IoT 보안 기술 동향

서화정 · 이동건 · 최종석 · 김호원
부산대학교 정보컴퓨터공학부

Ⅰ. 서 론

사물 인터넷, 즉 IoT(Internet of Things) 기술은 현재 해당 분야 관계자들이 각자 다양한 관점에서 IoT 기술을 보고 있기 때문에, 아직 명확하고 표준화된 정의가 존재하지 않는다. 국내에서는 2000년 초부터 USN(Ubiquitous Sensor Network)이라는 이름으로 IoT 관련 분야에 대한 활발한 연구 개발과 사업화가 추진되어 왔으며, 최근에는 ETSI의 M2M 기술 표준화와 더불어 M2M/IoT 포럼을 중심으로 관련 기술 표준화 활동과 기술 개발, 서비스 상용화 노력이 많이 이뤄지고 있다[1]. IoT는 USN이나 M2M을 포괄하는 개념이고, IoT를 바라보는 다양한 시각과 해석이 존재하므로 단순하고 명확하게 IoT의 특성을 나타내는 정의가 만들어지기는 한 동안 어려울 것으로 보인다.

IoT에 대한 정의 사례로서, 2005년 ITU에서는 IoT를 '모든 사물에게까지 네트워크 연결을 제공하는 네트워크의 네트워크'라고 정의했다. 2009년 CASAGRAS 프로젝트의 최종 보고서에서는 '데이터 캡쳐 및 통신을 통해 물리적인 오브젝트와 가상의 오브젝트를 연결하는 글로벌 네트워크 인프라'라고 정의했다. 위 두 가지 정의 사례는 IoT를 네트워크 관점에서 바라본 것이다. IoT를 네트워크 관점에서 바라보는 시각만 존재하는 것이 아니기 때문에 이와 같은 정의는 IoT의 특성을 제대로 표현한다고 볼 수는 없다. IoT를 사용자 중심의 서비스로 바라보는 시각도 존재하며, 또한, 지능형 사물로 보거나 거대한 빅 데이터 처리 플랫폼, 물리적인 센서 시스템, 소셜 네트워크의 한 부분으로 바라보는 다양한 시각이 존재하는 것이다.

IoT에 대한 다양한 시각 중에서 아래에 제시된 CERP-IoT 2009(Cluster of European Research Projects on the Internet of Things)에 의한 IoT 정의가 IoT가 지향하는 응용 서비스와 그 특성을 가장 잘 표현하고 있는 것으로 보인다. 그 정의를 보면 다음과 같다[2].

'IoT는 미래인터넷의 통합된 부분으로서 표준과 상호 호환 통신 프로토콜로 자가 설정 기능을 갖춘 동적 글로벌 네트워크 인프라로 정의될 수 있으며, IoT는 자기 식별자와 각각의 특성을 갖는 물리적인 사물과 가상 사물로 구성된다. 또한, 지능형 인터페이스를 가지며, 정보망에 잘 통합되는 특성을 갖는다. IoT에서의 사물은 비즈니스와 정보, 소셜 프로세스의 적극적인 참여자로서 사물간 혹은 환경과 데이터 및 센싱된 환경 정보를 상호 전달/반응할 수 있다. 사물은 자율적으로 물리적인 실환경 이벤트에 반응하거나, 인간의 직접적인 개입 유무와는 관련없이 서비스를 만들거나 특정 행위 동작을 촉발하는 프로세스를 실행한다. 서비스 형태에서의 인터페이스는 인터넷을 통해 이와 같은 스마트 사물과의 상호 작용을 촉진하고, 보안과 프라이버시 이슈를 고려하여 사물의 상태나 관련 정보를 질의 혹은 교환한다.'

위의 정의에서 알 수 있듯이 IoT는 센서/상황 인지 기술로 해석될 수도 있고, 통신/네트워크 기술, 칩 디바이스 기술, 경량 임베디드 네트워크 기술, 자

율적/지능형 플랫폼 기술, 대량의 데이터를 처리하는 빅데이터 기술, 데이터마이닝 기술, 사용자 중심의 응용 서비스 기술, 웹 서비스 기술, 보안/프라이버시 보호 기술 등 다양한 형태의 기술로 해석되거나, 통합된 기술로 해석될 수 있다. 이 때문에 본고에서 다루고자 하는 IoT 보안 기술의 적용 범위가 매우 광범위하고 복잡하다고 볼 수 있다. 필요로 하는 보안 기술도 현재 IT(Information Technology) 분야에서 전체에서 활용되거나, 필요로 하는 거의 모든 보안 기술을 필요로 한다고 볼 수 있다.

