Journal of KIIT. Vol. 17, No. 5, pp. 105-116, May 31, 2019. pISSN 1598-8619, eISSN 2093-7571 105
http://dx.doi.org/10.14801/jkiit.2019.17.5.105

개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘 구조

김진수*, 박남제**

Intelligent Video Surveillance Incubating Security Mechanism in Open Cloud Environments

Jinsu Kim*, Namje Park**

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임
[2017-0-00207,클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼 개발]

요 약

국내 대다수의 공공장소 및 사유건물은 범죄 예방 및 사후 조치, 내부자 보안, 시설안전 및 화재 예방 등을 위해 CCTV(Closed Circuit Television)를 설치하고 있으며, 매년 설치 대수는 늘어나는 추세이다. 늘어나는 CCTV에 대하여 진행된 설문에서는 다수의 반응이 CCTV의 촬영으로 인한 프라이버시 침해 등의 부정적 시선보다 설치로 인해 발생할 수 있는 범죄의 예방적 측면에서 긍정적으로 보고 있다. 하지만 CCTV는 프라이버시 측면에서 많은 위험성을 내포하고 있으며, 클라우드를 이용하여 영상 데이터를 수집할 경우 피사체의 개인정보가 유출될 수 있다. 인세캠은 각국의 CCTV 감시 영상을 실시간으로 중계하였으며, 중계 대상에는 노트북의 전면카메라까지 포함되어 큰 이슈를 불러일으켰다. 본 논문에서는 CCTV를 통해 영상정보에 대한 프라이버시 기법 처리를 통한 개인정보 유출 방지 및 클라우드 시스템 보안성 강화를 위한 시스템을 소개하기로 한다.

Abstract

Most of the public and private buildings in Korea are installing CCTV for crime prevention and follow-up action, insider security, facility safety, and fire prevention, and the number of installations is increasing each year. In the questionnaire conducted on the increasing CCTV, many reactions were positive in terms of the prevention of crime that could occur due to the installation, rather than negative views such as privacy violation caused by CCTV shooting. However, CCTV poses a lot of privacy risks, and when the image data is collected using the cloud, the personal information of the subject can be leaked. InseCam relayed the CCTV surveillance video of each country in real time, including the front camera of the notebook computer, which caused a big issue. In this paper, we introduce a system to prevent leakage of private information and enhance the security of the cloud system by processing the privacy technique on image information about a subject photographed through CCTV.

Keywords
closed circuit television(CCTV), cloud system, privacy risk, security, video surveillance

* 강원대학교 대학원 정보통신공학전공 석사과정
제주대학교 사이버보안인재교육원 연구원
- ORCID ID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등교육학과 교수(교신저자)
- ORCID ID: https://orcid.org/0000-0003-4434-8933

· Received: Feb. 08, 2019, Revised: Apr. 30, 2019, Accepted: May 03, 2019
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

최근의 영상감시 시스템은 영상분석, 컴퓨터비전, 패턴 인식 등의 기술을 적용함으로서 자동적으로 범죄자를 찾거나 화재 현장을 탐지하는 등의 지능형 영상감시 시스템으로 발전해나가고 있다. 이와 같은 지능형 영상감시 시스템은 공공시설, 철도, 공항, 백화점과 같은 다수의 사람이 이용하는 공간에서 테러와 같은 강력범죄나 미아, 납치, 분실 등의 사건사고를 예방 및 해결하기 위한 방도로서 사용되고 있다.

하지만, 지능형 영상감시 시스템은 불특정 다수에 대한 감시 시스템으로 감시 대상은 의도치 않게 시스템 사용자로부터 감시를 받게 된다. 고로 대다수의 시스템은 촬영된 피사체에 대한 개인정보 수집을 최소화하면서 역할을 수행함과 동시에 피사체에 대한 개인 정보가 유출되지 않도록 프라이버시 보호 기법을 적용하여야 한다[1].

또한, 지능형 영상감시 시스템에 클라우드와 빅데이터를 도입함으로서 보다 발전된 시스템 개발이 진행되고 있으며, 이는 촬영된 영상 데이터를 클라우드 서버에 저장함으로서 피사체의 개인정보 유출 경로의 증가와도 연관된다. 그러므로 앞으로의 영상감시 시스템은 기존의 영상감시 시스템에 대한 취약점뿐만이 아닌 도입되고 있는 클라우드와 빅데이터의 취약점을 분석하고 해당 취약점으로부터 피사체의 개인정보가 유출되지 않도록 보호할 수 있는 기술의 개발이 요구된다[2].

본문은 개방형 클라우드 환경에서의 지능형 영상감시 시스템의 취약점을 분석하고, 오픈소스 클라우드로서 IaaS 서비스를 지원하는 Openstack을 이용하여 개방형 클라우드 기반의 지능형 인큐베이팅 보안 플랫폼을 제안하고, Openstack 내의 구현을 위한 기능을 소개하도록 한다. 본문의 구성은 2장에서 기존 클라우드 보안 기술과 취약점을 분석하고, 3장에서 제안하는 메커니즘을 포함하는 개방형 클라우드 기반의 지능형 인큐베이팅 보안 플랫폼을 정의한다. 4장에서 제안한 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘의 인터페이스의 설계를 소개한 뒤, 기존 보안 메커니즘과의 차이점을 5장에 서술한다.

Ⅱ. 관련 연구

2.1 오픈소스 클라우드 Openstack 보안 기능

Openstack은 스토리지의 객체 데이터에 대한 암호화, 정당한 사용자임을 증명하는 사용자 인증, 역할을 기반으로 접근 권한이 없는 구역으로의 접근을 방지하는 접근제어의 3가지 기능을 제공한다[3].

2.1.1 Swift 오브젝트 스토리지 서비스 암호화

Swift는 사용자의 계정별로 저장 공간을 할당하는 오브젝트 스토리지 서비스이다. Swift에서는 선택적으로 오브젝트 데이터에 대한 AES-256(Advanced Encryption Standard) 암호화를 지원하는데, 암호화함으로서 제 3자가 접근 권한을 취득하였을 경우 사용자의 데이터 노출을 방지할 수 있다. 다음 데이터는 Swift가 정지되어 있는 동안 암호화된다[4].

