박사학위논문

메타데이터 비식별화 기법을 이용한 프라이버시 강화형 영상감시 프레임워크

제주대학교 대학원

과학교육학부 컴퓨터교육전공

이 동 혁

2018年 2月

메타데이터 비식별화 기법을 이용한 프라이버시 강화형 영상감시 프레임워크

指導敎授 朴 南 濟

李 東 燏

이 論文을 工學 博士學位 論文으로 提出함

2017年 12月

李東燏의 工學 博士學位 論文을 認准함

審査委員長 ____

委 員 ____

委 員 ____

委 員 ____

委 員 ____

濟州大學校 大學院

2017年 12月

A Privacy Enhanced Video Surveillance Framework using Metadata De-identification

Donghyeok Lee

(Supervised by professor Namje Park)

A thesis submitted in partial fulfillment of the requirement

for the degree of Doctor of Philosophy

2017. 12.

This thesis has been examined and approved.

Major of Computer Education

Faculty of Science Education

GRADUATE SCHOOL

JEJU NATIONAL UNIVERSITY

목 차

표 목 차

그 림 목 차

<국문초록>

메타데이터 비식별화 기법을 이용한 프라이버시 강화형 영상감시 프레임워크

이 동 혁

제주대학교 대학원 과학교육학부 컴퓨터교육전공

지도교수 박 남 제

최근의 영상감시 시스템은 다양한 영상분석 기술이 도입되어 지능형으로 발전하고 있다. 특히, 클라우드 기반의 영상감시 환경은 빅데이터 기반의 다양한 영상분석이 가능해지면서 영상 객체에 대한 신뢰도 높은 분석결과를 제공하고 있다. 이러한 부분은 지능형 영상감시 환경에 획기적인 성능 향상을 가져올 것이며, 보다 능동적인 감시 후 조치가 가능하여 CCTV 기반의 지능화된 치안 환경에서 크게 기여할 수 있을 것으로 보인다. 그러나, 이러한 이면에는 프라이버시 보호 이슈와 같은 다양한 문제가 발생할 수 있다. 특히, 클라우드와 빅데이터 환경에는 다양한 보안 취약성이 존재하고 있어 클라우드 기반의 영상감시 환경에서는 새로운 유형의 보안 사고가 발생할 수 있을 것으로 예상된다. 이러한 점은 결국 영상 객체의 개인정보 유출에 따른 프라이버시 침해로 이어지게 되어 심각한 사회적인 이슈로 부상할 우려가 있다.

현재 여러 지능형 감시환경 제품이 출시되어 서비스를 제공하고 있다. 여기에는 IBM의 Intelligent Video Analytics, Smart Surveillance System 등 다양한 제품이 존재한다. 또한, 미국 뉴욕시는 마이크로소프트사와 공동개발한 DAS(Domain Awareness System) 시스템을 구축하여 운용중에 있다. 이러한 제품은 주로 도시나 기관 단위에서 활용하고 있어, 시민의 안전한 프라이버시 보호를 위해 개인정보의 수집 및 관리에 있어 철저한 보안 대책이 필요한 상황이다.

그러나, 기존 CCTV 기반 클라우드 영상감시 환경에서의 보안 기법은 주로 프라이버시 마스킹, 데이터 암호화, RBAC 기반의 접근제어 등 종래의 보안 기법에 의존하는 경향이 있다. 그러나, 향후 빅데이터 분석 기술이 발달함에 따라, 다양한 메타정보가 발생하게 될 것이며, 이에 따라 새로운 비식별화 기술, 또는 클라우드 서버단위의 보안 동기화 기술, 차등레벨 접근제어와 같은 다양한 기술이 연구될 필요가 있다.

특히, 클라우드 환경에서는 내부자 공격 등 다양한 정보보호 취약점이 존재하는 것이 현실이다. 기존의 CVR 프레임워크 및 Hossain의 연구 등에서는 이러한 내부자 공격을 방지하기 위해 사설 클라우드와 공공클라우드의 망을 분리하는 보안 정책을 제안하였다. 그러나, 사설 클라우드에서도 내부 공격자가 존재할 수 있어 기존의 클라우드 환경에서의 보안 위협을 그대로 답습할 수 있다.

따라서, 데이터를 안전하게 보관하기 위하여, 결국 모든 데이터를 암호화 및 비식별화하여 보관하고, 전송 과정에서 종단간 암호화를 적용하는 것이 바람직하며, CCTV 전송부터 감시/클라우드 서버 및 모니터링 클라이언트까지 모든 단위에서 해커의 공격을 방지할 수 있는 구조가 필요하다.

본 논문에서는 클라우드 기반의 안전한 지능형 영상감시 환경을 제공하는 PEVS(Privacy Enhancing Video Surveillance) 영상감시 프레임워크를 제안하였다. 제안한 프레임워크는 CCTV 장치에서의 영상정보 수집, 클라우드 서버에서의 영상정보 보관, 사용자 클라이언트에서의 모니터링 과정에서 영상 객체의 프라이버시를 보호할 수 있는 방안을 제공한다. 이를 위해 본 논문에서는 영상정보에 대한 메타변환 기반의 비식별화 알고리즘을 제안하였으며, CCTV와 영상 감시 서버 간 안전한 영상데이터 동기화 방식 또한 제안하였다. 본 논문에서 제안한 방식을 통하여 CCTV와 영상 감시 서버 간 데이터 전송 과정에서의 스니핑 공격, 클라우드 영상 감시 환경에서의 내부자 유출 공격, 메타데이터 DB 분석 공격, 데이터 변조 공격 등에 안전함을 보인다. 또한, 제안한 프레임워크는 기존의 지능형 영상감시 프레임워크인 Rodríguez의 연구, CVR 프레임워크, Hossain의 연구 등에 비해 벤더 독립성, 데이터 백업상의 안정성, 세분화된 영상 접근제어, 메타정보 보안기능 등의 장점을 가지고 있다.

주요어 : 클라우드, 지능형 영상감시, CCTV, 비식별화, 프라이버시

I. 서 론

1. 연구의 배경 및 목적

최근 지능형 영상감시 환경의 도입이 활발해지고 있다. 지능형 영상감시 기술은 CCTV 등에서 수집된 영상 정보를 수집 및 분석하여 이를 기반으로 자동화된 처리가 가능하게 하는 기술이다. 지능형 영상감시 기술은 사람, 자동차, 건물, 환경 등 다양한 분야에 적용할 수 있으며, 클라우드 및 빅데이터 분석 기술과 결합하여 보다 의미 있는 상황 인식이 가능하다는 장점이 있다. 지능형 감시 기술의 응용분야로써, 특정 건물이나 지역의 화재감지 발생의 예측 및 감시, 대기오염 등 환경 감시, 태풍/지진/해일 등 기후 감시, 자동차 교통안전 감시 등 다양한 적용분야가 있을 수 있으며, 이 중에서도 중요한 분야로 주목되는 부분은 행동인식 기반의 위험도 감지를 통한 범죄예방 분야가 있다. 현재 미국 뉴욕에서는 DAS(Domain Awareness System)이라는 지능형 범죄예방 시스템을 운영하고 있으며, 국내에서도 송도국제도시에서 IBM의 스마트 감시시스템인 SSS(Smart Surveillance Solution)을 운영하고 있다. 딥러닝 기술의 발달에 따라 이러한 지능형 영상감시 시스템은 CCTV 영상에 대한 방대한 빅데이터 기반의 축적된 데이터 분석을 기반으로 더욱 신뢰도 높은 행동인식, 위험요소 추론이 가능해질 것으로 보인다.

그러나, 이러한 기술 발달의 이면에는 다양한 위험성이 도사리고 있다. 예를 들어, 지능형 영상 감시 시스템이 해킹을 당하게 될 경우 심각한 사회적 문제가 될 수 있을 것이다. 지능형 영상감시 시스템에서는 특정 개인의 위치, 이동 경로 등을 CCTV로부터 수집하여 클라우드 등 서버 스토리지 환경에 저장하게 될 것이며, 이러한 영상정보는 암호화하여 저장할 필요가 있다. 해킹 등에 의하여 영상정보가 노출되더라도, 공격자는 결국 암호화된 데이터만 습득할 수 있으므로 기밀성을 보장할 수 있다.

그러나, 영상정보를 암호화하여 저장하는 것만으로 해결책이 되지 않는다. 영상정보는 대용량 데이터로써, 영상 데이터 분석을 위해 원본 영상으로 복호화하는 과정에서 오버헤드가 발생한다는 문제가 있다. 또한, CCTV와 감시 서버간 종단간 기밀성 및 무결성 보장 방안이 필요하다.

2. 연구의 내용 및 범위

본 논문에서는 프라이버시 강화형 영상감시 방법인 PEVS(Privacy Enhancing Video Surveillance) 영상감시 프레임워크를 제안한다. PEVS 영상감시 프레임워크는 메타 비식별화 및 보안 동기화 기법을 기반으로 동작하며, 클라우드 서버에 보관된 메타정보를 비식별화 알고리즘으로 보호하고, CCTV와 클라우드 서버간 보안 동기화를 제공한다.

해당 프레임워크에서는 메타데이터 비식별화를 위한 COP-변환 방식을 제안하고 있으며, 이는 평문 메타데이터의 정보를 전혀 다른 문자로 변환하여 원본 데이터를 식별할 수 없게 하는 방식이다. 또한 CCTV와 감시 서버간 안전한 종단간 보안 통신을 제공하기 위한 보안 동기화 방식을 제안한다. 제안한 방식을 통하여, CCTV와 지능형 감시 서버 및 모니터링 클라이언트간 안전한 보안 동기화 기반의 기밀성 및 무결성 보장이 가능하며, 서버상에 저장된 데이터에 대한 내부자 공격 방지가 가능하다.

3. 프레임워크의 정의

본 연구에서 의미하는 프레임워크는 CCTV 환경에서 영상 객체의 프라이버시 보호를 목적으로 클라우드 기반 지능형 영상감지시스템에서의 CCTV와 엔드유저까지의 종단간 보안기능을 제공하고 비식별화를 기반으로 영상메타정보의 안전한 관리 방안을 제공하는 구조이며, 해당 프레임워크에는 본 논문에서 제안하는 메타데이터 비식별화 처리 및 CCTV 영상정보를 안전하게 동기화 처리하는 기술이 포함되어 있다.

II. 지능형 영상감시와 보안환경

1. 영상감시 개요

1) 지능형 영상감시

(1) 지능형 CCTV와 영상감시

최근 지능형 CCTV가 등장하면서 CCTV 영상 분석에 대한 관심이 증가하고 있다. 지능형 CCTV는 영상에 대하여 기존보다 더욱 많은 정보를 제공하며, 얼굴인식 뿐만 아니라, 객체의 행동 유형 등 다양하고 지능화된 분석이 가능하다. CCTV는 향후 도입될 지능치안 환경에 적합한 도구로 활용할 수 있으나 CCTV를 통한 불필요한 개인정보 수집은 최소화할 필요가 있다. 특히, 영상 데이터를 통계자료 제공 등에 활용할 경우는 얼굴 영상에 대한 적절한 비식별화 처리가 필요하며, 불필요한 개인정보를 식별할 수 없도록 기술적인 조치가 필요하다. 비식별화 처리는 정보주체를 식별하거나 식별할 수 있는 개인정보를 식별하지 못하도록 만드는 조치를 의미한다. 엄밀히, 비식별화는 암호화 방식과는 다르다. 영상 암호화 방식은 전체, 혹은 일부 영상만을 암호화하는 것으로서, 이는 암호화된 영역의 영상에 대한 정보를 전혀 식별할 수 없도록 하는 것이다. 비식별화는 이와는 차이가 있는 방법으로, 영상에 대한 일부의 정보는 식별이 가능하나, 촬영된 특정 개인이 누구인지 혹은 특정인의 개인정보를 유추할 수 없도록 하는 기술이라고 볼 수 있다.

대표적인 영상 비식별화 기술로는 얼굴 마스킹(Masking) 방식이 있다. 마스킹 방식은 개인이 식별되지 않도록 얼굴 영역에 해당하는 부분에 식별 불가능한 의미없는 픽셀로 대체하는 것이다. 이러한 마스킹 기반의 비식별화 방식은 현재 가장 많이 쓰고 있는 방식이다. 그러나, 이는 개인의 특징이 완전히 사라지게 되어 통계 등 일부정보 활용이 필요한 분야에 사용하기 어려우므로 엄밀한 관점에서는 일반적인 비식별화 방법과는 차이가 있다. 특히 예를들어 매장에 설치된 CCTV에 영상 암호화 처리를 하게 될 경우, 촬영된 손님 개인에 대한 성별, 대

략적인 연령, 외국인 여부 등을 마스킹된 데이터를 기반으로는 전혀 식별할 수 없게 된다.

즉, CCTV 마스킹 기법을 통해서는 통계자료 분석 및 학술적 목적 등에 의한 적법한 제공이 필요시에도 사용이 어렵게 된다. 따라서, 불가피하게 통계작업이 필요한 경우는 마스킹하지 않은 원본 데이터로 분석해야 하는 문제점이 존재하며, 이러한 구조는 프라이버시 보호에 있어서 치명적인 결함을 가지고 있다.

(2) IoT 기반의 지능형 CCTV

최근 여러 IoT 기반 기술이 생활속에 친근하게 다가오고 있다. 특히, 지능형 CCTV는 일종의 IoT 기반의 제품으로 작동하는 경우가 많으며, 지능형 영상감시 환경에서 IoT에 대한 부분은 필수적으로 논의될 필요가 있다. IoT 환경은 물리적 제품과 정보통신 기술이 결합하여 생활에 필요한 다양한 서비스를 제공해 줄 것이며, 사용자는 기존보다 더욱 편리한 생활을 영위할 수 있을 것이다. 향후 IoT 제품이 점차 지능화되어감에 따라, 기존에는 상상하지 못했던 여러 다양한 서비스를 제공받을 수 있게 될 것이며, IoT 시장은 점차 확대되어 미래의 주요한 성장 동력으로 작용할 것으로 보인다.

IoT 기기의 연결을 위한 여러 기술이 존재하나, 모바일 네트워크가 가장 대중적이며, 가장 처음으로 제공되었다. 모바일 네트워크는 20년전부터 제공되었으며, 그 이후로도 신뢰성 있고 가용성이 높으며 안전하고 비용 효율적인 서비스를 도입 중이다. 그러나, 이러한 이면에는 IoT 환경의 특성에 따른 다양한 위협요소가 도사리고 있다. IoT의 주요 분야인 홈/가전, 의료, 교통, 에너지, 제조분야 등에서 다양한 해킹 사례가 보고되었으며, 향후 스마트 홈/가전, 커넥티드 카와 같은 IoT 제품과 서비스가 생활 깊숙이 보편화되는 본격적인 IoT 시대를 맞게 되면, 기존에는 생각치 못했던 다양한 위협을 직면하게 될 것이다.

이러한 가운데 모바일 업계에서는 IoT의 가용성 확보를 위해 IoT의 필요성을 충족시키는 저전력 장거리 통신(LPWA) 기술을 셀룰러 통신 공간에 통합하는 방안을 추진 중이다. 이 통신 기술 클래스는 효과적으로 통신하는데 필요한 전력의 일부만으로도 모바일 네트워크의 광역 무선 연결을 제공한다. 이동통신 사업자는 LPWA 프로토콜과 기술을 제품에 통합하여 가까운 미래에 기업에 서비스와 솔루션을 제공할 예정이다.

한편, 신원 식별의 과제를 해결하기 위해, 모바일 업계의 표준 및 기술 제공을 크게 강화 중이다. 모바일 업계는 일반적으로 착탈식 SIM 카드와 연관되어 있으나, GSMA에서는 IoT에서 사용하기에 적합한 임베디드 SIM 원격 프로비저닝 아키텍쳐 (Embedded SIM Remote Provisioning Architecture)라는 SIM 기반 솔루션을 만들어 엔드포인트 장치에 더 깊은 구성요소 수준의 통합을 가능하게 하고 생산 비용을 절감하도록 한다. 또한, Over-The-Air 플랫폼을 통한 연결성 관리를 통해 IoT 종단 장치의 수명을 연장할 수 있다. 임베디드 SIM과 같은 ID 기술은 기본적으로 사이드 채널 분석 차단, 패시브 데이터 차단, 물리적 조작 차단, 신분도용 방지 등의 기능을 가질 수 있도록 제작되어 있다.

개인정보보호문제 해결 대응에 있어, 모바일 업계는 탄력적인 프로토콜, 프로세스 및 모니터링 시스템을 개발하여 보안을 강화하고 악의적인 공격 가능성을 줄였다. 예를 들어, 3G 및 4G 기술은 상호 인증을 지원하며, 엔드포인트와 네트워크의 신원을 확인한다. 이 프로세스는 상대방이 통신을 가로챌 수 없도록 한다. 또한, 네트워크 기술은 SIM 및 GBA 또는 EAP-SIM과 같은 기술을 사용하여 확보할 수 있다. 이러한 기술을 사용하여 SIM은 잘 알려진 프로토콜을 통해 애플리케이션 네트워크 통신에 사용될 수 있는 세션 보안 키를 제공받을 수 있다. 이 프로세스는 상대방이 장치 또는 서비스를 손상시키기 위해 애플리케이션 프로토콜을 조작할 수 있는 가능성을 줄인다. 따라서, 이 모델을 기반으로 네트워크와 응용프로그램 모두 보호가 가능하다.

그러나, 보안에 대한 우려는 아무리 하더라도 지나치지 않으며, 이에 대한 완벽한 대응책이 필요하다. 특히, IoT 환경에서는 기존의 정보통신 환경에 비해 더욱 다양한 보안 위협요소를 안고 있다. 물리적 기기들이 서로 연결된다는 것은 원격 해킹에 용이한 환경을 제공하는 측면에서 바라볼 수도 있다. 해킹을 통한 원격 조작 등으로 사용자에게 재산적, 신체적 피해를 직접적으로 발생시키는 것은 실제로 가능한 일이며, 다양한 IoT 제품에서 보안 결함이 발견된 사례가 있다. 이를 위해 제품 출시 전 설계 및 개발단계에서 기술적인 보호조치가 당연히 수반되어야 하며, 이에 따른 법제도적 대책도 함께 요구된다. 그러나 현행 법제도상의 보안규정으로는 IoT 제품 보안성을 완전히 보장하기에는 한계점이 있다.

IoT 환경은 물리환경과 기존의 IT환경이 접목됨으로써 많은 편의성을 제공해준다. 따라서, 사용자는 IoT 환경을 통하여 보다 편리하고 윤택한 생활을 누릴 수 있을 것이다. 그러나 IoT 환경에 있어 필수적으로 고려해야 할 사항은 IoT

보안이다. 현재 사물인터넷 환경이 현실화되고 있는 단계이나, IoT 보안에 대한 대책은 완전하지 않은 상태이다. IoT 환경은 기존 IT 환경과는 또다른 신체적, 물질적으로 직접적인 피해를 가져다 줄 우려가 있으므로, 보안에 대한 정책적, 기술적 고려가 반드시 필요하다. 본 항에서는 이러한 안전한 IoT 환경을 제공하고자, IoT 제품의 사후관리에 초점을 맞춘 보안대책을 제안한다. 현재 IoT 제품의 설계 및 개발단계에 대해서는 많은 연구가 되어지고 있으며, 이러한 연구를 바탕으로 보다 안전한 IoT 제품 설계 및 개발이 가능하다. 그러나, 이미 출시된 IoT 제품에 대한 보안 결함이나, 혹은 보안성 적합도를 만족한 제품이라 할지라도, 제품 출시 이후에 어떠한 신규 보안 취약점이 노출될지에 대해서는 확신할 수 없다.

IT 소프트웨어의 경우, 보안상의 취약점이 노출되더라도, 소프트웨어 업데이트로 처리하면 문제가 없으나, IoT 제품은 업데이트 가능 여부를 확신할 수 없다는 특징이 있다. 특히 IoT 제품의 특성상 제품의 하드웨어적 결함이 발생하면 소프트웨어 업데이트만으로는 해결할 수 없을 것이며, 이러한 경우는 리콜 등 제도적으로 해결할 필요가 있다.

소프트웨어 업데이트가 가능한 경우라도, 업데이트 패치 제작 시간이 소요되며, 그 기간 동안 만큼은 해당 IoT 제품이 불안정한 상태로 작동하게 될 것이다. 이러한 특성이 IoT 환경에서의 보안 위협을 가중시키고 있다.

2) 클라우드 환경에서의 영상감시

(1) 클라우드 기반의 객체 스토리지

최신 기술이 등장하고, SNS와 같은 소셜네트워크 서비스의 활발한 사용으로 텍스트, 이미지, 오디오, 비디오 스트림 등과 같은 비정형 데이터의 경우 특히 데이터 볼륨이 크게 증가하였다. IDC는 이러한 예측할 수 없는 비정형 데이터가 2020년까지 최대 40제타바이트까지 도달할 수 있다고 경고하고 있다. 이러한 대량의 대용량 데이터를 처리하기 위해 객체 저장 기술이 차세대 스토리지 플랫폼으로 부상하고 있다. 여기서 해결해야 할 주요과제는 성능저하 없이 데이터의 급격한 성장을 처리하는 데이터 관리, 대량의 비정형 데이터에 액세스하고 처리하

는 데이터 액세스 기능, REST 서비스 등에서의 데이터 보안 제공을 들 수 있다.

객체 스토리지 시스템은 클라우드에서의 대규모 데이터 관리 및 전달을 위한 차세대서비스 저장소 기술이며, 최근 여러 형태의 객체 스토리지 기술이 주목받고 있다. 이러한 기술 중 하나가 OpenStack Swift이다. OpenStack Swift는 웹서비스 REST 프로토콜과 같은 개방형 표준을 통해 관리되는 데이터 구성 및 검색을 위한 컨테이너 서비스 방법론을 기반으로 한다.

객체 기반 스토리지 시스템에는 Openstack Swift, Amazon S3 및 Windows Azure가 있다. 이러한 시스템은 무단 액세스로부터 데이터를 보호하기 위한 다양한 보안 메커니즘을 제공한다. Keystone은 OpenStack에서 제공하는 Identity 관리 및 인증 서비스이다. Keystone은 사용자 이름 및 암호, LDAP 및 TLS 클라이언트 인증을 포함한 다중 요소 인증을 지원한다. Amazon S3는 AWS 키 관리 서비스를 사용하여 객체를 암호화하는 데 사용되는 키를 만들고 관리한다. 또한 사용자는 사용 정책을 설정/수정할 수 있으며 감사를 모니터링하여 어떤 사용자가 데이터에 액세스하기 위한 키 사용 여부를 확인할 수도 있다. Amazon S3는 클라이언트 측 암호화를 위한 두 가지 옵션을 지원한다. 첫 번째 옵션은 키 생성 및 관리를 위해 아마존 내장 키관리 서비스(KMS)를 사용한다. 두 번째 옵션은 키가 로컬에서 생성되며, 메타 데이터 매개 변수로 저장된다. Windows Azure는 REST 프로토콜을 통해 SMAPI(Service Management API) 인증을 사용한다. 이 프로토콜은 SSL을 통해 실행되며 고객이 생성한 인증서와 개인키로 인증된다. 고객이 비공개 키에 대한 제어권을 가지고있는 한 높은 기밀성을 보장할 수 있다.

OpenStack Swift는 오픈소스 객체 저장 시스템이다. Swift는 OpenStack을 위한 분산된 궁극적으로 일관된 가상 객체 저장소를 제공한다. 스위프트는 여러 노드에 분산된 수십억 개의 개체를 저장할 수 있다. Swift는 파일, 이미지 및 비디오와 같은 멀티미디어 데이터, 웹 콘텐츠, 백업, 가상 머신 스냅샷 및 기타 비정형 데이터를 대규모로 저장하도록 설계되어 있다. 스위프트에는 스위프트 클러스터에서 각 객체를 세 번 복제하는 내장 중복 기능이 있으며, 파일 사이즈와 개체 수 측면에서 매우 확장성이 뛰어나다는 장점이 있다.

Swift의 사용자 요청은 기본적으로 HTTP Request로 이루어진다. Swift의 데이터 처리를 수행하기 위한 PUT, GET, POST 및 DELETE와 같은 다양한 HTTP 메소드를 포함한다. 한편, 인증 미들웨어는 클라이언트가 제공한 사용자

이름, 암호 및 계정의 유효성을 검사한다. 유효할 경우에는 각 사용자 요청과 함께 신속하게 보내야하는 인증 토큰을 생성한다. Swift는 인증을 제공하기 위해 TempAuth 미들웨어 또는 Keystone의 신원 관리 기법을 사용한다.

Swift는 권한이 없는 사용자가 HTTP 상태코드가 403일 경우 클러스터의 개체에 액세스하고 거부할 수 없도록 하며, 컨테이너 수준에서 개체에 대한 세분화된 접근제어도 지원한다.

(2) 해사클라우드 환경에서의 영상감시

① 해사클라우드 개요

국제 해사기구인 IMO에서는 선박운항과 정보기술을 융합하기 위하여 e-Navigation 전략을 수립한 바 있다. 과거에 선박사고의 대부분이 운항미숙과 과실 등 인적요인에 대한 해양사고가 많았던 바, 이러한 문제를 개선하기 위해 e-Navigation의 필요성이 크게 대두되고 있으며, 국내에서도 한국형 e-Navigation 구축을 목표로 진행중에 있다.

현재 다수의 해양사고는 인적과실이 원인인 것으로 알려져 있으며, 이러한 인적과실이 전 세계 해양사고의 82%에 달하는 것으로 추산되고 있다. 따라서 국제해사기구인 IMO에서는 이와 같은 해양사고를 줄이기 위하여 2020년까지 시행을 목표로 선박운항기술에 ICT기술을 융합한 e-Navigation 기술의 도입을 결정하였다. 국내에서도 해양수산부에서 2020년까지 1,300여억원의 투자로 한국형 e-Navigation 개발을 추진중에 있으며, 해사클라우드 기술의 국제 표준화에도 노력을 기울이고 있다. 2016년 12월에는 군산항 인근 해역에서 해양수산부가 덴마크 해사청과 함께 해사클라우드의 공동 시험을 성공적으로 실시한 바 있어, 국내의 어선, 소형선이 많은 특성을 고려하여 우리나라에 특화된 서비스를 제공하고, 유관 신산업 창출도 가능할 것으로 기대된다.

해사클라우드는 2012년 가을, 덴마크 정부 해사 기구(DMA:Danish Maritime Authority)의 내부 프로젝트로 시작되었다. e-Navigation 프로젝트의 일환으로, 당시 DMA는 e-Navigation 프로젝트 진행의 일환인 EPD(e-Navigation Prototype Display System)에서 해사클라우드의 연구를 진행한 바 있다.

기존에는 선박 측과 해안 측 사이를 통신할 때 여러 제한점이 있었으며, 특히

상이한 종류의 해사 서비스를 제공하려면 여러 제약점이 존재하였다. 여기에서는 주로 다음과 같은 세가지의 문제점이 지적되었다. 첫번째로, 대역폭 부족의 문제이다. 대역폭 부족은 제한된 분량의 데이터만 전송할 수 있다는 문제를 야기한다. 데이터 전송에 있어 종종 어플리케이션의 특정 AIS 메시지와 같은 복잡한 인코딩 스키마가 사용되는 경우가 있으며 이러한 경우 에는 대역폭 부족에 따른 문제가 발생할 수 있다. 두번째로, AIS 통신 시스템의 시뮬레이션을 위해서는 복잡한 개발자 환경이 요구된다는 문제점이 있다. 즉, 개발하는 과정에서 AIS 통신을 구현하기 위한 간단한 시뮬레이션 환경을 제공하는 것이 현실적으로 어렵다는 문제가 있다. 마지막으로, 신호 범위의 제한에 따른 문제점이 존재한다. 통신이 필요한 객체 모두가 무선 신호의 범위에 닿지 않는다면, 신호 범위 밖의 객체는 무선 통신이 어렵게 된다는 문제가 존재한다.

따라서, 해사 객체간 원활한 통신을 위해 새로운 인프라 환경이 필요하며, 해사클라우드는 이러한 배경 아래 개발되었다. 현재의 해사클라우드와 관련된 첫 프로토타입은 2012년 겨울에 제작되었으며, 2013년 봄 EPD에 구현된 바 있다. 이것은 단지 기본적인 point-to-point 통신을 특징으로 하고 있으며, 이는 현재 해사클라우드의 구성요소인 MMS(Maritime Message Service) 서비스에 해당하는 부분이라 볼 수 있다. 이후 2013년 여름에 해사에서의 원활한 통신을 위한 구체적인 틀이 제시되었으며, 여기에는 MMS와 같은 메시지 기반 프레임워크 외에도, 서비스 및 ID에 대한 레지스트리를 포함하고 있다. 해사클라우드(Maritime Cloud)라는 명칭이 다양한 기본 서비스를 위한 명칭으로 본격적으로 사용된 것은 이 시점이다. 이후 2014년에는 해사클라우드 참조 구현의 첫번째 릴리즈가 공개된 바 있다.

해사클라우드는 e-Navigation에서의 주요 통신 기반 기술이다. 이는 일반적인 스토리지 클라우드와는 개념이 다르며, 해상 도메인의 다양한 시스템 간, 그리고 여러 통신 링크간 원활히 정보 교환을 가능하게 하는 목적으로 추진되고 있다.

해사클라우드는 이용가능한 통신 시스템을 통해 인가된 모든 해상 관련 당사자들 간의 효율적이고 안전하며, 안정적이고 원활한 정보 교환을 가능하게 하는 통신 체계이다. 해사클라우드는 IMO의 전략에 따라 원활한 정보 전달을 지원하는 인프라의 개념을 설명하기 위해 제안되었다. IMO의 e-Navigation 전략에 따라 관련 당사자들 사이에 원활한 정보 전달을 제공하는 통신 인프라가 필요하였으며, 신뢰성 있고 상호 운용 가능한 서비스를 제공하기 위하여 해사클라우드의

필요성이 대두되었다. 특히 효율적이고 지속가능한 통신 인프라 체계의 확립이라는 점에서 의미가 크다. 해사클라우드는 e-Navigation 아키텍쳐에서 통신수단으로서 활용되며, 여러 통신 링크 간에 원활하게 정보 전달이 가능하게 한다. 또한, 해상 관련 당사자들이 특정 통신 시스템 또는 채널을 선택하는 복잡성을 해결하기 위하여 통신 인프라로서의 게이트웨이를 통해 정보를 교환하게 한다.

② 해사클라우드의 보안 취약성

해사클라우드는 e-Navigation 통신 기반 기술의 핵심으로, 전 세계를 대상으로 통신이 연결된다고 볼 수 있다. 이러한 특성에 따라, 해사클라우드에서의 보안은 필수적으로 고려되어야 한다.

해사클라우드는 여러가지 다양한 통신 인프라를 활용하여 데이터가 전달된다. 즉, 단순히 인터넷 뿐만이 아니라, 여러 다양한 모든 통신 채널이 모두 포함될 수 있다. 이러한 특징은 해사 환경에서의 통신 가용성 측면에서 큰 장점을 준다.

그러나, 이러한 이면에는 보안상 큰 위험성이 존재한다. 데이터의 전달을 위하여 여러 검증되지 않은 채널을 통할 수 있고, 전달 과정에서 수많은 전달자가 존재할 수 있다. 이러한 점은 데이터 전송에 대하여 메시지 위/변조 공격의 가능성이 종래의 인터넷 환경보다 더욱 넓어질 수 있음을 시사한다.

이러한 점은 선박의 안전과 직결될 수 있는 위험이 존재한다. 만약, 악의를 가진 자가 임의로 MSI 등 여러 해사 관련 메시지에 대한 위/변조 공격을 수행할 경우, 선박은 잘못된 해사 데이터를 수신하여 안전한 운항에 큰 지장을 초래할 수 있다. 또한, 여러 다양한 채널의 활용에 따라 더욱 강한 무결성의 보장이 필요하다. 데이터의 무결성은 선박 운항에 반드시 필수적인 요소이며, 여러 채널로 통신하는 과정에서 데이터의 손실이 발생하면 즉시 판단이 가능해야 하고, 갱신할 수 있는 구조가 필요하다.

안전한 e-Navigation 환경을 위해서는 핵심 통신 인프라인 해사클라우드의 보안이 필수적으로 요구된다. 여기에는 메시지의 무결성 뿐만 아니라, 통신 과정에서 발생할 수 있는 메시지 변조, 위조, 중간자공격 등 다양한 경우에 대비할 수 있어야 한다. 악의적인 공격자가 해사클라우드 통신 인프라에 무단 침입하여 불법적인 행위를 시도하는 경우, 선박의 안전에 직접적으로 위해를 끼칠 수 있기 때문이다.

그러나, 해사클라우드에 대한 연구는 아직 초기단계이며, 이에 대한 연구 가운데 정보보안에 대한 연구는 미진한 단계이다. 해사클라우드는 기밀성, 무결성과 같은 기본적인 서비스는 제공하고 있으나, 위장공격, 정보교란, 권한 탈취, 서비스 거부 공격, 메시지 도청 공격, 메시지 위/변조 공격, 불법정보 접근, 내부자 공격 등과 같은 여러 공격에 취약할 수 있다. 이러한 문제점에 따라, 해사클라우드를 기반으로 통신하는 분산 영상 감시 환경에서도 마찬가지로 보안 취약성이 그대로 노출된다. 스마트 카메라는 보안상 민감한 정보를 담고 있을 수 있으며, 안전한 영상정보 송수신에 대한 필수적인 보장이 필요한 상황이다. 분산 스마트 감시 시스템상의 보안적인 결함은 선박, 연안, 나아가 범국가적인 안전과도 직결될 수 있기 때문이다. 따라서, 해사클라우드에서의 안전한 분산 영상감시 환경을 위한 연구가 필수적으로 요구되는 상황이다.

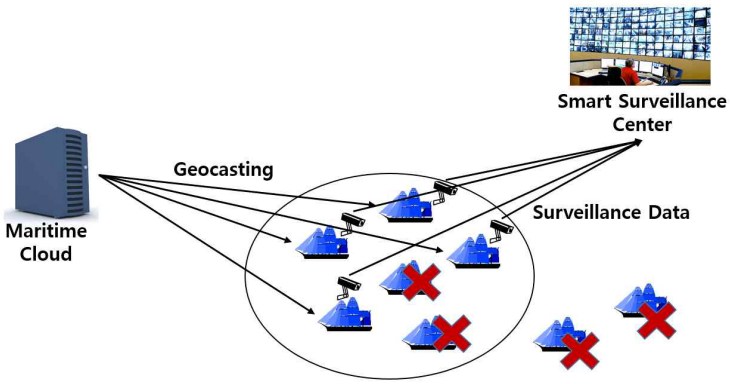
③ 해사클라우드의 주요 구성요소 및 영상감시 환경

해사클라우드의 주요 구성요소로서 해상 통신에서의 안전한 인증을 위한 해상 식별자 레지스트리(Maritime Identity Registry), 해사 서비스의 원활한 제공을 위한 해상 서비스 포트폴리오 레지스트리(Maritime Portfolio Registry), 사업자에 상관 없이 사용할 수 있는 메시지 허브인 해상 메시지 서비스(MMS)가 있다. 이러한 구성요소를 바탕으로 해사클라우드는 인가된 해상 행위자 커뮤니티에 다른 해양 행위자가 접근시 식별 및 인증을 수행하고, 안전한 데이터 접속 환경을 제공해 주며, 원활한 로밍을 기반으로 위치탐지 관련 정보 서비스를 제공한다. 아래 그림은 해사클라우드의 주요 구성요소를 나타낸다.

<그림 II-2> 주요 구성요소

해사클라우드 상에서 선박들은 국제 상호 운용성 서비스인 해상 메세징 서비스를 추가로 사용하여 통신 링크간 원활한 로밍을 실현할 수 있다. 즉, 해사클라우드를 통하여 상용화된 상업적인 데이터 링크에 의한 지오캐스트 MSI 서비스의 제공이 가능하며, 행위자는 자신의 위치 주변에 있는 지역에서 방송 또는 청취에 사용되는 통신 링크에 상관없이 논리적으로 해당 지역에서 방송을 하거나 청취할 수 있다.

한편, 스마트 감시(Smart Surveillance)라고 불리는 최근의 첨단기술은 영상정보에서 컴퓨터가 감시대상을 인식하고, 행동을 분석해서 감시목적에 부합하는 행동이 감지될 경우 이를 즉각 감시자에게 경고해 사전조치를 취하게 하는 시스템을 말한다. 이에 덧붙여, 향후 IoT환경이 현실로 도입되면 스마트 감시 영상정보를 분산 카메라를 기반으로 수집하여 통합 처리하는 분산 스마트 감시 시스템(Distrubuted Smart Surveillance System)의 필요성이 날로 증가될 것이다.



<그림 II-3> 해사클라우드 기반의 영상 감시 환경

분산 스마트 감시 환경에서는 훈련된 감시요원일지라도 사람의 능력으로는 처리 및 대응에 한계가 있을 것이며, 특히 대규모 환경에서 사람이 일일이 모니터링하여 대응하는 것은 거의 불가능에 가깝다고 볼 수 있다. 따라서 해양 스마트 감시에 필요한 영상정보를 클라우드 환경을 기반으로 통합 수집하여 관리할 필요가 있으며, 이를 원활히 제공해주는 적절한 인프라가 필요한 상황이다. 여기에서, 해사클라우드는 이에 적합한 최적의 인프라가 될 수 있다. 해사클라우드 인프라는 선박에 장착된 분산 스마트 카메라에 대한 육상에서의 영상정보 수집을 용이하게 하며, 결과적으로 클라우드 서버를 통한 분산 스마트 감시 시스템의 효율적인 활용이 가능할 것이다.

④ 해사클라우드의 Identity 관리

해사클라우드에서 신원(Identity) 관리가 의미하는 것은 기술을 사용하여 객체의 신원에 대한 정보를 관리하고, 리소스에 대한 액세스를 제어하는 프로세스를 의미한다. 신원 관리는 사용자 및 그들의 신원, 속성 및 인증 정보 관리와 관련된 비용을 절감하는 것과 동시에, 생산성 및 보안성을 향상시키는 것을 주요 목적으로 한다.

이를 위해 세계적인 규모의 해양 산업 전체에 대해 가장 일반적인 식별 요구사항을 충족시키는 솔루션을 만드는 것이 필요하나, 모든 솔루션이 소규모 선박에서부터 다국적 기업에 이르는 모든 가능한 사용자 시나리오를 지원해야 하므로, 간단한 부분은 아니다. 이러한 복잡성으로 인하여 향후 몇 년 동안에 걸쳐 여러 마일스톤을 통해 점진적으로 기능이 제공될 예정이다. 여기에는 인증 지원과 같은 기능 뿐 아니라, 해사클라우드가 지원하는 프로젝트의 사용자 요구에 따라 여러 기능 또한 추가될 예정이다.

신원 관리 및 보안은 매우 복잡하고 포괄적인 분야이며, 필수적이지 않거나 불필요한 기능은 가능한한 제한할 필요가 있다. 여기서 불필요한 기능이란, 예를 들어, 엑세스 권한이 필요하지 않은 엔티티의 정보 관리가 될 수 있으며, 또한, 보안에 대한 목적을 두지 않고 엔티티에 대한 정보를 유지하고 있는 경우도 들 수 있다.

필수적이지 않은 정보를 제외하는 주요 이유는 신원 정보 레지스트리에서는 등록된 정보를 상세하고 지속적으로 유지하고 있기 때문이다. 예를 들어, 선박에 대한 지리적 위치 뿐만 아니라, 노선이나 화물과 같은 상세정보가 같이 유지 관리되는 경우를 들 수 있다. 따라서, 정보 관리에 대한 범위가 필수적으로 고려될 필요가 있다.

가) 조직

해사클라우드에서의 조직은 집단적 목표를 가지고 외부 환경과 연결된 기관, 회사, 또는 협회와 같은 단체이다. 예를 들면, IMO, IALA, IHO 같은 국제기구 및, 미국 연안 경비대(US Coastguard), 스웨덴 해사 행정부 (Swedish Maritime

Administration)와 같은 조직뿐만 아니라 일반 상업 회사까지도 포함될 수 있다.

나) 선박

선박은 사람이나 물건의 운송에 사용되는 해양에 떠다니는 모든 객체가 될 수 있다. 해사클라우드에 선박을 등록해야 하는 주된 이유는 선박에 디지털 인증서를 발급받을 수 있으므로 선박간 보안 통신이 가능해 지며, 문서에 대한 디지털 서명도 가능하기 때문이다.

선박 인증서에는 이름, MMSI번호, IMO번호, 호출 부호 및 가능한 다른 속성이 디지털 인증서의 헤더에 포함된다.

다) 서비스

여기서 서비스란 디지털 서비스를 의미한다. 예를 들어, 기계 간 통신으로 타 서비스에서 활용 가능한 기상 서비스를 들 수 있다. 사용자 인증이 이루어질 수 있도록, 서비스가 레지스트리에 등록되어야 한다.

라) 사용자

여기에서 의미하는 사용자란, 서비스를 사용하는 주체, 즉 사람을 의미한다. 일반적으로 사용자는 로그인 시 ID와 패스워드를 사용하게 되므로, 타 객체와는 상호 작용 패턴이 다르다는 점에서 차이가 있다.

마) 장치

장치는 해사클라우드를 사용하여 인증해야 하지만, 위에 언급된 다른 객체의 범주에 속하지 않는 엔티티를 의미한다. 또한, 여기에서의 장치는 여러 엔티티의 집합이 될 수도 있다. 예를 들어, 등대가 될 수 도 있고, ECDIS, 또는 자체 인증이 필요한 서버일 수도 있다.

⑤ Identity 기반의 인증방법

인증은 시스템에 엑세스하려는 객체의 신원을 시스템이 검증하는 과정을 의미한다. 특히, 엑세스 제어는 일반적으로 리소스에 대한 엑세스를 요청하는 사용자

의 ID를 기반으로 이루어지므로, 인증은 효과적인 보안에 있어 필수적인 요소이다. 사람이나 물건의 신분을 밝히는 행위를 말하는 신분증과는 달리, 인증은 제공된 정보를 통해 신원을 실제로 확인하는 과정을 의미한다. 웹 사이트가 제공하는 디지털 인증서로 웹 사이트의 진위 여부를 확인하거나, 신원 확인 문서의 유효성을 확인하는 작업이 포함될 수 있다.

인증의 방법은 일반적으로 알고 있는 것과 같이 사용자가 알고 있는 것, 가지고 있는 것, 사용자의 고유한 특징의 세가지 범위로 가능하다. 현재 해사클라우드에서는 두가지 측면에서 인증이 이루어지며, 일반 사용자에게는 아이디/패스워드 기반의 인증으로 처리되며, 시스템 객체에 있어서는 디지털 인증서의 소유 확인에 대한 인증에 중점을 두고 있다. 여기서는 신원 레지스트리에서의 인증 방법에 대해 살펴본다.

가) Maritime PKI 기반의 M2M 통신

공개키 인프라(PKI)는 디지털 인증서를 작성, 관리, 배포, 사용, 저장 및 해지하고 공개 키 암호화를 관리하는데 필요한 일련의 하드웨어, 소프트웨어, 사람, 정책, 및 절차이다. 이를 통해 조직은 신뢰할 수 있는 네트워킹 환경을 구축하고 유지 및 관리할 수 있다. 보안 M2M 통신을 가능하게 하는 PKI 기반 솔루션을 사용하기 위한 고유한 요구사항은 별도로 존재하지 않는다. 그러나, 가장 일반적으로 사용되는 솔루션 및 소프트웨어, 모범 사례에 따라 해사클라우드에서는 M2M 통신을 위해서 X.509 표준을 기반으로 한 PKI 사용을 채택하였다.

PKI 아키텍쳐의 핵심은 디지털 인증서를 발행하는 엔티티인 PKI CA(Certificate Authority)이다. 인증서의 이름이 지정된 주체에 의해 공개 키의 소유권을 인증하는 디지털 인증서로써, 일례로 특정 선박에 발급된 인증서를 소지한 사람이 서명했음을 증명할 수 있는 선박 인증서를 만드는 경우를 들 수 있다.

현재의 해사클라우드 버전에서는 모든 인증서를 발급할 책임이 있는 단일 하위 CA가 있으며, 이 하위 CA는 해사클라우드의 신원 레지스트리에 존재한다. 그러나 이는 향후에 다른 PKI 계층 구조 디자인을 지원할 수 있도록 변경될 수도 있다.

CA의 가장 중요한 기능은 디지털 인증서를 발급하는 것이며, 이는 인증서의 지정된 주체로 공개키의 소유권을 인증한다. 이러한 신뢰 관계 모델에서 CA는

신뢰할 수 있는 제3자로, 인증서의 주체(소유자)와 인증서에 의존하는 당사자가 모두 신뢰할 수 있다.

해사클라우드의 경우, 이러한 인증서는 일반적으로 인터넷을 통한 해상 행위자 간의 안전한 연결을 위해 사용되며, 대상 서버의 경로에 있는 악의적인 사용자가 실제 대상인 것처럼 위장하지 않도록 man-in-the-middle 공격에 대비할 수 있는 인증서가 필요하다. 클라이언트는 보안 연결을 설정하기 전에 CA 인증서를 사용하여 서버 인증서의 CA 서명을 확인한다. 마찬가지로, 서버는 클라이언트의 인증서 연결을 허용하기 전에 클라이언트의 인증서를 검사할 수 있다. 예를 들어, 선박에 대한 새 인증서를 발급하려면 해당 선박을 소유한 조직의 관리자가 Maritime Cloud Portal에 로그인하여 새로운 인증서 발급을 위한 기능을 사용해야 한다. 발급되는 인증서에는 선박 이름, 소유자, MMSI 및 IMO 번호와 같은 기타 속성에 대한 정보가 포함된다. 그러나, 현재의 해사클라우드는 가입 당시 조직이 수락되어 있어야 한다는것 이외에는 이러한 정보의 유효성을 검증하지 않고 있다. 현재까지는 참여 당사자의 수가 상대적으로 적기때문에 큰 문제가 발생할 소지는 적으나, 향후에 더 많은 조직이 추가될 경우에 대비할 필요가 있을 것이다.

나) 사용자 로그인

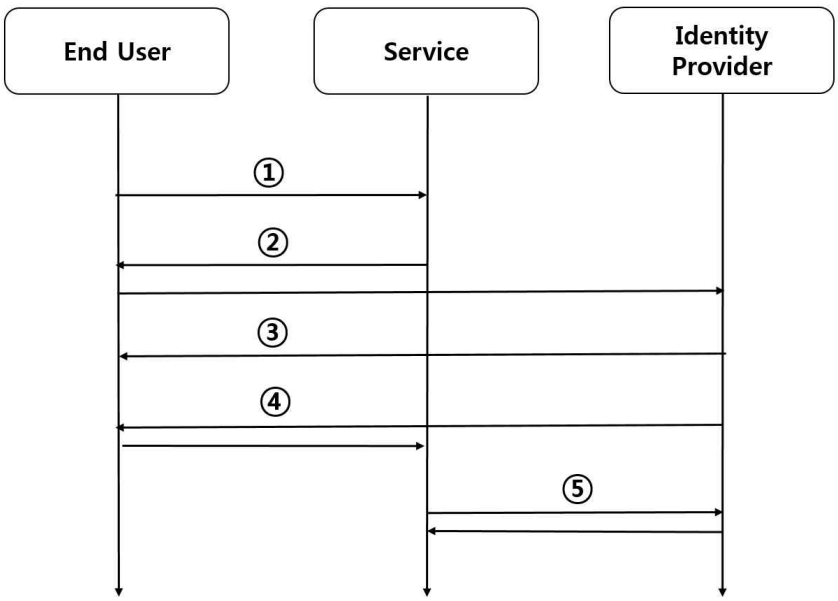
3.3.1에서는 M2M에서 사용하는 디지털 인증서에 대해 살펴보았다. 이러한 관점에서, 일반 사용자가 자신을 인증하기 위해서는 디지털 인증서를 사용하는 것은 기술적으로는 문제가 없으나, 실용적으로는 여러 문제가 존재한다. 즉, 기계간 통신 과정에서는 하드웨어의 구성 변경이 거의 존재하지 않으므로 큰 문제가 없으나, 인간인 사용자가 로그인할 경우는 엑세스가 이루어지는 컴퓨터 또는 휴대폰 등에 항상 인증서가 있어야 한다는 문제가 존재한다. 이는 해사클라우드의 활용성을 심각하게 떨어뜨릴 수 있게 되므로, 현재의 해사클라우드에서는 사용자 인증 과정에서는 디지털 인증서를 고려하지 않고 아이디/패스워드 기반의 인증 방식에 중점을 두는 측면이 있다.

한편, 해사클라우드에서는 연합(Federation)이라는 개념이 존재하며, 연합은 사람의 전자 신원 및 속성에 고유한 신원관리 시스템을 연결하는 수단이 된다. 예를 들어, 해운회사가 해사클라우드의 객체로 표시되는 방식으로, LDAP 또는 Active Drectory를 통해 모든 사용자를 해사클라우드에 노출시킬 수 있다. 따라

서, 연합을 통해 해사클라우드에서 사용자를 직접 관리해야 하는 번거로움을 피할 수 있다.

보안 도메인간 인증 및 권한 부여 데이터를 교환하기 위한 몇가지 표준이 존재한다. 특히, 여기에는 OpenID Connect라는 새로운 표준이 있으며, 이는 검증된 OAuth2 표준을 기반으로 구축되었다. 이는 Google 및 Microsoft와 같은 여러 대기업의 지원을 받고 있는 상황이다.

OpenID Connect의 작동 방식은 <그림 II-3>과 같다.



<그림 II-4> OpenID Connect 인증 흐름

OpenID Connect에는 해사클라우드의 사용자 연합에 유용하게 사용할 수 있는 여러 장점이 존재한다. 먼저, 이는 이미 존재하는 공개표준 (OAuth2, JWT)를 기반으로 한다는 것이며, 두번째로, 웹사이트/웹서비스 및 기본 스마트폰 응용 프로그램 모두를 인증하는데 사용될 수 있다는 장점이 있다. 마지막으로, 이미 오픈소스와 상업용으로 많은 구현이 되어있다는 장점이 존재한다.

<그림 II-3>에 나타난 OpenID Connect 인증의 세부 설명에 해당하는 부분은 <그림 II-4>와 같다.

1. 사용자는 웹 기반 서비스(신뢰 당사자)를 열고, “Maritime ID 로그인”을 클릭한다.
2. 사용자는 로그인 정보를 등록한 ID 공급자로 사용자를 리디렉션한다. 여기에는 예를들어, 그가 일하는 조직의 ID 공급자 설정을 들수 있다.
3. 사용자는 회사의 아이디/패스워드를 기반으로 로그인한 후, 정보를 신뢰 당사자에게 다시 전송하는 것에 동의한다.
4. 신원 제공자는 인증 코드를 사용하여 사용자(브라우저)를 신뢰 당사자에게 다시 리디렉션한다.
5. Replying Party는 신원 제공 기관에 인증 코드의 유효성을 검사하도록 요청한다. ID 공급자는 사용자에 대한 정보가 들어있는 JWT 토큰 세트로 응답한다.

<그림 II-5> OpenID Connect 인증 세부 설명

OpenID Connect는 실제 로그인을 사용자 조직에 위임하게 되므로, 사용자는 사용자가 실제로 누구인지 주장할 수 있는지 여부를 확인하는 방법에 대해 자체적인 제어가 가능하다. 즉, 사용자 아이디/패스워드 뿐만 아니라, 2 factor 인증 또는 생체 인식도 사용할 수 있다.

⑥ Identity 기반 권한 부여

신원 관리에서의 또다른 핵심 요소는 특정 신뢰할 수 있는 ID에 부여된 사용 권한 집합을 결정하는 것이다. 실질적으로 시스템이 사용자의 신원을 파악하면, 시스템은 사용자의 권한에 대해 판단이 가능하다. 권한 부여는 사용자 신원만으로도 결정될 수 있지만, 대부분의 경우는 역할, 제목, 플래그 상태 등과 같이 사용자에 대한 추가 속성도 필요한 경우가 많다. 권한 부여는 일반적으로 엑세스 중인 응용 프로그램 또는 서비스에 의해 로컬로 전달되거나, 혹은 응용프로그램 및 서비스의 위치에 관계 없이 인증정책 결정을 중앙집중화하는 두가지의 방법이 있다.

권한은 로컬상의 데이터베이스에 사용자 권한을 저장하는 것으로 엑세스 중인 응용 프로그램에서 수행이 가능하므로, 현재의 해사클라우드에서는 권한 부여에 있어 중앙집중화 방식보다는 로컬상의 사용자 권한 정책 부여 방식을 우선적으로 고려하고 있다.

일반적으로 역할기반 엑세스제어(RBAC) 기술이 많이 사용되며, 역할 권한, 사용자 역할 및 역할 관계와 같은 RBAC의 구성 요소를 사용하면 사용자에 대한 자격 할당을 용이하게 수행할 수 있다. 그러나, 해사클라우드 시스템에 RBAC을 채택할 경우, 몇가지 문제가 발생할 수 있다. 예를 들어, 누가 역할을 정의하고 글로벌 역할을 담당할지에 대한 부분이다. 또한, 특정 서비스 또는 특정 조직에 국한할지에 대한 부분도 문제가 될 수 있다. 예를 들어, 관리자 역할은 특정 조직의 권한과 다른 조직의 권한을 수반할 수 있으며, 이러한 이슈는 현재까지도 논의되고 있는 사항이다.

2. 개인정보와 영상감시 환경

1) 개인정보 개요

‘개인정보’는 개인 신상에 관한 모든 정보를 말하며, 여기에는 기본적으로 특정 개인의 식별이 가능한 정보가 포함되며, 만약 특정 개인의 식별이 어려운 경우라도 다른 정보와 결합하는 경우 유추가 가능한 경우도 포함한다. 현재의 개인정보보호법에서 정의하고 있는 개인정보란 ‘살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보’라고 정하고 있다. 전통적인 개인정보의 개념은 수동적이고 방어적인 관점이 부각되었으나, 최근에는 이러한 전통적인 개념에서 벗어나 보다 포괄적인 의미를 가지고 있다. 정보기술의 발달에 따라 전화, 인터넷 사용내역 등 개인의 상태를 간접적으로 추적할 수 있는 방법이 존재할 수 있다. 특히, 지능형 감시 시스템은 영상 및 메타정보, 센싱데이터에서 분석되어지는 다양한 정보가 개인에 대한 성향을 설명할 수 있는 개인정보로 활용될 수 있다는 특징이 있다. 이것은 지능형 감시 환경이라는 독특한 환경에서 발생하는 새로운 개인정보의 유형이며, 이러한 점에서 지능형 감시환경의 관점에서는 개인정보보호에 대해서 더욱 폭넓게 생각할 필요가 있다.

지능형 감시 시스템에서의 개인정보는 일반적인 개인정보의 정의와는 다소 다른 측면에서 바라볼 필요가 있다. 즉, 지능형 감시 시스템 환경에서의 개인정보는 지능형 감시 시스템 시스템에 관여하는 전체적인 대상, 즉, 영상 감시 객체,

감시 서비스 제공자, Third-party 등에서 사용되고 전달되어진다는 특성이 있다. 이러한 특성에 따라, 서비스 제공을 위한 여러가지의 다양한 정보들이 발생될 수 있다. 이 가운데 개인 신상에 대한 모든 정보, 혹은 단독 혹은 결합을 통하여 개인에 대한 식별이 가능하게 하는 모든 정보가 지능형 감시 시스템에서의 개인정보를 의미한다.

