KIICE 한국정보통신학회지 16권 2호
THE MAGAZINE OF KIICE
http://www.kiice.org

사물인터넷(IoT)에서의 정보보호 동향

이수연

백석문화대학교 인터넷정보학부

목 차

Ⅰ. 서 론

최근 스마트 기기의 보급화로 Wi-Fi, LTE 등을 이용한 무선인터넷 사용률이 대폭 증가한 반면 유선인터넷의 비율은 감소하고 있는 추세이다. 이렇듯 장소에 구애받지 않고 무선인터넷에 접속하여 사람과 사람뿐만이 아니라 사람과 사물간의 통신, 사물과 사물간의 통신으로 점점 통신 범위가 다양해지고 있는 추세이다. 특히, 스마트 자동차, 스마트 웨어러블과 같이 우리 생활에 밀접한 관계를 가지고 있는 사물들이 점차 통신을 통해 자료를 수집, 처리, 가공하도록 유도하고 있다.

이렇듯 급부상하고 있는 사물인터넷 기술과 서비스는 정보화 3세대라고 불리는 초연결사회의 근간 기술과 서비스로 주목받고 있다. 정보화 3세대에서는 사람뿐 아니라 주변의 수많은 사물들에게도 컴퓨팅 파워가 접목되며 이들은 일상적으로 네트워크에 연결된다. 하지만 여러 가지 요소기술들이 통합되어 특정 서비스를 구성하기 때문에 각 요소 기술 자체의 보안 취약성과 연동 시 새로운 보안 취약성이 발생할 가능성이 매우 높다. 따라서 사물인터넷은 기존의 보안위협을 포함하여 새로운 보안위협이 복합적으로 발생 할 수 있다.

이러한 사물인터넷은 새로운 정보통신기술이라는 관점보다는 새로운 정보통신 서비스와 산업의 관점에서 볼 때 여러 가지 기술적인 문제들을 해결해야할 것이다. 특히, 사물인터넷 플랫폼 기술이나 보안 기술이 향후 관련 산업에 상당한 영향을 끼칠 것이다.

본 논문에서는 현재까지의 사물인터넷(IoT) 개요 및 그에 관련된 정보보호 기술을 살펴보고 국내·외적으로 연구되어지고 있는 사물인터넷 보안정책 현황을 살펴볼 것이다.

Ⅱ. 사물인터넷(IoT)의 개요

2.1. 사물인터넷(IoT)의 개념

사물인터넷에 대하여 IETF, ITUT(MOC), 3GPP(MTC), ETSI(M2M) 등에서 각각 정의하였다. 이렇듯 사물인터넷에 대하여는 다양한 정의한 존재하는 데 이 중에서 CERT-IoT 2009에서 정의한 사물인터넷 개념이 가장 포괄적이면서도 명확한 정의로 보인다. 이에 따르면 사물인터넷은 미래인터넷의 통합된 부분으로서 표준과 상호 호환 통신 프로토콜로 자가 설정 기능을 갖춘 동적 글로벌 네트워크 인프라로 정의될 수 있으며 사물인터넷은 자기 식별자와 각각의 특성을 갖는 물리적인 사물과 가살 사물로 구성된다고 하였다. 정의를 보면 사물이라는 것이 물리적인 사물과 가상적인 사물을 모두 포함하는 개념이라는 것을 알 수 있는 데 여기서 가상적인 사물의 예로는 소프트웨어 서비스, 소프트웨어 객체, 행위 주체로서의 액터(Actor) 등이 있다.

그림 1. 사물인터넷 개념[1]

사물인터넷의 주요 구성 요소인 사물은 유무선 네트워크에서의 end-device 뿐만 아니라, 인간, 차량, 교량, 각종 전자장비, 문화재, 자연 환경을 구성하는 물리적 사물 등이 포함한다. 이동통신망을 이용하여 사람과 사물, 사물과 사물간 지능통신을 할 수 있는 M2M의 개념을 인터넷으로 확장하여 사물은 물론, 현실과 가상세계의 모든 정보와 상호작용하는 개념으로 진화하였다.

