Journal of KIIT. Vol. 17, No. 10, pp. 101-113, Oct. 31, 2019. pISSN 1598-8619, eISSN 2093-7571 101
http://dx.doi.org/10.14801/jkiit.2019.17.10.101

엣지 블록체인 기반의 CCTV 영상 프라이버시 보호 기법

이동혁*, 박남제**

CCTV Video Privacy Protection Scheme Based on Edge Blockchain

Donghyeok Lee*, Namje Park**

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[2019-0-00203,선제적 위험대응을 위한 예측적 영상보안 핵심기술 개발]. 그리고, 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:NRF-2019R1I1A3A01062789)

요 약

최근의 지능형 영상감시 기술은 인공지능 기반 영상분석을 통하여 기존에 제공하지 못했던 선제적 예측감시 등 다양한 서비스의 제공이 가능하게 되었다. 지능형 영상감시에 있어 보안성의 확보는 필수적이며, 원본 CCTV 영상 데이터에 대한 조작이 발생할 경우, 사회적으로 큰 문제로 이어질 수 있다. 따라서 본 논문에서는 블록체인 기반의 지능형 영상감시환경을 제안하였다. 제안한 방식은 CCTV 영상데이터의 위변조 방지를 보장하며, 엣지 블록체인을 통하여 ROI 프라이버시 보호가 가능하여 객체의 프라이버시 노출이 없다는 장점이 있다. 또한, 영상 중복제거가 가능하여 전송 효율을 높이고 스토리지를 절감할 수 있어 효율적이다.

Abstract

Recently, the intelligent video surveillance technology has become able to provide various services such as predictive surveillance that have not been provided previously. Securing the security of the intelligent video surveillance is essential, and malicious manipulation of the original CCTV video data can lead to serious social problems. Therefore, in this paper, we proposed an intelligent video surveillance environment based on blockchain. The proposed scheme guarantees the integrity of the CCTV image data and protects the ROI privacy through the edge blockchain, so there is no privacy exposure of the object. In addition, it is effective because it is possible to increase the transmission efficiency and reduce storage by enabling video deduplication.

Keywords
CCTV privacy, blockchain, cloud security, privacy protection

* 제주대학교 과학기술사회연구센터, 사이버보안인재교육원 학술연구교수
- ORCID: https://orcid.org/0000-0001-7516-469X
** 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수(교신저자)
- ORCID https://orcid.org/0000-0003-4434-8933

· Received: Jul. 24, 2019, Revised: Oct. 15, 2019, Accepted: Oct. 18, 2019
· 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

최근 클라우드/빅데이터 기반의 영상분석 기술이 발전하면서 지능형 CCTV 기술에 대한 관심이 증가하고 있다. CCTV 기반의 영상감시 기술은 과거에도 지속적으로 연구되었으나, 인공지능 기반의 의미론적 영상분석이 가능해지면서 현재의 영상감시 기술은 과거에 비해 크게 진화하고 있으며, 기존에는 제공하지 못했던 사고에 대한 선제적 예측 등 다양한 서비스를 제공하게 될 것이다[1]-[5].

한편, CCTV 기술은 실시간으로 객체의 이동, 상태, 행위 등 다양한 정보를 수집하게 되며, 이 과정에서 프라이버시 침해의 문제가 발생할 수 있다. 특히, 영상기술이 발전하면서 CCTV 데이터에 인공적으로 가공의 인물을 삽입하는 등 악의적인 조작이 이루어진다면 사회적으로 큰 문제가 발생할 것이다. 극단적으로, 특정인이 가지 않았던 장소에 CCTV 영상을 조작하여 해당 얼굴이나 신체적 특징을 임의로 삽입하여 그 장소에 있던 것으로 조작하는 경우를 생각해 볼 수 있다. 인공지능 기반의 영상 기술이 발달하면서 이러한 상황은 불가능한 것이 아니다. 따라서 CCTV 영상데이터는 강력한 보안 장치가 필요한 상황이다.

본 논문에서는 CCTV 영상데이터를 위/변조 위험 없이 안전하게 보관하기 위하여 블록체인 기술을 활용한다. 블록체인 기술은 데이터의 조작으로부터 무결성을 보장할 수 있어 이러한 목적에 적합하며, 분산 원장을 통한 영상정보의 안전한 보관에도 적합하다. 그러나 블록체인 기반의 CCTV 영상데이터 처리에는 대용량 데이터의 무결성 보장, 대용량의 대역폭 문제, 객체의 프라이버시 보호라는 세가지 요구사항이 존재하며, 과거의 블록체인 기반의 영상감시에 관한 연구에서는 이러한 요구사항을 보장하지 못하였다. 본 논문에서는 CCTV 영상감시에 필요한 메타정보 및 영상데이터의 안전한 보관을 가능하게 하는 새로운 기술을 제안하였다. 제안한 기술은 본 논문에서 제안한 엣지 블록체인 기술을 기반으로 영상의 조작 방지, 대역폭 절감, 객체 프라이버시 보호, 대용량 데이터의 효율적이고 안전한 전송 및 저장 방법을 제공하는 특징을 가진다[6]-[9].

Ⅱ. 관련 연구

2.1 블록체인 개요

2.1.1 블록체인

블록체인이란 블록으로 그룹화된 트랜잭션의 분산 디지털 원장이라고 볼 수 있다. 블록체인의 주요 작동원리로, 신규 생성 대상 블록에 대한 유효성을 확인하고 이에 대한 합의 과정을 거친 후 새로운 블록으로 인정하고 이전 블록과 연결하게 된다. 이렇게 추가되는 새로운 블록은 네트워크 내 모든 노드에 복제가 이루어지며, 만약 이 과정에서 충돌이 발생할 경우에는 사전 설정된 규칙으로 해결할 수 있다. 그러나 이러한 새로운 블록이 추가될 경우 이전의 블록을 수정하기는 매우 어렵다는 특징을 가지므로 무결성에 대한 보장이 가능하다[10]-[15][27].

블록체인에서의 단일 블록은 이전 블록헤더의 해시값을 포함하는 방식으로 이전블록과 서로 연결되어 유기적으로 블록체인을 형성한다. 이전에 생성된 블록에 변경이 발생한 경우에는 해시값이 서로 달라진다. 이러한 경우, 이후의 모든 블록도 다른 해시값을 갖게 되어 무결성의 확인이 가능하다. 이러한 방식으로 변경된 블록을 쉽게 감지하고 거부할 수 있다. 그림 1은 일반적인 블록체인의 구성을 나타낸다.

