

AI CCTV 단말을 위한 개방형 영상 보안 플랫폼 설계

박수완, 김진우
한국전자통신연구원

parksw10@etri.re.kr, kimgw@etri.re.kr

An Open Video Surveillance Platform Architecture for AI CCTV Devices

Suwan Park, Geon Woo Kim
Electronics and Telecommunications Research Institute.

요 약

최근 영상 보안 시스템은 AI 기반 기능을 통합하여 실시간 위협 감지가 가능한 방향으로 진화하고 있으나, 기존 CCTV 시스템은 폐쇄적인 제조사 중심 구조와 외부 보안 장치 의존으로 인해 보안성과 확장성에 한계가 있다. 본 논문에서는 이를 해결하기 위해 Android 기반 운영체제와 OSSA/ONVIF 표준을 준수하는 AI CCTV 단말용 개방형 영상 보안 플랫폼을 제안한다. 제안된 플랫폼은 제안된 플랫폼은 단말 내 하드웨어, 통합 프레임워크, 자율보호·자율안전 AI 엔진, 앱 실행 환경을 연동하여, 실시간 영상 분석과 내재적 보안 기능을 통합적으로 수행한다. 또한, 클라우드 앱-마켓을 통해 사용자가 자유롭게 앱을 설치하고 운영할 수 있는 스마트폰 유사 환경을 제공함으로써, 영상 보안 시스템의 확장성과 유연성이 보장되는 사용자 중심 생태계 구축을 가능하게 한다.

I. 서 론

기존 영상 보안 시스템은 방화벽(Firewall)이나 물리적 셀프 클로저(Self-closure)와 같은 외부 보안 장치에 과도하게 의존하는 구조로 인해, 정보 유출을 포함한 다양한 보안 사고에 쉽게 노출되고 있다. 특히 국내에서 운영 중인 약 1 천만 대 이상의 민간 CCTV 시스템 대부분이 외부 장치에만 의존하고 있어, 외부 공격에 매우 취약한 상태로 방치되고 있다. 또한, 현장 상황에 적합한 맞춤형 지능 기능을 지원하기 위해서는 CCTV 장치 내에 영상 위협 탐지 기능이 내장되어야 하지만, 대부분의 기능은 제조사에 의해 제한적으로 설치되므로, 설치 환경에 따라 필요한 서비스를 유연하게 구성하기 어렵다. 특히 최근 급속히 발전하는 인공지능(AI) 기술을 CCTV에 반영하려 해도, 폐쇄적인 제조사 생태계와 비공개 SDK의 한계로 인해 개발자, 사용자, 운영자가 직접 기술을 적용하기가 사실상 불가능한 실정이다.

이러한 문제를 해결하기 위한 국제적 노력으로, 글로벌 산업 간 디팩토(de-facto) 표준 연합체인 OSSA(Open Security & Safety Alliance)[1-3]가 2019년 출범하였다. OSSA는 Android 기반 IoT 표준 플랫폼 구축을 목표로 개방형 영상보안 생태계 조성을 추진하였으며, Android Open Source Project 기반 운영체제와 공통 백엔드 구조를 통해 제조사 종속 없는 애플리케이션 설치 환경을 제공하였다. 또한 ‘AndroVideo Smart Edge Camera’를 통해 앱 마켓 연동 기능을 실현하기도 했다. 이후 OSSA는 2023년 공식 해산되었으며 일부 기능은 ONVIF(Open Network Video Interface Forum)[4-5]로 이관되었으나, OSSA/ONVIF 표준을 준수하는 개방형 CCTV 영상보안 통합 프레임워크의 필요성은 여전히 크다.

이에 본 논문에서는 스마트폰처럼 사용자 누구나 원하는 기능을 자유롭게 개발하고 설치·관리·운영할 수 있는 개방형 영상 보안 플랫폼 기반의 AI CCTV 단말 시스템을 제안한다.

II. 본론

본 개방형 영상보안 플랫폼은 클라우드 기반 앱-마켓과 AI CCTV 단말 간의 유기적인 연동을 통해, 다양한 보안·안전 서비스를 유연하게 확장·제공할 수 있도록 설계되었다. 그림 1은 전체 시스템이 구성되는 논리적 구조를 시각적으로 표현한 것으로, 하드웨어 플랫폼을 기반으로 한 통합 프레임워크, 보호/안전 기능 엔진, 앱 실행 환경, 그리고 클라우드 기반 앱 마켓으로 구성된다. 각 블록은 상호 독립적이면서도, API와 데이터 스트림을 통해 유기적으로 연동되며, 지능형 영상 보안 서비스의 실시간 처리와 확장성을 동시에 지원한다.