- PUT 요청에 의한 객체 내용의 본문
- 내용이 존재하는 개체의 ETag(Entity Tag)
- 모든 맞춤 사용자 개체 메타데이터 값
  (PUT 또는 POST 요청에 대한 메타데이터)

Swift에서 제공하는 암호화는 keymaster와 암호화 두 개의 미들웨어 필터를 프록시 서버 WSGI(Web Server Gateway Interface) 파이프라인에 추가하고 proxy-server.conf 파일에 각각의 필터 구성 섹션을 포함하여 배포한다. keymaster 구성 옵션인 encryption_root_secret은 스토리지 암호화를 위한 비밀키로, 미들웨어가 사용되기 전에 최소 44개의 유효 기본 64자의 값으로 설정되어야하며 모든 프록시 서버에서 일관되어야 한다. 배포된 encryption_root_secret은 스토리지 내의 비밀키로서 적용되게 되고, 암호화를 해제할 경우 disable_encryption 옵션을 True로 설정함으로서 기존의 암호화 오브젝트는 암호화된 상태로 유지하며, 이후 추가되는 요청에 의한 데이터는 암호화를 진행하지 않도록 하고, 암호화된 데이터는 저장되어있는 encryption_root_secret를 호출하여 암호화를 해제한다.

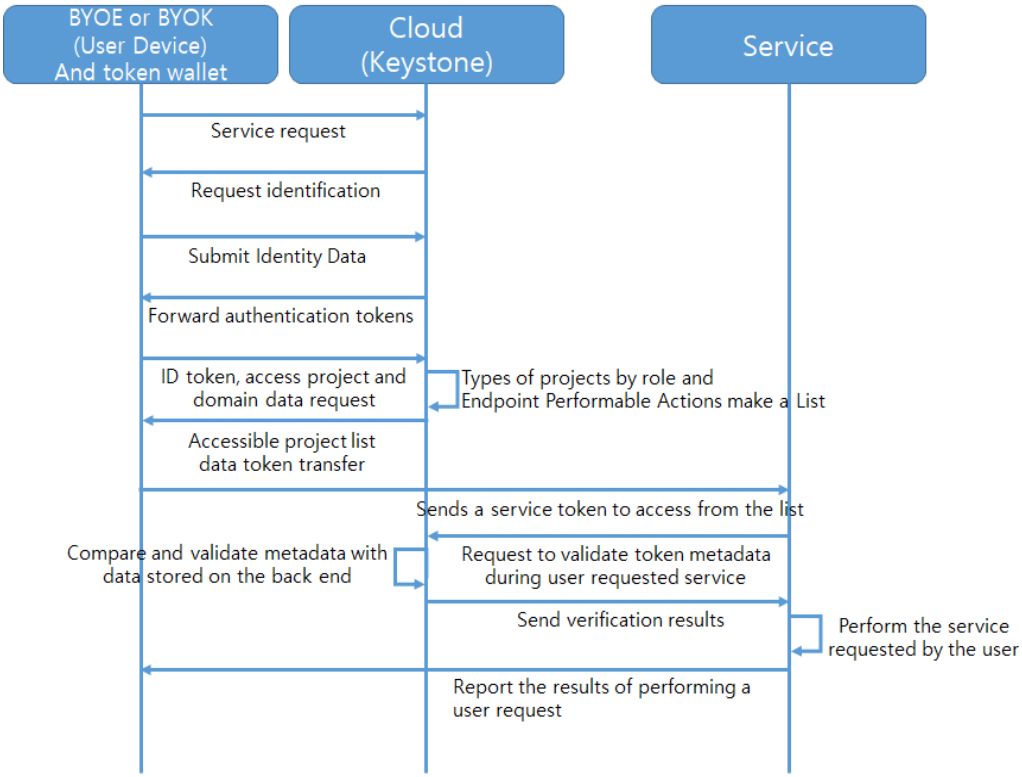

그림 1. keystone 인증 프로세스[5]
Fig. 1. keystone authentication process[5]

2.1.2 Keystone 사용자 인증 서비스

Keystone 서비스는 Openstack에서 사용자 인증 서비스를 제공한다. keystone 서비스에서는 사용자 인증을 위해 4개의 구성요소로 이뤄지는데, 관리를 위해 활동 범위가 제한된 사용자와 그룹, 프로젝트의 연합체를 의미하는 domain, 자원에 대한 권리를 가지는 보안그룹을 의미하는 project(tenant), Openstack 클라우드 서비스를 사용하는 user, 사용자의 구체적 동작 수행을 허용하는 특징의 집합인 role이 포함된다. keystone 서비스는 구성요소를 통해 사용자와 클라우드의 인증서비스, 사용자가 이용하고자 하는 서비스에서 다음과 같은 절차를 통해 시스템의 무결성을 제공한다.

2.1.3 Keymaster RBAC 접근제어 서비스

Openstack에서는 사용자에게 할당된 역할에 기반하여 접근을 통제하는 RBAC(Role-Based Access control)을 이용하여 리소스에 대한 사용자 접근을 제어하는데 사용된다. RBAC는 크게 역할 할당, 역할 권한 부여, 권한 승인의 3가지 규칙을 가진다. 접근하는 사용자에 대한 권한은 서비스마다 가지고 있는 policy.json에 저장된다. RBAC는 정확성과 무결성 검증을 위해 테스트를 거치게 되는데, 이 테스트를 실행하는 서비스를 patrole이라 칭한다. patrole은 policy.json에 저장된 내용을 바탕으로 접근제어 정책의 정확성과 무결성을 검증하게 된다[6].

2.2 기존 클라우드 서비스의 한계점과 취약점

2.2.1 영상정보 저장 위치에 따른 발생 취약점

현재 주로 판매되고 있는 영상감시 시스템은 촬영된 영상을 H/W나 클라우드에 저장하여 사용자에게 제공하고 있다. 하지만 독립적인 저장 공간을 가지는 H/W에 비해 클라우드는 공유되는 저장 공간을 제공하며, 다음과 같은 취약점을 가진다[7].

표 1. CSA 클라우드 컴퓨팅 취약점 목록[8]
Table. 1. List of CSA cloud computing vulnerabilities[8]

CSA - Top threats to cloud computing
R1: Data Breaches
R2: Insufficient Identity, Credential and Access Management
R3: Insecure Interfaces and APIs
R4: System Vulnerabilities
R5: Account Hijacking
R6: Malicious Insiders
R7: Advanced Persistent Threats
R8: Data Loss
R9: Insufficient Due Diligence
R10: Abuse and Nefarious Use of Cloud Services
R11: Denial of Service
R12: Shared Technology Vulnerabilities

2.2.2 개방형 전송 매체로 인한 발생 취약점

영상감시 시스템은 영상의 전송 매체로서 동축 케이블을 통한 폐쇄형 전송 또는 유·무선 네트워크를 이용한 개방형 전송을 제공한다. 이때, 전송 매체로서 네트워크를 사용하는 경우 다음과 같은 취약점에 노출될 수 있다[9].