이에, 본고에서는 먼저 2장에서 IoT 보안 취약성과 보안 이슈를 살펴본다. 그리고 3장에서는 언급된 IoT 보안 취약성 중에서 IoT 구성 요소의 운영체제나 응용 서비스의 보안 취약성, 프로토콜 보안 취약성을 다루는 사이버 보안이나 물리적 보안 특성, 암호 구현상의 보안 이슈 등을 다루지 않고 IoT 디바이스와 프로토콜, 플랫폼, 서비스 상에서 보안 요구사항을 중심으로 IoT 보안 기술을 살펴보고자 한다.

Ⅱ. IoT에서의 보안/프라이버시 이슈

IoT는 전술한 것처럼 다양한 기술과 프로토콜로 구성된 복합체이며, IoT 센서/디바이스, 게이트웨이, 미들웨어 플랫폼, 서비스 플랫폼, IoT 서비스 등이 상호 유기적으로 결합되어 상호 작용을 하는 유기적인 관계를 가진다. IoT는 물리적인 구성 요소뿐만 아니라, IoT의 각 구성 요소들 간에 작용하는 통신/네트워크 기술, 데이터 마이닝 기술, 서비스 매쉬업 기술, 서비스 API 기술, 사용자 인터페이스 기술 등 다양한 기술 요소를 가진다. IoT 서비스는 전술한 물리적 구성 요소와 기술 구성 요소가 말단의 센서로부터 시작해서 사용자의 서비스까지 seamless한 통신 및 정보 전달이 이뤄지기 때문에, 각 구성 요소 각각에 특화된 보안 취약성이 존재할 뿐만 아니라, 구성 요소가 연결 부분에서도 다양한 보안 취약성이 존재할 수 있다. 또한, 각 구성 요소에는 존재하지 않던 보안 취약성이 연결됨으로서 새로운 보안 취약성이 존재할 수 있게 된다. 아래 표는 IT 분야에서 쉽게 찾아볼 수 있는 보안 취약성 및 공격 유형이다. 아래 표 1을 보면 이러한 기존의 IT 분야 보안 취약성이 IoT 환경에서도 그대로 존재하며, 심지어 이러한 보안 취약성에 대한 대응이 기존 방법보다 더욱 어려운 경우가 많다.

〈표 1〉에서는 기존 IT 시스템에서 존재하는 보안

〈표 1〉 IoT 환경에서의 보안 취약성 및 공격 유형[3]

보안취약성 및 공격 유형	IoT 상에서의 대상 분야
Worm과 virus	IoT 통신/네트워크, 디바이스, 게이트웨이, 플랫폼, 응용 서비스
DoS 및 분산 DoS	IoT 통신/네트워크
비인가된 접근	IoT 디바이스, 게이트웨이, 플랫폼, 응용 서비스
패치되지 않는 시스템 OS/OS 보안 취약성	IoT 디바이스, 게이트웨이, 플랫폼, 응용 서비스
Antivirus 소프트웨어의 부적절한 사용	IoT 플랫폼, 응용 서비스
방화벽의 부적절한 사용	IoT 통신/네트워크
비인가된 서비스 접근	IoT 응용 서비스
프로토콜 보안 취약성	IoT 통신/네트워크
비인가된 사용자의 접근	IoT 응용 서비스
복제 공격	IoT 디바이스, 게이트웨이
비인가된 I/O 접근	IoT 디바이스, 게이트웨이, 플랫폼, 응용 서비스
부적절한 시스템 로그 기록	IoT 플랫폼, 응용 서비스
설정 오류 및 실수	IoT 디바이스, 게이트웨이, 플랫폼, 응용 서비스
기밀성/무결성 공격	IoT 통신/네트워크, 디바이스, 게이트웨이, 플랫폼, 응용 서비스
안전하지 않은 패스워드	IoT 응용 서비스
보호되지 않은 펌웨어	IoT 디바이스, 게이트웨이
프라이버시 침해	IoT 플랫폼, 응용 서비스

