http://dx.doi.org/10.14400/JDC.2016.14.10.295

IoT 환경에서 속성기반 암호화 기술을 활용한 메시지 통신 기법에 관한 연구

박중오
성결대학교 파이데이아학부

A Study of Message Communication Method Using Attribute Based Encryption in IoT Environment

Jung-Oh Park
Paideia College Dept. of Paideia, Sungkyul University

요 약 ICT 강국을 중심으로 국가자원에서 IoT기반의 기술을 지원하고 있으며, 기업 및 연구소에서도 기술 개발 및 생태계 조성을 위해서 활발히 연구되고 있다. 서울시의 도로 곳곳에서는 IoT기반의 공공시설이 도입되고 있으며, 사용자들로부터 다양한 서비스 및 편의성을 제공하고 있다. 하지만 IoT의 본격적인 도래와 발전을 위해서는 보안 및 프라이버시 침해와 생명과 안전에 대한 위협하는 사례가 빈번히 발생하고 있다. 또한 IoT 환경은 기존의 센서 네트워크, 이 기종 통신 네트워크, IoT 환경에서 최적화된 Device 등 다양한 환경기술을 포함하고 있으므로 기존의 보안 위협 및 다양한 공격 기법을 계승한다. 그러므로 본 논문에서는 IoT환경에서 안전한 통신을 위한 속성기반 암호화기술에 대해서 연구한다. 디바이스에서 수집된 데이터를 속성기반의 암호화 기법을 활용하여 전송하며, 키 생성 프로토콜을 설계하여 디바이스와 사용자에 대한 등급 및 권한을 식별하여 안전한 메시지를 전송하도록 한다. 성능평가를 수행하여 기존의 RSA 알고리즘 대비 암호화, 서명부분에서 대략 69%, 40%의 향상된 속도를 확인하였으며, IoT환경에서 발생하는 보안위협에 대해서 안전성을 분석하였다.

주제어 : 속성기반 암호화, 메시지 통신 설계, 사물인터넷, 접근제어, 인증

Abstract Many countries, especially ICT powers, are supporting IoT-based technology at a national level and this technology is actively being researched in the businesses and research institutes in an aim to develop technology and create an ecosystem. Roads in the Seoul city are building public facilities based on IoT to provide various services and conveniences for the users. However, for the full-fledged introduction and development of IoT, there are many cases where infringement on security and privacy and threat for life and safety happen. Also, as the IoT environment includes various environment technologies such as the existing sensor network, heterogeneous communication network, and devices optimized for the IoT environment, it inherits the existing security threat and various attack techniques. This paper researches the attribute based encryption technology for safe communication in the IoT environment. The data collected from the device is transmitted utilizing the attribute based encryption and by designing the key generation protocol, grades and authorities for the device and users are identified to transmit safe messages.

Key Words : Attribute Based Encryption, Access Control, IoT, Authentication, Message Communication

Received 2 September 2016, Revised 1 October 2016
Accepted 20 October 2016, Published 28 October 2016
Corresponding Author: Jung-Oh Park(Sungkyul University)
Email: jopark02@sungkyul.ac.kr

ISSN: 1738-1916

1. 서론

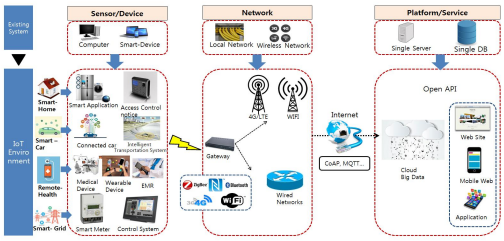
최근 IoT기반의 기술들은 급격히 발전되고 있으며 주변의 환경에서 접할 수 있다. 또한 다양한 디바이스와 스마트홈, 스마트 가전, 스마트 카, 스마트 그리드, 헬스케어, 웨어러블 디바이스 등과 같은 서비스가 제공되고 있다[1,11]. 2015년 네트워크기반에서 연결된 디바이스가 대략 49억대에 이르고 있으며, 2020년에는 250억대에 이를 것으로 전망하고 산업적인 측면에서 기여할 것을 예상하고 있다. 다양한 서비스와 편의성을 제공하여 효율성 있는 서비스를 제공하고 있으나 보안 및 프라이버시 침해에서 위험요소를 직면하고 있다[2,12]. 또한 IoT환경은 기존 센서 네트워크, 이기종 통신 네트워크, IoT 환경에서 최적화된 Device 등 다양한 환경기술을 포함하고 있어 기존의 발생하는 보안위협 및 다양한 공격 기법을 계승한다[3, 13]. 본 논문에서는 기기에서 수집된 데이터를 통신할 때 등급에 알맞은 사용자로부터 안전한 메시지를 전송할 수 있는 속성기반 암호화 기법에 대해서 연구한다. 그리고 키 생성 프로토콜을 연구하여 사용자 속성기반을 참고하여 권한 및 등급에 따른 메시지 프로토콜을 설계한다.