표 2. OWASP 네트워크 취약점 목록[10]
Table. 2. List of OWASP network vulnerabilities[10]

OWASP - OWASP Top 10
R1: Injection
R2: Broken Authentication
R3: Sensitive Data Exposure
R4: XML External Entities (XXE)
R5: Broken Access Control
R6: Security Misconfiguration
R7: Cross-Site Scripting (XSS)
R8: Insecure Deserialization
R9: Using Components with Known Vulnerabilities
R10: Insufficient Logging & Monitoring

2.3 국내·외 기술동향

클라우드 서비스는 크게 네트워크나 스토리지 등의 서버 자원을 제공하는 IaaS(Infrastructure as a Service), 서비스 제공을 위한 개발 환경을 제공하는 PaaS(Platfor m as a Service), 클라우드 환경에서 응용 프로그램을 제공하는 SaaS(Software as a Service)로 구분된다[11].

클라우드 서비스는 유형에 따라 다양한 기업에서 제공하고 있으며, PaaS는 대표적으로 IBM사의 Bluemix, Microsoft사의 Azure, 아마존사의 AWS(Amazon Web Service) 등이 있으며, 국내에서는 한국형 PaaS 서비스 제공을 위해 PaaS-Ta라는 서비스를 이용하여 기업과의 협약을 통해 성장을 도모하고 있다.

PaaS를 제공하는 기업은 각각의 기업마다 보안성을 강조하며 타 기업과의 차별성을 강조하고 있는데 다음은 위에서 소개한 해외 3사의 보안 기능을 소개한 것이다.

먼저 IBM사의 Bluemix 서비스는 HSM(Hardware Security Module)을 기반으로 하는 암호화, 다운타임을 방지하는 Trusted Execution, 소프트웨어 측면에서 보안성을 강화한 보안 소프트웨어, SSL 인증서를 통한 사용자간 암호화된 보안 연결 설정의 기능을 제공한다[12].

다음으로 Microsoft사의 Azure 서비스는 내부 감사, 보안 교육, 침입 탐지 등을 제공하는 보안 플랫폼, 사용자 데이터 관리, 조건부 접근제어, 엄격한 개인정보 표준을 제공하는 개인정보 보호 및 제어, 보안 센터, 컨트롤 허브를 통한 규정 준수, 데이터 접근, 보호, 관리를 통해 제공하는 데이터 투명성의 4가지 측면에서 보안 서비스를 제공한다[13].

아마존사의 AWS 서비스는 네트워크 접근제어를 위한 인프라 보안, DDoS(Distributed Denial-of-Service Att ack) 공격에 대한 복원력 제공, 클라우드 내의 데이터 암호화, AWS 서비스의 상태 모니터링 및 로깅, 접근 정책을 관리하기 위한 자격증명 및 접근 제어를 제공한다[14].

PaaS-Ta 서비스는 개방형 생태계로서 국내의 업체들과 협력하여 응용 SW개발, 미들웨어 확대, 개발자 육성, 공공기관 클라우드 서비스 제공, 민간 서비스 등을 제공하고 있다[15].

III. 제안된 개방형 클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼

클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼은 영상감시 시스템으로부터 전송되는 영상 데이터를 분석하여 Deep-learning 기술을 통해 사람과 차

량, 교통사고 발생과 번호판을 인식하여 긴급 상황에 대해 관제센터에 알리고, 그렇지 않은 상황에선 피사체가 되는 사람이나 차량의 인식 가능한 정보를 알아보지 못하도록 처리하는 플랫폼으로 그림 2와 같이 구성된다. 이 플랫폼은 인식신경망 인큐베이터, 신경망 분석, 실증 치안 DB(DataBase) 구축 및 온라인 학습, 지능형 인큐베이팅 보안의 4가지 서브시스템으로 구성된다.