취약성이 IoT 환경에서도 존재한다는 것을 보였다. IoT 분야에서는 <표 1>에 기술된 보안 취약성/공격 유형뿐만 아니라, IoT 서비스를 위해 각 구성 요소/기술 요소가 상호 유기적으로 조직됨에 따라 더욱 심각하게 다뤄지는 보안 취약성 유형이 존재한다. 이와 같은 대표적인 사례로서 프라이버시 침해 문제가 존재한다. IoT 서비스의 근간은 사물과 사물, 환경과 관련된 데이터를 센싱하여 이를 가공하여, 고급 정보 및 지식을 얻어 이를 활용하는 것이므로 적절한 프라이버시 침해 대응 기법을 제공하지 않는다면 해당 IoT 서비스를 사용할 수 없을 정도로 심각한 프라이버시 침해 문제가 발생할 수 있다. 특히 국내에서는 2011년 9월 30일부터 강화된 개인정보보호법이 시행되었기 때문에(실제는 2012년 10월 1일부터 시행됨. 1년 동안의 유예 기간을 둠) IoT 서비스 개발자 등, IoT 관련 분야 연구/개발자들이 프라이버시 침해 문제에 대해 적극적인 대응책을 세우지 않으면 IoT 서비스 활성화/상용화는 불가능한 것이다. 특히 강화된 개인정보보호법에는 정보 주체에 대한 자기 정보 통제권 부여를 원칙으로 언급하고 있기 때문에, 정보를 가공하여 다른 형태로 변환하여 활용하는 IoT 서비스의 기본 기능이 개인정보보호법에 의해 제약을 받을 가능성이 높다. 다음 장에서는 본 장에서 언급한 IoT 서비스에 대한 프라이버시 침해 문제에 대한 해결 방법과 IoT 분야의 대표적인 보안 취약성 해결 방법을 디바이스, 프로토콜, 플랫폼, 서비스 분야에서 각각 기술한다.

Ⅲ. IoT 보안/프라이버시 보호 기술

본 장에서는 IoT 분야의 대표적인 보안 취약성에 대한 대응책으로서 IoT의 주요 구성 요소인 디바이스, 프로토콜, 플랫폼, 서비스 분야의 보안 기술을 언급하며, 또한, IoT 서비스에서 더욱 중요하게 다뤄지게 될 프라이버시 보호형 데이터 마이닝 기법에 대해 기술한다.

3-1 IoT 디바이스에서의 경량 보안/인증 기술

IoT 디바이스의 보안을 위해서는 디바이스간 통신에서의 기밀성, 무결성 및 기기간 인증 측면에서의 보호를 고려해야 한다. PC를 기반으로 하는 전통적인 보안 체계에서는 주로 표준으로 정해져 있는 AES[4] 및 DES[5]를 이용하여 기밀성을 제공하였으며, SHA-1, SHA-2[6], MD5[7], 그리고 최근에 표준으로 제정된 SHA-3[8] 등의 해쉬 함수를 이용하여 무결성을 제공하거나, RSA[9]를 기반으로 하는 PKI를 통해서 인증 기능을 제공하였다. IoT의 구조를 웹의 관점에서 가장 잘 정의하고 있는 ITU-T의 Framework[10]에서는 IoT를 구성하는 디바이스를 연산이나 전력 측면에서 자원이 풍부한 non-constrained device와 자원이 풍족하지 않은 constrained device로 나누어서 정의하고 있다. 우리는 여기에서 앞서 살펴보았던 기존의 전통적인 암호 체계를 constrained device에 그대로 적용할 수 없음을 주목할 필요가 있다.

IoT를 구성하는 가장 핵심적인 요소 중 하나인 constrained device는 연산 능력과 저장 능력, 통신 능력 등에 있어 기존의 전통적인 암호 체계를 그대로 사용하기에 한계점을 가진다. 따라서 IoT Device와 같은 constrained device를 위한 경량의 암호 기술이 적용될 필요가 있다. 최근에는 국내외적으로 경량 암호에 대한 관심이 높아지면서, 다양한 경량 암호가 소개되고 있다. 대표적인 사례로써, PRESENT[11]의 경우 반복적으로 키 XOR 연산과 4비트 입출력을 가지는 Sbox와 64비트 permutation만을 수행함으로써 암호화를 수행한다. Katan과 Ktantan[12]은 2개의 LFSR을 이용한 구조를 가지며, HummingBrid[13] 알고리즘의 경우 rotor machine을 모티브로 만들어졌다. 국내에서도 경량 암호에 대한 연구가 많이 진행되었는데, Hight[14]의 경우 국내 표준으로 제정된 알고리즘으로써, 32 비트 단위의 연산과 다중 Feistel