본 논문은 구성은 다음과 같다. 2장에서는 IoT 보안위협 및 보안 요구사항, 속성기반 암호화 알고리즘에 대해서 관련연구를 다룬다. 3장에서는 설정 및 키 생성, 기기 등록, 통신 프로토콜을 제안하며, 4장에서는 제안된 프로토콜의 안전성 분석 및 효율성 평가 및 보안성을 분석한다. 5장에서는 본 논문의 향후연구계획에 대해 결론을 제시한다.

2. 관련연구

2.1 IoT 보안위협 및 보안 요구사항

미래의 IT 산업의 새로운 기회로 부상하면서 다양한 환경에서 활용되고 있는 IoT는 사용자들로 하여 폭넓은 서비스가 진행되고 있다. 연구기관 및 기업에서는 다양한 디바이스들이 네트워크 환경에서 자유롭게 연결되고 호환성을 높이기 위해 연구되어 지고 있다[3, 4, 11]. IoT 기반의 구성도 및 시스템은 [Fig. 1]과 같다.



[Fig. 1] System Configuration based on IoT

<Table 1> Security Requirement in IoT Environment

Security requirements	Explanation
Confidentiality	SR-C1 : The messages transmitted between the IoT devices should be safely encrypted to prevent wiretapping and sniffing.
	SR-C3: Among the data collected in IoT devices, the encryption key and important data should be safely processed and saved to prevent information leakage.
	SR-C5 : IoT devices should manage the identifiable information to be processed safely for the prevention of duplication, theft, and leakage.
Integrity	SR-I1 : The IoT environment devices should provide the technology that verifies the integrity of data.
	SR-I2 : The controllable devices should provide the platform that can verify the integrity.
Availability	SR-A2 : IoT devices should provide a function that transmit the information on the equipment status to prevent physical destruction and abnormal installment.
	SR-A6 : IoT devices require a function that can set up safely to be incorporated into diverse environment safely.
Authentication/ Authorization	SR-AU1 & AU2 : IoT devices should provide the user authentication function to block the approach of the unauthorized users.
	SR-AU4 : IoT devices should provide the mutual authentication function to be applied to the various and autonomous communication environment safely.
	SR-AU7 : IoT devices should provide the function that can verify the identification number of the equipment to prevent the duplication, alteration, and theft.

사용자들로 단말기도 보급되고 대중화 단계에 이르기에 따라 보안관련 과제들이 이슈로 부상되고 있다. IoT 기술은 특성상 데이터를 생성, 보관, 처리하고 할 수 있으며 통신 기능과 함께 데이터를 확보할 수 있어 해커들의 공격기법들이 발생하고 있다. 특히 IoT 환경이 보급된 환경의 단말기는 연산능력이 단순하고 보안성도 많이 취

약하다[2, 6, 12, 18]. IoT기반의 자동주행차량시스템 역시 자동차와 연결되는 디바이스를 통하여 바이러스, 악성코드로 인해 작동오류를 발생시켜 대형 사고를 발생할 수 있다는 지적을 제기하고 있으며, 스마트 그리드환경에서는 전력공급을 차단시켜 재산 및 인명피해를 발생할 수 있다고 심각성을 주장하고 있다.