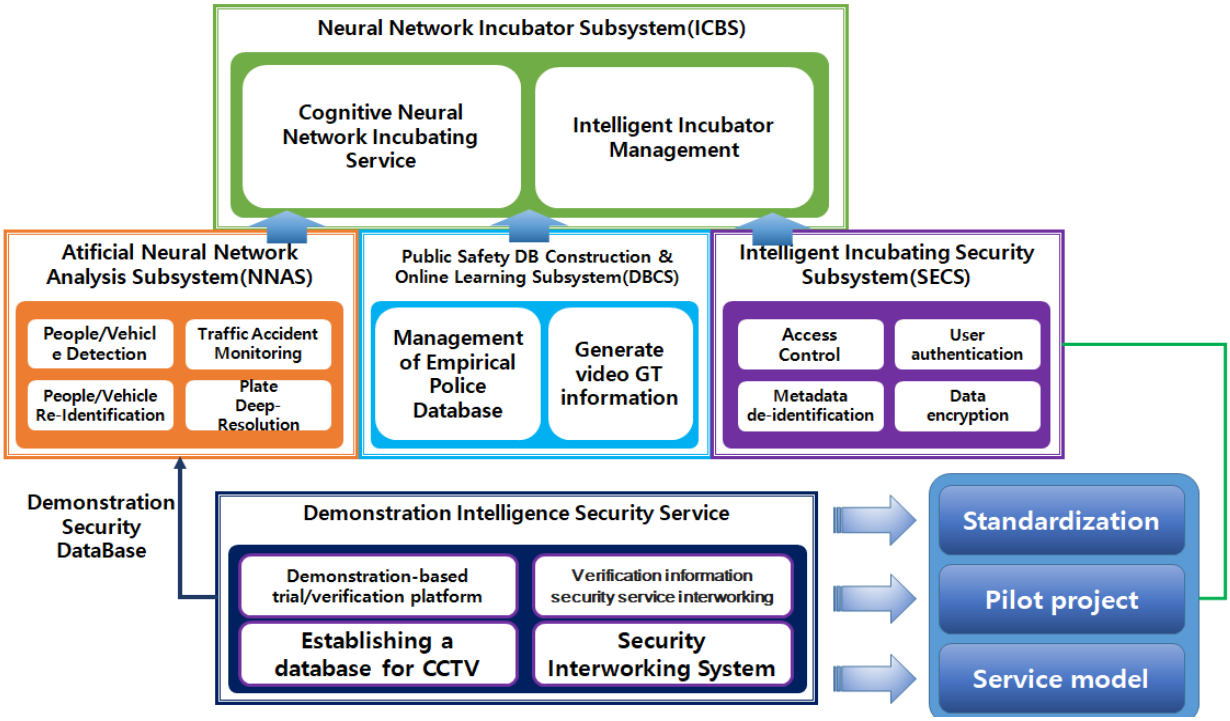

그림 2. 제안된 플랫폼 전체 구성도
Fig. 2. Proposed overall platform configuration

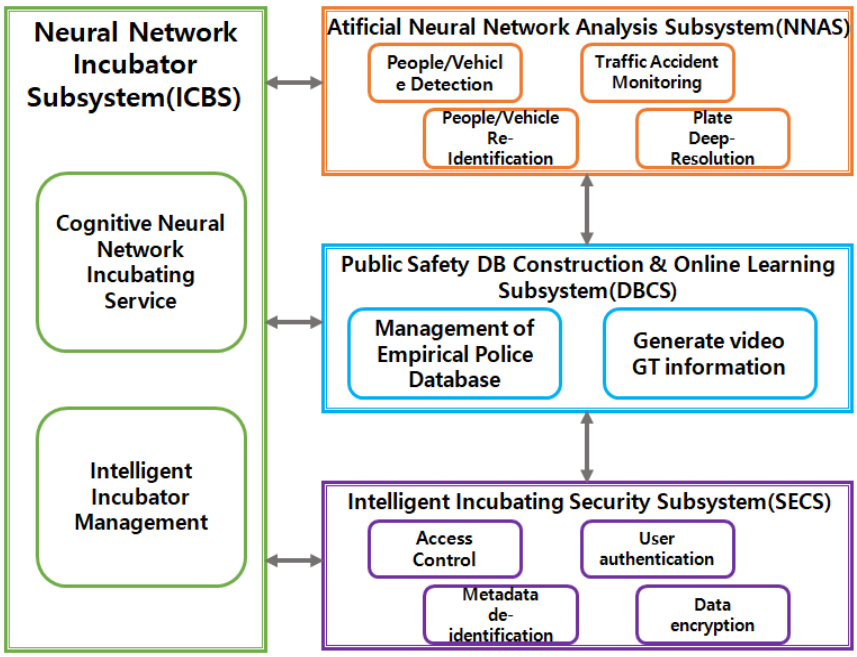

그림 3. 제안된 플랫폼의 논리적 구조
Fig. 3. Logical structure of the proposed platform

본문에서 제안하는 메커니즘은 클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼의 서브시스템 중 하나로 개인정보 노출 가능성이 있는 메타데이터의 비식별화, 중요 데이터 암호화, 정당한 사용자 인증, 접근 권한 외의 시스템 접근 방지를 위한 접근제어 기능을 제공하는 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘이다.

3.1 용어 정의

표 3. 용어 정의
Table. 3. Term definition

Term	Definition
Recognition neural network	Intelligent learning model for image analysis
Incubator	Image recognition neural network generator reflecting user needs
Incubating platform	Virtual environment-based operating environment capable of managing multiple incubators
Intelligent video recognition technology	Object Detection and Classification based on Deep Learning and Simple Risk Identification
License plate Deep Resolution	Technology to reverse-referenced the license plate collected in the real world using Deep Learning technology
Re-Identification	Image technology to continuously identify a specific person or object using multiple CCTV

3.2 제안된 플랫폼의 논리적 구조와 기능 정의

제안하는 시스템은 지능형 CCTV 적용 환경에서 영상을 수집하고, 수집된 영상을 해당 플랫폼 내의 학습 서브시스템을 통해 위험사항을 인식할 수 있도록 학습시켜 실제 사용 환경에 최적화된 지능형 영상인식 솔루션을 제공하는 플랫폼에 적용되는 서브시스템의 하나로, 플랫폼은 지능치안 서비스를 위한 신경망 분석(NNAS: Atificial Neural Network Analysis Subsystem), 실증치안 DB 구축 및 온라인 학습(DBCS: Public Safety DB Construction & Online Learning Subsystem), 지능형 인큐베이팅 보안(SECS: Intelligent Incubating Security Subsystem), 클라우드 기반 인식신경망 인큐베이터(ICBS: Neural Network Incubator Subsystem)의 4개의 서브시스템으로 구성되어 있다. 다음은 클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼의 논리적 구상도이다.

지능치안 서비스를 위한 신경망 분석 서브시스템은 클라우드 기반의 인식신경망 학습을 진행하며 유형별 위험상황 인지를 위해 신경망의 생성·저장·관리를 사람 및 차량 검출, 사람 및 차량에 대한 Re-IDentification, 차량 번호판 Deep-Resolution, 교통사고 감지의 4개 모듈로 구분하여 진행한다[16].

실증 치안 DB 구축 및 온라인 학습 서브시스템은 지능형 클라우드 인큐베이팅 학습을 위한 DB를 구축하고 온라인 학습을 위해 요구되는 지능형 실제 위치에 대한 GT(Ground Truth) 정보 생성 및 생성된 정보를 DB화하여 관리하는 역할을 수행한다.

클라우드 기반 인식신경망 인큐베이터 서브시스템은 원격 클라우드 환경을 이용하여 서비스 환경을 구축하고, 구축된 환경을 이용하여 인식신경망 인큐베이터 생성 및 관리 기능과 UI를 통해 인큐베이터의 관리 및 사용 기능을 제공한다.

지능형 영상보안 인큐베이터 보안 서브시스템은 개인 정보가 노출 될 수 있는 메타데이터에 대한 비식별화 처리, DBCS에 저장되는 개인을 식별하는 데이터의 암호문 생성을 위한 암호화, 플랫폼 접근 권한을 확인하기 위한 접근제어, 정당한 사용자 외의 시스템에 대한 접근을 방지하는 사용자 인증 기능을 수행한다.

IV. 제안된 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘 구조

4.1 제안된 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘 정의

개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘은 원격 클라우드 환경을 이용하여 영상인식 신경망을 온라인으로 학습시키고, 실시간 업데이트하여 딥러닝 성능을 지속적으로 강화할 수 있는 인식신경망 인큐베이터 생성/관리/제공 기능을 제공하며, 이를 사용자가 활용할 수 있는 UI를 포함하는 서비스 환경을 제공하는 시스템이다. 여기에는 지능형 인큐베이팅 시스템이 가지고 있는 메타데이터에 대한 비식별화 기반의 데이터보안 및

비식별화된 메타데이터에 대한 보안 질의를 가능하게 하는 보안검색 질의 생성 기능을 가지고 있으며, 지능형 인큐베이팅 시스템의 안전한 접근제어를 위한 접근제어를 제공한다. 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘은 다음의 4개의 모듈을 가진다.

- 메타데이터 비식별화 모듈 : 개인정보가 노출될 수 있는 메타데이터에 대한 비식별화
- 암호화 모듈 : 암호화 처리를 통한 데이터 보호
- 접근제어 모듈 : 접근 기능을 확인하기 위한 접근제어
- 사용자 인증 모듈 : 제3자의 부정한 접속 방지

4.2 제안된 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘의 인터페이스 구조 설계

본문에서는 클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼에서의 인터페이스 구조를 살펴보고, 제안하는 지능형 인큐베이터 보안과 인터페이스를 공유하는 서브시스템간의 관계를 설명하고자 한다.