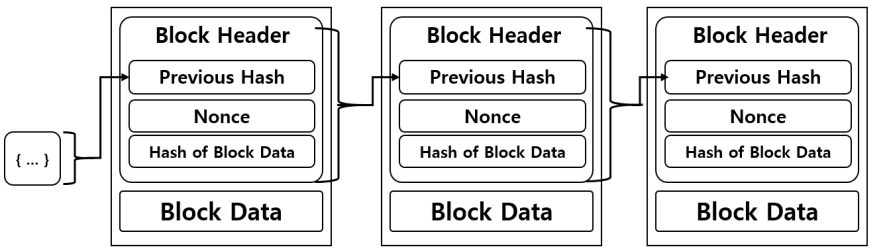

그림 1. 일반적인 블록체인의 구성
Fig. 1. Configuration of blockchain

이러한 블록체인 기술을 지능형 영상감시 환경에 접목하면 큰 장점을 가질 수 있다. 특히, 영상에 대한 위/변조 방지 및 무결성 보장이 가능하다는 점에서 블록체인 기술과의 접목이 요구되는 상황이다.

2.1.2 블록체인의 유형

일반적으로 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인으로 구분할 수 있다. 퍼블릭 블록체인의 경우, 어떤 노드도 시스템에 가입하고 탈퇴할 수 있다. 따라서 각 노드는 완전히 분산된 피어 투 피어 시스템과 유사한 측면이 있다. 그러나, 프라이빗 블록체인은 시스템에 참여할 수 있는 노드를 결정하는 접근제어 메커니즘이 별도로 있다. 따라서 모든 노드가 인증되어야 한다. 이러한 관점에서 보안상의 측면에서 프라이빗 블록체인이 훨씬 안전하다고 볼 수 있으며, 본 논문에서 제안한 방식도 프라이빗 블록체인으로 구성되어야 한다.

하이퍼레저(Hyperledger)는 현재 가장 대중적인 프라이빗 블록체인 중 하나이다. 퍼블릭 블록체인의 가장 잘 알려진 예인 비트코인의 경우 합의알고리즘으로 작업증명방식(PoW)를 사용하나, 이 방식은 비결정적이고 계산 비용이 많이 든다는 단점이 있으므로 대량의 처리에는 적합하지 않다. 현재 Zab, Raft, Paxos, PBFT 등의 합의 알고리즘이 활발히 사용되고 있다. 프라이빗 블록체인인 하이퍼레저의 경우 PBFT 프로토콜을 합의 알고리즘을 사용하고 있으나, 1.0의 경우 Kafka 기반의 순서제공 서비스를 바탕으로 한 프로토콜을 사용하고 있다.

2.2 기존의 영상감시 연구

CCTV 영상데이터는 대용량 데이터라는 특징이 있으며, 이는 데이터 보관 측면에서의 한계점을 야기한다. 향후 CCTV 화질의 개선으로 인해 영상 데이터의 용량은 더욱 커질 것으로 보이며, 이는 대용량의 스토리지 용량을 필요로 하며, 영상 데이터 처리에서의 비용 문제와 직결되어 있다. 따라서 현재는 CCTV에서 촬영된 영상은 일정 기간을 제거하는 방식으로 처리되고 있다. 물론, 치안 목적을 달성한 영상에 대해서는 스토리지에서 제거하는 것이 바람직하나 특정 목적에 의해 필수적으로 보관해야 할 영상의 경우는 장기간 보관이 필요할 수 있으며, 이러한 대용량 영상 처리에 대한 별도의 대책이 필요한 상황이다. D. A. Rodríguez-Silva 등은 영상감시를 위한 클라우드 환경을 제안하였다[1][6]. 대용량 데이터를 취급해야 하는 지능형 영상감시 환경 특성을 고려하여 Amazon S3 기반의 확장 가능한 클라우드 영상감시 아키텍쳐를 제안하고 있다. 해당 논문에서는 SSL 프로토콜 기반의 종단간 암호화를 고려하고 있으나, 클라우드 상에 탑재된 영상데이터에 대한 메타정보 및 영상데이터에 대해서는 어떠한 방식으로 보안기술을 적용할 것인지에 대해서는 언급하고 있지 않으므로 보안성에 취약한 측면이 있다.

또한, Yena Jeong 등은 블록체인 기반의 영상 감시 시스템을 제안하였다[2]. 해당 시스템은 신뢰가능한 내부 관리자가 있는 블록체인 네트워크로 구성되며, 영상정보의 메타데이터를 블록체인 기반의 배포 원장에 기록하는 것이 특징이다. 마찬가지로, Pierluigi Gallo 등은 블록체인 기반의 IoT 영상감시 환경을 제안하였으며, 스마트시티 환경에서의 비디오 감시를 위하여 블록체인 기반으로 메타정보를 안전하게 처리하는 방법을 설명하고 있다[3][16][17].

이러한 방식은 영상 메타정보의 신뢰성 있는 안전한 관리방안을 제공할 수는 있으나, CCTV 영상데이터 자체가 훼손될 경우에 대한 문제는 해결하지 못하고 있다. 즉, 영상감시 환경에서는 메타정보뿐만 아니라 원본데이터인 대용량 CCTV 영상데이터를 모든 노드에 전파하는 것이 주요한 관점이며, 이를 위해 영상데이터를 손실없이 안전하게 보관할 수 있는 구조가 필요하다[18]-[20].

한편, 영상데이터에 대한 프라이버시 보호기술이 필요하다. CCTV에는 기본적으로 정보주체가 미인지된 상태로 개인정보가 실시간 수집되며, 이러한 영상정보는 비인가된 사용자나 악의적인 공격자에 의해 해킹이 발생하면 개인 프라이버시의 심각한 훼손이 발생할 수 있다. 특히, 영상 객체의 동의 없이 개인정보를 상업적 혹은 정치적으로 활용하는 경우, 혹은 영상 객체의 개인정보 파기 및 삭제요구에 대한 사후조치가 필요할 수 있으며, 이러한 경우 개인정보 얼굴 마스킹 기법 적용이 필요하다. 얼굴 마스킹은 일방향 마스킹 기법, 혹은 복원이 가능한 ROI 영역의 부분 암호화 방식, 스크램블링 방식 등

다양한 기법이 존재하며, 필요시 이러한 프라이버시 마스킹을 추가적으로 적용할 수 있어야 한다[21]-[26].

이를 위해 본 논문에서는 엣지 블록체인 기반의 CCTV 영상감시 구조를 제안하였다. 제안한 기법은 영상의 메타정보 뿐 아니라, CCTV 영상데이터 전체를 안전하게 관리할 수 있으며, 영상 민감정보를 엣지 블록체인에 별도로 보관하는 방법으로 프라이버시를 보장함으로써 앞서 연구된 기법들에 비해 더욱 안전한 CCTV 영상감시 환경을 제공한다.

