IoT 센서 데이터의 속성기반 암호화를 통한 안전한 서비스 모델 개발*

함나연[1], 김형종[1]

[1]서울여자대학교 정보보호학과

A Study on a secure model with attributes-based encryption(ABE) of IoT sensor data

Na-Youn Ham, Hyung-Jong Kim

Division of information security, Seoul Women University

요 약

인터넷을 통해 다양한 사물들을 연결하는 IoT의 시대가 도래하면서 데이터의 통신 또한 활발하게 이루어지고 있다. 하지만 개인 정보나 산업 정보와 관련된 데이터들이 무분별하게 통신 되면서 개인 정보의 침해가 우려되고 있다. 이에 따라 적절한 기준에 따라 암호화를 하고, 권한을 가진 사용자만이 복호화를 할 수 있도록 하는 정책의 필요성이 대두되고 있다. 이에 특정 속성과 일치하는 수신자만이 데이터를 열람할 수 있도록 하는 속성기반 암호화(ABE)정책을 사용하여 데이터의 허가 받지 않은 접근을 차단할 수 있다. IoT 센서의 데이터에 속성기반 암호화를 적용하면 개인의 속성을 기반으로 암호화가 이루어지며 속성의 집합과 일치하는 경우에만 복호화가 가능하다. IoT 센서들의 활용과 함께 데이터 암호화의 표준이 요구되고 있는 지금, 속성기반 암호화를 적용한 정책은 안전한 통신과 더불어 IoT의 활용을 증가시킬 수 있을 것으로 기대된다.

Keyword: IoT, Attribute Based Encryption, Privacy Protection

I. 서론

IoT 기기와 서비스의 규모가 커지면서 IoT의 센서 데이터를 이용한 통신 또한 활발하게 이루어지고 있다. 2020년까지 130조의 기기가 연결되어 가정, 의료, 산업 등 다양한 분야에서 활용될 것으로 예측된다[1]. 하지만, IoT의 성장과 더불어 IoT 보안의 필요성은 사이버 보안에서 제일 중요한 사안으로 대두되고 있다. 특히 센서를 사용하는 데이터의 경우 센서의 값들이 허가되지 않은 접근으로 인한 유출이 될 위험이 크다. 데이터의 무분별한 접근은 센서 데이터를 통해 개인의 현재 위치나 심장 박동수 같은 생체 정보에도 접근할 수 있으며 카메라 센서 데이터에 접근해 개인의 사생활도 침해할 수 있다는 문제가 있다. 2017년 FDA에서는 심장 박동 조절 장치의 송신기에 권한이 없는 사용자가 환자의 RF에 원격으로 액세스할 수 있다는 성명문을 발표했다. [2] 이러한 문제점을 해결하기 위해 속성기반 암호화 (ABE) 정책을 통해 센서 데이터를 개체의 속성에 따라 암복호화를 실시할 수 있도록 할 수 있다. 본 논문에서는 속성기반 암호화를 통해 IoT 센서 데이터가 안전하게 통신 될 수 있는 서비스 모델에 대해 제안하였다. 2장에서는 IoT 장치 간 통신에 관한 연구와 속성기반 암호화를 이용한 연구에 대해 소개하고, 3장에서는 속성기반 암호

*이 연구는 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2017R1D1A1B03034644).

화를 IoT 데이터에 적용한 서비스 모델에 대해 제안하고 있다.

II. 기존연구

2.1 IoT 장치 간 통신에 관한 연구

IoT 통신환경에서 사용되는 암호화 방식은 현재 대칭 키 암호화, 공개 키 암호화 방식을 사용한 인증 등이 사용되고 있다[3]. 국내에서는 세션 키 방식을 이용해 IoT 암호화 기술을 설계한 연구가 진행되었는데, 인증 및 키 관리를 위한 서버를 따로 추가하여 IoT 기기 사이에서 등록, 인증 중계, 세션 키 관리를 담당함으로써 데이터 암호화와 서버의 진위를 따지는 추가적인 인증 처리를 가능하게 하였다. 공개 키 암호화 방식을 사용한 인증기술을 변형하여 세션 키 공유를 할 수 있으며, 추가적인 인증을 통해 인증 및 키 관리 서버를 확인할 수 있다. 또한, 암호화 키가 유출되었을 때 세션키 방식으로 대처할 수 있다는 점을 시사하였다.

