도시 안전을 위한 블록체인 기반의 감시카메라 영상 관리 시스템 모델 및 설계 방법

(Block-Surveillance: Blockchain-based Surveillance Camera Video Management System Model and Design Method for City Safety)

이지운*, 서희석**

(Ji Woon Lee, Hee Suk Seo)

요 약

이 논문에서는 현대 도시 관리에 필수적인 요소로 자리 잡은 비디오 감시 시스템에 대한 새로운 접근 방식을 제안한다. 블록체인과 IPFS를 활용하여 데이터의 무결성과 프라이버시 보호를 강화하고, 객체 탐지 기술을 통해 이상 행위 탐지 및 영상 자동 저장함으로써 도시 안전과 보안을 향상시킬 수 있다. 이 통합 접근법은 감시 시스템의 효율적인 관리 방법론이 되어 도시 관리자와 시민들에게 더 안전하고 효율적인 감시 환경을 제공할 것이다.

■ 중심어 : 블록체인 ; 분산파일시스템 ; 객체탐지 ; 감시카메라 ; 도시안전

Abstract

This paper proposes a new approach to video surveillance systems, which have become essential components in modern urban management. By utilizing blockchain and IPFS, it enhances data integrity and privacy protection. Additionally, anomaly detection and automatic video storage are enabled through object detection technology, thus improving urban safety and security. This integrated approach serves as an efficient management methodology for surveillance systems, providing city administrators and citizens with a safer and more effective monitoring environment.

■ keywords : Blockchain ; IPFS ; Object Detection ; City Safety

Ⅰ. 서 론

오늘날 비디오 감시 시스템은 지난 수십 년 동안 도시 관리에 필수적인 도구로 자리 잡았다. 이 시스템들은 범죄 예방, 교통 관리, 공공 서비스의 효율성 향상 등 다양한 목적으로 활용되며, 도시 안전을 위한 중요한 수단으로 인식되고 있다. 그러나 대규모 감시카메라 네트워크의 효과적인 관리와 운영은 데이터 무결성, 프라이버시 보호 등의 측면에서 중요한 과제를 안고 있다[1]. 이러한 문제를 해결하기 위해, 본 논문에서는 블록체인(Blockchain)과 IPFS(InterPlanetary File System) 기술을 활용한 새로운 감시카메라 영상 관리 시스템을 제안한다. 블록체인은 분산된 원장 기술로서 데이터의 무결성과 투명성을 보장하며, 중앙 집중식 관리의 필요성을 줄여준다. 이 기술을 감시카메라 영상 관리 시스템에 적용함으로써, 데이터의 안전한 저장과 전송, 신뢰할 수 있는 접근 관리, 그리고 개인정보 보호를 강화할 수 있다[1,2]. 제안하는 블록체인 기반의 감시카메라 영상 관리 시스템은 객체 탐지 기술을 통한 이상 행위 탐지 및 해당 영상의 자동 저장 기능을 포함한다. 이는 도시 안전을 향상하는 데 중요한 요소로, 특히 대규모 감시 시스템에서의 효

* 정회원, 한국기술교육대학교 융합학과 기술연구원

** 정회원, 한국기술교육대학교 컴퓨터공학부 교수

이 논문은 2023년도 한국기술교육대학교 교수 교육연구진흥과제 지원에 의하여 연구되었음

접수일자 : 2023년 12월 27일 게재확정일 : 2024년 01월 29일

수정일자 : 1차 2024년 01월 11일, 2차 2024년 01월 25일 교신저자 : 서희석 e-mail : histone@koreatech.ac.kr

율적인 관리와 운영을 가능하게 한다.

객체 탐지 기술은 실시간으로 감시카메라가 촬영한 영상을 분석하여 특정 행동 패턴이나 이상 징후를 자동으로 식별한다[3]. 예를 들어, 무단 침입, 의심스러운 움직임, 교통 규칙 위반 등이 탐지되면, 시스템은 즉시 해당 영상을 자동으로 저장하고 필요한 경우 경보를 발령할 수 있다. 이는 보안 관리자가 신속하게 대응할 수 있도록 하며, 사후 분석과 증거 수집에도 중요한 역할을 한다. 또한, 블록체인과 IPFS 기술의 적용은 이러한 영상 데이터의 무결성과 보안을 강화한다. 각 영상은 블록체인과 IPFS에 기록되어 변경이나 조작할 수 없으며, 이는 법적 증거로서의 가치를 높인다. 블록체인과 IPFS의 분산된 특성은 중앙 집중식 데이터 저장소의 취약점을 해소하고, 대규모 감시 시스템에서 발생할 수 있는 데이터 관리의 복잡성을 줄여주고, 기술 통합이 어떻게 대규모 감시 시스템의 관리를 효율적으로 운영될 수 있는지에 대한 방법론이 될 수 있다[4]. 이는 감시카메라 시스템의 자동화, 데이터 관리의 효율성, 그리고 신속한 대응 능력 향상에 기여할 것으로 기대된다. 이를 통해 도시 관리자와 시민들은 더 안전하고 효율적인 감시 환경을 경험할 수 있을 것이며, 도시 관리자와 시민들에게 새로운 이점을 제공할 수 있다[5]. 블록체인 기술을 활용한 감시 시스템은 도시 안전과 보안을 강화하는 데 중요한 기여할 것으로 기대한다.

II. 관련 연구

1. 블록체인과 분산 파일 시스템 기술의 적용

블록체인 기술은 감시 시스템에서 데이터 무결성, 보안 및 투명성을 강화하는 데 중요한 역할을 한다. 이 기술은 각 데이터 블록을 시간 순서대로 체인에 연결하여 데이터의 변경이나 조작을 방지한다. 이는 감시카메라에서 수집된 데이터의 신뢰성을 높이는 데 매우 유용하다. 블록체인의 분산 원장 구조는 중앙 집중식 데이터 저장소의 취약점을 해소하고, 대규모 감시 네트워크에서 발생할 수 있는 데이터 관리의 복잡성을 줄여준다.