III. 새로운 블록체인 기반 영상처리 기법 제안

본 장에서는 블록체인 기반 CCTV 영상감시 환경을 위한 기술적 요구사항을 살펴보고, 엣지 블록체인 기반의 안전한 영상정보 처리기법을 제안한다.

3.1 제안 기법 개요

본 논문에서는 안전한 지능형 CCTV 영상감시 시스템을 구성하기 위하여 블록체인을 활용하였다. 특히, 엣지 블록체인이라는 신뢰된 영역에서의 블록체인을 별도로 구성하는 방법을 제안하였으며, 이를 통하여 CCTV 영상정보에서 촬영객체의 프라이버시를 보호할 수 있으며 비식별화된 상태로 안전하게 클라우드 서버에 영상정보의 업로드가 가능하다. 또한 중복제거 기술을 통하여 전송시의 대역폭을 절감하여 효율적인 영상감시 환경 구성이 가능하게 하였다. 여기에서 엣지 블록체인은 프라이빗 블록체인으로 구성하여 외부에서의 불법적인 접근을 차단할 수 있어야 하며, 메타 블록체인은 허가형 블록체인으로 구성하여 적절한 권한을 가진 자는 접근이 가능하여야 한다.

3.2 CCTV 기반 영상감시의 요구사항

본 절에서는 블록체인 기반의 CCTV 영상감시 환경을 위하여 효율성 및 보안성 관점에서의 기술적인 요구사항을 분석한다. CCTV 기반의 지능형 영상감시 환경에서는 이러한 요구사항이 반드시 고려될 필요가 있으며, 본 논문에서 제안하는 블록체인 기반의 CCTV 영상데이터 처리방식을 통하여 이러한 요구사항을 해결할 수 있다.

3.2.1 영상 데이터의 무결성 보장

영상데이터는 전송과정에서 손실되거나, 원본이 훼손되지 않아야 한다. 즉, CCTV에서 촬영된 정보와 실제 스토리지 서버에 저장된 정보가 다르지 않다는 것을 검증할 수 있어야 한다. 즉, 원본과 동일함을 검증 가능해야 하며, 위/변조 등 해커에 의한 악의적인 데이터 훼손이나, 혹은 다른 원인에서의 변경이 발생하였다면 감지가 가능해야 한다.

3.2.2 대역폭의 최소화

CCTV에 촬영된 영상데이터는 대용량이라는 특징을 가지며, 이러한 점은 처리 과정에서 큰 대역폭을 발생시켜 성능을 저하시키는 원인이 될 수 있다. 이러한 한계를 극복하기 위하여 중복제거 등 다양한 방식을 활용하여 대용량 영상데이터를 전송 및 저장할 경우에도 최소한의 대역폭을 갖게 하여 보다 효율적으로 처리할 수 있어야 한다.

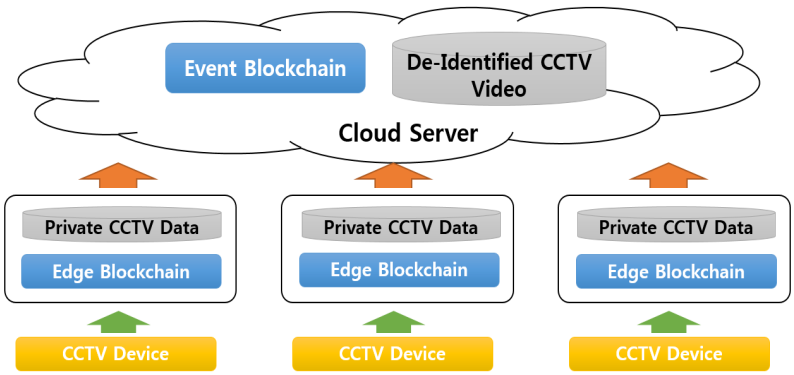

그림 2. 제안 방식 개요
Fig. 2. Overview of proposed method

3.2.3 객체 프라이버시 보호

CCTV 영상데이터는 객체의 이동경로, 얼굴, 행동양식 등의 정보를 고스란히 담고 있어 프라이버시 마스킹 등 적절한 기법을 활용하여 객체의 프라이버시가 침해받지 않도록 해야 하며, 필요시에는 권한이 있는자가 원본 영상을 복원할 수 있어야 한다. 또한, 서버에 해킹이 발생하더라도 영상 민감정보가 노출되지 않도록 적절한 사전조치가 필요하다.

3.3 세부사항

본 절에서는 블록체인 기반의 CCTV 영상 프라이버시 보호를 위한 세부 구성 방법을 설명한다.

3.3.1 표기법

본 논문에서 제안한 방식의 설명에 필요한 약어는 표 1과 같다.

3.3.2 CCTV 영상정보의 블록체인 구성

CCTV 영상정보를 블록체인에 구성하게 될 경우, 그림 3과 같이 구성이 가능하다. CCTV에서 촬영되는 영상은 대용량 데이터로써 블록체인상에 영상정보를 그대로 저장하기에는 가용성 측면에서 한계가 있다. 따라서 블록체인에는 영상정보에 대한 속성정보인 메타정보를 저장하고, 해당 파일은 별도의 데이터 스토리지에 저장하여 연결관계를 지을 수 있다. 특히, 영상에 대한 Merkle Tree는 블록헤더상에서 가지고 있으며, 이러한 방식을 활용하면 무결성을 보장하는 블록체인의 장점과, 확장성이 강한 클라우드의 장점을 동시에 가질 수 있다. 여기에서, CCTV에서 촬영되는 데이터는 블록체인 및 스토리지 구성의 용이성을 위하여 특정 길이의 구간만큼 블록단위로 분할하여 처리하게 된다.