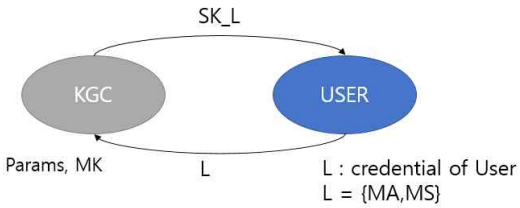
2.2 속성기반 암호화를 이용한 연구

속성기반 암호화는 ID 기반 암호화 (IBE)의 확장된 개념으로 각 개체의 속성을 기초로 암호화, 복호화가 실시되는 구조이다[4]. 해당기술을 메신저 환경에 적한 연구가 국내에서 제안되었으며, 디바이스 간의 안전한 암호화와 키 동기화 기능을 가능하게 하여 스마트 폰 기기 분실, 변경에 따른 메시지 동기화를 제안하였다[5]. 또 다른 연구에서는 속성기반 암호화 기술을 이용해 다중 서버 패스워드 프로토콜을 제안하였다[5]. 패스워드 인증 키 교환 프로토콜은 서버와 클라이언트가 서로 인증하고 키를 교환하는 알고리즘이다. 속성 기반 암호화 방식을 이에 적용하여 속성 값을 패스워드로 하여 별도의 키를 생성하지 않고, 공개키로 서버를 암호화 하는 방식을 고안하였다.

III. 연구내용

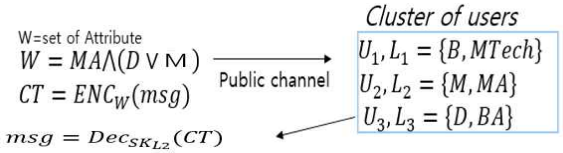
3.1 속성기반 암호화 배경지식

속성기반 암호화는 1-to-1 방식을 사용하는 PKE와 IBE 방식과는 달리, 1-to-many 방식을 사용하여 브로드캐스트의 문제를 해결할 수 있다는 장점이 있으며 Fine-Grained 접근제어를 사용한다는 특징이 있다. 개체의 속성 정보의 집합과 속성의 접근 구조를 바탕으로 암복호화를 실시하는 방식으로, 접근 구조를 암호화시에 지정하는 CP-ABE(Cipertext-Policy)와 키 생성이 접근구조를 지정하는 KP-ABE(Key Policy)로 나뉘게 된다.



[그림 1] KGC 키 발급 과정

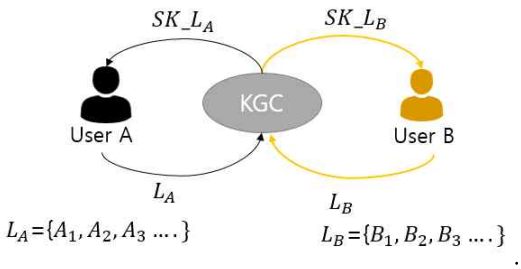
여기서는 암호문 생성시 접근구조를 사전에 정의하는 CP-ABE로 서비스를 설계하였다. 다음은 ABE가 사용자에게 키를 발급하는 과정이다. [그림 1]의 KGC는 Key Generation Center로 , 키 발급 센터이다. 사용자는 자신의 정보인 L를 KGC로 전송하고, KGC는 사용자의 속성을 Params와 MK(Master Key)로 받아 사용자를 식별하는 SK_L을 보내게 된다. 사용자의 개인 정보를 기반으로 한 키 발급이 이루어진 후에 암호화, 복호화가 가능하다. 다음 예시는 암호화와 복호화가 이루어지는 과정이다. 사용자들의 속성의 집합인 W로 메시지를 암호화하여 전송하며, 사용자의 속성으로 다시 복호화하게 된다. 학교 데이터베이스를 예시로 들었을 때, 복호화 규정인 W는 MA(Math)학과이고 학위는 D(Doctor) 이거나 M(Master)인 경우만 복호화가 가능하다고 규정하고 있다. 메시지인 msg는 KGC에서 사용자의 속성을 기반으로 발급하였던 비밀키를 기반으로 보호하게 된다. 속성의 집합에 의해 CT로 암호화 된 상태인 것이다. Cluster of Users에서 규정과 일치하는 U_2인 사용자가 복호화를 할 수 있는 속성을 갖게 되고 그 외의 사용자들은 접근이 제한되게 된다. 복호화는 암호문인 CT에 권한이 있는 사용자 U_2의 속성인 L_2를 기반으로 복호화 하게 된다.



