식으로 구성되어있기 때문에 외부와의 연결이 요구되지 않아 높은 폐쇄성을 지닌다. 단일 서버 구성은 위와 같은 장점을 가지나 반대로 단일 서버상의 데이터의 위변조에 대한 사실을 인지하기가 어려우며, 위변조된 데이터의 복원을 위한 추가절차와 비용이 요구된다는 단점을 가진다[3-5].

블록체인은 단일 서버 구성에 의해 발생할 수 있는 단점을 보강하기 위한 효과적인 수단으로서 적용할 수 있으며, 분산형 네트워크에 기반한 공유 원장을 기반으로 기록되어있는 데이터의 위변조 검증뿐 아니라 네트워크 참여자의 다수가 보유하고 있는 데이터로 자동적으로 복원한다. 또한, 에러가 전체적인 네트워크에 큰 영향을 끼치는 단일 서버 방식에 비해 블록체인 네트워크의 특정 노드에서 발생한 문제가 네트워크상에 큰 영향을 끼치지 않으며 서비스의 가용성을 보장할 수 있다[6].

본 논문에서는 조직에서 관리하는 물적 자산에 대한 RFID 기반의 물품 반출입 기록 관리 시스템에 대해 블록체인을 적용함으로써 반출입에 대한 원장 블록과 분산 네트워크 방식을 활용하여 기록된 데이터의 무결성을 강화하고, 반출입 관리 현황을 파악할 수 있도록 하는 메커니즘을 제안하다.

Ⅱ. 관련 연구

2.1 RFID

RFID는 Radio-Frequency IDentification의 약자로 주파수를 이용하여 고유식별번호를 통해 대상을 식별하는 방식을 의미한다. RFID는 전파를 이용하여 원거리에서 정보를 인식하는 기술로써 안테나와 집적회로로 구성되어 식별정보를 가지는 RFID 태그와 안태나를 통하여 전송되는 데이터를 판독하기 위한 RFID 판독기가 요구된다[7]. 적용되는 분야는 일반적인 바코드와 유사하나 원거리의 태그에 대한 식별뿐만 아니라 판독기와 태그 사이의 물체를 통과하여 정보를 수신한다는 점에서 유용하게 사용되고 있다.

2.2 블록체인

블록체인은 관리를 위한 데이터들을 소규모 데이터 규모인 “블록”이라는 단위로 정의하며, 블록의 집단을 체인 형태와 같은 연결고리에 기반한 분산 데이터 저장 환경에 저장함으로서 제 3자에 의한 수정으로부터 데이터를 보호하고, 이 결과를 네트워크 참여자 전체에 공유하는 방식의 분산 컴퓨팅 기술 기반의 원장 관리 기술을 의미한다. 블록체인은 분산 컴퓨팅 환경을 적용하기 때문에 기존의 단일 서버 방식의 중앙화 집적 방식과 달리 탈중앙성을 가지며, 특정 블록의 변경을 위해서는 해당 블록 이후의 모든 블록에 대해 해시연산을 재수행하여야 한다는 점에서 무결성을 강화할 수 있다[8].

2.3 블록체인 기반 RFID 관리 기술 연구동향

RFID와 블록체인을 접목하는 연구는 그 효과성에 의해 많은 연구가 진행되고 있으며, 실제 식품 공급망이나 물품 관리, 물류 공급망 관리 등의 다양한 분야에 적용되었다. 본 절에서는 RFID와 블록체인을 접목한 연구 동향을 소개한다.

Wanjun(2018)은 블록체인과 RFID를 이용하여 조류 식품 안정성의 검증을 위한 발가락지(Foot Ring)을 설계하였다. 해당 연구는 발가락지 형태의 통신

장치를 조류의 발목에 장착시키고, 이를 통하여 조류의 수명주기에 대한 정보를 블록체인에 기록함으로써 조류 식품의 신뢰성을 향상시키는 방법을 설계하였다[9].