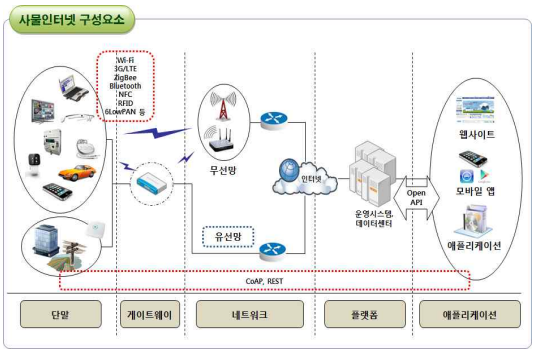

그림 2. 사물인터넷 구성 요소

2.2. 사물인터넷(IoT) 서비스 사례[2]

2.2.1 국내

제주도에서는 M2M기반의 지하수 관측 통합 관제 시스템 및 지하수 무인 자동관측시스템을 서비스하였다. 이는 먹는 샘물 취수원의 수위 및 수질 데이터의 수집/분석과 제주도 전역에 분포된 지하수 관측망의 동 시간에 신뢰성 있는 데이터 확보가 필요했기 때문이다. 단지, 몇 가지 개선점이 나와 보완 작업을 하고 있는 상황이다.

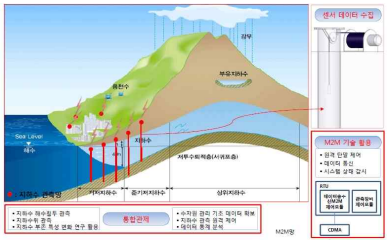

그림 3. 지하수 자동관측시스템

2.2.2 해외

뉴욕시는 마이크로소프트와 협력해 DAS(Domain Awareness System)라는 대테러 감지시스템을 구축하였다. 이는 맨하탄 지역에 설치된 4,000여 대의 CCTV, 600여 대의 방사능 감지기, 100여대의 자동차번호판 인식장치를 연계하여 의심스러운 사람이나 물품, 차량 관련 정보를 분석해 현장경찰과 소방서 등 관련 기관에 즉시 제공하였다. 예를 들어 범죄나 테러 현장 주변의 CCTV 영상을 통해 범죄 용의 차량 정보를 포착하면 DAS를 통해 해당 도시 전역의 실시간 CCTV 영상을 분석해 용의 차량 위치를 파악하고 추적이 가능하게 하였다.

그림 4. 대테러 감지시스템(DAS)

2.3. 사물인터넷(IoT) 주요 기술

사물 인터넷은 기존과 다른 방식으로 정보가 입력되고 처리되어진다. PC 시대의 키보드와 마우스, 모바일 시대의 손가락과 스타일러스 펜과 달리 사물인터넷에서는 음성이나 제스쳐 혹은 스마트폰 등의 기존 기기를 이용해 기기를 조작하게 된다. 또한, 일부 기기는 별도의 조작없이 자동으로 데이터가 입력되어 동작되기도 한다. 즉, 다양한 종류의 입력장치를 통해서 사물인터넷 기기가 조작되어진다. 그런만큼 기존과 다른 다양한 입력 기술을 필요로 한다. 또한, 주위환경에서

정보를 얻을 수 있는 센서와 같은 물리적인 기술 및 사용자 인증을 위한 인식 기술 또한 주목받을 것이다.

특히, 사물 간에 서로 연결되어 동작이 이루어지기 때문에 M2M(Machine to Machine) 기술과 인터넷에 연결되어 축적된 데이터를 저장하는 클라우드도 중요하다. 가장 주목할 기술은 빅데이터(BIG data)와 machine learning 기술이다. 결국 사물인터넷은 기존의 디지털 기기보다 더 자주, 거대한 데이터들을 저장하고 이들 데이터를 기반으로 새로운 가치를 만들어낸다. 그런 만큼 방대한 데이터를 보관하고 이를 활용하기 위해 데이터를 분석하는 data science에 대한 중요도가 높아질 것이다.[3]

더 나아가 이들 데이터를 통해서 사용자의 context를 추출하는 context aware 기술에 대한 중요성도 함께 커질 것이다. 이들 기술을 기반으로 기계는 자가 학습을 하면서(machine learning) 인공지능을 가지게 되고 이러한 기술이 기계가 사람을 이해하고 자동으로 서비스를 제공하는 패러다임을 만들어갈 것이다. 이들 기술은 곧 소프트웨어 산업에 새로운 기회를 가져다 줄 것이다.