개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘은 실증 치안 DB 구축 및 온라인 학습, 인식신경망 인큐베이터 와 인터페이스를 공유하며, 인터페이스 상에서 이뤄지는 통신 프로토콜을 소개한다. 그림 4는 인터페이스의 구조를 도식화한 것이다.

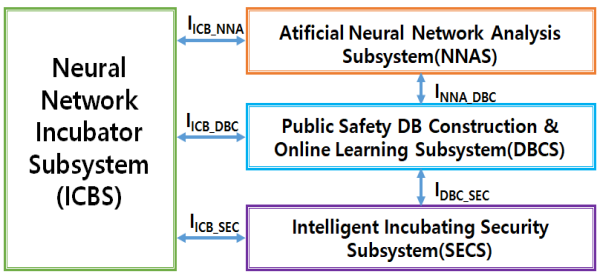

그림 4. 제안된 플랫폼의 인터페이스 구조
Fig. 4. Interface structure of the proposed platform

4.2.1 ICBS-SECS 프로토콜 설계

ICBS의 요청에 따라 SECS에서는 로그인을 통한 정당한 사용자 인증과 사용자에게 허가된 기능을 기반으로 한 서비스 접근제어를 수행한다. 두 서비스는 각각 하나의 모듈 형태로 구성된다.

본 시스템으로의 서비스를 제공받기 위해서는 서비스를 담당하는 ICBS를 거친다. 사용자의 요청을 받은 ICBS에서는 해당 사용자가 시스템에 접근이 허가된 정당한 사용자임 증명하기 위해 전송한 식별정보(ID/PASSWORD, 생체정보 등)를 SECS로 전송하여 사용자의 신원증명을 요청하게 된다. ICBS로부터 전송된 인증 요청은 SECS 내의 인증 모듈의 인증 인터페이스 처리부로 전송된다. 인증 인터페이스 처리부는 사용자 식별정보를 사용자 인증 처리부로 전송하고, 사용자 인증 처리부에서는 요청된 식별정보와 저장되어있는 식별정보를 대조하여 사용자를 인증하고 인증 결과를 반환한다.

결과를 반환받은 ICBS에서는 사용자에게 허용되는 기능을 확인하기 위해 SECS로 사용자에게 허가된 기능에 대한 정보를 요청한다. 요청을 받은 SECS에서는 사용자의 접근 제어 기능을 확인하기 위해 접근제어 모듈의 접근제어 인터페이스 처리부로 요청을 전달하며, 요청을 전달받은 접근제어 인터페이스 처리부는 접근제어 정책 테이블에 있는 정책을 확인하고 결과를 ICBS로 전송한다.

결과를 전송받은 ICBS는 전송받은 정책을 이용하여 사용자에게 제공될 수 있는 서비스를 확인한다. 사용자는 관리자, 사용자로 구분되며, 관리자는 원본 영상정보, 사용자의 인증 및 접근 권한 정보, 암호화 및 비식별화 복원 키 등에 대한 열람, 기록, 수정, 삭제의 기능을 가지며 사용자는 자신이 녹화한 범위의 영상에 한정하여 열람, 기록, 삭제의 기능을 제공한다. 표 4는 ICBS- SECS 인터페이스의 유니트와 역할을 정리한 것이다.

표 4. ICBS - SECS 모듈의 기능 정의
Table 4. Define the functionality of the ICBS - SECS module

Module	Unit	Captions
authentication	Authentication interface	1 request authentication to Authentication processing unit 2 Return results to ICBS
	Authentication processing	1 Perform user authentication with identification key com parison
Access Control	Access control interface	1 AC table reference 2 Adding and changing AC table data
	Access control Policy table	1 Save AC policy 2 Policy decisions when per forming AC