기업의 측면에서는 NAS나 라우터뿐만 아니라 휴먼머신 인터페이스와 같은 중요 기반의 집중적으로 공격이 시도될 것을 예상하고 있으며, Smart-Home, 자동화 및 보안시스템에서 취약점을 겨냥한 공격이 증가할 것으로 예상하고 있다. 또한 악의적인 사용자의 이해서 데이터 전송, 처리, 관리부분에서 데이터에 대한 유출이 발생할 수 있다.

위와 같은 보안위협을 대응하기 위해 사물인터넷표준(IoTFS-0060)문서에서 기밀성, 무결성, 가용성, 인증/인가 관련부분에서 보안요구 사항을 정의하고 있다[6, 7, 14].

2.2 속성기반 암호화 알고리즘

속성기반의 암호화 방식은 기존의 신원기반의 암호화 방식에서 파생되었으며 정보의 속성을 기반으로 암•복호화를 수행하는 방식을 정의한다. 대표적으로 CP-ABE (Ciphertext-Policy), KP-ABE(Key-Policy)가 있으며, 다중기관에서 속성을 관리하고 중간기관이 관리하여 키를 발급하는 속성 기반 알고리즘이 연구되고 있다.

2.2.1 Bilinear map

두 개의 곱셈 순환군 G1, G2,에 대해서 다음과 같은 성질을 만족하는 함수를 Bilinear map이라 정의한다[7,9,15].

- Bilinear : 임의의 군 원소는 g1, g2 ∈ G1 와 a, b ∈ Z에 대해 $e(g_1^a, g_2^b) = e(g_1, g2)^{ab}$가 성립된다.
- Non-degenerate ; g ∈G1의 생성원은 e(g,g) ≠ 1에 대해서 만족해야 한다.
- Computability : 임의의 생성원 G1에서 e(g1,g2)를 계산할 수 있는 효율적인 알고리즘이 존재한다.

2.2.2 속성기반 암호화 알고리즘

다중 키 발급을 사용하는 속성기반의 알고리즘은 Global Setup, Auth Setup, KeyGen, Encrypt, Decrypt와 같은 5 가지 알고리즘으로 구성된다[8,10].

(1) Attribute Base Encryption Global Setup(GP, θ) -> Global Parameter : Security Parameter를 입력받은 후 Global Parameter를 생성한다. Global Parameter는 참여된 사용자들로부터 분배된다.

(2) Attribute Base Encryption Auth Setup(GP, θ) -> $\{Apk_\theta, Amk_\theta\}$: 발급기관은 θ번째 키를 Global Parameter를 입력받아 공개키/개인키를 생성한다.

(3) Attribute Base Encryption Key Gen(GID, Amk_θ, u, GP, θ) -> $Apk_{GID,u}$, Amk_θ : 기관들은 사용자의 GID기반으로 Amk_θ를 발급한다.

(4) Attribute Base Encryption Encrypt(M, Q, Apk_θ,GP) -> CT : 암호화를 수행하기 위해서 접근정책 Q,기관의 공개키 Apk_θ, Global Parameter 기반으로 암호문 Ciphertext 추출과정을 수행한다.

(5) Attribute Base Encryption Decrypt(Ciphertext, Q, Apk_θ,GP)

3. IoT 환경에서 속성기반 암호화 통신 프로토콜 설계

3.1 제안 시스템 구성도

<Table 2> Abbreviation

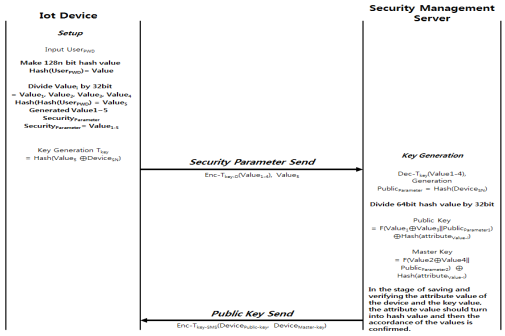
Sign	Description
$Security_{Parameter}$	Security Parameter
$Device_{SN}$	Device Serial Number
$Public_{Parameter}$	Public Parameter
$Master_{key}$	Master Key
$KeyServer_{nonce}$	Generation nonce of Key Server
T_{key}	Temporal Key
$Attribute_{value}$	Attribute Value
SMS_{nonce}	Generated nonce of Security Management Server
$User_{ID}$	Attribute Grade
$User_{pwd}$	ID of User
$Device_{Data}$	Password of User
$Timestamp$	Gather Data of Device