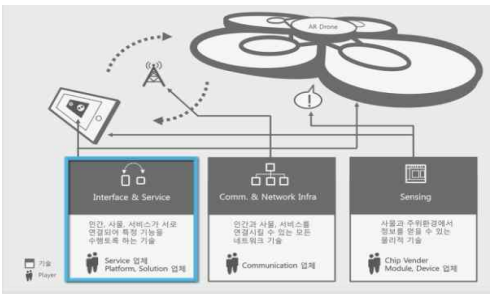

그림 5. 사물인터넷 주요 기술

Ⅲ. 사물인터넷(IoT) 보안위협

3.1. 사물인터넷 보안 취약성 사례[

사물인터넷의 빠른 확산과 함께 사물인터넷 보안 위협에 대한 우려도 크게 늘고 있다. 기존의 PC와 스마트폰 뿐 아니라 앞으로 인터넷에 연결될 다양한 사물인터넷 디바이스 및 서비스에 대한 보안 경각심이 요구되고 있다.[4]

사물인터넷의 보안 위협은 다양한 사례를 통해 확인할 수 있다. [그림 6]은 체중계가 인터넷에 연결되고 각종 분석 기능과 다양한 서비스와 연동이 가능한 사물인터넷 제품/서비스 사례를 보여주고 있다. 사용자가 측정한 체중 정보는 서비스 제공업체의 클라우드에 전송되며 해당 정보를 사용자는 스마트폰과 같은 단말에서 앱을 통해 확인할 수 있다. 언급한 체중 정보 흐름은 단순해 보이며 서비스도 단순해 보이지만 개인의 체중 정보는 매우 다양한 형태의 서비스에 활용될 수 있다. 예를 들어, 어떤 사물인터넷용 체중계는 측정한 개인의 체중 정보를 개인의 선택에 따라 트위터와 같은 SNS에 업로드할 수 있다.

그림 6. 사물인터넷 제품(체중계) 사례에서 본 보안 취약성

이는 공개된 정보이므로 보험회사에서 해당 정보를 활용하여 사용자에게 맞춤형 보험 상품 판매 영업을 할 수 있다. 또한, 이미 보험 가입자라면 체중의 변화에 따라 건강 위험도의 변화로 인식하여 자사의 보험 손실을 우려하여 해당 사용자에 영향력을 미치고자 할 수도 있을 것이다. 아울러, 서비스 업체에 저장된 개인의 체중 정보가 악의적인 목적으로 사용될 수도 있으며, 서비스 업체가 자사의 이익을 위해서 분석/가공을 통해 회사 입장에서는 부가가치가 높은 다른 정보로 변환할 수도 있을 것이다. 예를 들어, 만약 업체에서 자사가 보유하고 있는 정보를 가공하여 제3의 업체에 판매한 경우, 판매 이후에는 정보를 제공한 업체에서는 해당사용자의 정보를 통제할 수 없을 것이며, 가공된 정보는 원래의 정보라고 볼 수 없기 때문에 최초의 체중 정보 소유자가 이 경우에 해당 정보에 대한 통제권을 가진다고 볼 수도 없게 된다. 지금까지 단일 업체에 의한 정보 처리 및 관리가 이뤄졌고 사물인터넷 환경처럼 여러 주체가 관계되는 경우는 없었기 때문에

기존의 프라이버시 관련법과 체계는 새로운 사물인터넷 환경에 맞게 정비될 필요가 있다. 언급한 프라이버시 침해 가능성뿐만 아니라 [그림 6]에서 보듯 체중계에서 센싱되어 무선 통신채널로 전송되는 정보를 악의적인 공격자가 가로챈다면(sniffing), 공격자는 해당 정보를 활용하여 사용자의 신체적 특성을 유추하여 이를 악의적인 목적에 사용할 수 잇을 것이다. 많은 사물인터넷 디바이스와 플랫폼에 접근 제어, 인증/인가 기술에 있어서 높은 등급의 기술이 구현되지 않기 때문에 상대적으로 공격에 취약하다. 따라서 사물인터넷 제품과 서비스에서는 각별히 보안과 프라이버시 침해 문제를 살펴볼 필요가 있다.

3.2. 사물인터넷(IoT) 보안 위협[5]

사물인터넷 구성 요소별 보안 위협을 살펴보면 다음과 같다.