Feng Tian(2016)은 중국 농식품 공급망의 신뢰성을 강화할 수 있는 수단으로서 RFID와 블록체인을 접목한 공급망 추적 시스템을 제안하였다. 이 시스템은 공급망의 신뢰성을 보장할 수 없는 환경에 적용하여 농식품 정보 추적을 가능하도록 하여 데이터의 공유를 통하여 무결성을 강화하였다[10].

Petri(2016)는 다수의 조직 단위의 참여자에 의해 구성되는 글로벌 공급망의 실시간 추적의 중요성을 강조하며 다수의 공급망 참여자가 참여하는 공급망과 물류의 실시간 추적 시스템을 제안하였다. RFID를 이용하여 실시간으로 공급망과 공급되는 물류에 대한 정보를 받고 블록체인을 활용해 물류에 대한 무결성을 강화하였다[11].

III. 제안하는 메커니즘

제안하는 블록체인 기반의 RFID 물품 반출입 관리 메커니즘은 공개되어있는 네트워크 상에서 블록 네트워크를 구성하며, 물품의 반출입 관리를 위해 물품의 정보를 기록하는 반출입 목록 블록, 반출입 기록의 관리를 위한 물류 반출입 블록, 조직에서 허가된 사용자에 대한 정보를 기록하는 사용자 정보 블록의 3가지 블록으로 구성된다. 또한 제안하는 메커니즘은 크게 관리자, 사용자, RFID 태그, 관리 시스템, 블록 네트워크로 구성된다. [그림 1]은 제안하는 메커니즘에서 블록 구성을 보이는 것이다.

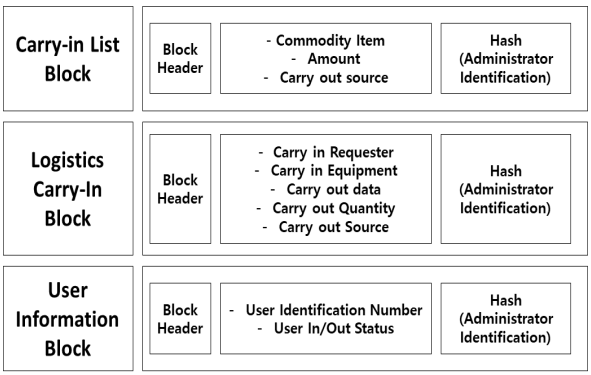


그림 1. 프레임워크 구조
Fig. 1. Framework architecture

시스템의 구성은 반출입 관리를 진행하는 다양한 조직의 관리자가 하나의 블록 네트워크에서 정보를 관리하는 것으로 가정한다. 서로 다른 조직에 속해 있는 관리자에 의해 하나의 블록 네트워크상에서 블록을 생성할 경우 해당 조직의 정보가 동일한 블록 네트워크에 속한 타 조직 관리자에 의해 데이터가 유출될 수 있는 점에 대해 공개키 기반 암호화를 통해 암호화된 내용만을 블록에 기록한다. 블록은 블록의 구조에 대한 정보를 가지는 헤더와 사용자 정보나 물품의 반출입 기록 등을 기록하는 블록 내용, 관리자가 생성한 블록의 식별을 위해 관리자 식별정보를 기록하는 관리자 식별 블록으로 구성하여 식별정보에 따라 정보를 요청할 수 있도록 한다.