개인은 프라이버시를 보장받을 권리가 있다. NIST의 CSWG(Cyber Security Working Group)내 프라이버시 서브 그룹에서는 개인이 보장받아야 할 프라이버시를 크게 네가지로 정의하고 있으며, 지능형 감시에서의 개인정보는 주로 개인정보 프라이버시에 대한 내용에 직접적으로 연관되어 있다. 그러나, 다른 세가지의 측면도 중요한 고려 대상이다. 개인정보 프라이버시는 특정 개인을 식별할 수 있는 개인정보에 대한 통제 및 접근에 대한 권리를 의미한다. 이러한 특성에 따라 개인은 자신의 개인정보를 적절한 범위 내에서 통제할 수 있어야 하며, 현행의 개인정보보호법도 이런 부분에 대하여 명시하고 있다. 한편, 지능형 감시 시스템의 특징에 따라, 개인 프라이버시, 즉, 자신의 신체에 대한 무결성을 통제할 권리도 필요하다. 또한, 자신의 활동과 선택이 공유되지 않으며, 기밀로 유지될 수 있는 권리도 보장되어야 하며, 개인의 위치 추적 내용 등 여러 가지 정보에 대하여 부당한 감시, 모니터링 등에 대하여 보호받을 권리가 있다.

2) 영상감시 환경에서의 개인정보 수집

지능형 감시 환경에서, 영상 촬영 정보과 개인적으로 식별 가능한 정보를 연계하면 객체의 취향, 위치, 취미, 라이프사이클 등 개인정보로서 또 다른 연계된 정보가 생성된다. 그러나 원활한 클라우드 감시 서비스 제공을 위해, 서비스에 필요한 최소한의 개인정보는 스마트 감시를 통하여 불가피하게 수집할 필요가 있다. 소비자가 원활하게 서비스를 제공받으려면 서비스 제공자는 소비자의 개인정보를 사전에 알고 있어야 하기 때문이다.

‘개인정보’는 개인 신상에 관한 모든 정보이며, 그 정보 자체만으로 특정인의 식별이 가능하거나, 추가적인 정보를 조합하여 특정인의 식별 가능성이 있는 정보를 의미하며, 스마트 시티 환경에서는 여러가지 다양한 개인정보가 노출될 수 있다. 여기에서 개인정보는 이름, 주소 뿐만 아니라 CCTV, 센서, 미터기 등에서

발생되는 수치화 가능한 다양한 정보가 수집될 수 있다. 즉, 다음과 같이 수치화되어 저장되는 개인정보에 대한 안전한 저장방법이 필요한 상황이다.

(1) CCTV 추적정보

지능화된 CCTV에서는 객체를 인식하고, 이러한 객체에 대한 추적정보가 발생한다. 객체의 행적을 위치정보로 나타내어 수집하게 될 것이며, 이러한 점은 특정 개인이 어떤 시간에 어디에 있었는지에 대한 부분을 나타내므로 매우 심각한 개인정보 침해요소가 될 수 있다.

(2) 센싱 데이터

스마트 헬스케어를 위해 수집되는 개인 센싱정보, 스마트 홈 등에서 수집되는 정보 등 여러 센서에서 발생하는 다양한 센싱정보가 발생할 수 있다. 이러한 데이터는 IoT 서비스 등 다양한 용도로 수집될 수 있으며, 특정 개인의 신체적, 물리적 정보를 실시간으로 수집하고 현재의 상태를 직접적으로 나타낼 수 있어 강력한 보호가 필요하다.

(3) 스마트 미터링 데이터

개인의 전력 소비 성향, 라이프 스타일, 선호하는 가전기기 등 여러가지 정보가 파악될 소지가 있어 개인의 사생활 침해와 직결될 수 있다. 심지어 범죄로의 악용으로도 연결될 소지가 있으므로, 스마트 미터링 정보를 데이터베이스에 저장시는 최대한 안전한 방법을 동원하여 저장할 필요가 있다.

3) 개인정보 영상감시의 고려사항

여기서는 NIST의 개인정보보호실무지침 권고사항을 기반으로 제3자에 대한 개인정보 취급시 고려사항에 대하여 살펴본다. 여기에서 설명하는 고려사항은 개별적으로 다루기보다는 종합적인 측면에서 고려하는 것이 효과적이다.

(1) 개인정보보호고지

감시 데이터를 공유하려는 제3자는 데이터 처리에 관한 사항 및 소비자의 허가 없이는 해당 데이터가 다른 제3자에게 공개되지 않을 것을 명시한 명확한 내용을 소비자에게 고지할 필요가 있다.

또한, 규정에 의해 조직 내에서 발생한 중대한 변화가 있을 경우, 이러한 부분이 제3자 또는 계약대리인에게 에너지 사용 데이터의 공개와 관련이 있을 경우에도 별도로 고지되어야 할 것이다.

고지는 소비자와 사업적 관계를 가지는 제3자가 작성해야 하며, 해당 트랜젝션에 직접적으로 관여하지 않는 주체는 별도로 고지를 전달할 필요는 없다.

(2) 공개에 관한 소비자의 허가

개인정보는 소비자가 공개를 허가하지 않는 한 다른 제3자에게 공개해서는 안되며, 이러한 허가를 획득하는 과정에서 다른 제3자의 신원을 소비자에게 고지해야 한다. 제3자가 소비자의 허가를 구하고자 할 경우, 허가 절차 가운데 에너지 소비 데이터의 공개에 관해 소비자가 선택할 수 있는 범위를 명시해야 한다.

만약 소비자가 이미 허가한 서비스 또는 제품을 공급하거나, 소비자에 대한 기타 의무를 이행할 때에는 회사가 법률을 준수하는 한도 내에서는 별도로 소비자의 허가를 취득할 필요는 없다.

한편, 제3자는 감시 서비스 제공자가 본인의 감시 데이터에 대한 엑세스 권한을 가지고 데이터에 존재하는 부정확성의 시정을 요청할 수 있는 절차를 개발하고 소비자에게 알려야 한다. 데이터 엑세스 권한을 획득하기 위한 절차는 평균적인 소비자에게 비교적 간단한 절차가 되어야 할 것이다.

(3) 정보 공개의 범위

제3자가 수집할 수 있는 감시 데이터는 소비자가 허가하는 특정한 목적을 이행하는 데 필요한 데이터로 한정하여야 한다. 만약, 기존에 허가된 목적과 다른 목적으로 사용하여야 할 경우는 별도로 소비자의 허가를 취득해야 한다.

(4) 소비자 교육 및 인식

제3자는 제3자의 개인정보보호 정책 및 지침을 소비자에게 알려야 하며, 조직이 개인정보의 무단 사용에 관한 잠재적 위험을 완화하기 위해 취하는 조치를 요약하고 소비자가 본인의 위험을 완화하기 위해 취할 수 있는 조치를 설명한 교육 및 인식 자료를 소비자에게 제공할 필요가 있다. 한편, 영상 감시 데이터는 기술, 시기 및 평가상의 차이와 같은 요인에 차이가 발생할 수 있다는 점을 소비자에게 인식시킬 필요도 있다.

(5) 정보 수집의 최소화

제3자에 의한 에너지 사용 데이터 수집은 서비스 또는 제품의 제공 등 소비자가 허가한 목적을 이행하는 데 필요한 정보에 국한되어야 한다. 만약 필요에 의해 수집된 데이터가 특정 시간 이후 필요성이 사라졌을 경우는 정책에 따라 폐기조치를 해야 할 필요가 있다.

(6) 데이터 품질

영상감시 데이터를 사용하는 제3자 및 제3자 계약 대리인은 데이터의 정확성과 완전성을 보장하기 위해 할 수 있는 최대한의 조치를 수행할 필요가 있다.

경우에 따라 제3자는 영상감시 데이터를 수정해야 하는 경우도 있을 것이다. 따라서 데이터의 정확성 및 완전성은 데이터를 제공받은 당시에 한한 것이라는 것을 염두에 두어야 한다.

(7) 데이터 보안

제3자는 데이터 보안에 관한 정책, 절차 등을 통해 무단 엑세스, 복사, 수정, 부적절한 공개, 또는 분실로부터 정보를 보호해야 하고, 제3자의 계약대리인 또는 다른 제3자에게 공개되는 데이터의 정확성을 보장해야 한다. 이러한 정책 및 절차는 정기적으로 검토 평가가 이루어져야 하며, 데이터를 적절히 처리할 필요

성에 따라 갱신해야 한다. 또한, 제3자는 보안 및 개인정보보호정책을 적절하게 유지, 갱신 및 준수할 업무를 담당할 직위 및 직원을 배정하여야 한다.

(8) 위험 평가

제3자는 제3자의 계약대리인에게 영상 감시 데이터를 공개하는 절차에 대해 정기적인 영향 및 위험평가와 분석을 실시하고 문서화해야 한다. 해당하는 경우, 관련 정책 및 실무지침을 갱신하는 경우에도 개인정보보호 위험분석 및 영향평가를 실시해야 한다.

(9) 영상 데이터 보관 및 폐기

특별한 경우를 제외하고, 제3자는 수집 목적을 이행하는데 필요한 경우나 합리적으로 판단했을 때 법적 또는 규제적 요건을 준수해야 할 의무를 진 것으로 해석되는 경우를 제외하고는 영상 감시 데이터를 보유하지 않아야 한다. 만약 영상 감시 데이터가 연구용으로 사용될 경우, 이러한 활동에 관해 데이터를 보유 및 익명화할 정책 및 절차를 확립해야 할 필요가 있다.

또한, 데이터 보유 정책을 소비자 고지 형식으로 소비자에게 고지해야 하며, 수집 보유에 대한 허가를 철회한 이후에 데이터를 영구적으로 파기해야 하는 상황과 방법을 명시해야 할 필요가 있다.

(10) 데이터 침해

제3자는 제3자 또는 계약대리인에게 적용될 수 있는 데이터 침해에 대한 제도적인 요건을 사전에 숙지해야 하며, 무단 침해가 발생하는 경우 정책에 따라 고지의 의무를 다해야 한다.

(11) 직원 교육

제3자 및 제3자의 계약대리인은 문서화된 시행 절차와 함께 공식적으로 문서화된 보안 및 개인정보보호 인식/교육 정책을 개발, 배포하고 정기적으로 검토하

고 갱신할 필요가 있다. 또한, 조직은 개인정보보호에 관한 기초 인식 교육을 비롯하여 각 직원의 보안 및 개인정보보호 교육에 대한 활동을 문서화하고 유지 및 모니터링 할 필요가 있다.

3. 영상감시를 위한 보안기술

1) DB 암호화

데이터베이스 질의 처리가 용이하도록 하는 변형된 암호화 방식인 순서유지 암호화 기법(Order-Preserving Encryption)이 있다.

일반적인 암호화 알고리즘을 데이터베이스에 적용한다면, 암호화된 데이터의 순서가 평문과 달라지므로 데이터베이스의 인덱스를 구성할 수 없다. 이러한 문제를 극복하기 위해 제안된 방법으로, 암호화된 상태 그대로 데이터베이스 인덱스 처리를 하여도 문제없이 작동하고, 별도의 절차 없이 범위검색, 전방일치검색, 통계질의 등이 가능하게 하는 기술이다.

순서보존 암호화 기술 중 대표적인 연구로 Agrawal이 제안한 OPES가 있으며, 이는 수치 데이터에 대한 순서는 보존하면서, 분포를 변경하여 원본 데이터에 대한 정보 노출을 최소화한다는 장점이 있다.

그러나, 순서보존 암호화 알고리즘은 평문과 정렬 순서가 같다는 치명적인 단점이 존재한다. 극단적으로, 평문 데이터의 집합과 그 순서를 알고 있다면, 암호화된 데이터베이스에서도 평문의 순서대로 나열하면 결국 동일한 데이터를 얻을 수 있을 것이다.

한편, 순서보존의 특성상 여러 가지 다양한 공격이 가능할 수 있으며, 특정 두 값의 대소 비교만으로도 많은 정보가 노출될 수 있기 때문에 보안성 측면에서는 많은 취약성이 존재한다.

2) 데이터 비식별화

비식별화(De-Identification)기술이란 개인정보의 침해 위험을 최소화할 목적으로 데이터를 변경하거나 일부를 삭제하여 특정 개인을 식별할 수 없도록 하는

기술을 의미한다. 최근 빅데이터와 환경이 도입되면서 방대한 개인정보를 실시간으로 분석하여 비즈니스 활용의 근거를 제공하는 등 개인정보의 침해 위험이 높아지고 있다. 이에 따라, 2013년 9월 안전행정부는 효과적으로 개인정보를 보호하기 위한 목적으로 개인정보 비식별화 기준을 발표한 바 있다. 또한, 최근 NIST에서는 개인정보 비식별화에 관한 보고서인 'De-Identification of Personal Information'을 발표하였다. 또한, 2012년 3월에는 개인정보의 비식별화 가이드라인인 'Protecting Consumer Privacy in an Era of Rapid Change'을 수립한 바 있으며, 개인을 식별가능한 장치와 연관될 수 있는 것은 어떤 경우라도 보호의 대상이 되어야 한다고 규정하였다. 특히, 개인 및 컴퓨터 및 장치에 대한 정보를 식별할 수 있는 데이터의 삭제, 수정, 'noise' 추가, 샘플링 등 적절한 방법으로 반드시 비식별 조치를 취해야 함을 명시하고 있다.

일반적으로 개인정보를 비식별화하는 방법은 가명처리(Pseudonymization), 총계처리(Aggregation), 데이터 값 삭제(Data Reduction), 범주화(Data Suppression), 데이터 마스킹(Data Masking) 등이 있다.

그러나 이러한 방법들만으로는 스마트 감시 환경에서 측정된 데이터로부터 개인정보를 안전하게 보호하기는 쉽지 않다. 알려진 비식별화 방법은 감시 데이터의 특성과 적합하지 않다. 즉, 감시 데이터는 개인 활동사항이 측정되는 정보로서, 총계처리나 범주화 등으로 명확하지 않은 값으로 보관하면 서비스의 원활한 제공에 지장이 생길 수 있고, 통계 처리에 있어 명확하지 않은 부분도 발생하기 때문이다. 예컨데, 구체적으로 어떤 시간에 전력이 많이 소비된다는것을 알고자 한다면, 스마트 미터링 데이터를 상세하고 구체적으로 가지고 있을 필요가 있다.

그러나, 감시 데이터는 일종의 개인정보로서 평문 그대로 가지고 있는 것은 매우 위험하다. 감시 데이터를 분석하면 사용자의 습관 등 라이프 스타일을 추정 가능하기 때문에, 결국 해당 데이터의 주체가 누구인지 판별이 가능할 수 있다. 따라서, 감시 데이터에 적합한 보안 기술이 필요한 상황이다.

3) 프라이버시 마스킹

프라이버시 마스킹 기술은 일반적으로 영상의 얼굴 데이터를 알아볼 수 없도록 변경하는 것을 의미한다. 예를 들어, 블러링, 픽셀화, 얼굴영상 제거방식을 들

수 있는데, 이러한 방식은 근본적으로 복원이 필요한 경우에도 원본 영상으로 완전하게 복원할 수 없다는 한계점을 안고 있다.

<그림 II-6> 영상 마스킹 기술

프라이버시 마스킹 기술은 구현의 용이성 및 프라이버시 보호의 장점이 있으므로 현재 다수의 CCTV 보안 제품에서는 마스킹 기법을 활용하고 있다. 그러나 향후 빅데이터 기반의 영상 복원기술인 Deep-Resolution 기술이 도입되면, 공개된 영상만으로도 블러링 및 픽셀화된 얼굴 정보가 원본에 가깝게 복원될 수 있을 가능성이 있어, 프라이버시 위험에서 안전을 보장할 수 없다.

일방향 프라이버시 마스킹 기법의 단점을 보완하기 위해 ROI(Region of Interest) 영역의 부분 암호화 방식도 제안된 바 있다. ROI 부분암호화 방식은 영상 내의 얼굴 등 특정 영역만을 암호화하는 것으로, 통상적인 암호화 알고리즘과 동일하게 암호화 시는 얼굴정보를 식별할 수 없으나, 암호화 키를 활용하여 영상을 복호화할 경우 원본 영상을 복원할 수 있는 방식이다. 그러나 부분 암호화 방식은 암호화된 ROI 영역에 대한 메타정보를 어떻게 생성하고 보호할 것인지에 대해서는 언급하지 않고 있다. 구체적으로, 암호화된 영상 스토리지 상에서 특정인만 검색하여 원본 영상으로 복원하고자 할 경우는 실질적으로 처리할 수 있는 방법이 없으며, 이를 위해 임의로 검색 메타정보를 생성할 경우는 해당 메타정보에 그대로 영상 주체가 노출된다는 문제점이 존재한다.

4. 영상감시 관련 정책적 이슈

1) 현행 법제도 현황

(1) 개요

최근 IoT(Internet of Things)가 많은 관심을 모으고 있으며, 관련 연구가 활발하게 진행되고 있다. IoT는 실생활을 인터넷과 연결시켜 준다는 측면에서 생활에 많은 편의를 가져다 주며, 시장에서도 IoT 관련 제품의 출시가 점차 증가하는 추세이다.

그러나, 향후 IoT 환경이 안정적으로 정착하기 위해서는 보안에 대한 신뢰가 보장되어야 함은 자명한 사실이다. IoT는 사물과 인터넷이 결합된 형태로 실제 물리적 환경과 밀접하게 연결되어 있어, IoT에 대한 보안의 위협은 현실의 신체적, 물질적 손실로 그대로 다가올 수 있으며, 이는 IoT 환경 도입의 큰 걸림돌로 작용할 것이다. 특히, IoT 환경의 특성상 종래의 IT환경보다 피해규모가 훨씬 더 커질 수 있다. 따라서 IoT 제품은 설계, 개발, 운영 단계에서 여러가지 다양한 보안 요소가 사전에 고려되어야 한다.

한편, 현재 출시된 IoT 제품에 대한 보안성 유지관리 방안에 대한 대책마련도 시급하다. 현재 IoT 제품의 보안 취약성을 통하여 사용자의 개인정보 침해 등 여러 피해가 접수된 사례가 있으며, 이러한 사고의 빠른 대응을 위한 체계가 필요한 상황이다. 따라서 현재 국내에서는 민관 협력단체인 'IoT 보안 얼라이언스'가 구성되어 있으며, IoT 제품 및 서비스의 기본적인 보안성 확보 지원 및 제도적인 대책을 마련하고 있다.

아직까지 IoT 보안에 대한 정책적 대응은 진행중에 있다. IoT 환경은 실생활과 밀접하게 관련되어 있는 바, 보안 사고가 발생하면 큰 피해가 예상되므로 시급한 보안 대책 수립이 필요한 상황이다.

따라서, 본 절에서는 개인정보 감시 기반기술인 IoT 제품의 정책 및 제도적 현황을 살펴본다.

(2) 국내외 개인정보보호법 현황

개인정보보호는 EU와 미국을 중심으로 발전해 온 양상을 보인다. 기본적으로 EU는 개인정보를 개인의 기본권 측면에서 접근하고 있으므로, 개인정보의 처리 기준, 방법, 절차 등을 구체적으로 명시하고 있다. 한편, 미국은 개인정보를 프라이버시 보호의 측면에서 접근하는 경향이 있다. 즉, 민간에 있어 최소한의 보호를 원칙으로 사후적으로 취급하는 경향이 있다. 또한, 정부의 규제가 금융, 의료, 통신 등 특정 영역에서 제한적으로 행해진다는 특성이 있다.

국내에서는 민간에서의 개인정보보호를 위한 “신용정보의 이용 및 보호에 관한 법률” 및 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”에 개인정보보호에 대한 부분을 명시하고 있다. 그러나 이러한 부분으로 개인정보를 안전하게 보호하는 데에는 한계가 있어, 공공 및 민간 전체에 적용되는 “개인정보보호법”을 제정하여 2011년에 시행된 바 있다.

한국의 경우는 정치/경제적으로 미국의 영향을 받는 편이나, EU와 같은 개인정보보호 규제제도를 운영하고 있다는 특징이 있다. 미국의 경우에는 법률 위반 시에 민사법으로 처리되나, EU와 한국은 동일하게 형사법으로 처리된다.

지능형 감시환경의 개인정보보호에 대한 법적 문제를 고려할 때는 현행의 개인정보보호법이 지능형 감시환경을 명시적으로 지칭하지 않았다 하더라도 지능형 감시환경에서 생성되는 개인정보에 적용되는지 여부를 확인하는 것이 중요하다. 현재의 개인정보보호법이 지능형 감시환경 기반기술에 의해 수집, 저장 및 전송되는 개인데이터에 적용되는지에 대한 여부가 확실하지 않은 부분이 있더라도, 지능형 감시환경이 새로운 개인정보보호 문제를 일으킬 소지가 있다는 것을 염두에 두어야 한다.

(3) 영상기기 관련 제도 현황 및 개선방향

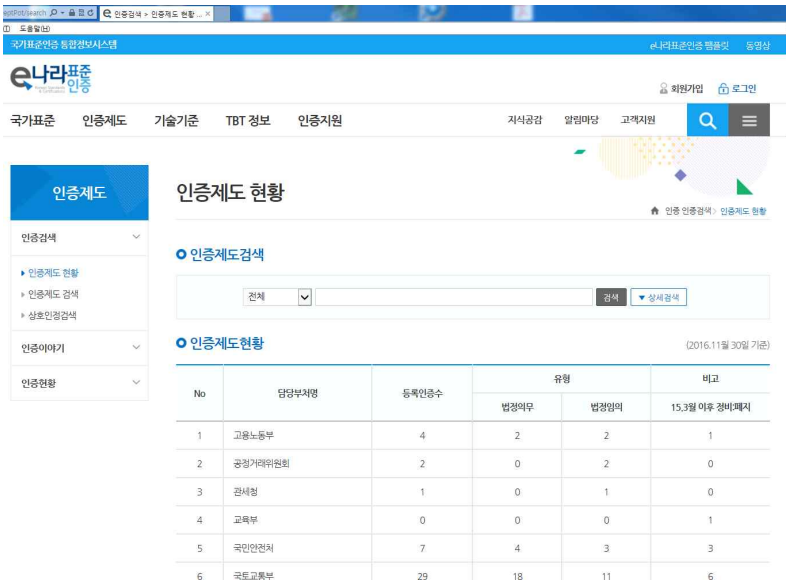
① IoT 유관 품질인증제

현재 각 부처에서는 제품 생산시에 필요한 인증제도를 운영하고 있다. 품질인증이란 해당 제품이 특정 품질 기준을 준수하여 적합하다는 평가를 받음으로써

지속적으로 생산할 자격을 갖추었는지를 증명하기 위한 제도이다.

인증제도는 개별 법령에 의해 운영되는 강제인증과 필요에 의해 이루어지는 임의인증으로 구분되며, 이는 강제성 여부가 주요 기준이 된다. 또한, 법적 근거의 유무에 따라 법정인증제도와 민간인증제도로 구분할 수도 있다. 현재 각 부처에서 인증, 형식승인 검정, 형식검정, 형식등록 등 제품의 특징에 따라 다양한 명칭으로 운영되고 있다.

국가기술표준원에서는 국가표준인증 통합정보시스템(e나라 표준인증)을 운영하고 있으며 국가/국제 표준과 국내 부처별 각 인증제도 현황을 제공한다.



<그림 II-7> 표준인증 통합정보시스템

2017년 2월 현재 각 부처별 다양한 인증제가 존재하고 있으며, 법정의무 72건, 법정임의 98건으로 총 170건의 등록인증이 실시되고 있다.

각 인증제는 관련 법률에 근거하고 있다. '전기용품안전관리제도'는 전기용품안전관리법에 근거하며, 산업통상자원부가 소관하고 있다. 이는 IoT 홈/가전 제품에서 의무적으로 받아야 하는 인증이며, 전기용품을 생산/조립/가공하거나 판매/대여 혹은 사용할 때의 안전관리에 대한 사항을 규정하고 있다.

또한 스마트미터의 계량기에 적용될 수 있는 '계량기 형식승인 및 검정' 제도가 산업안전보건법에 근거하여 법정의무사항으로 실시되고 있다. 한편, 커넥티드

카에 실시될 수 있는 '자동차 및 자동차부품 자기인증'이 자동차관리법에 근거하여 국토부의 소관으로 실시되고 있다.

이와 같이 다양한 법령에 근거하여 IoT 제품에 적용되는 품질인증제도가 국내에 운영되고 있으나, 해당 품질인증제도는 대부분 보안에 대한 사항은 고려하지 않고 있는 실정이다.

한편, 관련법에 근거하는 기술기준도 존재한다. 기술기준이란 정부와 단체에 의해 채택되었거나 계약에 의해 채택되어 법적 구속력을 갖는 표준으로, 상품, 공정 및 생산방법에 적용되는 기술규범을 의미한다. 이러한 기술기준은 각 부처가 소관 분야에 따라 개별적으로 관리운영을 실시하고 있다. 본 논문에서 법정의무 인증제와 기술기준을 다루는 이유는, 해당 제도에 대응하는 IoT 제품 출고시 인증제 및 기술기준에 필수적으로 적합해야 하며, 이러한 점에 근거하여 제품 출시 이전에 제도적인 강제성을 부여할 수 있다는 특징이 있기 때문이다. 즉, 해당 인증제도 및 기술기준에 대해 보안성에 대한 항목을 추가하는 것만으로 IoT 제품의 정책적 보안 규제가 이루어질 수 있다는 점에서 의의가 크다.

② IoT 영상기기 제도 개선방향

가) 개요

현재 다양한 IoT 유관 품질인증제도 및 법적 기술기준이 존재하고 있다. 기술기준은 정부가 환경, 안전, 보건 등 국민의 권리를 위해 법적 구속력을 가지고, 법률에 의하여 강제력을 가지는 기술규범이다.

앞서 언급하였듯, 현행 시행되는 대부분의 인증제 및 기술기준은 제품 자체의 기기적 안전 또는 사용자의 신체적/재산적 안전, 또는 환경에 대한 부분을 규정하고 있는 것이 일반적이다.

본 논문에서는 주요 제도 개선 접근방법으로, 한국인터넷진흥원(KISA)이 제시하고 있는 IoT 7대 공통 보안 원칙에 근거하여 각 IoT 제품별 적합한 보안 조항을 그에 대응하는 제도의 항목에 추가하는 방법으로 접근하였다. IoT 7대 보안 원칙은 제품의 설계, 개발, 운영 등 IoT 제품의 전 주기에서 단계별로 고려해야 할 사항을 명시하고 있어 개선 목적에 적합하다. 본 논문에서는 제도적 개선 대

상 기술기준으로써 국토교통부고시 제2016-64호, 미래창조과학부고시 제2016-30호, 산업통상자원부고시 제2016-14호로 제정되어 있으며 IoT 제품과 밀접하게 연관되는 기술기준인 '지능형 홈네트워크 설비 설치 기준'을 선정하였다. 다음 절에서는 해당 기술기준에 대한 개선(안)을 제시하고자 한다.

나) 지능형 홈네트워크 설비 설치기준 개선방향

'지능형 홈네트워크 설비 설치 기준'은 지능형 홈네트워크 설비의 설치에 필요한 사항을 규정하고 있으며, 주택법 제35조 및 주택건설기준 등에 관한 규정 제32조의2에 근거하여 법적 구속력을 가진다.

따라서, 해당 기술기준에 보안항목을 추가하여 보완하는 것으로, 홈네트워크 IoT 환경에서의 보안 설계가 의무화될 것으로 기대된다.

당 기준의 제5조(홈게이트웨이)부분은 홈게이트웨이의 설치 위치, 전원 공급 여부, 작동상태 확인 여부에 대한 조항을 명시하고 있으며, 해당 조항에 아래와 같이 4항으로 신규항을 추가할 것을 제안한다.

◉ 제5조 현행과 동일
◉ ((1~3) 각 항 현행과 동일)
◉ ④ 홈게이트웨이는 데이터통신 및 개방형 플랫폼에서 안전성을 보장하는 보안 프로토콜을 준수하여야 하며, 안전한 파라미터가 설정되어야 한다.

홈게이트웨이는 보안 기능 미비시 IoT 보안 취약성에 노출될 가능성이 있으므로, 상호인증 및 안전한 보안 통신의 제공이 필요하다. 현재 다양한 국내외 표준기구에서 보안 기술이 논의되고 있으며, MQTT, CoAP, LwM2M, Zigbee와 같은 IoT 제품 및 서비스에 활용 가능한 경량 통신 프로토콜이 존재한다. IoT 기기에는 통신 및 플랫폼에서 안전성을 보장하는 통신 프로토콜이 적용되어야 한다. 특히, 프로토콜 상에서 보안 모드를 설정하도록 되어 있는 경우, 안전한 파라미터의 설정이 필요하다. CoAP는 기기간 통신을 위하여 다양한 인증 방식을 제공한다. CoAP에는 4가지 보안 모드가 있다. No Security 모드를 제외하면 DTLS가 지원하는 대칭키 암호 AES, 공개키 암호 ECC 등이 지원되며, 이를 사용하면 더 높은 보안수준을 활용할 수 있다는 특징이 있다.

한편, 제7조(원격제어기기)부분은 취사용 가스벨브의 원격제어 유무, 조명제어기 설치 여부, 디지털도어락과 월패드의 연동 여부를 명시하고 있다. 해당 조항에 아래와 같이 4항으로 신규항을 추가할 것을 제안한다.

◉ 제7조 현행과 동일
◉ ((1~3) 각 항 현행과 동일)
◉ ④ 원격제어기기는 암호화 통신을 지원하여야 하며, 안전한 초기 보안 설정으로 출고된 제품을 사용하여야 한다.

원격제어기기는 해킹에 노출될 우려가 있다. 특히, 원격제어기기에서 초기 보안설정의 미비로 인한 보안 취약성 사례도 발견된 상태이다. 따라서 위와 같은 조항을 추가하였다. 제13조(단지서버)에는 클라우드 컴퓨팅 서비스를 이용하는 부분에 관한 내용이 명시되어 있으며, 5항에서는 암호화 등을 통하여 클라우드 컴퓨팅 서비스 이용 과정에서 보안문제가 발생하지 않아야 할 것을 명시하고 있다. 해당 조항에 아래와 같이 6항으로 신규항을 추가할 것을 제안한다.

◉ 제13조 현행과 동일
◉ ((1~5) 각 항 현행과 동일)
◉ ⑥ 5항에서 보안문제가 발생하였을 경우, 적절한 IoT 침해사고 대응체계를 갖추어야 하며, 책임 추적성이 확보되어야 한다.

IoT 시스템에서 클라우드 컴퓨팅 서비스를 이용하는 것은 여러 다양한 보안문제를 야기할 수 있으며, 제13조5항에 이미 암호화 등을 통한 사전 보안 고려사항을 명시하고 있다. 그러나, 클라우드 컴퓨팅의 특성상 보안 침해시 사고 발생에 따른 대응체계 및 책임 추적성이 별도로 요구되며, 해당 기술기준에는 이에 대한 항목이 별도로 존재하지 않으므로 해당 조항의 6항으로 추가하여 보안성을 확보하였다.

제16조(주동출입시스템)에서는 주동출입시스템의 설치 위치, 화재발생 등 비상시 작동, 설치방법, 접지단자 설치여부를 명시하고 있으며, 5항에서는 월패드간의 통신이 가능할 것을 명시하고 있다. 본 논문에서는 해당 조항에 아래와 같이 6항을 추가할 것을 제안한다.

◉ 제16조 현행과 동일
◉ ((1~5) 각 항 현행과 동일)
◉ ⑥ 5항에서 주동출입시스템과 월패드 간 통신 시 암호화 등 검증된 보안 프로토콜을 지원해야 한다.

주동출입시스템은 월패드와 통신이 이루어지며, 통신이 원활치 않을 시 화재 발생 등 비상시에 신체적재산적 피해를 발생시킬 수 있다. 만약 해커가 주동출입 제어시스템과 월패드간 통신 네트워크에 침입하여 변조, 위조, 차단등의 공격을 감행하는 경우 사용자의 직접적인 피해가 우려되므로 월패드간 통신시에는 반드시 검증된 보안 프로토콜을 사용할 수 있도록 하는 것이 바람직하다.

제17조(원격검침시스템)에서는 각 세대별 원격검침장치가 운용시스템의 동작 불능시, 정전시에도 작동할 수 있어야 함을 규정하고 있다. 본 논문에서는 해당 조항에 아래와 같이 3항을 추가할 것을 제안한다.

◉ 제17조 현행과 동일
◉ ((1~2) 각 항 현행과 동일)
◉ ③ 원격검침장치는 데이터 암호화, 무결성 확보 등을 통하여 보안 문제가 발생하지 않아야 한다.

스마트미터 등 원격 검침장치에는 사용자 프라이버시 노출 위협 등 보안이슈가 존재한다. 따라서, 가능한한 데이터를 암호화 후 저장하여 검침 데이터 및 사용자의 프라이버시를 보호할 필요가 있다. 또한, 검침 데이터의 손실/변경이 발생하지 않아야 하며, 이러한 부분을 해결하기 위한 무결성 확보 대책이 필요하다.

(4) 전력기반의 스마트 감시 관련 법제

① 지능형 전력망 촉진법

2011년, '지능형전력망의 구축 및 이용촉진에 관한 법률'이 제정되었다. 이는

지능형전력망을 종합적이고 체계적으로 다룬 법률로써, 우리나라가 세계최초로 제정했다는 점에서 큰 의의가 있다.

이는 지능형전력망의 구축 및 이용촉진을 함으로써 관련 산업 육성 및 환경변화에 대처하고 미래산업의 기반을 조성하는 것을 목적으로 하고 있다. 지능형전력망법의 주요 내용으로는 먼저 지능형전력망 추진체계 구축에 대한 부분, 그리고 지능형전력망 기반조성 및 이용촉진, 마지막으로 지능형전력망 정보의 수집·활용 및 보호 등으로 나누어 볼 수 있다.

지능형전력망 촉진법 제4장에서는 지능형전력망의 안전성을 위하여 정보보호 관련 조항을 포함하고 있다. 제4장 제22조에는 개인정보의 수집 조항이 포함되어 있으며, 여기에는 개인정보를 동의없이 수집하거나 처리할 수 없다는 내용과, 정보주체는 정보의 열람, 정정 삭제에 대한 요구가 가능해야 한다는 내용을 명시하고 있다.

또한, 제23조에는 개인정보의 제공시에 대한 조항을 포함하고 있다. 이는 타 업체에게 정보 제공시 정보 주체에게 동의를 구해야 한다는 내용을 명시하고 있다.

② 지능형 전력망 보호지침

지능형전력망 촉진법에 대한 세부적인 지침으로, 지식경제부고시 제2012-129호로 제정된 '지능형전력망 정보의 보호조치에 관한 지침'이 제정되어 있다. 해당 지침에는 '지능형전력망의 구축 및 이용촉진에 관한 법률'의 제26조 제3항에 의거하여 지능형전력망 정보의 신뢰성과 안전성 확보를 위해 지능형전력망 사업자 측면에서 준수할 필요가 있는 세부 기준을 정하고 있다.

이 지침은 지능형전력망 정보에 대한 기술적·물리적·관리적 보호조치를 규정함과 동시에, 지능형 전력망의 개인정보보호를 위한 지침을 규정하고 있다. 지침의 보호대상은 지능형 전력망 정보 및 개인정보 전체를 포괄하고 있으며, 이 가운데 기술적 보호조치 11개 조항, 물리적 보호조치 3개 조항, 보안관리정책 10개 조항이 있으며, 개인정보보호 정책은 15개의 조항으로 규정하고 있다.

해당 지침은 각각 제2장에서 기술적인 부분에 대한 보호조치, 제3장에서는 물리적인 보호조치, 제4장에서는 관리적인 보호조치에 대한 내용을 명시하고 있다.

여기에서 제4장의 제2절이 지능형전력망 개인정보에 대한 조항으로, 여기에는 개인정보에 대한 수집, 고지 또는 명시, 수집의 제한, 이용 및 제공의 제한, 비밀유지, 개인정보의 위탁, 양도 또는 통지, 파기 등의 내용을 담고 있다.

③ 전력망 감시 환경의 개인정보 위험성

에너지 데이터와 개인정보는 명시적으로나 암시적으로 특정 개인, 개인들의 집단 또는 개인의 활동에 관한 정보를 노출시킬 수 있다. 사용 빈도, 에너지 생성 데이터, 에너지 소비 보고의 기능이 있는 가전기기 및 장치의 사용이 증가함에 따라 에너지 사용량 측정치와 같이 스마트그리드 데이터에 따른 새로운 영역의 개인정보가 발생하게 된다.

스마트그리드에서는 기존의 전력계 대신 스마트미터라고 칭하는 새로운 전력계를 가정이나 사무실 등의 전력 소비지에 설치한다. 스마트미터는 단순히 누적 소비량과 월간 소비뿐만 아니라 네트워크 회선을 사용하여 소비전력 등의 정보를 실시간으로 전력회사에 전송한다.

스마트 미터는 각 공장이나 가정에 설치하여 전기 사용량의 변화를 자세히 파악할 수 있다는 특징을 가진다. 그러나, 이러한 스마트 미터를 통해 얻은 데이터는 사생활 침해의 위험성을 안고 있다. 그것은 스마트 미터에 의해 얻어진 전기 사용량의 변화를 알게 함으로써 외출 시기와 같은 생활 스타일을 어느정도 파악할 수 있게 된다는 특징이 있기 때문이다. 이러한 특성에 따라, 데이터를 장기간 수집 시 특정 개인의 라이프 로그로 활용될 우려가 있고, 이것은 개인에 대한 범죄로의 악용 등 심각한 문제로 이어질 우려가 있으므로 이러한 문제에 대해서 검토하고 대책을 마련할 필요가 있다.

집 또는 건물 안에서의 상세한 활동은 기기의 전자서명, 각 가전기기의 사용 데이터, 사용 시간의 패턴 및 기타 데이터를 통해 도출할 수 있다. 특히 이러한 장시간 수집 및 분석된 정보는 점유자의 활동과 생활방식을 파악하는 기초자료로 악용될 수 있다. 예를 들어, 이러한 정보를 토대로 부재 여부, 취침 일정, 작업 일정과 같은 여러 가지의 일상적인 활동을 예측할 수 있다. 이러한 부분은 서비스 공급자 및 이용자에게 여러 이점을 가져다 줄 수도 있지만, 한편으로는 개인정보보호에 영향을 미칠 것이다.

이외에도 스마트그리드에서 다루어야 할 개인정보보호 취약점은 상당수 존재하며, 이는 스마트그리드 시스템의 구현이나 효용성에 영향을 미칠수도 있다. 예를들어, 에너지 소비량에 대한 개인정보보호 노출의 우려가 있는 상태라면, 소비자에 대한 신뢰의 결여가 발생함으로, 스마트그리드 활성화에 악영향을 미칠 우려도 있다.

④ 지능형 전력망 보호지침의 한계점

가) 목적 구분의 불명확성

현재의 지능형전력망 보호지침은 정보 이용 및 제공의 목적에 대한 구체적인 구분 방법을 명시하지 않고 있다. 이러한 점은 개인정보 사용에 있어 어떤 목적의 구분 없이 모두 동일한 정책을 따르는 문제가 발생한다. 즉, 고객의 개인정보에 대해 반드시 필요한 서비스에서 사용되는 경우와, 부가적으로 취급되는 개인정보에 대해 사용되는 경우는 구분하여 처리될 수 있어야 한다.

개인정보보호법의 제3조 제1항에서는 '개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고, 그 목적에 필요한 범위내에서 최소한의 개인정보만을 적법하고 정당하게 수집되어야 한다'라고 명시하고 있으며, 제2항에서는 '개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 사용해서는 아니된다'라고 명시하고 있다. 이러한 규정에 의거하여, 개인정보는 그 사용의 목적에 맞게 각각 다른 정책을 가지고 처리될 필요가 있다.

본 논문에서는 이러한 구분을 1차적 목적과 2차적 목적에 따른 구분이라고 규정하며, '1차적 목적'이라 함은 고객이 서비스 제공에 따라 자신의 개인정보의 이용이 발생할수 있다는 부분을 충분히 예상할 수 있는 경우를 의미하고, '2차적 목적'이라 함은 고객이 자신의 정보가 제공될 것이라는 부분에 대해 명확히 알 수 없는 경우를 의미한다.

1차적 목적과 2차적 목적이라는 정의는 타업체에 대한 개인정보의 위탁과는 근본적으로 다른 관점의 내용이며, 서비스 제공자 당사자라고 할지라도 통계 등의 목적으로 정보를 수집하는 경우는 2차적 목적이 될 수 있다.

나) 정보주체의 개인정보 통제방법 명시 필요

정보주체는 개인정보를 적절히 통제할 수 있어야 한다. 개인정보보호법 제4조 제2항에서는 '개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리가 있다'라고 명시되어 있다. 이는 정보주체가 자신의 개인정보 처리와 관련하여 가지는 기본적인 권리이다. 이러한 부분에 대해 지능형전력망 보호지침의 제28조 제1항에서는 '누구든지 자신의 의사에 반하여 자신의 지능형전력망 개인정보가 위법하게 침해되거나 공개되지 않을 권리를 가지며, 자신의 지능형전력망 개인정보를 자율적으로 통제할 수 있어야 한다.'라고 명시하고 있다. 그러나 이에 대해 구체적으로 어떤 방식으로 통제해야 하는지에 대해서는 명시되어 있지 않은 상태이다.

개인정보의 통제는 1차적 목적과 2차적 목적을 구분하여 통제에 대한 정책을 정할 필요가 있다. 2차적 목적에 대해서는 정보주체에 의한 더욱 세부적인 통제가 가능하여야 한다.

다) 익명화/집계 데이터 처리방법 명시 필요

개인정보보호법의 제3조 제4항에서는 '개인정보처리자는 개인정보의 처리방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다'라고 명시되어 있으며, 제7항에서는 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다'라고 명시하고 있다.

따라서, 개인정보에 대한 익명처리가 가능한 경우에는 익명성을 유지하여야 한다. 특히, 통계를 위한 집계 데이터는 반드시 익명화가 필요하다. 집계 데이터는 일종의 데이터의 집합이며, 여기에는 특정 개인을 식별할 수 있는 개인정보가 포함되어서는 안된다. 만약, 반드시 필요한 경우는 개인정보에 대한 익명화가 필요하다. 여기에서 중요한 것은 익명화한 데이터는 알려진 방법으로는 원 데이터를 추정하기는 매우 어려운 방식이 되어야 한다는 것이다.

지능형전력망 보호지침의 제32조 제2항에서는 '통계작성·학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여

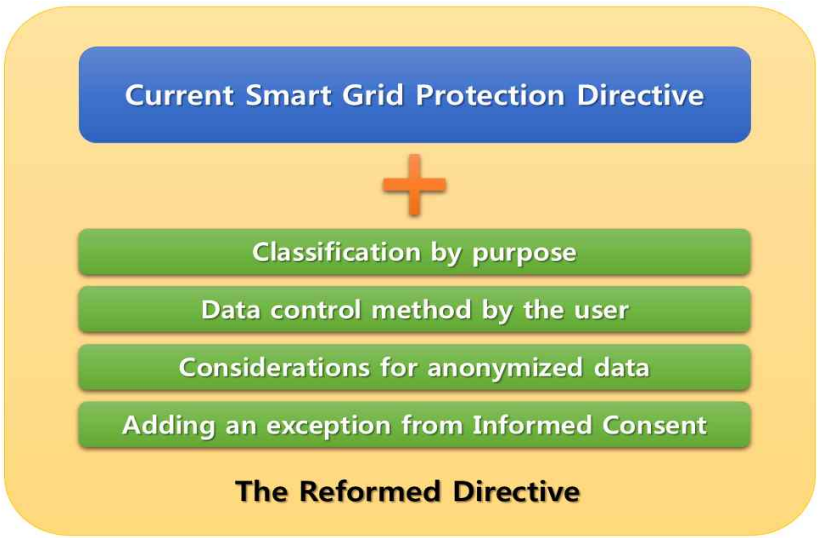
제공하는 경우'에 한해서 정보제공이 가능하다고 명시하고 있으나, 이러한 익명화 및 집계시에 대해서 구체적인 사항을 명시하지는 않고 있다. 스마트그리드의 특성상 개인정보와 에너지 사용 관련 데이터가 매핑되어 있으며, 이러한 데이터에 대한 통계를 위한 집계작업이 여러 상황에서 이루어질 것이다. 따라서, 통계를 위한 집계시, 그리고 데이터의 익명화시에 유의해야 할 사항에 대해 더욱 구체적으로 명시할 필요가 있다.

라) 사전 동의 예외사항 보완 필요성

지능형전력망 보호법의 제32조 제1항에서는 지능형전력망 사업자가 개인정보를 제30조에 따른 고지의 범위 또는 이용약관에 명시한 범위를 넘어 이양하거나 제3자에 제공하는 것은 불가함을 명시하고 있으나, 이에 대한 예외상황을 별도로 두고 있다. 여기에는 다음과 같은 3가지의 항목이 있다. 첫째, 서비스 제공에 따른 요금정산에 필요한 경우, 둘째, 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우, 셋째, 법률에 특별한 규정이 있는 경우로 한정하고 있다.

스마트그리드 시스템의 특성상 개인의 생명이나 재산에 대한 위협이 발생할 상황과 연계될 수 있다. 예를 들어, 보일러의 작동에 심각한 이상이 발생한 경우라던가, 화재경보기에 이상이 감지된 경우 등을 들 수 있다. 이러한 경우는 개인의 생명 및 재산에 치명적인 손실이 발생할 수 있으므로, 고객의 집 주소나 연락처와 같은 개인정보를 우선적으로 제공하여야 할 필요가 있다. 따라서, 예외사항 항목에 이러한 부분이 명시되어야 할 것이다. 개인정보보호법 제18조 제2항 3호에 따르면 개인정보처리자는 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 의하여 필요하다고 인정되는 경우에는 개인정보를 목적외의 용도로 사용하거나 이를 제3자에게 제공할 수 있도록 명시되어 있다.

⑤ 지능형 전력망 보호지침 개선방향



<그림 II-8> 지능형 전력망 보호지침 개선방향 개요

지능형 감시환경에서 주요한 이슈는 전력 데이터 감시 시스템이다. 스마트시티 환경에서 최소한의 필요한 전력 데이터 감시 이외에 불법적인 정보수집을 할 수 없도록 지능형 전력망 보호지침의 수정이 필요하다. 앞서 지능형전력망 보호지침에 대한 한계점을 제시하였다. 본 장에서는 앞서 분석한 한계점을 바탕으로 지능형전력망 보호지침을 개선(안)을 제시한다.

가) 목적에 따른 구분

앞서 언급하였듯, 본 논문에서는 정보이용의 목적에 따라 통제권한을 구분하고자 하며, 이를 위해 먼저 1차적 목적과 2차적 목적에 따른 정의를 명확하게 구분해야 할 필요가 있다. '1차적 목적'이라 함은, 이용자가 충분히 예상할 수 있는 경우를 의미한다. 즉, 이용자가 서비스 제공을 받고자 할 경우에 서비스 공급자 측에서 서비스 제공을 위해 개인정보를 어떤 경우에 이용할지에 대한 예측이 이용자 측면에서 가능한 경우를 말한다. 한편, '2차적 목적'이라 함은 고객의 예측이 어려운 경우를 의미한다. 즉, 이용자 측면에서 서비스 제공과 밀접히 관련이 있어 보이지 않는 경우를 말하며, 예를 들어 서비스 공급자의 통계적 목적으로 활용될 경우가 여기에 해당한다.

개인정보에 대한 사용의 목적을 구분하기 위해, 현행의 제2조에의 각 호에 덧붙여 1차적 목적과 2차적 목적의 용어 정의를 아래와 같이 추가하여 제시한다.

◉ 제2조 (정의) 현행과 동일

◉ ((1~15) 각 호 현행과 동일)

◉ 16. “1차적 목적”이란 고객이 주도한 서비스 제공 또는 합당한 사유가 있는 고객 관리를 위하여 개인정보 및 이용자의 에너지 사용 데이터를 사용할 것이 예상 가능한 경우를 말한다.

◉ 17. “2차적 목적”이란 서비스 제공자나 위탁업체가 고객에게 제공한 거래 및 기존 서비스와 관련하여 개인정보의 제공을 고객이 예측 가능하지 않은 경우를 말한다.

나) 고객의 데이터 통제권한 부여

개인정보보호법에 따라, 이용자는 자신의 개인정보에 대한 적절한 통제 권한을 가지며 이러한 통제 권한을 충분히 행사할 수 있어야 한다. 정보의 통제권한은 1차적 목적과 2차적 목적에 따라 구분될 것이며, 2차적 목적의 경우에는 보다 자세하게 명시될 필요가 있다.

현행의 지능형전력망 보호지침에는 그러한 부분에 대해서는 별도로 구분짓고 있지 않다. 따라서 본 논문에서는 이용자가 데이터 통제권한을 좀더 많은 부분에 한해서 행사할 수 있도록, 아래와 같이 2차적 목적의 경우에는 이용자 동의 프로세스를 통해 외부 업체에 의해서 이용자의 데이터 통제가 가능함을 제32조 4항 및 5항으로 추가하여 제시하고자 한다.

◉ 제32조 현행과 동일

◉ ((2~3) 각 항 현행과 동일)

◉ ④ 이용자는 자신의 데이터에 관한 일정 수준의 통제 권한 행사가 가능해야 한다.

◉ ⑤ 2차적 목적의 경우 이용자는 다음 각 호의 사항을 만족하는 이용자 동의 프로세스를 통해 외부 업체에 의한 이용자 데이터를 통제할 수 있어야 한다.

◉ 1. 이용자가 자신의 데이터를 공유하는 것에 대한 선택을 할 수 있는 방법을 설명

◉ 2. 어떠한 항목의 이용자 데이터를 어떠한 목적으로 얼마의 기간동안 제3자와 공유할 것인지를 구체적으로 설명

◉ 3. 복수의 제3자에 대한 여러 가지 이용자 데이터 공개 유형을 이용자 스스로 지정이 가능해야 함

◉ 4. 이용자가 기존에 특정 제3자에게 허용하였던 공개 권한을 취소할 수 있어야 함

◉ 5. 데이터를 제3자와 공유하기 전 2차적 목적을 위한 이용자 데이터 공개에 관한 동의 여부를 구체적이고 확실하게 명시할 것

◉ 6. 허위 동의에 따른 공개로부터 고객을 충분히 보호해야 할 것

◉ 7. 이용자가 인증을 취소한 경우, 인증이 만료된 경우 또는 서비스를 중지한 경우는 공개를 중지할 것

다) 익명화/집계 데이터 처리방법 명시

개인정보의 익명화가 가능한 경우에는 익명화 처리될 필요가 있다. 특히 통계를 위한 데이터 집계시에는 반드시 익명화가 필요하다. 또한, 이러한 익명화한 데이터는 알려진 방법으로는 정보주체인 이용자를 식별할 수가 없어야 한다. 이러한 익명화 및 집계 데이터를 처리하는 상황과 집계시 고려해야 할 사항에 대하여 현행의 지능형전력망 보호지침에는 특별히 규정된 부분은 없는 상태로, 이러한 세부적인 규정에 대해서는 별도의 조항이 필요해 보인다.

제안하는 개선안에서는 데이터의 집계·익명화시의 고려사항과 집계·익명화 데이터의 이용시의 지침을 제43조로 추가하여 별도의 조항으로 규정하는 것을 제안한다.

◉ 제43조 (데이터의 집계·익명화) ① 집계 데이터에는 개별 이용자의 개인정보는 포함하지 않아야 한다.

◉ ② 이용자의 재식별 가능성을 줄이기 위하여 집계 데이터에는 상당수의 이용자가 포함되어야 한다.

◉ ③ 단일 집계 데이터에 여러 이용자 등급이 존재할 경우, 등급간 에너지 사용 패턴의 차이를 고려해야 한다.

◉ ④ 익명화 데이터에는 개별 이용자의 개인정보는 포함하지 않아야 한다.

◉ ⑤ 특정 이용자의 부하 상황 및 에너지 사용 패턴이 특이하여 다른 이용자와 뚜렷하게 구별이 되는 경우는 삭제해야 한다.

◉ ⑥ 동일한 데이터 세트에 여러 분야의 이용자가 있는 경우 개별 이용자의 익명성이 떨어질 수 있으므로 그룹별로 구분해야 한다.

◉ 제44조 (집계·익명화 데이터의 이용) ① 집계·익명화 데이터는 서비스 제공자와 제3자간 계약을 통해 공유할 수 있다.

◉ ② 제1항의 경우 제3자는 이용자를 재식별하는 시도를 해서는 아니된다.

◉ ③ 집계·익명화된 경우라도 알려진 방법으로 서비스 제공자의 개인정보 식별이 가능한 경우에는 이용 및 배포할 수 없다.

라) 사전 동의 예외사항 추가

현행 지능형전력망보호지침에는 정보이용시 사전동의 예외사항에 대한 규정이 있다. 예외사항에 해당하는 내용은 첫째, 서비스 제공에 따른 요금정산에 필요한 경우, 둘째, 통계작성 및 학술연구 또는 시장조사를 위하여 필요한 경우, 셋째, 법률에 특별한 규정이 있을 경우로 규정되어 있다. 본 논문에서는 이에 한가지의 예외상황을 더 고려하고자 한다.

스마트그리드 환경의 특징에 따라, 물리적인 손실이나 이용자에 대한 직접적인 피해가 발생할 수 있는 여지가 있다. 즉, 전기보일러의 오작동이나 누전으로 인한 화재 등 여러 가지 상황으로 인해 이용자의 재산에 대한 큰 손해, 혹은 이용자의 생명에 대한 위급한 비상상황이 발생할 가능성도 염두에 두어야 한다. 본 논문에서는 이러한 경우를 충분히 고려하여 아래와 같이 제32조에 생명 및 재산 피해에 대한 사전동의 예외사항을 추가하는 것을 제안한다.

◉ 제32조 현행과 동일

◉ 제1항 현행과 동일

◉ ((1~3) 각 호 현행과 동일)

◉ 4. 서비스 제공자 또는 제3자가 이용자의 생명이나 재산에 대한 피해가 임

박한 비상 상황에 대처할 경우

◉ ((2~3) 각 항 현행과 동일)

◉ ((4~5) 각 항 개정(안)과 동일)

2) 국외 관련 가이드라인 현황

(1) 개요

IoT는 최근들어 가장 큰 이슈로 부상하고 있다. IoT는 사람과 사람 또는 사람과 사물을 연결하는 기술이며, 현실세계와 인터넷이 연결되어 다양한 서비스를 제공받을 수 있음에 따라 생활에 편리함을 가져다 준다. 따라서 IoT는 미래의 경제성장동력으로 부상하고 있으며, 전 세계적으로 이에 대한 대책을 세우고 있는 상황이다. 미국은 IoT를 국가 R&D 우선과제로 지정하고 차세대 IoT 과학기술 공학분야에 150개의 프로젝트에 대한 연구투자를 지원하고 있다. 또한, EU는 IoT의 활성화를 위해 기본적으로 추진할 실행과제인 'IoT 액션플랜'을 수립한 바 있다. 본 항에서는 이러한 IoT 보안분야에 대한 제도적 동향에 대해 살펴본다.

(2) GSMA IoT 보안 가이드라인

① GSMA IoT 보안 가이드라인 개요

IoT(Intetnet of Things)의 출현으로 새롭고 혁신적인 커넥티드 제품 및 서비스를 개발 가능하게 되었다. 전문가들은 향후 수십년에 걸쳐 IoT 서비스의 개수가 급증하고, 이에 따라 다양한 새로운 IoT 장치를 연결하게 될 것이라고 예측하고 있다. 이러한 사물인터넷의 급속한 성장은 새로운 생태계의 모든 구성원에 신규 서비스 제공을 확대하고 고객 기반을 늘릴 수 있는 중요한 토대를 마련하게 될 것이다. 그러나, IoT 서비스에서는 보안 위협이 큰 장애가 될 것으로 예측되며, 특히 다양한 IoT 서비스에 광역 연결을 제공하면 전체 IoT 생태계가 보안 공격에 노출될 수도 있어 위험성이 크게 확대될 수 있다. 이미 현재까지도 IoT

제품의 해킹사례가 다수 존재하고 있는 상황으로, 이에 대한 대책이 시급한 상황이다. IoT 서비스 제공 업체는 특정 신규 시장 부문에 대해 새로운 형태의 서비스를 개발하게 될 것이며, 이 과정에서 서비스가 직면할 위협에 대해 미처 파악하지 못하게 될 수 있다. 이러한 위협요소는 악의를 가진 해커에 의해 악용될 수 있다는 문제가 존재한다.