- 디바이스 계층

  기기 정지 및 오작동 유발에 의한 인프라 마비 및 생명위협 등 물리적 위협, 기기 분실/도난, 기기 위변조 등에 의한 정보 변조·유출, 디바이스 간 악성코드 전이 및 공격 위협, 경량/저전력 요구 기기에 대한 IP 보안 기술 적용 어려움

- 네트워크 계층

  이기종 사물 네트워크 간 연동 통신과정에서 정보 변조·유출, T2T기기, 네트워크 및 게이트웨이 해킹 공격 및 크로스 네트워크 기기로 피해 확산, 대단위 사물봇에 의한 사물인터넷 서비스 거부(DoS: :Denial of Service)

- 플랫폼/서비스 계층

  악성 기기/사용자의 플랫폼 불법 접속 및 공격, 불법 포획 후 암호키 해킹에 따른 플랫폼 붕괴, 클라우드, 빅데이터-개인 정보유출 및 프라이버시 침해

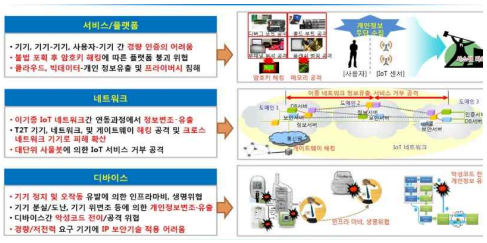

그림 7. 사물인터넷 보안위협(산업연구원 2014)

이렇듯 사물인터넷은 디바이스, 네트워크, 서비스/플랫폼 등 다양한 기술요소들을 결합하여 특정 서비스를 구성한다. 따라서 각 기술 요소들을 안전하게 보호하는 보안기술이 존재한다 하더라도 이를 통합/연동하는 방법이 없다면 보안 취약성이 발생할 수 있다는 특징을 가지고 있다.

Ⅳ. 사물인터넷(IoT) 보안기술

4.1. 사물인터넷 보안 요구 사항

본 절에서는 ITU가 사물인터넷 서비스 참조모델은 통해 정의한 사물인터넷 기본 보안 요구 수준을 소개한다.

보안	구 분	보안 요구 사항
일반	디바이스 계층	권한설정, 인증, 단말 무결성 검증, 접근통제, 데이터 기밀성 무결성 보장
	네트워크 계층	권한설정, 인증, 데이터/신호 정보의 기밀성 및 무결성 보장
	플랫폼/서비스 계층	권한설정, 인증, 데이터 기밀성, 무결성, 프라이버시 보장, 보안 감사 수행, 안티 바이러스 설치
특별	모바일 결제 등 특수한 상황에 요구되는 보안요구사항	

첫째, 사물인터넷 서비스를 위해 개방된 장소에 설치된 사물인터넷 장치에 대해 권한이 없는 사람의 물리적 접근과 파손에 대해 이를 방지하기 위해서는 기기 인증과 물리적 접근 통제가 먼저 요구되어진다. 둘째, 사물인터넷에서 유무선 통신 구간에서의 도청, 훔쳐보기(Sniffing) 또는 정보를 저장하고 있는 서버/DB로의 비인가 접근을 막기 위해서 인증과 데이터에 대한 기밀성과 무결성이 요구되어진다.

마지막으로 사물인터넷 서비스/플랫폼 계층 보안 요구 사항은 크게 보안 및 인증 관리 및 자원관리로 구분할 수 있다. 먼저 보안 및 인증 관리를 위한 사물인터넷 단말 미들웨어는 외부로부터 유입되는 데이터로 인해 단말의 운영체제, 하드웨어 등이 영향을 받지 않도록 운영체제와 논리적으로 완전히 격리가 이뤄져야 한다. 두 번째 자원관리는 사물인터넷 단말이 그 특성

상 자원이 매우 제한적이라는 점에 기인해야한다.

4.2. 사물인터넷 보안 기술

앞서 살펴본 사물인터넷 구성 요소 별 보안요구사항을 충족하기 위한 기술적인 부분에 대해 알아보고자 한다.