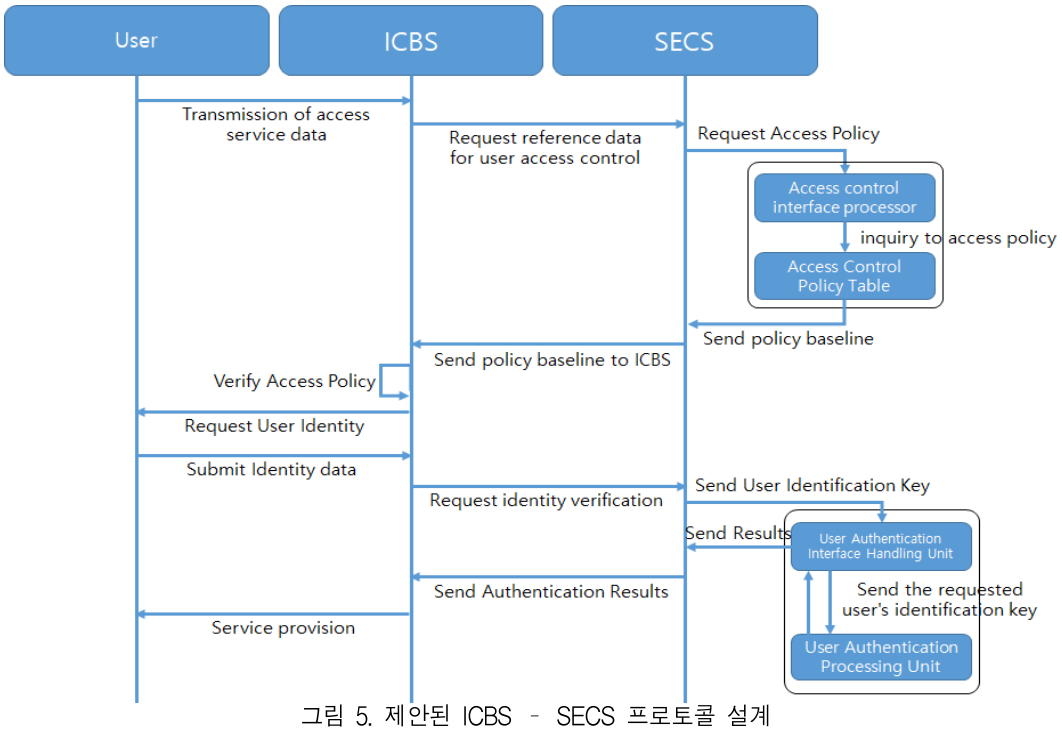

그림 5. 제안된 ICBS - SECS 프로토콜 설계
Fig. 5. Proposed ICBS - SECS protocol design

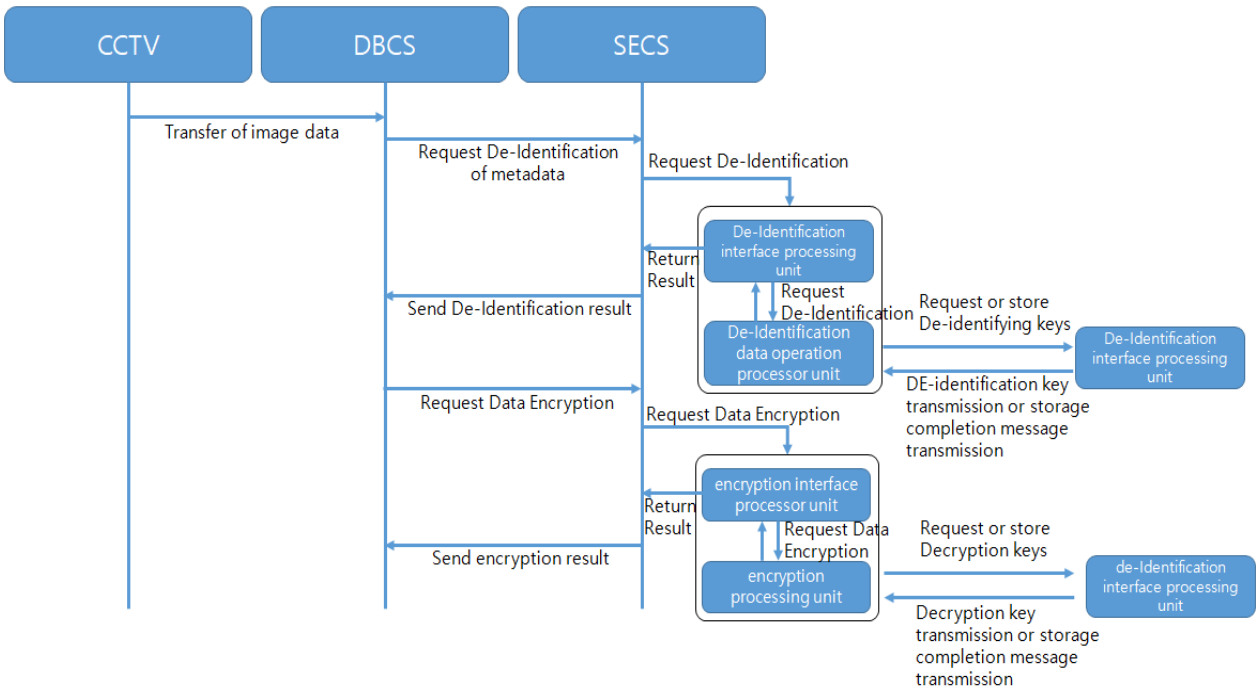

그림 6. 제안된 DBCS - SECS 프로토콜 설계
Fig. 6. Proposed DBCS - SECS protocol design

4.2.2 DBCS-SECS 프로토콜 설계

먼저 영상감시 시스템으로부터 영상정보가 전송되면 DBCS는 SECS로 피사체의 개인정보 유출이 의심되는 데이터에 대한 비식별화 처리를 요청한다. SECS는 메타데이터 비식별화 모듈의 비식별화 인터페이스 처리부로 요청을 전송하며, 요청받은 비식별화 인터페이스 처리부는 비식별화 데이터 연산

처리부로 전송한다. 비식별화 요청을 받은 비식별화 데이터 연산 처리부는 평문 메타데이터에 대응하는 연산 처리를 통한 비식별화 영상정보를 생성하여 결과를 비식별화 인터페이스 처리부로 반환한다 [26]-[29]. 데이터 연산처리부는 비식별화를 진행한 영상에 대한 복원용 키를 저장하며, DBCS에서는 해당 영상을 비식별 처리가 진행된 영상으로 대체한다.

다음으로 영상 데이터의 안전성을 높이기 위하여 영상 데이터를 암호화 처리하는 과정을 진행하는데, DBCS로부터 SECS로 영상 데이터의 암호화를 요청하면 SECS는 암호화 모듈의 암호화 인터페이스 처리부로 요청을 전송한다. 암호화 인터페이스 처리부는 암호화 처리부로 요청을 전달하고, 요청을 받은 암호화 처리부는 요청받은 데이터 파라미터에 대한 암호문을 생성한 뒤 결과를 암호화 인터페이스 처리부로 반환한다. 암호화된 영상에 대한 복호화키는 암호화 처리부에서만 가지게 되며, 복호화를 진행하기 위해서는 암호화된 영상에 대한 복호화키를 SECS로 요청해야만 하며, 복호화 요청이 들어올 경우 해당 영상의 복호화키를 전송하여 DBCS에서 복호화를 진행한다. 이후 같은 영상에 대한 암호화는 새로운 영상으로서 새로운 암호화키를 적용하여 암호화를 진행하게 된다. DBCS에는 암호화된 영상정보만을 저장한다.

표 5. DBCS-SECS 모듈의 기능 정의
Table 5. Define the functionality of the DBCS-SECS module

Module	Unit	Captions
De-identification	de-identification Interface	1 request de-identification 2 Return de-identification results
	de-identification data operation	1 Generate de-identification data
encryption	encryption Interface	1 request encryption 2 Return Encryption Results
	Encryption processing	1 Create a cryptogram

DBCS의 암호화된 영상은 외부에 유출되어도 복호화키가 요구되며, 이에 대한 복호화키는 SECS에서 가지고 있으므로 공격자가 영상정보를 탈취하고자 하는 경우 두 모듈에서 필요한 정보를 별도로 획득해야만 한다. 표 5는 DBCS-SECS 인터페이스의 유니트와 역할을 정리한 것이다.

Ⅴ. 기존 영상감시 시스템과의 차이점

5.1 일반적인 CCTV 시스템과 제안된 시스템의 영상 전송 과정

기존의 영상감시 시스템은 촬영된 영상을 클라우드에 전송하는 과정에서 파이프라인에 암호화 미들웨어를 접목함으로서 전송되는 데이터에 대한 암호화를 진행한다. 클라우드 서버 내에 저장되는 데이터는 사용자의 비밀키를 통해 암호화가 이루어진 암호문으로 사용자를 제외한 타인에 대해 영상이 공개되지 않아야 하므로 암호화된 영상정보를 저장하는 클라우드는 암호문에 대한 복호화키를 필요로 하지 않는다. 그림 7은 영상 전송 과정의 차이를 간략히 나타낸 것이다[20].

본문에서 제안한 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘은 영상감시 시스템으로부터 전송받은 영상 데이터의 사람 및 차량에 대한 검출 및 사고 감지 기능 제공을 위해 플랫폼 내에서 원본 데이터를 가공할 필요성이 존재한다.