비디오 감시카메라 시스템에 블록체인 기술을 적용하여 데이터의 무결성과 보안을 강화하는 기법으로서 비디오의 메타데이터(Metadata)는 블록체인의 분산 원장에 기록하여, 데이터의 위조나 변조를 방지한다. 이는 시스템은 감시 데이터의 신뢰성을 높이고, 중앙 집중식 데이터 저장소의 취약점을 해소하는 데 기여할 수 있다[1]. 또한 감시카메라의 데이터 검증 시스템에 블록체인을 적용하여 저장된 영상의 신뢰성을 보장할 수 있다. 이 시스템은 비디오가 변경되었는지를 검증할 수 있게 하며, 원본과 변조된 영상을 구별할 수 있다[2].

IPFS는 분산형 파일 시스템으로, 데이터를 전 세계의 여러 노드에 분산하여 저장한다. 이 시스템은 대규모 비디오 데이터를 효율적으로 저장하고 관리하는 데 사용될 수 있으며, IPFS는 각 파일에 고유한 해시를 할당하고, 사용자는 이 해시를 통해 파일에 접근할 수 있다. 이는 비디오 데이터의 무결성을 보장하고, 빠른 접근을 가능하게 한다. 또한 감시카메라에 DID(Decentralized Identifier)를 적용하는 것은 여러 가지 이유로 중요하다. DID는 각 감시카메라에 고유한 식별자를 제공하여, 각 감시카메라의 식별을 명확하게 확인하고 관리할 수 있게 한다. 이는 다음과 같은 이점을 제공한다.

① 보안 강화와 신뢰성 있는 감시 시스템 구축: 각 카메라에 고유한 DID를 부여함으로써, 시스템은 각 카메라의 데이터와 행위를 정확하게 추적하고 검증할 수 있다. 이는 데이터 조작이나 무단 접근을 방지하는 데 도움이 된다. 또한 각 카메라의 신원을 명확히 할 수 있어, 감시 시스템 전체의 신뢰성을 높일 수 있다. 이는 법적 증거로서의 가치를 높이는 데도 중요한 역할을 할

수 있다.

② 데이터 관리 효율성: DID를 사용하면 각 카메라에서 생성된 데이터를 효율적으로 관리하고 분류할 수 있다. 이는 대규모 감시 시스템에서 데이터를 쉽게 찾고 접근하는 데 유용하다.

③ 개인정보 보호 및 규정 준수: DID를 통해 각 카메라의 접근 권한을 관리하고, 민감한 데이터의 접근을 제한할 수 있다. 이는 개인정보 보호 규정 준수에도 도움이 된다.

블록체인과 IPFS의 통합은 시스템의 효율성과 신뢰성을 크게 향상할 수 있다. 이러한 기술 적용은 특히 도시 규모의 감시 시스템에서 중요한 역할을 하며, 보안과 공공 안전을 위한 실시간 모니터링과 대응에 필수적이다.

2. 스마트 감시 시스템

스마트 감시 시스템은 이미지 분석 기술과 머신러닝 알고리즘을 통합하여 의심스러운 활동이나 잠재적인 위험 상황을 자동으로 탐지하는 접근 방식을 채택했다고 할 수 있다. 이는 무단 침입, 비정상적인 움직임, 교통 규칙 위반과 같은 사건들을 자동으로 식별하고, 즉각적인 대응을 가능하게 함으로써 공공 안전을 크게 향상한다. 싱가포르의 스마트 도시 프로젝트는 스마트 감시 시스템의 효과적인 구현을 보여주는 사례이다. 도시 전역에 설치된 수천 개의 감시카메라는 블록체인 기반 시스템을 통해 관리되는 것으로 알려져 있으며, 각 카메라에서 촬영된 영상의 무결성을 보장하고 불법 접근을 방지한다[3]. 또한, 실시간 데이터 분석을 통해 공공 안전을 강화하는데 기여한다. 이러한 접근 방식은 블록체인 기술이 비디오 감시 시스템을 혁신하는 방법을 보여주며, 다른 도시들에도 중요한 인사이트를 제공한다[2,3,4].

CNN(Convolutional Neural Network)은 이미지 처리에 특화된 딥 러닝 모델로, 감시카메라의 비디오에서 객체를 탐지하고 분류하여 이상 행동을 식별하는 데 사용된다. 예를 들어, CCTV 영상에서 사람의 움직임을 감지하거나 차량의 번호판을 인식하는 등의 작업에 효과적으로 활용될 수 있다. 이러한 활용은 감시 시스템의 지능을 향상해 더욱 정확하고 신속한 대응이 가능하다[5].

이러한 기술적 적용은 스마트 감시 시스템이 도시 안전과 보안을 위한 중요한 도구로서의 역할을 더욱 강화하고 있음을 나타낸다. 블록체인과 CNN과 같은 첨단 기술의 통합은 감시 시스템의 효율성과 효과성을 향상하고, 도시 관리자와 시민들에게 새로운 이점을 제공할 수 있다.

3. 데이터 관리 및 프라이버시 보호

블록체인과 IPFS 기술의 통합은 시스템에서 수집된 데이터의 안전한 저장과 관리를 가능하게 한다. 데이터 처리 과정에서 개인정보 보호를 중시하며, 개인의 프라이버시를 존중한다고 할 수 있다. 이는 감시 시스템에서 수집된 데이터를 법적 증거로 활용하는 데 가치를 높이고, 개인정보 보호와 데이터 보안을 강화하는 데 기여한다. R. A. Michelin[6]은 감시카메라의 데이터 무결성을 확립하기 위해 경량 블록체인 기술을 사용하는 방법을 제시하였다. 이 연구는 감시카메라에서 수집된 비디오 데이터의 메타데이터를 블록체인에 저장하여, 데이터의 위조나 변조를 방지하는 방법을 제안하였다. 이러한 접근은 감시 시스템의 신뢰성을 높이고, 중앙 집중식 데이터 저장소의 취약점을 해소하는 데 기여할 수 있다.