4.2.1 디바이스 보안기술

디바이스 보안기술로는 저전력, 경량 보안 기술이 필요하다. 대부분의 사물인터넷 디바이스는 기본적으로 저전력 모드에서 동작하며 연산이나 저장 능력 등이 낮은 경량 디바이스이다. 따라서 저전력, 경량 사물인터넷 기기의 성능 및 필요 보안 강도를 고려한 저전력, 경량 암호 알고리즘이 필요하다. 그리고 무정지 및 오작동 감내 기능이 필요하며 물리적 위협 방지 기능이 필요하다.

세계적으로 현재 다양한 사물인터넷 보안 기술 개발이 진행 중이다. 경량 암호화 기술로서 해외에서는 의 PRESENT, KATAN 이 있고 국내에서는 LEA, HIGHT 등이 있다. 그러나 현재까지 개발 된 경량 암호화 기술은 부채널 공격 등의 해킹에 취약성을 가진 것으로 알려져 있다. 국내는 스마트폰용 HW 보안모듈을 한국전자통신연구원(ETRI)이 개발 중이다.[6]

그림 8. 보안모듈 MTM(Mobile Trusted Module)

4.2.2 네트워크 보안기술

현재 사물인터넷에서는 주로 근거리 통신 기술로 IEEE 802.15.4 저전력 통신 기술인 ZigBee, 스마트폰 등에 널리 쓰이면서 그 활용이 보편화된 IEEE 802.11 무선랜 기술인 Wi-Fi, 그리고 기존 바코드를 대체하여 사물 자동 인식을 위해 도입된 전자 태그 기술인 RFID(Radio Frequency IDentification) 등이 있다. 원거리 통신 기술로는 널리 보급된 무선이동통신, 즉 3G 나 LTE 등이 있다.[7]

▪ ZigBee

ZigBee는 낮은 수준의 보안을 위한 SSM(Standard Security Mode)과 높은 수준을 제공하기 위한 HSM(High Security Mode) 방식이 있으며 각각의 ZigBee 장치는 Open Trust Mode 방식으로 동작하기 때문에 장치 자신에 대한 신뢰성을 보장한다. 따라서 각각의 ZigBee 장치 간 통신과정에서의 기밀성과 무결성이 보장된다면 신뢰를 담보할 수 잇다. 하지만 모든 통신구간에 대한 암호화가 이루어진 것은 아니기 때문에 비 암호화 구간에 대한 별도의 보안대책 마련이 요구된다.

▪ Wi-Fi

Wi-Fi는 IEEE802.11 표준 기반의 무선 랜 기술로 고성능 무선 통신이 가능하다. Wi-Fi는 무선으로 통신이 이루어지기 때문에 보안 위협으로부터 특히 취약하다. Wi-Fi 사용 시 통신 데이터의 암호화가 이루어지지 않을 경우 도청, 스니핑, 비 인가 접근 등의 공격이 이루어질 수 있다.

따라서 무선 구간의 데이터를 안전하게 보호하기 위한 방법으로 IEEE802.11 표준에서 제시한 WEP (Wired Equivalent Privacy) 인증 프로토콜이 있으며 WEP의 단점을 개선한 WAP(Wi-Fi Protected Access)와 WPA2를 IEEE802.11i에서 제안하였다. 또한 무선 구간의 통신 과정 외에 접속 과정에서의 보안을 위하여 암호화 알고리즘 TKIP(Temporal Key Integrity Protocol)과 CCMP(Counter mode with CBC-MAC Protocol)의 사용을 권고하고 있다.

▪ RFID

RFID는 사물의 자동 인식을 위하여 무선 주파수를 이용하는 기술로 ISO 18000-7 표준에 기반 한다. RFID는 물리적, 시각적 접촉과 무관하게 사물에 부착한 태그 정보를 인식하는 무선 네트워크 기술로 최근 USN(Ubiquitous Sensor Network) 환경 구축을 위해 가장 주목받는 기술이라 할 수 있다. RFID 시스템에서 주고 사용되는 수동형 태그는 제한된 연산 능력과 사용할 수 있는 전력량에 한계가 있으므로 높은 수준의 보안 기술을 적용하기 어렵다는 단점이 있으며 무선 통신에 기반 하므로 정보유출 등의 보안 위협으로부터 취약하다. 이에 USN에서의 보안 요구 사항으로는 데이터 통신에 대한 기밀

성 및 무결성이 요구되며 안전한 키 관리 및 분배 기능이 요구된다. 또한 센서 네트워크의 특성을 고려한 안전한 플랫폼 설계가 필요하다. 최근, RFID/USN 환경에서 전송되는 데이터 보안을 위하여 노드와 노드 간의 상호 인증을 위한 다양한 기법들[8]이 연구되고 있다.

