KIPS Tr. Software and Data Eng.
Vol.4, No.9 pp.409~418 pISSN: 2287-5905

http://dx.doi.org/10.3745/KTSDE.2015.4.9.409

Access Control Policy of Data Considering Varying Context in Sensor Fusion Environment of Internet of Things

You-jin Song† · Aria Seo†† · Jaekyu Lee††† · Yei-chang Kim††††

ABSTRACT

In order to delivery of the correct information in IoT environment, it is important to deduce collected information according to a user's situation and to create a new information. In this paper, we propose a control access scheme of information through context-aware to protect sensitive information in IoT environment. It focuses on the access rights management to grant access in consideration of the user's situation, and constrains(access control policy) the access of the data stored in network of unauthorized users. To this end, after analysis of the existing research 'CP-ABE-based on context information access control scheme', then include dynamic conditions in the range of status information, finally we propose a access control policy reflecting the extended multi-dimensional context attribute. Proposed in this paper, access control policy considering the dynamic conditions is designed to suit for IoT sensor fusion environment. Therefore, comparing the existing studies, there are advantages it make a possible to ensure the variety and accuracy of data, and to extend the existing context properties.

Keywords : Internet of Things, Sensor Fusion, Context Awareness, Access Control Policy, Access Structure Tree

사물인터넷 센서퓨전 환경에서 동적인 상황을 고려한 데이터 접근제어 정책

송 유 진† · 서아리아†† · 이 재 규††† · 김 의 창††††

요 약

IoT 환경에서는 정확한 정보의 전달을 위하여 사용자의 상황에 따라 수집된 정보를 추론하여 새로운 정보, 즉 상황 정보를 생성하는 것이 중요하다. 본 논문에서는 IoT 환경에서 센싱 되는 민감한 정보를 보호하기 위해 상황인식을 통한 정보의 접근제어 기법을 제안하고자 한다. 이는 사용자의 상황을 고려하여 접근을 허가하는 접근권한 관리에 중점을 두고 있으며 승인되지 않은 사용자가 네트워크에 저장되어있는 데이터에의 접근 제약(접근제어 정책)을 둔다. 이를 위해 기존에 연구된 CP-ABE 기반의 상황 정보 접근제어 기법에 대해 분석한 후, 상황 정보의 범위에 동적인 상황을 포함시켜, 확장된 다차원 상황 속성(Context Attribute)을 반영하는 접근제어 정책을 제안한다. 본 논문에서는 동적인 상황을 고려한 접근제어 정책을 IoT 센서퓨전 환경에 적합하도록 설계하였다. 따라서 기존의 연구와 비교해 데이터의 다양성 확보 및 정확한 정보의 수집이 가능하고, 기존 상황 속성의 확장이 가능하다는 장점을 갖는다.

키워드 : 사물인터넷, 센서퓨전, 상황인식, 접근제어 정책, 접근구조 트리

1. 서 론

최근 센서 네트워크와 유비쿼터스 컴퓨팅(Ubiquitous Computing) 기술의 발달로 인하여 IoT(Internet of Things, 사물인터넷), 즉 인터넷을 기반으로 모든 사물들을 연결하여 사람과 사물, 사물과 사물 간의 상호 소통을 가능하게 하는 지능형 기술 및 서비스의 시대로 진입하고 있다. IoT는 문화, 생활, 건강, 교육, 교통 등 여러 분야에서 새로운 서비스로 창출되고 있으며 향후에도 다양한 영역의 사회 문제를 해결하기 위한 중요한 기술 분야로서 더욱 발전할 것이다.

또한, 가정, 자동차, 사무실 등의 일상생활에서뿐만 아니라 의료, 화학, 원자력 등의 특수한 환경에서 사용자 지원을 가능하게 함으로써 지금까지 불가능했던 다양한 서비스를 제공하게 되어 새로운 가치를 창출할 수 있을 것으로 예측된다.

※ This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(2013R1A1A2011581). This work was also supported by the Dongguk University Research Fund of 2014.
† 정 회 원 : 동국대학교 경영학부 교수
†† 비 회 원 : 동국대학교 테크노경영협동과정 정보기술전공 박사과정
††† 비 회 원 : 동국대학교 테크노경영협동과정 정보기술전공 석사과정
†††† 종신회원 : 동국대학교 경영학부 교수
Manuscript Received : August 4, 2015
First Revision : September 1, 2015
Accepted : September 3, 2015
* Corresponding Author : You-jin Song(song@dongguk.ac.kr)

이와 같이 사물인터넷은 우리 주변에 있는 스마트 폰, 태블릿 PC 등의 스마트 디바이스, 신발, 시계, 패치, 밴드 등의 웨어러블 디바이스, 텔레비전, 오디오, 냉장고, 가스레인지 등의 가전제품을 비롯한 공장 내의 각종 부품, 거리의 상점, 상점 내의 물품 등 모든 사물이 인터넷과 연결되어 우리의 삶을 더욱 풍요롭게 만들 것으로 예상되고 있다.

IoT 환경에서는 정확한 정보의 전달을 위하여 사용자의 상황에 따라 수집된 정보를 추론하여 새로운 정보, 즉 상황정보를 생성하는 것이 중요하다. IoT 환경이 구축된 사회에서는 모든 사물의 지능화를 통해 자율적으로 주변 환경정보를 센싱 하여 주변 상황을 인식하고 사물을 제어할 수 있는 네트워크가 형성될 것이다. 이를 위해 다양한 센서를 통한 정보 수집이 이루어져야 할 것이며 이 중에는 사용자의 개인정보나 신체정보 등 민감한 정보도 포함될 수 있다.

대부분의 인터넷 애플리케이션이 사용자가 인지한 상태에서 이루어지는 것에 비해, 사물인터넷이 가져올 변화 중 큰 차이는 IoT 기기는 사람들에게 보이거나 느껴지지 않는 상황에서 환경 안에 내포되어있기 때문에 '무의식적인 노출'이 상시로 이루어질 수 있다는 것이다.

이러한 상황 정보(상황, 맥락, 문맥)에 포함된 민감한 정보의 역기능으로 인하여 개인정보 보호 문제가 발생하고 있다. 인터넷에 연결된 단말기 중 90%가 개인정보를 취득하고 있지만 70%의 단말기가 암호화되지 않은 네트워크를 사용하고 있으며, 대부분의 IoT 제품이 개인정보를 수집하고 있음에도 불구하고 충분한 정보 보호 대책이 이루어지지 않은 제품이 많이 나오고 있는 실정이다[1].

