情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

Cloud Computing에서의 IoT(Internet of Things) 보안 동향

손 태 식*, 고 종 빈**

요 약

클라우드 컴퓨팅과 IoT 기술은 미래 ICT(Information Communication Technologies)의 핵심이 되는 기술이다. 급속한 ICT 기술의 발전과 함께 우리 주변의 모든 사물을 연결하고 주변의 다양한 정보를 습득하는 IoT 인프라에서 발생하는 데이터의 처리와 활용을 위해서도 클라우드 컴퓨팅 환경은 밀접히 고려되어야 할 것이다. 하지만 이러한 두 기술 모두 각각의 보안 취약점이 존재하고, 미래에 두 기술이 병합될 때 추가적인 보안위협이 발생될 수 있다. 본 논문에서는 클라우드 컴퓨팅과 IoT 기술 및 보안 동향에 대해 알아보고 두 기술의 접목 시 발생하게 될 보안 위협요소를 식별하여 이에 대한 대응방안에 대해 검토하여 보고자 한다.

Ⅰ. 서 론

클라우드 컴퓨팅(Cloud Computing)은 컴퓨팅 환경뿐만 아니라 관련 산업의 패러다임을 변화시키고 있는 ICT(Information and Communication Technologies) 분야의 주요 이슈 기술이다. 또한 사람을 중심으로 언제 어디서 통신을 제공하는 환경에서 주변의 모든 사물에 통신 기술을 접목시키는 IoT(Internet of Things) 패러다임이 미래 인터넷 기술로써 많은 조명을 받고 있다. 궁극적으로 IoT는 클라우드 컴퓨팅과 접목되어 활용 분야를 확장시킬 것이며, 이를 통한 진정한 유비쿼터스 컴퓨팅 시대로의 도약이 멀지 않았다고 볼 수 있다.

특히 페타·엑사(Peta·Exa) 수준의 데이터로 일컬어지는 빅 데이터의 시대에 있어 클라우드 컴퓨팅을 통한 활용이 화두로 등장하고 있지만 이러한 유비쿼터스 컴퓨팅의 실현을 위해 선결해야할 문제들이 다방면에서 지적되고 있다. 그중에서 가장 큰 문제는 보안 문제의 해결이라고 할 수 있을 것이다. 모든 사물이 인터넷을 통하여 연결되어 있고, 여기서 생성된 된 빅 데이터들을 클라우드 서비스를 이용해 재가공하여 사용자를 위한 가치 있는 정보로 활용하기 위해서는 사용자의 프라이버시(Privacy)의 보호를 비롯한 여러 보안 문제점들에 대응책이 필수적으로 적용되어야 할 것이다.

본 논문에서는 현재 이슈가 되고 있는 클라우드 컴퓨팅과 IoT 기술 동향 및 보안 현황과, 클라우드 컴퓨팅 환경에서의 IoT 관련 융합 보안의 필요성에 관하여 고찰해 본다.

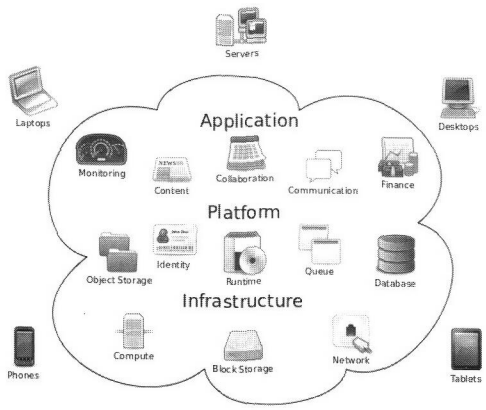
Ⅱ. 클라우드 컴퓨팅 동향[1]

2.1 클라우드 컴퓨팅의 정의

클라우드 컴퓨팅이란 "규모의 경제에 입각한 대규모 분산 컴퓨팅 패러다임; 거대한 IT 자원들(파워, 스토리지, 플랫폼, 서비스 등)을 추상화, 가상화, 동적 확장이 가능한 체계이며 인터넷을 통해 사용자가 필요한 만큼 제공하는 컴퓨팅 서비스 환경"으로 정의 할 수 있다. 즉, 사용자가 인터넷을 통하여 컴퓨팅 능력을 빌려 쓰고, 이에 대한 사용료를 지불하는 서비스로 IT 자원을 사회 간접재 형태로 사용하는 새로운 패러다임으로 볼 수 있다. IEEE과 IBM을 비롯한 주요 기관 및 기업에서 정의하는 클라우드 컴퓨팅의 개념은 다음과 같다.

- IEEE : 정보가 인터넷 상의 서버에 영구적으로 저

* 아주대학교 정보컴퓨터공학부 조교수 (tsshon@ajou,ac,kr)
** 아주대학교 대학원 컴퓨터공학과 박사과정 (nitefly7@gmail.com)



〔그림 1〕 클라우드 컴퓨팅 개념도

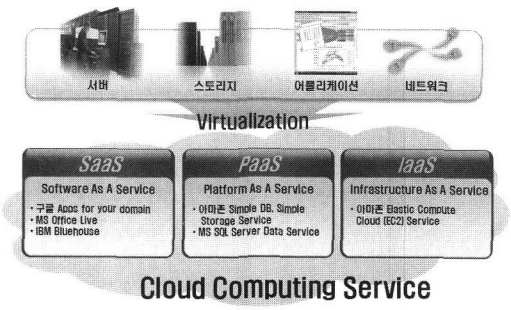
장되고 데스크 탑이나 노트북, 휴대용 기기 등의 클라이언트에 일시적으로 보관될 수 있는 컴퓨팅 스타일

- NIST : 표준화된 IT 기반 기능들이 IP를 통해 제공되며, 언제나 접근이 허용되고, 수요의 변화에 따라 가변적이며, 사용량이나 광고를 기반한 과금 모형을 제공하며, 웹 혹은 프로그램적인 인터페이스를 제공하는 형태
- IBM : 웹 기반 애플리케이션을 활용하여 대용량 데이터베이스를 인터넷 가상공간에서 분산 처리하고 이 데이터를 데스크톱 PC, 휴대 전화, 노트북 PC, PDA 등 다양한 단말기에 불러오거나 가공할 수 있게 하는 환경
- 포레스터 리서치 : 표준화된 IT 기반 기능들이 IP를 통해 제공되며, 언제나 접근이 허용되고, 수요의 변화에 따라 가변적이며, 사용량이나 광고를 기반한 과금 모형을 제공하며, 웹 혹은 프로그램적인 인터페이스를 제공하는 형태
- 위키피디아 : 인터넷에 기반한 개발과 컴퓨터 기술의 활용을 말하는 것으로 인터넷을 통해서 동적으로 규모화 가능한 가상적 자원들이 제공되는 컴퓨팅

2.2 클라우드 컴퓨팅 서비스 모델

미국의 국가 표준기술 연구소인 NIST(National Institute of Standards and Technology)는 클라우드 컴퓨팅의 서비스 모델을 크게 세 가지 모델로 정의하고 있다.