자동차, 의료, 가전제품 등 여러 분야에서의 서비스 제공 업체는 특정 보안 요구사항이 시장에 고유한 것으로 간주할 수 있으나, 일반적으로는 그렇지 않은 경우가 많다. 거의 모든 IoT 서비스는 다른 통신, 컴퓨팅 및 IT 솔루션과 유사한 기술을 포함하는 엔드포인트 장치 및 서비스 플랫폼 구성 요소를 사용하여 구축되므로, 서로 다른 서비스가 직면하는 위협과 해결방안은 일반적으로 유사하다는 특성이 있다.

따라서, 서비스별 공통적으로 적용이 가능한 가이드라인이 필요하며, GSMA에서는 이러한 IoT 서비스를 개발하고자 하는 서비스 제공 업체를 위하여 보안 가이드라인을 수립하였다. 이는 'GSMA IoT Security Guidelines'라는 제목으로 발표되었다. 해당 가이드라인은 IoT 서비스와 결합된 개인정보보호문제와 현재 우려가 되는 사이버 보안 문제에 적극적으로 대응하기 위한 실제적인 방안을 제공하고 있다.

② 가이드라인의 대상 및 구성

IGSMA의 IoT 가이드라인은 다음과 같은 대상자를 기준으로 작성되었다.

가) IoT 서비스 제공자 : 신규 IoT 서비스를 개발 예정인 기업/조직

나) IoT 기기 제조자 : IoT 기기를 제공하는 제조자

다) IoT 개발자 : IoT 서비스 제공자를 위한 서비스의 대행 개발자

라) 네트워크 통신 사업자 : IoT 서비스 제공을 위한 통신 서비스를 제공하는 사업자

<그림 II-9> GSMA의 IoT 보안 가이드라인(GSMA, 2016)

GSMA IoT 보안 가이드라인은 다음과 같이 네가지 부분으로 구성되어 있다.

가) CLP.11 : IoT 기술 및 서비스의 개발자에게 안전한 제품을 개발하기 위한 설계 가이드

나) CLP.12 : IoT 제품 또는 서비스의 모든 구성요소를 평가하기 위한 가이드라인

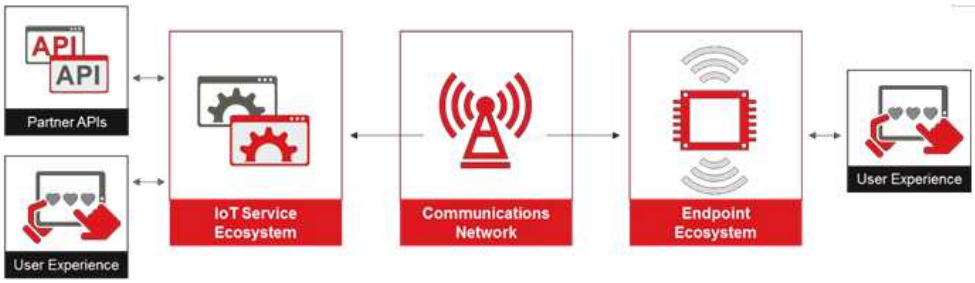
다) CLP.13 : IoT Endpoint 기기 관점에서 서비스의 구성요소를 평가하기 위한 가이드라인

라) CLP.14 : IoT 네트워크 사업자를 위한 시스템 및 데이터 프라이버시 보안 가이드라인

GSMA의 IoT 보안 가이드라인은 안전한 제품을 구축하기 위한 일련의 설계 지침을 IoT 제조사, 사업자 및 서비스 개발자에게 제공하는 것을 목표로 한다. 또한, 해당 문서는 새로운 IoT 사양이나 표준을 만드는 것을 목표로 하는 것은 아니며, 현재 사용 가능한 솔루션, 표준, 및 모범 사례를 참조하고 있다.

③ IoT 모델

아래 그림은 표준 IoT 모델이 서비스 및 종점 생태계의 구성 요소로 표시되어 있음을 보여준다. 각 구성 요소는 하위 구성 요소로 구성되며, 주 구성 요소에 각각 초점을 맞추어 개별적으로 문서가 작성되어 있다. 예를 들어, 엔드포인트 구성요소 및 해당 위험요소는 GSMA IoT 가이드라인에 제공된 Endpoint Ecosystem 문서에서 자세하게 언급하고 있으며, 서비스 구성요소는 Service Ecosystem 문서에 요약되어 있다.



<그림 II-10> GSMA의 IoT 모델

아래 그림은 대부분의 최신 IoT 서비스 또는 제품 모델에서 생산 준비가 된 기술을 배포할 대 필요한 기본 구성 요소를 정의하고 있다. 통신 네트워크 구성 요소는 IoT에 내재되어 있으며, 이 모델의 목적을 위해 IoT Service Ecosystem과 Ecopoint Ecosystem은 통신 링크의 끝부분과 연결되어 있다.

가) 서비스 생태계(Iot Service Ecosystem)

서비스 생태계는 기능을 저장하고 현장에 배포된 끝점에서 데이터를 수집하는데 필요한 일련의 서비스 플랫폼, 프로토콜, 기타 기술을 나타낸다. 이 생태계는 일반적으로 종점에서 데이터를 수집하여 서버 환경에 저장한다. 이 데이터는 일반적으로 메트릭, 매개변수 또는 명령 형태이며, 서비스 인프라에서 시작된 API를 통해 권한이 부여된 제3자에게 전달될 수 있다. 이는 일반적으로 IoT 서비스 제공 업체가 서비스에서 수익을 창출하는 방식이다. 해당 서비스 생태계 보안 지침은 앞서 1장에서 언급한 CLP.12에 상세히 설명하고 있다.

나) 엔드포인트 생태계(Endpoint Ecosystem)

엔드포인트 생태계는 여러 유형의 유선 및 무선 네트워크를 통해 물리적 세계와 디지털 세계를 연결하는 복잡성이 낮은 장치, 혹은 높은 장치 및 게이트웨이로 구성된다. 일반적인 종단점의 예로 모션 센서, 디지털 도어록, 자동차 텔레매틱스 시스템, 센서 구동 산업용 제어시스템 등이 있다. 엔드포인트는 주변의 물리적 환경에서 메트릭을 수집하고 네트워크를 통해 다양한 형식의 데이터를 에

코시스템에 푸시하여 응답을 받는다. 또한, 엔드포인트 자체 또는 서비스 에코시스템을 통해 얻은 데이터를 렌더링하는 풍부한 사용자 인터페이스를 포함할 수 있다. 엔드포인트 생태계 보안 지침은 CLP.13에서 상세히 설명하고 있다.

다) 위험 평가

위험 평가의 개념은 수십년 전부터 있어 왔으나, 많은 기업들은 정보보안보다는 일반적인 비즈니스 위험에 개념을 적용하는 것에 더 익숙한 편이다. 그러나, 정보보안 위험 평가 프로세스는 비즈니스의 기술적 측면의 안전한 운영과 수명을 위해 필수적이다. 특히, 비즈니스 성공에 주요한 요소가 될 수 있는 IoT 기술에서는 위험평가 프로세스가 매우 중요하게 작용한다. 위험평가 프로세스에 있어, 출발점이 될 수 있는 부분은 아래와 같다.

- 어떤 자산 (디지털 또는 물리적)을 보호해야 하는지 여부
- 어떤 유형의 사람들 (유형 또는 무형)이 잠재적인 위협 행위자인지 여부
- 조직에 대한 위협은 무엇인지 여부
- 취약점이 무엇인지 여부
- 보호된 자산이 훼손될 경우, 결과는 어떻게 되는지 여부
- 자산이 손상될 확률은 얼마인지 여부
- 다른 그룹의 공격자와 함께 있는 상황일 때 어떠한 결과가 발생하는지 여부
- 조직 및 파트너에게 자산의 가치가 어떠한지 여부
- 자산이 손상되었을 때 안전에 미치는 영향은 무엇인지 여부
- 잠재적인 취약점을 수정하거나 완화하기 위해 수행할 수 있는 작업은 무엇인지 여부
- 보안 격차가 어떻게 모니터링 될 수 있는지 여부
- 어떤 위협을 해결할 수 없는지, 조직에 어떤 위협이 있는지 여부
- 사고 대응, 모니터링 및 위험 관리를 통해 어떤 예산을 적용해야 하는지 여부

이러한 출발점은 엔지니어링 및 정보기술 팀이 조직과 보다 효과적으로 협력하는데 도움이 된다. 이를 통하여 비즈니스의 기술 측면에서 비즈니스 책임자와 함께 위험, 가치 및 개선 계획에 동의하는지 확인할 수 있다. 팀이 서로 협력할

경우, 비즈니스에 대한 위험뿐만 아니라 자산의 가치에 대한 보다 현실적인 전망을 창출하는데 도움이 된다.

위험 평가의 목표는 조직의 기술 부분에서 발견되는 보안상의 결함을 수정, 모니터링 및 대응하는 일련의 정책, 절차 및 제어 부분을 생성하거나 수정하는 것이다. 위험 평가 결과는 비즈니스가 기술 뿐 아니라 기술을 관리, 설계 및 배포하는 방법을 조정하는 데 도움이 된다. 위험 평가 결과가 조직에서 사용하는 정보 및 자원의 가치를 보다 적절하게 설명하면 직원, 프로세스 및 정책의 향상을 통해 전반적인 비즈니스를 확보할 수 있다.

위험 평가의 산출물을 사용할 때, 일반적으로 직원 인식 강화, 프로세스 강화, 정책 정의 도는 수정, 새로운 보안 격차 모니터링, 제품 또는 서비스의 질 향상이라는 이점이 있다.

④ GSMA 가이드라인 적용절차

일반적으로 보안성을 가장 용이하게 구현 가능한 시점은 엔지니어링 프로젝트가 시작되는 시점이다. 그러나 GSMA의 IoT 보안 가이드라인은 IoT 제품이나 서비스를 이미 설계, 제작, 배포된 조직에도 적용이 가능하다. 즉, 제품이나 서비스의 현재 상태가 어떤지에 무관하게 다음과 같은 다섯단계를 통하여 적용이 가능하다.

가) 기술 모델 평가

프로세스의 첫번째 단계로서, 조직의 자체 IoT 제품 또는 서비스를 이해하는 것이다. 보안 검토 및 위험 평가를 수행하려면 조직의 솔루션에 사용된 각 구성요소, 구성 요소 상호 작용 방법 및 구성요소가 환경과 상호 작용하는 방식을 잘 이해하고 있어야 한다. 제품이나 서비스에 대한 명확한 이해가 없다면 불완전한 검토를 하게 될 것이다.

먼저, 시스템에서 사용되는 각 구성요소를 설명하는 문서를 작성한다. 구성요소의 소스, 사용 방법, 필요한 권한 수준 및 전체 솔루션에 통합되는 방법을 식별한다. 또한, 각 구성요소를 각 종단 시스템 및 서비스 에코 시스템을 CLP.12,

CLP.13에 나타난 모델을 기반으로 매핑한다. 또한, 다음 사항에 대하여 고려한다.

- 어떤 구성 요소가 제품 또는 서비스를 구축하는데 사용되는지 여부
- 주어진 구성 요소에 적용할 수 있는 입력 및 출력은 무엇인지 여부
- 이러한 입력 및 출력에 이미 적용된 보안 컨트롤이 무엇인지 여부
- 구성 요소에 적용되는 권한 수준이 무엇인지 여부
- 조직의 누군가가 구성요소를 구현할 책임이 있는지 여부
- 조직의 누군가가 구성요소 모니터링 및 관리를 담당하는지 여부
- 구성요소에서 관찰된 위험을 수정하기 위해 어떤 프로세스가 마련되어 있는지 여부

이러한 사항을 확인하면 기술 구성 요소가 어떻게 상호 작용하는지 여부와 전체 구성 요소 또는 서비스가 각 구성 요소의 영향을 받는 방식을 이해할 수 있다. 이는 각 중요 비즈니스 자산에 대한 프로파일 개발, 보안 목적 개발을 지원하고 회사가 위험을 평가, 모니터링 및 대응하는 방법에 대한 토대를 마련한다.

나) 현재 제품 또는 서비스의 보안 모델 검토

여기서는 엔드포인트와 서비스의 보안 모델을 검토한다. 보안 모델이 검토되면, 개발중인 제품 또는 서비스에서 공격자가 가장 취약하거나, 가장 선호하는 기술을 잘 이해해야 한다. 이 정보는 엔지니어와 리더 모두 현재 모델에 대한 위협요소를 이해할 수 있도록 서로 공유할 필요가 있다. 그러나 이 시점에서 보안 모델을 조정하기 위한 특별한 조치를 취하지는 않아도 된다. 아키텍쳐를 변경하기에는 너무 이른 시점이기 때문이다. 이 과정에서는 잠재적인 보안 차이를 식별하고 이에 대한 우선 순위를 지정하며, 기술 모델을 향상시키는데 도움을 준다.

다) 권장 사항 검토 및 평가

여기서는 각 모델별 권장사항 부분을 검토하여, 보안 문제를 어떤 방식으로 해결하는지를 평가해야 한다. 여기서는 권장사항을 구현하기 위한 방법론을 제공할 뿐만 아니라 특정 권장 사항 구현과 관련된 문제를 파악할 수 있다. 각 권장사항 부분에는 방법에 대한 부분도 가지고 있으며, 이는 해당 보안 위험 요소를

수정하거나 완화하는데 도움이 되는 방법론을 제공한다.

라) 구현 및 검토

이 단계에서 명확한 보안 작업에 대한 윤곽이 나타나며, 비즈니스상 보안 취약점에 대해 더 잘 이해하게 된다. 현재 수정중인 각 구성요소에 대한 명확한 아키텍쳐 모델을 만들고 조직이 선택한 위험 평가 프로세스를 사용하여 각 구성요소 및 보안 작업에 적합한 권장 사항과 위험 요소를 통합하여 각 구성 요소의 위협 모델을 개발해야 한다. 아키텍쳐 모델이 완료되면 조직은 보안 태스크를 수행하기 위해 각 권장사항을 구현할 수 있다.

권장사항에 대한 구현이 완료되면 조직은 권고 하위 섹션과 구성요소 섹션 모두에서 위협을 검토해야 한다. 조직은 구성요소가 조직의 제품 또는 서비스에서 보안 문제를 해결할 수 있도록 보장해야 한다. 가능한 경우 트사 컨설팅 회사에 의뢰를 요청할 수도 있다.

마) 지속적 라이프사이클

보안 수명주기는 이 시점에서 중단되지 않는다. 종단점 및 IoT 서비스는 마치 살아있는 유기체와 같으며, 수명이 다할 때 까지 지속적인 서비스가 필요하다.

보안 요구사항은 시간이 지남에 따라 변경될 수 있다. 예를 들어 암호화 알고리즘은 시간이 지남에 영향을 받는다. 또한, 새로운 프로토콜 및 무선 기술도 제품 또는 서비스와 지속적인 상호운용이 필요하다. 기밀성, 무결성, 가용성 및 신뢰성이 유지될 수 있도록 제품이 배포된 이후에도 끊임없이 지속적인 관리가 필요하다.

⑤ GSMA 가이드라인의 적용 사례

여기에서는 자동차 추적 시스템이 GSMA 가이드라인을 사용하여 평가된다. 엔드포인트는 CLP.13문서를 사용하여 평가되며, 서비스 측면은 CLP.12문서를 사용하여 평가된다.

가) 기술 모델 평가

기술모델 평가 단계에서 엔지니어링 팀은 제품의 아키텍쳐에 따라 장치가 어떻게 작동하는지 평가한다. 엔지니어링 팀은 인력 구성, 보안 작업 할당 및 진행 상황 추적을 위해 솔루션에 사용된 기술을 항목별로 정리한 문서를 만든다. 이 예에서는 자동차 추적 시스템이 다음과 같은 기능이 있다고 가정한다.

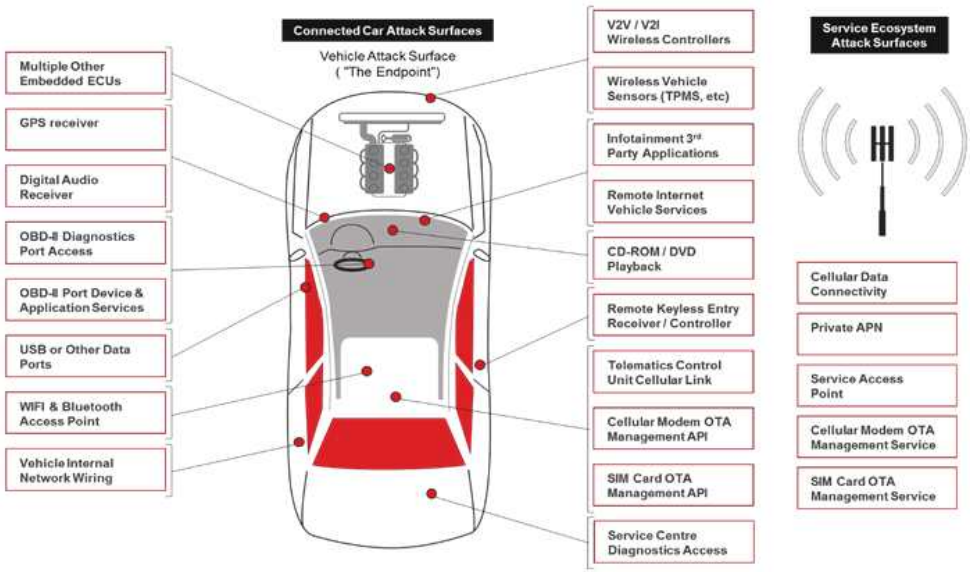
- 엔드포인트 : 그래픽 사용자 인터페이스(GUI), 셀룰러 모듈, SIM카드, 리튬 폴리머 배터리, CPU, 비휘발성 응용프로그램, RAM, EEPROM

- 서비스 : 셀룰러 데이터 연결성, 보안 개인 APN, 서비스 엑세스 포인트, 셀룰러 모뎀 OTA 관리 서비스, SIM카드 OTA 관리 서비스

각 기술과 관련된 정보를 표시한 후 팀은 각 가이드라인 문서의 모델 부분을 검토하고 적절한 기술 모델을 식별한다.

나) 보안 모델 검토

기술모델이 요약되면 보안모델을 검토해야 한다. 보안모델에서 팀은 공격자가 솔루션을 공격하는 방법을 평가한다. 예제에서는, 아래와 같이 공격 포인트가 셀룰러 네트워크와 차량에 특화된 공격의 두 가지 존재한다.



<그림 II-11> 커넥티드 자동차에 대한 공격 포인트

로컬 네트워크 연결이 없이 모바일 네트워크 연결만 수행되므로 공격자는 셀룰러 네트워크 연결을 손상하거나 개인 APN에서 통신 채널을 입력하거나 서비스 엑세스 포인트, 셀룰러 모뎀 OTA 관리 서버 또는 SIM 카드를 통해 진입해야 한다. 또한, 아래 그림과 같이 엔드포인트에는 여러 개의 진입점이 있으므로 주의하여야 한다.

다) 권장 사항 검토 및 평가

평가된 보안 모델을 기반으로 보안 작업을 할당해야 한다. 각 팀은 평가가 필요한 솔루션의 각 구성 요소에 특정 사용자를 지정한다. 이는 상위 레벨의 관점(엔드포인트, 네트워크 및 서비스)뿐만 아니라, 하위 구성 요소 관점에서도 평가되어야 한다. 예를들어, CPU에는 worker, 운영체제, 네트워크 서비스 등이 할당되어야 한다.

팀의 각 구성원은 최대한 많은 권장사항을 읽고 이해해야 하며, 특히 엔지니어는 구성요소가 전체 보안에 미치는 영향에 대하여 잘 파악할 수 있어야 한다. 이후, 구성요소 소유자는 권장사항이 이미 적용되었는지 여부를 결정하거나 보류중인 권장사항을 표시할 수 있다.

권장사항 검토 및 평가 이후 다음과 같은 보안 격차가 확인되었다.

- 비밀이 EEPROM에 비보호로 저장되었다.
- 비밀이 내부 RAM에서 처리되지 않는다.
- 사용자 인터페이스는 암호로 보호되어야 한다.
- 사용자의 개인정보가 사용자에게 인지되어야 한다.

라) 구현 및 검토

이 단계에서 합의한 보안 요구사항을 준수하도록 솔루션을 조정할 수 있다. 필요한 경우 구성요소를 다시 구현하고 필요한 경우 보안 제어 기능을 추가한다. 예를 들어 EPROM은 보안키로 암호화된 데이터로 인코딩되고, 인터페이스 접근 시 비밀번호 입력이 지원되도록 변경한다.

구현 이후 모든 보안 권장사항 및 위험을 재평가하고, 보안 모델을 검토하여 문제점이 해결되었는지 여부를 확인한다.

(3) OWASP Internet of Things Project

OWASP(The Open Web Application Security Project)는 신뢰할 수 있는 응용프로그램의 개발 및 운영 등을 위해 활동하고 있는 국제 웹보안표준기구이다. The OWASP Internet of Things Project 는 OWASP의 프로젝트 중 하나이며, IoT 기술의 구축/전개/평가시 이용자의 보안 검토를 지원하는 것을 목적으로 활동하고 있다. OWASP에서 2014년에 정리한 'Top 10 IoT Vulnerabilities'는 IoT에서 취약점을 발생하기 쉬운 10가지 포인트를 정리하고, 공격자 공격 방법, 보안 취약점, 기술적 영향, 비즈니스에 미치는 영향이 구체적으로 무엇인지 상세하게 정의하고 있다. 여기에는 취약점, 공격 등에 대하여 실례를 들어 설명하고, 문제를 해결하기 위한 지침을 기술하고 있다.

세부 내용은 아래 표와 같으며, 웹 인터페이스의 불안전성, 불충분한 인증 및 권한 등 IoT 환경에서 발생할 수 있는 10가지의 보안 취약점을 구체적으로 명시하고 있다.

<표 II-1> IoT 10대 보안 취약요소

일련번호	세부 내용	난이도	영향도
2014-I1	안전하지 않은 웹 인터페이스	하	상
2014-I2	불충분한 인증 및 권한	중	상
2014-I3	안전하지 않은 네트워크 서비스	중	중
2014-I4	암호화 및 무결성 검증의 소홀	중	상
2014-I5	개인 정보 보호 우려	중	상
2014-I6	안전하지 않은 클라우드 인터페이스	중	상
2014-I7	안전하지 않은 모바일 인터페이스	중	상
2014-I8	불충분한 보안 설정	중	중
2014-I9	안전하지 않은 소프트웨어/펌웨어	상	상
2014-I10	빈약한 물리적 보안	중	상

(4) OTA IoT Trust Framework

Online Trust Alliance(OTA)는 인터넷의 혁신과 활력을 촉진하는 미국 국내 세입법 제 501C항 3호에 근거하는 비영리 단체이다. OTA는 온라인의 신뢰성을 강화하는 것을 목적으로 Symmantec, Verisign 등 100개 이상의 조직이 가입하고 있다. 산하 워킹 그룹인 IoT Trustworthy Working Group(ITWG)는 'OTA IoT Trust Framework'를 개발/공개하였다. 이는 1) 홈오토메이션 및 홈네트워크 제품, 2) 건강 및 피트니스 분야용 웨어러블 기술에 초점을 둔 검토를 실시하였으며, 2016년 3월 3일 공개된 정식버전 (Released 3/2/2016)에서는 30개의 필수 및 권장사항을 규정하고 있다.

- 장비는 일반적으로 인정된 보안 통신 프로토콜을 지원해야 한다.
- 장비는 일반적으로 인정된 보안 통신 프로토콜을 지원해야 한다.
- 모든 인증정보는 salt를 이용한 해쉬와 암호화를 적용해야 한다.
- IoT를 지원하는 모든 웹사이트는 사용자 세션을 암호화해야 한다.
- 사이트의 보안 설정, 정기적인 모니터링 및 지속적인 개선이 필요하다.
- 취약점 보고를 관리하고 신속하게 대응하기 위한 시스템을 구축, 유지하여야 한다.
- 모든 소프트웨어 및 펌웨어 업데이트는 출처가 있어야 하며 보안/개인정보보호 설정을 변경해서는 안된다.
- 타사/오픈 소스 소프트웨어 인벤토리를 관리해야 하며 표준화된 개발 라이프 사이클 프로세스를 따라야 한다.
- 최종 사용자 통신(이메일, SMS 등)에는 인증 프로토콜을 적용해야 한다.
- 인증 확인이 되지 않는 이메일은 거부하는 정책을 구현해야 한다.
- 이메일을 사용할 경우 이메일 보안 기술을 포함한 전송레벨의 보안을 도입해야 한다.
- 사용자 엑세스의 경우 일회성 비밀번호를 제공하거나, 다른 보안 인증 자격증명을 사용해야 한다.
- 비밀번호 복구기능을 제공하여야 하며, 암호가 없는 경우 다른 확인 방법(이

메일, 전화 등)을 이용할 수 있어야 한다.

- 잘못된 로그인 시도가 반복되면 사용자 계정 및 지원 계정 잠금이 필요하다.
- 암호 재설정 또는 변경 시 보안 인증의 실시를 해야 한다.
- 보안 침해를 받은 경우의 대응책 및 사용자 통지 계획을 수립해야 한다.
- 사용자가 개인정보보호 정책을 쉽게 찾을 수 있도록 해야 한다.
- 제품 보증 범위 이상의 보안 및 패치 지원의 실시 기간을 개시해야 한다.
- 정보의 수집은 서비스 제공에 필요한 항목으로 한정한다.
- 네트워크 연결이 두절된 경우 작동하지 않는 기능 및 잠재적 영향에 대해 공개한다.
- 데이터 보존 정책 및 개인정보의 보유 기간을 제시한다.
- 타 장치, 플랫폼, 서비스 간 페어링 연결 시 사용자에게 통보/승인 요청이 필요하다.
- IoT 제품 및 서비스의 소유권 이전이 가능해야 하며, 그 방법을 공개해야 한다.
- 제3자와의 개인정보 공유는 사용자의 동의를 얻은 경우에만 가능하다.
- 사용자가 IoT 기기의 개인정보 설정이 가능하도록 기능과 설명서를 제공한다.
- 사용자정보를 판매 및 양도하는 경우가 없음을 서약한다.
- 제품 반품 시 개인정보보호가 가능하도록 기능이 제공되어야 한다.
- 정책에 대한 거부 시 제품의 기능에 미치는 영향을 명확히 설명해야 한다.
- 최소 2년치의 개인정보보호 고지의 변경 이력을 공개한다.
- IoT 기기의 사용 중단, 분실, 재판매시 개인정보 및 민감정보를 삭제하거나 익명화할 수 있는 기능을 제공하여야 한다.
- 분실 또는 재판매의 경우 기기의 데이터 및 서비스 데이터를 삭제해야 한다.

3) 관리적 측면에서의 고려사항

(1) 개요

정보보호의 중요성은 아무리 강조해도 지나치지 않다. 지금까지 많은 정보보호 위협이 있어 왔으며, IoT 환경에서는 기존의 IT 환경에서 나타날 수 있는 위

협들이 그대로 적용되어 발생할 수 있다.

또한, IoT 환경에서는 기존의 보안 취약점 뿐만 아니라 새로운 다양한 보안 취약점이 등장 할 것으로 예상되고 있다. 즉, IoT 환경에서의 보안 사고는 기존보다 훨씬 크게 발생할 것으로 보인다. IoT 환경은 IT와 물리환경에 결합되어 있다는 특성이 있으며 이러한 점에서 보안 문제는 신체적, 물질적 위협과도 직결되는 부분이기 때문이다.

이와 같이 주요 IoT 분야(홈/가전, 의료, 교통, 에너지, 제조)별 다양한 보안 위협들이 대두되고 있으며, 지능형 감시 환경에서도 IoT 기반 영상기기에 대한 제품 및 서비스가 보안 위협에 사전에 대응할 수 있도록 적절한 사후관리 체계가 필요하다. IoT 제품 및 서비스는 생산·판매·개발 이후 유지보수, 보안 업데이트 적용 등 사후 보안조치가 어렵거나 고비용이 수반된다는 문제가 있으므로 제품 사후관리, 보안성 유지관리에 필요한 개발 및 운영단계 뿐만 아니라 사후관리에 대한 정책이 필요하다. 본 장에서는 IoT 영상기기 개발 및 운영 측면에서의 관리적 보안대책에 대하여 먼저 논의하고, IoT 기반 영상기기의 제품 출시 이후에 보안 문제가 발생하였을 경우를 대비한 제품 출시 사후 관리 방안에 대하여 제안한다.

(2) 영상기기 설계시의 고려사항

IoT 제품은 다른 IoT 제품 및 불특정 장비, 시스템에 연결되어도 보안이 유지되어야 하며, 이상이 발생하더라도 상대측에 피해가 없도록 설계되어야 한다. 여기서는 IoT 제품 설계시 고려해야 할 사항에 대하여 살펴본다.

① 내/외부 및 물리적 보안 위협요소

IoT 제품 및 시스템에서 발생 가능한 위협 요소로, 외부 인터페이스, 내부적 위협, 물리적 접촉에 의한 위협 등이 있다.

외부 인터페이스를 통한 위협요소는 DoS 바이러스 및 스푸핑 등의 공격, 다른 기기에서 정상적이지 않은 데이터를 보낸 경우 등이 있다. 내부적 위협 요소는 장비 및 시스템의 설계 및 사양, 설정 등에서 보안 문제가 존재할 수 있는 부분

이며, 구체적으로는 잠재적인 결함, 악성 코드 등을 꼽을 수 있다.

물리적 접촉에 의한 위험은 IoT 제품의 분해, 부품의 무단 교체 등이 해당될 수 있으며, 이러한 위험에 대한 대책이 고려되어야 한다.

② 비정상 감지시 대응

소프트웨어 및 하드웨어의 결함이나 공격 등에 의한 비정상적인 동작이 발생하면 영향의 파급을 방지하기 위해 먼저 비정상적인 상태를 감지할 수 있도록 할 필요가 있다. 또한, 비정상 상태가 감지된 경우, 다른 IoT 제품에도 영향을 미칠 수 있으며, 이를 방지하기 위해 해당 IoT 장치를 네트워크에서 분리 하는 등의 대책이 필요하다.

IoT 제품이 네트워크에서 분리 또는 기능 정지가 발생한 경우, 해당 IoT 장치를 이용하는 다른 IoT 대한 영향이 최소화되어야 한다.

③ 사용자 안전에 대한 고려

IoT의 특성상 보안 위협 요소가 신체적 안전에 대한 위협요소로도 작용할 수 있다. 예를 들어, IoT 장치 또는 유관 시스템에 공격자가 무단으로 소프트웨어 및 데이터 조작 등을 감행할 경우 오작동이 발생할 수 있으며, 이러한 공격은 보안위협 뿐만 아니라, 실제 사용자의 신체적인 위협, 즉 사고로도 이어질 수 있다. 따라서 이러한 부분이 반드시 고려되어 설계되어야 한다.

④ 기기 상호간 인증 및 권한 확인

IoT 제품에 신뢰할 수 없는 불특정 기기가 연결될 수 있다. 이러한 경우 개인정보가 쉽게 유출되거나 예상하지 않은 동작이 발생할 가능성이 있다. 한편, 동일한 모델의 제품이어도 차후에 출시된 모델과 버전차이로 인하여 연결이 정상적으로 수행되지 않는 경우도 발생한다. 따라서, 연결 시 비정상 여부 판단 및 상대측 기기의 권한 확인, 제공 기능과 정보의 범위를 조절하는 방법 등에 대한 부분도 고려되어야 한다.

⑤ 설계에 대한 검증/평가 실시

IoT 제품의 보안 설계가 정상적으로 되었는지에 대한 검증 및 평가 절차가 필요하다. 제품 자체는 단독으로는 문제가 없다고 할지라도, 실제 다른 IoT 장치 및 시스템과 연결될 경우 생각지 않은 위협이 발생할 수 있다. 따라서, IoT 특유의 리스크를 고려한 검증/평가 체계가 필요하다.

(2) 영상기기 개발 및 운영상의 고려사항

IoT CCTV의 보안성 관리 대책은 보안위협과 공격방법을 기반으로 검토되어질 필요가 있다. 그러나, 완벽하게 안전한 관리 대책이란 존재하기 어려우며, 여러 대책을 조합하여 보다 심층적인 측면에서의 대응이 바람직하다.

한편, 보안성 관리 대책의 적용에도 일부 어려운 측면은 존재한다. 예를 들어 자원, 비용, 사고 발생시의 영향도 등 여러 측면을 고려하여 대책을 수립할 필요가 있다.

① 개발 단계

가) 보안 모듈 및 시큐어 코딩 적용

취약점을 가진 IoT 제품이 시장에 출하되는 것을 방지하기 위해, 개발 단계에서 미리 다음과 같은 부분을 고려해야 한다.

먼저, 새로운 취약점이 발견될 수 있는 소프트웨어 또는 펌웨어의 개발에 보안 모듈이 적용되어 개발되어야 하고, 개발 시에 시큐어 코딩 기법을 활용하여야 한다.

나) 외부 소프트웨어 취약성 고려

외부의 소프트웨어(예를 들어, 오픈 소스 등)을 이용하는 경우, 알려진 취약점

이 존재하는지에 대한 확인이 필요하다. 특히, 오픈 소스 소프트웨어는 소스코드가 공개되어 있다는 특징을 가지고 있으므로, 취약점 문제가 공개되기 쉽다는 측면이 있다. 따라서, 외부 소프트웨어의 취약점 관리가 소홀할 경우 공격자의 공격 수단으로 악용될 위험이 크다.

특히, 공개된 샘플 소스코드를 그대로 가져와 개발한 제품의 경우, 취약점이 혼입된 사례도 존재하였다. 따라서, 샘플 코드는 반드시 취약점이 존재하지 않는 것을 확인한 후에 이용할 필요가 있다.

다) 하드웨어 취약요소 고려

하드웨어에서 발생할 수 있는 취약요소가 고려되어 한다. 예를 들어 IoT 제품에 대해 물리적 공격이나, 의도치 않은 하드웨어의 훼손 등 다양한 상황이 발생할 수 있으며, 이를 염두에 두고 설계 및 개발이 되어야 한다.

라) 충분한 테스트 실시

제품 출하 전에 알려진 취약점 검사, 소스코드 검사 등 각종 테스트를 실시하여야 한다. 여기에서 테스트는 여러 가지 측면에서 충분하게 실시되어야 하며, 만약 테스트 시 이상이 발견 될 경우는 반드시 출하시에 취약점을 모두 제거한 후 출하하도록 한다.

마) 취약점 업데이트 기능 제공

개발 단계에서 취약점을 완벽히 없애는 것이 현실적으로 쉬운 일은 아니며, 미처 파악하지 못한 취약점이 제품 출시 이후에 발생할 수도 있다. 또한, 제품 출하 시점에서 취약점으로 판단되지 않더라도, 향후 시간이 지나면 해당 부분이 취약점으로 지적될 수도 있다. (예를 들어, 암호화 알고리즘 및 키 길에 대한 부분) 따라서, 제품 출시 후 취약점의 발견에 대비하여 소프트웨어 및 펌웨어의 업데이트 기능을 구현할 필요가 있다.

② 운영 단계

가) 지속적인 취약점 정보 수집

제품 출시 이후에 신규 취약점이 발생하는 경우를 대비하여, 지속적으로 취약점 정보를 수집하여야 한다. 제품 개발에 이용한 외부의 소프트웨어에 대한 새로운 취약점 등 여러 발생 가능한 취약 요소에 대해 취약점 대책 정보를 수집하고 관리할 필요가 있다.

나) 취약점 발생시 대응방안 수립 통지

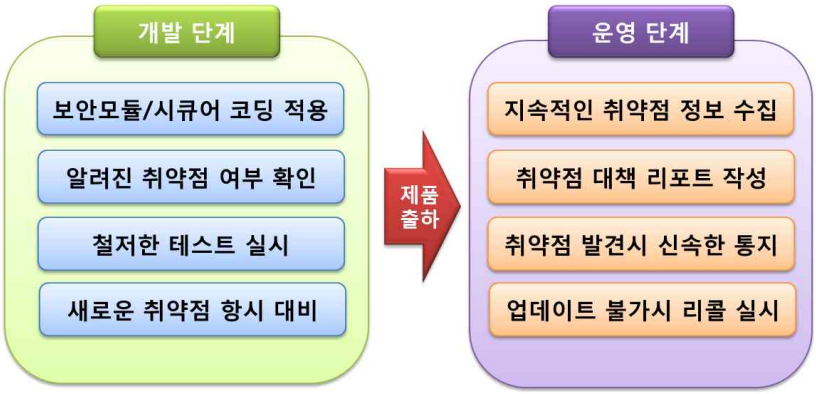
신규 취약점이 발생한 경우, 이에 대한 취약점 관련 정보를 신속히 수집하고 대응 메뉴얼을 작성하여야 한다. 여기에는 취약점의 개요, 심각도, 영향범위, 대책방안 등의 정보가 포함되어야 한다. 취약점 대응 매뉴얼이 작성되면, 신속히 관련자에게 전파하여야 한다.

다) 소프트웨어 업데이트 제공

소프트웨어 취약점의 경우 가장 일반적인 대책은 취약점을 해결한 업데이트 소프트웨어를 제공하고, 이용자에게 적용을 권고하는 것이다.

만약, 업데이트 소프트웨어의 제공에 일정 시간이 소요된다고 판단될 경우, 적절한 다른 방안을 고려해볼 필요가 있다.

정보기술에 익숙하지 않은 고연령층이 주 고객층인 제품 등 소프트웨어 업데이트 적용이 쉽지 않은 상황일 경우 원격 조작에 의해 자동으로 업데이트 소프트웨어를 적용하는 방법도 고려할 필요가 있다. 이러한 경우, 제품 출하시의 시점에서 제품의 자동 업데이트 기능에 대한 내용을 사전에 고지하여야 한다. 또한, 소프트웨어 업데이트를 통하여 제품이 가지는 기능이 변경될 경우, 자동 업데이트는 가급적 피하고 이용자의 동의를 거쳐 업데이트가 적용될 수 있도록 한다.



<그림 II-12> 개발 및 운영 단계에서의 관리적 보안대책

라) 업데이트 불가시 리콜 실시

소프트웨어 업데이트가 어려운 제품인 경우, 혹은 하드웨어상의 보안 취약점이 발견된 경우에는 즉각적인 리콜 실시가 필요하다. 이러한 경우, 제품을 일단 회수처리 한 후 차후 대책을 진행할 필요가 있다.

(3) 사후 보안관리 측면의 고려사항

① 사후 보안관리 개요

IoT 영상기기 제품 출하 이후의 신규 보안 취약점 발생 가능성은 항상 염두에 두어야 하며, 이는 취약점 여부를 지속적으로 모니터링하여 확인하여야 한다. 즉, 해커가 보안 취약점을 이용하여 악의적인 행위를 하기 이전에 미리 보안 취약점을 모니터링을 통하여 선발견하고, 선조치하는 체계가 필요하다.

또한, IoT 보안사고 발생시는 해당 침해사고의 심각성 및 영향도에 따라 책임부서를 명확히 하여야 한다. 즉, 제품의 위해성 분석을 통한 영향도 판단은 KISA의 인터넷 침해사고 대응지원센터(KrCERT)에서 진행하며, 해당 제품에 대한 상황 심각성이 경미할 경우는 제조사에 소프트웨어 업데이트를 통한 시정권고로 처리할 수 있으며, 개인정보 노출 등 심각한 보안 위협을 노출한 상황일 경우는 시정명령으로 처리한다. 한편, 소프트웨어의 즉각적인 업데이트가 어려우며, 기기 자체의 물리적인 오작동과 이를 기반한 사용자의 재산적/신체적 문제를 야

기하는 상황일 경우에는 한국제품안전협회로 이관하여 리콜 사건 접수로 처리한다. 한국제품안전협회에서는 제품에 대한 재산적/신체적 피해 영향도의 심각성에 따라, 리콜 권고 혹은 리콜 명령을 내릴 수 있다.

그리고 보안 결함 발생 시, 사용자가 제품 보안 결함 여부를 인지하지 못한 상태에서 해당 제품을 지속적으로 사용하게 될 수 있다. 따라서 사용자가 즉각 인지할 수 있는 체계를 확립하여야 한다.

한편, 소프트웨어 업데이트 시에 대한 보안 위협은 소프트웨어의 기술적 업데이트 체계를 확립한다. KrCERT에서는 소프트웨어 업데이트 파일의 적합성과 신뢰성 여부를 판단하여 IoT 기기에 소프트웨어 업데이트 적합 여부를 통지하여 소프트웨어 업데이트가 수행되도록 한다.

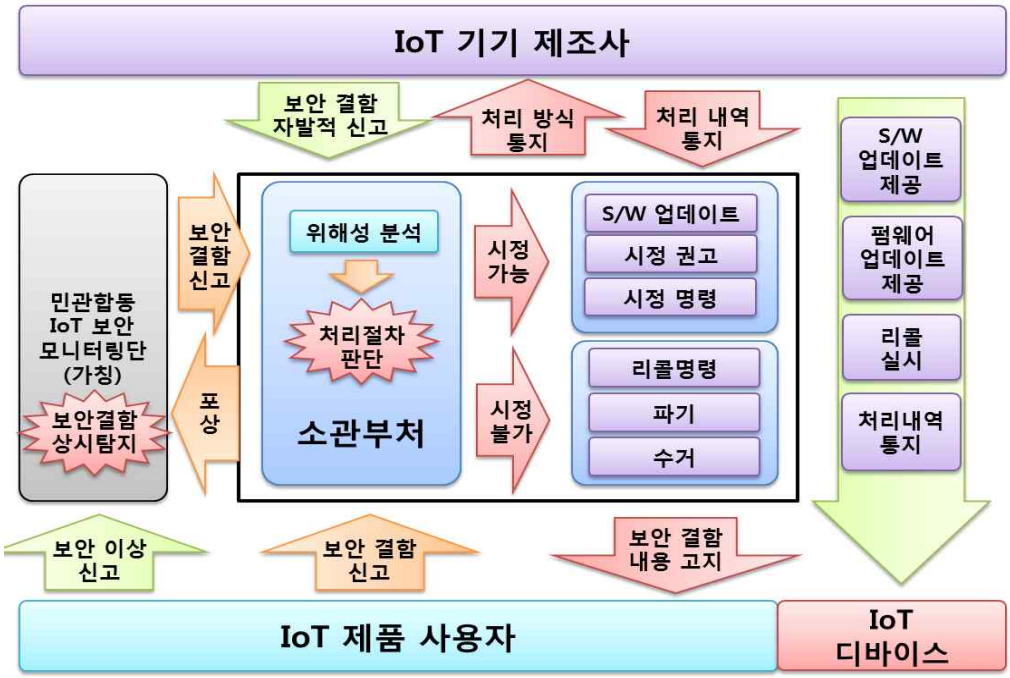
<표 II-2> 사후관리 보안위협과 대응방안

사후관리 보안위협	대응방안
출하 이후 신규 취약점 발생	취약점 여부를 모니터링 후 선조치 가능한 체계 확립
보안사고 발생시 책임부처의 모호성	보안 심각성 및 영향도에 따른 소관부처의 명확화
제품 보안 결함 인지체계 부재	보안 결함 발생시, 사용자가 인지 가능한 체계 확립
소프트웨어 업데이트 보안위협	소프트웨어 기술적 업데이트 체계 확립

② 사후 보안관리 방안

가) 사후 보안관리 개요

아래 그림은 본 논문에서 제안하고자 하는 IoT 보안에 대한 사후관리 프레임워크를 나타낸다. 여기에서는 IoT 제품 사용자, IoT 기기 제조사, 민관합동 IoT 보안 모니터링단이 유기적으로 상호작용하여 현행 IoT 제품의 보안 결함을 신고하고, 소관부처는 이를 접수하고 처리절차를 판단하여 이에 적합한 방식으로 처리한다. 처리방식은 상황의 심각성, 혹은 제품 업데이트 가능 및 즉시조치 가능 여부에 따라 소프트웨어 업데이트, 혹은 시정 권고/명령, 또는 리콜과 같은 방식이 될 수 있다.



<그림 II-13> IoT 영상기기 사후 보안관리 방안

나) 민관합동 IoT 보안 모니터링단

여기에서는 가칭 민관합동 IoT 보안 모니터링단의 구성을 제안하고자 하며, 이는 IoT 보안에 대한 분석 역량이 있는 모니터링 단원을 민관 합동으로 구성하여 IoT 보안 취약점을 상시로 분석하는 역할을 수행하게 한다. 민관 합동 모니터링단은 IoT 제품에 대한 다양한 경험과 IoT 보안 분야의 분석 능력이 있는 시민, IoT 보안의 전문 지식을 보유한 학계 전문가, IoT 해킹 분석 및 침해 대응 방안 능력이 있는 기업체 전문가, 관련 정부부처 및 담당기관으로 구성되며, 시민 측은 사용자 관점에서 제품의 결함 여부를 확인하며, 학계 및 기업체 전문가 측에서는 해당 사례에 대한 구체적인 결함 원인 및 영향 범위를 판단하는 역할을 수행한다. 정부 및 기관 모니터링단 위원은 주요 보안 결함 사례 분석을 위해 국가/공공기관에 업무 협조 요청을 수행한다.

만약, IoT 보안 결함이 발견되었을 경우 IoT 보안 모니터링단은 해당 소관부처에 결함 내용을 신고 처리한다. 이후 소관부처는 이를 접수하고, 보안 결함 여부 확인 후 포상을 통하여 IoT 보안 결함 의 신규 발견을 촉진시킨다.

다) IoT 영상기기 제조사

IoT 영상기기 제조사는 IoT 기기의 보안 결함 발생에 대한 책임을 갖는다. 품질 검수 시 보안 결함을 통과했다고 하더라도, 제품 출시 이후 알려지지 않았던 보안 문제가 얼마든지 발생할 수 있다. 따라서, 제조사는 자사의 제품에 해당 문제가 발견되면 소관부처에 자발적으로 신고하도록 한다. 이후, 해당 보안 취약점에 대한 소프트웨어 업데이트를 진행하여, 처리 완료 후 소관부처에 처리내역을 통지한다.

라) IoT 제품 사용자

IoT 제품 사용자는 IoT 제품을 사용하면서 보안 이상 징후 발견시, 민관합동 IoT 보안 모니터링단에 확인을 요청한다. 한편, 보안 결함이 사용자 스스로 명확히 확인될 경우는 소관부처에 직접적으로 보안 결함을 신고하도록 한다. 이후 소관부처는 IoT 기기 제조사측에 보안 결함을 통지하고, 시정 권고 혹은 명령을 내리며, 제조사 측에서의 소프트웨어 업데이트 제공을 통하여 IoT 디바이스를 업데이트하여 IoT 제품의 보안성을 유지한다.

마) 소관 부처

소관 부처에서는 IoT 제품 사용자, IoT 보안 모니터링단, IoT 기기 제조사 측에서 IoT 결함에 대한 신고를 상시로 접수받으며, 접수 확인시에 해당 문제에 대한 위해성을 분석하여, 처리를 어떻게 할 것인가에 대해 판단한다. 여기에서, 처리방법은 소프트웨어 업데이트로 즉시 시정 가능한 부분이 있을 것이며, 혹은 즉시 시정이 어렵더라도, 제조사 측에 사항의 경중에 따라 시정 권고 혹은 명령을 통지하여 제조사측에서 보안 대책을 조치할 수 있도록 한다. 한편, 보안 결함 내용과 처리 내역은 IoT 제품 사용자 측에 고지한다. 만약, 시정이 불가능한 경우는 제품에 대한 리콜명령, 파기, 수거의 조치를 진행한다. 제품의 보안 심각성이 굉장히 높을 경우, 즉 해당 IoT 제품으로 사용자가 재산상, 물질상의 피해를 입을 것으로 예상될 경우는 사용자측에 즉시 파기 권고를 내린다. 해당 파기된 제품은 제조사측에서 수거하여, 리콜 등 적합한 절차를 거치게 된다.

③ 사후 보안관리의 세부사항

가) 취약점 대책 보고서 작성

IoT 제품에 새로운 취약점이 발견된 경우, 취약성 대책 보고서를 작성하여야 한다. 해당 보고서에는 IoT 제품 결함에 대한 취약점, 개요, 심각도, 영향을 받는 범위, 예상되는 영향 대책 등에 대한 부분이 명확히 기술되어야 한다.

소프트웨어(혹은 펌웨어) 보안 취약점이 발생하였을 경우, 일반적인 대책은 취약점을 해결한 업데이트 소프트웨어 업데이트를 제공하고 이용자에게 적용을 권고하는 것이다. 그러나 업데이트 소프트웨어의 제공까지 시간이 걸림으로 이용자가 즉시 업데이트를 적용 할 수 없다고 판단되는 경우, 즉시 다른 해결 방법을 준비하여야 한다. 예를 들어, 제품의 특정 기능을 해제하여 취약점의 영향을 받지 않도록 하여야 하는 방법이 있을 수 있다.

나) 사용자에 대한 결함내용 통지

IoT 제품 사용자에게 전달할 취약점 관련 정보가 작성되면 즉시 신속하게 이용자에게 통지하여야 한다. 그러나, 여기에 앞서 취약점 정보가 악용될 위험성을 고려할 필요가 있다. 취약점 정보를 공개하는 것은 해커에게도 해당 취약점 정보가 노출될 수 있다는 점에서, 정보 공개의 수준을 적절히 조절할 필요가 있으므로 이 부분을 주의하여야 한다.

또한 제품에 적용할 수 있는 업데이트 소프트웨어를 제공하고 있는 경우 즉시 이용자에게 설치 권고를 해야 한다. 그러나 IT 기술에 익숙하지 않은 이용자가 사용할 가능성이 있는 제품이나 혹은 이용자의 업데이트 소프트웨어의 적용이 쉽지 않은 경우가 있을 수 있다. 이러한 경우는 원격 조작 등에 의해 자동으로 업데이트 소프트웨어를 적용하는 방법도 고려할 필요가 있다.

이러한 경우, 제품 출하시의 시점에서 제품의 자동 업데이트 기능에 대한 내용을 취급 설명서에 이용자가 알기 쉽도록 적절하게 고지해 두는 것이 필요하다. 만약 업데이트를 통해 제품이 가지는 기능이 변경 될 경우에는 자동 업데이트를 가급적 피하고, 이용자의 동의를 거쳐 업데이트를 적용하도록 하여야 한다.

다) 리콜 실시 절차 및 현행 이슈

소프트웨어 업데이트로 해결하기 어려운 경우 리콜을 실시할 필요가 있다. 즉, 업데이트 소프트웨어의 즉시 적용이 어려운 제품의 경우, 또는 하드웨어 취약점이 발생하였을 경우에는 IoT 제품 분야에 따라 리콜을 실시할 필요가 있다. 이러한 경우 제품을 일단 회수하고, 업데이트 보수 작업을 실시하는 절차가 필요하다.

한편, 현재의 리콜은 제품안전기본법을 근간하고 있다. 제품안전기본법 시행령 제5조의 4에서는 중대한 결함에 대하여 구체적으로 명시하고 있다. 여기에서 중대한 결함이란 '사망, 신체적 부상' 혹은 '질병, 화재 또는 폭발을 일으키거나 일으킬 우려가 있는 결함' 등으로 구체적으로 명시하고 있다.

현재 기술표준원 리콜명령의 주요 근거는 제품안전 기본법 시행령 제5조의4에 명시된 '중대한 결함'의 범위에 따르고 있다. 그런데 여기서 한가지 짚고 넘어갈 부분은, IoT 보안 결함에 대해서는 법제도상 명확하지가 않다는 부분이다.

물론, IoT 제품의 보안 결함 정도에 따라 제품 자체가 사용자에게 신체적, 물질적 손해를 일으킬 가능성은 충분히 존재한다. 그러나 IoT 제품에 따라 그러한 부분이 직접적으로 손해를 끼칠 수 있는 부분은 비교적 명확하게 알 수 있으나, 간접적으로 이용자에게 손해를 끼치는 부분에 대해서는 해당 결함이 사용자에게 끼칠 위해성을 명확히 단정지을 수 없다는데 IoT 제품 리콜의 이슈가 존재한다.

따라서 IoT의 보안 결함에 대한 부분을 해당 시행령에 구체적으로 명시하여 적용할 필요가 있을 것으로 보인다.

④ 관리적 개선방안의 시사점

현재 여러 IoT에 대한 보안 가이드라인, 프레임워크가 제안되고 있다. 앞서 언급한 GSMA 가이드라인은 주로 IoT 서비스를 제공하는 사업자들이나 개발자를 대상으로 작성되었다. 즉, 주요 대상을 IoT 서비스 개발 예정인 기업이나 조직과 같은 사업자를 기준으로 하고 있으며, 주요 내용으로 IoT 제품 제조시의 보안 위협과 취약점을 줄이는 방법에 대하여 제품 설계 및 개발단계에 대한 보안 권장사항을 제공하고 있다.

한편, OTA IoT Trust Framework는 커넥티드 홈, 건강, 웨어러블 기술에 초점을 두고 해당 분야에 대한 필수 보안 권장사항을 30가지 원칙으로 제공하고 있다. 또한, OWASP Internet of Things Project에서 제공하는 지침은 IoT에서 취약점이 발생하기 쉬운 10가지 포인트를 제공하고, 이에 대한 문제를 해결하기 위한 방법을 중심으로 기술하고 있다.

그러나 GSMA, OTA, OWASP에서 제공하는 내용은 공통적으로 IoT 제품 제조시 보안 위협에 대한 취약점을 줄일 수 있는 방법에 대하여 언급하고 있으며, 사후관리에 대한 위협과 발생 가능한 문제점을 구체적으로 어떻게 처리할 것인지에 대해서는 상세히 언급하고 있지 않다. 또한, 세 가이드라인 모두 주로 기술적인 부분을 위주로 하고 있다는 특징을 가지고 있으며, 정책 및 제도적인 부분에 대한 언급을 별도로 하지 않고 있지 않다는 특징이 있다.

즉, 현재까지 공개된 IoT 관련 가이드라인은 대부분 기술적인 부분에 초점을 맞추고 있다는데 한계점이 있다. 현재 IoT 환경이 급속도로 확산되는 가운데 IoT 보안 위협에 대응하는 정책 및 제도적인 논의가 시급하고, 반드시 필요한 시점에 있다.

제안하는 프레임워크는 IoT 제품 사후관리에 초점을 맞추고 있으며, IoT 제품에 대한 전방위 보안위협 탐지, 업데이트/리콜 정책, IoT 보안 모니터링 단 수립 등 IoT 보안 위협에 대한 전반적인 사후 보안관리에 대해 정리하고 있으며, 이러한 점에서 앞서 언급한 보안 가이드라인과 차이가 있다.

현재 각 부처마다 위험 발생시 대응하는 프레임워크를 가지고 있으나, IoT 사후 보안관리에 대한 체계는 아직까지 구체적으로 정립되지 않은 단계이다. 본 논문에서는 이러한 부분에 대하여 IoT 사후 보안 관리 체계를 구체적으로 정립하여 제시하였다.

IoT 환경은 사용자에게 많은 편리성을 제공해 주고 있으나, 그에 따른 보안의 위협도 크다. 아직 국내에서는 IoT 보안 해킹 사례가 많지 않은 편이나, 향후 커넥티드 카 등 다양한 IoT 기기가 보급되면 IoT 보안 위협은 점차 확대될 것이다.

또한, 보안은 사전 조치가 무엇보다 중요하나, IoT 제품의 특성상 이미 출시된 제품, 혹은 향후 발생될 보안 위협에 대해서는 사후 보안관리 체계 마련이 필요한 상황이다. 따라서, 본 논문에서는 IoT 환경에서의 사후 보안관리 프레임워크를 제안하였다.