표 1. 약어
Table 1. Notation

Abbreviation	Description
K	Preshared secret key
D	CCTV video data
D_i	i-th video block data
D_{DI}	DeIdentified video data
$h(\cdot)$	Hash result
$E(\cdot)_K$	Value encrypted with key K
ED	Event detection data
ROI	Region of interest

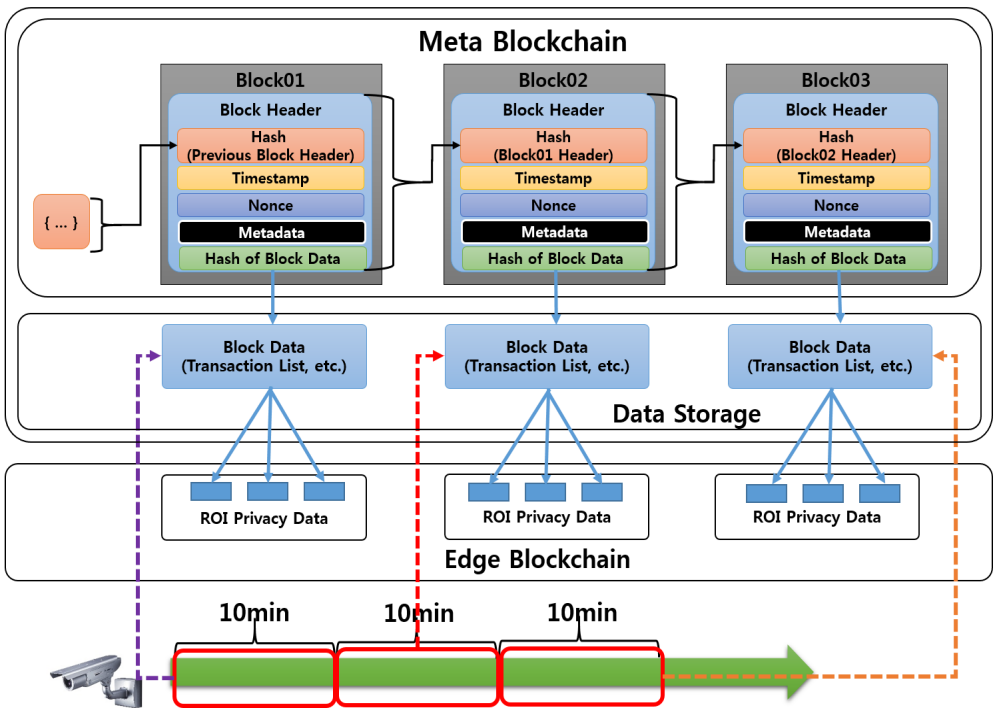

그림 3. CCTV 영상의 블록체인 구성
Fig. 3. Blockchain construction of CCTV video

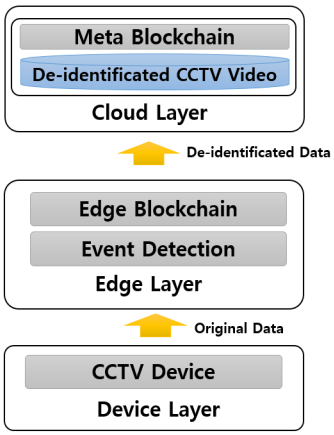

그림 4. 계층단위 데이터 흐름
Fig. 4. Hierarchical data flow

3.3.3 계층단위 데이터 흐름

CCTV에서 영상이 촬영되면 해당 정보는 엣지 계층(Edge Layer)에서 가공을 거친다. 이를 위해, 영상에 대한 이벤트 감지가 필요하다. 이벤트 감지를 통해 영상 내에 개인정보 침해요소가 없는지를 판단하고, 만약 개인정보 침해 요소가 있을 경우 해당 ROI 영역을 원래 영상에서 마스킹 등으로 안전하게 처리하고 해당 ROI 영역의 원본은 별도로 엣지 블록체인에 저장한다.

여기에서 엣지 계층은 신뢰된 영역으로 가정하고 있으며, 특히 엣지 블록체인은 프라이빗 블록체인 형태로 구성하여야 한다. 즉, 엣지 블록체인은 외부에서의 불법 접근을 차단할 수 있어야 한다. 엣지 계층에서 적절한 객체 비식별화를 거친 영상을 클라우드 서버에 전송하게 되며, 클라우드 서버는 이를 기준으로 메타 블록체인을 추가하고, 스토리지에 해당 영상을 저장한다. 여기에서, 클라우드 서버에는 비식별화된 CCTV 영상정보가 있으며, 만약 해커에 의해 영상정보가 노출되더라도 개인 프라이버시는 노출되지 않는다는 특징이 있다.

3.3.4 엣지 블록체인

엣지 블록체인은 CCTV 영상정보를 안전하고 효율적으로 처리하기 위해 보조적으로 필요한 블록체인으로 정의할 수 있으며, 엣지 블록체인 내에는 이벤트 감지 데이터와 ROI 프라이버시 데이터를 저장한다.

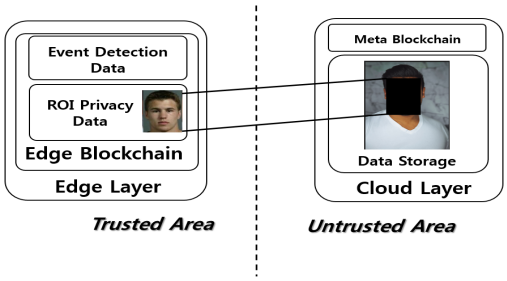

그림 5. 엣지 블록체인
Fig. 5. Edge blockchain

구체적으로, 최초 영상에서 이벤트 분석을 수행하고, 이를 기반으로 프라이버시의 침해 소지가 있는 민감정보에 대한 ROI 영역을 추출하고 해당 부분영상을 저장한다. 또한, 이 단계에서 CCTV 영상 데이터는 적절한 얼굴정보 마스킹이 수행되어 개인이 누구인지를 식별할 수 없도록 조치하여 클라우드 서버에 전송한다. 이 경우, 신뢰된 영역인 엣지 블록체인에서만 민감정보를 가지게 되고, 신뢰되지 않은 클라우드 서버에는 객체를 식별할 수 없는 비식별화된 영상정보만 남게 된다. 필요시 적절한 권한을 가진자는 엣지 블록체인으로부터 ROI 영상정보를 요청하여 해당 ROI 내의 원본 부분영상을 가져와서 원본 영상정보를 복원할 수 있다.

만약, 개인정보 침해 요소가 큰 영상일 경우 엣지 블록체인에 큰 용량의 데이터를 저장해야 할 경우도 발생할 수 있다. 이러한 경우 정책에 따라 영상 가운데 안면 인식이 가장 용이한 부분만을 선별하여 일부 영상만을 저장하는 방식으로 엣지 블록체인의 용량을 절약하는 방법도 고려할 수 있다.

엣지 블록체인은 개인정보 열람 권한을 가진 자에 한하여 접근권한을 가지며, 특히 로그 기록을 통해 책임추적성을 확보할 수 있어야 한다.

