IoT 기반 지능형 시큐리티 플랫폼에 관한 연구

김병희*
*한화시스템㈜
e-mail :apolo14.kim@hanwha.com

A Study on Intelligent Security Framework based IoT Platform

Byung-Hee Kim*
*TICN PE Team, HanwhaSystems Corp

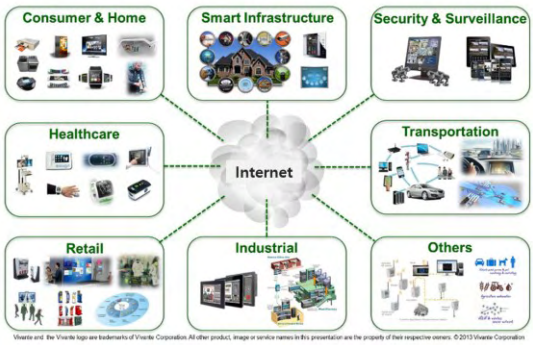
요 약

본 논문에서는 인간과 사물, 서비스 세 가지 분산된 환경 요소에 대해 인간의 명시적 개입 없이 상호 협력적으로 정보 센싱, 네트워킹, 정보 처리 등 지능적인 기능을 제공하는 표준 IoT 플랫폼 기반에 대량의 이벤트에 대한 융합분석이 가능한 CEP(Complex Event Processing) 및 시나리오 기반 자동화된 절차에 따라 대응이 가능한 워크플로우 기술을 적용하여 중요시설감지, 국경감시, 해안감시, 도시안전 분야 등 다양한 분야에 활용이 가능한 지능형 시큐리티 플랫폼을 제안하고자 한다.

1. 서론

인간과 사물에서 정보를 센싱하는 정보를 네트워크로 연결하는 IoT(사물 인터넷)는 최신 인터넷 기술로, [그림 1]에서 보는 바와 같이 가전분야, 스마트 인프라, 감시경계, 헬스케어, 교통, 소매업, 산업분야 등 다양한 분야에 적용이 가능하다.

[그림 1. IoT 적용분야]



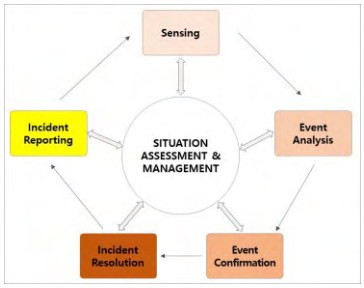
최근 다양한 IoT 서비스 플랫폼이 [표 1]과 같이 개발되어 각 응용분야별로 활용되고 있으며 글로벌 표준화를 위해 치열한 경쟁을 하고 있는 상황이다. 본 논문에서는 표준을 준수하는 IoT 플랫폼을 기반으로 센서로부터 발생한 이벤트에 대한 분석을 통해 상황인지 및 자동화된 대응이 가능한 지능형 시큐리티 플랫폼을 설계하고자 한다.

[표 1 IoT 서비스 플랫폼 현황]

솔루션	표준	응용분야	파트너
Weave	X	스마트홈	Google
HomeKit	X	스마트홈	Apple
AWS IoT	X	다양한 응용 지원	Amazon
AllJoyn	O	다양한 응용 지원	MS 등 200 개 회사
OCF(OIC)	O	다양한 응용 지원	인텔등 200 개 회사
oneM2M	O	다양한 응용 지원	LG 등 200 개 회사

본 논문에서는 제안하고자 하는 지능형 시큐리트 플랫폼에 요구되는 주요 요구기능은 [그림 2]와 같다.