구조를 기반으로 하며, 최근 개발된 LEA[15]의 경우, 덧셈, XOR, Rotate 등 단순한 연산만으로 구성된다는 특징이 있다. 무결성을 위한 해쉬 함수로는 최근 개발된 SHA-3를 비롯하여, Sponge Construction을 기반으로 하는 경량 해쉬 함수가 많이 등장하고 있다. Quark[16]은 Katan과 Grain[17]이라는 경량 암호를 모티브로 만들어졌으며, Photon[18]은 AES와 유사한 연산 구조를 가지도록 만들어졌다. Spongent[19]는 Present를 모티브로 하여 해쉬 함수를 구성하였다. 인증을 위한 기술로는 RSA보다 적은 비트의 키를 통해 유사한 안전성을 제공하는 타원 곡선 알고리즘[20]을 사용할 수 있다.

IoT에서 주로 사용될 것으로 생각되는 디바이스의 통신 기술은 Wi-Fi[21]를 비롯하여, ZigBee[22], DASH-7[23], Bluetooth[24] 등이 사용될 것으로 예상된다. Wi-Fi의 기밀성 및 무결성을 위한 WPA(Wi-Fi Protected Access) 기술의 경우 사전에 설정된 키를 기반으로 통신상의 트래픽을 암호화 하고, MAC을 통해 무결성을 제공하는데, 주로 이용되는 AES-CCMP (AES-Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)는 AES의 Counter 모드와 CBC 모드를 이용해 암호화와 무결성 체크 코드를 생성함으로써 기밀성과 무결성을 제공한다. ZigBee는 802.15.4의 물리 계층과 데이터 링크 계층을 활용한 통신 프로토콜로써, 802.15.4에서 정의하고 있는 AES-CCM을 확장한 AES-CCM*를 사용하고 있다. AES-CCM*는 AES-CCM이 제공하는 기밀성과 무결성을 필요에 따라 선택적으로 사용할 수 있도록 8가지의 모드를 제공하고 있다. DASH-7의 표준에서는 다양한 암호 알고리즘을 통한 상호 인증 프로토콜과 프레임 보호 기법을 정의하고 있다. 상호 인증을 위해서 사전에 분배된 키를 이용하는 방법과 AES와 SHA를 이용한 방법, HummingBird를 이용한 방법, 그리고 RSA, ECC 등의 공개키 비법을 이용한 방법 등이 정의되고 있다. 또한, 프레임을 보호하기 위한 기법으로 AES와 SHA1을 이용한 방법, AES를 이용한 CCM-7(CCM for ISO/IEC 18000-7)을 이용하는 방법, 그리고 HummingBird를 이용하는 방법 등이 정의되어 있다. Bluetooth는 최근까지도 새로운 표준이 제정될 정도로 계속해서 발전을 거듭하고 있으며, 세대를 거쳐 오면서 다양한 data rate와 통신 거리를 지원하는 스펙이 등장하였다. Bluetooth는 1세대의 BR(Basic Rate), 2세대의 EDR(Enhanced Data Rate)을 비롯하여, 3세대의 HS(High Speed)를 거쳐, 최근에 등장한 4.0에서는 LE(Low Energy)의 규격이 정의되었다. 보안 관련 체계는 BR/EDR/HS와 LE에 대해 다른 체계가 적용이 된다. BR/EDR의 경우 암호화를 위해 E_0라고 불리는 LFSR 기반의 stream cipher가 사용되며, 인증 과정에서는 SAFER+ 암호를 기반으로 하는 E_1 알고리즘이 사용된다. LE의 경우에는 프레임의 보호를 위해 AES-CCM을 사용한다.

3-2 IoT 플랫폼 보안 기술

IoT 플랫폼 상에서의 보안은 인터넷 상에서의 보안기술 및 모델과 큰 연관성을 가진다[25],[26]. 하지만 전통적인 인터넷 환경과는 달리 IoT 환경 상에서는 동일한 실행 환경이 제공되지 않으며, 일반적인 컴퓨터에 비해 연산 성능이 떨어져 통합된 형태의 보안 플랫폼을 제공하는 것이 어렵다. 이와 더불어 많은 수의 노드들 간의 통신과 노드 클러스트링 문제 또한 IoT 환경에서의 보안 고려 사항이다.