또한, RBAC과 같은 접근제어기법을 활용하여 개인정보에 불필요하게 접근할 수 없도록 하여야 한다. 여기에서 블록체인을 통해 보다 안전한 접근제어의 수행이 가능하다. 특히, ACL이나 접근제어 정책을 블록체인에 보관할 경우, 정책에 대한 접근 및 사용 기록 등을 관리할 수 있어 부정한 방법으로 접근을 시도한 경우를 확인할 수 있다. 아울러, 블록체인의 특성상 위변조가 불가능하다는 장점이 있어 접근내역의 위변조 방지 및 책임추적성도 확보할 수 있다. 특히 얼굴영상정보는 개인정보로서 이

에 대한 불필요한 접근을 안전하게 차단할 필요가 있으며, 얼굴영상정보에 대한 열람 내역 및 변조 방지 기록을 남기는데 블록체인이 효과적으로 이용될 수 있다. 즉, 접근제어 정책이나 ACL, 접근내역을 블록체인으로 관리하는 것으로 기존의 접근제어보다 더욱 안전하게 엣지 블록체인을 관리할 수 있으며, 신뢰할 수 있는 접근제어를 수행할 수 있다.

3.3.5 이벤트 기반 중복제거

엣지 계층에서는 이벤트 분석 처리를 통하여 영상 중복제거를 수행한다. 이론적으로, 영상정보의 블럭단위에 대한 파일 바이트 단위의 중복제거를 시도할 경우 미세한 차이라도 존재한다면 실제로 중복제거의 효과를 거의 기대할 수 없게 된다. 이는 클라우드 스토리지 용량 차원에서 큰 부담이 되는 측면이 있다. 그림 6에는 이벤트 기반 중복제거 방식을 나타낸다. 즉, (a)와 (b)는 영상 자체로는 미세하게 다른 부분이 있으나, 실제로 이벤트 분석을 수행할 경우는 (a)와 (b)는 동일한 결과가 발생한다. 따라서, 영상의 (a)블럭과 (b)블럭은 파일 바이트 단위로 비교할 경우 실질적으로 다른 내용을 가지고 있더라도, 이벤트 분석결과에 대한 비교치로는 동일한 영상으로 간주하고 중복처리가 가능하다. 즉, 영상 이벤트 분석결과에 대한 Merkle Tree를 비교하여 (b)에 대한 중복제거를 수행할 수 있다.

(a) (b) (c) (d)

그림 6. 이벤트 기반 중복제거
Fig. 6. Event-based deduplication

그림 7은 이벤트 기반 중복제거가 적용된 경우를 나타내고 있다. 실질적으로 메타 블록체인에서의 영상데이터 A에서 추출된 이벤트 정보와 영상데이터 B에서 추출된 이벤트 정보는 동일하다. 즉, 스토리지에서는 동일한 영상데이터 A와 B를 중복으로 저장할 필요가 없다. 이벤트 단위당 하나의 영상파일만 저장한다면 스토리지 공간의 획기적인 절감이 가능하고, 엣지 계층과 클라우드 계층(Cloud Layer)간 통신 과정에서의 대역폭 절감효과도 기대할 수 있다.

그림 7은 이벤트 기반 중복제거가 적용된 상태를 나타낸다. 각 계층별로 설명하면 다음과 같다.

① CCTV에서 촬영된 영상은 특정시간 단위로 구분(블록화)된다. (예를 들어 5분, 10분 등)

② 엣지 계층에서는 CCTV에서 촬영된 영상의 각 블록을 수신한다. 수신한 각각의 블록에 대해서 이벤트를 추출하고, 이벤트에 대한 해쉬값을 추출한다. 만약, 이벤트 해쉬값이 동일할 경우, 중복 제거 대상 블록으로 판단 가능하다.

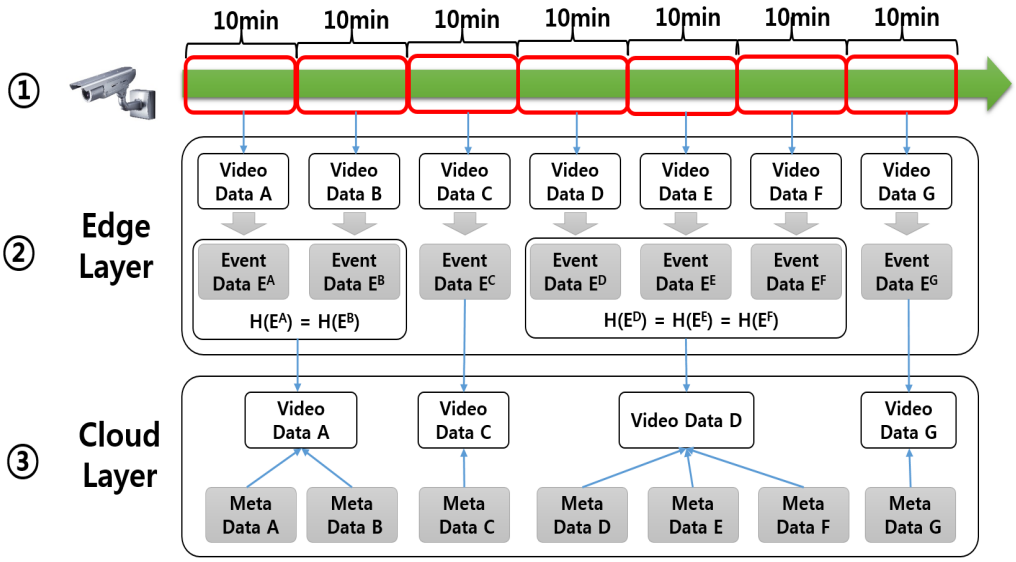

그림 7. 이벤트 기반 중복제거 적용
Fig. 7. Example of event-based deduplication

③ 클라우드 계층에서는 중복된 블록에 대한 영상 파일은 하나의 블록만 가진다. 한편, 영상에 대응하는 메타데이터는 모든 블럭 단위로 가지고 있다. 영상데이터와 메타데이터는 1:n 관계로 매핑 정보를 가진다.

이벤트는 배회, 침입, 방화 등 다양한 이벤트가 검출될 수 있다. 영상분석을 통하여 검출가능한 이벤트의 예는 표 2와 같으며, 경우에 따라 이 외에도 다양한 이벤트가 추가될 수 있다.

표 2. 이벤트 검출의 예
Table 2. Example of event detection

Event	Description
Wander	The whole body of the person wanders over a certain area for more than 5 seconds
invasion	A situation in which a human body invades a certain area and enters
Arson	Situations where smoke or flames occur immediately after a person's wandering
Fire	If a fire occurs naturally in an area where no human is detected
Throwing	When a person throws garbage, dirt, or explosives into a certain area
Accident	If you come in contact with a certain person while driving a car, motorcycle, etc.