A. Fitwi, Y. Chen[7]은 엣지(Edge) 컴퓨팅 환경에서 감시카메라를 위한 경량 블록체인 기반 프라이버시 보호 방안을 제안했다. 이 시스템은 실시간 비디오 분석을 가능하게 하면서도 영상에 포착된 개인의 프라이버시를 보호한다. 이는 감시 시스템이 개인정보 보호를 중시하는 동시에 효과적인 감시 기능을 수행할 수 있도록 하는 중요한 발전이다.

이러한 연구들은 블록체인과 IPFS 기술이 감시 시스템의 데이터 관리 및 프라이버시 보호에 어떻게 기여할 수 있는지를 나타낸다. 이들 기술의 통합은 감시 시스템의 효율성과 신뢰성을 향상하며, 동시에 개인정보 보호를 강화하는 혁신적인 접근 방식을 제공한다.

III. 시스템의 설계

본 논문에서 제안하는 시스템은 블록체인 기술을 기반으로 한 스마트 감시카메라 영상 관리 시스템(아하 Block-Surveillance)의 설계에 초점을 맞추고 있다. 제안하는 기법은 첫 번째, 블록체인을 단독으로 사용하여 감시 데이터의 무결성을 보장하는 것이 아닌 블록체인과 IPFS를 통합하여 데이터의 무결성뿐만 아니라 분산 저장과 효율적인 데이터 관리할 수 있다. 그럴 뿐만 아니라 각 영상은 블록체인과 IPFS에 기록되어 변경이나 조작할 수 없으며, 이는 법적 증거로서의 가치를 높이고, 개인정보 보호와 데이터 보안을 강화한다. 대규모 감시 시스템에서 발생할 수 있는 데이터 관리의 복잡성을 줄이고, 중앙 집중식 데이터 저장소의 취약점을 해소하는 데 기여한다. 두 번째, 객체 탐지 기술을 통합하여 실시간으로 발생하는 이벤트에 대한 신속한 대응을 가능하게 하며, 보안 관리자가 효과적으로 대응할 수 있도록 지원한다. 세 번째, 대규모 감시 시스템의 관리를 효율적으로 운영할 수 있는 방법론을 제시하여 감시 시스템의 자동화, 데이터 관리의 효율성, 그리고 신속한 대응 능력을 향상할 수 있다.

이러한 기술적 차별성은 기존 연구들과 비교하여 도시 안전과 보안을 강화하는 데 있어 효과적인 접근 방식을 제공할 수 있다. 시스템 설계의 개요는 다음과 같다.

① 블록체인과 IPFS 기반 데이터 관리

- 데이터 무결성 및 보안: 각 비디오와 관련된 데이터는 블록체인에 시간 순서대로 기록되어 데이터의 변경이나 조작을 방지한다. 이는 감시 시스템에서 수집된 데이터의 신뢰성을 높이는 데 중요하다.
- IPFS 저장 서비스: 대규모 비디오 데이터의 안전한 저장을 제공한다.
- 분산 원장 시스템: 중앙 집중식 데이터 저장소의 취약점을 해소하고, 대규모 감시 네트워크에서 발생할 수 있는 데이터 관리의 복잡성을 줄인다.
- 블록체인 기반 프라이버시 보호: 실시간 비디오 분석을 가능하게 하면서도 영상에 포착된 개인의 프라이버시를 보호한다.

② 스마트 감시 기능

- 이미지 분석 및 기계학습: 의심스러운 활동이나 잠재적인 위험 상황을 자동으로 탐지한다. 예를 들어, 무단 침입, 비정상적인 움직임, 교통 규칙 위반 등을 식별한다.
- 실시간 대응: 자동 탐지된 이벤트에 대해 신속하게 대응하여 공공 안전을 향상한다.
- CNN 기반: 이미지 분석 및 객체 탐지에 효과적으로 활용된다.

③시스템 아키텍처

- 분산 네트워크: 감시카메라에서 수집된 데이터는 블록체인 네트워크에 저장되며, 각 노드는 데이터의 무결성을 유지한다.
- 사용자 인터페이스: 관리자와 사용자는 시스템에 접근하여 데이터를 모니터링하고 관리할 수 있는 사용자 친화적인 인터페이스를 제공한다.

이러한 시스템 설계는 도시 안전을 위한 현대적이고 효율적인 감시 시스템을 구축하는 데 중요하며, 블록체인 기술의 통합은 감시 시스템의 효율성과 효과성을 향상하여, 도시 관리자와 시민들에게 새로운 이점을 제공할 수 있다.