제안한 사후 보안관리 방안은 IoT 제품의 사용자, 제조사, IoT 보안 모니터링 단이 협력하여 공동으로 IoT 보안 위협을 발견하고, 보안 위협 발견시 적절한 조치를 취할 수 있다는 특징이 있다. IoT 기반의 영상감시 환경은 점차 정착단계로 진행하게 될 것이며, 이에 대한 철저한 보안 대책이 시급하다. IoT에서 보안의 중요성은 아무리 강조해도 지나치지 않으므로, 향후에도 정책적/기술적 IoT 영상감시 보안 체계에 대한 지속적인 연구가 필요할 것으로 보인다.

III. 지능형 영상감시 관련 연구 분석

1. 영상감시 관련 제품 현황

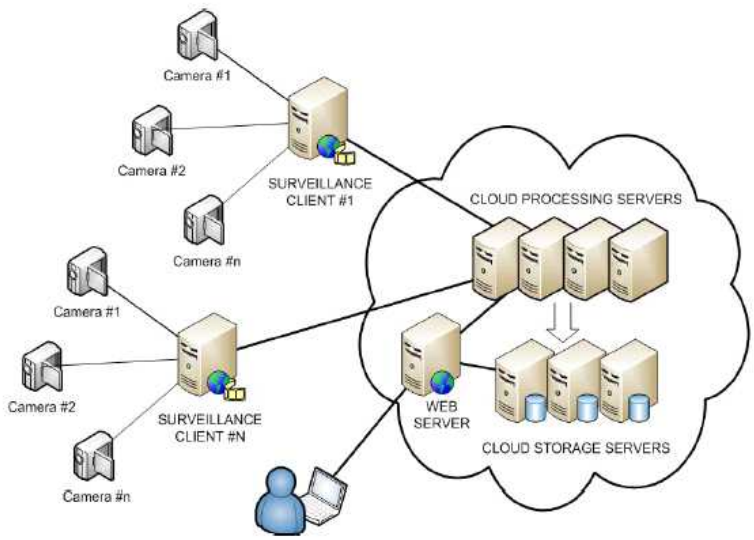
현재 CCTV 영상정보를 안전하게 관리하는 다양한 제품이 국내외에 출시되어 있다. IBM의 Intelligent Video Analytics, Smart Surveillance System 등 다양한 제품이 존재하며, 미국 뉴욕시는 마이크로소프트사와 공동개발한 DAS(Domain Awareness System) 시스템을 구축하여 운용중에 있다. CCTV 영상 처리에서는 영상 객체의 프라이버시 보호가 필수적이며, 지금까지 CCTV상의 영상정보를 보호하기 위한 다양한 방법이 제안되어 있다. 특히, 객체 프라이버시 보호를 위해 가장 널리 쓰이는 방법은 마스킹 기법으로써, 이는 얼굴 영역에 대해서 알아볼 수 없도록 마스킹 처리하는 객체 비식별화 방법이다. 유사한 기법으로 표준 포맷 MPEG-4에서 프라이버시 영역을 스크램블링하는 기법이 제안되어 있으며, 실시간 비디오 영상에 대해 ROI 영역을 추출하여 암호화하는 기법도 제안되었다. 한편, 국방부는 CCTV 및 드론의 촬영영상을 빅데이터로 분석하여 대응하는 D-Net 프로젝트를 진행중이고, 미국의 DARPA에서는 영상데이터에서의 특정행위를 자동 인지하는 VIRAT, 상황 및 행동을 분석하여 다음에 발생할 상황에 대해 예측하는 Mind's Eye 프로젝트가 진행중에 있다.

2. 지능형 영상감시 프레임워크

1) Rodríguez의 연구

클라우드와 빅데이터 환경의 발달은 많은 변화를 가져왔다. 특히, 영상정보 처리 기술은 빅데이터를 통하여 비약적인 발전을 거듭하는 단계이며, 최근에는 영상 객체 인식률이 신뢰성 있는 수준에 근접해 있다. 이러한 기술로 CCTV 기반의 지능치안 환경은 더욱 확대될 것이며, 우리에게 더욱 안전한 생활 환경을 제공해 줄 것이다. 그러나, 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 클라우드 기반의 영상감시 환경을 제안하였다(Rodríguez-Silva, 2012). 지능형 영상 감시 환경은 대용량 데이터를 취급한다는 특성이 있어 확장성과 가용성이 필수적으로 요구되어 Amazon S3 기반의 확장 가능한 아키텍처를 제안하고 있다. 해당 아키텍처는 프라이버시 보호를 위해 SSL 프로토콜로 종단간 암호화할 것을 명시하고 있으며, 암호화 문제는 Amazon S3에서는 자체 암호화가 지원되므로 보안 문제를 해결하였음을 언급하고 있으나, 영상정보 처리와 저장방식에 대한 부분으로 한정되어 있다는데 한계점이 있다. 즉, CCTV 영상 데이터는 클라우드 환경에서 암호화되어 처리되지만, 해당 영상에 대해 어떤식으로 메타정보를 구성하고, 보호할 것인지, 암호화된 데이터에 대한 검색을 어떻게 처리할 것인지에 대해서는 언급하고 있지 않다. 실질적으로 이러한 방식은 향후 빅데이터 기반의 지능형 영상감시 환경에 적용하기에는 한계가 있다.



<그림 III-1> 클라우드 기반의 영상감시

2) CVR 프레임워크

클라우드 비디오 감시 업계에서 인터넷 프로토콜 기반 카메라는 모든 IP 네트워크 기반의 감시 환경 측면에서 높은 수준의 서비스를 제공한다. 네트워크 기반의 감시 환경에 적합한 고품질의 비디오 데이터 전송을 위해서는 적절한 오디오 및 비디오 압축 알고리즘이 매우 중요하다. 예를 들어, H.264 코덱은 비디오 데이터에 대해 100 개 이상의 압축 비율을 만들 수도 있다. 이 코덱에서 750Mbit / s 데이터 크기를 갖는 30 프레임 속도의 1080P (1920x1080) 해상도 비디오는 인터넷 환경에서 8Mbit / s 또는 4Mbit / s로 줄일 수 있다. 대역폭 제한 및 스토리지 소비량 인 IP 카메라의 주요 병목 현상을 해결한다. H. 264-H는 MJPEG-H의 프레임 크기를 7 배, MPEG4 형식의 20 %를 줄인다. 압축 비율은 모든 IP 기반 비디오 감시를 훨씬 쉽게 만들어준다.

클라우드 컴퓨팅은 최근 몇 년 동안 뜨거운 주제이다. 여기에는 IaaS (Infrastructure as a Service), PaaS (Platform as a Service) 및 SaaS (Software as a Service)로 명명되는 세가지의 추상화 수준이 포함된다. 여기에는 IaaS 수준에서 제안된 Hadoop, Cassandra, Mongo DB와 같은 오픈 소스 소프트웨어가 많이 있다. 클라우드 서비스를 구축하는 편리한 방법을 제공한다. 또한 VMware 및 Xen 하이퍼 바이저와 같은 운영 체제 수준의 가상화 기술은 하드웨어와 소프트웨어를 분리하는 새로운 개념을 제공한다. 아래 그림에서 볼 수 있듯이 클라우드 컴퓨팅 시대에는 하드웨어와 소프트웨어가 범용 통신 인터페이스로 연결되어 있으며 소프트웨어 서비스는 너무 많은 물리적 호환 문제를 처리 할 필요가 없다. 이러한 방식으로 클라우드 스토리지 서비스와 같은 많은 확장 가능한 클라우드 서비스 및 애플리케이션이 출시되고 있다.

<그림 III-2> 클라우드 스토리지의 확장 개념도(Lin, C. F., 2012)

아래 그림은 제안된 클라우드 비디오 레코더 (CVR)시스템의 기능적 아키텍처이다. 해당 연구에서는 아래에 열거된 CVR 시스템의 설계 요소에 대한 몇 가지 클라우드 컴퓨팅 개념을 통합한다.

- 가상화 : 아래 그림은 CVR 시스템을 구축하는 하이퍼바이저의 자원 할당 예를 보여준다. 확장 가능한 아키텍처를 설계하기 위해 각 구성 요소는 인터넷 연결 분산 시스템에서 실제 사용을 기반으로 동적으로 모듈화되고 할당된다.

- 스트림 콜렉터 : 대규모 스트림 콜렉션 서비스를 지원하기 위해 코디네이터 인 Stream Collector를 사용하여 입력 스트림을 처리하면서 실시간로드를 동적으로 디스패치한다.

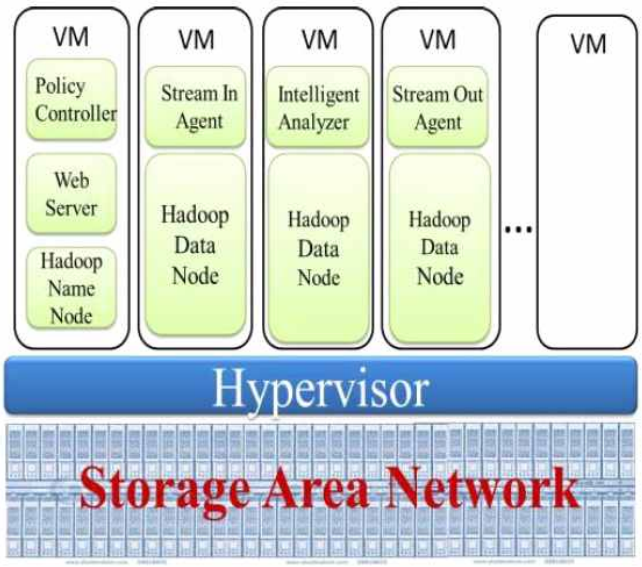
- 스트리밍 서버 : 스트리밍 서버는 분산 노드에서 계산 및 네트워크 I / O 로드를 공유하는 실행중인 각 가상 머신에 설치된다. 실시간 비디오 모니터링 기능을 위해 사용자에게 출력 스트림을 보내는 동안 디스크 I / O 오버헤드를 줄인다. 메모리 매핑 파일 (mmap) 기술은 임시 비디오 데이터를 저장하는 데 사용된다. 오픈 소스 소프트웨어 인 FFmpeg도 여기에 통합되어 실시간 비디오 포맷 및 해상도 트랜스 코딩을 지원한다.

- Hadoop File System : Hadoop 파일 시스템은 우리의 CVR 시스템에 적용되어 분산된 소프트웨어 백업 메커니즘을 지원합니다. 특정 클라우드 인스턴스에서 실행되는 Stream Collector 서비스가 비디오 스트림을 수신 한 후 Hadoop-Fuse 프로토콜을 사용하여 비디오 데이터를 Hadoop 파일 시스템에 저장한다.

- Policy Controller :이 구성 요소는 액세스 제어 및 처리 작업 로그에 사용된다. 이 deaman은 분산 데이터베이스 인 HBase와 통신하여 확장 성 제한을 극복한다.

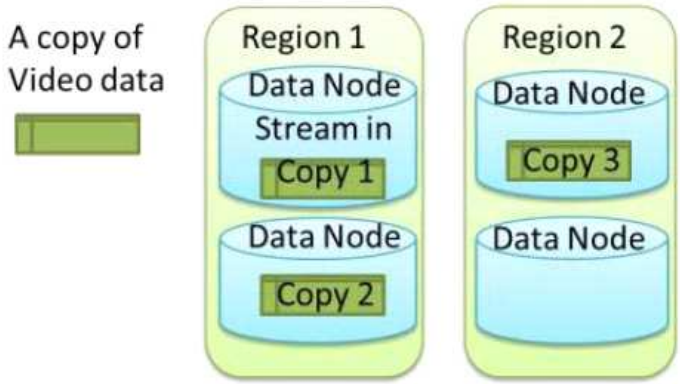
- 지능형 분석 : 비디오 데이터는 Hadoop의 파일 시스템에 저장되므로 Hadoop Map-Reduce 기능을 지능형 비디오 분석에 적용 할 수 있다. 이것은 중요한 모듈이지만 제안 CVR 시스템의 현 단계에서는 지원되지 않는다.

- 웹 서버:이 구성 요소는 사용자에게 콘텐츠 관리 시스템 (CMS)을 제공하고 스트림 아웃 서비스에서 비디오 데이터를 검색한다. 그러나 스트림 아웃 서비스는이 구성 요소와 격리되어 서비스 기능을 확장한다.



<그림 III-3> CVR 프레임워크 기능 아키텍처(Lin, C. F., 2012)

또한, 해당 시스템에서는 Hadoop 복제 메커니즘을 기반으로 한 소프트웨어 백업 기능을 제안하고 있다. 아래 그림에서 두 번째 복제본은 인접한 데이터 노드에 배치되고 세 번째 복제본은 다른 위치에 배치되어 장애 조치 메커니즘을 제공한다.

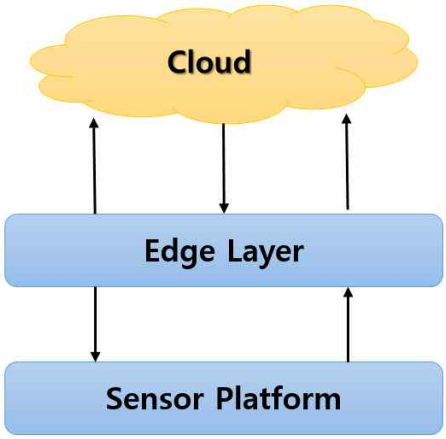


<그림 III-4> 복제본 기반의 Software 백업 기능(Lin, C. F., 2012)

3) Hossain의 연구

지능형 감시 시스템의 관점에서, 특히 클라우드 인프라를 기반으로하는 시스템의 경우 여러가지의 문제가 발생할 수 있다. 먼저, 공용 클라우드 설정에서 일반 사용자는 클라우드 인프라를 사용할 수 있다. 또한 클라우드 제공 업체 내부

에 남아 있기 때문에 감시 고객은 종종 데이터에 대한 통제력을 상실 할 우려가 있으며 잠재적인 데이터 손실이 우려된다. 그러나 Amazon 클라우드와 같은 현재 클라우드 공급자는 이러한 사고를 고객에게 보장하기 위해 최대한의 조치를 취한다. 한편, 사설 클라우드 기반 멀티미디어 감시 시스템에서 클라우드 인프라는 독점적으로 호스팅되는 단일 조직에서 사용되며 향상된 데이터 보안, 개인 정보 및 소유권을 보장한다. 세 번째 디자인 선택은 둘의 구성이다. 조직에서 중요한 감시 데이터를 사설 클라우드에 배치하고 기존 클라우드를 일반적인 데이터에 사용하도록 결정할 수 있다(Hossain, M. A., 2014).



<그림 III-5> 클라우드 기반 감시 개요

아래 그림은 제안된 클라우드 기반 멀티미디어 감시 프레임워크의 아키텍처를 보여준다. 그것은 여러 가지 디자인 측면으로 고려된다. 제안된 프레임워크 디자인은 다양한 콘텐츠 제공 업체, 감시 사용자 및 시스템의 내부 핵심 구성 요소 및 서비스를 강조 및 표시한다.

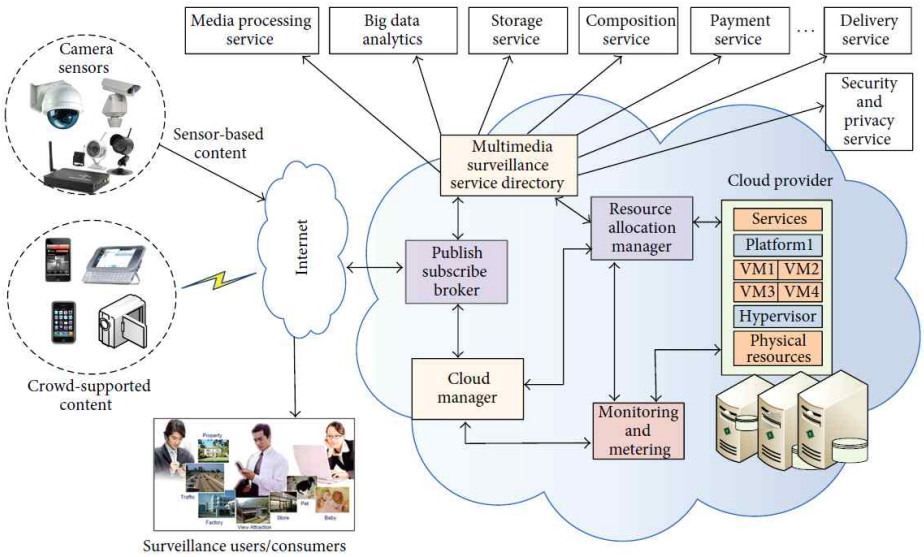
- 감시 콘텐츠 제공자 : 이 아키텍처에는 두 가지 유형의 콘텐츠 공급자가 있다. 하나는 고정 카메라, IP 카메라 및 PTZ 카메라와 같은 이기종 센서 장치이며, 다른 하나는 보안 사고를 보고하는 기능이 있다.
- 가입 메커니즘을 통해 클라우드로 전송된다. 여기서 다른 미디어 획득 대안을 고려합니다. 적절한 인증을 가진 사용자는 연결된 장치를 구성하고 미디어가 샘플링 속도를 제어 할 수 있다.
- 감시 사용자 또는 소비자 : 감시 사용자는 콘텐츠를 사용하는 사용자이다. 이 경우 콘텐츠는 멀티미디어 데이터 및 이벤트 하이라이트로 구성된 이벤트 정보

이다. 사용자는 CCTV 운영자와 같은 일반적인 감시 사업자이거나 어디서나 미디어에 액세스하는 보안 담당자일 수 있다. 그들은 일반적으로 관심사에 따라 감시 이벤트 또는 센서 영상을 구독하고 이에 따라 일치하는 이벤트 또는 스트림이 클라이언트에 전달된다.

- 핵심 시스템 구성 요소 : 이 프레임워크에는 몇 가지 핵심 구성 요소가 있다. 해당 디자인은 앞에서 설명한 문제를 고려한다. Publish-subscribe 중개인은 제안 된 프레임 워크의 가장 중요한 구성 요소 중 하나이며, 미디어 스트림을 게시하고 구독하고 관련 고객에게 관심있는 이벤트를 보급한다. 이는 대역폭과 성능 면에서 성능이 우수하기 때문에 클라우드 측에 위치한다. 확장성있는 유비쿼터스 비디오 감시 서비스를 제공하는 주된 백본이다. 멀티 캐스팅 접근 방식을 사용하여 감시 비디오 스트림을 다양한 감시 컨텐츠 제공자 및 사용자에게 연결하고 전달한다.
- 멀티미디어 감시 서비스 디렉토리 : 제안된 시스템은 서비스 지향 아키텍처 스타일을 채택하므로 모든 기능은 인터넷을 통해 액세스 할 수 있는 서비스로 노출된다. 이러한 서비스는 멀티미디어 감시 서비스 디렉토리에 등록된다.
- 클라우드 관리자 : 제안된 프레임워크의 클라우드 기반 운영에 대한 전반적인 관리는 이 구성 요소에 의해 관리된다. 사용자와 클라우드 기반 감시 시스템 구성 요소 사이의 다리 역할을 한다. 또한 게시 및 가입 브로커, 멀티미디어 감시 서비스 디렉토리, 리소스 할당 관리자 및 모니터링 및 미터링 구성 요소를 관리한다.
- 모니터링 및 계량 : 클라우드 컴퓨팅은 유틸리티와 유사한 리소스 사용 및 청구 방식 또는 pay-as-you-go 모델을 채택한다. 따라서 모니터링 및 미터링 구성 요소는 클라우드 가상 시스템 (VM) 리소스의 성능 모니터링 및 사용 추적을 담당하고 사용량 및 청구 통계를 제공한다.
- 리소스 할당 관리자 : 감시 시스템 및 관련 서비스를 실행하기 위한 다양한 VM 리소스를 관리하고 할당한다. 센서 미디어 스트림을 수신하면 새로운 VM 인스턴스가 요청에 따라 시작된다. 이러한 VM은 감시 미디어 처리 서버로 작동하며 클라이언트 장치 인터페이스와 직접 통신한다. 또한 현재 워크로드 요구 사항에 따라 VM 용량을 동적으로 구성한다. 물리적 서버간에 매핑된 VM 용량의 합이 용량보다 커지면 과부하 상태에서 물리적 서버를 꺼내고 물리적 서버가 로

드될 때 물리적 서버를 끄기 위해 물리적 서버간에 VM을 쉽게 마이그레이션 할 수 있다. VM에 매핑 된 VM은 다른 물리적 서버로 이동할 수 있다.

- 서비스 스택 : 표적 조사 업무를 수행하기 위해 다양한 서비스가 정의된다. 여기에는 미디어 처리 서비스 (예:얼굴 인식 서비스, 모션 검색 서비스, 이벤트 감지 서비스), 스토리지 서비스, 빅데이터 분석 서비스, 지불 서비스, 합성 서비스, 미디어 전달 서비스, 보안 및 개인정보보호 서비스를 제공한다.



<그림 III-6> Hossain의 아키텍처(Hossain, M. A., 2014)

IV. 영상감시 환경의 보안이슈와 취약점 발굴

1. 영상감시 환경의 보안이슈

1) CCTV 영상기기의 보안 취약성

(1) IoT 관점에서의 보안

향후 IoT 시장의 확대를 위해서 반드시 고려해야 할 부분이 보안이다. IoT는 현실세계와 인터넷이 서로 연결되어 기존 사이버 환경에서의 위협이 현실로 고스란히 전이될 수 있기 때문이다. 또한, 기존의 보안 위협요소 뿐 아니라, IoT 환경의 특성에 따른 새로운 보안 취약점이 등장할 수 있으며, 이는 사전에 충분한 보안 취약점이 검토되지 않는다면, IoT로 인해 발생할 수 있는 심각한 보안 사고를 미처 대응하지 못할 수 있다. 따라서, 안전한 IoT 환경을 위해 보안에 대한 철저한 대비가 필수적이라 볼 수 있다.

IoT 환경은 기본적으로 사물이 인터넷에 연결되는 특성을 가지며, 이러한 점은 기존의 IT 환경보다 더욱 많은 보안 취약성을 가질 수 있다. 즉, 기본적으로 기존의 정보통신 환경에서 갖는 보안 취약성은 그대로 가질 수 있으며, 물리 환경과 연동되는 과정에서의 보안 취약성 및 IoT 디바이스 자체의 보안 결함에 따른 디바이스의 무력화, 오용, 작동 정지, 기기 손상 등 다양한 증상을 야기할 수 있다. 이러한 문제점은 해당 IoT 디바이스와 직간접적으로 연동되는 타 IoT 디바이스의 작동에도 영향을 미치게 된다. 또한, IoT 제품의 보안 취약점은 사용자에게 신체적, 재산적 피해를 야기할 수 있다. 예를 들어, 스마트도어락의 해킹이 발생하였을 경우, 원격에서 문의 개폐가 가능해짐에 따라 사용자의 직접적인 재산피해를 발생시킬 수 있으며, 스마트 가스밸브의 해킹이 발생하였을 경우는 오작동이나 과도한 작동으로 사용자의 신체적 안전을 직접적으로 위협할 수 있다.

(2) IoT 영상기기의 보안 취약요소

IoT 기반의 영상기기는 여러 보안 취약 요소가 존재한다. 만약 로컬 API가 평

문을 기준으로 인터페이스가 구성된다면, 암호화되지 않은 상태에서 통신상으로 전송될 것이며, 이러한 점은 보안상 큰 문제를 야기한다. 비록 API상에서 암호화를 지원하더라도 IoT 장치간 통신을 위한 최신 암호화 표준을 적시에 지원하기 어렵다는 문제도 존재한다. 암호화 표준을 시기적절하게 적용하려면 IoT 디바이스에 연결된 모든 장치가 소프트웨어 업데이트 기능을 지원해야 하며, 업데이트가 실시간으로 이루어져야 한다. 그렇지 않으면 IoT 디바이스에 탑재된 소프트웨어 버전의 차이로 기기간 암호화 통신에 문제가 발생할 수도 있다. 한편, IoT 제품의 원격 쉘로 접근이 가능하게 될 경우에도 보안상 심각한 문제가 발생할 수 있다. 이러한 경우 침입자는 기기를 정상작동하지 않게 하거나, 기기 자체를 무력화시킬 수 있다. 또한 중요 데이터를 평문으로 저장하게 될 경우 인가되지 않은 자가 데이터에 접근하여 정보를 가져가거나 조작하게 될 수도 있다. 따라서, 해킹 방지를 위하여 IoT 제품에 대한 원격 쉘 접근은 제품 출시 이후에는 가능하지 않도록 차단하여야 하며, IoT 영상기기내의 중요 데이터는 반드시 암호화하여 보관하여야 한다.

IoT 영상기기 자체의 물리적 파괴나 분실이 발생할 수 도 있다. 이러한 경우는 통신기능 상실로 인하여 IoT 서비스의 중단을 야기할 수 있다. 또한, 기기 분실의 경우는 기기 내부에 포함된 개인정보 유출로도 이어질 수 있다. IoT 영상기기를 대상으로 한 서비스 거부(Denial of Service) 공격이 발생할 수 있다. 단말이나 센서는 정상적인 서비스 제공을 위하여 이들을 관리하는 게이트웨이를 통해 원격에서 연결요청이 수시로 수행될 것이며, 이를 기반으로 악의를 가진 공격자가 대량의 연결요청을 지속적으로 전송하는 것으로 서비스 공격을 일으킬 수 있으며, 이러한 공격에 따라 기기 자체의 전력 소모를 야기하여 결과적으로 정상적인 서비스가 이루어지지 않도록 할 수도 있다.

한편, IoT 제품의 원격 쉘로 접근이 가능하게 될 경우에도 보안상 심각한 문제가 발생할 수 있다. 이러한 경우 침입자는 기기를 정상작동하지 않게 하거나, 기기 자체를 무력화시킬 수 있다. 또한 중요 데이터를 평문으로 저장하게 될 경우 인가되지 않은 자가 데이터에 접근하여 정보를 가져가거나 조작하게 될 수도 있다. 따라서, 해킹 방지를 위하여 IoT 제품에 대한 원격 쉘 접근은 제품 출시 이후에는 가능하지 않도록 차단하여야 하며, IoT 장치내에서의 중요 데이터는 반드시 암호화하여 보관하여야 한다. 따라서, IoT 영상기기의 보안을 위해서는 검증된 보안 통신 프로토콜을 사용할 필요가 있다. 현재 IoT 보안을 위하여 다양한

국내외 표준 기구 및 사설 표준 기구에서 논의하고 있다. 표준화는 ITU, ETSI, IETF등에서 주도하고 있는 상황이며, IETF는 저전력/저성능의 경량화된 방식으로 메시지를 주고받을 수 있는 CoAP를 표준화하고 있다. CoAP는 REST 구조 기반의 프로토콜로 멀티캐스트 지원이 가능한 특징이 있으며, 빠른 서비스의 제공이 가능한 DTLS에 기반한 보안을 제공한다는 특징이 있다. 또한, OMA의 LwM2M 구조에서도 CoAP와 DTLS를 전송 프로토콜로 권고하고 있으며, LwM2M은 ETSI에서 규격 표준화를 진행중이며, 인증, 기밀성, 무결성의 제공이 가능하다.

IoT 환경이 본격적으로 도래하고 있는 현 시점에서, 이와 같은 보안 위협은 반드시 해결되어야 한다. 그러나, IoT 제품은 여러 보안 취약 요소가 존재한다. 만약 로컬 API가 평문을 기준으로 인터페이스가 구성된다면, 암호화되지 않은 상태에서 통신상으로 전송될 것이며, 이러한 점은 보안상 큰 문제를 야기한다. 비록 API상에서 암호화를 지원하더라도 IoT 장치간 통신을 위한 최신 암호화 표준을 적시에 지원하기 어렵다는 문제도 존재한다. 암호화 표준을 시기적절하게 적용하려면 IoT 디바이스에 연결된 모든 장치가 소프트웨어 업데이트 기능을 지원해야 하며, 업데이트가 실시간으로 이루어져야 한다. 그렇지 않으면 IoT 디바이스에 탑재된 소프트웨어 버전의 차이로 기기간 암호화 통신에 문제가 발생할 수도 있다.

(3) IoT 기기 해킹사례

최근 IoT 제품에 대한 다양한 보안 취약점이 보고되고 있으며, 실질적으로 IoT 제품이 해킹을 당한 사례 또한 다수 보고되고 있다. 예를 들어, 유아 모니터링 제품 상당수가 보안 취약점에 노출되어 있으며, 이러한 보안 취약점에 따라 카메라를 해킹하여 영상 링크를 유포하는 등의 사례가 발생한 바 있다.

또한, 2013년 미국 FDA에서 네트워크에 연결된 의료기기가 악성코드에 감염된 사례를 발표한 적이 있으며, 블랙햇 컨퍼런스에서는 의료기기 해킹을 통한 약물 과다 투여 상황을 직접 시연한 바가 있다.

한편, IoT 환경은 다양한 사회 분야에서 활용되고 있으며, 인간의 생활과 밀접하게 연관되어 있다. EU FP7 프로젝트를 수행 중인 IERC의 분류에 따르면, 도시, 환경, 보안/안전, 산업분야에서의 IoT의 활용분야는 매우 다양하며, IoT 기기

의 해킹을 통하여 이와 같은 사회적 서비스가 정상적으로 작동하게 되지 않아 큰 혼란을 초래할 수 있다.

미국에서는 2013년 말부터 2014년 초 10만 대 이상의 스마트 TV, 스마트 냉장고등 가정용 장비에 감염된 Thingbots을 통해 총 750,000건 이상의 피싱과 스팸 메일이 발송된 바 있다. 또한, 리눅스 달로즈 웜으로 PHP의 취약점을 악용하여 보안용 IP 카메라, 셋톱박스 등 리눅스 OS를 사용하는 IoT 기기들이 감염된 사례가 존재한다.

2013년에는 생화학 자동분석 시스템에 연결된 오라클 데이터베이스의 취약점을 이용한 해킹으로 원격에서 DB에 불특정한 정보를 삽입할 수 있음이 보고된 바 있으며, 2013 블랙햇 컨퍼런스에서는 보안업체 인가디언스가 무선 인터넷과 인슐린 펌프를 해킹하여 당뇨 환자에게 약물을 과다 투여하는 방식이 시연된 바 있다. 또한, 2013년 미국 FDA는 네트워크에 연결된 의료기기를 대상으로 하는 악성 코드에 감염된 사례를 발표한 바 있다.

또한, 2012년 미국 데이터 암호화 및 인증 절차의 부재로 고속도로 교통표시판(VMS) 및 교통 제어 시스템이 해킹된 사례가 있다. 또한, 2013 블랙햇 컨퍼런스에서는 자동차의 디지털 콤파스, 휠 인코더, 관성 측정 유닛 등의 센서에 잘못된 정보를 흘려 급정거하거나 차선 이탈 등의 조작이 시연되었다.

2008년 3월에는 미국 조지아 해치 핵발전소에서 운영중인 시스템에 소프트웨어 업데이트 후 48시간 동안 발전소 가동이 중지된 바 있다. 2013년 1월에는 미국 오하이오의 Davis-Basse 원자력 발전소의 보안 모니터링 시스템이 슬래머 웜에 의하여 약 다섯시간동안 작동 불능 상태가 된 바 있다.

한편, 2014년 독일 철강회사를 대상으로 한 공격으로 인해 제철소 시스템에 실제 피해가 발생하였음이 보고된 바 있다. 제철소의 사이버 공격의 결과로 제어 컴포넌트에 문제가 발생하여 용광로가 제어되지 않은 채 중단됨으로써 심각한 손실이 발생하였다. 산업제어시스템은 다양한 산업분야에 걸쳐 폭넓게 사용되고 있으며, 향후 IoT 기반의 산업제어시스템이 보편화되어 보안 위협이 더욱 증가할 것이다.

IoT 환경은 이와 같이 해킹을 당할 경우 개인 뿐 아니라 사회적인 영향을 미치게 될 수 있어 철저한 보안 대책이 필요한 상황이다.

(4) IoT 영상기기 보안의 두가지 관점

IoT 제품을 제도적인 보안성 측면으로 볼때, 크게 두가지의 관점이 존재한다. 먼저, 제품 출시 전 단계에서의 보안성 확보 방법으로, 적절한 규제를 통하여 보안상 안전이 검증된 제품만을 출시하도록 하는 방법이다. 이는 제품의 설계/개발 단계에서 사전에 해당 규제를 충분히 만족하도록 하는 것이며, 안전한 IoT 환경을 위해서는 최소한의 강력한 규제가 필요하다고 볼 수 있다. 이러한 제도가 정착되면 기본적인 보안성이 확보되지 않은 제품은 시장에 출시되지 않을 것이다.

두번째 관점으로, 제품 출시 이후의 사후관리가 필요하다. 이는 IoT 제품의 운영/관리 단계에서 필요한 부분에 해당한다. 제품의 출시 전에 미처 발견되지 않았던 보안상의 허점이 제품 출시 이후에 발견될 수도 있으며, 이러한 취약점이 발견된 경우에는 기본적으로 소프트웨어 업데이트로 해결해야 하며, 이를 위해 IoT 제품에는 자동 업데이트 기능 탑재가필수적으로 요구된다. 그러나 경우에 따라 소프트웨어 업데이트가 불가능한 경우나, 하드웨어 결함이 존재하는 경우에는 리콜과 같은 대책을 실시할 필요가 있다. 또한 보안 허점을 통하여 사용자의 신체적, 재산적 안전에 큰 영향을 미칠 수 있는 경우에는 즉시 해당 제품에 대하여 수거 또는 파기와 같은 조치가 필요할 수도 있다. 여기에서는 IoT 제품 보안의 현행 법제도적 한계점을 제도상의 규제와 사후관리의 두가지 관점에서 분석한다.

① IoT 영상기기 보안성 확보의 한계점

현재 많은 IoT 제품이 시장에 출고되고 있다. 그러나 제품의 보안성에 대한 법제도적 대응책은 미비한 상태에 있는 실정이다.

한국인터넷진흥원(KISA)에서는 IoT 보안과 관련된 몇가지의 기술안내서를 제공하고 있다. 여기에는 IoT 제품 개발 시 공통적으로 고려해야 할 보안 원칙과 가이드라인을 제시하고 있는 'IoT 공통보안 원칙', 'IoT 공통보안 가이드'가 있으며, IoT 환경에서의 경량 암호화 활용을 위한 '사물인터넷(IoT) 환경에서의 암호 인증기술 이용 안내서'가 존재하고 있다. 그러나 해당 기술안내서는 IoT 제품 설계 및 개발 단계에서 참고로 하여 적용은 가능하나, 법제도적인 강제성을 포함하고 있지 않다는데 한계점이 있다. 만약 특정 IoT 제품의 출시일이 임박할 경우,

보안에 대한 대책과 검증을 소홀히 한 상태에서 IoT 제품을 출시하게 되는 경우를 상상해볼 수도 있다.

한편, 현재 IoT 환경을 규제할 수 있는 단일 법률은 존재하지 않는 상태이다. 2015년 12월 사물인터넷에 대한 단일화 법제를 추진하기 위하여 입법 공청회가 개최된 바 있으며, 여기에서는 '사물인터넷 진흥에 관한 법률안'에 대하여 논의된 바 있다. 해당 법안에는 IoT 환경에 대한 정책적 추진, 기반조성, 활성화 방안과 같은 주요 내용을 담고 있다.

IoT 단일화 법률이 구체적으로 시행되지 않고 있는 현재 시점에서는, 정보보안을 명시적으로 규정하고 있는 '국가정보화 기본법', '개인정보보호법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '정보통신기반 보호법', '위치정보의 이용 등에 관한 법률'과 같은 통상적인 법률에 의존해야 한다. 이러한 법률은 생활의 편익 증진으로 법의 목적이 유사한 편이며, 궁극적으로 정보보호라는 동일한 목적을 지향한다고 볼 수 있다. 그러나 개별법규의 성격상 수범주체와 보호방법에 차이가 있다. IoT 환경은 물리환경과 정보통신기술이 결합되는 것으로, 이에 적합한 법제도적 마련이 필요하며, 법률 단위에서의 규제와 동시에 품질인증, 기술기준과 같은 현행 제도에서도 제품 보안성 항목을 명시적으로 언급할 필요가 있다. 특히 각 제품별로 보안 고려사항이 다를 수 있으므로 보안성 검토에 대한 부분은 각 인증제별로 가급적 상세히 명시되어야 하는 것이 바람직하다.

그러나 대부분의 인증제도는 정보보안에 대한 인증항목을 가지고 있지 않은 것이 현실이다. 여기에서 보안성에 대한 부분은 해당 품질인증제에서 고려할 것이 아니라 별도의 인증제도를 만드는 것이 타당하다고 생각할 수도 있으나, 현실적으로 제도적인 효율성 측면에서 별도의 제품별 보안인증제도를 만들기보다는 현행의 인증제도나 기술기준에 보안성 항목을 부여하는 것이 효율적이다.

현재 미래부의 소관으로 정보통신망법과 국가정보화기본법에 근거한 '정보보호관리체계인증(ISMS)'과 '정보보호시스템 평가인증(CC인증)'제도가 존재하고 있으나, 이는 법정임의 인증제로서 강제성을 띠고 있지 않으며, 단일 인증제로는 제품별 특성에 맞는 보안항목에 대해서 상세히 규정하기에는 한계가 있다.

안전한 IoT 환경을 위해서는 제도적인 강제성을 부여하는 법정의무 인증제도와 기술기준에 IoT 보안 항목이 들어가는 것이 가장 합리적이다. 따라서, 본 논문에서는 현재의 제품별 법정의무 품질인증제도와 기술기준에 보안항목을 적용하는 것을 제안한다.

② 보안성 유지관리 측면에서의 한계점

가) 사후 보안성 관리 개요

IoT 제품 출시 이후, 미처 생각치 못한 보안 허점이 발견될 수 있다. 제품 설계상의 허점이 아니더라도, 예를들어 암호화 알고리즘 자체나 보안 표준상의 취약성이 발견되는 등 외부적인 요인에 의하여 IoT 제품의 보안성이 크게 위협받을 수도 있다.

이러한 경우, 상황의 심각도에 따라 소프트웨어 업데이트를 즉각적으로 실시할 수 있는 자동 업데이트 시스템이 필요하며, 이러한 업데이트 과정에서 해킹의 위협이 없도록 설계하여야 한다. 또한, 업데이트 파일 자체가 해킹을 통하여 변조되었을 경우도 고려하여 원본 파일이 무결성을 유지할 수 있어야 한다. 그러나 현재 출시된 IoT 제품 가운데 이러한 자동 소프트웨어/펌웨어 업데이트가 적용되지 않은 제품은 향후 발생 가능한 보안의 취약점에 능동적으로 대응하기 어려운 것이 현실이다.

한편, 소프트웨어 업데이트만으로 해결이 불가능한 경우도 있다. 이러한 부분은 하드웨어 자체를 교체해야 하며, 리콜과 같은 제도적인 절차에 따라 IoT 제품 자체나 그 일부를 교체하여야 한다.

그러나 현재의 리콜제도는 정보보호의 측면보다는 사용자의 안전에 중점을 두고 있는 것이 현실이다.

통상적으로 말하는 리콜제도란 제조사가 제품을 판매한 이후, 사용자의 신체적 위협 또는 재산적인 피해가 발생할 우려가 있는 제품 결함이 발견될 경우에 사업자나 기관의 주도로 해당 제품을 수거하여 교환 또는 환불 조치를 하는 것을 말한다.

리콜은 기본적으로 제품안전기본법에 근거하고 있다. 해당 법률의 시행령 제5조의4에서는 중대한 결함을 '사망, 신체적 부상이나 질병, 화재 또는 폭발을 일으키거나 일으킬 우려가 있는 결함'으로 구체적으로 명시하고 있다.

현재로서는 IoT 보안 결함에 대해서는 제품안전기본법에 근거하여 리콜을 적용받기가 모호한 실정이다. 만약 매우 명백한 보안 결함으로 사망, 화재 등 신체

적/물질적 피해 사례가 다수 보고될 경우는 해당 항목에 근거하여 조치할 수 있겠으나, 피해가 우려되고 있는 상황 또는 실질적인 피해 사례가 많지 않은 상황, 제조사에서 결함 사실을 인정하지 않는 경우 등에 대해서는 해당 법의 적용이 사실상 어려운 것이 현실이다. 특히, IoT 환경에서는 제품과 제품간 통신을 하며, 해당 제품에 대한 보안 결함이 해당 제품과 통신하는 다른 제품에 간접적으로 영향을 발생시킬 경우도 문제가 될 수 있다.

현실적으로 IoT 제품에 대한 리콜 등 사후관리에 대한 법제도적 안전장치는 마련되어 있지 않은 실정이며, 소프트웨어 자동 업데이트의 제도적 의무화, 제품안전기본법 등 관련법의 개선을 통하여 IoT 제품에 대한 사후관리 환경을 조성하는 것이 시급하다.

나) 출하 이후 신규 취약점 발생 가능성 존재

제품 출하 이전 IoT 제품 테스트 시 보안 취약점을 발견할 수 없었더라도, 제품 출하 이후에 보안 취약점이 신규로 발견되는 문제가 발생할 수 있다. 즉, 이미 제품이 시장에서 출시되었고, 다수의 이용자가 해당 기기를 사용하고 있는 상황에서는 해당 신규 보안 취약점이 불특정 다수에 공개되는 경우에 IoT 제품을 사용하는 전체 사용자가 해커의 표적이 될 수 있으며, 이러한 경우는 심각한 문제로 이어질 수 있다. 그러나, 현재 이러한 부분에 대한 제도적인 대응책은 마련되어 있지 않다. 현재 KISA의 소프트웨어 신규 취약점 신고포상제도가 존재하고 있으나 이는 소프트웨어의 취약점을 발견한 신고자에게 포상을 부여하는 제도로서, 제도적인 강제성이 없고, 실질적으로 IoT 제품의 특성에 적합한 제도가 아니므로 제품의 보안 취약점 발생 시 IoT 기기 제조사의 즉각적인 조치를 강제할 수 없다는 부분에서 한계점이 있다. 따라서, IoT 기기 제조사가 즉각적으로 신규 취약점에 대응할 수 있는 제도적인 체계가 반드시 필요하다.

다) IoT 보안사고 책임부처의 모호성

IoT 제품의 보안사고가 발생하였을 시 책임 전담부처가 명확하지 않다. 이는 IoT 제품이 물리적 환경과 IT 환경의 성격을 동시에 가지고 있다는 점에서 기인한다. 즉, IoT 제품의 보안 결함이 발생하였을 경우에, 보안 결함의 영향도에 따

라 소관 부처가 달라질 수 있다. 예를 들어, IoT 기기에 해킹을 통하여 개인정보의 노출 등이 발생할 우려가 있는 경우와 IoT 스마트 도어락 기기의 오작동 등을 기반으로 물리적인 재산적 손실이 발생 가능한 경우를 들 수 있다 이 두 가지 경우에 본질 자체는 IoT 기기의 보안 결함에서 기인하나, 실질적으로 해당 결함으로 피해를 입을 수 있는 형태가 달라지게 된다. 특히, 기기에 대한 배터리 화재 등을 야기하는 작동이나, IoT 의료기기의 오작동을 야기하는 해킹을 통하여 인체에 치명적인 영향을 유발하게 될 경우는 즉각적인 리콜로 처리해야 하며, 이러한 경우는 제품의 리콜 소관부처가 담당해야 한다. 이에 대한 정책적 체계가 아직 명확하지 않은 상태이다.

라) 사용자의 제품 보안 결함 인지체계 부재

IoT 제품에 대한 보안 결함이 발생하였을 경우, 해당 제품을 사용자가 지속적으로 사용하는 것은 큰 문제를 야기할 수 있다. 특히, 소프트웨어의 즉각 업데이트 조치가 어려운 경우, 사용자는 해당 보안 결함이 있는지를 인지하지 못한 채 IoT 기기를 그대로 사용하게 될 것이다. 즉, IoT 기기의 보안 결함이 발생한 경우 해당 장치를 사용하는 사용자에게 해당 보안 결함이 무엇인지, 특히 해당 보안 결함에 따라 침해될 수 있는 범위와 영향도가 무엇인지에 대하여 구체적으로 인지할 수 있는 체계가 필요하다. 경미한 보안 결함인지, 혹은 일부의 개인정보 노출 등 다소 심각성을 가질 수 있는 보안 결함일 경우인지 여부를 사용자가 구체적으로 인지할 수 있게 하고, 제품 이용을 즉각적으로 중지할 것인지에 여부를 판단하게 할 수 있도록 하여야 한다.

마) 소프트웨어 업데이트 시 보안위협

제품의 보안 취약성이 소프트웨어 업데이트로 해결 가능한 경우는 즉각적인 업데이트가 실시되어야 한다. 그러나 소프트웨어 업데이트 시에는 다양한 보안 위협이 존재할 수 있다. 대표적으로 업데이트 소프트웨어의 무결성 손실로 인하여 부적합한 상태의 업데이트 파일이 배포되는 경우를 생각해 볼 수 있다. 또한, 해커의 악의적인 개입으로 불법 소프트웨어에 대한 배포가 발생할 수 도 있으며, 통신 과정에서의 변조 공격 등이 발생할 수도 있다.

무엇보다 소프트웨어에 대한 무결성과 신뢰성을 확인하고 설치하는 것이 가장 중요하며, 이러한 부분이 제도적으로 관리될 필요가 있으나, 현재는 이러한 체계가 확립되어 있지 않은 상태이다.

2) 클라우드 영상감시의 보안 취약성

(1) 개요

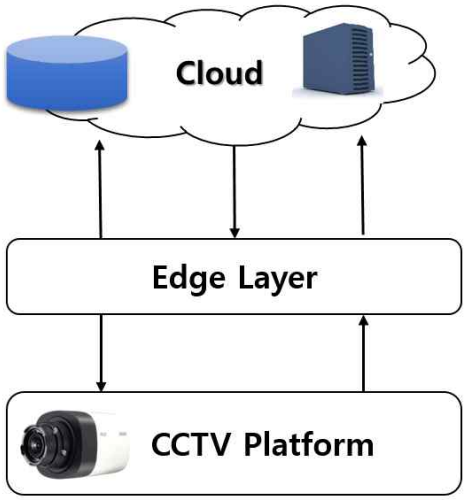
클라우드 기반 지능형 감시가 가장 잘 활용될 수 있는 분야는 스마트시티이다. 스마트시티는 정보통신 기술을 활용하여 도시 인프라, 사람, 환경 등 도시 구성요소를 통합하고 관리 및 효율성을 극대화하기 위한 것이다. 이러한 스마트시티는 환경, 에너지, 수자원, 교통, 헬스, 치안을 포함하는 개념이며 단순한 정보통신 인프라 이상의 지능형 서비스를 제공하고자 하는데 목적이 있다.

이러한 스마트시티는 현재 각국에서 추진되고 있으며, 지능형 첨단 기술을 바탕으로 시민에게 직접적으로 필요한 지능화되고 친환경적인 다양한 서비스를 제공해 줄 것으로 기대된다.

이러한 스마트 시티의 지능형 서비스 제공을 위해서는 센서를 통한 정보수집, 상황 감지, 상황 인지 등 다양한 기술이 필요하다. 여기에는 사람의 행위, 사물의 동작에 대한 다양하고 체계적인 정보 수집이 필요하며, 이러한 특징으로 원활한 스마트 시티에 있어 스마트 감시 체제의 역할이 중요하게 작용한다.

지능형 감시 체제에 있어 반드시 고려되어야 할 부분은 사용자의 프라이버시 보호 문제이다. 데이터가 수집되는 사람이나 사물에 대한 프라이버시를 고려하지 않는다면 심각한 개인정보 침해로 이어질 수 있다. 예를들어 측정된 센싱 데이터나 전력 정보를 기반으로 특정 개인이 언제 외출하고 있는지, 어떤 전자기기를 사용하는지 등 여러 라이프스타일에 대한 추정이 가능하며, 이러한 점은 도시 내 각각의 구성원에 대한 전체적인 라이프 로그를 스마트 시티 환경에서 수집하게 될 수 있어 매우 심각한 프라이버시 침해 요소가 될 수 있다. 따라서, 스마트시티 환경에서는 안전한 프라이버시 보호를 전제로 한 스마트 감시 대책이 필수적이다. 특히, CCTV 추적정보, 센싱 데이터, 미터링 데이터 등은 필수적으로 보호되어야 할 항목이며, 이러한 데이터는 안전한 취급이 필요하다.

그러나, 현재의 스마트 감시 체제에서는 이러한 부분에 있어 한계점이 존재한다. 특히, 클라우드 기반의 스마트 감시 환경에서는 보안에 대한 문제를 더욱 심각하게 고려해야 한다. 공용 클라우드의 경우는 다양한 서비스가 클라우드 시스템에 연결되어 있으며, 스토리지 및 데이터베이스를 공통적으로 활용한다. 이러한 부분은 클라우드 서버 내의 데이터를 해킹 할 경우에는 큰 취약점으로 작용할 수 있다. 아래 그림은 다양한 서비스에서 취득된 센싱 데이터, CCTV 추적정보, 미터링 정보가 클라우드 환경에 수집되는 경우를 나타낸다.



<그림 VI-1> 클라우드 서버의 데이터 수집

이러한 정보가 클라우드 환경에 수집될 경우, 특정 개인의 헬스케어 정보 등 다양한 센싱정보, CCTV에 촬영된 개인 추적 정보, 전력 사용에 따른 미터링 데이터 등 다양한 정보가 공용 클라우드 환경에 저장될 것이다. 이러한 부분은 심각한 문제가 될 수 있어 해당 데이터에 대해서는 반드시 안전한 보안 기술을 확보하여 관리할 필요가 있다. 스마트 감지 환경에 클라우드 환경을 도입하면 클라우드 환경의 특성에 따른 여러 보안 위협을 그대로 답습할 수 있기 때문이다.

여기에서, 데이터를 암호화하는 방안을 생각해 볼 수 있으나, 암호화된 데이터는 기본적으로 질의를 통한 통계 처리가 불가능하다. 암호화된 데이터의 정렬 순서는 평문과 상이하기 때문에, 범위검색, 전방일치 검색, 통계 질의에 대해서는 무의미한 결과를 리턴하기 때문이다. 이러한 문제로 인하여, 현실적으로는 통계처리 및 가용성 등 개인정보 활용 측면에서 보안성 뿐만 아니라 효율성도 동시에 고려될 필요가 있다.

한편, 클라우드 환경은 멀티테넌트 아키텍처에 근거하여 여러 사용자가 리소스를 공유하게 되므로 클라우드 환경에서의 다양한 보안 침해가 발생한다. Openstack Swift 기술은 사용자 이름, 암호 및 계정으로만 데이터의 유효성을 검사하는 TempAuth 미들웨어를 사용하여 보안 인증을 처리한다. 그러나, 높은 수준의 데이터 보안을 달성하려면 암호화가 반드시 필요하다. 암호화가 수행되는 위치에 따라 서버측 암호화와 클라이언트 측 암호화로 분류된다. 서버측 암호화는 데이터를 안전하게 보호하는 반면 클라이언트 측 암호화는 전송 중에 데이터를 보호한다는 특징이 있다. 그러나 Swift에서 데이터를 암호화하고 키를 구성할 수 있는 자동화된 메커니즘이 없다는 문제가 있어 해결책이 요구된다.

일반적인 클라우드 저장소는 대체적으로 PPI(pay-per-use) 비즈니스 모델을 따른다. 따라서 많은 클라우드 서비스가 클라이언트 측의 중복제거를 적용한다. 이 개념은 클라우드 서버에 중복 데이터를 저장하지 않고 네트워크 대역폭을 줄인다. 클라우드는 멀티테넌트 환경이므로 많은 보안 문제를 야기한다. 특히, 특정 파일의 소유권 문제가 발생할 수 있고, 특정 파일에 어떤 사용자가 매핑되었는지 여부를 서버에서 확인할 수 있다. 이러한 점은 프라이버시 관점에서 문제가 될 수 있으며, 중복제거된 파일을 삭제하면, 해당 파일을 소유한 모든 계정의 파일이 논리적으로 사라지게 된다는 문제점도 존재한다.

2. 프라이버시 관점에서의 보안 이슈

1) 개인정보 노출범위 및 침해유형

지능형 감시 환경의 특성상 개인정보는 더욱 다양하게 노출될 수 있다. 원활한 서비스 제공을 위해서는 최소한의 개인정보의 취급은 필수불가결하나, 이를 안전하게 관리한다는 전제가 반드시 필요하다. 여기서는 지능형 감시환경에서의 개인정보보호 취약요소를 분석한다.

(1) 개인정보 노출 범위

지능형 감시환경에서 다루어야 할 개인정보보호우려는 방대하게 존재한다. 이

는 지능형 감시환경 시스템의 구현이나 효용성에 영향을 미칠 수 있다. 예컨대, CCTV 영상 데이터의 보안 및 개인정보보호에 관한 개인 신뢰의 결여는 전면적인 소송전은 아닐지라도 잠재적인 문제로 작용할 수 있다. 일반적으로, 지능형 감시환경에 관한 개인정보 노출은 다음의 두 가지 범위 중 하나에 속한다. 여기에는 첫번째, 기존에는 쉽게 수집할 수 없었던 개인정보의 획득이 있으며, 두번째, 기존에도 개인정보 수집이 가능했던 정보에 대한 새로운 정보 획득이 있다.

첫번째 범위의 예시로는 해당 위치의 합법적 및 불법적 작동 시기와 개인적 패턴을 나타내는 특정 의료기기 및 전자기기의 사용에 관한 정보, 각 가전기기와 측정 위치에서의 전력 소비에 관한 세분화된 시계열 데이터를 비롯하여 주어진 위치에서 사용 중인 가전기기 및 장비에 관한 다양한 상세 정보를 들 수 있다. 두번째 범위는 개인정보가 다른 출처에서 제공되고 지능형 감시 시스템이 이러한 정보의 새로운 출처가 되는 경우가 속한다. 예컨대, 개인의 물리적 위치는 오늘자 신용카드와 휴대전화 기록으로 추적할 수 있다. 전기자동차 충전의 경우에는 새로운 에너지 소비 데이터를 통한 물리적 위치의 추적 가능성이 제기된다.

집 또는 건물 안에서의 활동의 상세 내역은 기기 전자서명과 시간패턴으로 추론할 수 있다. 이러한 서명과 패턴은 소유자의 활동에 대한 파악의 근거가 될 수 있다. 이러한 개인정보 노출의 몇가지 예는 다음과 같다.

첫째, 에너지 사용 데이터로 다양한 정보에 대한 파악이 가능하다. 집안에서의 개인의 행동 패턴과 활동, 수면, 샤워, TV시청과 같은 활동을 비롯하여 전기 사용 패턴과 가전기기 사용을 모니터링하여 파악할 수 있는 집안에서 일어나는 행동 패턴, 습관, 활동에 대한 정보가 노출될 수 있다. 또한, 실시간 에너지 사용 데이터를 통해 집안에 사람이 있는지 여부와 무엇을 하고 있는지, 집 안의 어디에 위치하고 있는지 등 실시간 행동에 대한 모니터링도 가능해진다는 우려가 있다.

둘째, 전기자동차의 충전 정보를 통해 위치정보의 파악이 용이해진다. 즉, 이러한 정보는 전기자동차의 충전 이력을 통하여 마지막 충전 이후 사용범위를 파악하는데 사용될 수 있다. 따라서 이러한 정보는 사용자의 운전 습관 등의 파악을 통하여 보험료 산정, 마케팅 등에 활용될 수 있다.

셋째, 소비자 소유의 장비는 스마트 가전기기를 통해 직접적으로 파악이 될 수 있다. 이러한 정보는 손해사정(예를 들어, 기기가 주택 화재로 인해 파괴되었다고 주장할 경우), 위험을 증가시킬 수 있는 기기 존재시의 보험료 산정 등에

활용이 될 수 있다. 한편, 절도할 표적자산을 확인하는 행위, 개인정보를 수집하기 위해 바이러스 또는 기타 공격을 유입시키는 행위 등의 악의적인 목적으로 활용될 우려도 존재한다.