즉, IoT 이전 기술인 M2M 기술에서 기기들 간의 보안 통신을 위한 플랫폼이 중요시 되었다면 IoT에서는 M2M을 포함하여 인터넷에 연결 가능한 모든 전자기기와 컴퓨터 그리고 해당 기기들과 통신이 가능한 모든 기기들 간의 안전한 보안 플랫폼이 제공되어야 한다. 현재 IoT 보안 플랫폼은 IoT 시스템의 하위 단에서 부터 상위 단까지 발생하는 모든 문제점들을 해결하기 위해 설계되어 사용된다. 해당 문제점은 물리적 보안, 정보 획득 보안, 정보 전송 보

안, 정보 처리 보안을 포함한다[27],[28]. 먼저 물리적 보안의 경우, 악의적인 사용자가 환경 속에 설치된 저가의 태그와 센서에 접근하여 데이터 정보를 파악하거나 불법적인 인가작업이 할 수 없도록 안전한 암호화와 프로토콜이 사용되어야 한다. 정보 접근 및 획득에 대한 보안에서는 이기종의 기기들 간의 다중 미디어 스위칭 기술과 위치 관리 기술로 인해 발생하는 다중 정보 접근에 대한 보안 취약성을 제거하여야 한다. 또한, 무선 통신에서 사용되는 무선 인터페이스의 공개성으로 인해 전송되는 메시지가 캡쳐되어 변조될 위험도 있다. 해당 문제는 일반적인 무선 네트워크 환경에서 발생하는 문제와 동일하며, IoT와 같은 많은 수의 노드들이 통신하는 경우에는 denial of service 공격을 통해 네트워크를 마비시킬 수도 있으므로 이에 대한 보안 요구사항이 구비되어야 한다. IoT의 응용 단에서는 다양한 응용의 통합과 다양한 시스템에서의 정보의 처리를 통해 발생할 수 있는 정보의 누수를 막을 수 있어야 한다. 현재 이러한 보안 요구사항을 만족하기 위한 많은 연구가 진행되고 있으며, 다양한 신뢰 프레임워크가 제안되고 있다[29],[30]. 이러한 연구들을 종합해 보면 신뢰 플랫폼은 IoT 상에서의 보안 요구사항과 특징을 모두 만족하도록 되어 있다. 일반적인 신뢰 보안 시스템은 신뢰되는 안전한 관리 시스템과 보안 게이트웨이, 통합된 IoT 서비스 플랫폼, 보안 기반시설, 통한된 정보 교환 플랫폼으로 생각해 볼 수 있다. 이러한 신뢰 플랫폼을 통한 보안 제공은 인증되지 않은 사용자의 터미널 장비에 대한 접근을 효율적으로 막을 수 있는 장점을 가진다.

3-3 IoT 서비스 보안 기술

IoT 서비스란 사용자 중심의 서비스를 의미한다. 사용자 중심의 IoT 서비스를 구성하기 위해서 최근에는 WoT(Web of Things)와 같이 웹을 이용하여 서비스를 구성하여 사용자가 언제 어디서든지 서비스를 사용할 수 있도록 제공한다.

3-3-1 웹 서비스 보안

웹 서비스는 WSDL(Web Service Definition Language), UDDI(Universal Discovery and Integration of Business for Web), SOAP(Smple Object Access Protocol) 등 세 개의 표준으로 이루어진다.

안전한 웹 서비스를 제공하기 위해서는 특히 메시지 전송을 담당하는 SOAP의 기밀성, 무결성에 대한 고려가 필요하다. SOAP 보안은 OASIS에서 제안한 WS-Security(Web Services Security) 표준[31]으로 적극적으로 활성화 되었으며, 그 외에 W3C에서 제안한 XML Signature[32],[33]/Encryption[34],[35], XKMS 2.0[36], SOAP-SEC[36]과 OASIS에서 제안한 SAML[38],[39], XACML[40] 등이 있다.

IoT 웹 서비스를 구성하기 위해서 웹 서비스간의 통신을 위한 SOAP 뿐만 아니라, 디바이스 간의 통신을 위한 CoAP(Constrained Application Protocol)[41]을 사용한다. 현재까지 CoAP 보안을 위한 표준은 DTLS(Datagram Transport Layer Security)[42]이 있지만, 디바이스에서 구동하기 위해서는 CoAP 자체 보안을 개선해야할 필요가 있다.