사물인터넷은 센싱정보에 기반한 지능형 서비스를 제공하는 것으로 개인정보 해킹과 보안침해 등 많은 위험이 잠재하고 있다. 자동차 운전 기록이나 습성, 블랙박스나 길거리 CCTV 장치를 통한 원치 않는 노출이 이루어지고, 스마트 미터링을 통해 특정 가족의 에너지 사용이 검침되고, 스마트 시티화에 의해 시민들의 움직임이나 활동 특성이 모아지고 분석된다. 또한, 내가 먹는 음식의 양이나 칼로리, 운동량, 거리, 경로를 모아서 분석하고 내 운동 특성이나 개인 활동의 정량화(계량화), 즉 건강관리의 디지털화가 이루어지고 있다.

이와 같이 사물인터넷 환경에서 발생할 수 있는 위험은 사용자에게 공유된 장소뿐만 아니라 사적인 공간과 건물 내부의 센싱 되는 데이터는 바로 사람들에게 부착되는 웨어러블 기기나 스마트 기기를 통해 생성되는 개인정보나 활동 데이터(디지털 라이프 로그) 등에 대한 동의와 신뢰가 이루어지지 않은 상황에서 예기치 못한 보안사고가 발생할 수 있을 것이다.

FTC 보고서[2]에서는 이러한 문제를 해결하기 위해 세 가지의 시책을 언급했다. 제품이나 서비스의 디자인과정에서 개인정보 보호 및 보안위험에 대한 충분한 검토를 우선하는 '보안 디자인의 채용'과 대량의 개인정보를 수집 및 저장할수록 유출 가능성이 높아지기 때문에 데이터의 수집 및 저장을 최소화하는 '데이터 최소화 원칙', 마지막으로 예상치 못한 정보의 유출이 발생할 시 소비자에게 적절하고 신속하게 정보를 공개하는 '시스템의 투명성 확보'이다.

또한, FTC 보고서[2]에 따르면 개인정보 보호에 특히 위험이 높은 3가지 요소를 정보 수집의 편재화, 개인정보의 목적 외 사용, 그리고 악의적인 공격으로 분류했다. 데이터 수집의 편재화는 센서 및 모니터링 기술이 발달함에 따라 언제 어디서나 개인정보의 수집이 이루어진다는 것이다. 건강 및 피트니스를 위한 IoT 헬스케어 기기에서 수집된 개인정보가 유출되어 보험 회사가 건강 보험과 생명 보험의 요율을 계산하기 위해 사용되는 사례를 예로 들 수 있다. 이와 같은 문제는 사용자가 편리성을 추구하는 동시에 자신도 모르는 사이에 자신의 개인정보가 유출되는 결과로 이어질 수 있다.

한편, 미국 국립표준연구소(NIST) 빅데이터 참조 아키텍처[3]에서는 IoT를 데이터 공급자(Data Provider)와 데이터 소비자(Data Consumer) 관점에서 다루고 있다. 즉, IoT는 다양한 소스에서 추상 데이터 형을 생성하고 다양한 기능 인터페이스에서 사용할 수 있는 형태로 제공하는 '데이터 공급자'이며, 빅데이터의 출력 값을 받는 "데이터 소비자"인 쌍방에 관련된 새로운 기술로 자리매김하고 있다(Fig. 1).

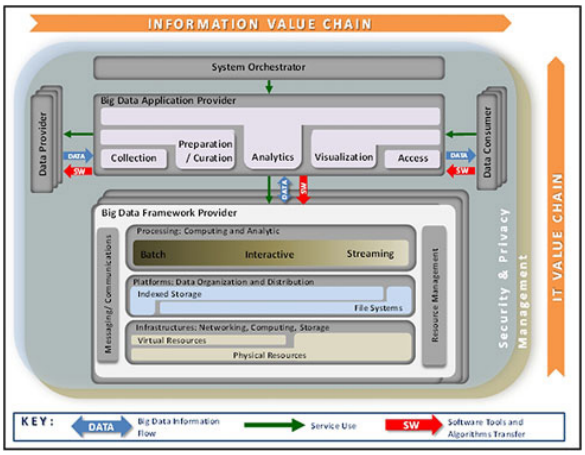

Fig. 1. NIST Big Data Reference Architecture[3]

이러한 IoT의 오픈아키텍처 특성으로 인해 보안성은 IoT 개념의 확산을 저해하는 요소가 되고 있다. 상황을 이해하는 컴퓨팅과 같은 새로운 기술과 센서퓨전과 같은 IoT융합 기술을 이용하면, 사용자 데이터 및 접근권한의 정확한 분석을 통해 보다 보안성이 강화된 IoT 환경을 제공할 수 있다.

이러한 관점에서 상황 정보에 포함된 민감한 데이터를 어떻게 저장하고 활용하며, 누가 이용할 수 있도록 하는 것인가에 대해 보다 투명한 관리 및 상황인식을 통한 접근제어는 향후 IoT의 안전한 서비스를 위해 필수 불가결하다. 여기서, 데이터를 안전하게 저장하고 공유하기 위한 속성기반 암호화 등의 기법이 필요하고, 프라이버시 관련 데이터를 이용할 수 있는 권한을 제한할 수 있는 접근제어 기법이 필요하게 된다.

본 논문에서는 IoT 환경에서 센싱 되는 민감한 정보를 보호하기 위해 상황인식을 통한 정보의 접근제어 기법을 제

안하고자 한다. 이는 사용자의 상황을 고려하여 접근을 허가하는 접근권한 관리에 중점을 두고 있으며 승인되지 않은 사용자가 네트워크에 저장되어있는 데이터에의 접근 제약(접근제어 정책)을 둔다.

이를 위해 기존에 연구된 CP-ABE(Ciphertext Policy-Attribute Based Encryption) 기반의 상황 정보 접근제어 기법[4]에 대해 분석한 후, 상황 정보의 범위에 동적인 상황을 포함시켜, 확장된 다차원 상황 속성(Context Attribute)을 반영하는 접근제어 정책을 제안한다. 본 논문에서 동적인 상황을 고려한 접근제어 정책은 IoT 센서퓨전 환경에 적합하도록 설계함으로써 기존의 연구와 비교해 데이터의 다양성 확보 및 정확한 정보의 수집이 가능하고, 기존 상황 속성의 확장이 가능하다는 장점을 갖는다.

본 논문의 1절에서는 연구의 목적과 배경에 대하여 서술했고, 2절의 관련 연구에서는 기존에 연구된 상황 정보의 정의 및 분류, 상황 정보 접근제어 그리고 센서퓨전을 통한 상황인식에 대해 조사하였다. 3절에서는 상황 정보를 3차원으로 확장하여 센서퓨전 환경에서 동적인 상황을 고려한 CP-ABE 기반의 데이터 접근제어 정책을 제안하였고, 4절에서 기존의 연구 결과와 본 연구의 결과를 비교 분석하였다. 마지막으로 5절에서 결론과 향후 연구 과제를 제시했다.