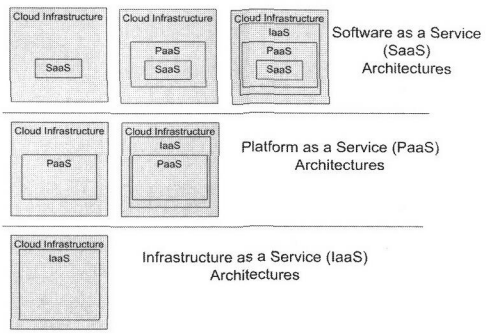
- SaaS(Software as a Service) : 메모리·CPU 등 논리적으로 가상화된 컴퓨팅 자원이나 이미지·동영상 등의 자료를 저장할 수 있는 스토리지 자원 등 서버 인프라를 인터넷을 통해 인터넷을 통해 제공하는 서비스



〔그림 2〕 클라우드 컴퓨팅 서비스 모델

- PaaS(Platform as a Service) : 컴파일 언어·웹 프로그램·제작 툴·DB 인터페이스·과금 모듈·사용자 관리 모듈 등 사용자가 소프트웨어를 개발할 수 있는 토대를 제공해 주는 서비스 모델
- IaaS(Infrastructure as a Service) : 클라우드 컴퓨팅 서비스 사업자가 인터넷을 통해 소프트웨어를 제공하고, 사용자가 원격 접속해서 이메일·ERP·CRM 등 다양한 애플리케이션을 활용하는 클라우드 컴퓨팅 최상위 계층에 해당하는 모델

인터넷을 통하여 사용자에게 서비스를 제공하는 것을 목표로 갖는다는 점은 이 세 가지 서비스 모델의 공통점으로 유사성을 갖는다. 하지만 각각의 서비스 모델은 서비스를 제공받는 대상에 따라 구분할 수 있다. 각각의 서비스 모델은 독자적인 구조를 가질 수도 있으나, 보통은 IaaS부터 PaaS, SaaS까지 연계되어진 형태로



〔그림 3〕 클라우드 컴퓨팅 서비스 모델별 아키텍쳐

시스템을 구성한다. IaaS 서비스가 기본적인 아키텍처이며, PaaS 서비스는 IaaS 서비스 기반 또는 독자적인 아키텍처 모습을 가지고 있다. SaaS는 PaaS 서비스 기반 또는 독자적인 아키텍처를 갖는다. 물론 세부적인 아키텍처는 각 서비스의 종류에 따라 달라질 수도 있다.

최근에는 위의 세 가지 서비스 모델 외에도 클라우드 컴퓨팅 판매자들이 자사의 클라우드 컴퓨팅 서비스를 차별화하기 위해 DaaS(Datacenter as a Service), BaaS (Business as a Service) 등을 강조하면서 이른바 XaaS (X as a Service) 형태로 새로운 비즈니스 모델을 만들어 나가고 있다.

2.3 국내외 클라우드 컴퓨팅 관련 산업 동향

클라우드 컴퓨팅 기반 서비스를 제공하기 위해서 선행되어야 하는 것은 하드웨어 장비 인프라가 갖춰져 있는 데이터 센터 구축이다. 그리고 주문형 서비스, 동적 자원할당, 데이터 동기화, 서비스 과금체계 등 클라우드의 특징을 충족하기 위한 다양한 기술 솔루션이 요구된다. 클라우드 컴퓨팅 관련 산업은 이러한 요구사항들을 기반으로 하여 위에서 나열한 서비스 모델별 특징에 부합하는 다양한 서비스를 제공하고 있다.

○ 국외 관련 산업 동향

- 아마존(Amazon) : 2006년부터 전자상거래용 대규모 데이터센터 기반으로 IaaS 서비스 (AWS : S3, EC2)를 제공 중이며, PaaS 서비스까지 확대하고 있고 2009년부터 싱가포르에 클라우드 아시아 센터를 출범, 일본 데이터센터 구축(`11.3월) 및 한국지사 설립(`11.7월) 등 아시아 클라우드 시장 선점에 주력
- 구글(Google) : 소프트웨어 개발 능력과 웹 기반의 두터운 고객층을 기반으로 플랫폼 및 개인·기업용 클라우드 서비스 중심으로 시장 공략이며, 구글 Apps, 구글 Apps Engine 등 Paas 및 SaaS를 아우르는 다양한 클라우드 서비스 제공 중
- MS(Microsoft) : 기존 PC용 소프트웨어(윈도우즈, MS 오피스 등) 경쟁력을 바탕으로 Public 및 Private 클라우드를 아우르는 통합 클라우드 솔루션 제공사업을 추진 중이며, 특히 MS Azure를 중심으로 한 PaaS 영역에 집중하여 MS SW의 글로벌 클라우드 플랫폼 化와 윈도우 모바일 폰과 연계한 모바일 클라우드 서비스 시장 본격 공략 중
- 애플(Apple) : 단말(아이폰, 아이패드, 아이팟, 애플 TV, 맥북 등) 및 콘텐츠 경쟁력을 활용하여 모바일 클라우드 기반의 개인화 서비스인 iCloud 서비스 출시(`11.10월)하였으며, 자사의 모든 단말 간 자동 동기화 및 온라인 저장공간과 스트리밍 서비스 등을 제공하는 모바일 클라우드 서비스에 주력
- 버라이존(Verizon) : 2009년부터 CaaS(가상인프라 서비스)를 비롯하여 스토리지(Cloud Storage와 백업 서비스를 제공 중이며, 환자의 진료기록을 온라인상에서 제공하는 SaaS 형태의 HIE(Health Information Exchange) 서비스를 제공 중
- 델(Dell) : 퍼블릭 클라우드 서비스 출시 및 고객의 프라이빗 클라우드 구축을 위한 컨설팅 서비스 제공, VM웨어의 커넥터 SW를 이용한 하이브리드 클라우드 서비스 출시 예정
- IBM : 클라우드 애플리케이션을 통합해주는 SaaS 형태의 솔루션 제공업체인 캐스트아이런 인수, 보안과 관리 등 클라우드 요소를 기반으로 원격 및 로컬 서비스를 하나로 통합해주는 하이브리드 클라우드 솔루션 공개
- 오라클(Oracle) : CRM SaaS 신규 버전인'CRM On-Demand R19' 공개, ERP 및 HRM(인적자원관리) 등도 SaaS 형태로 제공