이벤트 중복제거를 적용할 경우, 정책에 따라 이벤트 중복제거 레벨을 설정할 수 있다. 레벨 1~2의 경우는 중요도가 높은 영상에 한하여 작지만 중요한 영상차이 분석이 필요할 경우에 적용될 수 있다. 영상의 중요도에 따라 표 3과 같은 이벤트 중복제거 레벨의 설정이 가능하다.

표 3. 이벤트 중복제거 레벨
Table 3. Event deduplication level

Deduplication Level	Description
1	Do not perform deduplication
2	Delete after checking by the administrator for the deduplicated block
3	Delete all deduplicated blocks after a certain period of time
4	Deduplication only if video object is not detected
5	Delete blocks immediately when deduplication is detected

경우에 따라, 영상의 중요도가 매우 높거나 정밀한 분석이 요구될 경우는 이벤트 중복제거를 통한 효율성 보다 정밀한 영상분석이 더 중요할 수 있다. 이벤트 중복제거 레벨 정책은 1~5단계로 설정할 수 있으며, 영상 자체를 증적으로 남겨야 하거나, 면밀한 영상분석을 위해 1단계로 설정하여 모든 영상에 대하여 중복제거를 수행하지 않게 할 수 있다. 또한, 2단계로 설정하여 중복제거된 블록에 대하여 관리자에 의한 확인을 거친 후에 최종 제거할 수 있으며, 3단계로 설정하여 중복제거된 모든 블록은 일정 기간(예를 들어, 30일)만 보관하고 삭제하는 방법을 적용할 수 있다. 4단계에서는 영상객체 검출건수가 0일 경우, 즉, 영상 자체에 감지되거나 이동하는 객체가 전혀 없다고 판단되는 경우에 한하여 삭제 처리를 수행하고, 5단계에서는 중복제거 감지시 해당 블럭을 즉시 삭제하여 공간 효율성을 높인다.

3.3.6 CCTV-엣지간 전송 프로토콜

CCTV 장치와 엣지 계층간 전송 프로토콜은 그림 8과 같다. CCTV와 엣지 계층간은 인터넷을 거치므로 적절한 암호화가 필요하다. 여기에서, 암호화 키 K는 각 계층간 사전 공유된 값이어야 하며, 인터넷을 통한 영상정보 전송시는 암호화가 필요하다.

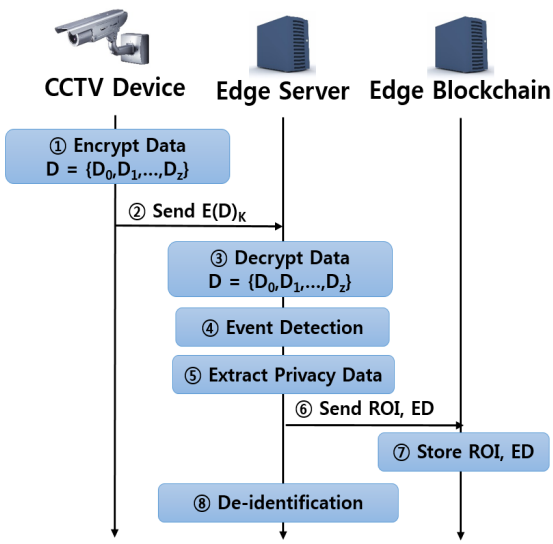

그림 8. CCTV-엣지간 데이터 전송 프로토콜
Fig. 8. CCTV-to-edge data transfer protocol

암호 알고리즘은 AES와 같이 검증된 암호 알고리즘을 사용해야 하며, 효율성이 요구될 경우 LEA와 같은 경량 암호 알고리즘이 사용될 수 있다.

프로토콜을 단계별로 설명하면 다음과 같다.

① CCTV는 영상정보를 블럭 처리를 위하여 일정한 시간대로 분할하고, 암호화를 수행한다.

② CCTV는 엣지 서버에 암호화된 데이터를 전송한다.

③ 엣지 서버는 암호화된 데이터를 사전 공유된 키로 복호화 처리하여 원본 데이터를 얻는다.

④ 엣지 서버는 전송된 CCTV 영상 데이터에 대하여 이벤트 검출을 수행한다.

⑤ 엣지 서버는 앞서 분석된 이벤트로부터 민감정보를 판단하여 ROI 영역을 추출한다.

⑥ 엣지 서버는 엣지 블록체인에 ROI 영상과 이벤트 검출정보를 전송한다.

⑦ 엣지 블록체인은 ROI 영상과 이벤트 검출정보를 저장한다.

⑧ 엣지 서버는 영상정보에 대하여 비식별화를 수행하고, 원본 영상정보는 마스킹 처리된다.

3.3.7 엣지-클라우드간 전송 프로토콜

엣지-클라우드간 전송 프로토콜은 먼저 클라우드에 이벤트 기반의 중복되는 CCTV 영상블럭이 있는지를 판단하고, 중복되지 않은 데이터를 선별하여 클라우드 서버에 전송하여 클라우드 스토리지 및 메타 블록체인에 저장하는 과정이다.

세부 단계를 설명하면 다음과 같다.

① 엣지 서버는 클라우드 서버에 이벤트 해시 리스트를 전달한다. 이벤트 해시 리스트는 이벤트 Merkle-Tree이며, 이벤트 해시 리스트가 동일한 데이터는 중복으로 저장할 필요가 없다.

② 클라우드 서버는 메타 블록체인으로부터 이벤트 해시 리스트를 검색한다.

③ 메타 블록체인은 동일한 이벤트 해시리스트의 존재 여부 결과를 응답한다.

④ 엣지 서버는 동일한 해시리스트를 갖는 블럭을 제거한 영상데이터를 클라우드 서버 키 K로 암호화하여 전달한다.

⑤ 클라우드 서버는 전송된 데이터를 복호화한다.

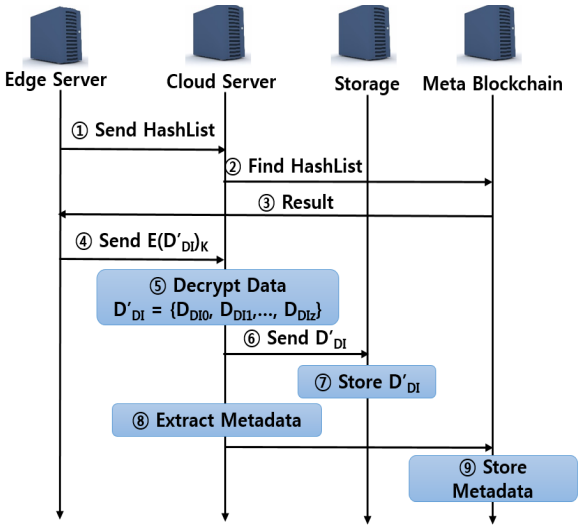

그림 9. 엣지-클라우드간 데이터 전송 프로토콜
Fig. 9. Edge-to-Cloud data transfer protocol

⑥ 클라우드 서버는 스토리지에 복호화한 데이터를 전송한다.