3-3-2 ID 관리 기술

IoT 서비스를 제공하기 위해서 식별자(ID)와 인증정보를 설정하여 사용장 중심의 서비스를 제공할 수 있다. 최근에는 ID 관리 문제로 의한 개인정보 누출, 주민번호 도용 등의 문제가 발생하면서 사회적 관심을 받고 있다. 이러한 ID 관리 문제를 해결하기 위해서 국내외적으로 ID 관리에 대한 연구가 진행되고 있다. 2005년 Microsoft 사의 "Law of Identity"[43]을 만족하며, URL 기반으로 인증을 수행하는 OpenID 1.1/2.0[44],[45] 등을 비롯한 다양한 ID 관리 기술이 제안되었다. 국내에서는 한국전자통신연구원에서 CoT(Circle of Trust)[46]를 이용한 e-IDMS(ETRI-Identity Mana-

gement System)[47]가 있다.

3-4 IoT 프라이버시 보호 기술

일반적인 IT 환경에서의 프라이버시 보호 방법은 크게 다음과 같은 네 가지 방법이 존재한다.

- 정보 수집시 정보 주체로부터 수집 정보에 대한 동의 획득을 통한 프라이버시 보호
- 암호학적 기법을 사용한 프라이버시 보호
- 접근제어/권한 제어 기법을 통한 프라이버시 보호
- 시스템 보안을 통한 프라이버시 보호

정보 수집시 정보 주체로부터 센싱하고자 하는 대상 정보와 이를 어떤 IoT 서비스에 활용하고자 하며, 언제까지 이를 활용할 것이냐라는 점을 정보 주체에게 명확히 밝히고, 이에 대한 동의를 획득하는 것이 프라이버시 보호를 위한 첫 번째 단계다. 두 번째 언급된 암호학적 기법을 사용한 프라이버시 보호 기법으로는 주민 번호나 지문 정보 등 민감한 정보를 수집(센싱)하여, 이를 저장할 경우에는 개인정보 보호법에 의하면 반드시 암호화하여 저장하도록 하고 있다. 즉, 암호학적인 기법을 사용하여 데이터베이스를 암호화하거나 IoT의 통신/네트워킹 시의 정보에 대한 기밀성 제공, 이를 위해 필요한 키 관리 기법 등이 두 번째에 해당한다. 세 번째의 접근 제어/권한 제어는 역할 기반 접근 제어 기법(Role Based Access Control: RBAC)이나 속성 기반 접근 제어 기법(Attribute Based Access Control: ABAC) 등, IoT 구성 요소나 서비스 등에서 적절한 권한에 따른 인증/인가를 통해 정보에 대한 프라이버시 침해를 줄일 수 있게 된다. 마지막으로 IoT 구성 요소 시스템의 OS 보안 취약성이나 응용 서비스 보안 취약성 방지를 통해 불법적인 접근을 방지하거나 중요한 정보 유출을 막을 수 있게 된다.

전술한 네 가지 방법은 IoT 환경뿐만 아니라, 일반적인 IT 시스템에서 이미 적용하고 있는 전통적인 프라이버시 보호 기법이다. IoT 환경에서는 이 뿐만 아니라, IoT 디바이스로부터 센싱한 데이터를 가공하고 다른 센싱 정보와 융합(fusion)함에 따라 초기 정보에서는 프라이버시 침해가 일어나지 않았어도 가공된 정보(지식)에서는 프라이버시 침해가 발생할 수 있게 된다. IoT 서비스와 시스템을 구축하는데 있어서 이를 고려한 기술 개발이 필요하다. 구체적인 예로서, IoT 서비스에서 사용하는 데이터처리 및 데이터 마이닝 기법은 프라이버시 침해 가능성을 높이기 때문에 프라이버시 보호형 마이닝 기법(privacy preserving data mining)을 개발 및 사용할 필요성이 있다. 이에 대한 대표적인 네 가지 기술 유형을 소개하면 다음과 같다[48].

- 프라이버시 보존형 데이터 퍼블리싱 기법
- 데이터마이닝 결과 변형 기법
- 쿼리 감사 기법
- 분산 프라이버시 기법

프라이버시 보존형 데이터 퍼블리싱 기법은 데이터 처리 및 가공 후, 그 결과 값이 프라이버시 침해가 되지 않도록 변형을 가하는 기법이다. 예를 들어 결과 값에 난수 값(random number)를 특정한 통계적 분포로 추가하는 perturbed data 기법이 이에 해당한다. 이를 위한 기법으로는 난수화 기법(Randomization), K-익명성 기법(K-anonymity), L-다양성 기법(L-diversity) 등이 존재한다. 두 번째로 데이터 마이닝 결과값 변형 기법은 데이터 마이닝 알고리즘 자체를 변형함으로써 실현된다. 대표적인 예로서 Association Rule Hiding 기법이 존재한다. 쿼리 감사(Query Auditing) 기법은 쿼리 결과값을 수정하거나 제한하여 프라이버시 침해 정보에 대한 누출을 방지하는 기법으로서 Query Output Perturbation 기법, Query Restric-

tion 기법이 존재한다. 마지막으로 분산 프라이버시 기법은 데이터 분산화를 통해 프라이버시를 보호하는 기법으로 Pinka의 multiparty 프로토콜이 이에 해당한다.

