속성 숨김 및 효율적인 매치 테스트를 지원하는 속성 기반 IoT 데이터 공유 프로토콜

전우진 [1], 유동현 [2], 이제민 [1]
[1] 성균관대학교 전자전기컴퓨터공학과, [2] 대구경북과학기술원 전기전자컴퓨터공학과
dnwls0116@g.skku.edu, xaos4715@dgist.ac.kr, jemin.lee@skku.edu

Attribute-based IoT data sharing protocol supporting hidden attribute and efficient match test

WooJin Jeon[1], Donghyun Yu[2], Jemin Lee[1]
[1]Department of Electrical and Computer Engineering, Sungkyunkwan University,
[2]Department of Electrical Engineering and Computer Science, DGIST

요 약

본 논문은 Internet-of-things (IoT) 데이터 공유 환경에서 다수의 수신자에게 안전하고 효율적으로 데이터를 전달할 수 있는 보안 프로토콜을 제안한다. 기존의 속성 기반 암호화를 재 디자인하여 활용함으로써 속성 기반 접근 제어를 가능하게 할 뿐만 아니라 암호문에 속성이 드러나는 기존의 문제점을 해결해 데이터에 대한 완전한 기밀성을 지원한다.

Ⅰ. 서 론

IoT 는 4 차 산업 혁명의 핵심 기술들 중 하나로, 사물들과 인터넷을 연결하여 정보와 데이터를 공유하는 기술이다. 그러나 대부분의 IoT 기기들은 안전하지 않은 무선 채널을 통하여 데이터를 공유한다. IoT 데이터에는 IoT 기기의 사용자의 프라이버시와 관련된 민감한 개인 정보가 포함될 수 있기 때문에 데이터의 노출 및 위조는 심각한 위험을 초래할 수 있다.

이러한 문제를 해결하기 위해 다양한 일대일 보안 프로토콜이 제안되었다 [1]. 그러나 다수의 수신자에게 데이터를 공유해야 할 경우, 수신자 수만큼 프로토콜이 수행되어야 하므로 낮은 계산 리소스를 가진 IoT 기기에 적용되기에는 비효율적이다.

우리 연구에서는 속성 기반 암호화 기법을 사용하여 다수의 수신자들에게 안전하고 효율적으로 데이터를 공유할 수 있도록 한다. 또한, 속성 기반 암호화에서 속성이 드러나는 문제를 해결하여 데이터에 대한 정보 노출이 발생하지 않도록 하였다.

본 논문에서는 시스템 모델 및 보안 요구사항을 제시하고, 기존의 속성 기반 암호화를 재 디자인한 새로운 속성 기반 암호화를 소개한 후, 연구에서 제안하는 IoT 데이터 공유 프로토콜을 설명한다. 마지막으로 보안 분석을 통해 프로토콜의 안정성을 입증한다.

Ⅱ. 시스템 모델 및 보안 요구사항

본 논문에서는 그림 1 과 같이 IoT 기기, 클라우드 서버, 다양한 데이터 수신자들, 그리고 trust authority (TA)가 있는 시스템 모델을 고려한다. 모든 엔티티들이 신뢰할 수 있는 기관인 TA 는 시스템 파라미터를 생산 및 관리하며 시스템 내 사용자들에게 안전하게 키를 분배한다. IoT 기기는 생산한 데이터를 암호화하고 이를

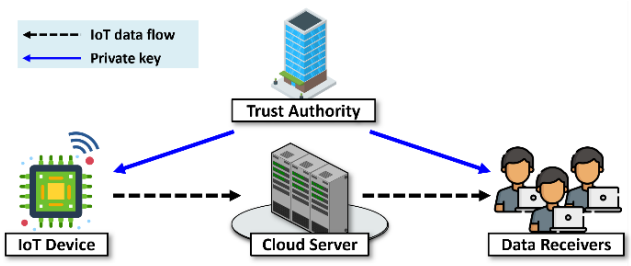

그림 1. IoT 데이터 공유 시스템 모델

클라우드 서버를 통해 수신자들에게 전송한다. 클라우드 서버는 IoT 에게 받은 암호문을 저장 및 데이터 수신자들에게 전달해주는 역할을 한다. 데이터 수신자는 수신 받은 암호문의 속성 집합이 자신의 속성 정책과 만족하는 지에 대한 매칭 테스트를 실시하고, 테스트가 통과할 경우 복호화를 진행해 데이터를 얻는다.