제안 시스템은 Iot환경을 기반으로 제안 프로토콜을 설계하였다. 속성기반의 암호화 방식을 활용하여 통신에서 수행되는 세션키 생성 및 발급 과정을 제안하였다. 그

리고 세션키 생성단계에서 사용자에 따른 권한 등급을 부여하여 사용자에 알맞은 접근제어 시스템을 설계하였다. 키 설정 및 생성 과정, 디바이스 등록 단계, 사용자 인증 및 통신 프로토콜 과정을 설계하였다. 제안 프로토콜의 약어에 대한 설명은 <Table 2>와 같다.

3.2 설정 및 키 생성 단계

사용자는 IoT Device를 사용하기 전 Secure Management Server에서 설정을 완료 후 공개키, 마스터를 생성 받은 후 등록 및 인증, 메시지 통신을 수행한다. 기존의 속성기반 암호화 방식에서 권한등급 값을 해쉬함수를 수행하여 접근제어 파라미터를 설계하였다. 사용자가 IoT Device를 활용하여 Security Management Server에서 공개키를 발급과정은 [Fig. 2]와 같으며 수행절차에 대한 설명은 아래와 같다.



[Fig. 2] Setup and Key Generation Phase

1. 사용자는 IoT Device에서 사용자가 알 수 있는 $User_{Pwd}$를 입력 한다. 이후 Device에서는 해쉬함수를 사용하여 128 Bit의 해쉬함수 값을 출력한다.

   $Hash(User_{Pwd}) = Value$

2. 생성된 해쉬값에 해쉬함수를 수행하여 파라미터 값을 생성한다. 해쉬함수을 수행하기 이전 생성된 128비트의 해쉬값을 32bit 단위로 나누고 각각의 값을 지정한다. (해쉬함수에서 생성된 파라미터 값을 나누어서 $Value_1$, $Value3$을 Public Key, $Value_2$, $Value_4$을 Secret Key로 사용함 비트단위로 나눈다.) 이후 사용자의 패스워드 값을 속성기반의 파라미터를 사용하기 위해 해쉬함수를 한 번 더 수행하여 임시키 값으로 파라미터를 암호화 수행하여 전송할 때 사용한다.

   $Value_i$ Split = $Value_1, Value_2, Value_3, Value_4$

   $Hash(Hash(User_{Pwd}) = Value_5$

3. 이후 임시키를 생성 후 Security Parameter를 Security Management Server로 전송한다.

   $Enc_{-Tkey}(Value_{1-4}), Value_5$

4. Security Management Server에서 수신된 메시지를 복호화 후 $Public_{Parameter}$를 생성한다.

   $Public_{Parameter}(Hash_{Device})$

5. $Value_{1-4}$ 의 해쉬값을 연접 후 32비트로 나눈 다음에 공개키, 마스터키를 생성한다. 공개키 및 마스터키를 생성할 때 $attribute_{Value}$의 값은 IoT 통하여 사용자의 Parameter 값을 기반으로 권한별 등급에 알맞은 값을 부여한다. $attribute_{Value}$값을 보호하기 위해서 해쉬함수를 수행한다.

   $Public = F(Value_1 \oplus Value_3 \| Public_{parameter1}) \oplus Hash(attribute_{Value})$

   $Master = F(Value_2 \oplus Value_4 \| Public_{parameter2}) \oplus Hash(attribute_{Value})$

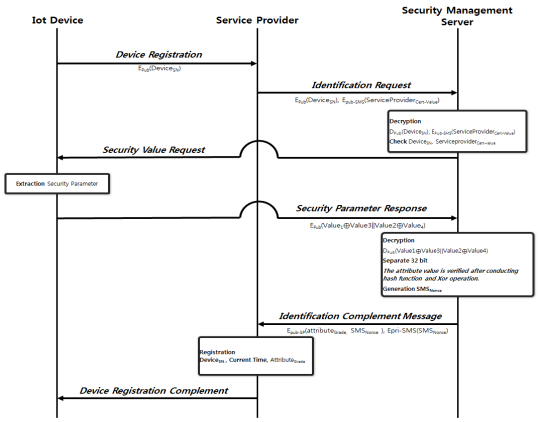
6. 생성된 Public Key와 Master Key는 생성된 임시키로 암호화를 수행 후 Iot Device로 전송한다.