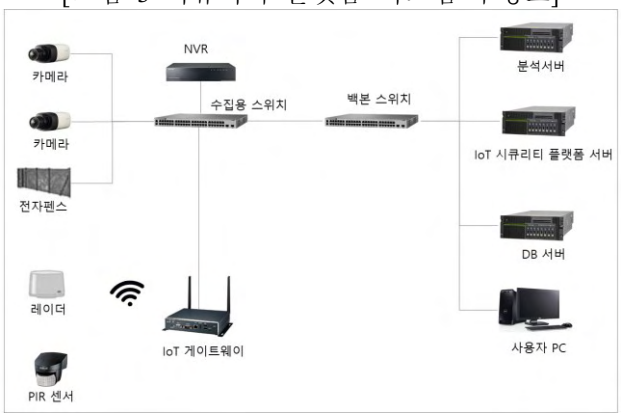
[그림 2 시큐리티 플랫폼 주요 요구기능]



- Sensing : 감시센서를 활용한 감시기능 제공
- Event Analysis : 감지된 이벤트 분석기능
- Event Confirmation : 이벤트 분석결과에 대한 결정기능
- Incident Resolution : 사건/사고 결정 및 관리기능
- Incident Reporting : 사건/사고 보고서 기능

[그림 3]은 제안하고자 하는 IoT 기반 지능형 시큐리티 플랫폼이 요구기능을 충족하는지 검증하기 위한 시스템 구성도이다. [1][2][3][4][5]

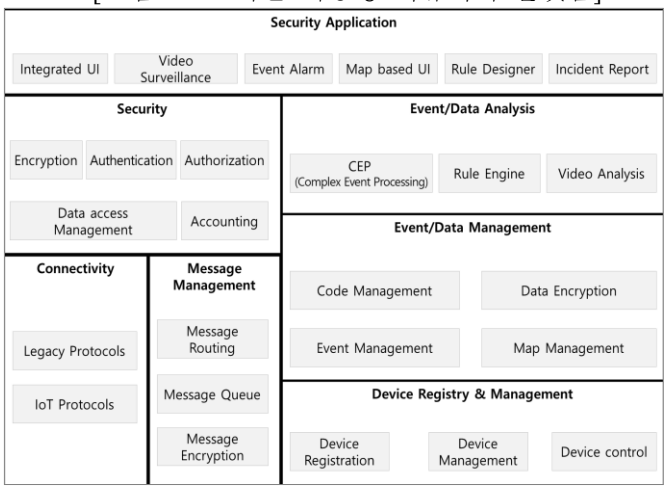
[그림 3 시큐리티 플랫폼 시스템 구성도]



2. 본론

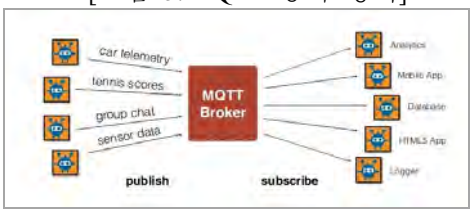
본 논문에서 제안하고자 하는 IoT 기반 지능형 시큐리티 플랫폼은 [그림 3]과 같으며 제공하는 기능은 아래와 같다.

[그림 4. IoT 기반 지능형 시큐리티 플랫폼]



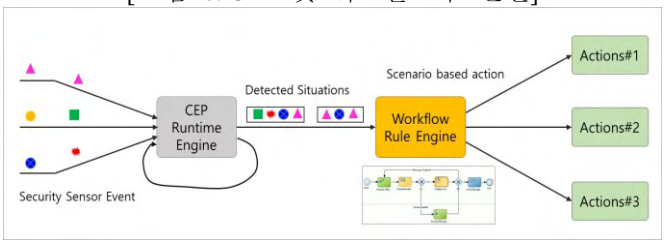
- **Connectivity** : IoT 용 프로토콜(MQTT, XMPP, CoAP, HTTP&WebSocket 등) 및 센서별 사용하는 Legacy 프로토콜(Backnet, Modbus, LonWorks, SNM))을 사용하여 센싱정보 수신 및 센서제어를 위한 통신 기능을 제공한다. [그림 5]은 IoT 용 프로토콜중 대표적인 MQTT 프로토콜의 동작방식을 설명한 것이다.