▪ 3G/LTE

3G 이동통신 네트워크는 도입 초기에 회선 교환(Circuit Switch)기술을 기반으로 음성 서비스를 주로 제공하는 폐쇄형 구조였지만 점진적으로 패킷 교환(Packet Switching)기술을 기반으로 음성 외에 데이터 서비스를 확대하는 구조로 진화하였다. 하지만 최근 모바일 악성코드의 증가로 감염 단말의 악성, 비정상 트래픽이 3G/4G 망으로 유입되고 있다. 이로 인해 다양한 보안 위협이 발생하고 있다. 따라서 기존 인터넷환경에서 사용된 보안 장비를 그대로 적용하기 어려운 경우가 많다. 이들 보안 장비는 3G/4G 망 고유의 물리적 취약점을 노리는 공격을 탐지하거나 대응하기 어려운 한계가 있다.

위에서 살펴보았듯이 사물인터넷 서비스를 위해 네트워크를 통한 침입 또는 분산 서비스 거부 공격(DDoS)과 같은 공격을 차단하는 보안 기술이 필요하다. 이기종 기기가 초 연결된 사물인터넷 네트워크에 대한 침입 차단을 위한 사물인터넷 게이트웨이, 그리고 사물 봇 공격 차단 아직 연구 개발 초기 단계에 있는 것으로 평가된다. 인텔, Freescale, Eurotech 등에서 사물인터넷 게이트웨이를 개발하였으나 실시간 보안 모니터링이나 침입 참지 등 사물인터넷 디바이스 및 네트워크에 대한 보안 관리 기능은 적용되어 있지 않은 실정이다.

4.23 플랫폼/서비스 보안기술

사물인터넷 플랫폼/서비스에서는 외부의 센서 또는 단말과 기존 응용 계층의 서비스의 매쉬업 형태로 새로운 서비스를 추가·개발 가능한 개방형 구조를 가져야한다. 이를 위한 연구가 IoT-Architecture(IoT-A)프로젝트를 중심으로 활발히 진행되고 있다.

사물인터넷을 구성하는디바이스, 사용자, 서비스들 간의 상호 인증 및 통신 암호화, 프라이버시 보호 기능을 제공할 필요가 있다.

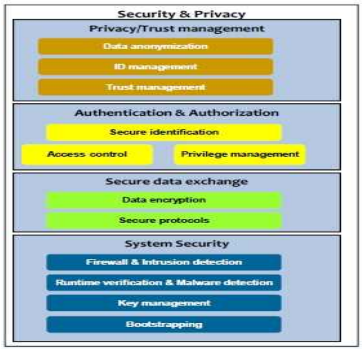

그림 9. 사물인터넷 서비스 보안기술

[그림 9]에서 보듯이 사물인터넷에서는 사람의 개입 없이 기기들 간의 자동화된 인증 및 통신 암호화가 필요하다. 즉 새로운 기기의 서비스 참여 등록과 키 분배 기능을 서비스 구종에 맞게 제공하는 기술이 필요하다. 그리고 사물인터넷에서 수집되는 다양한 센싱 정보 등을 결합하여 빅 데이터 분석을 수행하면 개인 프라이버시가 침해될 가능성이 생긴다. 다라서 빅 데이터 사후 분석에 의한 개인 식별/추적위험을 방지하기 위한 자동화된 개인정보 수집 차단 및 비식별화 기술이 필요하다.

해외에서는 사물인터넷 기기 인증을 위한 서비스 등록 및 키 관리를 위한 연구를 진행 중이나 국내는 PKI 등 기존 인터넷에서 이용자 인증에 사용되는 기술을 그대로 적용하는 수준이다. 의료, 자동차, 홈 네트워크 등 고성장 응용 서비스 분야는 빠르게 성장하고 있지만 응용 서비스 보안 기술 개발은 미흡한 상태인 것으로 평가된다.