   $Enc_{-Tkey-SMS}(Device_{public-key}, Device_{master-key})$

3.3 디바이스 등록 단계

사용자는 IoT Device를 사용하기 전 Secure Management Server에서 설정을 완료 후 공개키, 마스터를 생성 받은 후 등록 및 인증, 메시지 통신을 수행한다. 디바이스 등록 단계에 대한 프로토콜은 [Fig. 3]과 같다. 사용자가 IoT Device를 Security Management Server에 등록하는 단계를 수행한다. 사용자는 IoT Device를 Service Provider에 등록을 요청하고, Security Management Service를 통

하여 검증받는다. 이후 Device 등급을 부여 받고 등록 단계를 마친다.



[Fig. 3] Device Registration Phase

1. IoT 디바이스를 Service Provide에 등록한다. Service Provider에서는 Service Provider의 식별 값을 첨부하여 Security Management Server로 식별 요청 메시지 암호화 수행 후 전송한다.

$E_{Pub}(Device_{SN})$

$E_{Pub}(Device_{SN}), E_{Pub-SMS}(ServiceProvider_{Cert-value})$

2. Security Management Server에서는 수신된 메시지를 복호화 후 Device의 Serial Number, 식별 값을 검사한다. 이후 Device로부터 Security Value을 요청메시지를 전송한다.

$D_{Pub}(Device_{SN}), D_{Pub-SMS}(ServiceProvider_{Cert-value})$

Checking $Device_{SN}, ServiceProvider_{Cert-value}$

3. Iot Device는 메시지를 수신하고 $Security_{Parameter}$를 추출한다. 이후 추출된 $Security_{Parameter}$를 암호화 하여 Security Management Server로 발송한다.

$E_{pub}(Value_1 \oplus Value_3 \| Value_2 \oplus Value_4)$

4. 수신된 메시지를 복호화 후 연접된 값을 32비트 나눈다. 이후 속성 값을 해쉬함수를 수행하여 연산을 통하여 식별 요청 메시지를 검증한다.

$D_{pub}(Value_1 \oplus Value_3 \| Value_2 \oplus Value_4)$

4. 이후 Security Management Server에서는 $nonce$를 생성 후 Service Provider로 식별 완료 메시지를 전송한다.

$E_{pub-SP}(Attribute_{Grade}, SMS_{nonce})$,
$E_{pri-sms}(SMS_{nonce})$

5. Service Provider에서는 수신된 메시지를 복호화 후 $Device_{SN}$와 현재 시간, 속성 값을 저장한다. 이후 등록 완료 메시지를 전송 후 등록단계를 마친다.

3.4 사용자 인증 및 메시지 통신 단계

등록된 디바이스를 활용하여 사용자가 스마트 폰의 어플리케이션을 접속 후 디바이스로부터 수집된 메시지를 전송받는 단계이다. 사용자 인증 및 메시지 통신에 대한 프로토콜은 [Fig. 4]과 같다. 메시지를 전송받기 전에 사용자 인증을 수행하여 식별하고 이에 등급에 알맞은 메시지를 전송한다.

1. 사용자는 등록된 Device를 사용하여 서비스 요청 메시지를 전송한다.

$User_{ID}, E_{pub}(User_{Pwd})$

2. Service Provider에서는 Security Management Server로 인증 요청 메시지를 전송한다. 그리고 Security Management Server에서는 수신된 메시지를 복호화 후 $User_{ID}, User_{Pwd}$를 검사 후 사용자 정보를 등록한다.