○ 국내 관련 산업 동향

- KT : 2010. 6월 개인 및 기업 대상의 Public 클라우드 서비스 'u-클라우드'를 출시하였으며, 서비스의 범위를 스토리지에서 컴퓨팅 파워, 백업, 데이터베이스 등으로 확대 중. 그리고 천안에 국내 최초로 고집적·고효율·무인 자동화된 클라우드 데이터센터를 구축하였으며, 기존 IDC를 CDC(클라우드 데이터센터)로 전환 추진 중
- SK텔레콤 : 2011. 1월 기업 대상의 Public 클라우드 서비스 'T 클라우드 비즈'를 출시하여 클라우드 호스팅, VDI 및 스토리지 서비스 등을 제공 중이며, 다양한 IT기기간 콘텐츠를 공유하고 통합관리할 수 있는 Personal 클라우드 서비스(PCC) 준비 중
- 삼성SDS : 2009년부터 클라우드 서비스 및 기술개발에 투자하고 있으며, 최근 자사의 모든 정보기기간 동기화 및 통합관리기능을 제공하는 'sCloud' 서비스 준비 중

- NHN : 무료 비즈니스 모델을 경쟁력으로 2009. 3월 클라우드 스토리지 서비스 'N-드라이브'를 출시, 2010. 9월 웹오피스인 네이버 워드를 출시하는 등 Personal 클라우드 서비스에 주력하고 있으며, 향후 카페·블로그·SNS 등과 연동한 개인화 서비스를 통해 이용자의 Lock-In 효과 극대화전략 추진 중
- 다음(Daum) : 클라우드 환경에서의 시맨틱 검색 서비스 개발 및 기존 서비스와의 클라우드 연동을 전략적으로 추진 중으로, 2011년 3월 클라우드 스토리지 서비스 출시와 함께 각종 개인 서비스와 연동하여 다음 사용자를 유지 및 확보하겠다는 전략

Ⅲ. IoT(Internet of Things) 동향[2]

3.1 IoT의 정의

IoT(Internet of Things)는 2005년 ITU의 SPU(Strategic Planning Unit)의 보고서를 통해 처음으로 개념이 소개되었다. "기존의 통신 환경에서 사람과 사물, 사물과 사물간의 통신이 새로운 통신의 유형으로 등장할 것이라는 것"이 보고서에서의 IoT에 대한 정의이다. 현재 일반적인 IoT의 정의는 "사람의 관여 없이 사물 간에 이루어지는 통신"을 의미하여, 사람은 사물이 생성하는 데이터의 입력에 관여할 수 없고 선택적으로 출력물만 획득할 수 있는 통신을 의미한다. ITU 뿐만 아니라 유럽의 ETSI나 3GPP2와 같은 표준과 기구에서도 비슷한 개념의 M2M(Machine to Machine Communication) 혹은 MTC(Machine Type Communications)를 정의하고 표준화를 추진 중이다. 우리나라는 IoT를 사물지능통신 혹은 사물통신이란 단어로 정의하고 있으며, 궁극적으로 IoT, M2M, MTC, 사물지능통신은 모두 같은 개념으로 볼 수 있다.

IoT 패러다임의 실현을 위해서는 일상생활에서 접하는 모든 사물이 각각의 아이덴티티(Identity)를 가지며, 상호를 식별할 수 있고 이를 네트워크를 통해 전송하고 데이터를 수신하여 처리하는 컴퓨팅 능력을 지니고 있어야 한다. 사물에 대한 식별은 RFID(Radio Frequency Identification)을 통해 수행 하며, 각각의 사물이 정보를 수집하는 것은 센서 기술을 이용하여 각 사물의 대상에 대한 상태 변화를 감지 할 수 있다. 이를 통해 주변 정보의 변화를 감지하고, 네트워크에 연결되어 다양한 정보를 주고받는 네트워크를 형성하게 될 것이다.

3.2 국내외 동향

○ 미국
- 미국의 NIC 보고서는 IoT와 관련된 기술개발 로드맵을 정의하였고, IoT는 RFID에서 출발하여 센서를 활용하는 기술로 발전하여 향후 사람들의 위치정보와 모든 사물들이 네트워크에 연결되는 방향으로 발전할 것을 예측하고 있음
- NIST를 중심으로 스마트그리드(Smart Grid)의 개발 및 확산 주도 및 이동통신의 새로운 서비스 모델로 M2M에 대해 주목하고 있음

○ 유럽연합(EU)
- 모든 사물들이 네트워크에 연결되어 수많은 트래픽을 생성하는 환경에 대응하여 미래 인터넷(Future Internet)의 필요성을 인지하고 미래 인터넷을 구성하는 중요한 기반기술로 IoT와 IoS(Internet of Service)를 고려하고 있음
- 2008년 11월 IoT의 기술 개발 및 보급에 앞서 IoT가 보급됨으로써 발생할 수 있는 개인의 프라이버시 문제를 인지하고, 이에 대한 투자를 결정해 제7차 프레임워크 프로그램(FP7)에서 532억 유로를 투자하여 연구를 진행 중
- FP7의 하나인 CASAGRAS(Coordination And Support Action for Global RFID-related Activities and Standardization) 프로젝트에서는 "Internet of Things"에 대하여 관련 연구를 2008년부터 진행하였으며, 그 후속으로 CASAGRAS II 프로젝트를 추진 중에 있음
- CERP-IoT(Cluster of European Research Projects on the Internet of Things) 프로젝트를 통해 IoT를 실현하기 위한 비전과 위험요소를 분석