IoT 데이터 공유 환경에서 요구되는 보안 요구사항은 다음과 같다.

1. 기밀성 (Confidentiality): IoT 기기에서 보내는 암호문에 포함된 데이터는 기밀이어야 한다.
2. 무결성 (Integrity): 데이터가 네트워크를 거쳐 수신자에게 전달될 때까지 데이터의 내용이 변경되거나 손상되어서는 안 된다.
3. 상호 인증 (Mutual authentication): 프로토콜을 수행하는 상호 엔티티들은 서로가 합법적인 엔티티인지 인증 및 검증해야 한다.
4. 접근 제어 (Access control): IoT 기기가 보내는 데이터는 적합한 권한을 가진 수신자들만 접근할 수 있어야 한다.
5. 속성 숨김 (Hidden attributes): 접근 제어를 지원하기 위해 활용되는 암호문의 속성들은 데이터에 대한 정보를 포함하고 있기 때문에 외부로 드러나서는 안 된다.

K_{CS-IoT_i}	***Cloud Server***와 IoT_i간의 대칭 키
K_{CS-R_j}	*Cloud Server*와 $Receiver_j$간의 대칭 키
$sk_{\mathbb{A}_j}$	$Receiver_j$의 개인 복호화 키
$tk_{\mathbb{A}_j}$	$Receiver_j$의 매칭 테스트 키
$HKP.Enc(pk, m)$	메시지 m을 공용 키 pk를 이용하여 속성 기반 암호화
$HKP.Test(C, tk_{\mathbb{A}_j})$	암호문 C를 $tk_{\mathbb{A}_j}$를 이용하여 매칭 테스트
$HKP.Dec(C, sk_{\mathbb{A}_j})$	암호문 C를 $sk_{\mathbb{A}_j}$를 이용하여 속성 기반 복호화
$E_K(\cdot)$ & $D_K(\cdot)$	대칭 키 K 로 암호화 및 복호화
$H(\cdot)$	해시함수
N	Nonce 값

표 1. 제안된 프로토콜에서 사용되는 기호 및 의미

III. 속성 기반 암호화

본 논문에서는 key-policy 속성 기반 암호화 (Key-policy attribute-based encryption, KP-ABE)[2]를 재디자인한 Hidden-attribute KP-ABE (HA-KP-ABE)를 제안한다. HA-KP-ABE 는 데이터 송신자에 의해 정의된 속성 집합으로 데이터를 암호화하고, 암호문의 속성 집합이 개인키에 종속된 접근 정책을 만족할 경우 복호화가 이루어지는 형태의 공개 키 암호화 기법이다. 다만 기존 KP-ABE 와 다르게 HA-KP-ABE 의 암호문에는 속성 집합이 드러나지 않는다.

제안된 프로토콜은 HA-KP-ABE 를 사용하여 암호문의 속성을 숨긴 채 데이터를 공유하고, 또한 매치 테스트 알고리즘을 수행하여 수신자가 권한이 있는 데이터에 효율적으로 접근할 수 있도록 한다.

IV. IoT 데이터 공유 프로토콜

본 섹션에서는 제안된 프로토콜에 대해 서술한다. 표 1 은 제안된 프로토콜에 사용되는 기호들에 대해 설명한다. 프로토콜이 수행되기 전, 안전한 채널을 통하여 TA 가 각 엔티티들을 검증 및 각각에게 적합한 개인키를 전송하는 과정이 선행된다고 가정한다. 이러한 가정에 기초하여, IoT 데이터 공유 환경을 위해 제안된 프로토콜은 그림 2 와 같다.