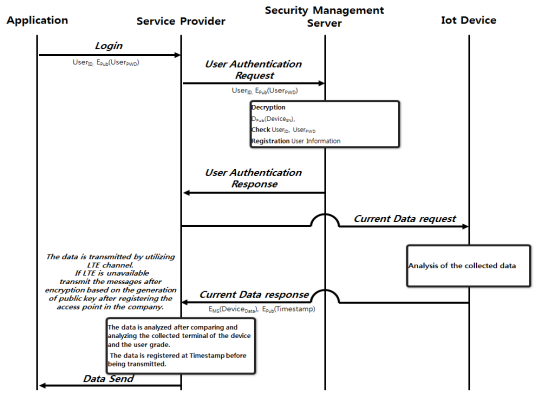
3. Security Management Server에서는 사용자 인증 완료 메시지를 Service Provider로 송신한다. Service Provider에서는 IoT Device로 수집된 데이터를 요청한다.

4. IoT는 수집된 데이터를 분석 후 Service Provider로 데이터를 전송한다.

$E_{MS}(Device_{Data}), E_{Pub}(TimeStamp)$

5. Service Provider에서는 수집된 데이터와 사용자의 등급을 비교분석 후 데이터를 전송한다. (LTE 채널이 아닌 Wi-fi를 통하여 데이터를 전송할 때는 회

사에서 등록되어 공개키를 발급받은 Access Point (유·무선공유기)를 통하여 데이터를 전송한다.) 그리고 Application으로부터 데이터를 전송하기 이전에 Timestamp를 등록한다.



[Fig. 4] User Authentication and Message Communication Phase

4. 성능평가

4.1 안전성 분석

데이터 위변조 및 기밀성의 보장 악화 : IoT 환경은 기존의 무선네트워크 환경에서 발생하는 공격기법을 계승하고 있으며, 신규 및 변종 공격에 대한 타겟이 될 수 있다. 중간자 공격, 재생공격과 같은 공격뿐만 아니라 악의적인 사용자에 의한 위장공격을 받을 수 있다. 이를 방지하기 위해서 기존의 암호화 방식이 아닌 속성기반 암호방식을 활용하여 데이터의 기밀성을 강화하였으며, 메시지 통신 및 디바이스 등록을 통하여 $Security_{Parameter}$, $ServiceProvider_{Cert-value}$, $User_{ID}$, $User_{Pwd}$을 검증 후 상호인증을 수행하여 데이터를 안전하게 전송하도록 설계하였다.

인가되지 않은 사용자의 접근제어 및 키 관리 : IoT Device는 비인가 된 사용자의 접근 및 도난/분실로 인하여 Device의 제어권을 획득하여 장치를 오남용할 수 있는 사례가 발생하고 있다. 하지만 본 논문에서는 Device의 접근제어를 강화하기 위해 설정 및 키 생성과정에서 $Security_{Parameter}$ 발급과정을 수행하였다. 그리고 디바이스 등록과정에서 $Security_{Parameter}$ 검증 및 공개키 및 마스터키를 활용한 식별 메시지를 검증하여 인가되지 않은 사용자의 접근을 차단하였다.

하이재킹 및 데이터 무결성의 위협 : 하이재킹은 종간과 종간과의 데이터를 가로채어 모든 작업을 감시 또는 제어할 수 있으며 사용자가 제공하지 않은 정보들은 누출될 수 있다. 네트워크 카메라, Iot기반의 스마트 환경, 스마트 헬스케어 환경에서 발생하고 있다. 이를 방지하기 위해서 속성기반의 암호화기능을 수행하여 종단과 종단과의 데이터의 무결성을 보완하였으며, 디바이스 등록 및 사용자인증 단계에서 공개키 검증 및 마스터키를 사용하여 암·복호화를 수행하여 데이터에 대한 무결성을 검증하였다.

데이터 수집으로 인한 사용자의 사생활 침해 유출 : Iot환경에서는 사용자의 등록된 사용자와 수집된 디바이스의 데이터에 대한 관리가 보장되어야 한다. 데이터에 대한 접근 권한 관리가 필수적이며, 권한등급에 알맞은 사용자로 데이터가 올바르게 전송되어야한다. 본 논문에서는 디바이스 등록단계에서 디바이스의 $Attrivute_{grade}$를 부여하였고, 메시지 인증단계에서는 사용자에 대한 등급을 비교, 분석하여 등급에 따른 알맞은 데이터를 전송하도록 설계한다.