개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘은 플랫폼 내에 존재하는 피사체의 개인정보가 포함된 원본 데이터에 대한 프라이버시와 안전성을 제공한다. 영상정보는 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘을 통해 피사체의 개인정보 보호를 위해 비식별화 처리를 진행한 영상 데이터로 변환한다. 이 과정을 거친 영상정보는 기존의 영상감시 시스템과 다르게 피사체의 개인정보를 포함하지 않는다. 제안된 메커니즘은 영상정보를 탈취하기 위해서는 영상정보를 저장하고 있는 모듈과 영상에 대한 비식별/암호화에 대한 복원키를 가진 모듈을 모두 공격하여 영상정보와 영상정보에 대한 복원키를 획득해야만 영상정보의 원본 영상을 얻을 수 있다.

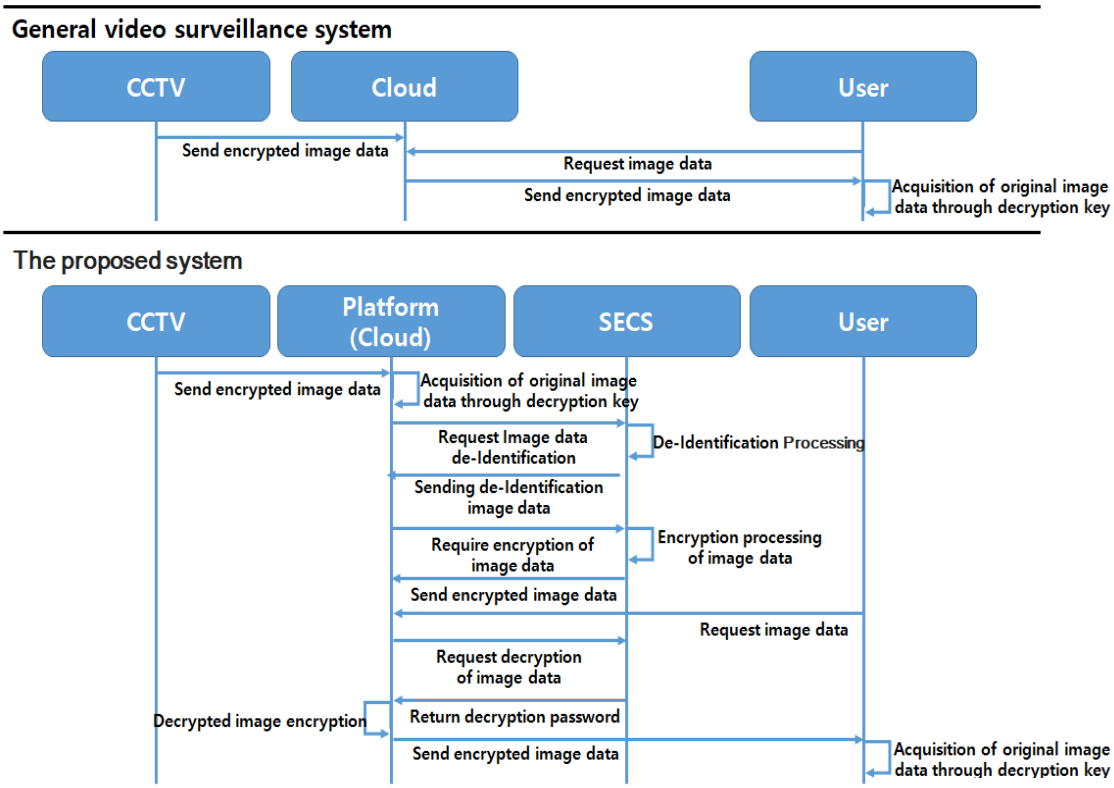

그림 7. 일반적인 CCTV 시스템과 제안된 시스템의 영상 전송 과정
Fig. 7. Process of image transmission of a typical CCTV system and a proposed system

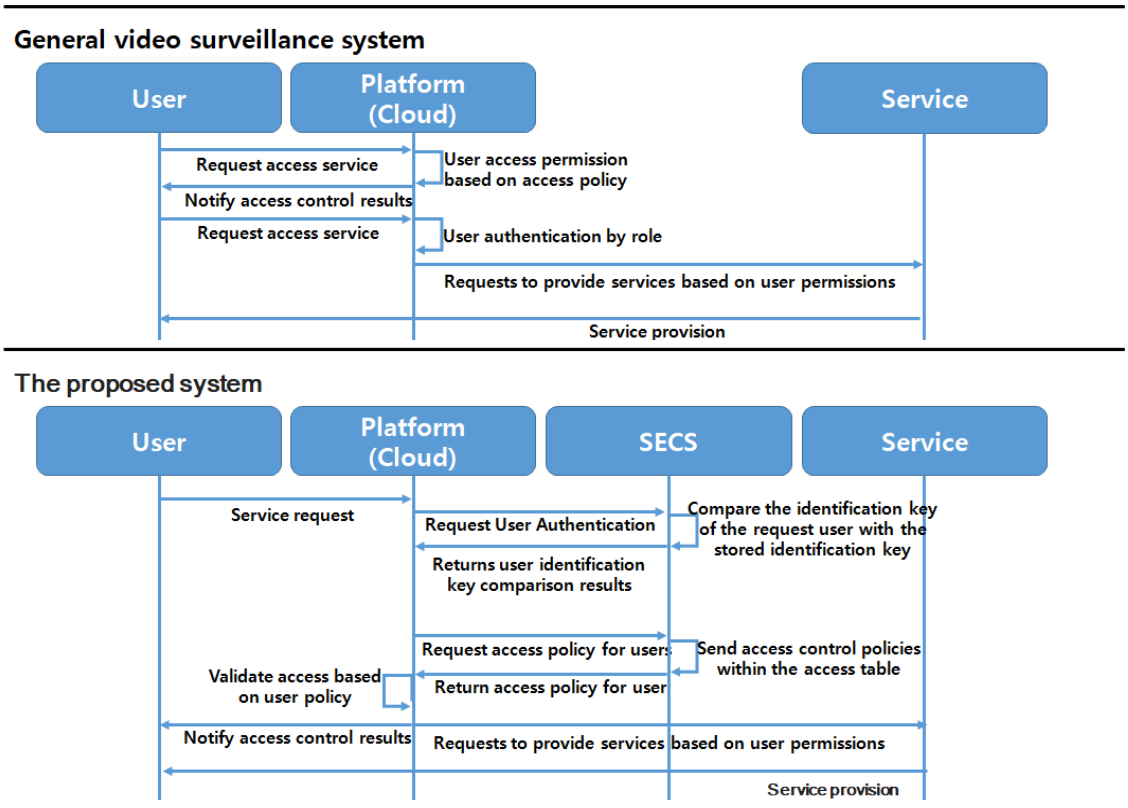

그림 8. 일반적인 CCTV 시스템과 제안된 시스템의 사용자 인증 과정
Fig. 8. User authentication process of general CCTV system and proposed system

5.2 일반적인 CCTV 시스템과 제안된 시스템의 사용자 인증 과정

다음으로 사용자의 시스템 접근과 사용자 인증에 대해 기존의 클라우드 내의 접근제어는 각각의 서비스가 하나씩의 사용자의 역할에 대한 정책을 가지며, 해당 정책에 의거하여 사용자의 권한을 파악하고, 사용자의 역할 권한에 따라 서비스를 제공하였다.