2. 관련 연구

2.1 상황 정보의 정의 및 분류

상황은 사건, 주장, 상황, 사상의 배경을 이루는 주변 정황 또는 사실로 정의된다[4]. 소프트웨어 프로그래밍에서는 상황인식 애플리케이션을 개발한다는 개념이 존재해왔다. 상황인식 애플리케이션은 누가, 어디서, 언제, 무엇을 하는지 조사하며, 소프트웨어 설계자는 이러한 배경 정보를 사용하여 어떠한 상황이 왜 일어나는지 판단하고 애플리케이션에 인코딩 한다. 이러한 정의를 기준으로 상황인식은 'Location, Identity, Time, Activity'의 네 가지 가장 중요한 범주의 정보로 구성된다[5].

Charith Perera et al.(2014)의 연구에서는 IoT의 관점에서 상황인지를 조사하여 상황에 맞는 라이프 사이클에 대한 심층적인 분석을 했다. Fig. 2는 Conceptual Perspectives와 Operational Perspectives의 두 개의 서로 다른 관점에서 상황을 분류한 것이다. Primary Context는 현재의 상황을 고려하지 않고 취득된 데이터 혹은 센서 데이터 추론 과정을 거치지 않은 데이터이며, Secondary Context는 Primary Context를 사용하여 계산될 수 있는 임의의 정보로서 웹 서비스 호출과 같은 센서 데이터 융합 또는 데이터 검색을 이용하여 계산될 수 있다. 먼저 Primary Context는 location, identity, time, activity의 네 가지 유형으로 구분하였으며 여기서 발견될 수 있는 Secondary Context를 정의하였다. 예를 들면, 사람의 'identity'로 Primary Context를 고려할 때 전화 번호, 주소, 이메일 주소 등의 관련 정보를 획득할 수 있다. 즉, 두 가지의 관점에서 분류하는 것 모두 중요하다는 것을 알 수 있다.

한편, 상황 정보는 사람의 감성 정보 및 생체 정보 등과 같이 지속적으로 변화하는 동적인 속성을 갖는다. 즉, 제시된 2차원적 구성을 넘어 다차원으로 확장시킬 필요가 있다. 본 논문에서는 동적 상황 정보의 속성을 갖는 Composite Context를 포함시켜 x, y, z의 3축을 이루는 3차원의 관점에서 상황을 분류하였다.

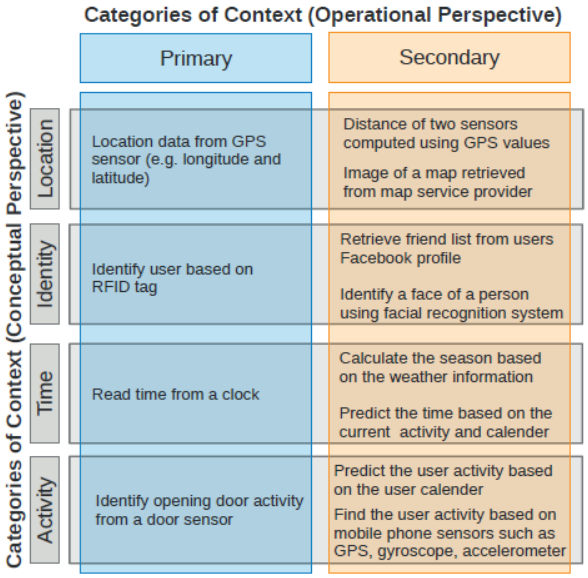

Fig. 2. Context Classified in Two Perspectives[4]

2.2 상황 정보 접근제어

기존에 연구된 다양한 접근제어 방법들[6-8]은 IoT 환경에 적용하는 데 따르는 문제들로 인하여 효과적이지 못하다. DAC(Discretionary Access Control) 모델은 보안 수준이 상대적으로 낮으며, MAC(Mandatory Access Control) 모델은 전체 시스템 관리자에 따라 접근 규칙이 생성되어 권한 결정이 사용자의 신원에 기초하기 때문에 위의 두 모델은 IoT 환경에 적절하지 않다. 또한 RBAC(Role-based Access Control) 모델은 접근 권한 관리의 복잡성을 단순화할 수 있으나 네트워크 환경에서 알 수 없는 사용자를 위한 접근제어와 권한 부여 및 위임을 수행할 수 없다.

Ling Yu, et al.(2013)의 연구에서는 기존의 접근제어 모델의 문제점을 해결하고자 CP-ABE(Ciphertext-Policy Attribute-Based Encryption) 알고리즘을 기반으로 유비쿼터스 학습 시스템 자원의 상황인식 접근제어 방식을 제안했다. Fig. 3과 같이 접근제어 정책을 설정하는 목적은 자원에 해당하는 암호화를 실행하고 자원을 아웃소싱 하는 것이다.

이러한 CP-ABE 기반 접근제어 정책은 유연한 접근권한 관리 기능을 제공할 수 있어서 시스템의 확장성이 좋다. 또한 CP-ABE와 대칭키 메커니즘을 결합하여 효율성을 높일 수 있는 편리한 방법이다. 그러나 IoT 환경에서 정확한 상황 정보의 생성과 제공을 위해서는 다중센서를 통해 정보의 수집이 이루어져야 하며, 따라서 감성 정보, 생체 정보 등과

같은 동적인 센싱 정보가 포함될 수 있다. 이 경우 제안된 구조와 같이 2차원적 접근이 아닌 다차원적 접근이 필요하다.

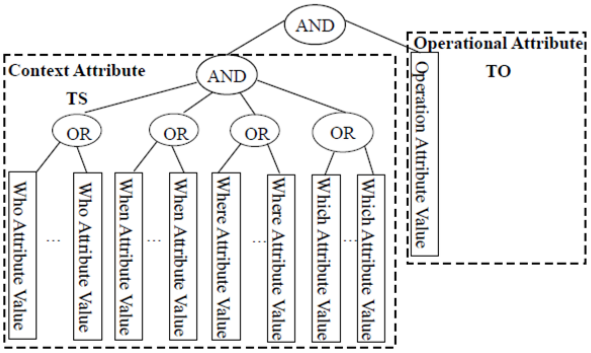

Fig. 3. The General Structure of an Access Control Policy Tree[9]

본 논문에서는 기존의 상황 정보 접근제어 방식의 한계점을 해결하고자 상황 정보의 범위에 동적 속성을 포함시켰으며 확장된 다차원 상황 속성을 기반으로 접근제어 정책을 제안한다.