⑦ 스토리지는 데이터를 블럭단위로 저장한다.

⑧ 클라우드 서버는 파일 블럭에 대한 메타정보를 추출한다.

⑨ 메타 블록체인에 추출한 메타정보를 저장한다.

VI. 안전성 및 효율성 분석

4.1 안전성 분석

4.1.1 영상정보의 기밀성

제안한 방식에서는 CCTV 장치 계층, 엣지 계층, 클라우드 계층간 통신 과정에서 암호화를 수행하여 전송하므로 데이터 전달 과정에서 스니핑 공격이 발생하더라도 사전 공유되어 있는 키 K를 획득하지 못하면 원본을 확인할 수 없다. 특히, 엣지 계층과 클라우드 계층간 통신하는 정보는 비식별화된 정보이며, 이 가운데 엣지 블록체인은 프라이빗 블록체인으로써 클라우드와 엣지 블록체인간 각각의 데이터가 분산되므로 공격자가 클라우드 서버를 해킹하더라도 유의미한 정보를 확인하기 어렵다.

4.1.2 무결성

무결성 보장은 블록체인이 갖는 가장 큰 장점 중 하나이다. 본 논문에서 제안한 방법은 지능형 CCTV

영상감시 환경을 블록체인을 통해 프라이버시 보호와 무결성을 갖도록 하는 것이 특징이며, 특히 무결성에 대한 부분은 엣지 블록체인과 메타 블록체인의 두가지 블록체인이 사용되므로, 공격자가 클라우드 및 엣지 계층 모두의 블록체인 데이터를 조작하기란 매우 어렵다. 즉, 본 논문에서 제안한 기법은 무결성 측면에서 큰 장점을 가진다.

4.1.3 프라이버시 보호

본 논문에서 제안한 방식은 민감 ROI 영역을 엣지 블록체인에 별도로 보관하는 것으로써 메타 블록체인, 스토리지와 엣지 블록체인의 데이터를 모두 얻지 못하면 의미있는 영상정보를 복원할 수 없다. 특히, 엣지 블록체인은 프라이빗 블록체인으로써 사용자의 식별 가능한 정보만 별도로 분할되어 엣지 블록체인에만 저장되며, 상대적으로 해킹의 가능성을 배제할 수 없는 클라우드 스토리지에는 비식별화된 정보만 저장하므로 프라이버시 측면에서 안전을 보장할 수 있다.

4.2 효율성 분석

4.2.1 전송의 효율성

본 논문에서 제안한 기법은 엣지 서버와 클라우드 서버의 통신간 이벤트 해시 데이터를 확인 후 중복되지 않은 영상 블록만을 업로드하므로 전체 영상 데이터를 업로드하지 않는다는 장점이 있다. 이러한 측면은 중복된 블록이 많이 발생할수록 전송에 있어 효율성을 가져온다. CCTV 영상데이터는 대용량의 정보이며, 효율적인 전송을 위한 중복제거를 적용함으로써 전송 효율을 크게 높일 수 있다.

4.2.2 스토리지 절감 측면

중복제거는 데이터 전송의 효율성을 높임과 동시에 스토리지의 효율성을 높일 수 있다. 클라우드 스토리지의 절감은 곧 비용 절감으로 이어지는 큰 장점이 있다. 향후 CCTV 화질 개선 등 영상정보의 보관을 위해 더 많은 스토리지 공간이 필요한 시기가 도래할 확률이 높으며, 특히 블록체인 환경에서는 다수의 노드가 동일한 원장을 공유하므로 용량 절감이 주요한 이슈가 될 것이다. 본 논문에서 제안한 영상 중복제거 기법은 이러한 측면에서 큰 장점을 갖는다.

4.3 기존 방식간의 비교

기존의 D.A.Rodríguez-Silva 등이 제안한 방식은 대용량 데이터를 취급해야 하는 지능형 영상감시 환경의 특성을 고려한 Amazon S3기반의 확장가능한 클라우드 영상감시 아키텍쳐를 제안하였다. 이는 특정 벤더에 의존하는 것으로, 영상중복제거, 프라이버시 보호 기능에 있어 명확하다고 볼 수 없다. 한편, Yena Jeong 등이 제안한 블록체인 기반 영상감시 기술은 영상정보의 메타데이터 기반에 적용하는 것이 특징이며, Pierluigi Gallo의 기법 또한 이러한 방식을 채택하고 있다. 그러나 실제 영상정보를 별도 보관하는 것은 프라이버시 문제를 완전히 해결하지 않는다. 또한, 영상중복제거에 대한 부분에 별도의 언급이 없어 대역폭 상 한계점이 존재한다.

본 논문에서 제안한 방식은 엣지 블록체인을 통하여 프라이버시 문제를 해결하였고, 영상중복제거 기능을 지원함으로써 영상 전송 과정에서의 효율성을 높였다.

표 4. 기존 방식간 비교
Table 4. Comparison between existing methods

Method	Distributed environment	Deduplication	Security
Rodríguez-Silva[1]	○	△	△
Yena Jeong[2]	○	×	○
Pierluigi Gallo[3]	○	×	○
Proposed method	○	○	○

Ⅴ. 결 론

CCTV 기반의 지능형 영상감시 기술은 지속적으로 발전하고 있으며, 최근 인공지능 기술의 비약적인 발전으로 인하여 선제적 예측감시와 같은 기존에 제공하지 못한 다양한 서비스를 제공할 수 있게 되었다. 그러나 지능형 영상감시 기술에는 프라이버시 노출 문제, 데이터 조작 등과 같은 역기능이 발

생할 수 있어 이에 대한 대비는 필수적이다.

따라서 본 논문에서는 블록체인 기반의 CCTV 영상데이터 처리기법을 제안하였다. 제안한 기법은 대용량의 영상정보를 안전하게 저장할 수 있고, 전달 과정에서의 대역폭을 최소화할 수 있다. 또한, 저장과정에서 프라이버시 노출이 없다는 장점을 가지고 있다. 특히, 블록체인의 장점인 위/변조 공격으로부터 안전하다는 장점을 그대로 가지고 있어 인공지능 기반의 지능형 감시환경에 적합하다.