○ 일본
- 2006년에 발표한 "IT 신 개혁 전략"에 따라 모든 사람이 IT 기술이 가져오는 이익을 누릴 수 있는 유비쿼터스 네트워크 사회의 구현을 목표로 연구개발을 추진 중
- 이미 시장에 활성화 된 RFID 기술을 토대로 센서 네트워크 등을 접목시켜 IoT의 실질적 실현에 무게를 두고 있음

- 현재 바코드 시장을 RFID로 대체하는 작업이 진행 중이며, RFID 시장은 매년 10%씩 증가할 것으로 전망
- 2009년 METI(Ministry of Economy, Trade and Industry)가 유럽 집행위원회의 DG INFSO(Information Society and Media Directorates-General)와 MoU를 체결하고 RFID, 무선 센서 네트워크 및 IoT의 분야의 협력을 진행 중

○ 한국

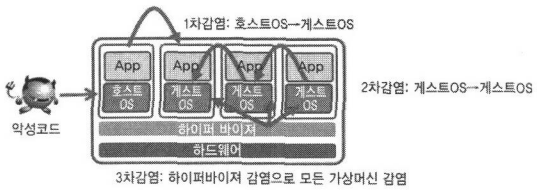
- 2005년부터 USN(Ubiquitous Sensor Network) 시범 사업, u-City 사업 등을 통해 지역별 서비스 인프라를 구축해 오고 있으며, 국가 인프라로 기상관측망 및 수질 측정망을 구축·운영 중
- 사물지능통신을 u-City, u-Health, u-교통, u-환경 등 사회 안전, 재난·재해방지, 에너지 절감, CO2 감축에 기여할 수 있는 지능형 그린 IT 서비스 확산에 필수적인 인프라로 정의하고 방송통신위원회 미래 10대 서비스의 하나로 선정
- 2009년 방송통신위원회에서 "사물통신기반 구축 기본계획"을 발표하였으며 사물통신 기반 구축, 서비스 활성화, 기술 개발, 확산환경 조성의 4대 분야에 대한 세부추진과제를 포함하고 있음

Ⅳ. 클라우드 컴퓨팅과 IoT에서의 보안

4.1 클라우드 컴퓨팅 보안

4.1.1. 클라우드 컴퓨팅 보안 취약점[3]

2011년 10월 한국인터넷진흥원(KISA)에서 발간된 "클라우드 서비스 정보보호 안내서"에 따르면 클라우드 서비스는 모든 연산 및 데이터 처리가 클라우드 서버에서 이루어지므로 기본적으로 사용자가 소유한 정보의 관리를 서비스 제공자에게 위탁한다. 그리고 사용자별로 할당된 자원은 논리적으로는 독립적이지만 물리적으로 동일한 자원을 공유하는 특성을 지니기 때문에 클라우드 서비스의 보안위협은 주체와 관점에 따라 다양한 방법으로 분류될 수 있다. NIST, 가트너(Gartner) 등 주요 기관에서 제시하는 클라우드 컴퓨팅의 대표적인 보안 위협 분석사례에서 핵심 보안요소를 도출한 것은 다음과 같다.



〔그림 4〕 가상화 취약점에 따른 악성코드 감염

○ 가상화 취약점(악성코드 및 서비스 가용성 침해

- 클라우드 서비스는 시스템 자원을 통합/재분배 하여 제공하는 인프라 계층의 특징으로 인해 가상화 시스템의 취약점을 상속하므로 악성코드 감염, 서비스 장애 등 신규 취약성에 노출될 가능성이 높음
- 하이퍼바이저(Hypervisor)를 통해 동시에 복수의 가상머신을 구동하는 구조이므로, 하이퍼바이저를 통해 악성코드 확산 가능

○ 정보위탁(소유와 관리 분리)에 따른 정보 유출 위협

- 사용자의 정보의 저장 및 관리를 원격의 클라우드 서버에서 담당하기 때문에 내부자 또는 악의적인 공격자에 의해 유출될 가능성이 높음
- 사용자의 정보가 동의 없이 복사, 이동, 수정되어도 실제 사용자가 이것을 알 방법이 없음

○ 자원 공유 및 집중화에 따른 서비스 장애

- 클라우드 서비스를 이용하는 사용자들은 클라우드 서비스 제공자의 물리자원을 공유하므로 물리자원에 장애가 생길경우 공유하는 사용자 모두의 서비스가 중단될 수 있음
- 서비스 중단에 대한 원인 및 대책 등에 대한 상황을 사용자가 바로 알 수 없으므로, 민감하거나 긴급성을 요구하는 정보를 클라우드 서비스를 통해 이용하는 것에 대한 불신이 생길 수 있음

○ 단말 다양성에 따른 정보 유출

- 사용자의 선택에 따라 PC, 스마트폰, 태블릿PC, 스마트TV 등 다양한 형태의 단말이 클라우드 서비스에 접속하게 되므로 각각의 단말이 지니는 고유의 보안위협이 클라우드 서비스에 상속됨

○ 분산 처리에 따른 보안 적용의 어려움

- 대용량의 데이터가 분산파일 시스템을 통해 많은 서버들에 분산 저장·관리 되므로 데이터 암호화,

인증, 접근제어 등의 보안 기술 구현에 어려움이 증가함
- 관리시스템이 노출될 경우 악의적인 해킹, 이용자의 데이터 손실 및 유출 등의 보안위협이 존재

○ 법규 및 규제의 문제
- 서버가 분산배치 될 수 있는 클라우드 서비스의 특성 상 기존의 법규 및 규제로 모든 상황을 통제할 수 없음
- 특히 국외의 서버를 이용하는 경우 국내법 적용을 통한 통제가 매우 어려움

4.1.2. 클라우드 컴퓨팅 보안 대책[5]

클라우드 컴퓨팅에 대한 보안은 크게 사용자 관점과 서비스 제공자 관점으로 나눌 수 있다.