[그림 5. MQTT 동작 방식]



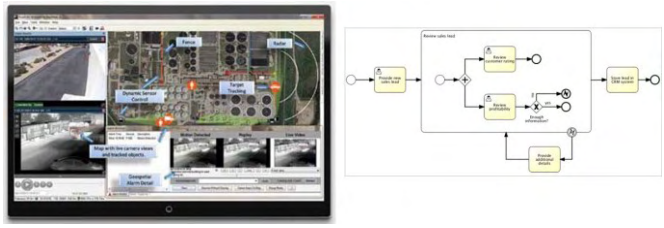
- **Message Management** : 시큐리티 플랫폼에서 송신하는 메시지와 센싱장비로부터 수신하는 메시지에 대한 포멧변환 및 암호화, 메시지 라우팅 기능을 제공한다.
- **Device Registry & Management** : 센서장비에 대한 등록/관리, 장비관리는 장비 구성정보 관리 및 제어, 모니터링 및 진단기능, 소프트웨어 업데이트 및 유지관리 기능을 제공한다.
- **Security** : 사용자에 대한 인증 및 사용자 권한, 데이터 접근권한, 데이터에 대한 암호화, IoT API에 대한 암호화 기능을 통해 시큐리티 플랫폼의 중요정보를 보호하는 보안기능을 제공한다.
- **Event/Data Management** : 센서장비로부터 수신한 이벤트에 대한 관리, 시스템의 코드관리, 사용자 UI 를 위한 Map 관리기능을 제공한다.
- **Event/Data Analysis** : 센서로부터 수신한 이벤트는 [그림 3]과 같이 CEP(Complex Event Processing) 엔진에서 분석을 수행하고 분석된 결과를 워크플로우 엔진에 전달하여 사용자가 정의한 시나리오에 따라 대응이 가능하다. 또한 영상정보는 지능형 영상분석과 연동하여 영상분석기능을 제공한다.

[그림 6. CEP 및 워크플로우 엔진]



- **Security Application** : 맵 기반의 통합된 사용자 UI, 영상감시, 사용자가 상황대응 시나리오를 직접 구성할 수 있는 룰 디자이너 사건/사고에 대한 보고서 기능을 제공한다. [그림 7]은 사용자 통합 UI 및 시나리오을 정의할 수 있는 Rule 디자이너 어플리케이션이다. [1][2][3][4][5]

[그림 8. 시큐리티 어플리케이션]



3. 결론

본 논문에서 최신 ICT 기술인 IoT 플랫폼을 기반으로 감시센서로부터 이벤트를 수신하고, 수신한 이벤트에 대한 분석 및 분석결과를 기반으로 사용자가 사전에 정의한 시나리오에 따라 자동화된 대응이 가능한 지능형 시큐리티 플랫폼을 설계하였다. 제안한 지능형 시큐리티 플랫폼은 중요시설감시, 해안감시, 국경감시등 다양한 분야에 적용이 가능하다.

향후 본 논문에서 제안한 구조에 대한 상세설계 및 기능구현을 통해, 제안한 IoT 기반 지능형 시큐리티 플랫에 대해 검증하고자 한다.

참고문헌

[1] Ayla Networks, “White Paper - How To Select the Right IoT Platform Considerations Beyond”
[2] Antonio Almeida and Jaime González-Arintero, “Gentle Introduction to IoT Protocols: MQTT, CoAP, HTTP & WebSockets”, June 14, 2017
[3] IEC, “White Paper - IoT 2020: Smart and secure IoT platform”
[4] John Weber, “Fundamentals of IoT device management, http://iotdesign.embedded-computing.com/articles/fundamentals-of-iot-device-management/”, March 3rd, 2016.
[5] Gil Press, “6 Hot Internet of Things (IoT) Security Technologies, https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#7da2f3741b49”, MAR 20, 2017
[6] ALFIO PAPPALARDO, “A FRAMEWORK FOR THREAT RECOGNITION IN PHYSICAL SECURITY INFORMATION MANAGEMENT”, April 2013