Ⅳ. 결 론

본고에서는 다양한 기술과 프로토콜로 구성된 복합체이며, IoT 센서/디바이스, 게이트웨이, 미들웨어 플랫폼, 서비스 플랫폼, IoT 서비스 등, 구성 요소 간 상호 유기적으로 결합되어 원하는 특정 서비스를 수행하는 IoT 분야에 대한 보안 취약성과 이에 대한 보안 기술을 기술하였다. 본고에서 언급된 보안 취약성은 운영 체제나 응용 서비스의 보안 취약성, 프로토콜 보안 취약성, 물리적 보안 취약성, 암호 구현상의 보안 취약성 해결을 위한 보안 기술이 아닌 IoT 디바이스와 프로토콜, 플랫폼, 서비스 상에서 필요로 하는 보안 기술을 살펴보았다. 또한, IoT 서비스에서 더욱 중요하게 다뤄지는 프라이버시 보호 문제를 다루고 있으며, 이에 대한 구체적인 기술로 프라이버시 보호형 데이터 마이닝 기법에 대해 기술했다.

참 고 문 헌

[1] M2M/IoT 포럼, "http://www.m2miot.or.kr"

[2] CERP-IoT, "Internet of things - Strategic research roadmap", Sep. 2009.

[3] A. Wright, "Cyber security for the power grid: cyber security issues & Securing control systems", *ACM CCS*, Nov. 2009.

[4] J. Daemen, V. Rijmen, "AES proposal: Rijndael", *NIST AES Proposal*, 1998.

[5] NIST, FIPS PUB 46-3 Data Encryption Standard (DES), 1999.

[6] NIST, FIPS PUB 180-4 Secure Hash Standard, 2012.

[7] IETF, RFC-1321 The MD5 Message-Digest Algorithm, 1992.

[8] Guido Bertoni, Joan Daemen, Micahël Peeters, and Gilles Van Assche, "The Keccak reference", http://keccak.noekeon.org, 2011.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[10] ITU-T, "Framework of Web of Things", 2012.

[11] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher", In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 07)*, pp. 405-466, 2007.

[12] C. Cannière, O. Dunkelman, M. Knežević, Katan, and Ktantan - "A family of small and efficient hardware-oriented block ciphers", In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 09)*, pp. 272-288, 2009.

[13] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm", In *Proceedings of the 7th International Conference on RFID Security and Privacy(RFIDSec'11)*, pp. 19-31, 2011.

[14] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "Hight: a new block cipher suitable for low-resource device", In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 06)*, pp.

46-59, 2006.

[15] 국가보안기술연구소, "LEA", 2013.

[16] J. P. Aumasson, L. Henzen, W. Meier, and M. N. Plasencia, "QUARK: a lightweight hash", http://131002.net/quark, 2012.

[17] M. Hell, T. Johansson, A. Maximov, and W. MeIer, "A stream cipher proposal: Grain-128", In *IEEE International Symposium on Information Theory (ISIT 2006)*, 2006.

[18] J. Guo, T. Peyrin, and A. Poschmann, "The photon family of lightweight hash functions", in *Crypto 2011*, Lncs, vol. 6841, pp. 222-239, 2011.

[19] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varici, I. Verbauwhede, and Spongent: "The design space of lightweight cryptographic hashing", http:// sites.google.com/site/spongenthash, 2012.

[20] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, vol. 48, no. 77, pp. 203-209, 1987.

[21] Wi-Fi Alliance, http://www.wi-fi.org

[22] ZigBee Alliance, http://www.zigbee.org

[23] DASH7 Alliance, http://www.dash7.org

[24] Bluetooth, http://www.bluetooth.org

[25] O. Savry, F. Vacherand, "Security and privacy protection of contactless devices", In *The Internet of Things*, pp. 409-419, 2010.

[26] P. de Leusse, P. Periorellis, T. Dimitrakos, and S. K. Nair, "Self managed security cell, a security model for the internet of things and services", In *Advances in Future Internet, 2009 First International Conference* on, pp. 47-52, 2009.