이를 위해 먼저 2장에서 블록체인과 지능형 영상감시환경의 개요를 살펴보고, 블록체인 기반의 영상감시에 대한 연구 동향을 살펴보았다. 또한 3장에서는 지능형 영상감시 환경에 필요한 기술적 요구사항을 먼저 살펴보고, 세부적인 전송 및 저장 절차를 설명하였다. 또한 4장에서는 안전성과 효율성 측면에서의 분석을 진행하였다.

블록체인 기술은 무결성이 요구되는 인공지능 기반의 지능형 CCTV 환경에 매우 적합하다. 특히 CCTV 영상보안 기술은 개인의 프라이버시 문제와 직결된 만큼, 블록체인 기술 등 강력한 보안 기술을 적용하여 설계되어야 할 것이며, 이에 대한 다양한 연구가 향후에도 지속적으로 필요할 것이다.

References

[1] D. A. Rodríguez-Silva, L. Adkinson-Orellana, F. J. Gonz'lez-Castaño, I. Armiño-Franco, and D. Gonz'lez -Martínez, "Video surveillance based on cloud storage", 2012 IEEE Fifth International Conference on Cloud Computing, IEEE, Honolulu, HI, USA, pp. 991-992, Jun. 2012.

[2] Yena Jeong, Dongyeop Hwang, and Ki-Hyung Kim, "Blockchain-Based Management of Video Surveillance Systems", 2019 International Conference on Information Networking (ICOIN), IEEE, Kuala Lumpur, Malaysia, pp. 465-468, Jan. 2019.

[3] Gallo, Pierluigi, Suporn Pongnumkul, and Uy Quoc Nguyen, "BlockSee: Blockchain for IoT Video Surveillance in Smart Cities", 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/ I&CPS Europe), IEEE, Palermo, Italy, pp. 1-6, Jun. 2018.

[4] Michael Kerr, Fengling Han, and Ron G. van Schyndel, "A Blockchain Implementation for the Cataloguing of CCTV Video Evidence", 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, Auckland, New Zealand, pp. 1-6, Nov. 2018.

[5] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Journal of Sensors (Basel), Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[6] Jinsu Kim and Namje Park, "Electronic iLightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing", Personal And Ubiquitous Computing, https://doi.org/10.1007/s00779-019-01299 -w, 2019.

[7] Mendki, Pankaj, "Blockchain Enabled IoT Edge Computing", Proceedings of the 2019 International Conference on Blockchain Technology, ACM, Honolulu, HI, USA, pp. 66-69, Mar. 2019.

[8] Waheed, Amtul, and Jana Shafi, "Efficient Cyber Security Framework for Smart Cities", Secure Cyber-Physical Systems for Smart Cities, IGI Global, pp. 130-157, 2019.

[9] 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", Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[10] G. Medioni, I. Cohen, F. Bremond, S. Hongeng, and R. Nevatia, "Event detection and analysis from video streams", IEEE Transactions on pattern analysis and machine intelligence, Vol. 23, No. 8, pp. 873-889, Aug. 2001.

[11] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network

Environment", Journal of AWNTA, pp. 741-748, Jan. 2006.

[12] 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, pp. 412(1-15), Apr. 2019.

[13] Karuna B. Ovhal, Sonal S. Patange, Reshma S. Shinde, Vaishnavi K. Tarange, and Vijay A. Kotkar, "Analysis of anomaly detection techniques in video surveillance", 2017 International Conference on Intelligent Sustainable Systems (ICISS), IEEE, Palladam, India, pp. 596-601, Dec. 2017.

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

[15] Pierluigi Gallo, Suporn Pongnumkul, and Uy Quoc Nguyen, "BlockSee: Blockchain for IoT video surveillance in smart cities", 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/ I&CPS Europe), IEEE, Palermo, Italy, pp. 1-6, Jun. 2018.

[16] Naveed Islam, Yasir Faheem, Ikram Ud Din, Muhammad Talha, Mohsen Guizani, and Mudassir Khali, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services", Future Generation Computer Systems, Vol. 100, pp. 569- 578, Nov. 2019.

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

[18] Deeraj Nagothu, Yu Chen, Erik Blasch, Alexander Aved, and Sencun Zhu, "Detecting Malicious False Frame Injection Attacks on Surveillance Systems at the Edge Using Electrical Network Frequency Signals", Sensors, Vol. 19, No. 11, 2424, May 2019. doi: 10.3390/s19112424.

[19] 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. 2016, No. 1, Jan. 2016. doi: 10.1155/2016/2965438.

[20] Andrei Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations", Proceedings of the 6th international workshop on trustworthy embedded devices, ACM, Vienna, Austria, pp. 45-54, Oct. 2016.

[21] Ji Hee Han, Sang Hun Ok, Kyu Song, and Dong Young Jang, "CCTV Monitoring System Development for Safety Management and Privacy in Manufacturing Site", Journal of The Korean Society of Manufacturing Technology Engineers, Vol. 26, No. 3, pp. 272-277, Jun. 2017.

[22] Namje Park and Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[23] Donghyeok Lee and Namje Park, "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.

[24] 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, pp. 735, Jul. 2019.

[25] Jinsu Kim and Namje Park, "Inteligent Video Surveilance Incubating Security Mechanism in Open Cloud Environments", Journal of KIIT, Vol. 17, No. 5, pp. 105-116, May 2019.

[26] Seok-Cheon Park, "Design and Implementation of Personal Information Identification and Masking System Based on Image Recognition", Journal of IIBC, Vol. 17, No. 5, pp. 1-8, Oct 2017.

[27] Soyeong Ji, Seungeun Kim, Eunju Yun and

Dae-Young Seo, "Time Synchronization between IoT Devices in a Private Network using Block-Chain", Journal of IIBC, Vol. 18, No. 5, pp. 161-169, Oct 2018.

저자소개

이 동 혁 (Donghyeok Lee)

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2018년 2월 : 제주대학교 컴퓨터교육학과 공학박사
2007년 6월 ~ 2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월 ~ 2015년 6월 : KT 플랫폼개발단 과장
2018년 3월 ~ 현재 : 제주대학교 과학기술사회연구센터, 사이버보안인재교육원 학술연구교수
관심분야 : 블록체인, 클라우드, 지능형 영상감시 시스템, IoT, 컴퓨터교육 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 일반대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 교육부 창의교육거점센터장, 과학기술사회(STS)연구센터 부센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등