1. 시스템의 구성

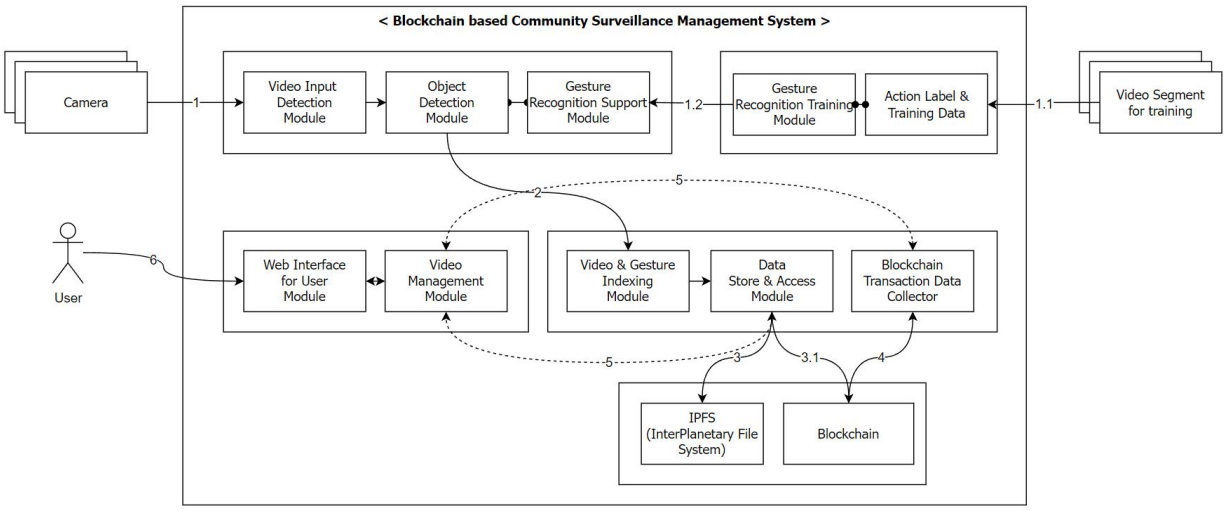

그림 1. 제안하는 시스템의 구성도

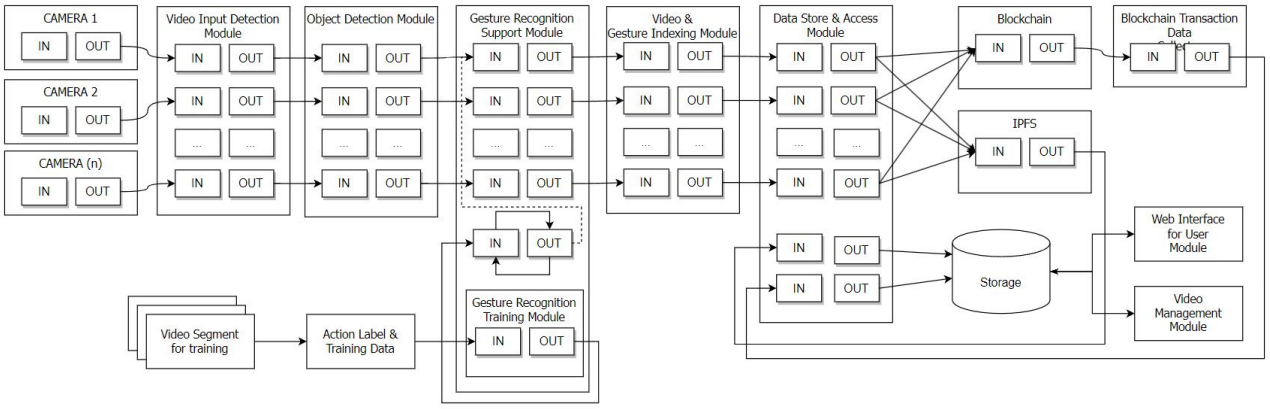

그림 2. 모듈별 데이터 입출력 구성도

제안하는 시스템인 Block-Surveillance는 10가지의 모듈로 보유하며, 시스템의 구성도는 [그림 1]과 같다. 각 모듈의 주요 역할은 다음과 같다.

① 비디오 입력 감지 모듈(Video Input Detection Module): DID가 적용된 카메라로부터 입력되는 영상신호를 탐지하며, 카메라의 위치 정보와 이상 정보 관리를 목적으로 한다. 카메라의 이상동작이 감지될 경우, 관리자에게 이상을 통보할 수 있다.

② 객체 탐지 모듈(Object Detection Module): 기본적으로 객체를 탐지하는 역할을 목적으로 하며, 제스처 인식 지원 모듈에 의해 사전에 정의된 의심스러운 활동이나 잠재적 위험 상황 탐지를 수행한다.

③ 제스처 인식 지원 모듈(Gesture Recognition Support Module, 학습을 위한 모듈을 포함): 객체 탐지를 지원하기 위한 모듈로서, 의심스러운 활동이나 잠재적 위험 상황을 탐지하기 위한 데이터를 제공하고, 데이터의 삽입, 갱신을 위한 모듈을 내장해 정확성 및 최신화를 지원한다.

④ 사용자를 위한 웹 인터페이스 모듈(Web Interface Module): 웹 기반의 인터페이스를 지원하는 모듈로서 사용자 관리를 목적으로 한다. 접근하는 사용자의 로그인을 비롯한 관리와 역할 내지 권한을 부여한다.

⑤ 비디오 관리 모듈(Video Management Module): ②, ③, ⑥번 모듈에 의해 생성된 비디오 정보를 탐색과 함께 제어, 모니터링 등을 제공한다.

⑥ 비디오 & 제스처 인덱싱 모듈(Video & Gesture Indexing Module): ②, ③번 모듈에 의해 탐지된 비디오 신호를 영상파일과 메타데이터를 생성하는 것으로 목적으로 한다. 탐지 기준 시간(Timestamp)을 기준으로 사용자가 설정한 시간 전후를 모두 저장하며, 부가적으로 섬네일과 함께 메타데이터를 생성한다.

⑦ 데이터 저장 및 접근 모듈(Data Store & Access): 생성된 비디오 파일은 분산 네트워크 파일 시스템인 IPFS에 저장하고, 메타데이터는 블록체인에 저장한다. 필요시 데이터에 접근하는 것을 목적으로 한다. 그 외 시스템을 운영하기 위한 데이터베이스(Database, DB) 관련 서비스를 제공한다.

⑧ 블록체인 트랜잭션 데이터 수집 모듈(Blockchain Transaction Data Collector): 메타데이터를 저장할 때 발생하는 트랜잭션 데이터를 수집과 트랜잭션 조회를 위한 캐싱(Caching) 서비스를 제공하는 것을 목적으로 한다. 블록체인 네트워크에서 직접 데이터를 조회하는 것이 불가한 것은 아니지만, 사용자를 위한 빠른 검색 결과의 반환을 위함이다.