○ 사용자 관점의 보안 대책

먼저 개인의 정보를 클라우드 서비스 판매자에게 위탁하는 점을 충분히 인지하고 있어야 한다. 따라서 사용자 자신의 클라우드 서비스 사용에 대한 필요성에 대해 충분히 타진해볼 필요가 있으며, 때에 따라선 클라우드 서비스와 자신의 컴퓨팅 환경을 공존하여 사용할 것을 고려할 필요가 있다. 또한 공개된 클라우드 서비스 판매자의 정보보호 대책, 안정성, 감사 및 정보 공개 여부, 피해 복구 방안 등의 항목을 참조하여 클라우드 서비스 제공자를 선정하는 것이 바람직하다.

○ 클라우드 서비스 제공자 관점의 보안 대책

위에서 서술한 바와 같이 사용자는 자신의 정보를 클라우드 서비스 제공자에게 위탁해야 하므로, 이러한 사실 자체가 위험성을 감수해야한다는 부담이 생기게 된다. 클라우드 서비스 제공자는 자사의 경쟁력 강화 차원뿐만 아니라 기본적인 클라우드 서비스의 보편화를 위해서라도 자사 서비스의 보안성을 확보하고 이를 사용자에게 적극적으로 공시할 의무가 있다.

클라우드 서비스 제공자가 기본적으로 제공해야할 보안 대책으로는 클라우드 데이터 센터에 대한 공격, 사고에 대한 예방, 감시 및 사후 복구 대책을 전담할 조직을 운영해야 하며 이에 따른 결과를 항시 사용자에게 제공해야한다. 또한, 허가되지 않은 사용자의 접근 및 데이터 조작에 대한 강력한 인증 및 접근제어 기법의 적용이 필수적이다. 더불어 가상화 환경을 사용하므로 각 사용자간의 명확한 분리 정책이 필요하며, 개인정보 혹은 기업의 정보 등 민감도 높은 중요 데이터의 보호를 위해 강력한 암호화 기술을 적용이 필수적이다.

향후 클라우드 서비스의 의존도가 높아지면 클라우드 서비스의 가용성(Availability)는 무엇보다도 중요하다고 할 수 있다. DDoS 등의 공격 및 재난 등으로 인한 클라우드 서비스의 가용성을 무너트리는 상황에 대한 명확한 복구 대책이 마련되어야 한다. 또한, 클라우드 데이터 센터 등에 대한 물리적인 보안대책(CCTV, 출입제한) 역시 고려되어야 한다.

4.1.3. 클라우드 컴퓨팅 보안 기술[5]

○ 안전한 가상화 기술 (Secure Virtual Machine)
- 클라우드 컴퓨팅의 근간이 되는 기술은 가상화 기술이라고 해도 과언이 아니다. 사용자가 클라우드 서비스를 통해 접하게 되는 가상OS는 클라우드 서비스 호스트에서 동작하는 호스트OS 위에서 동작하게 된다. 만일 공격자가 가상OS를 통해 호스트 OS의 권한을 획득하게 되면 클라우드 서비스에 대한 많은 종류의 공격이 가능하게 될 것이다. 이러한 가상화 기술에 대한 취약성 및 실제 공격사례가 보고되고 있는 만큼 이에 대한 SecureVM, Secure Hypervisor 등의 신뢰성 있는 보안 기술 적용이 필수적이다.

○ 저장 데이터 보호 기술
- 클라우드 데이터 서버에 저장되는 데이터들에 대한 변경, 유출, 소실 등의 보안 위협에 대한 대책으로 강력한 암호기술 적용이 필요하다. 외부로부터 요구되는 서비스에 효율적으로 대처하기 위해서는 강력한 암호 기술뿐만 아니라 이를 원활히 처리할 수 있는 고속의 연산 기능, 접근제어와 익명성이 제공될 수 있는 암호 기술이 필요하다. 또한 암호화 기술의 핵심인 키 관리 기술 역시 클라우드 서비스 환경에 적합한 새로운 형태의 기술이 필요하다.

○ 인증 기술
- 앞에서 설명한 바와 같이 클라우드 서비스의 가상화 기술 관점에서 인증은 무엇보다도 중요하다. 또한, 클라우드 서비스 제공자 입장에서 사용자의 부

당한 서비스 사용 방지와 사용량, 사용방법에 따른 적합한 과금 관리를 위한 사용자의 인증기능이 필수적으로 필요하다. 또한, 클라우드 서비스를 통한 사용자의 작업이 장시간 지속되며 한개 이상의 클라우드 서비스를 복수로 이용하는 등 인증 상황에 대한 지속이 필요할 경우가 있을 수 있다. 따라서 이런 상황에 대한 대응책으로 클라우드 환경에 적합한 Kerberos, SSO(Single Sign On) 등의 기술 적용이 필요하다.

○ 관리 기술

- 클라우드 서비스의 가용성 문제 해결과 투명한 클라우드 서비스 제공을 위해서 클라우드 서비스 제공자는 자신의 클라우드 서비스에 대한 다방면의 관리 기술 적용이 필요하다. 특히 클라우드 데이터 센터에 대한 불법적 접근 기록이나 데이터 유출 및 훼손에 대한 경위 파악 등을 위해 클라우드 서버의 로그 파일 관리가 필요하다. 또한, 클라우드 서비스 데이터에 대한 위법행위를 적발하고 이를 법적 증거로 활용하기 위한 디지털 포렌식 기술이 마련되어야 한다. 추가적으로 클라우드 서비스 제공자는 사용자 혹은 외부 기관으로부터의 감사 요구에 대해 명확하게 대응하여야 하며, 이와 같은 감사 도중에도 원활한 서비스 제공이 가능하도록 적합한 관리 기술이 제공되어야 한다.

4.1.4. 클라우드 컴퓨팅 관련 보안제품 개발 동향

지속적으로 클라우드 서비스 업체들이 증가 추세에 있고 빈번하게 서비스 장애 및 중단 사고가 발생하는 등 보안 문제점이 지적됨에 따라 클라우드 서비스를 대상으로 하는 보안 제품의 상용화가 진행되고 있다.