제안하는 메커니즘의 전반적인 흐름은 다음과 같이 정리할 수 있다. 먼저 사용자에 의해 물품에 대한 반출입 요청이 발생하는 경우 관리 시스템에서는 블록 네트워크의 사용자 정보 블록을 요청하여 사용자의 인증을 진행하고 사용자 블록 내의 반출입 상태를 통하여 무분별한 반출입을 방지한다. 이후 사용자가 정당한 사용자임이 인증되면 사용자에게 반출입 요청 항목을 보낼 것을 요청하고, 사용자는 자신이 원하는 목록에 대한 정보를 관리 시스템에 전송한다. 관리 시스템은 블록 네트워크로부터 반출입 목록 블록을 요청하여 블록 내의 물품의 항목과 개수, 반출처를 통하여 물품의 현황을 파악하고 반출입이 가능한 경우에만 관리자에게 사용자로부터 반출입 요청이 발생했음을 알린다. 관리자는 관리 시스템으로부터 받은 정보를 검토하고 반출입 허가를 관리 시스템에 전송한다. 반출입 허가를 받은 관리 시스템은 블록 네트워크에 사용자의 식별번호와 요청한 물품, 반출 일자와 반출 수량 등의 기록을 공개키로 암호화하여 물류 반출입 블록의 생성을 요청한다. 이후 블록 네트워크에서 물류 반출입 블록의 생성이 종료되면 해당 사실을 관리 시스템에 전달하고 관리 시스템은 이 사실을 반출입 요청 사용자에게 전달하여 반출입이 허가되었음을 알린다. 블록을 생성하는 과정은 RFID의 신규 물류가 등록되는 과정과 사용자에 의해 물품의 반출입 요청이 발생하는 두가지 단계로 나눌 수 있다. 다음 표 1은 사용된 용어를 정리한 것이다.

표 1. 용어 및 약어
Table 1. Terms and abbreviation

Content	Abbreviation
RSA Encryption	ERSA
RSA Dencryption	DERSA
Commodity list	L
User Identification	IDU
Hash operations	Hash
Administrator public key	PKADM

3.1 RFID 물류 등록 과정

관리자는 RFID 장비를 관리 시스템에 등록하는 권한과 사용자의 반출입 요청에 대한 허가 여부를 판단하는 역할을 수행한다. 관리자는 관리 시스템에 물류에 대한 등록을 진행할 수 있다. 먼저 관리자는 블록 네트워크의 해시 연산을 수행하여 요청한 관리자에 의해 작성된 반출입 목록 블록의 요청을 진행한다. 반환된 반출입 목록 블록에는 RSA 공개키에 의해 암호화된 물품의 항목과 개수 및 반출처 등이 기록되어 있다. 관리 시스템은 블록의 내용을 복호화한 뒤 요청된 물류의 식별정보와 장비의 항목을 토대로 하여 해당 물류의 식별정보를 관리 시스템의 항목과 매칭함으로서 각 식별번호를 항목으로 관리한다. 요청된 식별번호가 기록되지 않은 경우 해당하는 항목에 식별번호를 기록하여 새로운 반출입 물류 블록의 생성을 요청한다. 이후 블록 네트워크는 블록을 생성하고 그 결과를 관리 시스템을 통하여 관리자에게 전송한다. 그림 2는 RFID 물류의 등록 절차를 간략히 보이는 것으로 RFID 물류의 등록 절차는 다음과 같이 진행된다.

1단계 : 새로운 물품의 등록이 요구되는 경우 관리자는 RFID의 식별정보를 토대로 관리 시스템에 등록을 요청한다.

2단계 : 관리 시스템은 관리자의 공개키에 대한 해시를 수행하고 결과값을 기반으로 블록네트워크에 전송하여 반출입 목록 블록을 요청한다.

$$Block\,Identifier = Hash(PK_{ADM}) \tag{1}$$

3단계 : 반환된 반출입 목록 블록은 관리자 비밀키를 통해 복원한다.