⑨ 분산 파일 시스템 모듈(IPFS Module): 프라이빗(Private) 분산 파일 시스템 사용을 목적으로 한다. 프라이빗 네트워크를 구성할 때, 비밀키를 가진 피어(Peer)만 연결을 허용한다. 또한 데이터에 대한 완전 제어를 제공하고 미디어(예: 비디오 파일)에 대한 주소 지정을 지원한다.

IPFS의 경우, 샤미르 암호 공유(shamir secret sharing) 채택하고 있어 그 파일 자체가 IPFS 상에 그대로 올라가지는 않는다. 파일을 업로드할 때는 원본 파일로부터 추출된 메타데이터만을 업로드되고, 원본 파일은 이후 여러 조각으로 분할되어 네트워크상에 분산 저장한다.

⑩ 블록체인(Blockchain): 프라이빗(허가형, 하이퍼레저 패브릭) 블록체인 네트워크로서 다음과 같은 조건을 만족해야 한다.

- 참여자들이 식별/식별 가능해야 함
- 허가형이어야 하는 네트워크
- 높은 트랜잭션 처리 성능
- 낮은 트랜잭션 확정 지연 시간
- 트랜잭션의 개인정보 보호와 기밀성

또한 허가형 블록체인인 하이퍼레저 패브릭의 구성 요소인 MSP(Membership Service Provider), Channel을 통해 기본적으로 무분별하게 정보가 공개되지 않으며, Channel을 이용해 특정 사용자(혹은 기관)에게만 데이터의 공유를 할 수 있도록 제한할 수 있다. 추가로 Private Data Collection을 하여생성되는 모든 거래가 전체 채널 사용자들 내에서도 프라이버시를 유지할 수 있다.

⑥번 모듈에 의해 생성된 메타데이터를 저장하는 것을 목적으로 한다.

표 1. 모듈별 데이터 입출력 사항

모듈명	입력	출력	설명
Video Input Detection	카메라에서의 실시간 비디오 스트림	비디오 스트림	비디오 스트림 신호 감지
Object Detection	비디오 스트림	객체탐지 결과	비디오 내 객체 식별 및 분류
Gesture Recognition Support	객체탐지결과	제스처 인식 결과	행동 패턴 식별 및 분류
Video & Gesture Indexing	비디오 스트림 제스처 인식 결과	색인화된 비디오 및 제스처 관련 메타데이터	비디오 데이터에 제스처 데이터를 결합하여 색인화
Data Store & Access	색인화된 데이터	저장된 데이터 및 접근 권한	데이터의 안전한 저장과 접근을 관리

Blockchain	메타데이터	트랜잭션 데이터	데이터의 무결성을 보장하고, 변경 불가능한 기록을 제공
Blockchain Transaction Data Collector	트랜잭션 데이터	트랜잭션 수집 데이터	블록체인에서 트랜잭션 데이터를 검색하고 수집 후 제공
IPFS	비디오 파일	CID(Hash), 파일명, 크기	분산파일시스템에 비디오 파일 저장
Web Interface	사용자 요청	사용자에게 제공되는 정보	사용자 요청에 따른 정보제공
Video Management	사용자 요청	관리 및 제공된 비디오 데이터	사용자 요청에 따른 정보제공
Action & Training	액션 라벨 및 학습 데이터	학습 결과	학습 모델을 향상하기 위한 데이터 제공

[그림2]와 [표1]은 시스템의 데이터 흐름도(Data Flow Diagram)로서 시스템 내에서 데이터가 생성, 처리, 저장되고 최종 사용자에게 전달되는 경로를 도식화한 것이다. 각 요소는 특정 데이터 처리 역할을 맡으며, 이들 사이의 데이터 흐름은 시스템의 동작을 이해하는 데 중요한 역할을 한다.

① 카메라(CAMERA): 기본적인 입력 장치로, 실시간 비디오를 캡처하고 스트림(Stream)을 전송한다. 이 스트림은 보안 감시의 근본적인 출발점이다.

② 비디오 입력 탐지 모듈: 카메라로부터 받은 비디오 스트림에서 실시간으로 비디오 신호에 대한 이상을 감지하고 그 정보를 다음 단계로 전달한다.

③ 객체 탐지 모듈: 탐지된 이벤트를 기반으로 비디오 내의 객체들을 식별하고 분류한다. 이는 사람, 차량 등과 같은 특정 객체에 대한 정보를 추출하는 단계이다.

④ 제스처 인식 지원 모듈: 객체의 움직임을 분석하여 특정한 제스처나 행동 데이터를 제공한다. 더욱 복잡한 분석을 위한 기초 데이터를 제공하는 단계이다.

⑤ 비디오 및 제스처 색인 모듈(Video & Gesture Indexing): 학습된 데이터를 기반으로 비디오와 제스처 정보와 함께 색인화하며, 타임스탬프(Timestamp) 생성하여 전후 정보(비디오 파일 포함)를 생성한다. 이는 검색 및 검색 결과를 빠르게 제공한다.

⑥ 데이터 저장소 및 접근 모듈(Data Store & Access): 처리된 데이터를 저장하고, 사용자가 접근할 수 있도록 관리한다. 이는 데이터 보안과 무결성을 유지하기 위한 전처리 단계이다.

⑦ 블록체인(Blockchain): 처리된 데이터를 블록체인에 기록하여 불변성을 보장한다. 이는 데이터의 신뢰성을 확보하며, 법적 증거로서의 가치를 부여하는 단계이다.

⑧ 블록체인 트랜잭션 데이터 수집기(Blockchain Transaction Data Collector): 블록체인에서 거래 데이터를 수집하고 사용자의 요청에 따라 수집기에서 데이터를 우선 검색 후 제공하는 단계이다.