2.3 센서퓨전을 통한 상황인식

Kaivan Karimi[5]는 센서퓨전(Sensor-fusion)과 이를 통한 감각데이터 감지 및 처리에 대한 연구를 진행하였다. 센서퓨전이란 마이크로 컨트롤러를 활용하여 다양한 센서에서 수집된 별개의 데이터를 융합함으로써 각각의 개별 센서 자체에서 나온 데이터를 사용하는 것보다 더 정확하고 신뢰성 높게 데이터를 확인할 수 있도록 하는 기술이다. 센서퓨전은 상황인식을 지원하며, 이는 IoT에서 막대한 가능성을 가지고 있다.

특히 센서퓨전의 작동방식을 인간이 외부 환경을 경험하는 감각 획득 및 처리 사례를 들어 설명하고 있다. 즉 시각, 청각, 화학적 감각(후각 및 미각), 표면 감각(촉감)의 감각정보를 받아 말초신경계를 통해 두뇌로 전달되고, 두뇌는 주어진 상황이나 경험에 대해 어떻게 대응할 것인지 결정한 후 여러 기관을 통해 행동하게 하는 것이다. IoT환경에서도 센서퓨전은 비슷한 역할을 한다. 센서퓨전은 다양한 센서의 입력을 통합하여 더 정확하고 신뢰성 높은 센싱을 실현함으로써 훨씬 높은 수준의 인지력과 새로운 응답을 제공할 수 있다.

인간, 자연, 환경, 기계·인프라 사이의 상호 작용은 Fig. 4와 같이 상황인식을 판단하는 데 유용한 데이터를 제공한다. 센서는 인간의 사고방식에 대한 액세스를 제공함으로써 경험을 더 '개인적'인 것으로 만들어준다.

또한 Kaivan Karimic[5]는 의료 전자공학 및 비의료 애플리케이션의 멀티 센서 프로세싱 용도와 관련하여 진행되는 호세 페르난데스 비야세뇨르(José Fernández Villaseñor) 박사의 연구를 소개하고 있다. 이 연구에 따르면 신체 활동으로 인해 증가되는 심장 박동은 흥분으로 발생된 아드레날린으로 인해 증가되는 것과 다른 패턴 및 기울기를 가진다. 따라서 알고리즘을 사용하고 센서 데이터를 분석하면 사람이 표시하는 감정의 유형을 전자적으로 감지할 수 있다. 따라서 생리적 변수와 상태를 모니터링 하고 데이터를 수집하여 감정을 전자적으로 감지할 수 있다. 예들 들어, 압력 센서를 통해 근육 이완(MR: Muscle Relaxation) 및 근육 수축(MC: Muscle Contraction) 정도를 확인할 수 있으며, 2극 심전도 침을 통해 심장박동 변화(HRV: Heart Rate Variability)를 확인할 수 있다. 또한 정전용량 센서를 통해 땀(S: Sweat)의 정도를 확인할 수 있으며, 가속도계를 사용한 신체의 이완 상태(발작적인 동작, 흔들림 없는 손)의 모니터링을 통해 태도(A: Attitude)를 확인할 수 있다.

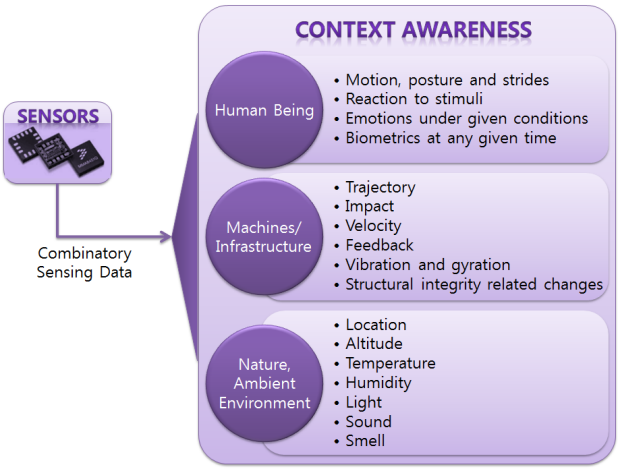

Fig. 4. Sensor Fusion Enables Context Awareness[5]

본 논문에서는 감성데이터와 생체데이터 등 지속적으로 변화하는 동적인 속성이 갖는 상황 정보를 추가하여 3차원의 상황 분류 체계를 구성한다. 또한, 동적 속성 집합을 구성하기 위해 감성(Emotion), 생체(Biology), 인프라(Infra), 환경(Environment) 속성 값을 사용한다.

3. 시스템 구조 제안

3.1 3차원 상황 정보 확장

본 논문에서는 기존의 개념적 속성(Conceptual Attribute)과 운영적 속성(Operational Attribute)의 관점에서 상황을 분류하던 2차원 구성에서 동적으로 변화하는 상황 정보를 포함하여 3차원의 상황분류 체계를 구성했다. 이를 위해 x, y축에 z축을 추가하여 동적 속성(Dynamic Attribute)을 구성했다.

개념적 속성은 기존 연구와 같이 가장 기본이 되는 상황 정보인 'Location, Identity, Time, Activity'를 두고 운영적 속성에서 현재의 상황을 고려하지 않고 취득된 데이터 혹은 센서 데이터 추론 과정을 거치지 않은 데이터 Primary와, 이를 사용하여 계산될 수 있는 임의의 정보인 Secondary로 구분한다. 동적 속성에서는 생체 데이터와 Secondary의 데이터 융합에서 추론될 수 있는 감성 정보, 생체 정보, 인프

