Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.353

클라우드 컴퓨팅에서 안전한 사물인터넷 데이터를 위한 키 관리

성 순 화†‡
충남대학교 소프트웨어 연구소

Key Management for Secure Internet of Things(IoT) Data in Cloud Computing

Soon-hwa Sung†‡
Chungnam National University, Software Research Center(SOREC)

요 약

IoT 보안은 공유 목적을 위한 결함 없는 시스템과 일련의 규정을 필요로 하기 때문에 기술적 문제보다 더 필요하다. 따라서 본 연구는 IoT 데이터 보안을 위한 클라우드 컴퓨팅에서 IoT 데이터가 신뢰받을 수 있는 효율적인 키 관리를 제안한다.

기존 센서 네트워크의 키 분배센터와는 달리, 제안한 클라우드 프락시 키 서버의 연합키 관리는 중앙집중적 관리가 아니며, 능동적인 키 복구와 업데이트가 가능하다. 제안한 키 관리는 사전 설정된 비밀키 방식이 아닌 자율적인 클라우드의 클라우드 프락시 키 서버의 키 정보 공유로써, 키 생성과 공간 복잡도를 줄일 수 있다. 또한, 이전의 IoT 키 연구와는 달리, 클라우드 프락시 키 서버의 연합키는 데이터가 이동하는 동안에 유의미한 정보를 추출해 낼 수 있는 능력을 제공한다.

ABSTRACT

The Internet of Things(IoT) security has more need than a technical problem as it needs series of regulations and faultless security system for common purposes. So, this study proposes an efficient key management in order that can be trusted IoT data in cloud computing.

In contrast with a key distribution center of existing sensor networks, the proposed a federation key management of cloud proxy key server is not central point of administration and enables an active key recovery and update. The proposed key management is not a method of predetermined secret keys but sharing key information of a cloud proxy key server in autonomous cloud, which can reduce key generation and space complexity. In addition, In contrast with previous IoT key researches, a federation key of cloud proxy key server provides an extraction ability from meaningful information while moving data.

Keywords: Internet of Things(IoT), federation key management, cloud computing, proxy key server

I. 서 론

사물인터넷(Internet of Things:IoT) 기술은 다양한 물리 공간의 사물들과 가상 공간의 프로세스 및 데이터 콘텐츠들이 인터넷으로 상호 연결되어 초연결사회(hyper-connected society)를 구축한다. 이는 사용자 중심의 지능형 서비스를 제공하기 위해 거대한 정보가 활용되는 광범위한 기술이며, 작은 장

Received(02. 24. 2017), Modified(04. 07. 2017), Accepted(04. 07. 2017)

† 주저자, shsung@cnu.ac.kr
‡ 교신저자,shsung@cnu.ac.kr(Corresponding author)

치와 가상의 콘텐츠까지 연결하려는 초연결 인터넷 개념으로 자리 잡고 있다. 몇몇 전문가들은 사물인터넷은 컴퓨터, 인터넷, 모바일 통신 네트워크, 다른 산업 이후 새로운 정보 산업으로 예측하고 있다[1]. 그리고 이는 독립적인 연합 서비스와 응용 개발을 위한 기본으로서 개체 식별, 센서, 연결 능력 등을 제공한다[2,3].

인터넷에 연결된 장치 수의 증가는 공격할 수 있는 대상의 증가와 위협 요소의 확장으로 IoT 보안 기술을 요구한다. IoT 기술 특성 상 주변의 일상 사물들이 연결되므로 개인 정보 유출이나 프라이버시 침해가 우려되는 범위가 증가할 것이며, 그 침해 정도도 현재와 비교할 수 없을 정도로 증폭될 것이다. 따라서 IoT에 대한 인증과 기밀성, 데이터 무결성의 연구 관심이 더 많이 고려되고 있다[3,4]. IoT 서비스는 센싱 정보를 토대로 사람, 사물, 서비스의 통합 및 데이터 공유를 지향하므로 프라이버시 침해 발생은 필연적이다. 이러한 프라이버시 침해 문제를 해결하지 못할 경우, 전자주민증, 인체내장형 Radio Frequency Identification(RFID) 같은 IoT 서비스 활성화는 불가능하다.