$$DE_{RSA}(E_{RSA}(L)) = L \tag{2}$$

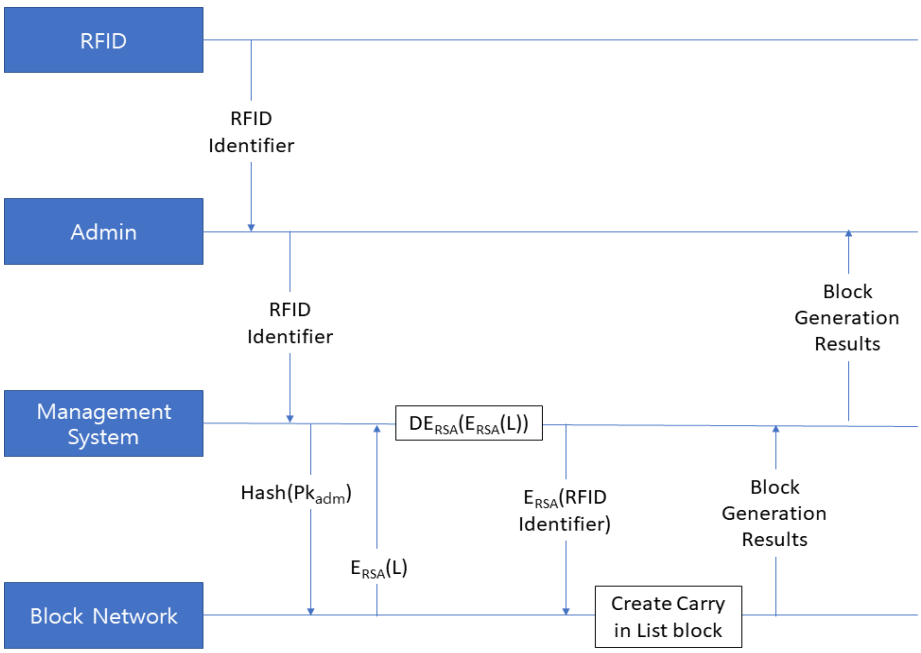


그림 2. RFID 물류 등록 과정
Fig. 2. RFID logistics registration process

4단계 : 블록 정보를 기반으로 물류의 식별정보를 매칭하고 새로운 식별정보의 경우 해당 식별번호를 포함한 반출입 목록 블록의 생성을 요청한다.

$$Carry \in List\,Block = E_{RSA}(RFID\,Identifier) \quad (3)$$

3.2 물류 반출입 요청 과정

사용자는 물류에 대한 반출입 요청을 진행할 수 있다. 반출입 요청의 경우 사용자는 관리 시스템에 물품의 반출입 요청을 전송하고 관리 시스템은 요청한 사용자에게 식별정보를 전송할 것을 요청한다. 사용자는 자신의 식별정보를 공개키를 이용하여 암호화하여 관리 시스템에 전송한다. 관리 시스템은 사용자 인증을 위해 블록 네트워크에 사용자 정보 블록을 요청한다. 사용자 정보 블록을 받으면 사용자 정보 블록의 내용과 사용자 정보를 매칭하여 정당한 사용자인지 인증을 진행하고 정당한 사용자인 경우 반출입 항목을 제출할 것을 요청한다. 이후 사용자는 자신이 희망하는 반출입 항목을 관리 시스템에 전송하고 관리 시스템은 블록 네트워크에 기록되어있는 물류 반출입 블록을 요청하여 요청된 항목을 검토한다. 이때, 반출입이 가능한 경우 관리자에게 반출입 허가 요청을 전송하고, 관리자에 의해 요청이 허가되는 경우에만 블록 네트워크에 물류 반출입 블록과 사용자 정보 블록의 개정을 요청한다. 블록 네트워크로부터 블록의 생성이 정상적으로 이뤄졌음을 확인하는 정보를 관리 시스템에 전송하면 관리 시스템은 최종적으로 허가 결과를 사용자에게 전송한다. 그림 3은 물류 반출입 요청 과정을 보이는 것으로 다음과 같은 절차를 통하여 진행된다.

1단계 : 사용자는 관리 시스템에 반출입 요청을 전송하고 사용자 인증을 위해 사용자의 식별정보를 전송받는다.