[그림 2] 속성기반 암호화, 복호화 과정

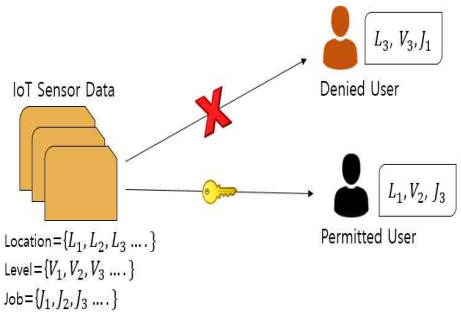
3.2 서비스 개요

제안하는 시스템은 키 발급기관 KGC(Key Generation Center), 데이터를 전송하는 IoT기기, 사용자 USer A와 UserB로 이루어져 있다. 제안하는 서비스에서 사용자들은 통신에 앞서 KGC에서 자신의 속성을 기반으로 키를 발급받아야 데이터 암, 복호화를 할수 있다고 가정한다. 이때 속성은 사용자를 식별할 수 있는 다양한 개인정보가 될 수 있다. 본 서비스에서는 사용자가 IoT기기와 데이터 통신을 할 때, 통신되는 데이터에 속성기반 암호화를 적용하였다. 사용자의 속성을 기반으로 데이터를 암호화 한 뒤, 일치하는 속성일 시에 복호화를 하는 것으로 고안하였다.



[그림 3] UserA ,UserB의 키 발급예시

위 그림은 UserA와 UserB가 암호화와 복호화를 하는 절차이다. 우선 User A와 User B는 키 발급센터인 KGC에서 통신에 사용할 키를 발급 받기 위해 자신의 속성 집합인 L_A와 L_B을 KGC로 보낸다. 그리고 KGC에서는 이 속성 집합을 기반으로 비밀키 SK_ L_A와 SK_L_B를 보내준다. 이때, 사용자가 보내는 속성은 개인의 생체정보, 실시간 위치 등 센서로 측정될 수 있는 다양한 데이터가 될 수 있다. KGC에서 발급 받은 키로 IoT 기기와 데이터를 주고받을 때, 데이터를 암호화하게 된다. 복호화 시에는 사용자의 속성 집합으로 생성하였던 비밀키를 기반으로 사용자의 속성과 일치하는 경우에 한 해, IoT의 데이터를 복호화할 수 있도록 한다. 키를 발급 받은 다음, IoT Sensor Data에 접근할 수 있다.

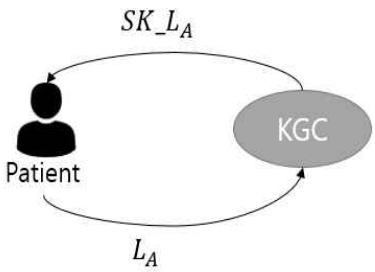


[그림 4] 권한 승인과 거절의 과정

Location	Level	Job
L_1	V_2	J_3
L_3	V_3	J_1

[표 1] 속성기반 암호화 규정

Location, Level, Job등 다양한 개인의 속성의 집합이 있을 시, 복호화 규정은 [표 1] 와 같이 구성될 수 있다. 이 규정과 일치하는 $\{L_1, V_2, J_3\}$, $\{L_3, V_3, J_1\}$의 속성을 가진 사용자만이 복호화 권한을 가질 수 있다. 따라서 [그림 4]와 같이 승인된 사용자와 거절된 사용자로 분류될 수 있다. [그림 5]는 속성기반 암호화를 헬스케어 IoT 데이터 센서에 적용하였을 때의 암호와와 복호화 예시이다.