○ 시만텍(Symantec)

- 최근 발표한 '시만텍 엔드포인트 프로텍션(SEP, Symantec Endpoint Protection)'에 클라우드 서비스를 겨냥한 가상화 환경에 적합한 형태의 바이러스 백신을 포함
- 다중 사용자에 의한 병목현상 제어를 위해 가상머신 별로 백신 동작 시간을 조정하는 등 성능 과부하에 대한 대책을 수립

○ IBM

- 클라우드 환경에 적용 가능한 단일 보안제품 및 기업별 클라우드 IT 전략수립과 비즈니스 모델 운영을 위한 컨설팅 서비스 등 기업의 안전한 클라우드 환경 구축 및 운영을 지원
- 소프트웨어 개발 솔루션 '티볼리(Tivoli)'에 중앙집중식 인증, 정책관리 및 접근 제어 서비스 등을 추가 제공하여 클라우드 환경에 적용 가능하도록 보안 기능 확대 제공

○ 파수닷컴

- '파수 모바일 게이트웨이', '파수 컨텍스트 센시티브(Context-Sensitive) DRM' 등 클라우드 내부 정보 유출 방지 제품 출시

○ 안철수연구소

- 클라우드 컴퓨팅을 활용한 보안서비스 전략 ACCESS(AhnLab Cloud Computing E-Security Service) 발표
- 종합 위협 분석 시스템을 클라우드 플랫폼 형태로 구축하고 각종 위협에 대한 대응 방법을 실시간으로 생성/공유하는 방식으로 DDoS 등 위협에 종합적인 대응체계 지원

4.2 IoT 보안[9]

IoT를 구성하는 기반기술은 RFID(Radio-Frequency Identification), USN(Ubiquitous Sensor Network), IPv6, 융합센터, 지능형 로봇, Baseband Modem Chip 등이 있으며, IoT 패러다임 구축에 가장 큰 비중을 차지하는 것은 통신 기능을 담당하는 RFID/USN 기술이라 할 수 있다. 본 논문에서는 RFID와 USN의 보안 요구사항 및 대응방안에 대해 알아보도록 한다.

4.2.1. IoT 보안 취약성

○ RFID 보안 요구사항

- RFID는 각각 고유의 ID를 가지고 있고, 해당 ID는 RFID가 부착된 물건에 관한 ID이다. 또한 해당 물건에 대한 직접적인 정보는 RFID에 저장되는 것이 아니라 원격의 서버에 저장되게 된다. 따라서 RFID 태그가 부착된 물건에 대한 정보를 얻기 위해서는

여러 단계의 과정을 거친 후에야 해당 정보로 변환되어지는 근본적인 차이점을 지닌다. 기존 정보보호 기술 적용 시 발생하는 문제점은 [표 1]과 같다.

〔표 1〕 기존 정보보호 기술 적용시의 문제점

기존 정보보호 방안	RFID 적용시 문제점
클라이언트 서버 간 인증에 의한 도용 방지	RFID 인증만으로는 개인정보 수집 불가
클라이언트 서버 간 통신 데이터 암호화	정보 교환 시 절차가 기존과 상이
정보 수집 규제에 대한 동의	사용자 접근환경 상이
직접적인 정보 수집 및 활용 주체에 대한 규제	정보 수집 주체의 모호성

- RFID의 위협은 크게 두 가지로 나눌 수 있는데 RFID 응용을 위한 각 요소들(태그, 리더, 서버, 통신채널, 글로벌 RFID 네트워크)에 대한 공격과 도청, 추적, 개인정보의 악용 위험성을 지닌 정보의 불법적 유출 가능성이다. 또한, RFID는 개인 신상정보의 유출과 개인의 위치 추적 등 프라이버시와 관련된 문제가 가장 우려되고 있다.
- 이러한 프라이버시 위협의 대두는 RFID 태그가 부착된 물품의 소유주가 RFID 태그 부착에 대한인지가 불명확하며, 무작위로 대규모 정보의 수집이 가능한 문제가 있기 때문이다. 또한, 비접촉식 방식에 의해 RFID 리더가 RFID 태그의 정보를 읽어올 수 있으므로 RFID 리더의 은닉에 대한 문제점 역시 존재한다. RFID 시스템의 각 구간별 정보보호 위협요소는 [표 2]와 같다.

○ USN 보안 요구사항

- USN은 다수의 센서 노드로 구성된 무선 네트워크로써 다양한 환경에 설치된 센서 노드로부터 사람, 사물, 환경에 대한 정보를 인식하고, 인식한 정보를 통합·가공해 언제 어디서나 이용할 수 있게 하는 정보 서비스 인프라를 뜻한다.
- 일반적으로 USN의 데이터의 수집을 원하는 지역에 많은 수의 센서를 설치하고, 대상에 대해 감지된 데이터를 중앙의 베이스 스테이션으로 전송하는 구조를 갖는다. 각 센서 노드가 데이터를 중계하여 베이스 스테이션으로 전송 하는 구조는 애드혹(Ad hoc) 네트워크와 매우 흡사하지만, USN의 센서는 그 크기가 매우 작고 한정된 배터리 자원으로 인해 컴퓨팅 능력이 크게 제한된다는 특징이 있다. 이와 같은 USN의 근본적 특성으로 인해 일반 네트워크에 비해 훨씬 보안에 취약하다. 일반적인 USN의 보안 취약점은 다음 [표 3]과 같다.

〔표 2〕 RFID 정보보호 위협요소

구간	위 협 요 소
태그	- 태그 데이터 무단 조작 - 태그의 복제 에뮬레이션
태그-리더	- 불법적인 도청 - 악의적인 리더의 불법 접근
리더-서버	- 무선 인터페이스 교란 - 불법적인 도청
디렉토리 서버	- 디렉토리 서버 공격 - 정보서버 주소의 불법 획득
정보서버	- 정보서버 공격 - 정보서버 내용의 불법 획득

〔표 3〕 USN 보안 취약점

구간	위 협 요 소
센서 노드의 특성	- 컴퓨팅 환경의 열악함으로 인해 다양한 보안 기술 적용이 힘듬
센서의 물리적 설치 위치	- 노드에 대한 물리적 접근이 쉬움 - 불법적인 도청 - 불법적인 센서 노드 제거 - 불법적인 센서 노드 설치

4.2.2. IoT 보안 기술[10]

○ RFID 보안 기술

RFID에 대한 보안 기술은 많은 부분 RFID 태그와 RFID 리더 사이의 프라이버시 보호를 위한 기술이다. 본 절에서는 대표적인 RFID 프라이버시 보호 기술에 대해 살펴본다.