⑨ 웹 인터페이스(Web Interface for User Module): 사용자가 시스템과 상호작용할 수 있는 인터페이스이며, 사용자는 이를 통해 데이터 요청을 하며, 시스템은 요청된 정보를 제공한다.

⑩ 비디오 관리 모듈(Video Management Module): 사용자의 요청에 따라 비디오 데이터를 관리하고 필요한 작업을 수행하며. 시스템은 사용자가 요청한 비디오 정보를 제공한다.

⑪ 액션 라벨 및 훈련 데이터(Action Labels & Training Data): 시스템의 CNN 모델의 훈련을 위한 데이터를 제공한다. 이는 시스템의 지속적인 학습과 발전을 가능하게 한다.

그 외 저장소(Storage)에서는 처리된 모든 데이터를 안전하게 보관하며, 데이터는 장기 저장을 위해 구조화되어 관리된다.

2. 시스템의 동작

제안하는 시스템의 운영 과정을 시퀀스 다이어그램을 통해 상세하게 나타내었다. [그림3,4]의 시퀀스 다이어그램은 시스템 내 각 모듈 간의 상호작용과 데이터 흐름을 시간 순서에 따라 그래픽적으로 표현한 것으로, 각 모듈 간의 상호작용과 데이터 교환 포인트를 명확하게 보여줌으로써, 시스템의 인터페이스 설계를 검증하고 문제점을 사전에 발견할 수 있다.

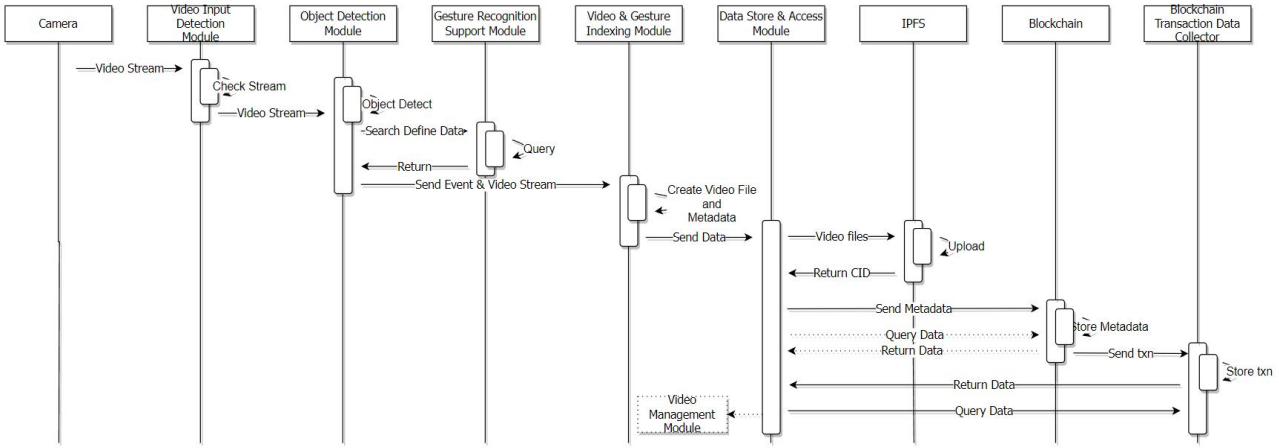

그림 3. 모듈별 데이터 입출력 구성도

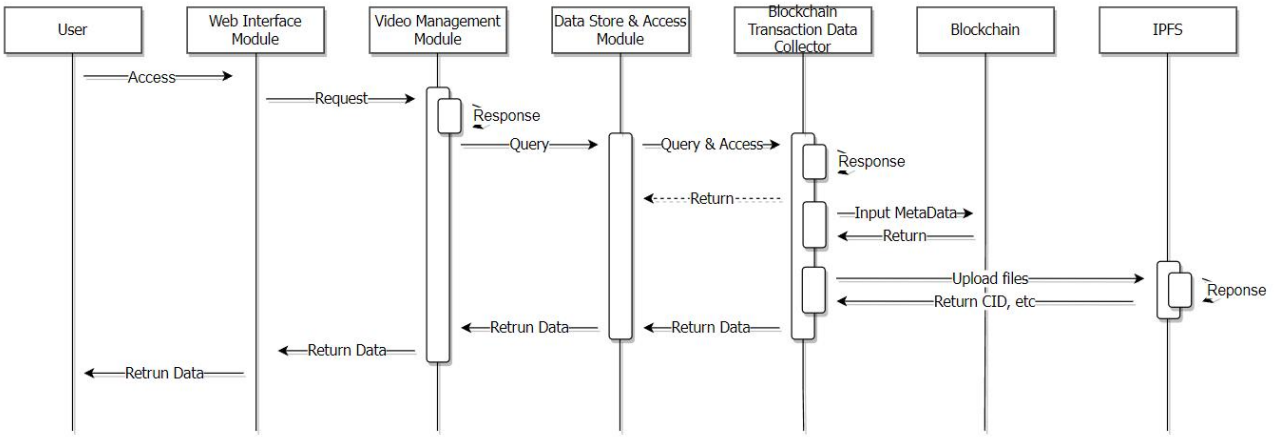

그림 4. 웹 인터페이스 시퀀스 다이어그램

부가적으로 시스템이 예상치 못한 상황이나 오류를 어떻게 처리하는지를 이해할 수 있게 하며, 시스템의 견고성을 향상하는 데 도움이 된다. 그리고 블록체인과 IPFS를 통한 데이터 처리와 저장 단계를 보여줌으로써, 시스템이 데이터 보안과 무결성을 어떻게 유지하는지 확인할 수 있다.

3. 메타데이터의 구조

[표2]와 [그림5]와 같이 JSON((JavaScript Object Notation) 형식은 사용한 데이터 구조를 제안한다.