[27] J. Zhang, M. Liang, "A new architecture for convertged internet of things", In *Internet Technology and Applications*, *International Conference* on, pp. 1-4, 2010.

[28] B. Zhang, X. X. Ma, and Zhi-Guang Qin, "Security architecture on the trusting internet of things", *Journal of Elecrtonic Science and Technology*, 2011.

[29] L. Hongpei, "What is trusted network architecture", *Network & Computer Security*, no. 2, pp. 36-38, 2005.

[30] Z. Yanwe, W. U. Zhenqiang, and Y. E. Jiangca, "Study of new trusted network framework", *Computer Application*, vol. 29, no. 9, pp. 2535-2565, Sep. 2009.

[31] OASIS, Web Services Security: SOAP Message Security 1.0(WS-Security 2004), http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf, Mar. 2004.

[32] J. Reagle, "IETF RFC2807 XML Signature Requiremets", Jul. 2000.

[33] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core, Feb. 2002.

[34] W3C, XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenccore, Dec. 2002.

[35] W3C, Decryption Transform for XML Signature, http://www.w3.org/TR/xmlencdecrypt, Dec. 2002.

[36] W3C, XML Key Management Specification (XKMS) Ver 2.0-Candidate Recommendation, http://www.w3.org/TR/xkms2, Apr. 2004.

[37] W3C, SOAP Security Extensions: Digital Signature, http://www.w3.org/TR/2001/NOTE-SOAP-dsig-20010206, Feb. 2001.

[38] OASIS, Web Services Security: SAML Token Profile - working drafts, http://www.oasis-open.org/committees/download. php/7837/WSS-SAML-15.pdf, Jul. 2004.

[39] OASIS, Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees /security, Jul. 2004.

[40] OASIS, eXtensible Access Control Markup Language(XACML) Version 1.0 - Standards, Feb. 2003.

[41] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol(coap)", 2013.

[42] E. Rescorla, N. Modadugu, "Datagram transport layer security", 2006.

[43] K. Cameron, The Laws of Identity, http://www.identityblog.com/?page_id=354, May 2005.

[44] D. Recordon, B. Fitzpatrick, OpenID Authentication 1.1, http://www.openid.net/specs/openidauthentication-1_1.txt, May 2006.

[45] D. Recordon, D. Reed, "OpenID 2.0: a platform for user-centric identity management", In *Proceedings of the Second ACM Workshop on Digital Identity Management*, pp. 11-16. ACM, 2006.

[46] T. Wason, "Liberty ID-FF architecture overview", *Liberty Alliance Project*, 2004. http://www.projectliberty.org/specs

[47] 조영섭, 진승헌, 문필주, 정교일, "ID 연계 기반의 인터넷 ID Management System: e-IDMS", 전자공학회논문지, 43, 2006년.

[48] 김호원, 제 4회 스마트그리드 보안 워크샵, 2013년 7월.

≡ 필자소개 ≡

서 화 정

2010년 2월: 부산대학교 정보컴퓨터공학부 (공학사)
2012년 2월: 부산대학교 컴퓨터공학과 (공학석사)
2012년 2월～현재: 부산대학교 컴퓨터공학과 박사과정 재학중
[주 관심분야] IoT, 정보보호, 타원곡선 암호

이 동 건

2009년 2월: 부산대학교 정보컴퓨터공학부 (공학사)
2011년 2월: 부산대학교 컴퓨터공학과 (공학석사)
2011년 2월～현재: 부산대학교 컴퓨터공학과 박사과정 재학중
[주 관심분야] IoT, 정보보호, 부채널공격, 오류주입공격, VLSI Design

최 종 석

2011년 2월: 동명대학교 정보보호학과 (공학사)
2011년 3월～2013년 2월: 부산대학교 컴퓨터공학과 (공학석사)
2013년 3월～현재: 부산대학교 컴퓨터공학과 박사과정
[주 관심분야] IoT, 모바일 보안, 페어링 암호, 분산시스템 보안

김 호 원

1993년 2월: 경북대학교 전자공학과 (공학사)
1995년 2월: 포항공과대학교 전자전기공학과 (공학석사)
1999년 2월: 포항공과대학교 전자전기공학과 (공학박사)
1998년～2008년: 한국전자통신연구원(ETRI) 정보보호연구단 선임연구원/팀장
2008년～현재: 부산대학교 정보컴퓨터공학부 부교수
[주 관심분야] IoT, 스마트그리드 보안, RFID/USN 보안, PKC 암호, VLSI, Embedded System 보안