- Faraday Cage

RFID 태그가 부착된 물건 위에 금속성의 박막을 입혀 무선 주파수 교신이 이루어지지 않도록 하여 무분별한 데이터의 수집을 막는 기술이다. 반면에 대형 마트 같은 곳에 RFID를 이용한 무인 자동 결제 시스템이 설치되어 있다면 이 기술을 악용해 태그 리더에 인식이 안 되도록 하며 공짜로 물건을 들고 나갈 수 있는 등의 역기능이 존재한다.

- Hash-Lock

RFID 태그의 고유 ID 이외에 Key 값을 해쉬한

metaID 정보를 태그가 저장하고 있으며, 데이터베이스와의 통신을 통해 metaID를 확인하여 인증하는 기법이다. 2003년 MIT에서 최초 제안 되었으며 이 기법을 개선한 RHLP(Randomized Hash-Lock Protocol), HIVP (Hash-based ID Variation Protocol), LCAP(Low-Cost Authentication Protocol), MAP(Mutual Authentication Protocol) 등의 방식이 존재한다.

- Re-Encryption

재암호화(Re-Encryption) 기법은 공개키 암호화를 통해 암호화한 고유 번호를 태그에 삽입하는 방법으로 이루어진다. RFID 태그는 하드웨어적 제약사항 때문에 신뢰할 수 있는 공개키 암호 시스템을 적용하기 어렵다. 따라서 RFID가 아닌 외부 공개키 암호 연산기를 통해 이를 실현하는 방식이다.

- One-Time Pad

RSA에서 고안한 RFID 전용 암호화 기법으로써 기존의 One-Time PAD의 키의 길이가 평문의 길이와 같아야 되는 등의 비현실적인 단점을 개선한 방법이다. 오로지 XOR 연산만을 이용한 암호화 기법으로 요구되는 컴퓨팅 능력이 매우 낮아서 RFID에 적합한 암호화 시스템이다.

- 'Kill' Tag

RFID 태그에 8비트의 패스워드를 삽입하고 RFID 태그가 이 패스워드와 'Kill' 명령을 수신할 경우 RFID 태그가 비활성화 되는 방식이다. RFID 내부의 단락회로 자체를 끊어서 사용을 불가능하게 만들기 때문에 RFID 태그의 재활용조차 불가능하게 만드는 단점이 있다. 또한 8비트라는 패스워드 길이의 문제점 역시 본 기술의 단점이다.

○ USN 보안 기술

USN에 대한 보안 기술 연구는 USN의 적용분야와 활용도로 인해 RFID에 비해 많은 부분 연구가 이어졌다. USN에 대한 보안 기술 연구는 키 분배 및 관리, 인증, 보안 네트워크 구조, 보안 라우팅 등 다양한 방면에 걸쳐 진행되어 왔다. 본 절에서는 대표적인 USN 보안 기술에 대해 살펴본다.

- 인증 기법

대표적으로 SPINs(Security Protocols for Sensor Networks)를 들수 있다[12]. SPIN은 데이터의 기밀성을 제공하는 SNEP(Secure Network Encryption Protocol)과 인증을 위한 μTESLA로 구성되어 있다. 각 센서 노드는 베이스 스테이션과 공유하는 마스터키를 사전 분배 받고, 마스터키로부터 유도된 새로운 키와 카운터 값을 이용해 데이터를 암호화한다. 여기에 카운터 값과 MAC 키를 이용해 MAC 값을 만들어 암호화된 데이터에 붙여서 전송하는 방식이다. μTESLA는 기존의 TESLA를 센서 네트워크에 적합하도록 변형한 방식으로 베이스 스테이션에서 인증 키 체인을 생성하고 센서 노드들에게 브로드 캐스팅한다. μTESLA는 해시 체인을 이용하여 효과적으로 데이터 인증을 제공할 수 있고 수신 노드들의 입장에서 중간에 패킷이 분실되더라도 다음 패킷을 통해 이전 패킷을 검증할 수 있다. 하지만 모든 노드들의 시간 동기화가 필요하고, 네트워크 전송 지연등에 대한 추가적인 고려를 위해 별도의 저장 공간이 필요한 단점이 존재한다.

- 키 관리 기법

USN에서 암호키는 대부분 그룹키에 의해 이루어 진다. 이는 베이스 스테이션과의 통신이 여러개의 노드로 이루어진 그룹과 이루어지기 때문이다. USN을 위한 수많은 그룹키 관리 기법이 제안되었지만 대부분의 기법은 μTESLA를 통해 안전하게 그룹키를 전송하고 단방향 해시 함수를 적용하여 데이터의 무결성을 보장하는 방식을 적용한다. 대표적인 그룹키 관리 기법으로는 LEAP(Localized Encryption and Authentication Protocol) 등이 있다[13].

- 안전한 네트워크 구조

USN의 큰 문제점 중 하나는 데이터를 수집하는 단일 베이스 스테이션으로 네트워크 내의 모든 센서 노드가 데이터를 집중하는 구조 자체이다. 이러한 구조는 라우팅 경로의 단순화를 초래하며 센서 노드간 데이터 전송에 대한 일관적인 방향성을 생성하며, 이에 따라 특정 센서 노드가 원치 않게 게이트웨이의 역할을 수행하게 되는 문제가 발생한다. 이는 해당 센서 노드의 부하를 초래하며 배터리 소모를 가속화 시키는 문제가 있다. 따라서 안전한 네트워크 구조는 여러 개의 베이스 스테이션을 설치하여 네트워크 내에 다중 라우팅 경로를 생성함으로써 일부 경로에 문제가 생길경우 다른 경로를 제공한다. 또한 베이스 스테이션의 ID를 은닉하여 해커의 공격으로 부터 보호할 수 있다[15].