4.2 효율성 평가 및 보안성 분석

본 논문에서는 제안한 암호기법의 효율성을 분석하기 위해서 윈도우(Windows 7 Enterprise) Intel(R) Core i7-4970(3.6GHz), 8.00 GB 메모리환경에서 Eclipse Tool을 활용하여 Java Code기반의 암복호화 성능을 비교분석하였다. 기존의 공개키 개인키 방식은 RSA, Identification Based Encryption(IBE)와 암호화방식을 비교분석 내용은 <Table 3>과 같다.

암호화 속도, 복호화 속도, 메시지통신의 암·복호화 수행속도, 서명과정에 대해서 비교분석하였으며, 수치는 나노세컨드로 나타내었다. 기존의 RSA, IBE(Identify based encryption)과 제안된 시스템(ABE : Attribute Based Encryption)기반의 암호성능 평가에서는 RSA보다는 암복호화 측면에서 대략69%, 서명부분에서 대략 40% 향상된 수치를 확인할 수 있었다. 그러나 IBE 부분

에서는 암복호화 측면 대략 38%, 서명부분에서는 23%의 저하된 수치를 확인하였다.

<Table 3> Comparison of Proposed Protocol and Existing System

Performance of Cipher System	RSA	IBE	Proposed Protocol (ABE)
Encryption	10744869	1953612	1873482
Decryption	7915449	1884630	1928342
Message encryption and decryption speed during communication	695436934	154540274	212129145
signature process speed	543900482	321729721	396541324

(Number Point : nanosecond)

기존의 IBE 암호성능보다는 효율성부분에서는 저하된 수치가 나왔지만, 본 논문에서 제안된 암호화방식은 IBE 암호방식의 진화된 방식으로 접근제어부분에서 보안성이 높다. 제안된 암호기법(ABE)은 안전성에 대한 특징으로는 Server가 공격을 당하더라고 T_{key}와 $Public_{Key}$만 누출되고 중요한 $Secret_{key}$는 상호인증으로 통하여 보존됨으로써 키 관리 부분에서 보안성이 높다[10, 13]. 속성기반의 암호기반을 활용하면서 $Attribute_{Value}$를 기반으로 Device와 사용자 등급에 알맞은 메시지를 전송할 수 있다. 그리고 설정 및 키 생성 과정에서 등급에 따른 알맞은 키를 생성, 관리를 수행함으로써 송신된 메시지에 대한 기밀성 및 데이터의 프라이버시를 강화할 수 있다.

5. 결론

본 논문에서는 IoT환경에서 기존의 PKI, IBE 암호시스템과는 달리 속성기반의 암호시스템을 적용에 대해서 연구하였다. IoT Device을 등록하기 이전의 설정 및 키 생성 절차를 수행하였다. 이를 기반으로 Device 등록과 사용자 인증 및 메시지 통신 시스템을 설계함으로서 안전하고 권한에 따른 알맞은 메시지를 송신할 수 있도록 설계하였다.

IoT환경에서 데이터의 기밀성, 무결성뿐만 아니라 인가되지 않은 접근제어, 데이터의 유출에 대한 프라이버시에 대한 보안위협을 방지하도록 설계하였다. 성능평가 부분에서 IoT환경에서 발생하는 공격기법에 대해서 안전성을 분석하였으며, 효율성을 평가하였다. 기존의 암호시스템 RSA, IBE과 제안된 암호시스템과의 비교분석하였다. 전체적인 성능부분에서는 RSA 암호화부분에서는 69%, 서명부분에서는 40%에서는 향상된 수치가 나왔으나, IBE에서는 전체적인 38%, 서명부분에서 28%에의 저하된 수치가 나왔다. 그러나 보안성 부분에서는 사용자 권한 및 키 관리 부분을 설계하여 안전한 통신을 수행할 수 있었다.