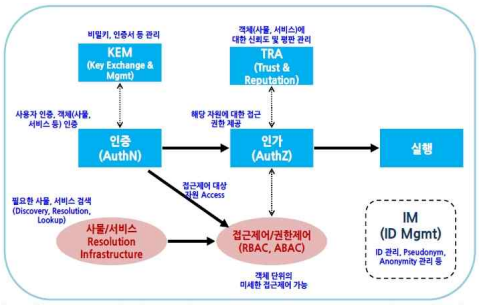

그림 10. 사물인터넷 보안기술의 관계도

Ⅴ. 사물인터넷(IoT) 관련 국내·외 보안정책 현황

본 장에서는 국내·외적으로 사물인터넷 보안에 관련된 정책을 알아본다.[9][10][11]

5.1. 국내

미래부는 사물인터넷의 보안이 설계 초기부터 고려되어야한다는 사실에 입각하여 보안 로드맵을 통해 보안 내재화기반을 마련하고 글로벌 융합보안 시장을 선도하는 9대 보안 핵심 기술 개발 및 사물인터넷 보안 산업 경쟁력 강화 등을 2018년까지 추진하기로 했다. 이를 통해 미래부는 세계 최고의 스마트 안심 국가를 실현하고자 하는 계획을 제시하고자 했다.

그림 11. 사물인터넷 보안 추진전략

특히, 선도 기술 개발로 디바이스, 네트워크, 서비스 환경과 관련 된 사물인터넷 정보보호 로드맵 9대 과제를 2014년 발표하였다.

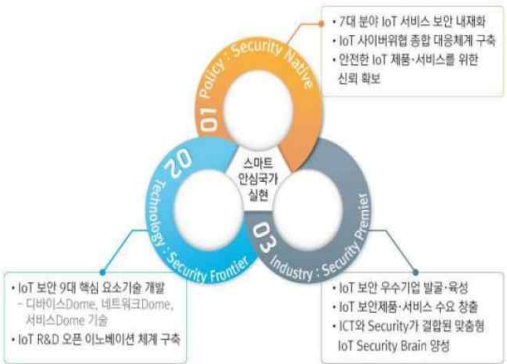

그림 12. 사물인터넷 정보보호 로드맵 9대 과제

5.2. EU

EU는 다양한 사용자의 데이터를 관리하고 보호하기 위한 정책적 차원의 노력을 반영하기 위해 유럽은 현재 정책을 유지하는 무조치(No Action)와 엄격한 법규제를 집행하는 경성법(Hard Law)과 대별되는 유연한 접근 방식으로 자유로운 경쟁 시장 조성으로 인해 유럽 사회가 구현하고자 하는 프라이버시 및 보안 정책을 실현하기 어렵고 반대로 경성법 정책 시 사물인터넷 발전 자체가 저해될 수 있는 반작용이 있을 수 있다. 따라서 사물인터넷 시장에서 사업자들이 자발적으로 참여하되 프라이버시 및 보안 관련 이슈에세도 정책적 목표를 달성할 수 있는 연성법 차원의 접근이 제시되고 있다.

5.3. 미 국

미국의 사물인터넷 정책은 유럽의 포괄적인 접근방법과 달리 부문별 접근방식을 채택하고 있다. 이에 따라 사물인터넷 생태계에서 프라이버시 및 보안을 다루는 정책 역시 분야별로 추진 중에 있다.

국가 차원에서 오바마 행정부는 빅데이터 시대를 열기 위해 관련 정책 보고서를 공식 발표하였고 사물인터넷 시대에서 프라이버시 및 보안을 보장하기 위해 FTC를 중심으로 소비자들의 사물인터넷 사물에 대한 정책에 관여하고 있다.

5.4. 일본

사물인터넷 정책 구현에서 있어서 프라이버시에 대한 고려보다 사물인터넷 활성화에 대한 측면을 더욱 강조하는 경향을 보여 왔다. 최근에는 사물인터넷이라는 개념보다 빅데이터 개념에 초점을 두고 빅데이터에서 사용되는 개인정보 문제를 사전 검토하고 이에 대한 침해 우려를 경감할 수 있는 정책을 표방하는 방식으로 추진되고 있다. 아직은 기업의 빅데이터 활용에 무게를 더 두고 있다는 점은 일본이 개인정보보호 문제와 관련하여 가장 부각되고 있는 개인식별번호제도 도입과 관련된 내용이다. 이는 일본 행정 시스템 전반에 상당한 영향을 미칠 수 있는 제도로서 이 제도의 도입 및 적용의 성공 또는 실패 여부가 일본 내 개인정보보호의 성패를 좌우할 수 있다고 볼 수 있다

사물인터넷 프라이버시 및 보안 관련 정책 역시 사물인터넷 활용 단계에서 발생할 수 있는 가능성을 다루는 방식으로 제시되고 있다.