각 블록을 구성하는 상세 기능과 역할은 다음과 같다.

1) 개방형 CCTV 하드웨어 플랫폼

안드로이드 운영체제 기반의 영상 보안 플랫폼을 개발하기 위해서는 안드로이드 호환 칩셋 기반의 전용 CCTV 보드가 요구된다. 보드의 메인 칩셋은 연산 처리 기능(CPU), 그래픽 연산 처리 기능(GPU), 신경망 연산 처리 하드웨어 가속 기능(NPU), 외부 인터페이스 제어 기능(USB, 이더넷, 영상 출력 등에 대한 인터페이스 제어 및 데이터 처리), 메모리 제어/관리 기능 등을 수행한다.

2) 개방형 통합 프레임워크

개방형 통합 프레임워크는 안드로이드 운영체제를 기반으로, CCTV로서 동작하는 데 필요한 기본 기능들을 수행한다. 통합 프레임워크는 기본적인 영상 감시 기능 외에도 자율보호 엔진 및 자율안전 AI 엔진과의 연동을 통해 고도화된 지능형 영상보안 기능을 지원한다. 이를 위해 통합 프레임워크는 자율보호 및 자율안전 기능들이 기본 CCTV 기능들과 통합되어 원활히 작동할 수 있는 기반 기능들을 제공한다. 주요 기능으로는 입력 영상 처리, 주 영상 스트림 처리, AI 분석용 영상 프레임 공유, 분석 메타데이터의 수신 및 처리, 그리고 이들을 사용자에게 전달하기 위한 영상과 메타데이터의 동기화 및 스

트리밍 기능이 포함된다. 또한, 사용자/시스템 이벤트 및 이미지/영상 인코딩/디코딩을 처리하는 기능도 포함한다. 무엇보다, 개방형 통합 프레임워크는 OSSA 및 ONVIF와 같은 국제 표준을 준수하며, 하드웨어 및 소프트웨어 간의 상호 호환성을 확보할 수 있는 표준 API 개발이 필수적으로 요구된다.



그림 1. 개방형 영상 보안 시스템 구성

3) 자율보호 엔진

자율보호 엔진은 개방형 영상보안플랫폼의 보안성과 신뢰성을 확보하기 위해 필수적인 보안 기능들을 제공한다. 먼저, 영상 프라이버시 마스킹 기능과 영상 경량/실시간 암호화 기능은 영상 내 민감 정보 보호와 데이터 전송 보안을 담당한다. 또한, 비상상황 대응 기능은 기기의 탈취나 분실 등 예기치 못한 상황에서 내부 영상 및 키 정보의 외부 유출을 방지하기 위해 해당 상황을 인지하고 보안 조치를 수행한다. 비정상 프로세스 실시간 감지 기능은 개방형 구조와 안드로이드 기반 시스템의 특성상 증가하는 보안 위협에 대응하여, 실행 중인 프로세스의 상태를 모니터링하고 이상 행동을 유발할 수 있는 비정상 프로세스를 실시간으로 감지 및 차단한다. 마지막으로, 영상 키 관리 및 디바이스 인증 기능은 암호화 및 비식별화 기능 수행에 필요한 키를 생성·관리하며, 기기와 사용자에 대한 인증 기능을 제공하여 플랫폼의 무결성을 보장한다. 이러한 자율보호 엔진의 기능들은 상호 유기적으로 작동하여 고도화된 영상보안 환경을 구현하는 핵심 기반을 형성한다.