JSON은 사람이 읽고 이해하기 쉬운 텍스트 형식이다. 개발자와 시스템 관리자가 데이터 구조

를 쉽게 읽고 수정할 수 있으며, 중첩된 객체와 배열을 사용하여 복잡한 데이터 구조를 표현할 수 있다.이는 블록체인의 불변성과 투명성을 활용하여 감시 시스템의 신뢰성을 더욱 강화와 다양한 시스템과 플랫폼에서 사용될 수 있으며, 이는 시스템 간의 상호 운용성을 높이고, 다양한 환경에서 통합을 쉽게 하는 장점이 있다. 그리고 데이터의 구조는 다음과 같은 목적을 만족하도록 구성하였다.

표 2. 메타데이터의 상세 구조 설명

구분	하위 구분	설명
cameraIdentity	did	카메라의 DID, 고유식별자
	manufacturer	카메라 제조사
	model	카메라 모델명
	installationDate	카메라 설치 날짜
	location	카메라 위치 정보 (위도, 경도)
videoMetadata	frameRate	초당 프레임 수
	resolution	비디오 해상도
	duration_sec	비디오 길이 (초 단위)
	Video_hash	비디오 데이터의 해시값, 데이터 무결성 확인용
	ipfs_hash	IPFS 해시값, 분산 파일 시스템에서의 비디오 위치 식별용
	abnormal_event	이상 사건 정보 (유형 인덱스, 설명)
transactionData	transactionId	블록체인 트랜잭션 ID
	blockId	블록체인의 블록 ID
	previousHash	이전 블록의 해시값
auditTrail	createdBy	데이터 생성 주체
	createdAt	데이터 생성 시간
	modifiedBy	데이터 수정 주체
	modifiedAt	데이터 수정 시간
security	encryption	사용된 암호화 방식
	hashingAlgorithm	사용된 해싱 알고리즘
accessControl	authorizedUsers	데이터 접근 허가된 사용자 목록
	encryptionKey	데이터 암호화에 사용된 키

①효율적인 데이터 관리: 카메라의 DID 정보를 포함한 위치 정보, 비디오의 생성 날짜, 이상 사건의 유형 등을 기록함으로써, 필요한 데이터를 신속하게 검색하고 분석할 수 있다.

② 데이터 무결성 및 신뢰성 보장: 비디오 파일의 기본 정보(해상도, 프레임 속도, 비디오 길이 등)를 기록하여, 비디오 데이터의 무결성을 확인할 수 있다. 또한, 비디오의 해시값과 IPFS 해시를 포함해, 데이터의 원본성과 변경 여부를 검증할 수 있다.

③ 보안 및 프라이버시 강화: 보안 관련 정보(예:암호화 방식, 해싱 알고리즘)와 접근 제어 정보(예: 허가된 사용자, 암호화 키)를 포함해, 데이터의 보안성을 강화하고 무단 접근을 방지할 수 있다.

④ 감사 추적: 데이터의 생성 및 수정 정보를 기록함으로써, 데이터의 변경 이력을 추적할 수 있다. 이는 시스템의 투명성을 높이고, 잠재적인 문제 발생 시 원인 분석에 도움이 된다.

⑤ 블록체인과의 통합: 블록체인의 트랜잭션 ID와 유형 등을 기록함으로써, 필요한 데이터를 신속하게 검색하고 분석할 수 있다.