(2) 개인정보 침해유형

① 개인정보의 노출

개인정보가 노출되는 경우는 일반적인 시스템 환경에서도 공통적으로 가지고 있는 문제이다. 그러나 지능형 감시 환경에서는 에너지 소비량과 같은 다양한 데이터가 존재한다. 기존에도 개인정보의 노출 자체는 가능하였으나 기존의 감시 환경에서는 데이터 조작 또는 노출 가능성이 비교적 낮은 편이었다. 그렇지만 빅데이터 기반의 지능형 감시 환경에서는 새로운 방식의 개인정보의 노출이 용이해지게 될 우려가 있다.

② 개인의 행동패턴/사용기기 파악

홈 자동화 네트워크 또는 지원기술이 탑재된 다양한 IoT 기기는 특정 가전기기의 시용을 추적할 수 있다. 예를 들어, 스마트미터는 집의 특정 영역에서의 전기 사용 위치와 시기를 노출시킬 수 있는 데이터 사용 프로필은 작동되거나 사용된 가전기기의 유형을 노출시킬 수 있다. 이러한 정보는 가전기기 제조업체의 제품 신뢰성 및 품질 보증을 위해서, 혹은 표적 마케팅을 위해서 활용될 수 있다.

③ 실시간 원격감시 실시

CCTV 영상정보에 접근이 가능한 경우, 어느 시설이나 주거지에 사람이 있는지 여부, 무엇을 하고 있는지에 대한 정보, 기상 및 수면 패턴, 건축물 내부의 어디에 위치하고 있는지, 몇 명이나 있는지에 대한 정보 등이 노출될 수 있다. 이러한 CCTV 영상정보를 토대로 향후에도 여러 감시 방법이 나타날 수 있다.

④ 상업적인 데이터 사용

CCTV에 촬영된 객체의 영상데이터 저장은 광범위한 제품 및 서비스의 공급업자를 비롯한 다수의 업체에게 가치를 가지는 생활 방식 및 정보를 노출시킬 수 있다. 공급업자는 표적 판매 및 마케팅 캠페인에 유용한 속성 목록을 입수할 수도 있는데, 정작 대상은 이를 긍정적으로 생각하지 않는 경우가 많다. 보험 등의 목적으로도 데이터가 활용될 수 있을 것이다. 기존의 감시 시스템에서는 활동에 관한 상세 정보를 노출시킬 정도로 세부적인 파악은 어려웠으나, 지능형 감시 환경은 빅데이터 기반의 다양한 분석 및 동종업계 비교를 위해 판매되고 사용될 수 있는 사용 시기, 수요, 장비의 직접 부하 제어에 관한 상세한 데이터를 생성하며, 이러한 정보는 제3자에게 유용하게 활용될 수 있을 것이다.

2) 메타정보 암호화와 가용성의 비양립성

향후 영상 감시 환경에서는 빅데이터를 기반으로 CCTV 영상데이터를 분석하여 특정 개인을 인식할 뿐만 아니라, 해당 객체의 현재 행동을 인식하며 행동 패턴을 분석하고 추론할 수 있게 될 것이다. 따라서 영상 메타데이터의 범위는 단순히 특정 개인의 신원을 인식하는 수준이 아니라, 개인에 대한 감정, 현재 상태, 행동에 대한 예측, 위험 수준 등 다양한 정보를 수집하고 메타데이터상에 기록하게 될 수 있다.

이러한 영상 분석 메타데이터는 직접적인 개인정보를 담고 있다고 볼 수 있다. 예를 들어 지능 치안 환경을 위해 용의자 등 특정 인물에 대한 CCTV 기반의 위치 추적 정보, 현재 행동, 위험도 판단 등 다양한 분석이 실시간으로 이루어질 수 있으며, 이러한 정보를 메타데이터로 저장할 경우 직접적으로 정적 개인정보뿐만 아니라 동적 개인정보까지 실시간으로 저장되므로 더욱 안전한 관리가 필요하게 될 것이며, 만약 메타데이터에 대한 해킹 등이 발생한 경우라도 반드시 안전이 보장되어야 할 필요가 있다.

공격자가 데이터베이스에 접근 권한을 획득하는 경우, 영상 메타정보에 대한 질의가 가능할 것이며, 이 과정에서 메타데이터를 평문으로 보관하고 있을 경우

에는 해당 영상 메타 데이터가 공격자에게 그대로 노출될 것이다. 외부에서의 해킹 이외에 내부자에 의한 데이터 유출 공격 사례도 다수 존재하는 바, 개인정보 보호 관점에서 메타데이터를 평문 그대로 저장하는 것은 심각한 개인정보 침해로 이어질 수 있어 매우 위험하다고 볼 수 있다. 따라서 영상 메타데이터도 일종의 개인정보로 간주하고 보호해야 한다.

그런, 영상 메타데이터를 데이터베이스에 평문 형태로 저장하지 않고 암호화하여 저장할 경우, 데이터베이스에서의 질의가 매우 어렵게 된다는 문제점이 있다.

예를 들어, 영상 내의 특정 범위 내 위치에 접근한 사람을 검색하고자 할 경우, 암호화된 상태에서는 범위검색 질의를 할 수 없다. 이는 암호화된 데이터가 평문의 순서와 달라지는 것이 원인이며, 암호화된 데이터의 결과를 기준으로 범위검색을 수행한다면 원하는 결과와는 전혀 다른 데이터를 가져오게 된다.

이러한 문제를 해결하기 위한 방법으로 순서보존 암호화(OPE:Order-Preserving Encryption) 방식이 제안된 바 있다. 그러나 이러한 OPE 방법을 사용하게 될 경우 암호화된 결과값이 평문과 순서가 동일하게 되므로 실질적으로 보안성에 있어 취약하다고 볼 수 있다. 또한, OPE 방식은 원본 데이터가 수치 데이터로 구성되어야 한다는 단점이 존재한다. 실질적으로 문자와 숫자의 정렬방식에는 차이가 존재한다. 데이터베이스에서는 예를 들어, 수치 데이터의 경우 100보다 20이 작은 값으로 간주되나, 문자열 데이터의 경우에는 20이 더 큰 값으로 간주된다. 영상 메타데이터는 수치 데이터와 문자열 데이터 복합적으로 취급된다. 기존의 순서보존 암호화 알고리즘은 수치 데이터에만 유의미하게 작동하며, 문자열 데이터에는 평문과 정렬순서가 다르게 되어 영상 메타데이터의 보안기법으로는 적합하지 않다.

실질적으로 기밀성 확보와 데이터 검색에서의 효율성은 양립이 쉽지 않다. 원활한 데이터 검색을 위해서는 원본 데이터에 대한 최소한의 정보가 필요하여 실질적으로 기밀성 유지가 불가능하기 때문이다.

이와 같이 프라이버시 보호와 효율적인 영상 감시는 동시에 달성하기가 어려운 문제이다. 그러나, 향후 영상인식 기술이 점차 발전하고, 빅데이터 기반의 보다 세밀하게 분석된 영상정보가 메타데이터상에 상세히 기록될 것으로 예측되는 바, 영상감시 환경에서의 프라이버시 문제는 반드시 해결되어야 할 필요가 있다. 이미 법제도적으로 CCTV 영상 데이터에 대한 안전성 확보를 명시하고 있다. 현

재 개인정보보호법 제25조(영상정보처리기기의 설치·운영 제한)의 제6항으로써 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 함을 명시하고 있어 이에 대한 고려가 반드시 필요한 상황이다.

3) 영상 프라이버시 보호의 한계점

영상 프라이버시를 보호하기 위한 다양한 방법이 제안되어 있다. 가장 일반적으로 사용하는 방법은 얼굴영상 마스킹 방법이며, 이는 얼굴 영역에 해당하는 부분을 알아볼 수 없는 픽셀로 대체하는 것으로, 사용자의 프라이버시 보호는 가능하지만 얼굴 자체에 대한 특징이 남아있지 않으므로 통계자료 제공에서 크게 제약을 받는다. 특히, 범인 검거 등 영상 추적이 필요할 경우에 취약하다는 특징이 있다. 한편, ROI 영역을 기반으로 하는 얼굴 영상 암호화 방법이 제안되어 있으며, 이는 영상 내의 특정 영역에 대해 암호화 혹은 스크램블 등으로 복호화가 가능한 형태로 처리하는 방법이다. 그러나, 이러한 방법은 암호 키가 노출될 경우에 얼굴 영상에 대한 복원이 가능하다는 위험이 있다. 특히, CCTV 영상을 클라우드 서버에 업로드시 복호화 키 관리에 대한 이슈사항도 존재한다.

또한 얼굴 영상에 대해 모자이크 혹은 블러 형태로 처리하여 프라이버시를 보호하는 방법이 존재하나, 이는 부분적 얼굴 윤곽이 일부 남아 있을 수 있으며, 향후 빅데이터 기술의 발전에 따라 흐릿한 영상에서 분석을 통하여 원본 이미지에 가깝게 복원이 될 수도 있다는 위험성이 존재한다. 마지막으로 얼굴 대체 혹은 합성 등을 통한 얼굴 비식별화 방식이 존재하며, 이는 얼굴의 형태를 변화시켜 개인의 프라이버시를 보호하는 방식이다. 그러나 이러한 방식은 필요시 얼굴 영상 복원이 되지 않는 것이 일반적이며, 정보공개 정도를 조절할 수 없다.

3. 영상감시 보안요구사항 도출

1) 영상 데이터 암호화

CCTV 카메라에서 영상을 촬영한 후, 영상감시 관제 서버로 촬영된 영상을 전

송할 경우 영상정보를 암호화된 형태로 안전하게 전송하여 종단간 보안성을 유지해야 한다. 또한, 영상감시 관제 서버는 수신된 영상을 보관할 경우 암호화/비식별화 처리를 통하여 프라이버시 노출이 발생하지 않도록 영상정보를 안전하게 보관하여야 한다. 모니터링 클라이언트를 통해 영상감시 관제 서버에 접근하는 경우에도 암호화 및 비식별화 조치를 통해 불필요한 개인정보 노출이 발생하지 않도록 하여야 한다.

2) 안전한 데이터 송수신

CCTV 카메라와 영상 감시 관제 서버, 영상_요청자와 클라이언트간 안전한 데이터 송수신이 이루어져야 한다. 이를 위하여, SSL 등을 활용하여 안전한 보안 채널 기반의 데이터 송수신이 필수적이며, 영상정보 전달 과정에서 기밀성 및 무결성을 유지한 상태에서 영상정보 전송이 이루어져야 한다. 또한, 영상정보 전달 시 도청, 위/변조 등의 공격에서도 안전하게 보호되어야 한다.

3) 안전한 영상 접근제어

영상정보에 접근시 안전한 영상 접근제어가 이루어져야 한다. 특히, 영상 감시 서버 접근 시 RBAC과 같은 높은 수준의 안전한 영상 접근제어 방안이 적용되어야 한다. 본 논문에서는 영상 객체 위험도 기반의 향상된 RBAC 적용 방안을 제안하고 있으며, 이러한 방안을 통하여 보다 안전한 영상 접근제어를 실현할 수 있다. 또한, CCTV 카메라, 연동 서버, 모니터링 클라이언트 등에 안전한 인증방식 적용이 필수적으로 요구되며, 안면 인식 기술 등 생체인식을 통한 안전한 인증이 필요하다.

한편, 프라이버시 보호를 위해 촬영된 영상정보는 마스킹 기법 적용 등을 통하여 개인정보가 침해되지 않도록 안전하게 관리되어야 한다.

V. 영상감시 보안 프레임워크 설계 제안

본 장에서는 본 논문에서 제안하는 기술적 영상 보안 감시환경 모델을 살펴보고, COP-변환 알고리즘과 이를 이용하여 지능형 영상감시 환경에서 CCTV 영상 데이터를 안전하게 보호할 수 있는 방법을 제안한다.

1. 영상감시 보안 프레임워크의 고려사항

1) 개요

최근 지능형 CCTV가 등장하면서 CCTV 영상 분석에 대한 관심이 증가하고 있다. 지능형 CCTV는 영상에 대하여 기존보다 더욱 많은 정보를 제공하며, 얼굴인식 뿐만 아니라, 객체의 행동 유형 등 다양하고 지능화된 분석이 가능하다. CCTV는 향후 도입될 지능치안 환경에 적합한 도구로 활용할 수 있으나 CCTV를 통한 불필요한 개인정보 수집은 최소화할 필요가 있다. 특히, 영상 데이터를 통계자료 제공 등에 활용할 경우는 얼굴 영상에 대한 적절한 비식별화 처리가 필요하며, 불필요한 개인정보를 식별할 수 없도록 기술적인 조치가 필요하다. 비식별화 처리는 정보주체를 식별하거나 식별할 수 있는 개인정보를 식별하지 못하도록 만드는 조치를 의미한다. 엄밀히, 비식별화는 암호화 방식과는 다르다. 영상 암호화 방식은 전체, 혹은 일부 영상만을 암호화하는 것으로서, 이는 암호화된 영역의 영상에 대한 정보를 전혀 식별할 수 없도록 하는 것이다. 비식별화는 이와는 차이가 있는 방법으로, 영상에 대한 일부의 정보는 식별이 가능하나, 촬영된 특정 개인이 누구인지 혹은 특정인의 개인정보를 유추할 수 없도록 하는 기술이라고 볼 수 있다.

대표적인 영상 비식별화 기술로는 얼굴 마스킹(Masking) 방식이 있다. 마스킹 방식은 개인이 식별되지 않도록 얼굴 영역에 해당하는 부분에 식별 불가능한 의미없는 픽셀로 대체하는 것이다. 이러한 마스킹 기반의 비식별화 방식은 현재 가장 많이 쓰고 있는 방식이다. 그러나, 이는 개인의 특징이 완전히 사라지게 되어 통계 등 일부정보 활용이 필요한 분야에 사용하기 어려우므로 엄밀한 관점에서는 일반적인 비식별화 방법과는 차이가 있다. 특히 예를들어 매장에 설치된

CCTV에 영상 암호화 처리를 하게 될 경우, 촬영된 손님 개인에 대한 성별, 대략적인 연령, 외국인 여부 등을 마스킹된 데이터를 기반으로는 전혀 식별할 수 없게 된다. 즉, CCTV 마스킹 기법을 통해서는 통계자료 분석 및 학술적 목적 등에 의한 적법한 제공이 필요시에도 사용이 어렵게 된다. 따라서, 불가피하게 통계작업이 필요한 경우는 마스킹하지 않은 원본 데이터로 분석해야 하는 문제점이 존재하며, 이러한 구조는 프라이버시 보호에 있어서 치명적인 결함을 가지고 있다.

2) 영상감시 환경의 고려사항

영상감시 환경이 보편화되며, CCTV가 IoT기기로 진화되고 있음에 따라, 보안에 대한 철저한 대비가 필요하다. 그러나 아직 영상감시 환경의 도입에는 각종 보안 위협이 도사리고 있다. 지능형 영상감시 환경이 효과적으로 도입되기 위해서는 우선적으로 몇 가지 문제를 해결할 필요가 있다. 이러한 해결과제는 다음과 같다.

- 가용성(Availability) : 엔드포인트와 각 서비스 간의 지속적 연결 보장
- 신원(Identity) : 서비스/엔드포인트를 운영하는 고객 또는 최종사용자 인증
- 개인정보(Privacy) : 개별 최종 사용자에게 피해를 줄 가능성을 감소
- 보안(Security) : 시스템 무결성을 확인, 추적 및 모니터링이 필요함

가) 가용성

엔드포인트 장치와 최종 사용자 및 백엔드 서비스간에는 지속적으로 통신이 가능하여야 한다. 이를 달성하기 위해서는 지속적인 연결을 가능하게 하는 새로운 기술을 설계해야 한다. 여기에는 몇 가지 고려사항이 있다. 예를 들어, 저전력 광역 통신망(LPWAN)이 현대의 셀룰러 시스템과 비슷한 수준의 보안으로 구현될 수 있어야 하고, CCTV 단말과 감시 서버간 강도높은 보안을 지원하여, 종단점간의 네트워크 신뢰가 확보되어야 한다.

나) 정보 접근자 신원 식별

영상감시 서비스 생태계 내에서 정보 접근자의 신원을 안전하게 식별할 수 있어야 한다. 지능형 영상감시 서비스에서 중요하고 기본적인 부분은 데이터가 누구에게 전달되고 있는지에 대한 부분이다. 정보와 서비스에 대한 안전한 접근을 위해, 몇 가지 고려사항이 필요하다. 여기에는 서비스상에서 최종 사용자의 신원을 확인하는 방법과, 가장 공격이 행해지는지 파악 가능 여부, 장치의 신원이 변조나 조작되었을 경우에 대한 부분 등이 있다.

다) 개인정보보호

영상감시 서비스에서 프라이버시 보호는 부가적인 기능이 아니라, 필수적으로 반영되어야 할 기능이다. 특히, 지능형 영상감시 환경에서는 물리적 공간이 사이버 공간과 직접적으로 영향을 받기 때문에, 프라이버시가 모든 행동이 허가되고 확인되더라도 행동 및 관련 메타데이터가 허가받지 않은 당사자에게 노출되지 않아야 한다. 이는 제품 또는 서비스에 대한 적절한 아키텍쳐를 정의해야만 달성이 가능하다. 여기에서 엔지니어가 가능한한 높은 수준의 보안성 확보를 통해 이러한 제품과 서비스를 유지하고 신체적 상해의 위험을 줄이며 개인 정보 관련 데이터를 노출하는 것이 중요하다. 따라서, 개인정보보호가 사용자 당사자 뿐 아니라, 영상감시 서비스에 미치는 영향에 대해 확인할 필요가 있다. 예를 들어, 엔드포인트의 신원은 권한이 없는 사용자에게 노출되는지, 영상감시 서비스 식별자로 최종 사용자 또는 종단점을 물리적으로 모니터링하거나 추적할 수 있는지, 영상감시 서비스에서 발생하는 데이터가 사용자에게 직접적인 물리적 속성과 연관이 되는지, 사용자별 개인식별정보를 어떻게 저장하고 처리하는지, 최종 사용자가 영상감시 서비스 또는 제품에서 개인식별정보의 저장 또는 사용을 제어할 수 있는지 여부이다.

라) 설계 단계에서의 보안

지난 수십년간 인터넷 보안이 크게 향상되었으나, 지능형 영상감시 환경에서는 다양한 공격 위협이 존재하므로, 방대한 사용자 그룹과 물리적 시스템에 위협

을 초래하지 않도록 엔드포인트와 지능형 영상감시 서비스 모두에서 정보보안에 대한 철저한 대비가 필요하다. 이는 기술적 뿐만 아니라, 정책적인 요소에도 해당된다. 예를 들어, 프로젝트 초기단계에서의 보안성 확인, 보안 수명주기 고려, 엔드포인트 또는 응용프로그램에서 보안상 이상 여부를 감지할 수 있는지, 예외사항에 대한 처리가 어떻게 되는지, 손상 후에 서비스 및 자원 복원이 가능한지 여부 등이다.

2. 영상감시 보안 프레임워크의 구성요소

1) CCTV 영상기기

CCTV 영상기기는 특정 공간에 설치된 촬영기기를 의미하며, 실제로 개인영상정보를 수집하는 역할을 한다. CCTV 영상기기를 통하여 촬영된 영상정보는 종단간 보안성이 확보된 보안 채널을 통하여 유무선상으로 안전하게 영상감시 서버로 전송된다.

2) 영상감시 서버

영상감시 서버는 CCTV 영상기기로부터 수신한 영상정보를 저장하고, 수집된 영상정보에 대한 안전한 관리 기능을 제공하며, 필요시 모니터링 클라이언트를 통한 영상정보 모니터링 측에 영상정보를 제공한다. 실질적으로 영상정보가 저장되는 곳은 클라우드 서버이며 영상정보는 암호화 및 마스킹된 상태로 저장된다. 영상감시 서버는 클라우드 서버에 저장된 영상정보를 안전하게 관리하는 역할을 수행한다.

3) 클라우드 서버

실제 CCTV 데이터는 클라우드 서버에 저장된다. 클라우드 서버는 클라우드 스토리지 역할을 담당하며, 영상감시로부터 비식별화, 암호화된 데이터가 클라우

드 서버에 저장된다. 여기에서, 클라우드 서버는 관리자에 의해 항시 노출될 수 있다는 것을 가정하고, 이에 대한 보안 조치를 충분히 취한 뒤 데이터를 저장할 필요가 있다.

4) 클라이언트

CCTV 영상에 대한 모니터링이 필요한 사용자에 의해 조작되는 클라이언트로써, PC, 노트북, 모바일 등에 설치된 클라이언트 어플리케이션을 의미한다. 클라이언트는 영상감시 서버로부터 적절한 접근제어 및 인증을 거친 뒤 영상정보를 수신하고, 사용자에게 영상을 제공한다.

3. 프레임워크 모델링

1) 영상보안 감시환경 모델

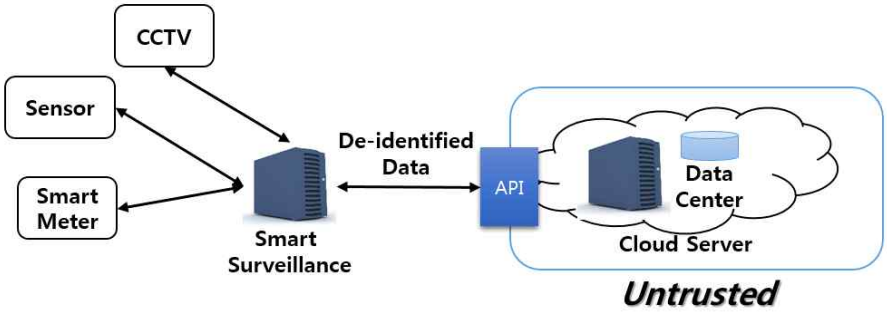
지능형 감시 기술이 대중화되면서 데이터 저장공간, 가용성 등 여러 이유로 인하여 스마트 감시가 클라우드 환경과 접목되고 있다.

아래 그림에서는 클라우드 환경에서의 스마트 감시 서비스 제공 모델을 나타낸다. 여기에서 스마트 감시 서비스 제공자는 신뢰된 구간 내에 속해 있다. 그러나, 실제 데이터는 신뢰된 구간 밖의 클라우드 데이터베이스에 저장되어 있다. 서비스 제공자는 클라우드 서버간 API 통신을 수행하여 클라우드 서버 내의 데이터에 대한 다양한 처리를 수행한다.

이러한 클라우드 환경에서는 CCTV 추적정보, 센싱 데이터, 미터링 데이터 등의 스마트 감시에서 수집된 개인정보가 신뢰된 영역이 아닌 외부에 존재하게 된다. 여기에서 클라우드 서비스는 신뢰되지 않은 영역으로 간주된다. 클라우드에 저장된 데이터의 다양한 보안 위협, 내부자에 의한 데이터 누출 등 여러 위험이 존재할 수 있기 때문이다..

이러한 점은 개인정보에 대한 직접적인 위협요소로 작용한다. 따라서, 데이터를 클라우드 서버상의 데이터베이스에 보관시에는 적절한 방법을 통해 데이터를 보호할 필요가 있다. 즉, 서비스 제공자가 클라우드상에 데이터를 보관 시에는

비식별화한 상태로 보관하며, 평문으로의 복원은 클라우드 서버로부터 데이터를 가져온 이후에 신뢰된 구간 내에서 처리하는 방법이 안전하다.



<그림 V-1> 영상감시 서비스 모델

물론 가장 안전한 것은 데이터베이스에 있는 값 전체를 암호화하는 것이다. 그러나, 이러한 경우는 데이터베이스의 효율을 심각하게 떨어뜨리고, 실제로 가용성을 기대할 수 없는 상태가 된다. 한편, 가용성을 위해서 평문을 그대로 저장하는 것도 큰 문제가 된다. 개인을 식별할 수 있는 정보가 그대로 노출되는 것이나 마찬가지이기 때문이다.

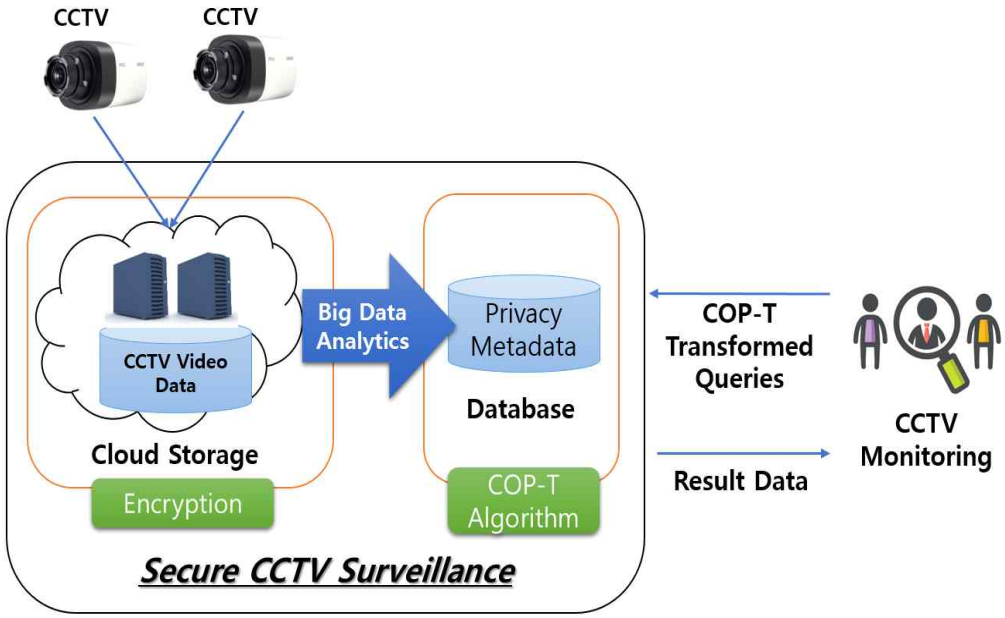
따라서 일반적으로 강한 수준의 안전이 요구되는 주요 필드에 대해서는 암호화를 수행하고 있다. 그러나, 암호화된 해당 필드는 인덱스를 구성할 수 없고, 범위검색, 전방일치 검색, 집계질의가 되지 않는다는 문제가 존재한다. 이러한 특성은 암호화된 필드의 경우에는 통계처리가 불가능하게 만든다.

지능형 감시 환경의 경우, CCTV 추적정보, 센싱데이터 및 미터링 데이터 등을 집계처리함에 있어 순서보존 암호화 등의 보완책을 고려해 볼 수 있으나, 이는 순서보존 암호화의 특성상 데이터의 분석이 암호화된 상태 그대로 가능하다는 점에서 해결책이 될 수는 없다. 따라서, 스마트 감시 데이터 특성에 적합한 별도의 비식별화 방법이 필요하다. 비식별화의 큰 장점은 비식별화된 상태 그대로 통계처리가 가능하다는 것이며, 데이터를 기반으로 개인정보의 추적이 어렵다는 특성이 있다. 본 논문에서는 이러한 점을 고려하여 감시 데이터를 비식별화하여 개인의 메타데이터를 분석하기 어렵도록 변경하는 방법에 대하여 제안하고자 한다.

2) 영상데이터 보안모델

아래 그림은 본 논문에서 나타내는 영상 보안 감시환경을 나타낸다. 본 모델에서 CCTV는 실시간 영상을 촬영하여 클라우드 스토리지에 영상을 저장한다. 여기에서, 감시 시스템의 클라우드 스토리지에서는 해당 영상을 암호화하여 저장한다. 한편, CCTV 영상은 빅데이터 기반으로 실시간 메타정보가 추출되며, 메타정보는 본 논문에서 제안하는 COP-변환 알고리즘을 사용하여 저장한다. 이 과정에서, 데이터는 어떤 경우에도 평문으로 저장되지 않는다.

권한이 있는 CCTV 감시자는 CCTV 감시 시스템으로부터 영상 데이터를 수집하고 확인한다. 이 경우, COP-변환 메타데이터를 기반으로 비디오 영상에 대한 직접 질의가 가능하며, 권한이 있는 감시자는 이를 기반으로 원하는 영상을 검색하여 가져올 수 있다. 예를 들어 '오후 10시경 A 지역에 John 이 있는 영상은?' 이라는 방식의 질의를 통한 영상 검색이 가능하다. CCTV 메타정보는 일종의 개인정보로서, 평문으로 저장되면 보안상 큰 취약점이 존재한다. 따라서, 본 논문에서 제안한 COP-변환 기법을 이용하여 변환된 메타데이터로 저장한다.



<그림 V-2> 영상데이터 보안 모델

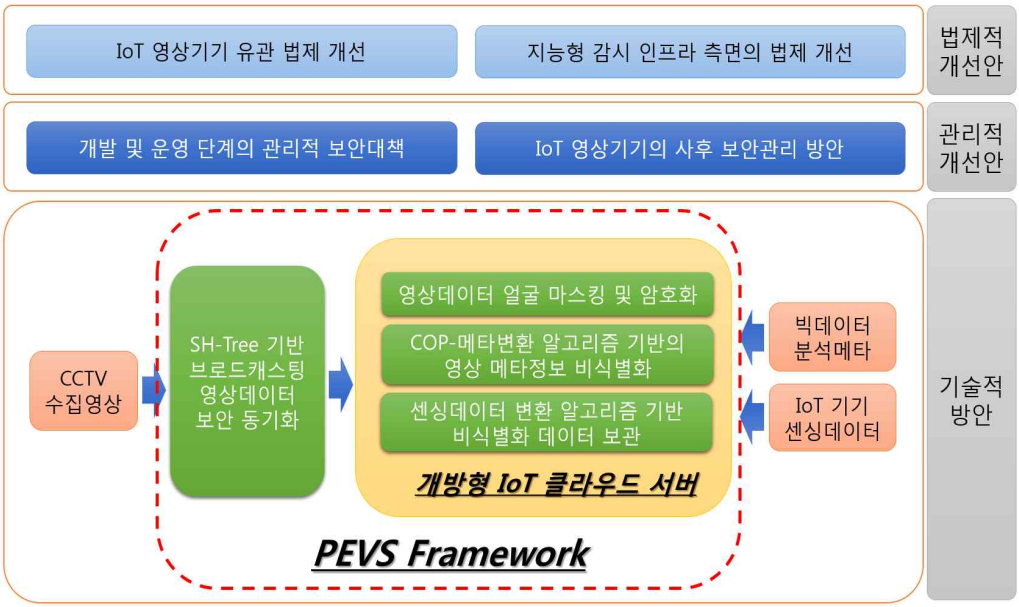
이러한 경우, 평문 메타정보 및 평문 CCTV 영상 비디오 데이터는 CCTV 감시 환경에 남지 않게 되어, CCTV 영상데이터에 대한 프라이버시 보장이 가능하

다. 즉, 공격자가 CCTV 감시 환경의 전산망에 해킹을 시도하여 비디오 영상정보 및 메타데이터의 탈취를 시도하여 실질적으로 영상정보 및 메타정보를 획득했다고 하더라도, 평문정보를 복원할 수 없다. 이러한 특성은 CCTV 감시 시스템 관련 운영업체 등 내부자에 의한 공격도 방지할 수 있다는 장점이 있다. 권한이 있는 감시자에 한해서 정상적인 방법으로 COP-변환 질의를 통하여 찾고자 하는 영상데이터를 정상적으로 가져올 수 있으며, 권한이 없는 접근자는 원본 데이터를 알아낼 수 없다.

4. 영상감시 보안 프레임워크 아키텍처

1) 프레임워크의 범위

PEVS 프레임워크 아키텍처는 아래 그림과 같다. PEVS 프레임워크는 본 논문에서 제안한 기술적, 관리적, 법제적 개선방안 가운데 기술적 부분에 대한 내용을 지칭한다. 개방형 IoT 클라우드 서버는 CCTV 장치로부터 영상데이터를 수집하고, 해당 영상 데이터를 빅데이터 기반으로 분석하여 실시간 영상 메타 데이터를 생성한다. 또한, IoT 기기로부터 다양한 센싱데이터를 처리하게 되며, 이 과정에서 영상 객체의 다양한 개인정보 침해가 발생할 수 있다.

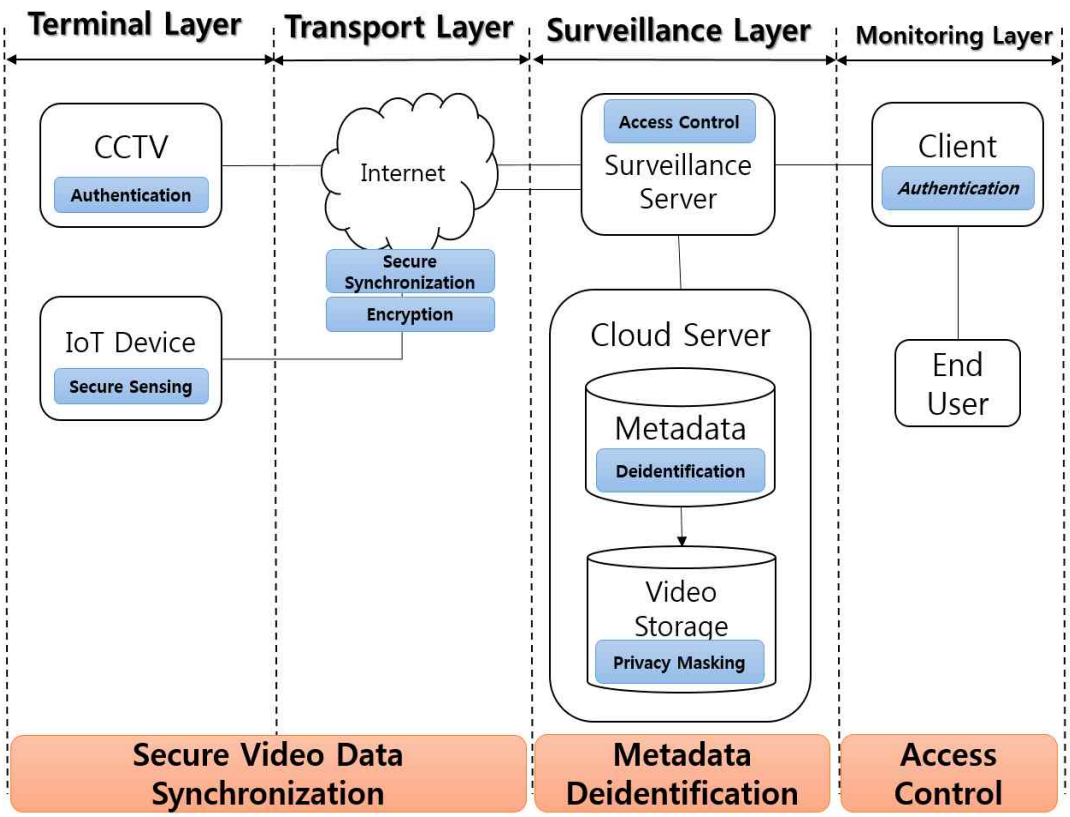


<그림 V-3> PEVS 프레임워크의 범위

PEVS 프레임워크는 개인영상정보에 대하여 얼굴 마스킹 및 암호화 처리, COP-메타변환 알고리즘 기반의 영상 메타정보 비식별화 처리, 센싱데이터 변환 알고리즘 기반의 비식별화된 형태의 데이터로 보관함으로써 개인영상 데이터의 프라이버시를 보장한다. 또한, 본 논문에서 제안한 SH-Tree 기반의 브로드캐스팅 영상데이터 보안 동기화 기법을 통하여 CCTV에서 수집되는 영상데이터 전송시의 무결성, 기밀성, 가용성을 보장한다.

2) 영상감시 프레임워크 아키텍처

PEVS 프레임워크 아키텍처는 아래 그림과 같다. PEVS 프레임워크는 단말계층(Terminal Layer), 전송 계층(Transport Layer), 감시 계층(Surveillance Layer), 모니터링 계층(Monitoring Layer)으로 나뉜다.



<그림 V-4> PEVS 프레임워크 아키텍처

단말 계층에서 CCTV나 IoT 단말을 통하여 영상이나 센싱정보 등을 수집하고, 전송 계층에서는 종단간 암호화를 사용하여, 안전하게 감시 계층에 전달한다. 감시 계층에서는 CCTV 데이터에 대한 비식별화, 메타정보 마스킹을 이용하여 데이터를 안전하게 보관/저장하고, 모니터링 계층에서는 실제 사용자가 감시 서버에 영상정보를 요청할때 인증, 접근제어 등 적절한 보안 기능을 수행하여 사용자에 대한 권한을 확인한 후 감시 서버에 접근하여 영상정보를 가져올 수 있다.

(1) 단말 계층(Terminal Layer)

단말 계층에서는 CCTV, IoT 장치 등에서 영상정보를 수집한다. 실질적으로 개인정보가 최초로 수집되는 계층이므로, 이 과정에서도 안전한 보안 방식의 적용이 필요하다. CCTV는 외부에서 인가되지 않은자가 접근되지 않도록 안전한 인증방식을 사용하여야 하고, IoT 장치는 센서 데이터를 비식별화 방식으로 안전하게 보호하여야 한다.

(2) 전송 계층(Transport Layer)

수집한 정보는 전송계층에서 종단간 암호화가 적용되어야 한다. 특히, 유/무선 인터넷에서의 공격자에 대한 정보 노출이 발생 가능한 점을 고려할 때, 안전한 종단간 암호화 기법이 필요하다. 한편, 공격자가 메시지 위/변조 공격을 수행할 수 있으므로, 무결성을 보장하는 프로토콜 또한 필요하다. 본 논문에서 제공하는 보안 동기화 기법은 영상 데이터의 무결성을 보장하며, 메시지 변조공격 등이 발생하더라도 변경 여부를 확인하고 정상적인 데이터로 재수신하는 방식으로 무결성을 보장한다.

(3) 감시 계층(Surveillance Layer)

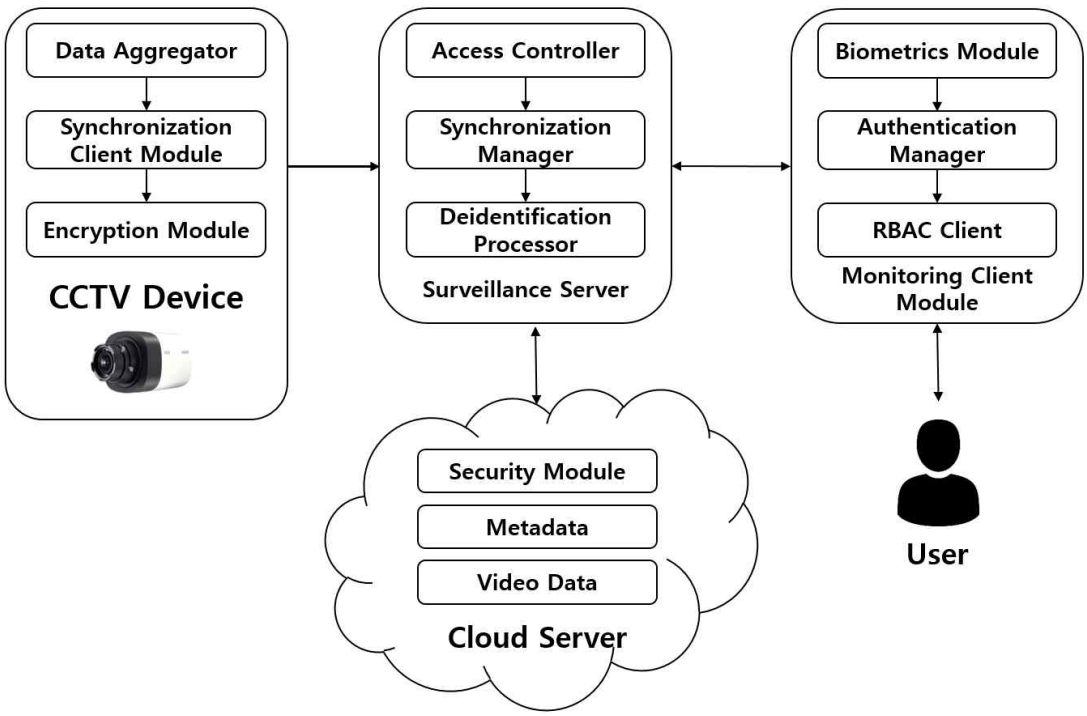
감시 계층은 실질적으로 개인정보에 있어 가장 중요한 영역이며, 여기에는 영상감시 서버와 클라우드 서버가 포함된다. 클라우드 서버는 메타정보를 포함하고

있으며, 영상데이터와 메타정보를 평문으로 보관하면 내부자 공격 등 다양한 개인정보 침해가 발생할 수 있으므로, 메타정보 비식별화 기법 등 다양한 보안 방식을 동원하여 데이터를 안전하게 저장할 수 있어야 한다. 한편, RBAC기반의 안전한 접근제어가 지원되어야 하며, 클라이언트로 부터 영상정보 제공 요청이 왔을경우, 클라이언트의 권한을 고려하여 영상정보를 얼마나 공개할 것인지를 결정하고 최소한의 개인정보를 공개하여야 한다.

(4) 모니터링 계층(Monitoring Layer)

사용자는 모니터링 계층을 통하여 영상정보에 접근한다. 여기에서 안전한 사용자 인증이 필요하며, 사용자의 역할에 따른 정보 접근제어가 필요하다. 개인정보를 불필요하게 많이 제공하여서는 안되며, 정보 접근자의 목적에 맞는 최소한의 개인영상정보를 제공하여야 한다.

3) 영상감시 기능 단위 구성



<그림 V-5> 영상감시 기능단위 구성도

위의 그림은 영상감시 기능단위 구성도를 나타내고 있다. 영상감시는 CCTV 장치(CCTV Device), 감시 서버(Surveillance Server), 클라우드 서버(Cloud Server), 모니터링 클라이언트(Monitoring Client)로 이루어진다. 여기서는 해당 구성의 세부 기능을 설명한다.

(1) CCTV Device

CCTV 장치는 CCTV 영상 데이터 수집을 위한 Data Aggregator와 감시 서버와의 동기화 통신을 위한 Synchronization Client Module, 통신 과정에서의 암호화를 위한 Encryption Server로 구성되어 있다. CCTV에서 수집된 정보는 암호화되어 전송될 필요가 있으며, 메시지 변경이 없이 안전하게 전송되어야 한다.

(2) Surveillance Server

감시 서버는 실질적으로 CCTV와 클라우드 서버의 매개 역할을 함과 동시에, 실제 감시 보안에 필요한 여러 기능을 수행하고 있다. Access Controller는 RBAC 기반의 접근제어를 수행하며, Synchronization Manager는 보안 동기화 시 무결성 확인, 변경 데이터 검출 기능 등을 수행한다. Deidentification Manager는 데이터에 대한 비식별화 기능을 수행한다. 실제로 비식별화된 데이터는 클라우드 서버에 저장된다.

(3) Cloud Server

클라우드 서버는 기본적으로 메타데이터와 실제 CCTV에서 촬영된 비디오 데이터가 저장된다. 여기에서, 메타데이터와 비디오 데이터는 암호화 및 비식별화되어 보관되어야 하며, 일반 평문 상태로 저장하면 보안상 큰 위험이 노출될 수 있음에 주의하여야 한다. 따라서, 클라우드 서버에도 자체적인 기본 보안 모듈이 제공되어야 하며, 본 논문에서 제안된 비식별화 알고리즘 뿐만 아니라, 자체적인 추가 보안 장치를 제공하여 이중의 보안 기능을 확보하여 안전성을 제공할 필요가 있다.

(4) Monitoring Client

정보 제공 시 모니터링 클라이언트를 통하여 제공한다. 여기에서 클라이언트는 안전한 인증을 위해 생체인증을 제공하여야 하며, 얼굴인식 등 보안에 필요한 조치를 수행할 수 있어야 한다. 또한, 서버에서 제공하는 RBAC 기능에 따라, 접근 권한에 따른 클라이언트 자체적인 불법 접근 방지 대책도 갖추어야 한다.

5. 세부절차 및 프로토콜 설계

1) COP-메타변환 알고리즘 설계

(1) 알고리즘 설계 개요

메타변환 알고리즘 설명을 위한 약어는 아래 표와 같다.

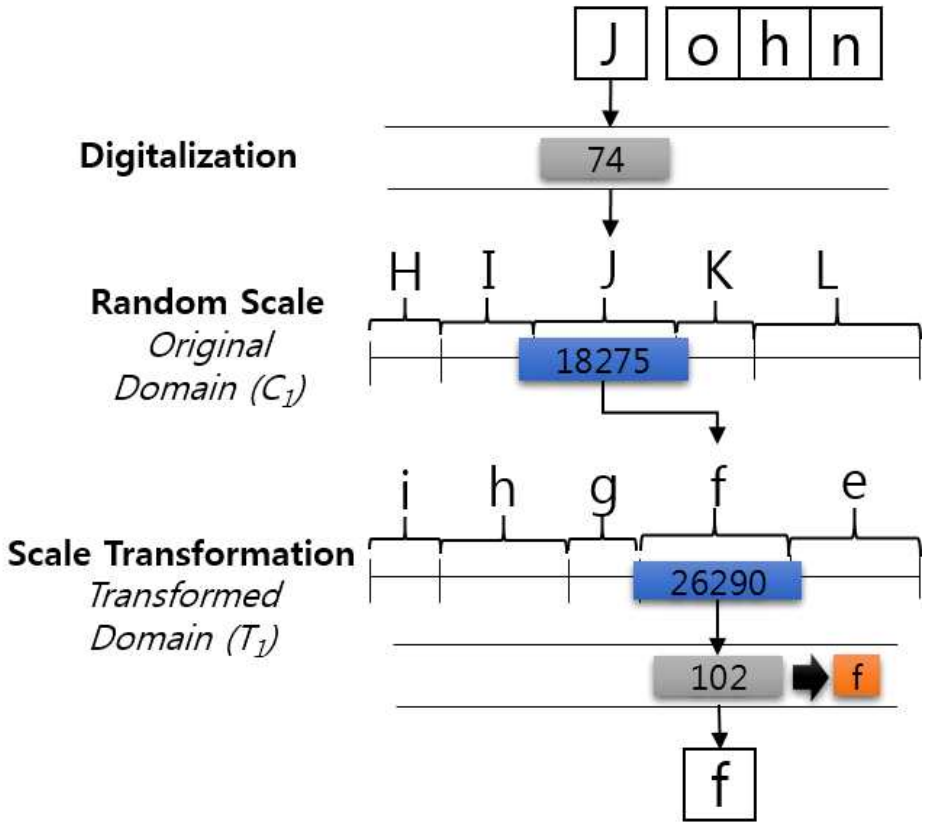
<표 V-1> 메타변환 알고리즘 약어

Abbreviation	Content
D	Pre-shared Initial Seed
C_i	i-th Character of C
P_i	i-th Random Scale Value
R_i	i-th Pseudorandom Number
$DIG(\cdot)$	Result of Digitalization
$CHR(\cdot)$	Result of Characterization
$PRNG(\cdot)^s$	Pseudorandom Number Generation
T_i	i-th COP-Transformation Value
x	The Last Element of Domain

COP 변환방식은 원본 문자열을 변환식을 이용하여 변환된 문자로 치환하는 기법으로, 문자열을 구성하는 단일 문자 단위로 변환 문자로의 치환을 수행한다. 여기에는 다음과 같은 특징이 존재한다. 특정 문자열의 도메인과 변환된 문자열의 도메인은 각각 정렬 순서를 가지고 있다. 그러나 변환된 문자열 도메인의 정렬 순서는 평문과 반드시 동일한 순서를 따르지는 않으며, 아래와 같은 연산에 의해 결정된다.

$$C_i < C_z \rightarrow \begin{cases} \text{if } u \bmod 2 = 0 & T_i \leq T_z \\ otherwise & T_i \geq T_z \end{cases}$$

아래 그림은 COP 변환기법을 간단히 도식화하고, COP-변환 알고리즘을 나타내고 있다. COP 변환기법은 단일 문자에 대한 수치화 단계, 의사난수를 기반으로 한 문자 도메인 기반 랜덤 측정 값을 연산하는 랜덤 스케일 단계, 랜덤 측정 값을 새로운 측정값으로 변환하고 해당 스케일 변환값을 문자로 변환하는 스케일 변환 단계로 구성된다.



<그림 V-6> COP-메타변환 알고리즘

Algorithm : COP-Transformation

While i≥n do
  A_i = DIG(C_i)
  $s=R_{i-1} + D$
  $R_i = PRNG(i)^s$
  $P_i = \sum_{k=1}^{A_i} R_k$
  j=0, u=0
  while u≤P_i do
    $M_j = PRNG(j)_{s+1}$
    u = M_j + u
    j=j+1
  end
  if (u mod 2) = 0 then
    T_i = CHR(j)
  else
    T_i = CHR(DIG(x) - j)
  endif
  i=i+1
end

<그림 Ⅴ-7> COP-메타변환 알고리즘 세부절차

(2) 알고리즘 세부설계

① 수치화(Digitalization) 단계

COP-변환기법은 원본 문자열에서의 단일 문자 단위로 치환 과정이 이루어진다. 여기에서, 먼저 단일 문자는 사전 정의된 매핑테이블에 근거하여 특정 숫자로 변환한다. 가장 간단한 방법으로, 아스키코드로 치환하는 경우를 생각해 볼 수 있다. 여기에서 아스키코드는 문자, 숫자, 특수문자를 모두 포함한다는 특성을 가지고 있다. 입력 문자에 따른 연산 결과 문자가 변환되어 출력되는 캐릭터 셋 영역은 매핑 테이블에서 정의되어 있는 전체 영역에서 발생할 수 있다. 따라서, 아스키코드를 매핑테이블로 정할 경우는 원본이 일반적인 숫자 및 문자만으로 구성되었다고 하더라도 COP-변환 결과값에는 특수문자가 포함될 것이다. 즉, 수치화 단계에서의 매핑테이블은 일반적인 아스키코드로 적용하더라도 연산에 문제는 없으나, 결과값에 특수문자를 포함하여 출력될 수 있다.

Table 6: ASCII Table

Char	Binary	Char	Binary	Char	Binary	Char	Binary
(nul)	00000000	(sp)	00100000	@	01000001	‘	01100001
(soh)	00000001	!	00100001	A	01000010	a	01100010
(stx)	00000010	”	00100010	B	01000011	b	01100011
(etx)	00000011	#	00100011	C	01000100	c	01100100
(eot)	00000100	$	00100100	D	01000101	d	01100101
(enq)	00000101	%	00100101	E	01000110	e	01100110

<그림 V-8> ASCII 기반 매핑 테이블

② 랜덤 스케일(Random Scale) 단계

이 단계에서는 수치화 단계에서 생성된 수치에 대응하는 랜덤 스케일 값을 측정한다. 이를 위해 먼저 의사난수의 seed 값을 결정한다. 의사난수의 초기 seed는 사전 분배된 D값으로 정하며, 최초 단일 문자 변환 이후 Ri의 연산에 필요한 seed는 Ri-1의 값을 취한다. 원본 문자열에서의 i번째 문자에 대응하는 랜덤 스케일값 Pi는 아래의 식으로 구할 수 있다.

$$P_i = \sum_{k=1}^{A_i} PRNG(i)^s$$

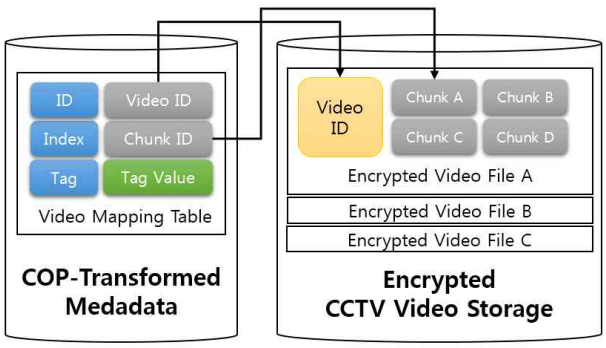
③ 스케일 변환(Scale Transformation) 단계

이 단계는 앞서 랜덤 스케일 단계에서 생성한 Pi값을 기반으로 새로운 매핑 숫자값을 연산하는 단계이다. 여기에서는 앞서 연산한 seed에서 1을 더한 결과를 이 단계에서의 seed로 정한다. 이후, 해당 seed를 기반으로 발생된 의사난수의 전체 합계가 랜덤 스케일 단계의 결과값인 Pi가 될때까지 반복하여 생성하고 해당 횟수를 카운팅한다.

이 결과에 의해 연산된 반복 횟수는 최종 결과값의 문자를 얻기 위한 매핑테이블에 대한 입력값이 될 것이다. 스케일 변환에서의 seed는 앞서 언급한 랜덤 스케일 단계에서의 seed와 다르게 적용되었으므로 최초 수치화된 결과값과 여기서 발생된 결과값은 서로 상이하다. 이 결과값을 앞서 수치화 단계에서의 매핑테이블을 역으로 적용하여 특정 문자로 치환하는 것으로 최종 변환된 결과값을 구할 수 있다. 앞서 언급한 단계를 문자열이 끝날때까지 반복하여, 전체 문자열에 대응하는 COP-변환 문자열을 구할 수 있다.

(3) CCTV 영상 데이터 매핑 구조

CCTV 영상은 스토리지에 암호화되어 저장된다. 암호화 알고리즘으로 AES 등 대칭키 암호화 알고리즘이 사용될 수 있으며, 암호화된 비디오 파일은 파일 단위로 Video ID가 부여되고, 하나의 비디오 파일은 세부적으로 여러 파일로 분할하여 각각 Chunk ID를 가지게 된다. CCTV 영상 파일은 대용량이라는 특성을 가지고 있어, 특정 비디오 영상 파일 내에는 별도로 다수의 Chunk 영역을 분할하여 가지고 있어야 한다. 예를 들어, John이 출현한 CCTV 영상파일 목록을 찾고자 할때, 특정 날짜에 촬영된 전체 파일을 복호화하여 찾게 된다면 효율성을 크게 떨어뜨릴 수 있다. 이 경우, 각 영상 파일에 John이 나타난 세부적인 Chunk 목록을 확보할 수 있다면, 해당 부분 파일에 대한 복호화만 수행하면 되므로 영상 복호화의 효율성에 있어 큰 이점을 가질 수 있다. 따라서, 본 논문에서는 영상 데이터를 세부적인 Chunk 파일로 분할하여 별도로 암호화하여 보관하는 구조를 제안한다. 이 경우, Tag 정보에 대한 검색에 따라, 해당 정보에 매칭되는 Video ID 및 Chunk ID를 확보하여, 해당 Chunk ID에 대응하는 파일의 일부만 복호화를 할 수 있어 성능상 효율성을 가져올 수 있다. 이 과정에서 CCTV 비디오 파일만 암호화가 되어 있고, 메타데이터를 평문으로 저장할 경우는 메타데이터 그 자체만으로 비디오 파일의 내용을 상세히 노출하고 있으므로 프라이버시 보호에 큰 문제가 될 수 있다. 따라서, 본 논문에서는 CCTV 영상을 암호화함과 동시에, 영상메타도 COP-변환값으로 저장하여 메타DB 및 스토리지상 어느곳에도 평문을 저장하지 않으므로 영상객체의 개인정보를 보호할 수 있다. 아래 그림은 영상 메타데이터와 실제 영상정보 간의 매핑 구조를 나타낸다.



<그림 V-9> 영상 데이터 매핑 구조

(4) COP 변환메타 질의 기법

COP-변환기법으로 변환된 메타값은 데이터베이스상에 평문이 아닌 변환메타로 입력된 상태에서도 메타데이터에 대한 직접 질의가 가능하다는 장점이 있다. COP-변환 데이터는 직접적으로 전방일치 및 범위검색 뿐만 아니라 통계를 위한 집계검색이 가능하다는 특징이 있다. 또한, 데이터베이스 인덱스 구성을 그대로 활용할 수 있다는 장점이 있다. 실질적으로 암호화된 데이터베이스는 일치검색 질의 이외에의 전방일치, 범위검색 등에 인덱스 사용이 불가능하여 데이터베이스의 효율을 크게 저하시키는 원인이 된다. 그러나 COP-변환 기법은 데이터베이스 질의시 인덱스 이용이 가능하여 평문 상태에서 질의하는 것과 효율성에서 차이가 없다고 볼 수 있으므로, 평문 데이터를 노출하지 않으면서 DB 질의 과정에서도 성능의 향상을 가져올 수 있다는 큰 장점이 있다.