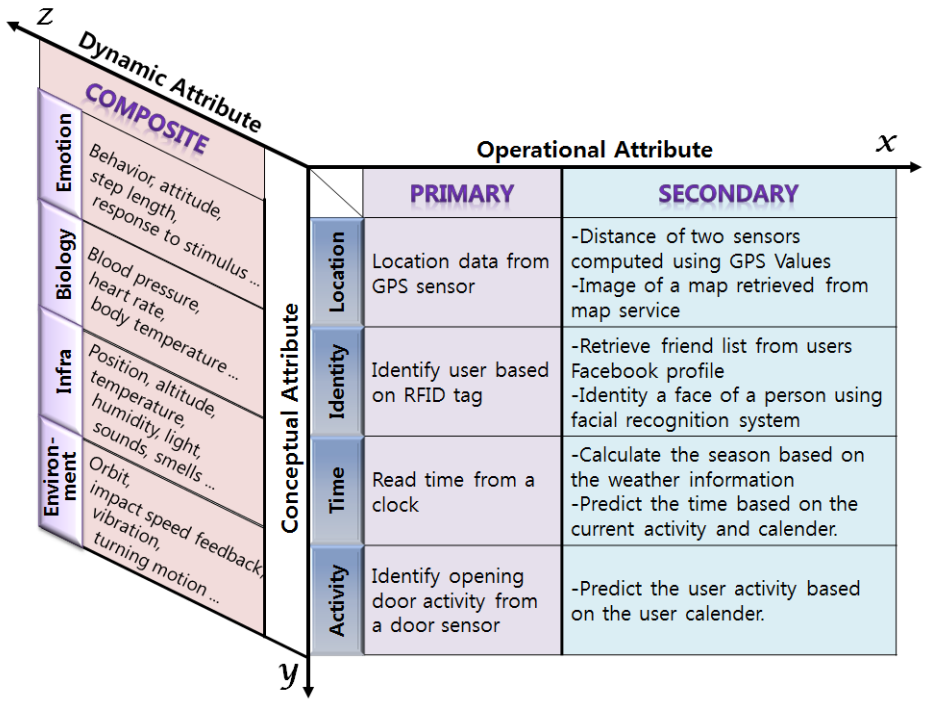

Fig. 5. Three-Dimensional Context Classification

라 정보, 그리고 환경 정보 등의 Composite를 추가한다(Fig. 5).

본 논문의 시나리오는 다음과 같다. IoT 환경에서 헬스케어 시스템(Health Care System) 사용자인 노인이 등산 중 실족하여 낙상했다. 시스템에서 센싱 된 노인의 위치 데이터가 일정 시간 동안 변화가 없고, 특히 해당 위치가 낙상 주의, 안개주의 등 고위험 구간이며 스마트 디바이스에서 감지한 충격 정도와 심박수 및 출혈로 인한 혈압 변화 등의 생체데이터를 기반으로 노인의 위험 상황을 인지하여 구조대에 지원을 요청할 수 있다. 이때 구조대원은 클라우드 상에 암호화되어있는 노인의 병력사항을 확인할 수 있다. 복호화된 노인의 병력사항을 통해 당뇨병을 확인하여 지혈과 혈액보충에 중점을 둔 응급 처치가 가능하고 이와 동시에 최적의 조건(거리, 전문성 등)에 있는 병원에 신속한 치료 준비를 할 수 있도록 한다. 즉, 의사와 구조대 및 환자를 포함하는 사용자가 암호화된 환자의 병력사항 등의 자원에 접근하려 할 때 각 상황의 속성에 따라 생성된 복호키를 이용하여 접근 권한을 검증하는 것이다.

시나리오에 따라 Fig. 5에서 설명하는 Location데이터를 예로 들면, Primary는 GPS로부터 얻은 위치 데이터이며, Secondary는 위치 데이터에 따라 해당 위치가 특정 사용자에게 고위험군의 여부를 파악할 수 있는 정보를 나타낸다. Composite는 사용자의 생체데이터의 변화를 통해 특정 사용자에게 발생한 사고를 추론할 수 있고 사용자의 상황에 적합한 병원의 위치와 거리를 파악할 수 있는 정보이다.

본 논문에서는 IoT 헬스케어 시스템 시나리오를 두고 있지만, 일반적인 시스템 디자인을 기본으로 하고 있어 데이터 접근 및 처리를 위한 다른 컴퓨팅 도메인에 적용될 수 있다.

3.2 시스템 구조

본 논문에서 제안하는 시스템은 Certification Center, 클라이언트, 그리고 클라우드 Storage Center로 구성되어있다(Fig. 6). Certification Center는 시스템의 보안 매개변수인 PK(Publick Key)와 MK(Master Key)를 생성하는 System Initialization 장치와 사용자 ID와 암호를 기록하는 데 사용되는 사용자 데이터베이스(User DB)를 유지하고 각 로그인 한 사용자의 ID를 확인, 그리고 인증된 사용자에 대한 보안 매개 변수 PK 및 클라이언트 소프트웨어를 배포하는 Certification장치, 마지막으로 사용자에 의해 제공되는 상황에 따라 복호키를 생성하는 Key Generation장치로 구성되어있다. 클라이언트는 사용자(예를 들면, 의사 및 환자)이며 Encryption 장치, 사용자의 상황을 수집하는 Context Aware 장치, 그리고 Decryption 장치로 구성된다.

(1) Certification Center의 System initialization은 시스템 보안 파라미터 PK 및 MK를 생성한 후, PK를 사용자 Certification에, MK를 Key Generation에 각각 전송한다.
(2) 최초 사용자는 시스템에 등록한 후, 클라이언트는 개인의 ID와 비밀번호를 입력하여 시스템에 로그인한다.
(3) Certification Center의 Certification은 User DB에 저장된 사용자 정보를 확인하여 검증된 사용자에게 PK를 전송한다.
(4) 클라이언트는 제안된 접근제어 정책에 따라 PK를 이용해 진료내역 등 자원을 클라우드 Storage Center로 업로드 한다.

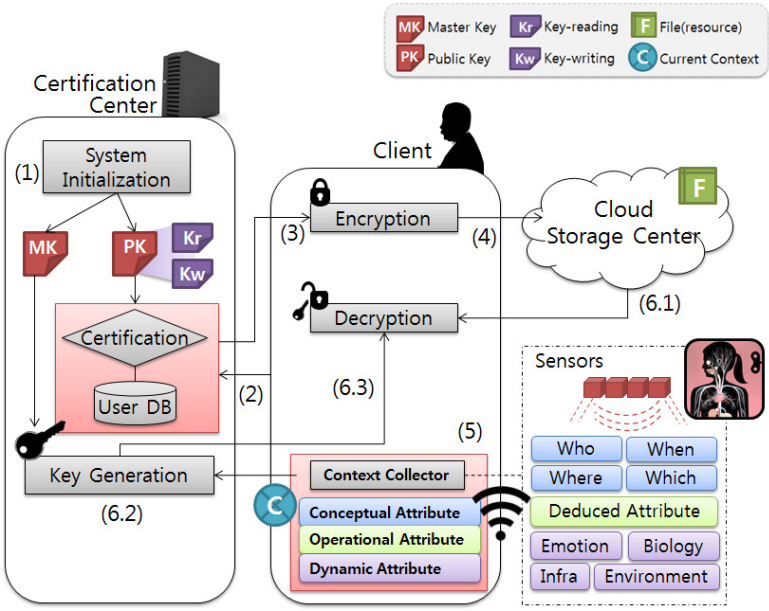

Fig. 6. System Architecture

(5) 클라이언트는 센서를 통해 사용자의 상황을 수집한다. 이때 상황은 다양한 속성으로 구분될 수 있다. 특히 사용자의 감성 정보 및 생체 정보, 인프라, 환경 정보 등 동적인 정보의 수집이 이루어질 수 있다.