2단계 : 관리 시스템은 사용자의 식별정보와 블록 네트워크에 기록되어있는 사용자 정보 블록을 매칭하여 사용자를 인증한다.

$$DE_{RSA}(E_{RSA}(ID_U)) = ID_U \quad (4)$$

3단계 : 허가된 사용자의 경우 요청 목록을 사용자에게 전송하고 물류 반출입 블록을 매칭하여 가능 여부를 확인한다.

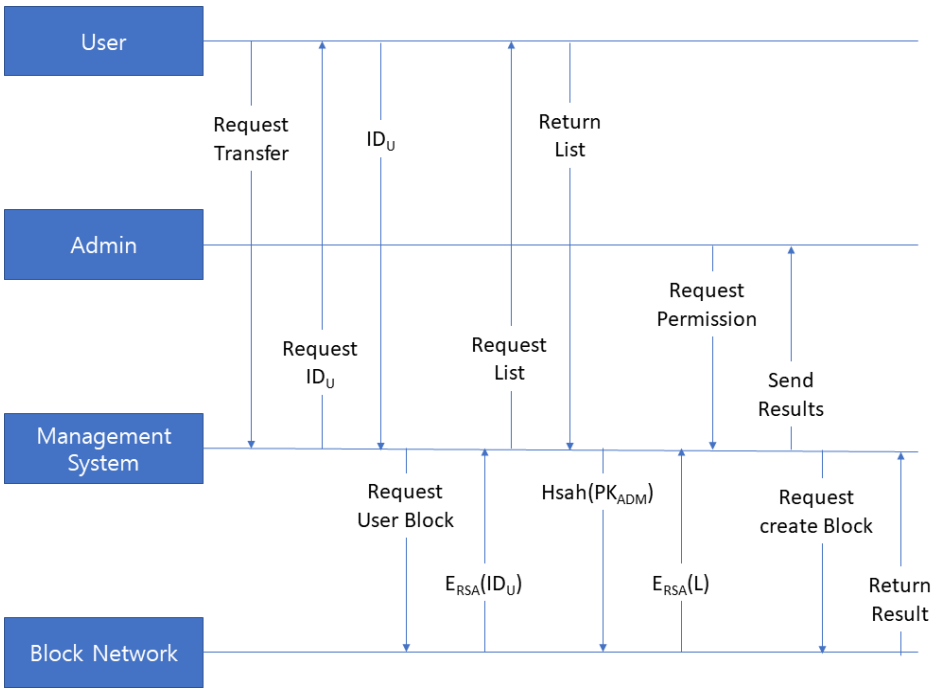


그림 3. 물류 반출입 요청 과정
Fig. 3. Logistics carry-out request procedure

4단계 : 반출입이 가능한 경우 관리자에게 승인을 요청하고, 승인이 되는 경우 블록 네트워크에 사용자 정보 블록과 물류 반출입 블록의 개정을 요청하고, 블록이 정상적으로 생성된 경우 사용자에게 반출입 허가에 대한 정보를 전송한다.

Ⅳ. 분 석

본 절에서는 일반적으로 사용되는 물품 관리 시스템과 제안하는 메커니즘간의 비교분석을 진행한다. 제안하는 메커니즘의 핵심이 되는 내용은 블록체인 적용을 통한 분산 컴퓨팅 환경에서 조직별로 구분된 물품 관리를 제공한다는 점에 있다. 표 2는 제안한 메커니즘과 기존 물품 반출입 관리 시스템의 비교분석을 진행한 것이다.

4.1 무결성

일반적으로 구성되는 물류 반출입 기록 관리 시스템의 경우 단일 서버에 구성되어 정보가 서버에 기록된다. 하지만 제 3자에 의한 위변조가 발생하는 경우, 이를 인지하는 것이 어렵고 복원을 위한 추가적인 비용이 요구된다. 하지만 블록체인은 특정 블록의 변경을 위해 발생한 모든 블록의 해시값을 수정하여야 하며, 블록 네트워크에 참여하고 정보를 공유하는 절반 이상의 사용자 데이터를 변조해야만 한다는 점에서 강화된 무결성을 보장할 수 있다.