본 논문에서 제안된 기법은 Iot기반의 Smart Home, Smart Health Care, Smart Grid환경에서 접목하기 위한 통신 프레임 설계에 대한 연구가 필요하며, Device와 제어할 수 있는 Application에 대한 접근 정책 및 규정이 제정되어야 한다. 그리고 기존의 IoT환경에서 발생하는 공격기법 분석과 신규 및 변종공격을 방지할 수 있는 차단할 수 있는 연구가 요구된다.

REFERENCES

[1] Lee S. H, IoT Status and Major Issue, Insight 04 IIIP, 2014.

[2] Lee YS, N. Security Requirements for Drone-based IoT Services, TTA, 2015.

[3] Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. SoK: Secure Messaging. IEEE Symposium on Security and Privacy, 2015.

[4] Yeon Tae Kim, “Secure Messenger System using Attribute Based Encryption”, Journal of Security Engineering, Vol.12, No.5, pp.469-486, 2015.

[5] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." Advances in Cryptology - .EUROCRYPT, 2005. Springer Berlin Heidelberg, pp.457-473, 2005.

[6] Chase, Melissa. "Multi-authority attribute based encryption." Theory of cryptography. Springer Berlin, Heidelberg, pp.515-534. 2007.

[7] A. Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of

Technology, Technion, Haifa, Israel, 1996.

[8] Kossinets, G. and D.J. Watts, “Origins of Homophily in an Evolving Social Network”, American Journal of Sociology, doi:10.1086/599247, Vol.115, pp. 405-500, 2005.

[9] Ham J., J.N. Lee and J. Lee, “Understanding Continuous Use of Virtual Communities: A Comparison of Technical and Social Perspectives”, Journal of Information Technology Services, Vol.12, No.4, 2013.

[10] V. Goyal, et al., “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security(CCS '06), pp. 89-98, VA, USA, Oct. 2006

[11] Jeong-Ick Lee, “Convergent Case Study of Research and Education: Internet of Things Based Wireless Device Forming Research”, Journal of the Korea Convergence Society, Vol. 6. No. 4, pp. 1-7, 2015.

[12] Jun-Young Go, Keun-Ho Lee, “SNS disclosure of personal information in M2M environment threats and countermeasures”, Journal of the Korea Convergence Society, Vol. 5, No. 1, pp. 29-34, 2014.

[13] Keun-Ho Lee, “A Security Threats in Wireless Charger Systems in M2M”, Journal of the Korea Convergence Society, Vol. 4, No. 1, pp. 27-31, 2013.

[14] Yoon Ku Jeon, “Efficient Revocation Scheme for Ciphertext Policy Attribute-Based Encryption“, Hanyang University, 2011. 2.

[15] R.Ostrovsky, A.Shai, and B.Waters, "Attrobute-Based Encryption with Non-Monotonic Access Structures," 14th ACM conference on Computer and communications security, 2007.

[16] Sang-Jo Oh, Yong-Young Kim, “A Study on Organizations Adopting Convergence-based Smart Work for Overcoming Constraints and Achieving Performance”, Journal of Digital Convergence, Vol. 13, No. 6, pp. 113-124, 2015.

[17] Young-Jae Park, “Development of a ICT Convergence Business Model based on Smart Phone“, Journal of Digital Convergence, Vol. 13, No. 6, pp. 81-89, 2015.

[18] Jin-Woo Jung, Jungduk Kim, Myeong-Gyun Song, Chul-Gu Jin, “A study on Development of Certification Schemes for Cloud Security”, Journal of Digital Convergence, Vol. 13, No. 6, pp. 81-89, 2015.

박 중 오(Park, Jung Oh)

・2000년 7월 : 성결대학교 컴퓨터공학과 졸업
・2003년 3월 : 명지대학교 전자계산교육 석사
・2011년 8월 : 숭실대학교 컴퓨터학과 박사
・2013년 3월 ~ 2016년 2월 : 동양미래대학교 통신과 조교수
・2016년 3월 ~ 현재 : 성결대학교 파이데이아학부 조교수
・관심분야 : 암호학, IoT
・E-Mail : jopark02@sungkyul.ac.kr