Original Query :

select video_id, video_idx
from metadata
where tag $> C_a$ *and tag* $< C_z$

Transformed Query :

select video_id, video_idx
from metadata

$$\begin{cases} \text{if } u_a \bmod 2 = 0 & \textit{where tag} \le T_a \\ \textit{otherwise} & \textit{where tag} \ge T_a \end{cases}$$

$$\begin{cases} \text{if } u_z \bmod 2 = 0 & \text{and } \textit{tag} \ge T_z \\ \textit{otherwise} & \text{and } \textit{tag} \le T_z \end{cases}$$

<그림 V-10> COP 변환 SQL 질의구조

위의 그림은 통상적인 SQL 범위검색 질의를 COP-변환 질의로 변경하는 방법을 나타낸다. COP 변환 값은 평문의 순서를 평문, 혹은 역순으로 랜덤하게 저장하고 있으며, 이는 COP 변환 과정에서의 스케일 변환(Scale Transformation) 단계의 결과값인 u 값을 기준으로 결정한다. 즉, u 값에 대한 mod 연산에 대한 결과값에 따라 범위검색시 대소 구분이 달라진다는 특징이 있다. 만약, 적합한 권한을 가지고 있지 않은 해커 등 공격자의 경우는 사전 공유된 D값 및 의사난

수의 seed값인 s를 알지 못하므로 Ca 및 Cz의 값을 알고 있다 하더라도 Ta 및 Tz 값을 생성할 수 없으므로 변환 쿼리를 구성할 수 없다.

2) 메타데이터 비식별화 처리절차

(1) 메타데이터 비식별화 개요

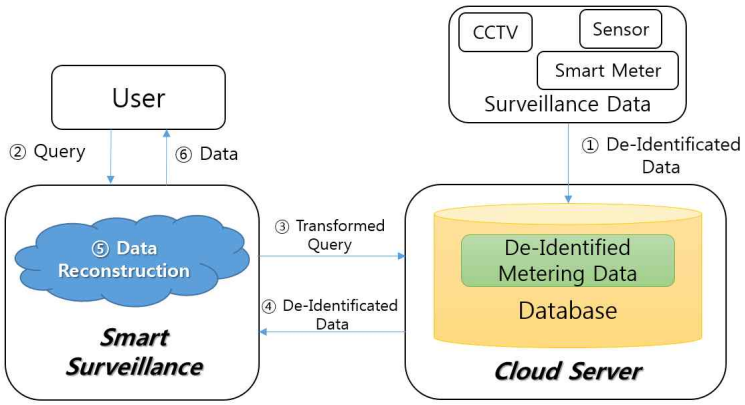
지능형 감시 환경은 향후 취급해야 할 데이터 증가가 예상됨으로 인하여 앞으로 클라우드 환경을 도입할 가능성이 크다. 그러나, 클라우드 환경을 도입하기에 앞서 보안에 대한 고려가 반드시 필요하다. 보안이 없이는 서비스의 활성화도 기대할 수 없을 뿐더러, 개인정보의 침해로 인해 여러가지 큰 이슈가 발생할 수 있으며, 큰 재앙으로 이어질 수도 있다. 특히, CCTV 추적 데이터, 헬스케어 등 개인 센싱 데이터, 스마트 미터링 데이터는 개인의 사생활 에 대한 각종 정보를 노출하고 있으므로 신뢰되지 않은 클라우드 환경을 도입한다면 반드시 비식별화가 필요하다. 따라서 본 절에서는 안전한 지능형 감시 환경을 위하여 감시 데이터에 대한 비식별화 기법을 제안한다. 먼저, 센싱데이터 비식별화 알고리즘의 설명을 위해, 약어를 아래 표에 제시한다.

<표 V-2> 센싱데이터 비식별화 방식 약어

Abbreviation	Content
s	의사난수 초기 seed
P_n^s	n번째 의사난수 값
GID_n	n번째 그룹 아이디
G_n	n번째 그룹
$H(\cdot)$	해쉬한 결과값
K	신뢰된 영역간 사전 공유된 암호화 키
$E(\cdot)^K$	K를 키로 암호화한 결과값
DT_n	n번째 시간값

아래 그림에서는 센싱데이터 비식별화 방식의 대략적인 개념을 나타낸다. 클라우드 서버에는 스마트 감시 데이터가 저장된다. 여기에는 수집된 감시 데이터의 내역이 시간대별로 존재한다. 만약, 비식별화가 이루어지지 않은 경우에는 감시 데이터가 그대로 클라우드 서버상에 저장될 것이다. 그러나, 본 논문에서 제

안한 방식을 기반으로 적절한 방식의 비식별화를 적용하면 클라우드 서버상에 저장되어 있는 정보만으로는 구체적으로 특정 개인의 상태에 대해 파악하기 어렵다. 이러한 원본 측정 데이터는 신뢰된 서버를 통해서만 가져올 수 있다. 신뢰된 서버는 클라우드 서버의 데이터베이스에 대한 질의를 통하여 비식별화된 데이터를 가져오고, 이에 대한 원본 데이터를 복원한다. 이러한 신뢰 서버를 기반으로 사용자는 원본 데이터에 대한 획득이 가능하며, 신뢰 서버는 쿼리 변환을 통해 집계검색 질의문을 구성할 수 있어 통계 처리도 가능하다. 또한, 이 과정에서 신뢰된 서버와 클라우드 서버 간 전달되는 질의문 및 질의에 대한 결과값이 중간자공격 등에 의하여 노출이 발생하더라도 원본데이터로 복원할 수 없어 안전하다.



<그림 V-11> 센싱데이터 비식별화 처리 모델

한편, 제안 방식에서는 신뢰된 서버는 안전한 영역으로 가정하고 있다. 따라서, 클라우드 서버와 신뢰된 서버 간에는 대칭키와 의사난수를 공유하고 있으며, 신뢰된 서버에 한해서는 특정 가입자에 대한 질의 및 복원이 가능하다. 따라서, 신뢰된 서버는 비밀정보를 안전하게 관리해야 할 의무를 갖는다.

전체적인 동작 절차는 아래와 같다.

① 감시 데이터는 실시간으로 비식별화되어 클라우드 서버에 보관된다.

② 사용자의 클라이언트 측에서는 신뢰된 서비스 제공자(신뢰 서버)에게 데이터를 질의한다.

③ 신뢰된 서비스는 질의문을 변환하여 재구성한다.

④ 신뢰 서버 측에서는 변경된 감시 데이터를 가져올 수 있도록 변환된 질의

문으로 클라우드 서비스 측의 데이터베이스에 질의한다.

⑤ 클라우드 서비스는 비식별화된 데이터 상태 그대로 신뢰 서버에 리턴한다.

⑥ 신뢰서버는 데이터에 대한 재식별화를 수행한다.

⑦ 재식별화된 데이터를 사용자 측에 전달한다.

(2) 세부 절차

① 시간 정보 암호화 및 그룹화 단계

감시 데이터에서 개인정보 노출 관점에서 유의미한 정보는 시간정보와 그에 매핑되는 측정 값이다. 반대로, 감시 데이터를 분석하려면 시간 정보에 기반한 분석이 필요하다. 다시 말해, 시간 정보를 알지 못하면 감시 데이터 자체만으로는 의미있는 정보 조합이 어렵게 된다. 따라서, 본 논문에서는 이러한 시간 정보를 암호화하여 저장하도록 한다.

그러나 시간 정보를 암호화하게 되면 시간 정보를 기준으로 범위검색을 수행할 수 없다. 암호화를 수행하면 평문과는 정렬순서가 완전히 달라지므로, 범위검색시 리턴되는 값은 의미가 없게 된다. 즉, 특정 시간 사이에 발생한 감시 데이터에 대한 질의문을 구성하기가 매우 어려워진다. 만약 데이터베이스의 모든 레코드에 대한 질의를 수행한다면 오버헤드가 매우 커지게 될 것이다.

이러한 문제를 해결하는데 시간단위 그룹화 방법을 사용한다. 즉, 인접한 여러 시간의 데이터를 하나의 단위로 묶어서 그룹으로 한다. 단, 여기에서 그룹내 데이터의 개수가 균일한 경우는 데이터 분석 공격으로 해당 기간 동안의 전력 사용량이 얼마인지를 분석하여 해당 시간대가 얼마인지에 대한 정보에 대한 대략적인 추정이 가능하다. 이러한 위험을 방지하기 위해, 그룹내 데이터 개수를 랜덤하게 설정한다. 이러한 데이터 개수는 의사난수를 기반으로 결정할 수 있으며, 여기서, 특정 그룹에 대한 사이즈(해당 그룹이 가진 데이터 개수) 값을 다음과 같이 정한다. 초기 seed와 n의 합, 즉, s+n을 seed로 정하고 이를 s'로 정한다. 이후, P_n^s‘의 결과값으로 그룹의 사이즈를 결정할 수 있다.

n번째의 그룹 아이디인 GID_n은 아래와 같은 식으로 구할 수 있다.

$$GID_n = H(\sum_{i=1}^{n} P_i^s)$$

GID_n을 구하기 위해서는 seed를 구체적으로 알고 있어야 한다. seed와 K는 신뢰된 영역간에 사전 공유하고 있는 값이며, 이러한 사전 정보를 알고 있지 않은 공격자는 정확한 GID_n을 생성할 수 없다. 아래 그림에서는 그룹 아이디가 추가되고, 시간값이 암호화된 상태를 나타낸다.

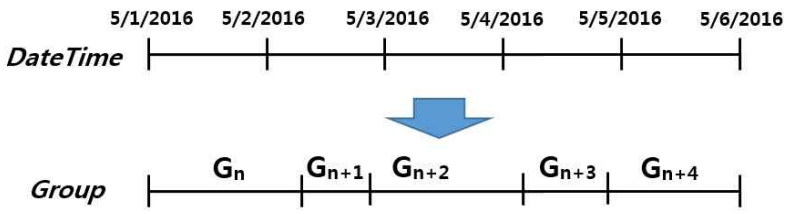
Time period	Usage (KWH)
2/1/2016 1:00	0.385
2/1/2016 2:00	0.365
2/1/2016 3:00	0.425
2/1/2016 4:00	0.5

Group ID	Time period	Usage (KWH)
$H(\sum_{i=1}^{n} P_i^s)$	$E(DT_n)^K$	0.385
$H(\sum_{i=1}^{n+1} P_i^s)$	$E(DT_{n+1})^K$	0.365
$H(\sum_{i=1}^{n+2} P_i^s)$	$E(DT_{n+2})^K$	0.425
$H(\sum_{i=1}^{n+3} P_i^s)$	$E(DT_{n+3})^K$	0.5

<그림 V-12> 시간 필드의 비식별화

아래 그림에서는 랜덤한 사이즈의 그룹이 적용된 예를 나타낸다. 한 그룹 단위에서 가질 수 있는 데이터 갯수, 즉, 그룹 사이즈는 랜덤하다.

클라우드 서버 측에서는 비식별화된 데이터의 특정 그룹 아이디에 해당되는 데이터를 카운팅함으로써 각 그룹에 속한 데이터의 개수가 몇 개인지를 알 수는 있으나, 그것 자체가 큰 의미를 갖지는 않는다. 그룹 아이디 자체는 연속된 일련의 숫자나 체계가 아니므로 특정 그룹과 다른 그룹의 순서를 연결 지을 수 없기 때문이다. 즉, 의사난수의 seed s를 알지 못하면, 특정 G_n 이후의 그룹 아이디가 G_{n+1}이라는 것을 알 수 없다. 따라서, 데이터는 각 그룹 단위로 독립적이라는 특성을 가지고 있다.



<그림 V-13> 그룹 사이즈 랜덤화

② 수치 데이터 변경 단계

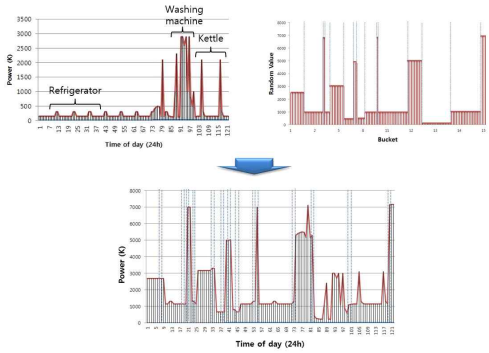
이 단계는 다항식을 기반으로 실제 감시 과정에서 측정된 데이터를 변경하는 단계이다. 참고로, 측정 데이터는 0보다 큰 임의의 실수로 측정되는 특성을 가진다.

여기에서, $f: X \rightarrow Y$인 함수 f에 대해 X에 속하는 0보다 큰 임의의 실수 데이터 x_1, x_2가 있을 때, $x_1 < x_2$ 인 모든 x_1, x_2에 대해 항상 $f(x_1) < f(x_2)$ 가 성립하는 강한 단조증가함수가 필요하다.

여기에서, 변경된 수치 데이터는 P_{n-2}^{s},P_{n-1}^{s},P_{n}^{s} 값을 기반으로 아래와 같은 식을 통하여 구한다.

$$f(x) = P_{n-1}^{s} x^2 + P_{n-2}^{s} + P_{n}^{s}$$

수치 데이터는 이와 같이 다항식을 기반으로 변경한다. 이는 특정 그룹 내에서는 원본 데이터의 분포를 그대로 가지게 되지만 실제 값은 변경되어 데이터에 기반한 분석공격을 어렵게 만든다. 만약 변경 식을 높은 항을 갖는 다차함수로 구성하였을 경우 보안성은 높아지나, 변경된 데이터의 사이즈가 크게 증가할 수 있으며, 이는 데이터베이스 특성에 따른 필드 사이즈 확보 문제 및 연산의 비효율성 문제가 발생할 수 있으므로 적절한 절충이 필요하다. 따라서, 본 논문에서의 변경식은 이러한 목적에 적합한 이차함수로 구성하였다. P_{n}^{s}의 값은 각 그룹 단위로 동일하다. 따라서, 단일 그룹 내에 대해서는 순서의 분포는 그대로 유지하고 있다는 특징이 있다. 따라서, 특정 그룹 내부에서는 범위검색 등 다양한 통계 질의가 가능하며, 실제로 유의미한 값을 전달받을 수 있다.



<그림 V-14> 수치 데이터 변환

위의 그림은 미터링 데이터를 예를 들어 나타낸다. 원본 데이터에서 냉장고, 세탁기, 전기주전자의 사용 현황을 미터링 데이터만으로 용이하게 분석이 가능하였으나, 변경된 데이터를 통해서는 이러한 분석이 매우 어렵다. 특히, 아래 데이터는 이해를 돕기 위하여 변경된 데이터도 시간 단위로 데이터를 나열한 것이나, 실제 공격자는 사전 공유된 키 K를 알지 못하므로 미터링 데이터를 아래 그림과 같이 시간 순으로 나열할 수 없다. 따라서, 공격자는 센싱 데이터 분석 공격을 할 수 없게 된다.

(3) 비식별화 데이터의 질의 및 복원 방법

비식별화된 데이터베이스에 신뢰된 서버가 접근하여 질의를 하고자 할 경우, 우선 해당 데이터에 대한 그룹 아이디를 구해야 한다. 여기서 신뢰된 서버는 seed를 알고 있으므로, 이를 기반으로 그룹 아이디를 추출할 수 있다. 만약 질의하고자 하는 데이터가 특정 그룹 내에 속해 있을 경우, 단 1회의 질의만 필요하여 질의 횟수는 평문을 대상으로 질의할 때와 동일하다. 즉, 그룹 아이디를 검색 조건으로 하여 해당 그룹내의 전체 데이터를 가져올 수 있으며, 사전에 암호화되었던 시간정보는 복호화를 통하여 원본으로 되돌릴 수 있다.

이후, 변경된 수치데이터를 기반으로, 원본 수치 데이터로의 복원이 필요하다.

여기에서, $f(x) = y$로 하였을 때, 원본 수치데이터인 x를 구할 수 있는 역함수 $f^{-1}(y)$는 아래와 같이 구할 수 있다.

앞서, 원본 수치데이터가 다음과 같은 식으로 변경되었다.

$$f(x) = P_{n-1}^{s} x^2 + P_{n-2}^{s} + P_{n}^{s}$$

여기에서, $y - P_{n-2}^{s} - P_{n}^{s} = P_{n-1}^{s} x^2$ 와 같이 이항하면, 아래와 같은 식으로 변환 가능하다.

$$\frac{y - P_{n-2}^{s} - P_{n}^{s}}{P_{n-1}^{s}} = x^2$$

따라서, 역함수 $f^{-1}(y)$ 은 다음과 같다.

$$f^{-1}(y) = \pm\sqrt{\frac{y - P_{n-2}^{s} - P_{n}^{s}}{P_{n-1}^{s}}}$$

수치 데이터 변경 및 복원의 구체적인 예를 들면 다음과 같다. 만약 P_n^s, P_{n-1}^s, P_{n-2}^s의 값이 각각 254, 691, 759라 가정하였을 때, 0.385를 변경하고자 할 경우, 수치 변경 공식에 따라, 변경된 수치 데이터를 아래와 같이 계산할 수 있다.

$$(691)(0.385)^2 + 759 + 254 = 1115.42$$

변경된 수치 데이터는 P_n^s, P_{n-1}^s, P_{n-2}^s의 값을 모두 알지 못한다면 복원이 불가능하다. 즉, 해당 데이터는 비식별화된 값이며, 의사난수의 seed를 알지 못하면 원본 데이터로 되돌릴 수 없다. 이러한 변경된 수치 데이터는 seed를 기반으로 의사난수 생성이 가능한 신뢰된 서버 측에서만 제시된 역함수를 통하여 아래와 같이 복원이 가능하다.

$$\sqrt{\frac{1115.42 - 759 - 254}{691}} = 0.385$$

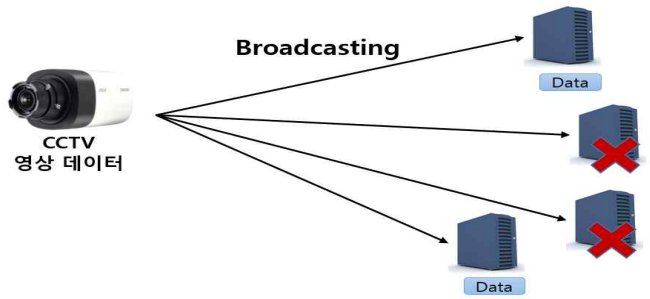
또한, 값에 대한 복원을 하지 않더라도, 비식별화된 데이터베이스 자체에 대한 질의만으로 통계처리에 일부 유의미한 결과를 얻을 수 있다. 원본 데이터가 반드시 필요한 경우는 복원이 필요하나, 만약 최대값 또는 최소값을 기록한 것이 언제인지, 혹은 상위 이용 구간 범위를 알고자 하는 경우, 비식별화된 데이터베이스 자체의 질의만으로 별도의 복호화가 필요없이 통계 처리가 가능하다는 장점이 있다.

3) 영상정보 보안전송 프로토콜

(1) 보안전송 프로토콜 개요

제안한 방법은 IoT 클라우드 환경에서 SH-Tree를 기반으로 데이터를 안전하게 동기화하는 방법에 관한 것으로, IoT 클라우드 서버 내의 데이터와 CCTV가 촬영한 영상데이터가 완전히 일치하게 동기화 하는 것을 목적으로 한다.

영상데이터 브로드캐스팅은 CCTV에서 불특정 다수의 백업서버를 대상으로 하며, 인가되지 않은 백업서버는 동기화 대상에서 제외된다. 또한, 대역폭 최소화를 위한 델타 업데이트를 지원해야 하며, 데이터 전송 과정에서의 위/변조 방지가 가능해야 한다.



<그림 V-15> CCTV 브로드캐스팅 보안기법

(2) 기존의 데이터 동기화 기법

데이터 동기화는 클라우드 환경에서 일반적으로 쓰이는 요소기술이며, 이는 여러 장치간 가지고 있는 데이터를 데이터 통신만으로 모든 장치가 동일한 데이터를 갖게 하는 것을 목적으로 한다.

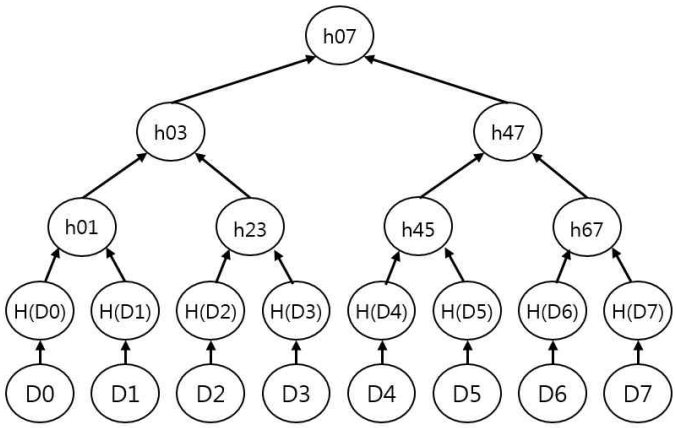
지금까지 동기화에 대한 여러 방면의 연구가 진행되된 바 있다. PC와 PDA간의 데이터 동기화를 시작으로, Palm OS상에서 디바이스 간의 동기화가 작동되도록 설계한 HotSync가 있으며, Windows CE기반에서 작동되는 Active Sync 등이 있다. 그러나 이러한 방식들은 단일 플랫폼에 종속적이라는 한계점이 있으며, 동기화 프로토콜 시 전체 데이터를 전송해야 하는 단점이 있어 효율성이 떨어지므로 클라우드 환경에서는 적합하지 않다. 이러한 단점을 보완하기 위해 델타 업데이트, 멀티 디바이스 동기화 지원, 파일 유사도 중복 체크등을 지원하는 다양한 동기화 방식의 연구가 진행되었다-.

본 절에서는 클라우드 환경에 적용 가능한 대표적인 동기화 방식으로 H-Tree 기반 동기화 방식, SyncML, Rsync 기반의 동기화 방식을 살펴보고, 클라우드

컴퓨팅 환경을 고려한 P2P 기반의 동기화를 지원하는 Uppoor의 연구를 살펴보도록 한다.

① H-Tree 기반의 동기화 방식

H-Tree(해쉬 트리)는 1979년 Merkle에 의해 처음으로 제안되었다. 이 방식은 데이터를 각 블록 단위로 분할한 뒤, 각각의 블록에 해쉬값을 수행하고, 이를 리프 노드에 입력한 후 단일 해쉬값이 만들어 질 때까지 트리 형태로 반복하여 해쉬를 하는 이진 해쉬트리 형태로 구성한 것이다. 이 경우 루트해쉬 값은 서명으로 사용할 수 있다. 이러한 방법은 주로 데이터의 무결성 확인에 사용된다. 아래 그림은 H-Tree의 구조를 나타낸다.



<그림 V-16> H-Tree

H-Tree는 동기화에 응용하여 사용될 수 있다. 이는 강력한 무결성이 요구될 때 주로 사용되며, 모든 블록 데이터에 대한 해쉬값을 각각 비교함으로써, 만약 값이 다를 경우는 해당 데이터를 갱신하는 방식으로 데이터의 동기화를 완료하는 방식이다.

그러나, H-Tree는 무결성을 제외하고는 기본적으로 보안에 대한 특별한 고려는 하지 않고 있다. 예를 들어 해쉬값의 일부를 임의로 변경하였을때는 무결성 여부의 판단이 가능하지만, 원본 데이터의 일부가 변조되었을 경우, 그 상태 그대로 해쉬값을 재구성하여 전달한다면 별도의 원본 서명값을 확보하지 않는 이상 무결성 확인이 불가능하다는 단점이 있다. 아울러, 데이터 삽입/삭제 시 델타 업데이트 처리가 지원되지 않는다는 단점도 존재한다.

본 논문에서는 이러한 H-Tree의 단점을 보완한 SH-Tree를 제안한다. 제안한 방식은 트리 자체만으로 데이터의 변경 여부 확인이 가능하다는 장점이 있으며, 원본에 대한 위/변조, 무결성이 동시에 요구되는 클라우드 환경에 적합하다. 또한, 델타 업데이트가 가능하여 대역폭을 최소화하면서 최소한의 시간 내 동기화 처리가 가능하다.

② SyncML

SyncML은 이기종 환경에서 서로 다른 플랫폼 간의 데이터 동기화를 지원하도록 개발된 개방형 표준 규격이다. SyncML 프로토콜 상에는 동기화에 필요한 여러 명령어와 메커니즘이 정의되어 있다.

SyncML 동기화 규격은 교환되는 메시지의 구조화 형태를 XML형식으로 정의한 자료 표현(Data Representation) 프로토콜, 동기화 명령과 여러 상태 메시지가 교환되는 방법에 대해 정의한 SyncML 동기화(Synchronization) 프로토콜, 메시지를 전송하기 위해서 사용하는 전송 바인딩(Transport Bindings) 프로토콜로 구성된다. SyncML은 확장성이 좋으며 여러 플랫폼과 디바이스에 대한 지원이 가능하다는 장점이 있지만, SyncML 메시지 구성시 오버헤드가 크고, 델타 업데이트를 통한 부분 동기화에 대한 명시를 별도로 하지 않고 있다는 단점이 있다.

③ Rsync

Rsync는 데이터 중복을 고려하여 변경된 부분만 동기화 할 수 있는 기법이다. Rsync는 중복 데이터를 검색하는 방법으로 롤링 체크섬(Rolling Checksum) 알고리즘을 사용한다. 이 알고리즘을 통하여 데이터 동기화 시 변경된 부분에 대한 데이터의 복사만 발생하게 된다. 이러한 방법은 동기화 시의 대역폭 절감에 있어서는 매우 효율적이라고 볼 수 있으나 중복 데이터를 갖지 않는 파일을 동기화 할 경우에는 오히려 오버헤드가 매우 큰 편이다. 또한, 파일 이름에 대한 변경이 있을 경우는 모든 파일에 대해 알고리즘을 적용해서 동기화해야 하는 문제가 있다. 기본적으로 클라우드 기반의 영상감시 환경 특성상, Rsync와 같이 파일 이름과 수정일자 기반으로 동기화 여부를 체크하는 것은 적합하지 않다. 본 논문에서 제안하는 방식은 파일명이 변경되더라도 추가 오버헤드를 가져오지 않는다.

④ Upper의 방식

Uppoor는 클라우드 컴퓨팅 환경을 고려하여 파일 시스템 계층을 분산 처리하여 멀티 디바이스간 효율적으로 데이터를 동기화 하는 방법을 제안하였다. 이 방식의 주요 특징으로 파일 메타데이터를 이용하여 클라우드 서비스 상에서 파일의 상태를 분석하여 데이터의 변경이 감지되었을 시 P2P 네트워킹으로 연결된 장치에 복제가 가능하다는 장점이 있다. 그러나 Uppoor의 연구에서는 동기화시의 오버헤드를 줄이기 위한 방법을 고려하지 않았다는 단점이 있다.

또한, IoT 클라우드의 특성에 맞는 데이터 동기화를 위해서는 새로운 동기화 방법이 필요하다. 즉, 동기화는 무결성의 관점에서 바라볼 필요가 있으며, 백업서버측의 데이터와 CCTV상의 영상데이터는 동일하게 일치해야 한다는 것을 염두에 두어야 한다. 즉, 동기화될 데이터의 기준은 서버가 중심이 되어야 하며, 만약 CCTV 및 백업서버 내의 데이터에 대한 위조, 훼손 등이 발생하였을 경우는 즉각 감지하여 원본으로 갱신될 수 있어야 한다.

(3) 영상감시 동기화 요구사항

여기서는 IoT 클라우드 기반 영상데이터 동기화 방식 설계를 위해 효율성과 보안성 측면에서의 기술적 요구사항을 분석한다.

① 대역폭의 최소화

동기화에 필요한 대역폭은 최소화되어야 한다. 정보 전달시 포맷은 최대한 간결해야 하며, 프로토콜 수행 과정에서 전달되는 데이터의 양은 최소화되어야 하며, 동기화 시 선박 측에서 데이터 대역폭을 필요이상으로 낭비하도록 설계되어서는 안된다.

② 델타 업데이트

데이터 변경 시 변경된 부분에 대해서만 업데이트가 가능해야 한다. 특히 대용량 데이터일 경우, 동기화를 이유로 전체 데이터가 전달되어서는 안된다. 이러

한 점은 대역폭의 증가와 직결되며, 동기화의 속도도 크게 증가하므로 효율성을 떨어뜨린다. 데이터의 일부만 변경되었을 경우는 그에 대한 검출 알고리즘이 필요하며, 변경된 부분을 감지 후 그에 대한 부분만 갱신되도록 하는 구조가 필요하다.

③ 분산 환경의 고려

분산 환경이 고려되어 설계되어야 한다. 즉, 서버와 오프라인 상태에서도 상대 백업서버의 데이터만으로도 동기화가 가능해야 하며, 안전하게 동기화가 마무리 되었는지, 즉, 원본 데이터에 위조가 있거나 상대측에서 위장공격이 없었음을 확인할 수 있어야 한다.

또한, 각 백업서버에서 가지고 있는 각각의 데이터가 상이해서는 안되며, 모든 선박이 단일한 데이터를 유지해야 한다.

④ 무결성 보장

영상데이터에 대한 훼손이 발생해서는 안된다. 이는 지능형 감시 서비스를 원활히 제공받는데 문제가 발생할 수 있으며, 개인의 안전에 직접적으로 영향을 미칠 수 있다. 만약 영상데이터가 변경되었을 경우는 그러한 부분을 검출해 내고, 즉각 갱신하여 정확한 원본을 유지할 수 있어야 한다.

⑤ 데이터 암호화

동기화 과정에서 데이터는 안전하게 보호되어야 한다. 악의를 가진 자에게 원본 데이터의 노출이 되지 않도록 인가되지 않은 백업서버는 동기화 과정에서의 데이터를 취득하더라도 원본 데이터를 식별할 수 없어야 하며, 반드시 인가된 그룹 내의 백업서버에 한해서만 데이터 동기화가 가능해야 한다.

⑥ 실시간 동기화

동기화는 실시간으로 이루어져야 한다. 여기서 실시간이란, 정책적으로 정하고

있는 특정 제한된 시간 내에 동기화가 완료되는 것을 의미하며, 필요시에는 즉각 갱신이 가능해야 한다.

(4) 세부 프로토콜 절차

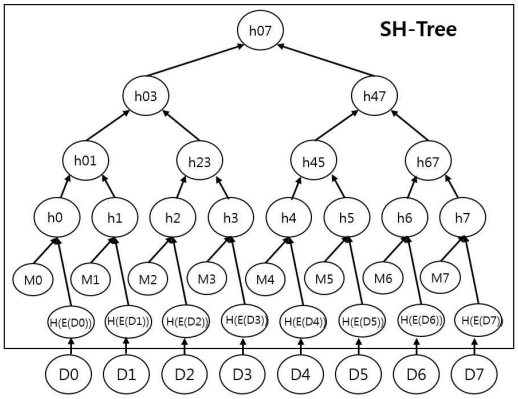
① SH-Tree

먼저, 제안하는 기법의 설명을 위해, 아래 표에서 약어를 설명한다.

<표 V-3> 보안 동기화 방식 약어

Abbreviation	Explication
Dn	n-th Data Block
Mn	Metadata of Dn
Vn	Last Version of Dn
K_p	Pre-Shared Key
H(·)	Hash Function
E(·)	Encryption

본 절에서는 IoT 클라우드 감시환경에서의 안전한 동기화를 위해 H-Tree를 변형한 SH-Tree(Secure Hash Tree)를 제안한다. 이는 평문을 암호화된 데이터와 메타정보로 분할하여 해쉬트리를 구성하는 것이 특징이며, 데이터 블록의 가변 사이즈 관리가 가능하다. 또한, 동기화된 정보와 메타정보 내의 값을 비교함으로써 데이터의 무결성, 위/변조여부의 확인이 가능하다. 아래 그림은 SH-Tree를 나타내며 아래 표는 메타정보 M이 담고 있는 항목들을 나타낸다.

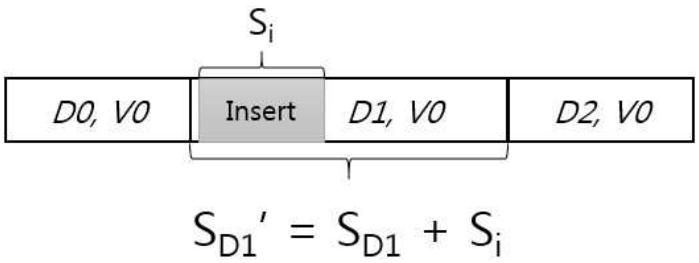


<그림 V-17> SH-Tree

<표 V-4> SH-Tree의 메타데이터

Abbreviation	Content
S_n	Size of n-th data
V_n	Version of n-th data
ts	Timestamp
h(Dn)	Hash value of n-th data

메타정보는 데이터 블록의 사이즈인 S_n, 버전 정보를 나타내는 V_n, 타임스탬프 ts, 평문 데이터 블록의 해쉬값을 나타내는 h(Dn)으로 각각 구성된다. 여기에서 S_n값은 가변 사이즈의 관리를 위해 필요하다. 만약, 데이터 블록에 값이 추가되어 삽입되었을 경우는 아래와 같이 S_n의 갱신이 필요하다. 기존 해시트리 방식에서는 데이터 삽입 시 해당 블럭 이후의 모든 블록에 대한 해쉬값이 변경되는 문제점이 존재하였다. 그러나, SH-Tree에서는 메타정보상에 블록 사이즈를 관리하는 방식으로 가변 사이즈를 처리할 수 있다. 즉, 데이터의 삽입이 일어나더라도 해당 데이터 블록의 해쉬값 및 메타정보 내의 사이즈 값만 변경되고, 다른 데이터 블록은 영향을 받지 않는다.



<그림 V-18> 블록 데이터의 사이즈

② SH-Tree의 구성 및 전달단계

데이터 암호화 단계는 데이터를 임의의 사이즈의 블록으로 분할한 뒤, 해당 블록에 대한 암호화를 수행하고, 메타정보와 함께 SH-Tree를 구성하는 단계이다. 원본 데이터를 블록 단위로 처리하는 이유는 효율성 및 부분 변경사항 검출에 목적이 있다. 데이터의 일부가 변경된 경우는 변경된 부분의 데이터 블록만 동기화를 수행하면 되며, 전체 데이터를 다시 동기화 할 필요가 없기 때문이다.

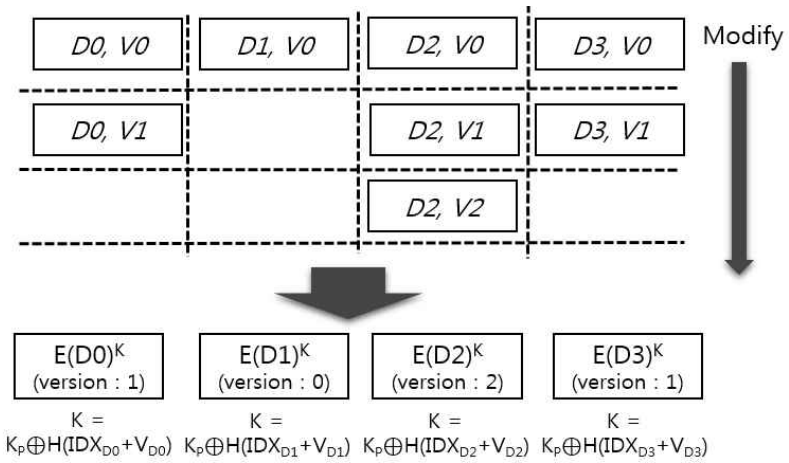
n 번째 블록에 대한 암호화 키의 구성방법은 다음과 같다. 아래의 식에 따라, 암호화 키는 각각의 데이터 블록 단위로 달라지게 된다.

$$K = K_P \oplus H(IDX_{Dn} + V_{Dn})$$

위와 같이 초기 키값인 K_P를 기반으로, 데이터 블록의 인덱스와 버전정보를 합하여 XOR처리하는 것으로 데이터 블록의 암호 키를 생성할 수 있다. n번째 데이터 블록의 인덱스값인 IDX_{Dn}은 아래의 식으로 구할 수 있다.

$$IDX_{Dn} = \sum_{i=1}^{n} S_i$$

아래 그림은 데이터 블록의 암호화 방법을 나타낸다. 각각의 블록은 버전정보가 별도로 관리되고 있으며, 이는 블록의 변경사항이 순서대로 이루어지는지를 판별하고, 필요시 데이터를 이전버전으로 복원하기 위한 목적으로 관리된다.



<그림 V-19> 블록데이터의 암호화

데이터의 암호화가 끝나면, 데이터 블록으로부터 메타정보를 추출하고, SH-Tree를 구성한다. SH-Tree는 브로드캐스팅 등 다양한 채널을 통하여 백업서버에 전달 가능하며, 백업서버는 SH-Tree의 값을 기반으로 동기화를 수행할 수 있다.

SH-Tree의 전달은 인가된 각 백업서버를 대상으로 브로드캐스팅을 기반으로 SH-Tree를 배포한다. 이는 불특정 다수의 백업서버 기반으로 암호화된 상태의 SH-Tree를 방송하며, 인가된 백업서버만이 SH-Tree를 복호화하여 수신할 수 있다. SH-Tree의 구체적인 생성 및 전달 절차는 아래와 같다.

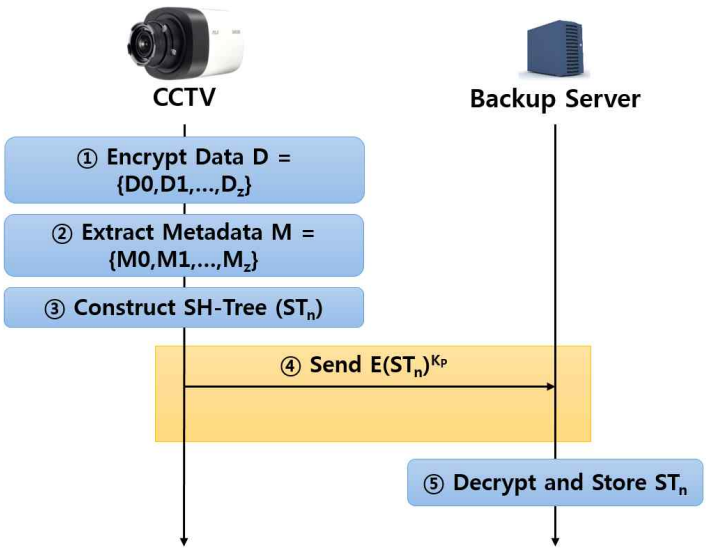
① 영상기기는 각 데이터 블록에 대응하는 키 K를 생성하고, 이를 기반으로 암호화를 실시한다.

② 영상기기는 각 데이터 블록에 대응하는 메타데이터를 생성한다.

③ 영상기기는 암호화된 데이터 블록과 메타데이터를 기반으로 SH-Tree를 구성하고, 이를 ST_n로 한다.

④ 영상기기는 지오캐스팅을 통하여 불특정 다수의 백업서버에 K_P로 암호화된 ST_n를 배포한다.

⑤ 백업서버는 데이터 수신 후 복호화하여 ST_n을 저장한다.

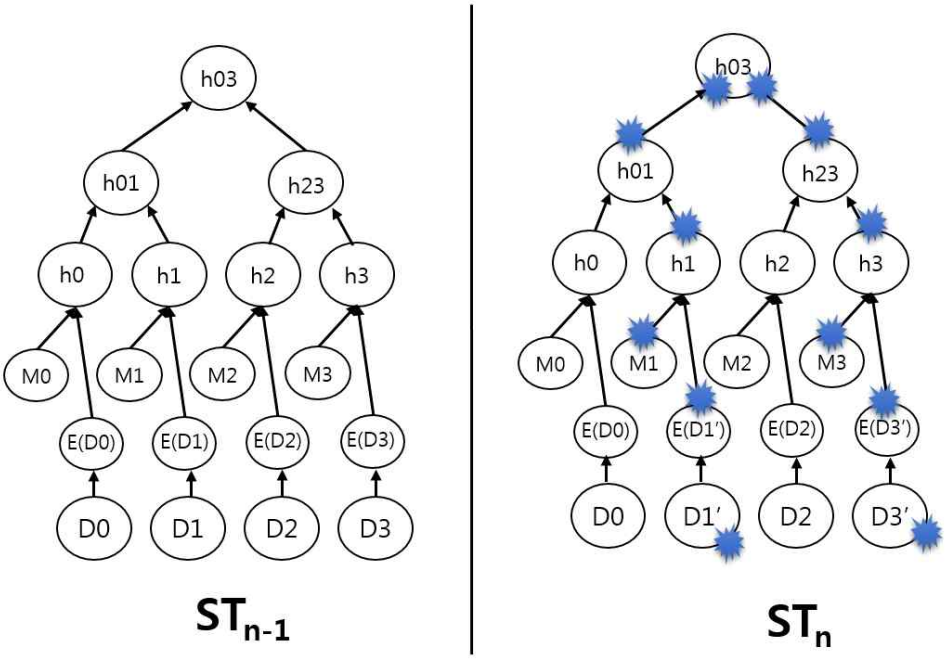


<그림 V-20> SH-Tree 구성 및 전달단계

③ 데이터 동기화 단계

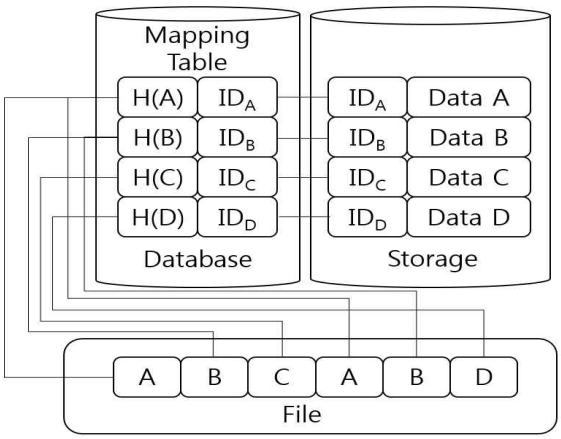
데이터 동기화 절차는 SH-Tree를 기반으로 데이터 변경사항을 검출하고 실제로 변경된 부분에 대한 데이터를 수신하는 단계이다. 아래 그림은 이전에 수신한 SH-Tree와 새로 수신한 SH-Tree' 간 차이점을 발견한 모습이다. 그림에서는 데이터 블록 D1과 D3이 변경된 것이 감지되었을 경우를 나타내며, 이러한 경우 해당 블럭에 해당하는 상위 트리에 대한 모든 값이 변경된다. 데이터 블록의 해쉬값을 트리형태로 관리하는 것은 선형적인 목록값으로 가지고 있는것 보다 변경사항 검출 속도를 증가시킨다는 장점이 있다. 데이터 블록의 해쉬를 리스트 형태

로 가질 경우 동기화를 위해 전체 해쉬 블록에 대한 선형 검색이 필요하므로 변경사항 검출시 O(n)의 시간이 소요되나, 트리로 구성하였을 경우는 $O(\log_n)$의 시간으로 변경여부의 검색이 가능하기 때문이다.



<그림 V-21> 변경사항의 검출

클라이언트는 변경된 블록을 서버에 요청하며, 서버는 해당 요청된 데이터 블록에 대하여 데이터베이스 및 스토리지 서버로부터 동일한 해쉬값을 가지고 있는 파일이 있는지를 찾는다. 이 경우, 매핑 테이블이 사용된다. 실제 파일은 클라우드 스토리지에 저장되어 있으며, 매핑 테이블은 해당 스토리지와 실제 파일의 해쉬값을 연결해 준다. 또한, 매핑 테이블은 데이터의 중복 제거 기능을 제공해 주어 데이터 사이즈 측면에서 크게 효율적인 스토리지 관리가 가능하다. 아래 그림은 스토리지와 연결된 데이터베이스의 매핑 테이블 구조를 나타낸다. 해당 그림에서는 동일한 값을 가진 데이터 블록에 대하여 스토리지상 복수로 보관하지 않고, 단 하나의 데이터 블록만 보관하여 중복 제거가 적용될 수 있음을 보인다.



<그림 V-22> 중복제거 매핑 테이블

아래 그림은 CCTV와 백업서버간의 데이터 동기화 절차를 나타낸다.

① 백업서버는 이전에 수신한 ST_{n-1}과 새로 수신한 ST_n을 비교하여 어느 블록에 대한 변경사항이 있는지를 감지한다.

② 백업서버는 변경사항이 있는 블록의 집합을 서버에 요청한다. 이때, 요청값은 각 데이터 블럭에 해당하는 해쉬의 암호화된 값으로 한다.

③ CCTV 장치는 요청된 블록에 대하여 복호화 후 데이터 블럭의 해쉬값을 얻는다.

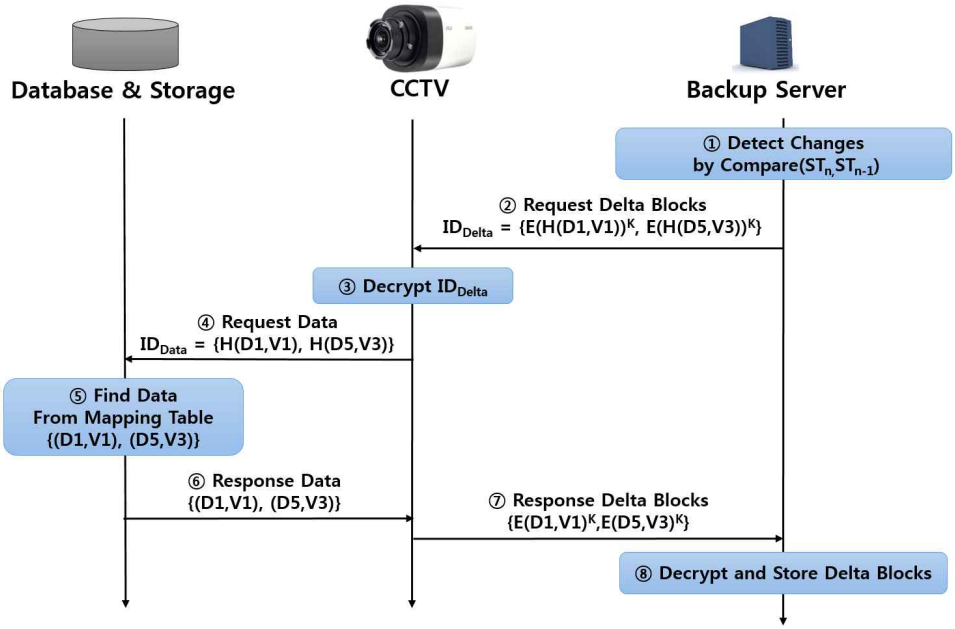
④ CCTV 장치는 데이터베이스 및 스토리지 서버에 해당 블록에 대응하는 데이터를 요청한다.

⑤ 데이터베이스의 매핑 테이블을 기반으로 스토리지 내의 실제 데이터를 얻는다.

⑥ 데이터베이스 및 스토리지 서버는 클라우드 서버측으로 실제 데이터를 전달한다.

⑦ CCTV 장치는 해당 데이터를 암호화하여 선박측에 전달한다.

⑧ 백업서버는 수신한 데이터를 복호화하고, 저장하여 동기화를 완료한다.



<그림 V-23> 데이터 동기화 단계

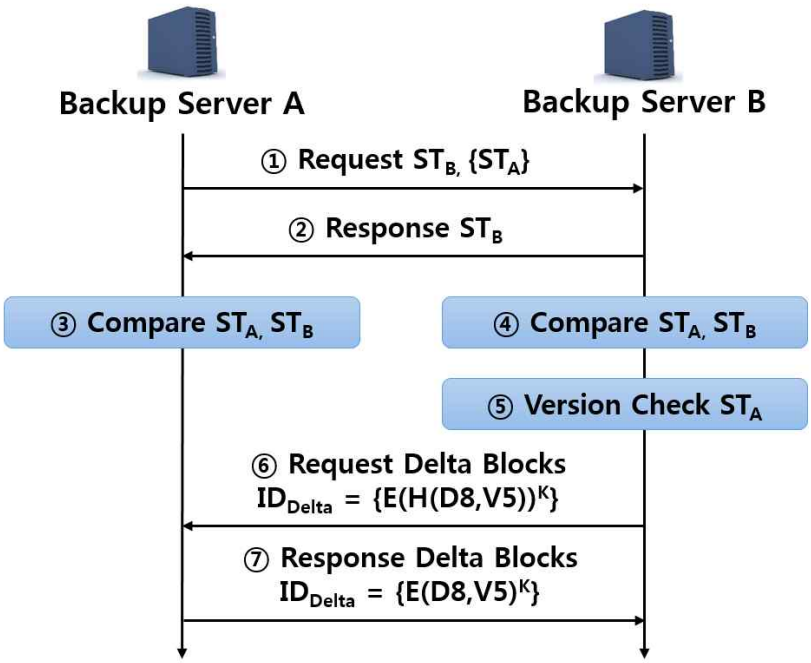
④ 통신 두절시의 데이터 갱신

지능형 감시 환경의 특성상, 백업서버 측의 통신 두절시의 환경도 같이 고려되어야 한다. 만약 통신 두절 사유로 인해 서비스가 중지된다면, 개인의 안전이 크게 위협받을 수 있기 때문이다. 기본적으로 통신 두절시는 CCTV 상의 최신 정보를 전체 백업서버에 배포하는 것은 불가능하다. 이러한 경우, CCTV 의 가장 최신 영상정보가 아니더라도, 무선 통신이 가능한 인근 백업서버간 소유한 데이터 가운데 가장 최신 정보로 갱신되는 방식으로 동기화가 가능해야 한다.

따라서 본 논문에서 제안된 방식은 IoT 클라우드의 CCTV 장치 측 뿐만 아니라, 인가된 그룹 내의 다른 백업서버에 대해서도 요청이 가능하다. 즉, CCTV 장치와 통신이 두절된 경우라 할지라도 백업서버간의 유무선 통신이 가능한 경우는 동기화 진행이 가능하다. 아래 그림은 백업서버간에 동기화가 이루어지는 경우를 나타내고 있다.

기본적으로, 이러한 문제는 백업서버 A와 백업서버 B간에 어느 정보가 가장 최신 것인지에 대한 고려가 먼저 필요하다. 즉, 각 백업서버에서 가지고 있는 데이터 블록 가운데 일부는 백업서버 A가 최신 데이터일 수도 있으며, 일부는 백업서버 B가 최신 데이터일 수도 있다. 이러한 관점에서 예를 들어, 백업서버 A

가 일방적으로 백업서버 B의 데이터를 신뢰하고 동기화해서는 안되며, 반대의 경우도 마찬가지이다. 만약 브로드캐스팅으로부터 전달되었던 CCTV 장치의 SH-Tree라면 최신것으로 판단하고 동기화를 진행하면 문제가 없으나, 백업서버 간의 동기화 시는 두 백업서버 간 어느 백업서버의 데이터가 최신 정보인지를 서로 비교하여 판단하는 것이 중요한 관점이다.



<그림 V-24> 백업서버 간의 동기화 절차

본 논문에서는 데이터 블록에 대한 버전정보를 별도로 관리하여, 두 데이터 블록 간 어느 것이 최신정보인지에 대한 판단이 용이하도록 설계하였다.

위의 그림에서는 선박간 SH-Tree의 교환 결과 백업서버 A의 데이터 가운데 8번째 블록인 D8이 가장 최신인 것으로 백업서버 B가 판단하고 최신 값으로 갱신하는 과정을 나타내고 있다.

① 백업서버 A는 백업서버 B의 SH-Tree를 요청함과 동시에, 자신이 소유하고 있는 SH-Tree인 ST_A를 전송한다.
② 백업서버 B는 백업서버 A에게 자신이 소유한 SH-Tree인 ST_B를 응답한다.
③ 백업서버 A는 ST_A와 ST_B를 비교하여 변경사항을 검출한다.
④ 동일하게, 백업서버 B는 ST_B와 ST_A를 비교하여 변경사항을 검출한다. 여기에서는 8번째 블록인 D8인 검출되었다.

⑤ 백업서버 B는 검출된 블록에 대한 버전값 비교를 통해, D8이 Ship A보다 낮은 버전임이 감지되었다.
⑥ 백업서버 B는 백업서버 A로부터 (D8,V5)를 요청한다.
⑦ 백업서버 A는 암호화된 (D8,V5)를 응답한다.

4) 영상기기 S/W 자동업데이트 프로토콜

IoT 영상기기의 사후관리의 기술적 측면에서 크게 중요하다고 볼 수 있는 부분으로 소프트웨어 업데이트가 있다. 본 절에서는 소프트웨어 업데이트의 기술적 방안에 대하여 논의하고, 세부절차를 제안한다.

(1) 사전 알고리즘 선정

소프트웨어 업데이트 파일의 배포 과정에서, 해커의 공격에 의해 업데이트 파일 자체가 변조될 수도 있으며, 이러한 원인으로 제조사에서 제공한 파일과는 전혀 다른 파일이 사용자에게 전달될 수 있다. 이러한 문제는 보안상 큰 위험을 야기할 수 있다. 특히, 현행의 IoT 제품은 보안에 대한 강도 높은 수준의 설계가 되어 있지 않은 제품이 많으며, 상당수의 IoT 제품이 보안 위협에 노출되어 있다.

소프트웨어 업데이트 파일을 명확하게 확인할 수 있는 방법은 업데이트 파일의 배포 과정에서 발생 가능한 위/변조 문제를 예방할 수 있는 무결성 기술을 적용하여야 함이 우선이다. 본 논문에서는 업데이트 파일의 배포/설치/구성 단계에서 기술적 관리 방법으로, MAC(메시지인증코드)을 사용할 것을 제안한다. MDC(변조감지코드)와 MAC의 차이점은, MAC은 원본 메시지에 대한 무결성과 메시지 출처 확인이 가능하다는 부분이다. 그러나 이러한 기능을 갖게 하기 위해서는 사전에 송신자와 수신자 사이 키 공유가 필요하다는 단점이 있다. MDC의 경우는, 암호학적으로 원본 메시지에 대응하는 해쉬 함수를 사용하는 것으로, 원본 메시지에 대한 무결성을 보장하기 위해 사용하는 방법이다. 그러나 메시지가 누구로부터 전송되었는지에 대한 확인은 할 수 없다. 또한, MDC는 반드시 안전한 채널을 통하여 전달하여야 한다는 단점이 있다.

<표 V-5> MAC과 MDC의 특성 비교

항목	MDC	MAC
채널 노출 안전성	X	O
발신자 인증	X	O
부인방지 제공	X	X
메시지 무결성	O	O

IoT 제품에 대한 업데이트 상황을 고려해 볼때, MDC보다 MAC이 적합하다. MAC은 해당 메시지에 대한 출처 확인이 가능하므로, 해커의 공격이 발생하였을 경우, 정당한 사용자에 의하여 생성된 MAC인지에 대한 감지가 가능하기 때문이다.

한편, IoT 제품에 적합한 초경량 암호화 기술이 요구된다. IoT 기기 특성상 저전력에 적합한 암복호화 기술이 적용되어야 하며, 현재 아래 표와 같은 여러가지의 경량 암호화 기술이 개발되어 있으며, 이러한 알고리즘의 위협요소인 부채널 공격부분에 대한 취약요소는 반드시 해결해야 될 과제이다.