5.5. 중국

중국은 국가 중심 전략의 일환으로 사물인터넷 정책 활성화를 추진해왔다. 동시에 중국은 미국 및 유럽과 같이 보안 위협의 문제를 예방하기 위해 관련 연구를 병행해 온 것으로 보인다. 이는 '사물 지능'이라는 통신 센터를 구축하고, '사물망 12-5 발전 규회'이라는 정책으로 사물인터넷에 대하여 집중적인 투자 전략을 채택한 데에서 알 수 있다. 중국은 프라이버시 및 보안 관련 법률 측면에서 유럽 및 일본에 비해 상대적으로 미흡해 보인다. 따라서 유럽과 같은 포괄적 정책을 그대로 수용하기는 어려울 것으로 판단된다 하지만 사물인터넷 개인정보보호를 관장하는 벌률 및 규정이라는 사물인터넷 10대 특별 계획을 고려해 보건대 프라이버시 및 보안 위협을 다루는 정책은 향후 발생할 수 있는 심각한 보안 위협을 사전에 방지할 수 있고 이를 통해 국가적 안전 및 통일성에 기여할 수 있을 것으로 보인다.

Ⅵ. 결 론

본 논문에서는 최근 ICT 기술과 스마트폰의 보급으로 인하여 관심이 증대된 사물인터넷 정보보호 동향에 대하여 살펴보았다. 최근 사물인터넷이 홈 가전, 의료, 교통 등 다양한 산업분야에 적용되고 있으며 본격적으로 시장 활성화가 진행 중에 있으므로 사물인터넷 활용분야가 우리 실생활의 모든 사물에 '직접 접목' 되며 기존 사이버공간의 위험이 현실 세계로 전이·확대되기 때문에 사물인터넷 제품·서비스의 보안위협에 대한 우려가 점점 증가하고 있다.

특히, 사물인터넷이 향후 국가 경쟁력에 커다란 영향을 미칠 것으로 예상된다. 따라서 각 국가는 사물인터넷 기술 및 서비스 투자뿐만이 아니라 사물인터넷 보안이 초기에 고려되어 사물인터넷 생태계에서 발생할 수 있는 프라이버시 문제를 다루기 위한 다양한 정책적 노력을 기울여야한다고 본다.

참고문헌

[1] 창조경제 실현을 위한 사물인터넷 기반 유망 시장 전망 및 과제, 한국정보화진흥원, 2013.07.

[2] 이상학, 사물인터넷 서비스의 국내외 사례, 전자부품연구원, 2011.

[3] 김호원, 사물인터넷 환경에서의 보안/프라이버시 이슈, TTA Journal Vol.153

[4] https://www.swbank.kr/introduce/bbs/knowledgeChannelList.do

[5] 김종덕, 사물인터넷 시대의 도래: 현황과 전망, 텔코경영연구소 보고서, 2014.12

[6] 김정녀, 초연결 사회로의 진화, 사물인터넷(IoT) 보안 기술, 2014.6

[7] 장봉임, 김창수, 사물인터넷 정보보안 기술, 보안공학 논문지, Vol.11, No.5 (2014), pp429-438

[8] D.Gessaner, A.Olivereau, A.Salinas Sergura, A.Serbanati, "Trustworthy Infrastructure Service for a Secure and Privacy-respecting Internet of Things", IEEE Conference on Trust, Security and Privacy, 2012

[9] 사물인터넷(IoT) 정보보호 로드맵 3개년 계획, 정보보호지원과, 2015. 6

[10] 김번수, 스마트기기 보급 확대에 따른 개인정보보호방안 연구에 대한 최종보고서, 2014.12

[11] Internet of Things Architecture, http://www.iot-a.eu/public

이수연(Suyoun Lee)

2003년: 성균관대학교 전기전자 및 컴퓨터공학부(박사)
1997년~현재: 백석문화대학교 인터넷정보학부 교수
※관심분야: 사물인터넷 보안, 암호프로토콜, 무선인터넷