(6.1) 클라이언트는 클라우드 Storage Center에서 진료내역 등의 자원을 다운로드 한다.

(6.2) Certification Center의 Key Generation은 수집된 사용자의 상황 정보를 받아 MK와 상황 속성에 따라 대응하는 복호키를 생성한다.

(6.3) 클라이언트의 Decryption은 Key Generation에서 전송된 복호키를 받아 복호할 수 있다.

3.3 다중 속성 접근제어 정책을 위한 접근구조 트리 구성

본 논문에서는 기존 연구[4]에서 제시되었던 개념적 속성과 운영적 속성의 2차원적 속성기반에 동적인 속성을 추가하여 3차원의 속성을 기반으로 한 상황인식 접근제어 정책을 제안한다(Fig. 7).

제안된 접근제어 정책은 기본적으로 다양한 환경에서 활용될 수 있으나, 본 논문에서는 IoT 환경에서 헬스케어 시스템을 이용하는 노인의 병력사항 기록에 접근하려 할 때 그 조건을 충족시키기 위한 시나리오와 CP-ABE 알고리즘을 기반으로 상황인식 접근제어 정책을 제안한다. 환자의 개인 의료정보는 매우 민감한 정보로서 안전성을 유지하기 위해서 보안에 대한 검증이 충분히 이루어져야 한다.

Fig. 7과 시나리오에 따라 상황인식 접근제어정책(T)은 개념적 속성(CA), 운영적 속성(OA), 그리고 동적 속성(DA)의 세 부분으로 구성된다. 또한 접근제어를 위한 기능적 속성에 따라 정책이 수립되도록 한다(ACA, Access Control Attribute).

T={OA AND CA AND DA}AND ACA
OA={CA AND DAV}
CA={Who AND When AND Where AND Which}
DA={EmAV OR BAV OR IAV OR EnAV}
ACA={RO OR RW}

2차원으로 구성된 OA는 Primary속성을 갖는 CA와 거기서 파생된 Secondary에 대한 속성을 모두 포함한다. CA는 사용자가, 언제, 어디서, 어떤 디바이스를 통해 접속하는지 4개의 서브 속성으로 구성되어있으며, DA는 감성 정보(EmAV, Emotion Attribute Value), 생체 정보(BAV, Biology Attribute Value), 인프라 정보(IAV, Infra Attribute Value), 환경 정보(EnAV, Environment Attribute Value)의 속성 값을 갖고 있다. 접근제어 속성은 자원에 대한 사용자의 권리를 표현하는 데 사용되며, 시스템과 서비스에 따라 유연하게 설정될 수 있지만 본 논문에서는 접근제어 속성을 읽기 전용(RO, Read-Only), 읽고 쓰기(RW, Read-Write)의 두 가지 기본 값으로 정한다.

따라서, 환자의 병력사항 기록 F에 대해 접근을 제어하는 다음의 정책을 설정할 수 있다.

T_RO={{RescueWorker OR Doctor} AND {Emergency OR Daily} AND {Mountain OR Hospital} AND {PC OR Pad OR Mobilephone} AND {DangerPlace OR NonMove}} AND {Shock OR LowBlodPressure OR LowTemperature} AND RO.

T_RW={{Doctor AND Daily AND Hospital AND PC} AND Examination} AND BioInfo AND RW.

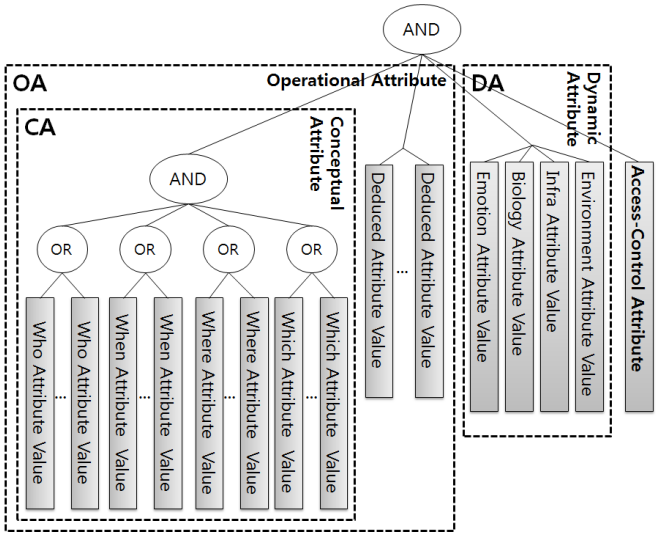

Fig. 7. Access Structure Tree Configured for Multi-Attribute Access Control Policy

정책 T_RO는 병력사항 F에 읽기 전용 모드로 동작할 수 있는 상황조건하에서 정의한다. 구조대원이 위치센서를 통해 환자가 산에 있고 위치센서의 변화가 없는 시간을 고려해 고립된 시간 데이터를 확인할 수 있다. 또한 위치센서가 표시한 지점이 사고 다발지역 또는 잦은 안개현상 지역 등의 위험지역 여부를 판단하고, 환자의 스마트 폰 단말기에 가해진 충격 데이터 등을 수집하여 환자의 위험여부를 판단한다. 즉, 일정 시간 동안 움직임이 없으며 충격을 받은 상황에서 낙상 환자가 발생함을 추론할 수 있기 때문에 구조대원이 환자의 병력사항에 접근했을 때 접근제어정책 T-RO에 부합하여 환자의 개인정보와 병력사항이 복호화된다. 구조대원은 환자의 병력사항을 읽고 그에 따른 응급처치를 할 수 있으나 그 정보를 수정할 수는 없다. 정책 T_RO는 Fig. 8과 같이 접근트리 형태로 도식화할 수 있다.

정책 T_RW는 병력사항 F의 읽기 및 쓰기 모드로 동작할 수 있는 상황조건하에서 정의한다. 환자의 질병과 낙상 상황을 고려하여 인접 전문병원으로 후송되면 새로운 접근자인 의사는 병력사항을 복호화하여 읽을 수 있을 뿐만 아니라 치료 상황에 따른 수정이 가능하다. 정책 T_RW를 투리 형태로 도식화하면 Fig. 9와 같다.