Ⅴ. 클라우드 컴퓨팅에서의 IoT 융합 보안 필요성

앞서 살펴본 클라우드 컴퓨팅 보안 동향을 통해 제기된 문제들은 클라우드 컴퓨팅을 구성하는 가상화 기술

을 바탕으로 한 시스템적인 측면에서의 보안과 그리고 그러한 클라우드 컴퓨팅 시스템 및 클라우드와 클라우드를 연결하고 기존 네트워크와 연동되는 부분에서의 보안 이슈를 주로 다루었었다. 그리고 IoT에서의 보안 동향은 기존 센서 네트워크나 RFID를 통한 정보 수집 및 전달 측면의 IoT 보안을 고려하였다. 하지만 IoT가 클라우드 컴퓨팅과 융합되는 환경에서는 클라우드 컴퓨팅이 다루는 데이터 자체에서의 개인정보보호 이슈 및 인증등도 큰 보안 요소로 볼 수 있겠지만 이러한 클라우드 컴퓨팅이 다루는 범주가 향후 IoT기반의 빅 데이터로 넘어가게 되면 이미 다루었던 시스템적 측면의 보안 이슈나 기존 네트워크와 연동이나 클라우드 측면의 네트워크 보안 이슈보다 훨씬 큰 파급 및 중요성을 가질 것이다. IoT에서 다루는 빅 데이터는 기본적으로 요즘 유행하는 SNS 데이터를 포함하여 다양한 웹 콘텐츠 데이터, 웹 구조 데이터, 웹 사용 기록, 각종 시스템에서의 로그 데이터, 이벤트 데이터, 센서 데이터, 모바일 폰에서의 위치, 문자 정보 등 그 종류를 이루 말 할 수 없다. 그러므로 IoT가 다루고 수집하는 데이터는 그 정보의 양이 페타/엑사 단위인 것은 물론이거니와 그 수집되는 데이터의 민감도나 중요도가 매우 높을 것이다. 이러한 IoT와 이 데이터를 처리하는 클라우드 컴퓨팅이 융합된 환경에서의 데이터 컨텐츠 보안은 개인정보보호를 포함하여 매우 중요한 요소임에 틀림없다.

또 다른 측면으로는 빅 데이터를 수집하고 처리를 요구하는 IoT는 필연적으로 클라우드 컴퓨팅 환경의 고성능·고신뢰성을 요구 할 것이고 다시 이러한 높은 수준의 성능과 신뢰성을 요청하는 환경에서의 시스템·네크워크 측면의 보안 이슈가 다시 불거질 것이다. 즉, IoT를 포괄하는 클라우드 컴퓨팅은 그 대량의 데이터를 안전하고 신뢰성 있는 방안으로 활용 및 처리해야 될 필요성을 가지기 때문이다.

따라서 클라우드 컴퓨팅에서의 IoT 융합 보안은 IoT로부터 발생하는 빅 데이터의 개인정보보호를 바탕으로 한 보안 이슈를 먼저 선결해야 하며 또한 이러한 데이터의 처리 및 관리 측면에서의 클라우드 컴퓨팅 자체의 고신뢰성·고성능을 보장해야 한다.

Ⅵ. 결 론

현재의 급속한 ICT 기술 발전과 함께 수많은 센서와 RFID/NFC등의 다양한 통신 방식을 통한 데이터의 수집을 가능케 하는 IoT 인프라는 필연적으로 클라우드 컴퓨팅을 요구 할 것이라 사료된다. 이에 따라 빅 데이터의 개인 정보보호 이슈를 해결하며 클라우드 컴퓨팅 환경의 기본적인 신뢰성과 보안성을 제공할 수 있는 새로운 보안 아키텍처가 필요할 것이다. 이제 우리가 놓인 빅 데이터 시대의 클라우드 기반 응용을 고려하며 이를 더욱 발전시키고 안전하게 활용 할 수 있는 세부적인 보안 기술의 연구가 시급한 실정이다.

참고문헌

[1] 민영기, 구원본, 유명호, 김종철, 서병진, "클라우드 국내외 동향조사 및 표준화 전략 수립" 보고서, KSA 한국표준협회, May 2011.

[2] 유상근, 김형준, "사물지능통신 정책 및 표준화 동향", *정보보호과학회지 특집원고*, 21-27, Sep 2010.

[3] 한국인터넷진흥원, "클라우드 서비스 정보보호 안내서", Oct 2011.

[4] 민옥기, 김학영, 남궁한, "클라우드 컴퓨팅 기술 동향", 전자통신동향분석, 제24권, 제4호, Aug 2009.

[5] 박춘식, 김형종, 김명주, "클라우드컴퓨팅 보안 동향", 정보통신산업진흥원 주간기술동향, 제1432호, 26-35, Feb 2010.

[6] J.Heiser, M.Nicolett, "Assessing the security Risks of Cloud Computing", Gartner, Jun 2008.

[7] 한국정보사회진흥원, "2009년 주요 IT 전략기술에 따른 보안 이슈 및 해결 방안", IT Issues Weekly, 제197호, Jan 209.

[8] 한국콘텐츠진흥원, "문화기술(CT) 심층리포트", 제11호, Feb 2011.

[9] 이영실, 박범수, 임효택, 이훈재, "사물지능통신망에서의 RFID/USN 기반 정보보호 기술동향", 정보과학회지 특집원고 1, 55-64, Sep 2010.

[10] 문송철, 나원식, "RFID System 환경에서의 보안 위협과 프라이버시 보호기술에 관한 연구", 남서울대학교 논문집, Vol. 13-3, 161-187, 2007.

[11] 나재훈, 채기준, 정교일, "센서 네트워크 보안 연구 동향", 전자통신동향분석, 제20권, 제1호, 112-122, Feb 2005.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th ACM/IEEE

International Conference on MobiCom, 2001.

[13] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Commu-nication Security(CCS), 2003.

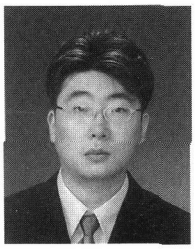
[14] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Network," Proc. of the 9th ACM Conference on Computer and Communications Security, 2002.

[15] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Department of Computer Science, University of Colorado, Apr, 2003.

〈著者紹介〉

손 태 식 (Taeshik Shon)
정회원

2000년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월 : 아주대학교 컴퓨터공학 석사
2005년 8월 : 고려대학교 정보보호대학원 박사
2004년 2월~2005년 2월 : University of Minnesota, Research Scholar
2005년 8월~2011년 2월 : 삼성전자 DMC 연구소 책임연구원
2011년 2월~현재 : 아주대학교 정보통신공학부 조교수
<관심분야> 무선/모바일 네트워크 보안, 무선 센서 네트워크, 이상탐지



고 종 빈 (Jongbin Ko)

2006년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2008년 2월 : 아주대학교 컴퓨터 공학 석사
2008년 2월~현재 : 아주대학교 컴퓨터공학 박사과정
<관심분야> 디지털 포렌식, 무선 센서 네트워크 보안스마트그리드 보안