4) 자율안전 AI 엔진

자율안전 AI 엔진은 크게 세 가지 핵심 기능으로 구성된다. 먼저, 영상 입력 수신 및 전처리 기능은 개방형 통합 프레임워크로부터 수신된 영상 프레임 스트림을 분석 대상 프레임으로 샘플링하고, AI 모델에 적합한 입력 형식으로 변환한다. 다음으로, AI 모델 실행 기능은 안드로이드 기반 AI 런타임 환경에서 사전에 학습된 모델을 로딩하고, 전처리된 데이터를 입력하여 추론을 수행하며, 결과 데이터를 후처리한다. 특히, 이 단계에서는 NPU(Neural Processing Unit)를 활용한 하드웨어 가속을 통해 고속 처리가 가능하도록 설계될 수 있다. 마지막으로, 분석 결과와 메타데이터 송신 기능은 추론 결과를 메타데이터(metadata) 형태로 변환하여 통합 프레임워크로 송신하며, 필요 시 각 프레임의 timestamp, sequence, ID 정보 등의 동기화 정보를 포함한다.

이러한 구조를 바탕으로, 자율안전 AI 엔진은 사람 얼굴 및 차량번호판 검출/인식, 차량 검출 및 모델 인식, 사람 Re-ID(재식별) 및 이상행동 감지(쓰러짐, 폭력, 낙상), 그리고 재난 감지(화재·산불) 기능까지 수행하며, 다양한 물리적 위협과 위협 상황에 능동적으로 대응할 수 있는 지능형 영상 분석 기능을 제공한다.

5) 앱-런처

앱-런처는 개방형 영상보안플랫폼에서 지능형 AI 앱마켓과 연동하여 보안·안전 서비스를 단말에 설치·실행하고 체계적으로 관리하는 실행 관리자 역할을 수행한다. 이를 위해 앱-런처는 하드웨어, OS, 네트워크 등의 상태를 수집·제공하는 기기정보 관리 기능, 사용자 정보를 등록·관리하는 사용자 등록 기능, 운영체제 및 앱 설치/업데이트와 관련한 설정을 포함하는 앱 설치/관리 기능, 앱마켓 접속 및 애플리케이션 설치·인증을 수행하는 앱-마켓 연동 기능을 제공한다.

6) 앱-마켓

클라우드 기반 앱-마켓은 CCTV 전용의 AI 앱 생태계를 구성하는 클라우드 기반 플랫폼으로, 단말과 연동되는 앱의 배포, 인증, 관리 기능을 수행한다. 이를 위해, 하드웨어 및 사용자 단말을 인증·등록하고 관리하는 기기 및 사용자 인증/등록/관리 기능, 운영체제 및 AI 앱의 원격 설치/업데이트를 지원하는 CCTV AI 앱 관리 기능, 자율안전 AI 엔진 등 CCTV 전용 앱을 개발·배포하기 위한 표준 앱 API 기반의 앱 개발 환경 제공 기능을 포함한다. 더불어, 다양한 AI 기반 앱의 신뢰성 확보를 위해 앱 테스트 및 검증 환경도 함께 구축되어야 한다.

III. 결론

기존 영상보안 시스템이 하드웨어 종속성과 확장성 측면에서 한계를 지녔던 문제를 해결하기 위해, 본 논문에서는 개방형 영상 보안 플랫폼 기반의 AI CCTV 단말 아키텍처를 설계하고, 그 구성 요소와 연동 구조를 제안하였다. 제안된 플랫폼은 유연한 소프트웨어 개발 환경을 바탕으로 다양한 AI 단말 응용 기술의 개발과 적용을 가능하게 하여, 영상 보안 시장의 확장성과 서비스의 다양화를 촉진할 수 있다. 특히, AI 및 보안 기술의 개발·설치·운영 권한을 제조사로부터 사용자, 운영자, 개발자에게 개방함으로써, 기술 혁신을 가속화하고 영상 보안 산업의 진입 장벽을 획기적으로 낮출 수 있다는 점에서 큰 의의를 갖는다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2024-00394190, 온-디바이스 자율보호가 내재화된 개방형 영상보안플랫폼 기술 개발)

참 고 문 헌

- [1] "A common Technology Stack for video security devices". Technical Committee, Open Security & Safety Alliance. Ver.1.0, 2019.11.
- [2] "OSSA Compliant Camera Device Specification". Open Security & Safety Alliance Technical Committee, v1.0, 2020.04.
- [3] "OSSA Camera Cyber Security Specification". Open Security & Safety Alliance Technical Committee, v1.1, 2021.09.
- [4] "ONVIF™ ONVIF Core Specification". ONVIF, 2023.12.
- [5] "ONVIF™ Streaming Specification". ONVIF, 2023.06.