4.2 가용성

분산 컴퓨팅 환경은 다수의 노드에 의해 성능이 결정되는 방식이다. 단일 서버에서 치명적 문제 발생은 곧 서비스에 큰 영향을 미치는 결과를 가져오나 블록체인 환경에서의 한 노드에서 발생하는 치명적 문제는 전체적인 네트워크상에 큰 영향을 끼치지 않는다. 이처럼 단일 서버 방식에 비해 블록체인 기반의 물류 반출입 관리 메커니즘은 서비스의 가용성 측면에서 상대적으로 장점을 가질 수 있다.

4.3 기밀성

시스템의 기밀성은 기록되어 있는 정보에 대해 당사자 외에는 접근이 불가해야한다는 측면에서 블록체인은 특성상 기록되는 모든 거래원장은 모든 사용자가 가지기 때문에 기밀성을 보장할 수 없다. 그러므로 거래원장의 기록이 외부에 유출되었을 때 큰 문제가 될수록 폐쇄된 형태의 네트워크 구성이 요구된다. 이와 같은 문제에 대해 제안하는 메커니즘에서는 관리자의 공개키에 의해 암호화된 정보 또는 해시연산 결과값만을 블록에 포함함으로써 그 의미를 해석할 수 없거나, 복원에 요구되는 비용을 발생시켜 접근을 방지하도록 할 수 있다.

Ⅴ. 결 론

일반적으로 물품관리 메커니즘은 일반적으로 식품이나 물품의 유통기록에 대한 정보를 공개하는 것을 목적으로 사용되며, 외부에 대한 공개가 요구되지 않는 물품의 반출입 관리에 적용되는 연구는 많지 않다.

표 2. 일반적인 방법론과 제안된 메커니즘의 비교분석
Table 2. Comparative analysis of proposed mechanisms with existing systems

	Existing management system	Proposal mechanism
Integrity	- single server configuration - Additional procedures and costs for restoring data forgery	- Distributed computing environment - No additional cost for restoring data falsified
Availability	- A fatal error in the server caused a service delivery failure	- Service can be provided in the event of fatal errors on a small number of nodes
Confidentiality	- Closed manganese potential - Blocking access by outsiders who do not know their destination	- Requires open-type mesh - Possibility of data leakage from public networks exists

기록에 대한 무결성 강화는 데이터의 무단 변경을 방지하기 위해 큰 요소로서 적용된다. 기존의 단일 서버의 경우 폐쇄된 네트워크에서 제 3자의 접근을 차단하여 무결성을 강화할 수 있으나, 이 경우에는 데이터의 위변조에 대한 인지가 어렵다. 이 문제에 대해 블록체인을 적용하여 분산형 컴퓨팅 시스템에서 발생하는 장점을 적용할 수 있다. 하지만 데이터가 공개된 상태를 유지한다는 점에서 향후 폐쇄된 네트워크에서 무결성을 강화하거나 공개된 네트워크에서 제 3자의 공격 발생비용을 증가시켜 공격을 예방하는 연구가 요구된다.

References

[1] Jie Xu, Shuang Guo, David Xie, and Yaxuan Yan, "Blockchain: A new safeguard for agri-foods", Artificial Intelligence in Agriculture, Vol. 4, pp. 153-161, Aug. 2020. https://doi.org/10.1016/j.aiia.2020.08.002.

[2] Jinsu Kim and Namje Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing", Personal and Ubiquitous Computing, pp. 1-9, Aug. 2019. https://doi.org/10.1007/s00779-019-01299-w.

[3] Robert Garrard and Simon Fielke, "Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry", Technology in Society, Vol. 62, 101298, Aug. 2020. https://doi.org/10.1016/j.techsoc.2020.101298.

[4] Siye Wang, Shaoyi Zhu, and Yanfang Zhang, "Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems", IEEE Symposium on Computers and Communications. Natal, Brazil, pp. 00074-00077, Jun. 2018.