<표 V-6> 경량 암호화 알고리즘 분석

명칭	ARIA	LEA	HEIGHT
구분	대칭키	대칭키	대칭키
키 길이	128비트	128비트	64비트
구조	Involutional Substitution-Permutation Network	ARX기반 GFN(Generalized Feistel Network)	일반화된 Feistel 변형 구조
보안성	낮음	높음	낮음
보안위협	부채널 공격에 취약		

(2) 소프트웨어 자동 업데이트 프로토콜

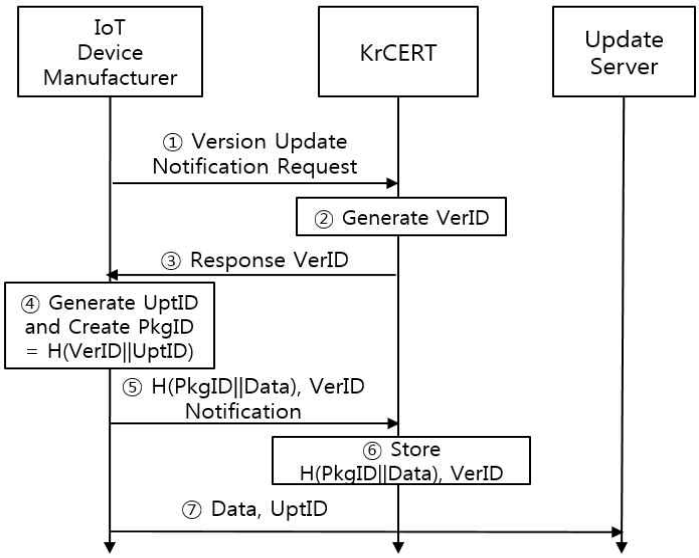
소프트웨어의 업데이트는 일반적으로 수동 업데이트와 자동 업데이트의 두가지 방법이 존재한다. 수동 업데이트는 사용자에 의하여 행하여지는 업데이트를 의미한다. 그러나 IoT 환경에서는 업데이트를 관리해야 할 장치가 너무 많음에

따라, 이용자가 모든 IoT 디바이스에 대하여 스스로 수동 업데이트를 하는 방식은 바람직하지 않다. 따라서 IoT 제품의 보안성 확보를 위하여 실시간 자동 업데이트의 기술적 방안이 필요하다.

본 논문에서 제안하는 소프트웨어 자동 업데이트 절차 설명에 필요한 약어를 정리하면 아래 표와 같다.

<표 V-7> 소프트웨어 자동 업데이트 절차 약어

약어	설명
PkgID	소프트웨어 업데이트 패키지 ID
UptID	업데이트 서버가 관리하는 ID
VerID	KrCERT에 의해 생성되는 버전 ID
Data	실제 소프트웨어 업데이트 파일
H(·)	특정 값의 SHA-1 기반 해쉬



<그림 V-25> 소프트웨어 자동 업데이트 파일 등록

자동 업데이트 과정에서는 업데이트 소프트웨어의 무결성 손실, 혹은 해커의 악의적인 소프트웨어 변경 배포, 통신과정에서의 변조공격 등이 발생할 수 있다. 따라서 본 논문에서는 최신 보안 모듈을 유지하기 위한 방법으로, 아래 그림과 같이 업데이트 과정에서의 문제를 방지할 수 있는 자동 업데이트 절차에 대하여 제안한다. 여기서는 안전한 통신을 위해서 두 장치간의 통신 및 보안 모듈이 동

일한 최신 버전을 갖추어야 함을 원칙으로 하고 있으며, 이에 따라, 두 장치 간 소프트웨어를 최신버전으로 갱신하여 통신하는 절차를 세부적으로 정의하고 있다. 위의 그림에서는 소프트웨어 자동 업데이트를 위해, 사전에 IoT 기기 제조사에서 업데이트 서버로 등록하는 단계를 나타내고 있다. 세부 절차는 다음과 같다.

① IoT 기기 제조사는 KrCERT 측에 새로은 버전의 소프트웨어 업데이트가 필요함을 알린다.

② KrCERT는 임의의 VerID를 생성한다. 이는 향후 IoT 기기와의 상호인증 시 사용될 것이다.

③ KrCERT는 VerID를 IoT 기기 제조사에게 응답한다.

④ IoT 기기 제조사는 임의의 UptID를 생성하고, 해당 값을 기반으로 H(VerID||UptID)를 통하여 PkgID값을 생성한다.

⑤ IoT 기기 제조사는 KrCERT측에 H(PkgID||Data) 값과 VerID 값을 전달한다.

⑥ KrCERT는 수신된 값을 쌍으로 저장한다.

⑦ IoT 기기 제조사는 업데이트 서버측에 실제 업데이트 파일과 UptID를 전송하고, 업데이트 서버는 해당 값을 쌍으로 보관한다.

또한, 다음 그림에서는 소프트웨어 자동 업데이트 등록이 완료되었을 경우, 실제 IoT 장치 A와 장치 B간 최신 업데이트된 소프트웨어로 갱신하여 통신하는 세부 프로토콜을 정의하고 있다.

제안한 자동 업데이트 프로토콜은 다음과 같다.

① IoT 장치 A는 장치 B에 소프트웨어 버전을 요청한다.

② 장치 B는 소프트웨어 버전을 응답한다.

③ 장치 A는 소프트웨어 버전을 확인한다. 여기서는 장치 B의 소프트웨어 버전이 낮을 경우를 가정하고, 업데이트가 필요함이 확인되었다.

④ 장치 A는 장치 B에 소프트웨어 버전 불일치를 통보한다.

⑤ 장치 B는 업데이트 서버로부터 최신 버전을 요청한다.

⑥ 업데이트서버는 장치 B로 최신 소프트웨어 파일 및 이에 대응되는 UptID

를 응답한다.

⑦ 장치 B는 제공된 소프트웨어 파일과 Pkg ID를 해쉬 처리한 H(PkgID||Data)값을 생성한다.

⑧ 장치 B는 H(PkgID||Data)값을 KrCERT측에 유효성 검증을 요청한다.

⑨ KrCERT는 유효성을 확인하여 이상이 없음을 검증 후, 이상 없음 및 VerID를 응답한다.

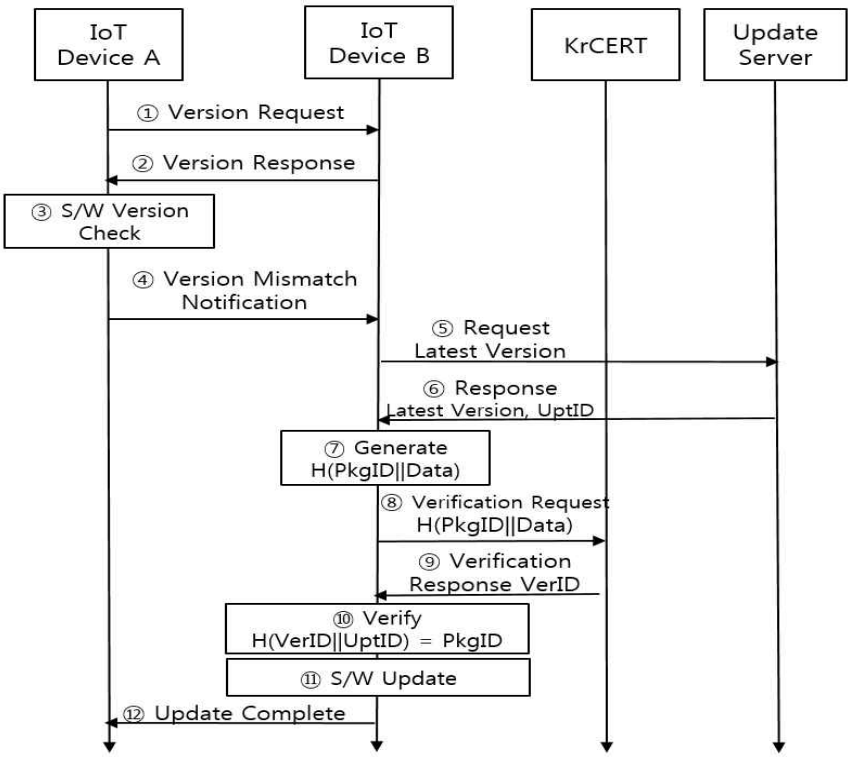
⑩ 장치 B는 ⑥에서 수신된 UptID와 ⑨에서 수신된 VerID의 해쉬값과 PkgID 값이 일치하는지를 판단한다.

⑪ 장치 B는 소프트웨어 업데이트를 수행한다.

⑫ 장치 B는 장치 A에게 소프트웨어 업데이트가 완료되었음을 알린다.

이러한 업데이트 방식을 적용한 경우, 업데이트 서버에서 특정 파일이 손실되었거나, 업데이트 과정에서 해킹이 발생하여 소프트웨어의 변조 공격 등이 발생하는 경우를 차단할 수 있다.

한편, 본 논문에서는 UptID값과 VerID값을 기반으로 KrCERT와 업데이트 서버의 신뢰성을 확인할 수 있도록 프로토콜을 구성하여, IoT 기기와 KrCERT 및 업데이트 서버간 상호 인증 기능을 가지므로 서버 위장 공격에 대한 방지가 가능하다. 또한, 업데이트 파일이 해킹 및 패킷 손실 등 다양한 경로로 원본과 다른 데이터로 변경이 발생하였을 경우, 업데이트 파일에 대응하는 해쉬값인 H(PkgID|| Data)값이 변경될 것이다. 해당 값은 유효성 확인을 위해 KrCERT 측에서 사전에 가지고 있는 값이며, 해당 IoT 장치에서 생성하여 KrCERT 측에 전달하는 H (PkgID||Data)값과 PkgID 값을 KrCERT측에서 비교한 후, KrCERT 측에서 사전 등록된 값과 일치하는지를 판단하여 적합성 여부를 IoT 기기에 전달해 주게 되므로, IoT 기기는 해당 업데이트 파일의 신뢰성을 확인하여 안전하게 소프트웨어의 자동 업데이트 수행이 가능하다.



<그림 V-26> 소프트웨어 자동 업데이트 프로토콜

VI. 시뮬레이터 구현 및 비교분석

1. 영상감시 시뮬레이터 설계 및 구현

1) 기능 설계

본 논문에서의 기능 및 성능 평가를 위하여 PEVS Framework를 구현하였다. PEVS Framework는 본 논문에서 제안한 메타 비식별화 기법 및 보안 질의 기법이 구현되어 있으며, RBAC 기준의 접근제어 정책으로 작동한다. 기존의 영상 마스킹은 화면내 객체에 대하여 일괄적으로 처리된 부분이 있다. 즉, 마스킹 여부의 결정은 공개 여부로 나뉘어지고, 특정 기준에 따른 세밀한 언마스킹 정책이 별도로 존재하지 않는다. 그러나, 지능형 영상감시 환경에서는 객체의 동의 여부, 혹은 위험도 정도에 따라 다양한 접근제어 정책이 필요하다. 즉, RBAC과 같은 접근제어 권한에 따른 보다 세밀한 언마스킹 정책이 필요한 상태이다. 정보 열람자의 권한(역할)과 피사체의 범죄 위험도를 종합적으로 판단하여 객체정보를 얼마나 공개할 것인지 결정하고 이를 반영하여 세밀하게 마스킹 처리를 조정할 필요가 있다. <그림 VI-1>은 프라이버시 정도에 따라 객체의 공개 수준이 변화하는 것을 나타내고 있다.

<그림 VI-1> 차등레벨 언마스킹 접근제어

한편, 영상을 마스킹 처리했다고 하더라도, 메타데이터를 기반으로 원본 영상 데이터에 대한 일정부분의 정보를 추정할 수 있다. 따라서, 영상에 사용된 메타정보는 비식별화 처리를 수행한다. 결론적으로, 원본 영상 파일에 대한 이미지/비

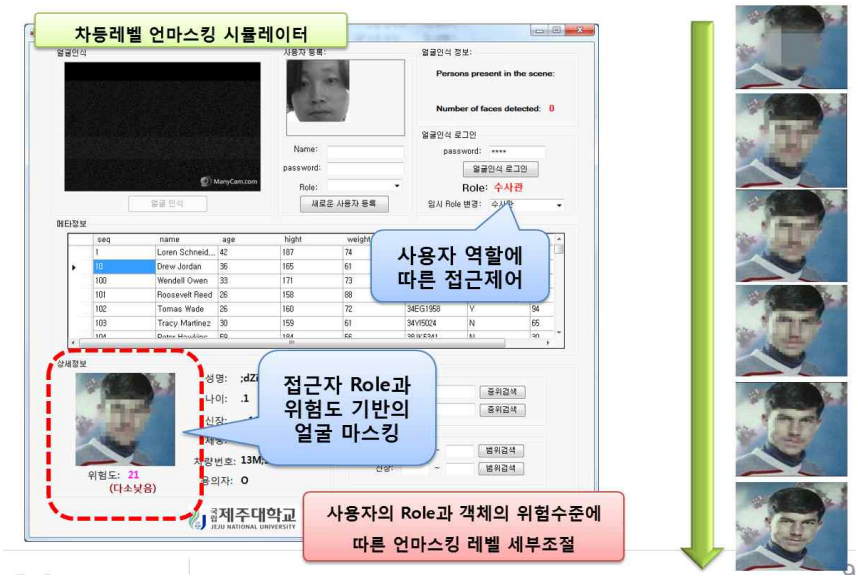
디오 정보는 마스킹 처리되고, 영상 메타데이터는 비식별화처리 되므로 최종적으로 개인의 프라이버시가 노출되지 않는다. 이러한 방법을 통하여 실제 클라우드 환경에 해커가 침입하여 원본 영상 파일과 메타데이터를 습득했다고 하더라도, 실제 원본에 대한 영상 정보를 추정하기 매우 어렵게 만들수 있다.

<그림 VI-2> 암호화 및 비식별화를 통한 영상데이터 보호

<그림 VI-3> PEVS 영상감시 시뮬레이터 아키텍쳐

2) 구현 화면

PEVS 시뮬레이터의 구현 화면은 <그림 VI-4>와 같다. 화면상의 클라이언트 화면은 사용자 역할에 따른 접근제어 및 접근자의 Role과 위험도 기반의 얼굴 마스킹 부분을 나타낸다.



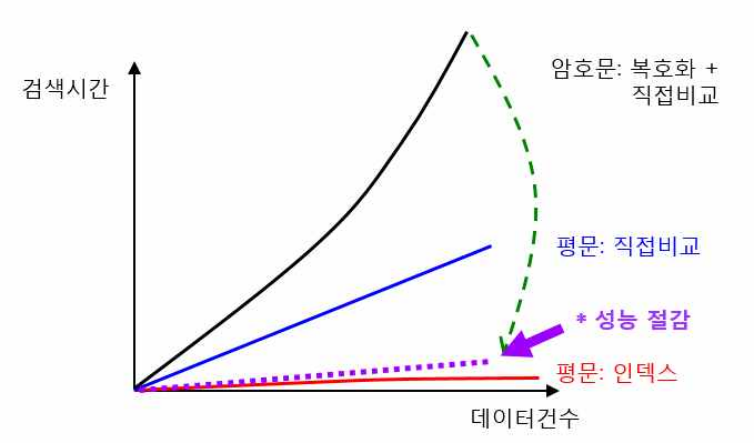
<그림 VI-4> 구현 화면

본 절에서는 4장에서 제안한 PEVS 영상감시 프레임워크에 대한 성능측정 방법을 설명한다. 성능측정을 위해 PEVS 시뮬레이터를 구현하였으며, 이를 기반으로 제안 방식의 정상적인 작동 여부를 검증하였다. 한편, 안전성과 효율성 측면은 정성적 평가를 통하여 검증한 후, COP-메타변환 알고리즘에 대하여 정량적 평가를 수행한다. 정량적 평가에서는 본 논문에서 제안한 COP-메타 변환 알고리즘은 기존 영상메타 암호화 기법 대비 높은 성능을 나타냄을 보인다.

3) 성능 측정

(1) 성능평가 모델

본 절에서는 영상메타데이터의 비식별화 처리속도와 평문 대비 오버헤드율을 측정한다. 여기서 오버헤드율이란, 영상 메타데이터를 비식별화 처리했을 경우 평문상태 메타데이터 대비 데이터 질의 오버헤드율을 의미한다. 특히, 영상메타데이터의 암호화 방식과 비식별화 방식의 DB처리 오버헤드 비교가 초점이 된다. 즉, 비식별화 된 상태에서도 데이터베이스 인덱스 구성을 통하여 평문 인덱스와 유사한 수준의 오버헤드 성능을 갖는다면 우수한 수준으로 판단할 수 있는 근거가 된다.



<그림 VI-5> 영상데이터 비식별화 성능 측정 모델

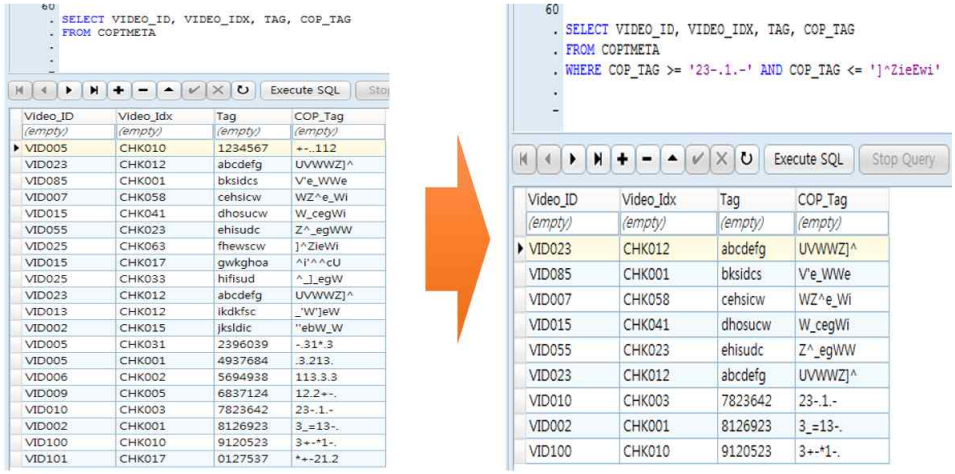
(2) 성능측정 환경

여기서는 제안 방식의 성능 측정 환경을 살펴본다. COP-변환 알고리즘에 대한 성능 측정 환경은 다음과 같다. 알고리즘은 C++로 구현하였으며, 데이터베이스는 OpenStack에서 사용하는 SQLite로 데이터를 구성 하였다. CPU는 i7-4790K@4.0GHZ 환경에서 수행하였으며, 메모리 사이즈는 6GB에서 수행하였다. 샘플 데이트는 영상메타데이터 누적 1천만건을 임의로 구성하였다.

(3) 비식별화 처리성능 측정결과

① 성능 측정 화면

아래 그림에서의 왼쪽 그림은 전체 데이터를 나타내고 있으며, 오른쪽 그림은 COP-변환을 통하여 재구성한 범위검색 질의를 나타낸다. COP-변환 질의 출력은 평문으로 구성된 데이터베이스 환경에서의 평문 질의 결과와 동일한 결과를 출력하는 것을 알 수 있다. 또한, 평문과 동일한 실행계획(Explain Query Plan)을 가지므로 변환된 상태에서도 인덱스를 평문과 동일하게 활용할 수 있어 질의상 효율적인 성능을 보인다.

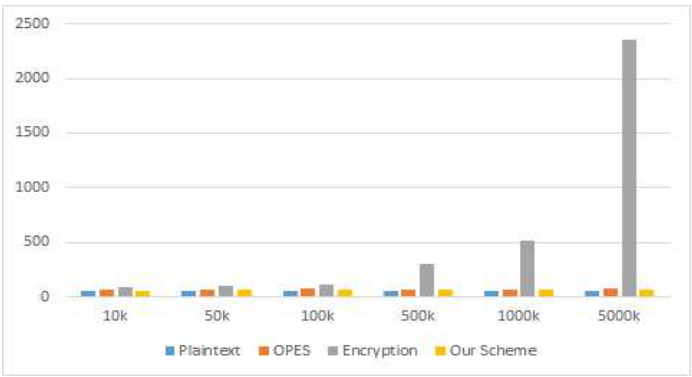


(a) Total Data *(b) Range Data*

<그림 VI-6> COP 변환 데이터의 SQL 질의

② 단일 질의 성능 측정

단일 측정 결과는 아래 그림과 같다. 평문으로 데이터베이스 질의를 수행하였을 때가 가장 성능이 높게 나오지만, 실질적으로는 순서유지 암호화 방식 및 제안하는 방식과 비교하면 큰 차이점은 존재하지 않는다. 이는 세 방식 모두 데이터베이스의 인덱스를 활용함으로써 빠른 속도로 데이터를 가져올 수 있으며, 인덱스된 데이터베이스 처리시간에 암호화 처리 시간만 추가되기 때문이다. 한편, AES 암호화를 수행하였을 경우는 데이터베이스 인덱스를 지원하지 않으므로 데이터베이스 질의에 매우 큰 오버헤드가 소요되는 것을 확인할 수 있다.

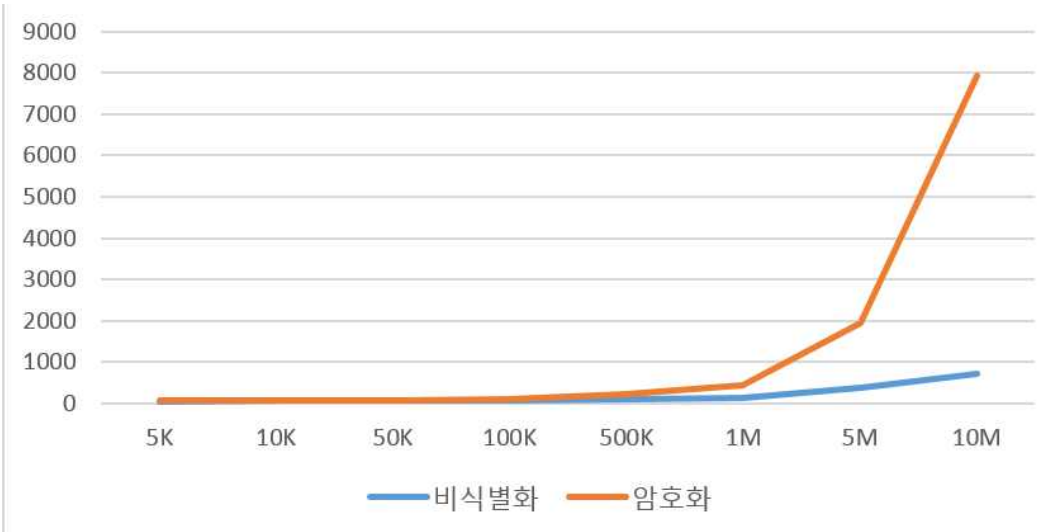


<그림 VI-7> 단일 질의 성능 측정

평문으로 데이터베이스에 질의할 경우와, 본 논문에서 제안한 COP-변환 기법으로 질의할 경우에는 질의 처리 속도 차이가 미미한 수준임을 알 수 있다. 기존의 순서유지 암호화 방식에서도 이러한 측면에서는 동일한 특성을 가지고 있으나, 기존 순서유지 암호화 방식은 평문과 동일한 순서를 가지고 있어 데이터에 대한 분석 공격이 가능함으로써 보안상 취약점이 존재한다. 본 논문에서 제안한 COP-변환 기법은 평문 및 순서유지 암호화 방식의 수준과 대등한 성능을 보이고 있으며, 실질적으로 순서 정보가 평문과 동일하게 적용되지 않고, 역순, 정순이 랜덤하게 적용되어 더욱 안전성이 높다는 장점이 있다. 한편, AES와 같은 일반적인 암호화 알고리즘의 경우는 데이터베이스의 인덱스 사용이 불가능하여 매우 큰 오버헤드를 발생시키며, 기존의 암호화 방법에 비해 제안한 방식이 더욱 효율적임을 나타내고 있다

③ 데이터 건별 성능 측정

데이터 건수 단위로 측정한 결과는 아래 그림과 같다.



<그림 VI-8> 건별 성능 측정 결과

<표 VI-1> 영상메타 암호화 대비 비식별화 성능향상율

누적데이터(건수)	암호화(ms)	비식별화(ms)	성능향상율(%)
5,000	61	64	4.6
10,000	68	69	1.4
50,000	69	87	20.6
100,000	72	103	30.1
500,000	91	241	62.2
1,000,000	127	447	71.5
5,000,000	391	1961	80.1
10,000,000	706	7936	91.1

영상메타 데이터 누적 1천만건 기준으로, 각 건별 성능 측정 결과는 다음과 같다. 기존 암호화 방식 대비 누적 데이터 건수 1백만건 이상인 경우 DB 질의시 70%이상의 성능향상율을 보이고 있다. 그러나 누적 5만건 이하는 실질적으로 차이가 크지 않으며, 누적 10만건 이상부터 암호화 방식 대비 기하급수적인 성능 차이를 보인다. 즉, 메타 비식별화는 평문으로 메타정보를 구성한 데이터의 처리 속도와 유사한 수준으로, 암호화 대비 오버헤드가 현저히 적음을 확인할 수 있으며, IoT 클라우드 기반의 영상감시 환경에 적합함을 알 수 있다.

(4) 동기화 처리성능 측정결과

제안한 영상측정 방식에서는 블록 ID가 블록의 해쉬값을 기반으로 결정되게 된다. 이러한 관점에서, 블록 사이즈는 동기화의 성능에 직접적으로 영향을 미친다. 여기에서는 블록 사이즈별 블록 ID 추출에 대한 실제 성능 측정을 수행한 결과에 대해 살펴본다.

아래 표는 성능 측정을 수행한 환경을 나타내고 있다. 여기서, 블록 ID 추출에 필요한 해쉬 알고리즘은 SHA-1을 사용하였다.

<표 VI-1> 블록 추출 시험 환경

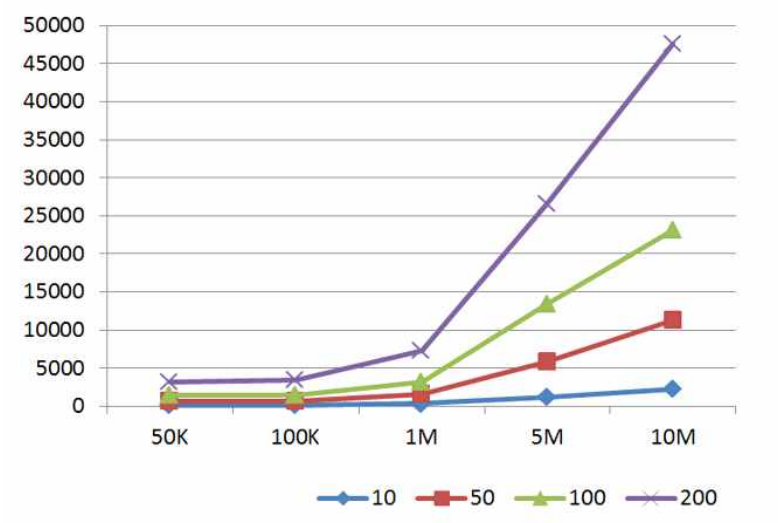
CPU	Intel i5-3470 @3.2GHz
RAM	4GB
O/S	Windows 7
Language	C++
Hash Algorithm	SHA-1

위의 표는 앞서 설명한 블록 ID 추출 방식에 대한 실제 성능 측정 결과치를 나타낸다. 여기에서는 블록 사이즈를 각각 50K, 100K, 1M, 5M, 10M로 가정하고, 블록 개수를 각각 10, 50, 100, 200일때의 성능을 측정하였다. 또한, 각각의 속도 결과값은 ms 단위로 측정하였다. 표의 결과에 따라, 블록 ID 추출 시간은 해당 블록의 사이즈에 비례하는 것을 알 수 있다.

<표 VI-2> 성능 측정 결과

블록개수	50K	100K	1M	5M	10M
10	142	150	317	1196	2301
50	671	689	1551	5879	11326
100	1439	1489	3142	13420	23158
200	3211	3396	7290	26579	47575

아래 그림은 각 사이즈별 블록 ID의 추출 성능을 그래프로 나타낸다. 여기서 블록 ID의 사이즈가 작을수록 빠른 처리속도를 나타내고 있다. 이는 실질적으로 해쉬 생성에 필요한 비용보다는 디스크 I/O 비용이 더욱 많음을 나타낸다. 따라서 동기화시 가능한 블록 사이즈를 크지 않게 하는 것이 동기화의 효율성을 높일 수 있음을 알 수 있다.



<그림 VI-9> 성능 측정 결과

2. 시나리오 기반의 안전성 평가

1) 영상감시 공격 시나리오 모델 도출

(1) 시나리오 도출 개요

지능형 감시 환경에는 보안에 대한 큰 위협이 존재하고 있다. 과거에는 불법적으로 개인정보를 획득하려고 하는 내부 공격자와 같은 위협이 존재하였으나, 현재는 정보기술의 발달과 함께 조직 내의 내부공격자 뿐만 아니라, 인터넷으로 연결된 외부에서의 조직적 기술 탈취, 해커의 정보 불법 수집 등 다양한 위협이 발생할 수 있다.

즉, 지능형 감시 환경 자체가 그대로 인터넷에 연결됨으로써 다양한 정보 접근 경로가 노출되며 기존에는 생각지 못한 다양한 형태의 보안 위협이 발생할 수 있다. 따라서, 지능형 감시 환경을 대비하여 이를 안전하게 보호할 수 있는 전문인력 양성이 시급한 상황이다.

보안에 대한 위협은 아무리 강조해도 지나치지 않은 측면이 있다. 특히, 4차산업 환경에서는 기존의 IT 환경보다 더욱 많은 보안 취약점에 따른 위협 노출이 우려되는 상황이며, 정보보안의 위협은 실질적으로 기업의 중요 정보 노출을 통한 경쟁력 손실 및 물질적 피해로 이어질 수 있다. 특히, 스마트시티 환경 등의 지능형 감시 환경에 대한 사이버 공격이 발생할 경우는 그 피해 규모는 엄청날 수 있어, 이에 대한 안전한 대책이 필요하다.

따라서, 본 절에서는 사이버 보안 전문인력 양성을 위한 모의훈련 방법을 제안하고자 한다. 해당 방법은 IoT 클라우드 환경에 적합한 사이버 모의해킹 훈련 방안이다. 주요 특징으로 기존의 메뉴얼 대응 방식이나 공격/방어 팀 기반의 방식과는 차이가 있으며, IoT 클라우드 환경에서 종전의 훈련방식으로는 구성하기 어려운 다양한 시나리오를 제안하는 훈련 환경을 통해 구성할 수 있다는 장점이 있다.

(2) 공격 시나리오 구성 접근방법

일반적으로 사이버 위협에 대응하는 훈련방법으로 크게 두가지의 접근방법이 있다. 먼저, 메뉴얼 기반의 대응 훈련 방법으로, 이러한 방법은 실제 사이버 해킹이 발생하였을 경우, 어떤 방법으로 대응해야 될지에 대한 구체적인 메뉴얼이 사전에 구성되어 있으며, 이를 기반으로 절차적인 대응을 수행하는 방법이다. 이러한 방법은 정보보안에 대한 깊은 지식이 없는 집단에서 훈련하기 적합한 방법이며, 메뉴얼의 내용을 따라 절차적인 수행을 진행하므로 비전문가 집단의 훈련 방식으로 널리 활용된다.

한편, 공격팀과 방어팀을 별도로 구분하여 가상의 침해대응 훈련을 진행하는 방법도 있다. 이러한 방법은 공격팀에서는 해킹에 대한 공격 시나리오를 구성하여 시나리오대로 해킹을 수행하고, 방어팀에서는 이러한 공격팀의 해킹에 대하여 차단하는 것으로, 메뉴얼 기반의 훈련 방식보다 더욱 효과적이고 실전적인 방식이다.

현재 정보보호 해킹 경연대회는 상당수가 이러한 공격/방어팀 체제로 이루어지고 있을 정도로 최근에 널리 보편화 된 방식이며, 이는 과거 육상에서의 실전 모의 전투훈련때부터 그 효과성이 입증된 방법이다. 다만, 이러한 방법은 비전문가 집단에서 수행할 수 있는 훈련방법으로 적합하지는 않으며, 정보보호 전문 부서나 보안 업체 등 정보보호에 대한 깊은 지식이 있는 집단에서 효과적으로 훈련할 수 있는 방법에 해당한다.

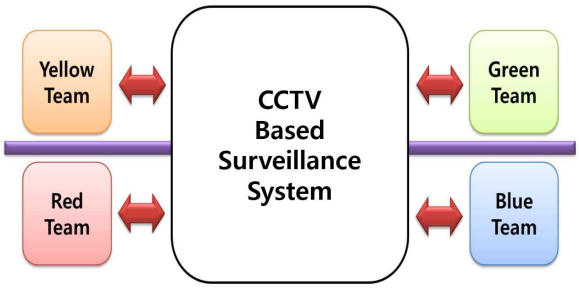
그러나, 이러한 공격/방어 기반의 훈련 방식은 지능형 감시 환경에서 보다 실전적인 훈련을 진행하기에는 한계가 있다. 따라서 본 논문에서는 이러한 공격/방어팀 기반의 훈련방법을 개선 및 보완하여, 새로운 모의해킹 훈련방법을 제안하고자 한다.

(3) 공격 시나리오 도출

본 절에서 제안하는 모의해킹 훈련방안은 종래의 공격/방어 팀 편성을 기반으로 하는 사이버 훈련 방법을 개선하여, 4개의 팀을 편성하여 보다 복합적이고 실전적인 훈련 시나리오를 구성하는데 목적이 있다.

기본 모의해킹 모델은 아래 그림과 같다. 그림에서 각각의 팀은 행위주체를

나타내며, 실무팀(Yellow Team), 운영팀(Green Team), 공격팀(Red Team), 방어팀(Blue Team)의 네 주체로 모의 해킹이 이루어 진다. 또한, 모든 팀은 메인 서버인 지능형 감시 환경에 접근할 수 있다는 것을 사전에 가정하고 있다.



<그림 VI-10> 감시환경 모의해킹 기본 모델

① 각 팀의 세부 역할

실무(Yellow)팀은 실제 환경에서 실무를 담당하는 CCTV 등 지능형 영상 장치 관제의 역할을 수행한다. 제안하는 방식에서 가정하고 있는 부분으로, 실무팀은 정보보안에 대한 전문적인 지식을 가지고 있지 않은 집단이라는 점이다. 또한 여기에서 중요한 점은, 실제 IoT 제품 및 모니터링 기기는 실무팀이 실제로 조작한다는 부분이며, 전문적인 지식이 없는 실무팀의 활동은 정보보안의 위협에 직접적으로 노출되어 있으며, 해커는 이러한 실무팀의 기기 조작 과정에서의 위장 공격, 도청, 메시지 변경 등을 수행할 수 있다.

운영(Green)팀은 IT 시스템을 운영하는 집단이다. 운영팀의 특징은, IT에 대한 지식을 가지고 있으며, 시스템상의 데이터에 직접적으로 접근할 수 있는 권한도 가지고 있다. 또한, 경우에 따라서 운영팀의 최고 관리자는 시스템에 루트 계정으로 접근하는 것도 가능하다. 그러나, 실무팀과 운영팀은 어디까지나 내부 직원 역할이므로, 운영팀의 속성은 악의를 가진 행동은 하지 않는다고 가정한다.

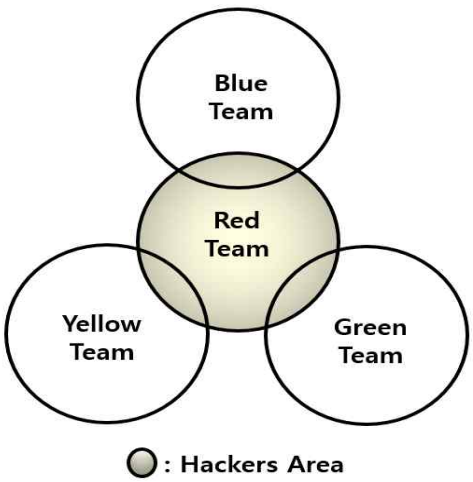
공격(Red)팀은 실질적으로 IoT 클라우드 시스템을 해킹하여 어떠한 정보를 갈취하거나, 시스템을 작동 불능에 빠뜨리거나, 메시지의 교란으로 시스템 가동이 원활하지 않게 하는 악의적인 해커 집단이다. 한편, 본 논문에서는 해커가 공격팀에만 존재하지는 않으며 다양한 곳에 해커가 존재할 수 있다는 기본 가정에서 시작하였으며, 공격팀에서는 실질적으로 팀단위로 조직적인 공격을 수행한다는 특징이 있다.

방어(Blue)팀은 해킹의 공격을 적극적으로 방어하는 보안팀에 해당한다. 방어팀의 주요 존재 목적은 해커의 공격을 원천적으로, 혹은 실시간으로 차단하는 데 있다. 방어팀은 보안전문집단이며, 보안에 대한 깊은 지식을 가지고 있다. 또한, 실무팀, 운영팀 등의 활동을 모니터링하여 잠재적 해커 여부도 확인할 수 있어야 한다.

② 해커의 활동 영역

본 논문에서는 해커가 모든 팀에 존재할 수 있는 것으로 가정하였다. 실제 환경을 가정하였을때, 해커는 기업 내외 어디에서나 존재할 수 있으며, 예컨데 내부자에 의한 정보 노출 행위도 발생할 수 있다. 여기서는 악의를 가진 내부직원까지 모두 포함하여 해커로 규정하며, 해킹의 목적은 기업 중요정보 유출이 될 수도 있고, 악의를 가진 측에 의한 산업시스템 무력화가 될 수도 있다.

아래 그림은 해커의 출현 범위를 나타낸다. 실질적으로 대부분의 해커는 공격팀에 속해 있으나, 실무팀, 운영팀, 방어팀 내부에도 일부의 해커가 있을 수 있다. 공격팀이 아닌 곳에 속한 해커는 잠재적 스파이 역할을 수행하며, 내부에서 독립적으로, 혹은 공격팀과 연계해서 IIoT/CPS 시스템에 해킹을 감행한다. 전제하는 것으로, 방어팀은 스파이의 존재 여부나 규모에 대해서는 알 수 없어야 한다.



<그림 VI-11> 해커의 공격범위

③ 기존 모의훈련 방식과의 비교

가) 대응 메뉴얼 기반 모의훈련 방식

대응 메뉴얼 기반의 모의훈련 방식은 근본적으로 다양한 해킹의 방식에 대해 완전하게 메뉴얼을 구성하기 어렵다는데 단점이 있다. 일반적으로 대응 메뉴얼 기반 방식은 훈련 발생 상황 시나리오가 정해지면, 그에 대응하는 절차를 따르도록 되어 있는 것이 일반적이며, 이러한 방법은 전문지식을 가지고 있지 않은 조직의 부서에서 수행하기에는 적절하나, 정보보안 전문가 집단의 훈련방법으로 사용되기는 어려운 경향이 있다.

나) 공격/방어팀 기반 모의훈련 방식

최근에 많이 수행되고 있는 방법으로, 공격팀과 방어팀을 구분하여 훈련 시나리오를 구성하는 것으로 대응 메뉴얼 기반의 모의훈련 방식보다는 실전적인 훈련이 가능하다. 그러나, 공격/방어팀의 구성만으로는 실제로 발생가능한 시나리오를 구성하는데 한계가 있다. 예를 들어, 내부자에 의한 데이터 노출 시나리오라던가, 실무자를 대상으로 한 변조, 위조 등의 시나리오인 경우는 실질적으로 운영팀과 실무팀의 가상 훈련 세트를 구성하지 않고서는 실질적으로 수행하기 어려운 측면이 있다. 특히, 본 논문에서 제시하는 '방어팀 내부의 스파이 존재'와 같은 시나리오와 같이 다양한 케이스의 시나리오 적용에는 한계가 있다는 단점이 있다.

다) 제안된 모의훈련 방식

제안하는 방식은 기존의 대응 메뉴얼 기반 방식 및 공격/방어팀 기반의 방식에 비해 보다 실제 환경에 적합한 시나리오를 구성할 수 있다는 데 장점이 있으며, 특히, 실무, 운영, 방어팀에 공격 스파이에 대한 배정이 가능함으로써 IoT 클라우드 환경에서의 예측하지 못한 위협에 대한 발견이 가능하다. 또한, 앞서 언급한 다양한 훈련 시나리오를 기반으로 여러 많은 복합적인 파생 시나리오를 생성할 수있어 제안한 방법을 기반으로 보다 실전적인 보안위협 및 해킹 시나리오를 생성할 수 있다는 장점이 있다.

앞서 분석된 내용을 바탕으로, 메뉴얼 대응 방식과 공격/방어팀 훈련 방식, 제안된 훈련 방식을 각각 비교하면 아래 표와 같다.

<표 VI-4> 사이버 모의해킹 훈련방식 비교

	공격 패턴 랜덤화	훈련 시나리오 다양성	실전적 훈련 여부
메뉴얼 대응 방식	낮음	보통	보통
공격/방어팀방식	높음	다소높음	높음
제안 방식	높음	높음	매우높음

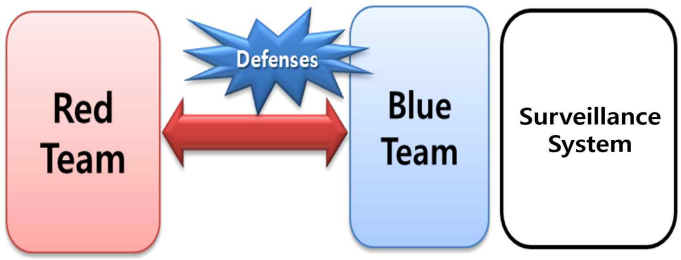
메뉴얼 대응방식은 공격패턴을 다양하게 생성하기 어려운 측면이 있으나, 공격/방어팀 및 제안 방식은 다양하고 즉흥적인 공격 패턴 생성이 가능하다. 또한, 훈련 시나리오의 다양성 측면에서는 메뉴얼 대응 방식은 짜여진 결과에 대한 시나리오를 작성해야 한다는 측면에서 한계가 있다. 한편, 공격/방어팀 방식은 이보다는 자유로운 공격방법의 구성이 가능하나, 실전과 유사한 훈련 환경 시나리오 제공에는 한계가 있다. 제안하는 방식은 앞서 언급된 시나리오를 기반으로 다양한 종류의 시나리오와 실전적인 훈련 환경을 제공할 수 있다는 장점이 있다.

2) 시나리오 #1 - 기본 공격과 방어

제안하는 방법에서 발생할 수 있는 세부 공격 시나리오는 크게 1) 기본 공격과 방어, 2) 적극적 공격 수행, 3) 중간자 공격 시나리오, 4) 내부자에 의한 공격의 네가지로 나눌수 있다. 본 장에서는 이에 대한 구체적인 세부 공격 시나리오에 대해 설명하고, 이에 대한 안전성을 분석한다.

가) Scenario #1 : 기본 공격과 방어

아래 그림은 기본적인 공격 시나리오를 나타낸다. 공격팀에서는 IIoT/CPS 시스템에 접근하여, 데이터 수집, 작동 교란, 시스템 무력화, 불법권한 취득 등 다양한 방식의 공격을 시도하고자 하며, 방어팀에서는 이러한 공격팀의 활동을 차단하는 역할을 수행한다. 여기에서 나타난 공격방법은 일반적이며 가장 기본적인 공격방법에 해당한다.

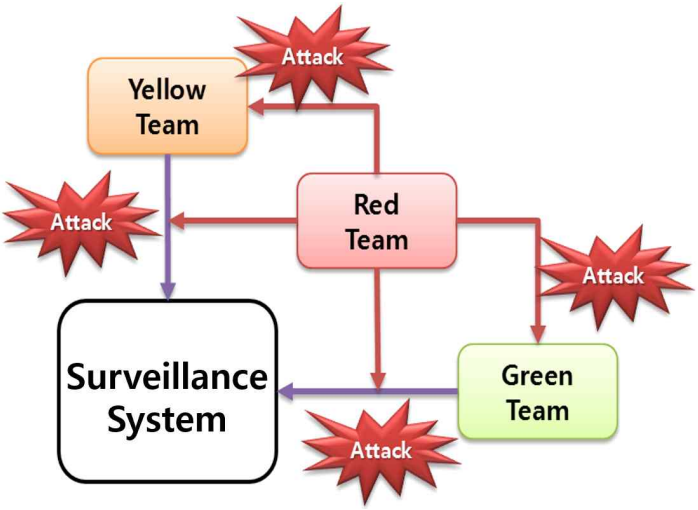


<그림 VI-12> 공격 시나리오 #1

제안한 프레임워크에서는 CCTV 영상 전달은 종단간 암호화를 수행하여, 데이터는 비식별화를 수행하여 평문을 노출하지 않는다. 따라서, 데이터 수집 등 불법적인 정보 수집에 있어 안전하다. 또한, CCTV와 영상감시 서버간 동기화 프로토콜을 제공하므로 작동 교란, 시스템 무력화의 공격이 발생하더라도, 영상정보 데이터에 대한 손실이 발생하지 않는다는 장점이 있다.

3) 시나리오 #2 - 적극적 공격 수행

아래 그림은 적극적 공격 수행 방법을 나타낸다. 이 시나리오에서는 공격팀에서의 실무팀과 운영팀에 대한 해킹 및 통신 채널상에서의 해킹을 가능하게 한다. 즉, 공격팀에서는 시나리오 #1에 비해 훨씬 다양한 방법을 동원한 해킹 시도가 가능하다. 여기에는 우선 CCTV 기기를 작동하는 실무팀과 기기간 메세지 교란, 위조, 도청 혹은 위장공격 등을 감행할 수 있다. 이러한 공격을 수행하면 지능형 감시 시스템이 정상적으로 작동하지 않거나, 도청 공격에 의해 CCTV 장비 작동 과정에서 발생하는 중요 정보가 취득될 수 있다. 또한, 운영팀에 대해서도 동일한 공격을 감행할 수 있으며, 실질적으로 운영팀이 메인 서버에 접근시 시스템 관련 주요 정보가 노출될 가능성이 크며, 시스템 접근권한의 불법취득에 따른 다양한 종류의 해킹과 오작동이 발생할 수 있다. 따라서, 이러한 다양한 해킹 공격에 대해 보안에 대한 대비를 철저히 할 필요가 있다.

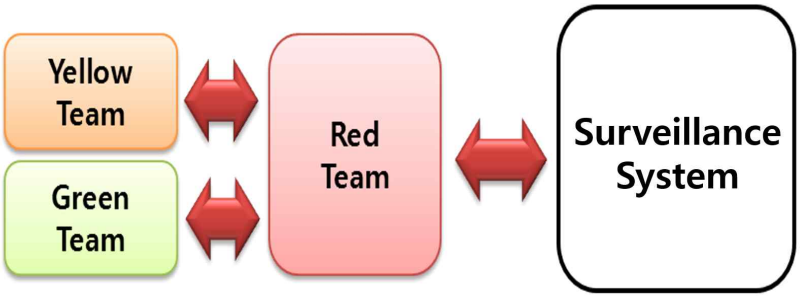


<그림 VI-13> 공격 시나리오 #2

제안한 방식은 기본적으로 동기화 과정에서 종단간 암호화가 제공된다. 따라서, 통신 채널상에서의 해킹이 발생하더라도 공격자는 평문을 복원할 수 없다. 평문 복원을 위해서는 반드시 복호화 키를 알고 있어야 하며, 이는 동기화 과정에서 서버에서 인가 받은 장치와 백업서버의 통신간에서만 알고 있으므로 공격자의 채널상 다양한 공격을 방지할 수 있다.

4) 시나리오 #3 - 중간자 공격

아래 그림은 중간자 공격 시나리오를 나타낸다. 여기에서는 공격팀이 운영팀과 실무팀의 통신 채널 사이에서 정보를 가로채거나 대신 발송하거나 응답할 수 있으며, 일반적으로 이 경우는 실무팀과 운영팀에서 중간자 공격 발생 여부를 감지하기가 쉽지 않다. 아래 그림은 실무팀과 운영팀이 지능형 감시 시스템에 접근하고자 하는 경우이며, 공격팀은 이러한 네트워크 통신을 조작하여 변경된 통신 내용을 발송할 수 있다. 중간자공격은 공격자의 노출을 최소화하면서 통신 내용에 대한 감청 및 위조가 가능한 특징이 있으며, 이에 대한 대응책을 방어팀에서 항시 대비하여야 한다.



<그림 VI-14> 공격 시나리오 #3

중간자 공격 시 CCTV상의 데이터를 임의로 조작하여 넣는 경우를 생각해 볼 수 있다. 그러나, 이러한 경우는 공격자가 암호화 키를 알지 못하므로, 데이터에 대한 블록 ID를 생성할 수 없다. 따라서, 변조된 데이터를 클라우드 서버에 전송하더라도 서버는 해당 블럭이 변경되었음을 감지할 수 있다. 또한, 종단간 전송되는 데이터는 모두 암호호되므로 중간자공격 시나리오에서 효과적인 공격을 수행할 수 없다.

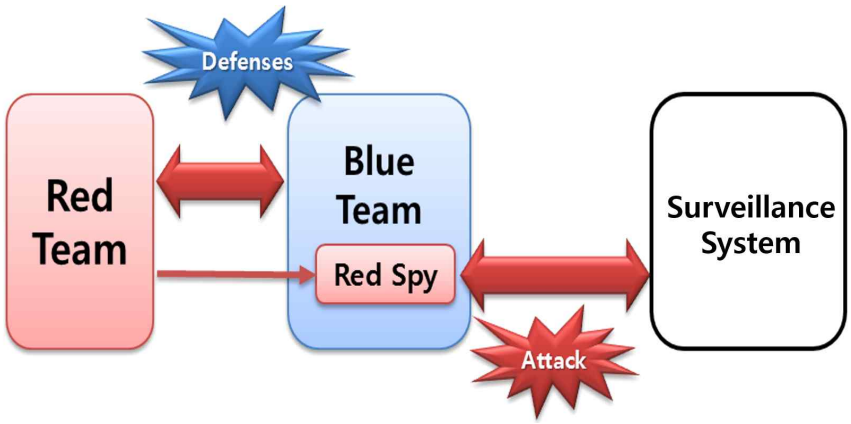
5) 시나리오 #4 - 내부자 공격

아래 그림은 내부자에 의한 시스템 공격 시나리오를 나타낸다. 실질적으로 여기에서는 공격팀이 직접 개입하지는 않으며, 실무팀이나 운영팀 내부 직원 가운데 악의를 가진 한명 또는 일부가 해당 팀의 팀원으로 존재하는 경우이다. 최근 내부자의 공격 빈도가 높아지고 있는 추세이며, 이러한 내부자의 공격에 대한 모의 방어훈련을 하기 위해, 각 팀에 스파이를 일부 투입하는 형태로 시나리오를 구성하였다. 실무팀에 속한 스파이는 공격자임에도 불구하고, 지능형 감시 시스템에 실무팀의 권한으로 그대로 접근이 가능하다. 이러한 위험성은 운영팀에서도 동일하게 적용되며, 운영팀에서는 관리 권한 및 중요 데이터베이스에 그대로 접근이 가능하므로 운영팀 내부자에 의한 공격은 매우 큰 보안 위협이 존재한다. 내부자의 공격위험을 방지하지 위해, 방어팀에서는 철저한 로그 관리 등 다양한 정보보안 대책을 수립할 필요가 있다.

<그림 VI-15> 공격 시나리오 #4

한편, 아래 그림은 방어팀의 내부에 스파이가 존재하는 유형의 시나리오를 나타내고 있다. 실질적으로 이러한 경우에 대해 가장 깊게 대응책을 고심할 필요가 있으며, 실제로도 이러한 상황이 발생하지 않는다는 보장을 할 수 없으므로 항시 대비가 필요하다.

본 논문에서는 이러한 다양한 상황을 가정하여 방어팀이 대응해야 하는 것을 제안하며, 이는 과거의 일반적인 메뉴얼에 따른 정보보안 대책이나 공격/방어 양팀을 통한 모의훈련 환경보다 더욱 해결 난이도가 높은 보안 훈련 환경을 제공한다는 특징이 있다.



<그림 VI-16> 공격 시나리오 #5

제안한 프레임워크에서는 내부자 공격 시나리오 상에서, 관리자 계정을 가진 자에 의해 접근이 가능할 경우에도 관리자는 비식별화된 메타정보만 획득할 수 있다. 즉, 인증된 영상감시서버가 가지고 있는 암호화 키를 알지 못하면 데이터베이스 혹은 스토리지에서 취득한 데이터에 대한 평문 복원이 불가능하다. 이러한 점은 제안한 프레임워크가 다양한 시나리오상에서 메타정보 및 스토리지에 저장된 영상정보를 안전하게 취급할 수 있음을 보인다.

3. 기존 방식과의 비교분석

1) 안전성 측면 비교

(1) 비식별화 알고리즘 비교

① 영상 데이터의 외부 노출

영상 데이터는 메타정보가 저장된 메타 데이터베이스와 실제 CCTV 영상이 저장된 영상 스토리지로 구성되어 있다. CCTV 영상 데이터는 그 자체만으로 개인정보의 성격을 가지고 있다. 비디오 영상에 촬영된 개인의 위치, 동선을 CCTV 영상정보만으로 직접적으로 파악할 수 있기 때문이다. 이러한 분석 정보는 영상 메타데이터상에 기록되며, 영상 CCTV 데이터 및 영상 메타 데이터는 그 자체로서 프라이버시 침해 요소를 지니고 있다고 볼 수 있다. 이에 대한 가장 안전한 방법은 데이터를 암호화하는 것이다. 본 논문에서 제안하는 방법에서는 실제 스토리지 상에 저장되어 있는 CCTV 영상 데이터는 모두 암호화를 적용하므로 공격자에게 스토리지상의 영상데이터가 노출되더라도 안전하다. 한편, 영상 메타데이터는 COP-변환 방식으로 변환된 데이터로 구성되어 으므로 공격자는 초기 비밀 공유값인 D와 의사난수 발생에 필요한 초기 seed를 알지 못하면 COP 변환 값을 구성할 수 없다. 즉, 메타정보, CCTV 영상정보 어디에도 직접적으로 개인정보를 평문 형태로 저장하지 않으므로 불가피하게 영상데이터 전체가 외부에 노출되더라도 안전성을 보장할 수 있다.

② 메타 질의과정 노출

검색을 위한 메타정보 질의시 메타정보 검색에 사용된 SQL문 및 질의 실행 결과값을 획득하는 것만으로 영상 CCTV 내용의 유추가 가능할 수 있다. 그러나, 제안한 방식에서는 영상메타 질의시 SQL상에 평문 메타를 노출하지 않는다. 또한, 데이터베이스상의 메타정보값 전체가 COP-변환 기법으로 변환되어 있으므로 SQL 질의를 통하여 검색된 결과값 또한 변환값 형태로 리턴한다. 따라

서, 영상메타 질의 및 리턴 데이터를 공격자가 모두 확보하게 되더라도, 해당 변환값으로부터 원본 평문을 복원할 수 없어 안전하다.

③ 내부자 공격

CCTV 비디오 영상은 대용량 데이터이므로 클라우드 스토리지상에 보관하는 경우가 많다. 특히, 클라우드 환경에서는 클라우드 시스템 운영자 등 내부자 공격에 주의할 필요가 있다. 여기에서, 내부자는 데이터베이스와 스토리지에 상시 접근이 가능하다. 본 논문에서 제안하는 기법은 초기 공유값인 D를 인가된 권한이 있는 자에게만 공유한다. 또한 메타정보를 포함한 데이터베이스는 COP 변환 기법을 적용하여 데이터가 변환되어 있으며, 스토리지 CCTV 영상 데이터는 전체 파일이 암호화되어 있다. 여기에서, 내부자 등 관리자 입장에서의 파일 및 데이터 접근 권한과 실제 영상감시 처리 업무자의 평문 데이터 확인 권한은 서로 다르게 적용될 필요가 있다. 즉, 초기 공유값인 D를 실질적인 정보 열람 권한이 있는 자에게만 공유하여야 한다. 따라서, 클라우드 스토리지 관리자는 암호화된 상태의 데이터에 접근은 가능하나, 정보 열람에 대한 권한이 없으면 데이터베이스 및 스토리지로부터 평문 정보를 복원할 수 없다.

④ 데이터베이스 노출

평문 데이터의 경우는 데이터베이스가 노출되면 모든 정보가 노출된다. 따라서, 개인정보는 고스란히 침해될 수 밖에 없다. 만약, 순서보존 암호화가 된 경우라면 평문 자체의 노출은 되지 않으나, 데이터의 순서가 노출되며, 이는 감시 데이터의 분석을 용이하게 한다. 예를 들어, 미터링 데이터의 분석으로 특정시간에 개인이 집에 있는지를 파악한다면 순서보존 암호화를 적용하더라도 그대로 나타나게 될 것이다.