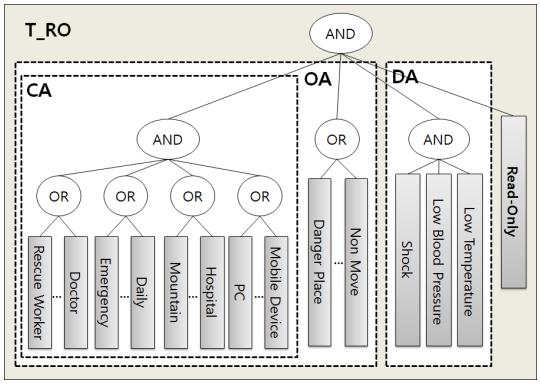

Fig. 8. T_RO Access-Tree

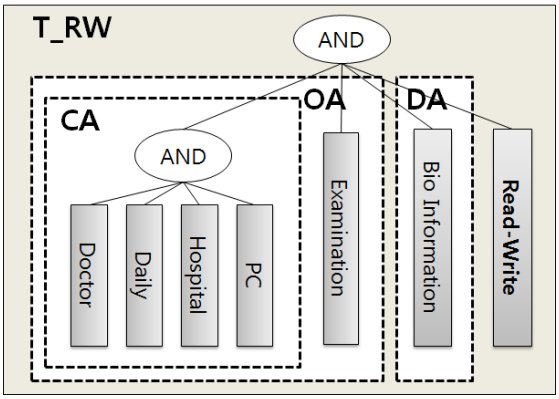

Fig. 9. T_RW Access-Tree

병력사항 등의 자원 F에 대해 사용자는 Certification Center의 System initialization에서 두 대칭키 Kr(Key-reading)과 Kw(Key-writing)를 무작위로 생성한다. 본 논문의 시나리오에 따라 T_RO 권한을 가질 수 있는 사용자는 키 Kr을 소유해야 하며, T_RO 권한을 갖고자 한다면 두 가지 키 Kr, Kw를 모두 소유해야 한다. Certification Center에서는 사용자로부터 제공된 접근제어 정책 T_RO와 T_RW에 따라 CP-ABE의 암호화 함수를 이용하여 Kr과 Kw를 암호화한다.

F에 대한 접근이 이루어지는 방식은 다음과 같다. 사용자가 직접 클라우드 Storage Center로부터 암호화된 파일, 즉 병력사항을 다운로드 해서 접근하는 것은 불가능하다. Context Collector에서 현재의 상황인 C를 수집하여 Certification Center의 Key Generation에 보내면, 수신된 상황에 따라, Key Generation는 복호키 CK를 생성하고 사용자의 클라이언트의 암호 해독 장치에 CK를 보낸다.

C는 접근제어 정책 T_RO에 일치하므로 대칭키 Kr은 암호문을 해독하기 위해 사용하고 F를 읽을 수 있다. 그러나 T_RW와는 일치하지 않아 암호문을 해독할 수 없고 쓰기권한을 가질 수 없다.

Table 1. Comparison with the Existing Studies

	기존 연구[4]	기존 연구[5]	본 연구
정보수집의 정확성	사용자의 단순 센싱 데이터로 상황을 인지하여 정확성이 상대적으로 낮음	사용자 센싱 데이터로부터 파생된 상황을 추론하여 정확성을 더욱 높일 수 있음	사용자의 동적인 속성을 포함하는 센싱 데이터로부터 상황을 추론하여 정확성이 매우 높음
상황속성의 확장성	1차원 접근을 통해 사용자의 정적인 상황 속성(who, when, where, which) 중심	개념적 속성(Location, Identity, Time, Activity)에서 파생되는 운영적 속성을 구분하여 2차원 상황 속성으로 확장	사용자의 동적상황 속성(감성. 생체, 인프라, 환경)을 반영함으로써 다차원 상황 속성으로 확장
접근제어의 유연성	정적데이터 중심의 상황을 기반으로 한 데이터의 변화에 따라 본 연구에 비해 유연한 접근제어가 불가능	수집된 센싱 정보에서 파생된 데이터를 통한 상황을 포함하여 그 범위가 넓어졌으며, 상황에 따른 접근제어 유연성을 높일 수 있으나 논문에서는 접근제어에 대해 다루지 않고 있음	동적상황 속성을 포함하여 상황인지의 가능 범위를 더욱 넓혔으며 지속적으로 변화하는 정보를 이용한 접근제어의 유연성은 매우 높음
접근정책의 민감도	4가지의 상황 속성을 기준으로 접근정책을 만족시켜야 함으로 본 연구에 비교하여 민감도가 낮음	2차원 속성의 상황을 통한 접근정책의 수립은 민감도를 높일 수 있으나 논문에서는 접근정책에 대해 다루지 않고 있음	개념적 속성, 운영적 속성, 동적 속성을 모두 만족시켜야 하는 접근제어정책에 따라 민감도가 높음

C= {{Doctor AND Daily AND Hospital AND PC} AND Examination} AND BioInfo
CK= Key(MK, C)

4. 비교 및 분석

본 논문에서는 동적인 상황을 고려한 접근제어 정책을 IoT 센서퓨전 환경에 적합하도록 설계하였다. 따라서 기존의 연구와 비교해 데이터의 다양성 확보 및 정확한 정보의 수집이 가능하고, 기존 상황 속성의 확장이 가능하다는 장점을 갖는다. 또한, 세밀화된(fine-grained) 접근제어가 가능하고, 확장된 Access Tree 기반의 복호화 정책을 통한 민감하고 개인화된 정보의 맞춤형 안전한 IoT 서비스가 가능하다. 기존 연구와 같이 CP-ABE 방식을 기반으로 하지만 이전에는 다루어지지 않았던 상황의 동적인 속성을 포함시켜 접근제어 정책의 효율성을 높였다.

상황 정보를 이용한 접근제어 정책을 위해 기존 연구[4]에서는 사용자의 Who, When, Where, Which의 단순 센싱 정보를 이용해 복호화키를 생성하고, 기존 연구[5]에서는 센싱 정보로부터 파생된 정보를 추가하여 복호화키를 생성한다. 예를 들어, 센싱된 위치 값을 통해 사용자가 위험한 지역에 있는지의 여부 등을 확인할 수 있다. 본 연구에서는 기존 연구에서 이용되던 센싱 정보에서 감성, 생체, 인프라, 환경 등의 동적인 속성 값을 포함시켜 복호화키로 이용함으로써 상황 정보 수집의 정확성과 확장성, 접근제어의 유연성, 그리고 민감도를 높일 수 있다(Table 1).

5. 결 론

본 논문은 CP-ABE를 기반으로 IoT 센서퓨전 환경에서 사용자의 접근제어 방식을 제안했다. 이는 기존에는 다루어지지 않던 동적인 상황의 속성을 키 생성 과정에 포함시켜 접근 권한관리를 유연하게 하고 시스템의 확장성을 높임과 동시에 정확한 정보의 수집을 가능하게 하였다.