[5] Jinsu Kim and Namje Park, "Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments", Applied Sciences, Vol. 10, No. 14, Jul. 2020. https://doi.org/10.3390/app10144718.

[6] Peter Verhoeven, Florian Sinn, and Tino T. Herden, "Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology", logistics, Vol. 2, No. 3, pp. 1-19. Sep. 2018. https://doi.org/10.3390/logistics2030020.

[7] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", ELECTRONICS. Vol. 8, No. 7, 735, Jun. 2019. https://doi.org/10.3390/electronics8070735

[8] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree", Multimedia Tools and Applications, Vol. 79, pp. 1-18, Mar. 2020. https://doi.org/10.1007/s11042-020-08776-y.

[9] Petri Helo and A.H.M. Shamsuzzoha, "Real-time supply chain—A blockchain architecture for project deliveries", Robotics and Computer-Integrated Manufacturing, Vol. 63, 101909, Jun. 2020. https://doi.org/10.1016/j.rcim.2019.101909.

[10] Wanjun Yu and Shiyuan Huang, "Traceability of Food Safety Based on Block Chain and RFID Technology", 2018 11th International Symposium on Computational Intelligence and Design, Hangzhou, China, pp. 339-3472, Dec. 2018.

[11] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology", 2016 13th International Conference on Service Systems and Service Management, Kunming, China, pp. 1-6, Jun. 2016.

[12] Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, and Chul Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, San Francisco, California, USA, pp. 1-15, Dec. 2018.

[13] Jinsu Kim and Namje Park, "A Face Image Virtualization Mechanism for Privacy Intrusion

Prevention in Healthcare Video Surveillance Systems", Symmetry, Vol. 12, No. 6, 891, Jun. 2020. https://doi.org/10.3390/sym12060891.

[14] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Peer to Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[15] Guk-Han Jo and Young Joon Song, "State Analysis and Location Tracking Technology through EEG and Position Data Analysis", JAITC, Vol. 8, No. 2, pp. 27-39, Dec. 2018.

[16] Jinsu Kim, Namje Park, Geonwoo Kim, and Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics, Vol. 8, No. 4, 412, Apr. 2019. https://doi.org/10.3390/electronics8040412.

[17] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things(IoT)", Journal of Distributed Sensor Networks, Vol. 12, No. 1, 438, Jan. 2016. https://doi.org/10.1155/2016/2965438.

[18] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conferences of Asia-Pacific Web Conference, Harbin, China, 741-748, Jan. 2006.

[19] Donghyeok Lee and Namje Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", The Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2017.

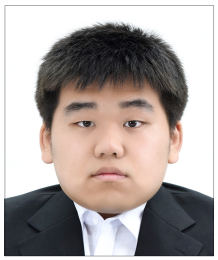
[20] Namje Park and Hyochan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Security and Communication Networks, Vol. 9, No. 6, pp. 500-512, Apr. 2016.

[21] N. Park and D. Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", Personal and Ubiquitous Computing, Vol. 22, No. 1, pp. 3-10, Feb. 2018.

[22] Prince Waqas Khan, Yung-Cheol Byun, and Namje Park, "A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities", Electronics, Vol. 9, No. 3, 484. Mar. 2020. https://doi.org/10.3390/electronics9030484.

저자소개

김 진 수 (Jinsu Kim)



2019년 9월 ~ 현재 : 제주대학교 융합정보보안학협동과정 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT 등

김 상 춘 (Sangchoon Kim)

1999년 8월 : 충북대학교 전자계산학과 박사
1983년 4월 ~ 2001년 3월 : 한국전자통신연구원 선임기술원
2001년 4월 ~ 현재 : 강원대학교 전자정보통신공학부 교수,
관심분야 : IoT보안, 융합보안 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI 정보보호연구단 선임연구원
2009년 1월 ~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 정보교육, STEAM, 정보보호, 암호이론 등