그러나 제안하는 방식은 데이터베이스에서의 노출이 있더라도, 시간 정보를 연결할 수 없어서 비식별화된 데이터만으로는 쉽사리 개인정보를 판단할 수 없다. 모든 시간정보는 전체적으로 암호화가 되어 있으므로, 측정 데이터와 시간정보를 매핑할 수 없어서 사용자의 패턴을 파악할 수 없기 때문이다.

⑤ 데이터 카운팅

데이터 카운팅 공격은 일반적인 암호 알고리즘을 적용하더라도 문제가 그대로 발생한다. 즉, 특정 데이터의 분포가 알려져 있을 경우, 해당 데이터가 몇개인지를 카운팅하는것 만으로 대략적인 원본 데이터를 유추할 수 있다. 이러한 공격은 동일한 평문에서도 각각 상이한 결과가 나타나는 알고리즘을 사용해야 해결이 가능하다. 제안하는 방식은 그룹단위로 랜덤값이 추가되어, 동일한 값이라 할지라도 버킷단위로 값이 다르게 발생한다. 만약, 그룹 사이즈가 일정하다면 데이터 카운팅에 대한 유효한 분석 방법이 존재할 수 있으나, 본 논문에서 제안하는 방식은 가변 사이즈의 그룹화를 적용하여 데이터 카운팅 공격을 어렵게 한다.

⑥ 질의문 분석 공격

제안된 방식에서는 만약 신뢰된 서버와 클라우드 서버간 질의문을 모두 엿볼 수 있다고 해도, 원본 데이터에 대한 노출은 발생하지 않는다. 신뢰 영역과 클라우드 서버는 그룹 아이디 기반의 질의만 수행되므로 질의문 분석 자체로는 평문을 유추할 수 있는 정보나 어떤 위험한 정보도 노출하지는 않는다. 다만, 질의문 상에서 어느 그룹 아이디가 얼마나 빈번히 질의되었는가 하는 부분에 대한 정보는 파악될 수 있다. 이러한 것이 비록 치명적인 부분은 아니나, 안전성의 향상을 위해 신뢰 서버와 클라우드 서버간 암호화된 채널을 통하여 질의문이 전달될 것이 권장된다.

⑦ 비식별화 안전성 비교분석

평문의 경우는 데이터베이스의 노출, 데이터 카운팅, 쿼리 분석 모두 취약함을 보인다. 이는 데이터베이스의 성능을 얻는 대신 안전성은 포기하는 것이라고 볼 수 있다. 한편, 대표적인 순서보존 암호화 알고리즘인 OPES의 경우는 데이터베이스 전체가 노출될 상황이 발생할 경우, 데이터의 순서가 그대로 노출되므로 결코 안전하다고 할 수는 없다. 그러나, OPES의 장점인 원본 데이터의 분포를 변경하는 특성에 따라, 일정 수준의 안전성은 가지고 있다. 한편, 데이터 카운팅에는 취약한 편이며, 이러한 특성은 일반적인 암호화 알고리즘을 적용하더라도 마

찬가지이다. 일치검색시 정확한 데이터를 가져오려면 모두 같은 키로 암호화를 해야 하기 때문이다. 제안한 방법은 그룹 아이디 및 시간정보의 암호화 적용을 통하여, 데이터가 노출되어도 시간순으로 수치 데이터를 배열할 수 없으므로 OPES에 비해 안전하다.

또한, 수치 데이터 변경 시 그룹 단위로 랜덤 값이 변경되므로 타 그룹간은 데이터 카운팅 공격을 실시할 수 없으며, 질의문 분석 시에도 그룹아이디 이외에 특별한 정보는 획득할 수 없다는 특성이 있다.

<표 VII-1> 센싱데이터 비식별화 보안성 분석

	Database Exposure	Data Counting	Query Analysis
Plaintext	×	×	×
OPES	△	×	△
Encryption	○	×	○
The Proposed Method	○	△	○

(2) 영상 동기화 방식 비교

① 데이터 변조 공격

H-Tree 기반의 동기화 방식은 데이터 변조 공격으로부터 취약한 측면이 있다. 변조하고자 하는 데이터 블럭을 임의로 수정하고, 해당 블럭에 대한 해쉬값을 취한 후 모든 상위 해쉬 트리에 대하여 재해쉬처리하면, H-Tree의 수신자는 해당 데이터가 변조되었는지를 확인할 수 없다. 만약 악의를 가진 자가 임의로 데이터를 수정하여 백업서버 측에 조작된 데이터를 전송한다면, 이는 개인의 안전에 큰 영향을 받게 될 수도 있다.

제안한 SH-Tree 방식은 변조되지 않았다는 부분에 대한 검증이 가능하다. SH-Tree의 메타정보상에 평문 데이터 블록의 해쉬값을 가지고 있으며, 동기화 이후 최종 상태에서 수신 데이터를 해쉬처리하고 이 평문 데이터 블록의 해쉬값이 일치하는지를 비교하면 실제로 변조되지 않았음을 알 수 있다.

즉, 공격자는 데이터를 임의로 변조하더라도 해당 평문 데이터 블록의 해쉬값을 생성할 수 없다. 이는 데이터 블록단위로 각각 다른 암호화 키를 가지고 있으므로 공격자는 해당 암호화된 데이터 블록으로 부터 평문을 복호화 할 수 없기 때문이다.

만약, SH-Tree상의 데이터를 무작위로 변경하였을 경우에도 실제 데이터의 블록 해쉬값과 SH-Tree상의 해쉬값이 일치하지 않으므로 정상적이지 않은 데이터임을 알 수 있을 것이다. 이러한 경우, 백업서버는 변조된 상황임을 감지하고 CCTV 영상장치로부터 다시 정확한 정보를 재요청하여야 한다.

② 무결성 보장

제안하는 방식은 H-Tree 방식과 동일하게 무결성을 보장해 준다. 데이터 통신 과정에서 손실 등으로 문제가 발생할 경우, 데이터의 해쉬값은 달라질 것이다. 이 경우, 최상위 트리값인 Root값 또한 달라지게 되며, 이를 기반으로 실제 데이터가 훼손되었는지를 안전하고 효율적으로 판단할 수 있다. 이러한 무결성 보장은 H-Tree에서 기본적으로 제공하는 속성이며, 제안한 방식은 이 장점을 동일하게 갖는다.

특히, 데이터의 손실이 어느 블록에서 발생하였는지를 구체적으로 알 수 있으며, 백업서버 측에서는 손실이 감지된 데이터 블록을 CCTV 영상장치에 재요청하여 갱신해야 한다.

③ 메시지 도청 공격

H-Tree 기반의 동기화 방식은 보안에 대한 별도의 고려를 하지 않고 있어, 메시지의 도청으로부터 안전하지 않다. 그러나, 제안한 방식은 전송되는 모든 데이터가 암호화되어 관리된다. 특히, 데이터 블록 단위로 각각 다른 키가 적용되어 암호화되므로, 공격자는 메시지 도청 공격을 실시할 수 없다. 또한, 이러한 특징은 데이터 블록이 어떤 반복적인 패턴을 가지고 있는지에 대한 추정도 어렵게 한다.

④ 안전성 비교

해쉬 목록만으로 변경여부를 감지하는 Hash List 기반의 동기화 방식과 H-Tree 기반의 동기화 방식은 메시지 변조 공격에 대해서 안전하지 않다. 변조된 데이터 및 상위 트리의 값을 재해쉬 처리하면 실제로 데이터를 수신한 측은 데이터의 변조가 일어났는지 여부를 판단할 수 없기 때문이다. 그러나, 제안하는 방식은 SH-Tree 자체만으로 데이터의 검증이 가능하여 데이터 변조 공격을 방지할 수 있다. 한편, 무결성은 해쉬 기반 동기화 방식이 공통적으로 갖는 장점이며, H-Tree 및 제안한 방식 모두 공통적으로 가지고 있다. 한편, Hash List는 Root Hash 값이 존재하지 않으므로, 단일 Hash 값으로는 데이터의 무결성을 확인할 수 없고, 전체 해쉬값에 대하여 선형검색을 수행함으로써 데이터의 무결성 확인이 가능하다는 단점이 있다. 또한, Hash List와 H-Tree 방식은 보안에 대한 고려는 명시하지 않고 있어, 스니핑 공격으로부터 안전하지 않다. 제안한 방법은 암호화된 데이터 블록을 기반으로 SH-Tree를 생성하며, 데이터 전송 과정에서 암호화가 발생하고, 각각의 블록 단위로 다른 키를 갖게 되므로 스니핑 공격에서 안전하다는 장점이 있다.

<표 VII-2> 영상데이터 보안 동기화 안전성 분석

	Hash List	H-Tree	SH-Tree (Our Method)
Modification	×	×	○
Integrity	△	○	○
Sniffing Attack	×	×	○

2) 효율성 측면 비교

(1) 비식별화 방식 비교

① 암호화 영상정보 처리성능

CCTV 영상 데이터 전체가 암호화된 경우, 이에 대한 메타 질의 등을 수행하더라도, 특정한 조건에 맞는 영상 파일을 획득하려면 해당 파일 전체를 복호화하

여야 한다. 이러한 점은 데이터 검색 속도를 현저히 떨어뜨리는 요인이 될 수 있어 비효율적이다. 제안하는 방식은 데이터 암호화 시 Chunk 단위로 파일을 여러 단위로 분할하여 암호화를 하는 특징을 가지고 있으어, 필요한 조건으로 영상메타 데이터에 대한 질의 수행시 영상 파일의 일부 조각에 해당하는부분 영상 파일에 대한 Chunk ID를 리턴받을 수 있다. 따라서, 제안하는 방식은 전체 CCTV 영상데이터를 복호화하지 않고 Chunk 단위의 검색 조건에 부합하는 부분영상정보만을 획득하여 복호화를 수행하므로 데이터 복호화 성능 관점에서 효율성을 갖는다.

② 질의문 구성의 효율성

메타정보 검색을 위한 질의문 구성시 COP-변환 기법을 적용한 데이터는 평문과 동일한 수준의 질의 처리 효율성을 갖는다. 즉, COP-변환 데이터베이스는 일치검색, 전방일치검색, 범위검색 뿐만 아니라 복수의 테이블에 대한 JOIN을 활용한 질의도 가능하다. 또한, 메타정보에 대한 통계분석 시에도 질의문을 간단히 구성할 수 있다. 예를 들어, 특정 조건 하에서의 MIN, MAX, COUNT, AVG와 같은 통계에 필요한 집계(Aggregation) 질의를 COP-변환 메타데이터상에 그대로 적용할 수 있다는 장점이 있다. 이러한 장점은 데이터베이스를 단순 암호화한 상태에서는 달성할 수 없다. 만약, 데이터베이스를 일반적인 암호화 방식으로 암호화하게 되는 경우 실질적으로 일치검색 이외에는 질의문 구성이 매우 어렵게 된다. 예를 들어, 범위검색 질의가 필요한 경우, 암호화된 데이터베이스는 평문의 결과값과 정렬 순서가 서로 상이하므로 전체 데이터를 복호화한 데이터를 별도로 보관하고 있지 않는다면 직접적인 SQL 범위검색 질의 구성은 불가능하다. 본 논문에서 제안하는 방식은 COP-변환 메타 그대로 범위검색 적용이 가능할 뿐만 아니라, 데이터베이스 인덱스 정보를 그대로 활용할 수 있어 속도 측면에서 크게 효율적이다. 아래 표는 메타정보에 대한 평문, 암호화, COP-변환의 경우에 대한 질의 처리 가능 여부를 나타내고 있다. 평문의 경우는 일치검색, 범위검색, 집계검색이 가능하나, 메타데이터를 암호화할 경우는 일치검색 이외 범위검색, 집계검색에 대한 질의문 구성이 불가능하다. 제안하는 기법은 평문과 동일하게 일치검색, 범위검색, 집계검색을 지원하며, 데이터베이스의 인덱스를 그대로 활용 가능하여 효율적이다.

<표 VII-3> COP-메타변환 방식 효율성 분석

Query Type	Plaintext	Encryption	The Proposed Method
Equation Query	○	○	○
Range Query	○	×	○
Aggregation Query	○	×	○

③ 범위검색

평문에 대한 범위검색은 1회의 SQL Select문을 구성함으로써 모든 정보의 검색이 가능하다. 한편, 제안한 비식별화 방식은 범위에 해당하는 그룹의 개수만큼 Select 문을 구성하는 것으로 처리한다. 만약, 데이터를 암호화 했을 경우는 범위내 모든 Row에 대한 개수만큼의 Select문을 구성해야 한다. 관리자의 입장과 가용성을 고려할때 간단한 SQL 질의만으로 정보를 가져오는 것이 효율적이고 편리하다. 그러나, 데이터의 안전성을 위해서는 암호화를 하는 것이 가장 안전하다. 하지만, 데이터의 암호화 수행 시 정렬순서의 범위검색이 불가능하게 된다는 부분에서 가장 큰 단점이 있다. 제안한 방법은 이러한 부분을 상호 보완해 주는 측면이 있다. 아래의 SQL은 질의로 가져와야 할 범위에 속하는 그룹이 두개일 때를 가정하고 있다.

◉ 평문의 경우 : Select {Field} from {Table} Where {Datetime} Between {A} and {B}

◉ 암호화 방식의 경우 : Select {Field} from {Table} Where {$E(DT_1)$} = {$E(DT_1)$}, ... , Select {Field} from {Table} Where {$E(DT_n)$} = {$E(DT_n)$}

◉ 제안한 방식 : Select {Field} from {Table} Where GroupID = {GID_1}, Select {Field} from {Table} Where GroupID = {GID_n}

제안한 방식은 두개의 Select로써 구성되며, 암호화된 방식은 Row 개수만큼의 SQL 질의가 필요하다. 만약 두개 이상의 그룹을 갖는 범위를 질의할 경우에는 해당하는 그룹 개수만큼 {GID_1}, ... , {GID_n}을 GroupID의 일치검색 조건으로 각각 질의하여 결과를 얻을 수 있다.

④ 집계검색

집계검색은 대표적으로 MIN,MAX,AVG, COUNT,SUM 과 같이 특정 데이터의 집합에 대한 단일한 결과를 리턴하는 질의 방법을 의미한다. 집계검색은 통계처리시 유용하게 사용되는 질의이며, 평문의 경우는 모든 집계검색이 유의미하다. 그러나, 암호화 방식을 적용한 경우는 순서의 불일치로 인하여 집계검색 질의를 적용할 수 없으며, 질의를 한다 하더라도 무의미한 값이 리턴된다. 그러나, 제안한 방식은 비식별화된 데이터에 대해 그대로 질의하더라도 MIN,MAX,COUNT에 대해서는 정상적인 결과를 보장한다는 장점이 있다. 그러나, 수치데이터 자체가 변경되므로 AVG와 SUM에 대해서는 정확한 값이 발생하지 않는다.

⑤ 질의 회수

범위검색과 집계검색시 각각 평문은 한번의 Select문의 질의만으로 데이터를 가져온다. 그러나, 암호화된 데이터는 범위내의 그룹 개수가 c라고 가정할 경우, c개의 그룹 내의 각각의 원소들의 개수를 모두 합산한 만큼의 질의가 필요하므로 매우 비효율적이다. 한편, 제안한 방식은 범위 내 그룹 개수인 c회 만큼의 질의만 수행하게 되므로 평문에 비해서는 다소 횟수가 증가하나 암호화 방식에 질의하는 것에 비하면 매우 효율적이라고 볼 수 있다.

<표 VII-4> 센싱데이터 비식별화 방식 효율성 분석

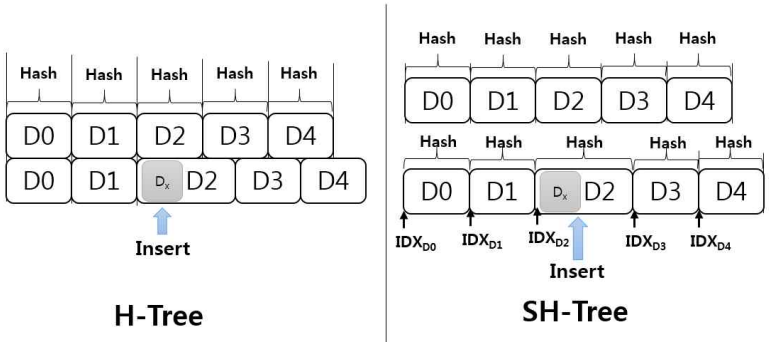
Item	Range Query	Aggregation Query
Plaintext	1	1
Encryption	$\sum_{i=1}^{c} P_i^{s\|\|i}$	$\sum_{i=1}^{c} P_i^{s\|\|i}$
The Proposed Method	c	c^*

* : MIN,MAX,COUNT Query

(2) 동기화 방식 비교

① 델타 업데이트

제안한 기법은 델타 업데이트 기능을 지원하며, 이러한 점은 대역폭을 절약하며 효율적인 동기화 정보 전송이 가능하게 한다. 즉, 변경된 특정 블록에 대한 정보만 업데이트가 가능하다. 델타 업데이트를 극대화하기 위한 방안으로, SH-Tree는 가변 사이즈를 지원한다. 각 데이터 블록에 대응되는 메타정보에서 사이즈 값을 별도로 가지고 있으며, 이를 기반으로 구간별 사이즈를 정확히 산출이 가능하다. 아래 그림은 기존의 H-Tree 방식과 SH-Tree 방식을 비교하고 있다. H-Tree 방식은 동일 사이즈 내 데이터 변경에 대한 델타 업데이트는 지원 가능하나, 데이터 삽입, 혹은 삭제에 대한 부분은 지원하지 않는다. 이는 특정 블록에 데이터가 삽입되거나, 삭제되면 해당 블럭 이후 모든 블록에 대하여 해쉬값이 변경되기 때문이다. 즉, 특정 블럭에 대한 삽입이 일어나면 해당 블럭 이후의 모든 데이터 블럭에 대하여 해쉬값을 갱신해야 한다는 큰 단점이 있다. 그러나, SH-Tree의 경우는 사이즈 값이 명확히 관리되므로, 특정 블록에 대한 데이터의 삽입, 삭제가 일어나더라도 해당 블록에 대한 데이터만 변경하면 되므로 크게 효율적이다.



<그림 VI-17> 델타 업데이트 비교

제안한 방식은 델타 업데이트의 지원에 따라 동기화를 위해 모든 파일을 업데이트하지 않아도 된다는 장점과 동시에, 동기화에 소요되는 속도 향상의 측면도 있다. 이는 원본의 부분 수정 후 동기화 시 전체 데이터가 갱신되지 않고, 변경

된 블록에 대해서만 데이터가 갱신되므로 동기화 대역폭 절감 뿐 아니라 동기화 완료에 필요한 시간도 대폭 절감되기 때문이다.

② 통신 두절 관리

IoT 클라우드 환경의 특성상 천재지변 등 여러 사유로 서버와의 통신이 두절될 상황을 충분히 고려해야 하며, 이러한 경우는 인근 유무선 통신이 가능한 백업서버간의 자원만으로 최신의 정보를 업데이트해야 한다.

제안한 방식은 백업서버와 데이터 통신이 두절된 상황이라 할지라도, 브로드캐스팅 영역 내에 있는 주변 백업서버로부터 최신 데이터의 동기화가 가능하다. 이는 SH-Tree의 메타정보 가운데 데이터 블록의 버전정보를 별도로 관리하기 때문이다. 각 블록의 버전값 비교를 통하여 어느 블록이 최신 버전인지, 어느 블록을 기준으로 갱신해야 할지를 결정할 수 있다.

③ 데이터 중복 제거

Hash List 방식과 H-Tree 기반의 동기화 방식은 데이터 중복 제거를 별도로 명시하지 않고 있다. 그러나, 이론상으로는 이러한 방식도 해쉬값에 대해서 매핑 테이블 기반의 중복제거 방식을 적용하면 데이터 중복 제거에 적용이 가능할 수 있다. 그러나, 이는 근본적으로 가변 사이즈의 데이터가 관리되지 않기 때문에 데이터 삽입/삭제 시 해당 블록 이후의 전체 블록에 대해서 데이터 변경이 일어나므로 실질적으로 데이터 중복 제거에 대한 효과를 크게 기대할 수 없다. 데이터 중복 제거는 동일한 내용을 가진 데이터 블록의 갯수가 최대한 많을수록 효율적이다. 이러한 관점에서는 데이터 삽입/삭제에 따라 데이터 변동폭이 큰 Hash List 및 H-Tree방식은 적합하지 않다고 볼 수 있다.

그러나, 제안한 방식은 가변 사이즈 방식의 데이터 블록 관리를 지원하며, 이러한 장점은 데이터 중복 제거에 있어서 큰 효과를 기대할 수 있다. 특정 블록에 대한 삽입과 삭제가 일어나도 해당 블록 이외의 블록에 대해서는 영향을 미치지 않고, 해당 블록에 대해서만 갱신하면 된다는 장점이 있어 데이터 중복 제거 효율을 크게 높인다.

④ 변경사항 추출 성능

SH-Tree 기반의 추출 방법은 블록 아이디를 단순 목록으로 가지고 있는 Hash List 방식에 비해 검색성능이 뛰어나다. 각 데이터 블록에 대한 해쉬값을 Hash List 방식으로 관리할 경우, 변경사항 검출시에 전체 데이터에 대한 선형 검색이 필요하므로 O(n)의 시간이 소요된다. 그러나, SH-Tree의 경우는 변경사항 검색에 O(logn)의 시간이 소요되며, 이는 종래의 H-Tree의 방식과 동일하게 장점을 가진다.

⑤ 각 방식의 효율성 비교

Hash List 방식 및 H-Tree 방식은 델타 업데이트에 대하여 동일한 사이즈 내의 변경사항에 한해서만 일부 지원하고, 데이터의 삽입, 삭제 등에 대해서는 델타 업데이트를 지원하지 않는다. 한편, 제안한 SH-Tree 방식은 메타정보에 사이즈를 별도로 관리하여 델타 업데이트를 지원한다는 장점이 있다.

또한, 통신 두절시 Hash List 방식과 H-Tree 방식으로는 데이터 동기화를 추가적으로 진행할 수 없다. 어느 데이터 블록이 더 최신 버전인지 판단할 수 있는 근거가 없기 때문이다. 그러나 제안하는 SH-Tree 방식은 블록에 대한 버전 정보를 별도로 관리하므로, 가장 최신 버전에 대한 데이터를 동기화하는 것으로, 통신 두절 시에도 인접 백업서버에 대한 데이터와 무선 통신으로 동기화가 가능하다.

한편, Hash List 및 H-Tree 방식을 데이터 중복제거 방식에 적용한다면, 특정 블록 이후로 모든 데이터가 변경되므로, 결국 해당 데이터 이후의 모든 데이터를 갱신해야 하므로 동기화 처리 비용은 선형 증가하게 된다. 그러나, 제안하는 방식은 특정 단일한 블록에 단 1회의 갱신 처리만 필요하다. 또한, 변경사항 감지에 있어서 Hash List 방식은 순차적으로 선형검색이 진행되므로, O(n)의 수행시간 내에 변경사항 검색이 가능하다. 한편, H-Tree 및 SH-Tree 방식은 동일하게 O(logn)의 시간에 변경사항 검출이 가능하다.

아래 표는 기 제안된 해쉬 기반의 동기화 방식과 본 논문에서 제안한 동기화 방식을 비교하였다. 제안한 방식은 대역폭 최소화를 위한 델타 업데이트를 지원하며, 통신 두절 상태에서도 서버와 동일한 것을 보장하지는 않더라도, 인접 서

버의 정보를 기반으로 가능한 최신 정보로 갱신하는 방식의 동기화 처리가 가능하다. 또한, 클라우드 서비스에 주요한 요소인 중복 제거를 지원하고, 효율적인 변경 감지가 가능하여 IoT 클라우드 환경에서의 동기화 서비스 제공에 적합하다고 볼 수 있다.

<표 VII-5> 보안 동기화 방식 효율성 분석

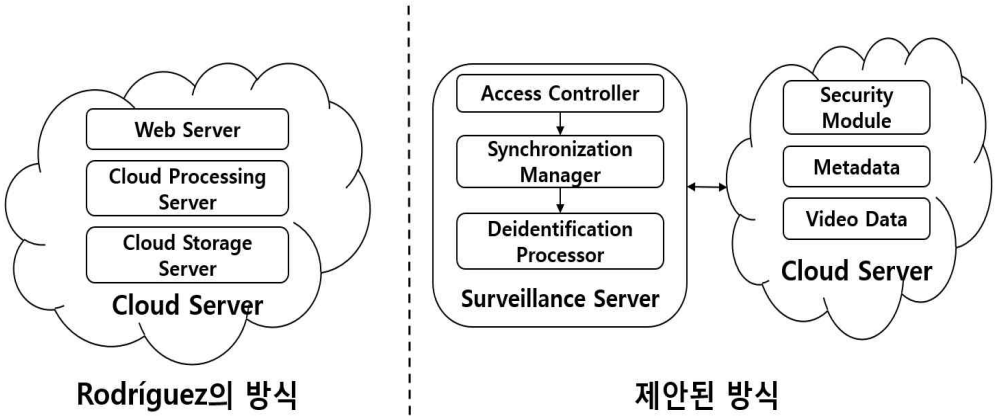
	Hash List	H-Tree	SH-Tree (Our Method)
Delta Update	△	△	○
Loss of Connection	×	×	△
De-dupli-cation	O(n)	O(n)	1
Chance Detection	O(n)	$O(\log_n)$	$O(\log_n)$

3) 기존 프레임워크와의 비교

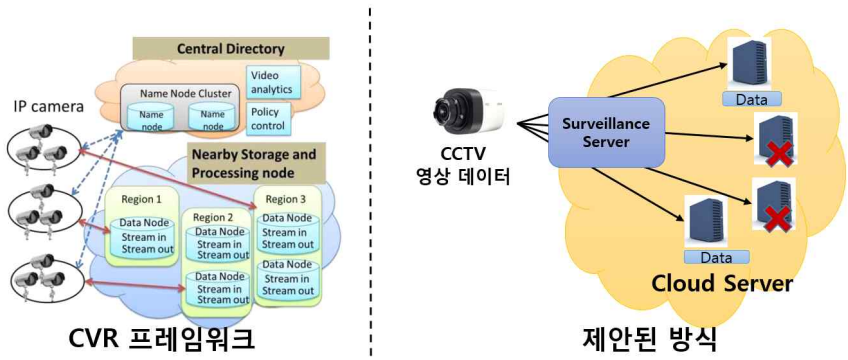
(1) 각 방식 비교

Rodríguez의 연구에서는 지능형 클라우드 영상감시 환경을 제안하였다. 또한, 해당 연구에서는 클라우드 환경에서의 보안 문제의 중요성을 언급하고 있다. 그러나, Rodríguez의 연구에서는 다음과 같은 한계점이 존재한다. 먼저, 프라이버시 보호를 위해 SSL 프로토콜을 이용할 것을 명시하고 있다. SSL은 일반적으로 널리 사용하고 있는 종단간 암호화 프로토콜이나, 실질적으로 프레임워크상에서 제공해 주는 암호화 메커니즘의 형태는 아니며, 지능형 보안 시스템 설계상의 허점이나, 내부자 공격 등에 취약할 수 있다. 또한, 데이터 저장 시 Amazon S3기반의 확장 가능한 아키텍쳐를 제안하고 있다. 즉, 클라우드 서버 전체를 지능형 감시 환경으로 사용하는 부분을 제안하고 있으나, 이러한 경우 내부자 공격에 매우 취약할 수 있다. Amazon S3에서는 자체 암호화 기능을 지원해 주나, 실질적으로 내부자 공격에 있어 자체 암호화 기능이 무력화될 수 있다. 제안된 방식은 감시 서버와 클라우드 서버를 별도로 분리하고, 클라우드 서버상에는 암호화된 데이터만 저장하도록 명시되어 있다. 즉, 클라우드 서버의 시스템 관리자 또는 내부자

라 하더라도 평문 정보를 확인할 수 없다. 평문은 반드시 감시 서버에서 재식별화 및 복호화되어 클라이언트에 전달되므로, 정보 보관시 데이터 노출이 발생하지 않는다. 또한, CVR 프레임워크에서는 사설 클라우드와 공공 클라우드를 동시에 활용하는 것으로 이러한 문제를 해결하고 있다. 실질적으로 사설 클라우드 환경을 활영하는 경우, 공공 클라우드에 비해 일반적으로 보안 위험은 크게 줄어든다. 그러나, CVR 프레임워크에서는 데이터의 전달 시, 중간자공격 또는 위장공격에 취약할 수 있다. CCTV에서 서버로 전달될 경우 각각 상이한 서버에 저장되는 과정에서 특정 서버가 실제 서버인지를 구체적으로 인증하여 위장공격 및 중간자 공격을 최소화할 필요가 있다. 제안한 방식에서는 클라우드 서버와 보안 동기화 기능을 제공해 주며, 이 과정에서 인증받지 않은 서버에는 데이터를 저장하지 않는다. 동기화 과정에서 반드시 암호 키를 알고 있는 서버만 CCTV 영상 정보를 획득할 수 있어 데이터 전송시 보안 기능을 제공한다.



<그림 VI-18> Rodríguez의 방식과 제안된 방식의 비교



<그림 VI-19> CVR 프레임워크와 제안된 방식의 비교

한편, Hossain의 연구에서 제안된 감시 프레임워크에서도 공공클라우드와 사설클라우드를 혼합하여 보안성을 제공할 것을 제안하고 있다. 또한, Hossain의 방식은 RBAC을 통한 역할기반 접근제어를 수행하여 보안성을 강화할 것을 제안하고 있다. 그러나, 실질적으로 RBAC에 있어 영상보안 정책을 어떤 방식으로 할 것인지에 대한 언급을 구체적으로 하지 않고 있으며, 기존의 RBAC은 비영상 정보에서 제공되었다는 점을 감안할 때, 차등화된 RBAC 접근제어 정보 제공이 필요하다. 실질적으로, 마스킹 정책은 정보를 완전히 차단하는것이 아니라, 일부를 공개하고 있기 때문에, 기존의 암호화된 데이터에 대한 RBAC 기반 접근제어와는 취급을 달리할 필요가 있다. 따라서, 본 논문에서는 차등레벨 RBAC 접근제어 기법을 제공한다. 이 방법은 영상을 얼마나 많이, 혹은 적게 공개할 것인지를 구체적으로 나타내고 있으며, 이러한 경우 프라이버시 마스킹에 대한 접근 수준을 제어할 수 있다는 장점이 있다.

(2) 각 프레임워크 비교 분석

Rodríguez의 방식은 외부 벤더를 사용할 것을 명시하고 있으며, CVR 프레임워크는 확장가능한 서버를 고려하여 설계되었으므로, 해당 아키텍처는 추가 확장성에 있어 용이하다. 그러나 Hossain의 방식과 제안한 방식은 추가 확장이 가능하나, CVR 프레임워크와 같은 구조적인 서버 확장 아키텍처를 세부적으로 제안하지 않는다는 측면에서 한계가 있다. 또한, Rodríguez의 방식은 Amazon S3 아키텍처를 기반으로 설계되어 실질적으로 벤더 종속적인 특성이 있다. 이러한 점은 보안 기능도 벤더에서 제공하는 보안 메커니즘을 제공받게 되므로, 독립적인 보안 기능을 제공하지 않으며, 벤더 변경 시 다른 정보보호 취약성에 대한 검토가 필요한 번거로움이 있다. CVR 프레임워크, Hossain의 방식 및 제안한 방식은 별도로 벤더의 영향을 받지 않으며, 벤더에 독립적이다.

또한, CVR 프레임워크는 자체 데이터 백업 기능을 제공하며, Rodríguez의 방식은 Amazon S3에서 제공하는 데이터 백업 기능을 통하여 데이터 백업에 대한 안정성을 가지고 있다. 그러나, CCTV와 클라우드 서버 간 보안 동기화 방식은 제공하지 않으므로, 실질적으로 클라우드 서버의 노드 레벨 단위의 인증은 이루어지지 않는다 제안한 방식은 보안 동기화를 지원하며, 보안 키를 가지고 있는

서버의 통신 과정에서 정보를 노출시키지 않으며, 인증된 서버에 한해서만 보안 동기화가 이루어질 수 있다는 장점이 있다.

한편, Rodríguez의 방식은 클라우드 망 분리상 보안기능을 제공하지 않는다. 즉, 특정 벤더 환경에 데이터가 저장되므로, 내부자 공격에 취약할 수 있다. CVR 프레임워크와 Hossain의 방식은 사설 클라우드와 공공 클라우드를 서로 분리하는 아키텍쳐를 제안함으로써 공공 클라우드의 시스템 관리자 등 내부자 공격에 안전하다. 제안한 방식은 감시서버와 클라우드서버를 별도로 분리한 구조를 제안하고 있으며, 클라우드 서버에 들어가는 데이터는 모두 비식별화 및 암호화 조치함으로써 내부자 공격 시나리오에서의 안전을 보장할 수 있다.

또한, 영상 접근제어 측면에서는 Rodríguez의 방식은 특정 벤더의 접근제어 정책을 따르게 되며, Hossain의 방식은 RBAC 기반의 접근제어 방식을 제공한다. 이러한 방식은 기본적인 접근제어 기능을 제공해 줄 수 있으나, 영상정보에 대한 얼마만큼의 정보를 제공할 것인지에 대한 차등레벨 접근제어 기능을 제공하지 않는다. 제안한 방식은 영상에 대한 차등레벨 접근제어 방식을 제공하여 보다 안전한 영상정보 관리 정책을 가질 수 있게 한다. 또한, Rodríguez의 방식, CVR 프레임워크, Hossain의 방식은 메타정보에 대한 별도의 비식별화와 같은 데이터보안 기법을 제공하지 않는다. 이러한 경우 메타정보 관리에 있어 클라우드 서버의 내부자 공격에 취약할 수 있다. 제안한 방식은 클라우드 서버상에 메타정보 보관시 비식별화 조치를 통하여 메타정보를 안전하게 보관함으로써 클라우드 기반의 지능형 감시 프레임워크에 적합하다.

<표 VII-6> 기존 프레임워크와의 비교

	Rodríguez	CVR Framework	Hossain	제안 방식
추가 확장성 고려	O	O	△	△
벤더 독립성	×	O	O	O
데이터 백업 안전성	△	△	×	O
클라우드 망분리 보안	×	O	O	△
영상 접근제어	△	×	△	O
메타정보 보안	△	×	×	O

VII. 결 론

향후 인공지능 기술의 발달에 따라, CCTV 기반 지능형 영상분석 기술 및 시장이 크게 발전하게 될 것이다. 그러나, CCTV 촬영 영상은 개인정보를 그대로 가지고 있으므로, 이에 대한 정보보호 대책이 필수적이다. 기존의 영상데이터 보호 방식은 영상 마스킹, 혹은 단순 데이터 암호화 방식에 의존하는 것이 일반적이다. 기 제안된 방식은 주로 부분적인 기술적 메커니즘의 범위 내에 제한적인 경우가 많으며, 지능형 영상감시 환경 보안을 위한 통합적인 프레임워크를 제안한 사례는 많지 않다. 현재 많은 지능형 영상감시 환경이 도입되어 사용되고 있으며, 이러한 영상감시 환경에 있어 보안에 대한 고려는 필수적이다. 실질적으로 정보보안을 고려하지 않는 경우 개인정보 침해 문제로 발전하여 심각한 사회적 이슈가 될 수 있다. 따라서, 본 논문에서는 프라이버시 보장형 영상감시 프레임워크를 제안하였다. 제안한 PEVS 프레임워크는 CCTV와 클라우드 서버 간 보안동기화를 통한 종단간 보안기능, 메타정보 암호화 기능, 차등레벨 접근제어 기능을 가지고 있다. 제안한 방식은 기 제안된 지능형 영상감시 프레임워크인 Rodríguez의 연구, CVR 프레임워크, Hossain의 연구 등에 비해 벤더 독립성, 데이터 백업상의 안정성, 세분화된 영상 접근제어, 메타정보 보안기능 등의 장점을 가지고 있다.

제안한 방식의 설명을 위해 먼저 2장에서 기존의 클라우드 기반의 영상감시 기반기술에 대하여 살펴보았고, 3장에서는 현행 클라우드 제품 및 연구동향을 분석하였다. 이후 4장에서는 클라우드 영상감시 환경을 위한 보안 취약성 및 요구사항을 도출하였으며, 5장에서는 본 논문에서 제안한 PEVS 프레임워크에 대한 세부적인 사항을 설명하였다. 이후 6장에서는 제안한 기법에 대한 안전성과 효율성 관점에서 정성적 평가를 수행하고 실제 프로토타입 환경을 구성하여 성능 측정을 수행하였다. 향후 빅데이터를 기반으로 보다 정밀한 CCTV 영상 분석이 가능해질 것으로 예상됨에 따라, 앞으로의 영상데이터는 더욱 많은 정보를 노출하게 될 것이다. 이는 CCTV 영상 객체의 프라이버시 침해와 직접적으로 연결될 수 있으므로 이에 대한 안전한 대책이 필수적으로 선행되어야 한다. 앞으로 지능형 영상 감시 환경의 보안대책에 대한 더욱 많은 연구가 필요할 것이며, 안전한 미래사회를 위한 필수적인 프라이버시 보호 기술로 자리잡게 될 것으로 보인다.

참 고 문 헌

이동혁, 박남제. (2017). IoT 기기의 보안성 확보를 위한 제도적 개선방안. 정보보호학회논문지, 27(3), 607-615.

이동혁, 박남제. (2017). 4차 산업시대의 사이버 보안 확보를 위한 모의해킹 훈련 방안. 한국정보기술학회논문지, 15(5), 47-56.

이동혁, 박남제. (2017). 해사클라우드 환경에 적합한 비밀분산 기반의 안전한 데이터 전송 기법. 정보과학회 컴퓨팅의 실제 논문지, 23(4), 232-237.

이동혁, 박남제. (2017). 안전한 IoT 환경을 위한 기술 및 정책적 사후 보안관리 프레임워크. 한국정보기술학회논문지, 15(4), 127-138.

이동혁, 박남제. (2017). 개방형 IoT 해사클라우드 환경에 적합한 안전한 Almanac 동기화 기법. 한국정보기술학회논문지, 15(2), 79-90.

이동혁, 박남제. (2016). 스마트그리드 개인정보보호를 위한 미터링 데이터 비식별화 방안 연구. 정보보호학회논문지, 26(6), 1593-1603.

이동혁, 박남제. (2016). 안전한 해사클라우드 환경을 위한 SH-Tree 기반의 데이터 동기화 기법 제안. 정보보호학회논문지, 26(4), 929-940.

이동혁, 박남제. (2016). 게이미피케이션 메커니즘을 이용한 초등 네트워크 정보보안 학습교재 및 교구 개발. 정보보호학회논문지, 26(3), 787-797.

이동혁, 박남제. (2016). 개인정보보호 강화를 위한 eID 온라인 인증스킴 개선방안. 한국정보기술학회논문지, 14(5), 89-98.

이동혁, 박남제. (2016). 스마트그리드 개인정보보호법제 개선. 정보보호학회논문지, 26(2), 415-423.

이동혁, 박남제. (2016). IoT 제품 보안 인증 및 보안성 유지 관리방안. 한국통신학회지(정보와통신), 33(12), 28-34.

이동혁, 박남제, 강유성, 최두호. (2016). 독일의 eID 동향 및 기술 분석. 정보보호학회지, 26(2), 39-44.

이동혁, 박남제. (2016). 스마트그리드 개인정보보호를 위한 정책적 고려사항. 정보보호학회지, 26(1), 99-104.

이동혁, 박남제. (2016). IT 패러다임의 변화에 따른 스마트그리드 개인정보보호 방안. 예술인문사회융합멀티미디어논문지, 6, 81-90.

이동혁, 박남제. (2017). 해사클라우드의 Identity 관리 기술 동향. 정보보호학회지, 27(6), 5-10.

이동혁, 박남제. (2017). GSMA의 IoT 보안 가이드라인 현황, 주간기술동향, 1797, 2-13..

차상육. (2016). 빅데이터의 활용에 따른 개인정보보호법제와의 충돌과 과제. 한양법학, 27‘1(1), 315-359.

장석호. (2016). 빅데이터 산업에서의 정보보호 현황과 전망. 정보보호학회지, 26(2), 31-34.

김동국, 이혁. (2015). 빅데이터 기반의 개인정보 비식별화 동향. 인터넷정보학회지, 16(2), 15-22.

박태환, 이가람, 김호원. (2017). 클라우드 플랫폼 환경에서의 프라이버시 보호기법 연구 동향 및 전망. 정보보호학회논문지, 27(5), 1149-1155.

신용녀, 전명근. (2014). 영상감시 시스템에서의 얼굴 영상 정보보호를 위한 기술적 및 관리적 요구사항. 정보보호학회논문지, 24(1), 97-106.

Donghyeok Lee, Namje Park. (2017). Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. The Journal of Supercomputing, 73(3), 1103-1118.

Hossain, M. A. (2014). Framework for a cloud-based multimedia surveillance system. International Journal of Distributed Sensor Networks, 10(5), 135257.

Rodríguez-Silva, D. A., Adkinson-Orellana, L., Gonz′lez-Castano, F. J., Armino-Franco, I., & Gonz′lez-Martinez, D. (2012, June). Video surveillance based on cloud storage. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, IEEE, 991-992

Lin, C. F., Yuan, S. M., Leu, M. C., & Tsai, C. T. (2012, September). A framework for scalable cloud video recorder system in surveillance environment. In Ubiquitous intelligence & computing and 9th international conference on autonomic & trusted computing (UIC/ATC), 2012 9th international conference on, IEEE, 655-660.

Donghyeok Lee, Namje Park. (2016). Security Enhancement Scheme supporting range queries on encrypted DB for Secure e-Navigation Era.

International Journal of Security and Its Applications, 10(2), 141-150.

Namje Park, Donghyeok Lee. (2017). Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. Personal and Ubiquitous Computing, 1-8.

Xiong, Y. H., Wan, S. Y., He, Y., & Su, D. (2014). Design and implementation of a prototype cloud video surveillance system. Journal of Advanced Computational Intelligence and Intelligent Informatics, 18(1), 40-47.

Xiong, Y., Wan, S., She, J., Wu, M., He, Y., & Jiang, K. (2016). An energy-optimization-based method of task scheduling for a cloud video surveillance center. Journal of Network and Computer Applications, 59, 63-73.

Dašić, P., Dašić, J., & Crvenković, B. (2016). Service models for cloud computing: Video Surveillance as a Service (VSaaS). Bulletin of the Transilvania University of Braşov, Series I: Engineering Sciences, 9(2), 83-90.

Wu, Y. S., Chang, Y. S., Juang, T. Y., & Yen, J. S. (2012, September). An architecture for video surveillance service based on P2P and cloud computing. In Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on, IEEE, 661-666.

Hassan, M. M., Hossain, M. A., & Al-Qurishi, M. (2014, February). Cloud-based mobile IPTV terminal for video surveillance. In Advanced Communication Technology (ICACT), 2014 16th International Conference on, IEEE, 876-880.

Prati, A., Vezzani, R., Fornaciari, M., & Cucchiara, R. (2013). Intelligent video surveillance as a service. In Intelligent Multimedia Surveillance, Springer Berlin Heidelberg, 1-16.

Song, B., Tian, Y., & Zhou, B. (2014, August). Design and evaluation of remote video surveillance system on private cloud. In Biometrics and Security Technologies (ISBAST), 2014 International Symposium on, IEEE, 256-262.

Dey, S., Chakraborty, A., Naskar, S., & Misra, P. (2012, October). Smart city surveillance: Leveraging benefits of cloud data stores. In Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, IEEE, 868-876.

Tsai, Y. H. (2013, March). The cloud streaming service migration in cloud video storage system. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, IEEE, 672-677.

Yi, S., Jing, X., Zhu, J., Zhu, J., & Cheng, H. (2012). The model of face recognition in video surveillance based on cloud computing. In Advances in computer science and information engineering, Springer, Berlin, Heidelberg, 105-111

Dey, S., Chakraborty, A., Naskar, S., & Misra, P. (2012, October). Smart city surveillance: Leveraging benefits of cloud data stores. In Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, IEEE, 868-876.

GSMA. (2016). IoT Security Guidelines : Overview Document.

<ABSTRACT>

A Privacy Enhanced Video Surveillance Framework using Metadata De-identification

Donghyeok Lee

Major of Computer Education
Faculty of Science Education Graduate School
Jeju National University
Supervised by professor Namje Park

Recently, video surveillance system has been developed as intelligent by introducing various image analysis techniques. In particular, the cloud-based video surveillance environment provides reliable analysis results for video objects as it enables various video analysis based on big data. This will lead to a dramatic improvement in the performance of the intelligent video surveillance environment, and it will be possible to make more active surveillance measures and contribute to the intelligent security environment.

However, there is a security problem behind this. In particular, there are various security flaws in the cloud and big data environment, and it is expected that a new type of security incident will occur in the cloud based video surveillance environment. This leads to privacy violation due to leakage of personal information of the video object, which may raise serious social issues.

In the existing CCTV-based cloud surveillance environment, security techniques mainly use existing methods such as privacy masking, data encryption, and RBAC-based access control. However, as the big data analysis technology develops in the future, various meta information will be generated. Accordingly, various techniques such as a de-identification technology, a

security synchronization technique on a cloud server basis, and a differential level access control are required. The proposed intelligent surveillance environment framework mainly tends to focus on applying the intelligent video surveillance environment to the structure suitable for the cloud environment. However, in the cloud environment, various information protection vulnerabilities exist such as insider attacks. The proposed CVR framework and Hossain's research have a security policy that separates private and public cloud networks to prevent such insider attacks. However, even in such a case, security can not be completely guaranteed. In particular, there may be an internal attacker in a private cloud, and in this case, the security threats in the existing cloud environment can be followed. In order to safely store the data, it is desirable to encrypt and unidentify all the data, and to apply end-to-end encryption in the transmission process. Also, there is a need for a structure that can prevent hacker attacks from CCTV transmission to monitoring/cloud server and monitoring client. Therefore, in this paper, we propose a Privacy Enhancing Video Surveillance (PEVS) video surveillance framework that provides a cloud - based secure and intelligent video surveillance environment. The proposed framework provides a metadata de-identification algorithm and supports secure security synchronization of CCTV video data. In addition, it is safe for attacks such as sniffing attacks in the data transmission process, insider outflow attacks in the cloud environment, metadata analysis attacks such as data counting, and tamper attacks. Moreover, it has advantages such as vendor independence, stability of data backup, granular video access control, and meta information security function compared to the research of the proposed intelligent video surveillance framework Rodríguez, CVR framework, and Hossain.

Keywords : Cloud, Video Surveillance, CCTV, Privacy, De-identification

A. 용어집

Rsync

Rsync는 데이터 중복을 고려하여 변경된 부분만 동기화 할 수 있는 기법이다. Rsync는 중복 데이터를 검색하는 방법으로 롤링 체크섬(Rolling Checksum) 알고리즘을 사용한다.

SyncML

SyncML은 이기종 환경에서 서로 다른 플랫폼 간의 데이터 동기화를 지원하도록 개발된 개방형 표준 규격이다. SyncML 프로토콜 에는 동기화에 필요한 여러 명령어와 메커니즘이 정의되어 있다.

H-Tree(Merkle Tree)

H-Tree(해쉬 트리) 방식은 데이터를 각 블록 단위로 분할한 뒤, 각각의 블록에 해쉬값을 수행하고, 이를 리프 노드에 입력한 후 단일 해쉬값이 만들어 질 때까지 트리 형태로 반복하여 해쉬를 하는 이진 해쉬트리 형태로 구성한 것이다.

SH-Tree(Secure-hash Tree)

H-Tree의 변형으로, 평문을 암호화된 데이터와 메타정보로 분할하여 해쉬트리를 구성하는 것이 특징이며, 데이터 블록의 가변 사이즈 관리가 가능하다.

델타 업데이트(Delta Update)

대용량 데이터일 경우, 동기화를 이유로 전체 데이터가 전달되어서는 안된다. 이러한 점은 대역폭의 증가와 직결되며, 동기화의 속도도 크게 증가하므로 효율성을 떨어뜨리는 원인이 된다. 델타 업데이트는 동기화 시 변경된 부분만을 검출하여 전송함으로써 효율적인 동기화 성능을 제공하는 기술이다.

프라이버시 마스킹(Privacy Masking)

프라이버시 마스킹 기술은 영상의 얼굴 데이터를 알아볼 수 없도록 변경하는 것을 의미한다. 예를 들어, 블러링, 픽셀화, 얼굴영상 제거방식을 들 수 있으며, 이러한 기술을 적용하면 영상정보에서의 개인 식별이 매우 어렵게 된다.

Openstack Swift

OpenStack Swift는 웹서비스 REST 프로토콜과 같은 개방형 표준을 통해 관리되는 데이터 구성 및 검색을 위한 컨테이너 서비스 방법론을 기반으로 한다.

해사클라우드(Maritime Cloud)

해사클라우드는 2012년 가을, 덴마크 정부 해사 기구(DMA:Danish Maritime Authority)의 내부 프로젝트로 시작되었다. e-Navigation 프로젝트의 일환으로, e-Navigation에서의 주요 통신 기반 기술이다. 해사클라우드는 해사 객체간 원활한 통신을 위한 클라우드 인프라 환경을 제공한다.

COP 변환방식

COP(Character Order Preserving) 변환방식이란 원본 문자열을 변환식을 이용하여 변환된 문자로 치환하는 기법으로, 문자열을 구성하는 단일 문자 단위로 변환 문자로의 치환을 수행한다. 여기에는 특정 문자열의 도메인과 변환된 문자열의 도메인은 각각 정렬 순서를 가지고 있다는 특징이 존재한다.

PEVS 프레임워크

PEVS(Privacy Enhanced Video Surveillance) 프레임워크는 CCTV 환경에서의 클라우드 기반 지능형 영상감지시스템을 위하여 영상 객체의 프라이버시 보호를 목적으로 CCTV와 엔드유저까지의 종단간 보안 및 비식별화 기반의 안전한 영상정보 관리 방안을 제공하는 구조이다.

B. 연구 실적

[SCI(E)]

1. Donghyeok Lee, Namje Park. (2017). Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. The Journal of Supercomputing, 73(3), 1103-1118.
2. Namje Park, Donghyeok Lee. (2017). Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. Personal and Ubiquitous Computing, 1-8.

[SCOPUS]

1. Donghyeok Lee, Namje Park. (2016). Security Enhancement Scheme supporting range queries on encrypted DB for Secure e-Navigation Era. International Journal of Security and Its Applications, 10(2), 141-150.

[International Conference, and Workshop]

1. Donghyeok Lee, Yousung Kang, Dooho Choi, Namje Park, A Privacy-Preserving Smart Metering Scheme for Preventing Data Analysis in Electronic Vehicle Application, ICESI, 2016
2. Donghyeok Lee, Namje Park, Developing Training Education Program for Financial Engineering Career, Advanced Green and Smart Technology 2016
3. Donghyeok Lee, Namje Park, Geocasting-Based Almanac Synchronization Method for Secure Maritime Cloud. In International Workshop on Information Security Applications (pp. 376-387). Springer, Cham.
4. Donghyeok Lee, Namje Park, An Efficient Synchronization Scheme for Mairitime Cloud Security, IRES 2016
5. Donghyeok Lee, Namje Park, Keonwoo Kim, A Fast and Secure Encryption for CCTV Surveillance Systems in Intelligent Cloud Environment
6. Donghyeok Lee, Namje Park, Dooho Choi, Inter-Vessel Traffic Service

Data Exchange Format Protocol Security Enhancement of User Authentication Scheme in Mobile VTS Middleware Platform, APNIMS 2015

7. Donghyeok Lee, Namje Park, Security Enhancement of Cloud Service in E-Navigation Environment, GST 2015
8. Donghyeok Lee, Namje Park, Security through Authentication Infrastructure in Open Maritime Cloud, Platcon 2016
9. Donghyeok Lee, Yousung Kang, Dooho Choi, Namje Park, A Privacy Preserving Smart Merering Scheme for Preventing Data Analysis in Electronic Vehicle Application, ICESI 2016

[Domestic Journal]

1. 이동혁, 박남제. (2017). IoT 기기의 보안성 확보를 위한 제도적 개선방안. 정보보호학회논문지, 27(3), 607-615.
2. 이동혁, 박남제. (2017). 4차 산업시대의 사이버 보안 확보를 위한 모의해킹 훈련 방안. 한국정보기술학회논문지, 15(5), 47-56.
3. 이동혁, 박남제. (2017). 해사클라우드 환경에 적합한 비밀분산 기반의 안전한 데이터 전송 기법. 정보과학회 컴퓨팅의 실제 논문지, 23(4), 232-237.
4. 이동혁, 박남제. (2017). 안전한 IoT 환경을 위한 기술 및 정책적 사후 보안관리 프레임워크. 한국정보기술학회논문지, 15(4), 127-138.
5. 이동혁, 박남제. (2017). 개방형 IoT 해사클라우드 환경에 적합한 안전한 Almanac 동기화 기법. 한국정보기술학회논문지, 15(2), 79-90.
6. 이동혁, 박남제. (2016). 스마트그리드 개인정보보호를 위한 미터링 데이터 비식별화 방안 연구. 정보보호학회논문지, 26(6), 1593-1603.
7. 이동혁, 박남제. (2016). 안전한 해사클라우드 환경을 위한 SH-Tree 기반의 데이터 동기화 기법 제안. 정보보호학회논문지, 26(4), 929-940.
8. 이동혁, 박남제. (2016). 게이미피케이션 메커니즘을 이용한 초등 네트워크 정보보안 학습교재 및 교구 개발. 정보보호학회논문지, 26(3), 787-797.
9. 이동혁, 박남제. (2016). 개인정보보호 강화를 위한 eID 온라인 인증스킴 개선 방안. 한국정보기술학회논문지, 14(5), 89-98.
10. 이동혁, 박남제. (2016). 스마트그리드 개인정보보호법제 개선. 정보보호학회

논문지, 26(2), 415-423.
11. 이동혁, 박남제. (2016). IoT 제품 보안 인증 및 보안성 유지 관리방안. 한국통신학회지(정보와통신), 33(12), 28-34.
12. 이동혁, 박남제. (2017). 해사클라우드의 Identity 관리 기술 동향. 정보보호학회지, 27(6), 5-10.
13. 이동혁, 박남제, 강유성, 최두호. (2016). 독일의 eID 동향 및 기술 분석. 정보보호학회지, 26(2), 39-44.
14. 이동혁, 박남제. (2016). 스마트그리드 개인정보보호를 위한 정책적 고려사항. 정보보호학회지, 26(1), 99-104.

[Domestic Conference]

1. 이동혁, 박남제, OpenStack Swift의 보안 취약점과 해결방안, 한국정보보호학회 동계학술대회, 2017
2. 이동혁, 박남제, 클라우드 기반의 지능형 영상 감시 시스템을 위한 영상 프라이버시 보호 방법, 한국정보보호학회 동계학술대회, 2017
3. 이동혁, 박남제, 지능형 CCTV 환경의 프라이버시 보장을 위한 유사도 기반 가상얼굴 생성기법, 한국정보보호학회 하계학술대회, 2017
4. 이동혁, 박남제, 지능형 IoT 제품 및 서비스 안전성 강화를 위한 보안성 유지 관리 체계 개선방안, 한국정보보호학회 하계학술대회, 2017
5. 이동혁, 박남제, 해사클라우드 환경에서의 안전한 비밀정보 공유 기법, 한국컴퓨터종합학술대회, 2016
6. 이동혁, 최유라, 이은국, 이지산, 김유미, 박남제, 정보보호 개념 학습을 위한 온라인 에듀게임 개발, 한국정보교육학회 하계학술대회, 2016
7. 이동혁, 박남제, IT환경의 변화에 따른 새로운 스마트그리드 개인정보보호 위협에 대한 대책방안, HSST 2016
8. 이동혁, 박남제, 중간자공격 방지를 위한 eID인증방식 개선방안, 정보처리학회 추계학술대회, 2015
9. 이동혁, 김범수, 박남제, 디지털 보이스 레코딩기반 몽타주 학습을 통한 사이버 범죄수사관 STEAM 진로 연계형 교재 개발, 정보과학회 동계학술대회 2015