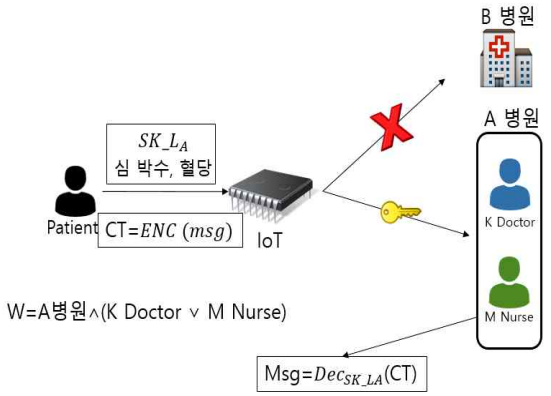


L_A= {이름,나이, 주소, 주치의, 담당 병원, 기타 의료정보 ...}

[그림 5] 헬스케어 IoT 사용자의 키 발급 과정

우선, 자신의 이름과 나이, 주소 등 기본적인 개인정보와 주치의, 담당 병원 등 기타 의료정보를 키 발급센터에 보내 자신의 속성을 기반으로 한 비밀키 SK_{L_A}를 발급받는다. 발급 받은 키SK_{L_A}로 환자는 헬스케어 IoT 서비스에

자신의 심박수나 혈당 같은 센서로 측정되는 의료 데이터를 CT로 암호화 한다. 사용자가 사전에 정의한 데이터 복호화 규정이 W라고 가정한다면, A 병원에 한해서, K의사와 M간호사만이 이 환자의 데이터 정보를 볼 수 있다. 한편 B 병원은 데이터에 접근할 수 있는 속성을 갖고 있지 않기 때문에 권한이 없다. 복호화의 과정은 암호화된 데이터 CT를 다시 SK_{L_A}를 기반으로 복호화 하는 것이다.



[그림 6] IoT 센서 데이터의 암복호화 과정

Ⅳ. 결론

본 논문에서는 현재 사용되고 있는 IoT 장치 통신과 속성기반 암호화에 대해 알아보았다. IoT 통신은 앞으로도 계속해서 증가하고 있는 추세이지만, 이에 대한 암호화의 정책은 미비한 편이다. 이에 본 논문에서는 IoT의 센서 데이터 통신에 속성 기반 암호화를 적용하여 암호화와 복호화시에 개인의 속성을 기반으로 데이터에 접근할 수 있는 방식을 제안하였다. 속성 기반 암호화를 적용할 시, 기존의 암호화 방식을 제공할때와는 달리, 1-to-many의 방식으로 통신을 할 수 있을 뿐만 아니라, Fine-grained접근 제어를 사용할 수 있는 장점이 있다. 이는 IoT 데이터 통신의 보안성과 효율성을 동시에 높여 줄 수 있는 방법을 제시하여 IoT의 활용을 더 높여줄 수 있을 것이다.

[참고문헌]

[1]“Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015,”Gartner, last modified: Nov. 11. 2014, accessed Nov. 11, 2018, https://www.gartner.com/newsroom/id/2905717

[2] “Cybersecurity Vulnerabilities Identified in St. Jude Medical’s Implantable Cardiac Devices and Merlin@home Transmitter,” FDA, last modified: Jan. 9. 2017, accessed Nov. 11, 2018, https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm

[3] 박종빈, 전준걸, 최안철. "사물인터넷 장치 간 End-to-End 정보 보안전송을 위한 암호화 기술 스터디와 세션 키 방식 보안기술의 설계." 대한전자공학회 학술대회, (2017.11): pp. 987-989.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. “Attribute-based encryption for fine-grained access control of encrypted data,” Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, pp. 89-98. 2006

[5] 김연태, 김효승, 조효진, 이동훈. “속성기반 암호화 기법을 이용한 안전한 메신저 시스템,” 보안공학연구논문지, 12(5), (2015.10) pp. 469-486

[6] 박민경, 조은상, 권태경. "속성 기반 암호화 방식을 이용한 다중 서버 패스워드 인증 키 교환." 한국통신학회논문지, 40.8 (2015.8): 1597-1605.