향후 과제로서 대칭키 방식을 함께 적용한 하이브리드 CP-ABE를 채택함으로써 보안의 효율성을 높이고자 한다. 또한, 상황인식 보안 플랫폼 구축을 위해 요구되는 센서퓨전, 즉 Multi-sensor에 의한 상황 정보 추론과정을 통해 민감한 상황 정보를 안전하게 수집, 전송 및 처리할 수 있는 Context Security Layer 구성이 필요하다. IoT 보안 계층 구조를 명확하게 규명하고 나아가 센서퓨전을 통해 수집되는 정보의 계량적 정확성을 검토할 것이다.

References

[1] Hewlett-Packard, “Internet of Things Research Study,” HP Report, 2014.
[2] ナターシャ·ロマス, “IoT企業はプライバシーとセキュリティーに

最優先で取り組め―FTC委員長がCES講演で強く警告", [Internet] http://jp.techcrunch.com/2015/01/13/20150108ftc-iot-privacy-warning/, 2015.
[3] 하수욱, 이강찬, "빅데이터 상호운용성 프레임워크와 JTC 1 빅데이터 참조 아키텍처 표준화", 미국국립표준연구소(NIST), 2015.
[4] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakpoulos, "Context Aware Computing for The Internet of Things: A Survey," *IEEE Communications Surveys & Tutorials*, Vol.16, No.1, 2014.
[5] Kavin karimi, "The Role of Sensor Fusion and Remote Emotive Computing(REC) in the Internet of Things," freescale, 2013.
[6] S. Osbom, R. Sandhu, and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and System Security*, Vol.3, No.2, 2000.
[7] H. Lindqvist, "Mandatory Access Control", springer, 2011.
[8] D. Ferraiolo, DR Kuhn, and R Chandramouli, "Role-based access control," ArtechHouse, 2003.
[9] Ling Yu, Bo Chen, Bei Huang, and Ning Wang., "CONTEXT-AWARE ACCESS CONTROL FOR RESOURCES IN THE UBIQUITOUS LEARNING SYSTEM USING CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION," PACIS, 2013.
[10] Zhou Ke, Li Chunhua, and Niu Zhongyin, "The storage security access control in large data center," *China Computer Federation Communication*, Vol.8, No.10, 2012.
[11] John Bethencourt, AmitSahai, and Brent Waters, "Cipher-text-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 2007
[12] 이승훈, "Trillion 센서 IoT 시대 열고 있다", LGERI레포트, 2014.
[13] Yoosoo Oh and Woontack Woo, "Context Integration System by Fusing Heterogeneous Sensors in a Mobile Phone" The Human Computer Interaction Society of Korea, 2010.
[14] AJ シプリー, "「モノのインターネット」におけるセキュリティ接續された未來に向けて過去から學ぶこと", 2013.
[15] Eric Openshaw, Craig Wigginton, John Hagel, John Seely Brown, Maggie Wooll, Preeta Banerjee Ichiro Nakayama, Toshifumi Kusunoki, Eitaro Matsunaga, Keiko Kamata, and Shintaro Imoto, "The Internet of Things Ecosystem-IoTに組み込まれたデバイスからビジネス価値を引き出す (日本語譯版)," Thought Leader's News Vol.4 Deloitte, 2014.
[16] FTC Staff Report, "internet of things privacy and security in a connected world," FTC, 2015.
[17] Mobile Working Group, "Security Guidance for Early Adopters of the Internet of Things(IoT)," Cloud Security Alliance, 2015.
[18] 藤井 秀之, "IoT時代に求められるプライバシー保護・セキュリティ對策～米國FTCによるIoT報告書を中心に～", http://www.icr. co.jp/newsletter/law/2015/law201502.html, 2015.
[19] カスペルスキー, "注目される「IoT (モノのインターネット) 」、專門家がセキュリティリスクを指摘", http://www.excite.co.jp/News/it_g/20150215/Harbor_business_25271.html, 2015.
[20] 笹原英司, "IoT標準化にみるビッグデータ連携と階層型のセキュリティとは？", http://www.itmedia.co.jp/enterprise/articles/1506/10/news036_3.html, 2015.

송 유 진

e-mail : song@dongguk.ac.kr
1982년 한국항공대학교(학사)
1987년 경북대학교(석사)
1995년 일본 Tokyo Institute of Technology (박사)
1988년～1996년 한국전자통신연구원 선임연구원
2003년～2005년 미국 University of North Carolina at Charlotte 연구교수
2006년～2006년 일본 정보보호대학원대학 객원교수
1996년～현 재 동국대학교 경영학부 교수
1998년～현 재 한국정보보호학회 부회장
2006년～현 재 국제 e-비즈니스학회 상임이사
2009년～현 재 한국인터넷방송통신학회 이사
2010년～현 재 한국인터넷전자상거래학회 이사
2006년～현 재 한국사이버테러정보전학회 이사
관심분야 : IoT/CPS Security and Privacy Protection, Secret Sharing, Cloud Computing, Context Aware Security 등

서 아 리 아

e-mail : seoaria@gmail.com
2011년 동국대학교 정보경영학과(학사)
2013년 동국대학교 테크노경영협동과정 정보기술전공(석사)
2012년～2014년 실감미디어 성과확산사업단 연구원
2014년～현 재 동국대학교 테크노경영협동과정 정보기술전공 박사과정
관심분야 : Ubiquitous, USN, Context-aware 등

이 재 규

e-mail : jaekyulee@dongguk.ac.kr
2015년 동국대학교 정보경영학과(학사)
2015년～현 재 동국대학교 테크노경영협동과정 정보기술전공 석사과정
관심분야 : USN, Context-aware 등

김 의 창

e-mail : kimyc@dongguk.ac.kr

1983년 동국대학교 수학과(학사)

1986년 동국대학교 컴퓨터공학과(석사)

1993년 동국대학교 컴퓨터공학과(박사)

1998년 University of Illinois 컴퓨터공학과 (Post-Doc.)

1991년～현 재 동국대학교 경영학부 교수

2000년～2003년 (주)카인정보시스템 대표

2005년～2006년 동국대학교 학생처장

2005년～현 재 한국디지털정책학회 상임이사

2008년～2009년 동국대학교 학생경력 개발원장

2009년～2010년 동국대학교 학사지원 본부장

2010년～현 재 한국인터넷전자상거래학회 상임이사

2012년～현 재 동국대학교 전자상거래 연구소장

2014년～현 재 동국대학교 인재개발처장

2015년～현 재 국제e-비즈니스학회 회장

관심분야 : Ubiquitous, USN, Big data, Distributed processing system 등