반면 제안된 보안 메커니즘은 독립된 별도의 서비스에서 하나의 플랫폼에서 제공되는 서비스로 제공할 수 있으며, 사용자에 대한 인증을 별도의 모듈에서 진행하고, 정당한 사용자임에 대한 인증 결과를 받고 난 후 사용자의 접근 권한에 대한 정보를 별도의 모듈에서 진행하여 관련 정보를 받아 플랫폼에서 확인하는 방식으로 사용자에 대한 식별정보와 접근 권한을 서비스를 제공하는 하나의 모듈이 아닌 별도의 모듈에서 진행하게 된다. 그러므로 서비스 제공 모듈이 아닌 별도의 보안 전용 모듈에서 식별정보와 접근정책을 저장하고, 이에 대한 확인을 서비스 제공 모듈에서 확인함으로서 보안성을 강화할 수 있다.

그림 8은 일반적인 CCTV 시스템과 제안된 시스템의 접근제어와 인증 서비스 과정을 간략히 나타낸 것이다.

Ⅵ. 결론 및 향후 과제

본 논문에서는 클라우드 기반 지능형 영상보안 인큐베이팅 플랫폼내의 데이터 보안과 피사체의 개인정보 보호를 위한 개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 메커니즘의 구조와 시스템간의 인터페이스를 소개하였다.

개방형 클라우드 환경의 지능형 영상감시 인큐베이팅 보안 서비스는 하나의 독립된 서비스로서 클라우드 상에서 영상감시 시스템에 대한 프라이버시 영상정보 비식별화, 클라우드 내의 데이터 암호화, 인가된 사용자의 시스템 접근 허가를 위한 접근제어, 접근한 사용자의 신분 확인을 위한 인증 기능을 수행하는 독립된 보안 서비스를 제공할 수 있다.

References

[1] Jin Su Kim, Min-Gu Kim, and Sung Bum Pan, "A Study on Optimization of Intelligent Video Surveillance System based on Embedded Modul", Journal of Smart Media, Vol. 7, No. 2, pp. 40-46, Jun. 2018.

[2] Hyeon-in Cha, Gwangho Song, and Yoosung Kim, "A Recognition of Violence Using Mobile Sensor Fusion in Intelligent Video Surveillance Systems", Journal of KIISE, Vol. 45, No. 6, pp. 533-544, 2018.

[3] Jinsu Kim, Sangchoon Kim, and Namje Park, "Openstack Security Techniques of Cloud Service", Conference of JCITPE, pp. 57-59, Aug. 2018.

[4] "Data encryption", Openstack, https://docs.openstack.org/security-guide/tenant-data/data-encryption.html. [accessed: Jan. 29, 2019]

[5] "Authentication procedure of open stack keystone", Zetawiki, https://zetawiki. com/wiki/%EC%98%A4%ED%94%88%EC%8A%A4%ED%83%9D_%ED%82%A4%EC%8A%A4%ED%86%A4_%EC%9D%B8%EC%A6%9D%EC%A0%88%EC%B0%A8. [accessed: Jan. 29, 2019]

[6] "Role-Based Access Control Overview", Openstack, https://docs.openstack.org/patrole/latest/rbac-overview.html. [accessed: Jan. 29, 2019]

[7] Donghyeok Lee and Namje Park, "CCTV Video Data Security Scheme for Open Distributed Cloud Environment", Conference of KSII, Vol. 19, No. 1, pp. 113-114, Apr. 2018.

[8] Top Threats to cloud computing, Cloud Security Alliance, pp. 8-36, 2017.

[9] Donghyeok Lee and Namje Park, "Proposal of Technol ogy and Policy Post-Security Management Framew ork for Secure IoT Environment", Journal of KIIT, Vol. 15, No. 4, pp. 127-138, Apr. 2017.

[10] OWASP, The Open Web Application Security Project, pp. 6-16, 2017.

[11] Tae-hwan Park, Ga-ram Lee, and Ho-won Kim,

"Survey and Prospective on Privacy Protection Methods on Cloud Platform Environment", Journal of KIISC, Vol. 27, No. 5, pp. 1149-1155, Oct. 2017.

[12] "IBM Bluemix", IBM, https://www.ibm.com/cloud-computing/bluemix/ko [accessed: Jan. 28, 2019]

[13] "Microsoft Azure", Microsoft, https://docs.microsoft.com/ko-kr/azure/security/ azure-security. [accessed: Jan. 28, 2019]

[14] "Amazon Web Sevice", Amazon, https://aws.amazon.com/ko/security/ [accessed: Jan. 28, 2019]

[15] "Paas-Ta", PaaS-Ta, https://www.paas-ta.kr/intro/forwarding_result. [accessed: Jan. 28, 2019]

[16] Hyeog Jang, Taehyeon Hwang, Hunjun Yang, "Highway Incident Detection and Classification Algorithms using Multi-Channel CCTV", Journal of IEIE, Vol. 51, No. 2, pp. 23-30, 2014.

[17] Donghyeok Lee, Namje Park, "Similarity-based Virtual Facial Generation Method for Privacy Protection of Intelligent CCTV Environment", Journal of CISC 2017, Jun. 2017.

[18] Namje Park, "Privacy Enhanced CCTV Video Security Framework using Metadata De-identification", Journal of ICICT, pp. 199-200, 2018.

[19] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", International Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[20] Donghyeok Lee and Namje Park, "ROI-based efficient video data processing for large-scale cloud storage in intelligent CCTV environment", International Journal of Engineering and Technology, Vol. 7, No. 2.33, pp. 151-154, Mar. 2018.

저자소개

김 진 수 (Jinsu Kim)

2017년 2월 : 강원대학교 정보통신공학전공 학사
2017년 3월 ~ 현재 : 강원대학교 전자정보통신공학전공 석사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT 등

박 남 제 (Namje Park)

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