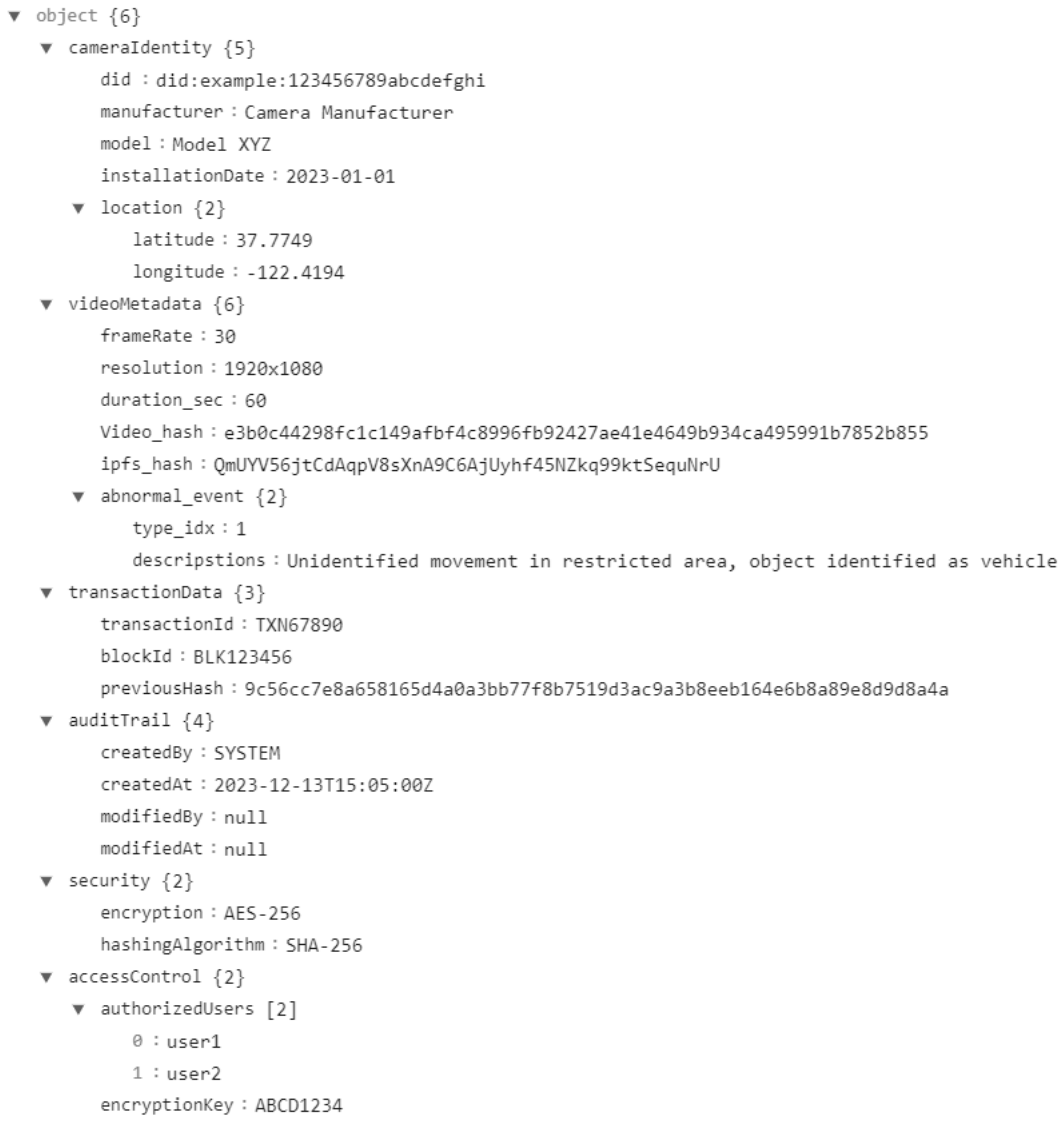

그림 5. 생성된 데이터 예시

Ⅳ. 결 론

본 논문에서는 블록체인, IPFS 기술, 그리고 객체 탐지 기술을 활용한 감시카메라 영상 관리 시스템의 설계를 제안하였다. 이 시스템은 도시 안전을 향상하는 동시에 감시 데이터의 신뢰성을 높이고, 프라이버시 보호 및 데이터 보안을 강화한다. 또한, 이 시스템은 대규모 감시 네트워크의 효율적인 관리를 가능하게 하며, 다음과 같은 특징을 갖는다.

① 블록체인과 IPFS의 통합: 블록체인과 IPFS를 결합하여 사용함으로써, 데이터의 무결성과 분산 저장 및 효율적인 데이터 관리를 가능하게 한다. 이는 대규모 감시 시스템에서 발생할 수 있는 데이터 관리의 복잡성을 줄이고, 중앙 집중식 데이터 저장소의 취약점을 해소하는 할 수 있다.

② 객체 탐지 기술의 적용: 객체 탐지 기술을 통해 이상 행위를 자동으로 탐지하고, 해당 영상을 자동으로 저장하여 실시간으로 발생하는 이벤트에 대한 신속한 대응이 가능하다. 보안 관리자가 효과적으로 대응할 수 있도록 지원한다.

③ 프라이버시 보호와 데이터 보안 강화: 각 영

상은 블록체인과 IPFS에 기록되어 변경이나 조작이 불가능하며, 이는 법적 증거로서의 가치를 높인다.

④ 대규모 감시 시스템의 효율적 관리: 대규모 감시 시스템의 관리를 효율적으로 운영할 수 있는 방법론을 제시한다. 블록체인과 IPFS 기술의 통합은 감시 시스템의 자동화, 데이터 관리의 효율성, 그리고 신속한 대응 능력 향상할 수 있다.

본 연구에서 제안한 시스템은 도시 안전과 보안을 위한 현대적이고 효율적인 감시 시스템을 구축하는 데 중요한 기여를 할 것으로 기대하며 향후 제안하였던 시스템의 각 모듈을 개발 및 구현하여 시스템에 대한 검증과 사용성 평가를 진행하고자 한다.

REFERENCES

[1] Y. Jeong, D. Hwang and K. -H. Kim, "Blockchain-Based Management of Video Surveillance Systems," *2019 International Conference on Information Networking (ICOIN),* Kuala Lumpur, Malaysia, pp. 465-468, 2019.

[2] Khan, Prince Waqas, 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, 2020.

[3] Smart Nation and Digital Government Office, "S mart Nation: The Way Forward," Singapore, 201 8. [Online]. Available: https://www.smartnation.s g.

[4] A. Victor Benevent Raj;B. Srikanth;A. Thilagavat hy;B. Mathivanan; "A Surveillance System Focus ed On Approved Blockchains and Computation of Edges," *JOURNAL OF PHYSICS: CONFERE NCE SERIES*, vol. 164, 2021.

[5] J. Li, X. Liu, J. Zhao, W. Liang and L. Guo, "Application Model of Video Surveillance System Interworking Based on Blockchain," *2021 IEEE 4th Advanced Information Management,* Communicates, Electronic and Automation Control Conference (IMCEC), Chongqing, China, pp. 1874-1879, 2021.

[6] R. A. Michelin, N. Ahmed, S. S. Kanhere, A. Seneviratne and S. Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras," *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* Toronto, ON, Canada, pp. 1-3, 2020.

[7] A. Fitwi, Y. Chen and S. Zhu, "A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge," *2019 IEEE International Conference on Blockchain (Blockchain),* Atlanta, GA, USA, pp. 552-555, 2019.

저 자 소 개

이지운(정회원)

2016년 서강대학교 정보통신대학원 석사 졸업

2021년 한국기술교육대학교 컴퓨터공학과 박사 졸업

2021년 한양대학교 산학협력단(서울) 연구원

2022년 ~ 현재: 한국기술교육대학교 융합학과 기술연구원

<주관심분야 : 블록체인, 클라우드 컴퓨팅, 정보보안>

서희석(정회원)

2000년 성균관대학교 산업공학과 학사 졸업

2002년 성균관대학교 전기전자및컴퓨터공학부 석사 졸업

2005년 성균관대학교 전기전자및컴퓨터공학부 박사 졸업

2005년 ~ 현재: 한국기술교육대학교 컴퓨터공학부 교수

<주관심분야 : 시스템보안, 클라우드 보안>