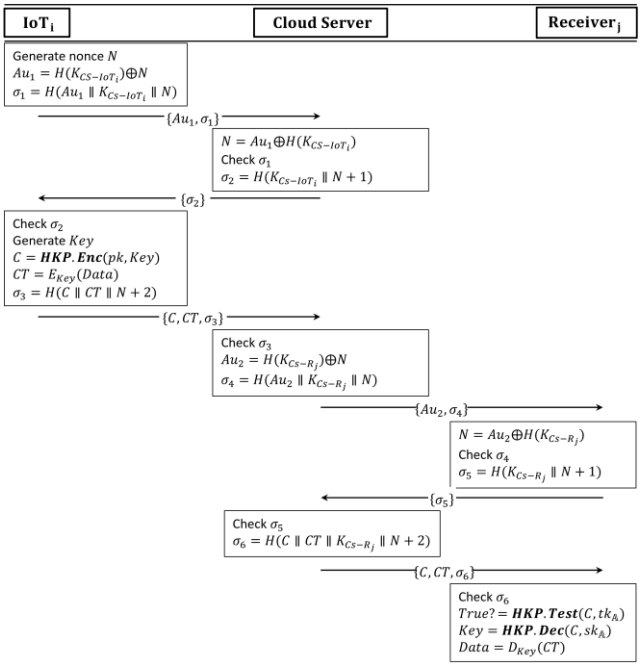

그림 2. 속성 숨김 및 효율적인 매치 테스트를 지원하는 속성 기반 IoT 데이터 공유 프로토콜

V. 보안 분석 및 결론

본 섹션에서는 제안된 프로토콜이 앞서 제시된 보안 요구사항들을 만족하는지 분석하여 프로토콜의 안정성을 입증한다.

1. 기밀성 (Confidentiality): 제안된 프로토콜에서는 Data 가 안전하게 교환되는 대칭 키 Key 로 암호화되어 공유된다. 대칭 암호화의 안정성을 통하여 데이터의 기밀성이 보장된다.
2. 무결성 (Integrity): Data 와 대칭 키가 암호화된 C 와 CT 는 σ_6 을 생성시에 필요하므로 수신자가 이를 검증함으로써 무결성을 확인할 수 있다.
3. 상호 인증 (Mutual authentication): 각 엔티티는 전송되는 $\sigma_1, \sigma_2, \ldots, \sigma_6$을 생성 및 검증함으로써 상호 인증을 수행한다. 해당 값은 TA 에게 받은 개인키를 소유한 경우에만 생성 가능하므로 해당 값에 대한 검증을 통해 상호 인증이 보장된다.
4. 접근 제어 (Access control): 데이터의 암호화에 사용된 속성 집합이 개인키에 종속된 속성 정책을 만족하는 경우에만 수신자는 $HKP.Dec$ 을 통해 Key를 얻어 데이터를 접근할 수 있다.
5. 속성 숨김 (Hidden attribute): $HKP.Enc$ 를 수행하여 생성된 암호문 C 에는 암호화에 사용된 속성 집합이 암호화되어 포함된다. 적합한 수신자 외에는 $HKP.Test$ 를 통과할 수 없으므로 속성 집합에 대한 정보를 얻을 수 있다.

제안된 프로토콜은 안전한 IoT 데이터 공유를 위해 보장 되어야하는 기밀성, 무결성, 상호 인증, 접근 제어, 그리고 속성 숨김을 만족함을 확인할 수 있다.

본 논문에서는 KP-ABE 를 변형한 HA-KP-ABE 를 활용하여 속성 숨김 및 효율적인 매치 테스트를 지원하는 속성 기반 IoT 데이터 공유 프로토콜을 제안하였고, 이에 대한 보안 분석을 통하여 안정성이 입증됨을 확인하였다.

ACKNOWLEDGMENT

본 연구는 정부(과학기술정보통신부)의 재원으로

한국연구재단의 지원을 받아 수행되었습니다 (No.

2020R1A2C2008878).

참 고 문 헌

[1] H. Huang, S. Lu, Z. Wu, & Q. Wei, “An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, pp. 1-21, Jul. 2021.

[2] Y. Rouselakis, & B. Waters, “Practical constructions and new proof methods for large universe attribute-based encryption,” in *Proc. ACM Conf. Comput. Commun. Secur.*, Nov. 2013, pp. 463-474.