IoT 시스템의 확장성은 보안에 있으며, 이러한 보안 문제는 센서 공격, 네트워크 콘텐츠 보안, 비인가 로그인, 침해 등이다. 또한 IoT는 정보 트래킹, 안전한 전자 제품 그리고 데이터 무결성 같은 다른 보안 장애물에 직면하고 있다.

IoT의 기술적 특성과 시스템 구조를 분석하는 기반에서, IoT의 키 기술은 매우 중요하다.

먼저, IoT 구조를 살펴보면 인식, 네트워크, 응용 단계로 나누어 볼 수 있다. 인식 단계의 주요 기능은 전체 인식으로써 RFID, 센서, 2차원 코드에 의해 언제 어디서나 정보를 습득할 수 있다. 인식 단계에서의 주요 기능은 RFID 기술, 센싱, 제어 기술로 칩 개발, 통신 프로토콜 연구, 스마트 노드 에너지 공급과 세그먼트를 포함한다.

네트워크 단계의 주요 기능은 실시간 정보를 전송하기 위하여 네트워크 통합을 통하여 데이터 인식과 정보 제어 사이 양방향 전송을 하는 것이다. 센서가 정보를 감지한 후, 사용할 네트워크를 통하여 그 배경을 이동한다. 네트워크 전송 정보 응용은 더 빠른 전송 속도, 더 넓은 대역폭, 더 똑똑한 접근과 네트워크 관리 등을 성장시키고 있다.

응용 단계는 특별한 서비스를 사용자에게 제공하기 위하여 데이터 분석과 진행을 한다. 클라우드 컴퓨팅 플랫폼은 많은 데이터를 저장하고 IoT의 중요한 부분뿐만 아니라 많은 응용의 기반이다. 응용 단계는 사물, 소프트웨어의 개발이 목적이며, 클라우드 컴퓨팅 기술로 사용자에게 IoT의 다양한 응용을 제공한다[5].

클라우드 컴퓨팅은 이용자의 모든 정보를 인터넷 상의 서버에 저장하고, 이 정보를 각종 Information Technology(IT) 기기를 통하여 언제 어디서든 이용할 수 있는 것으로 인터넷을 이용한 IT 자원의 주문형 아웃소싱 서비스라고 할 수 있다. 그러나 이는 서버가 해킹당할 경우 개인정보가 유출될 수 있고, 서버 장애가 발생하면 자료 이용이 불가능하다는 단점이 있다.

본 연구는 IoT 응용 단계의 서비스 활성화를 위하여 클라우드 컴퓨팅을 위한 안전한 센서 데이터를 지원하려고 한다. 이러한 클라우드 컴퓨팅 환경에서의 센싱 정보의 프라이버시를 위한 연속적인 키 인증이 가능한 키 관리를 제안한다.

본 논문 구성은 2장 관련 연구, 3장 클라우드 IoT 키 관리, 4장 클라우드 컴퓨팅의 연합 키 관리, 5장 분석, 6장 결론으로 구성된다.

II. 관련 연구

IoT는 여러 장치 사이의 수많은 데이터를 안전하게 전송하여야만 사용자 또는 기관에서 믿고 그 데이터를 사용할 수 있다. 다루기 힘들 만큼의 많은 센서 데이터를 보다 쉽게 사용할 수 있도록 지원하는 클라우드 컴퓨팅 기술을 도입할 수 있다.

클라우드 컴퓨팅은 아직 보안 문제가 존재하여 활성화되고 있지 않다. 일반적으로 데이터 위치를 알고 있을 때 데이터를 보호하기 위하여 암호화를 한다. 클라우드 환경에서의 암호화는 사용자가 원하는 데이터가 어디에 있는지 알지 못하므로 암호화할 키 관리 문제로 어려운 상황이다.

암호 기술로 데이터를 보호하기 위한 전통적이고 중앙집중적인 방법은 그룹키를 생성한 후, 각 그룹 멤버에게 이 키를 분산하는 것이다. 이러한 그룹키는 이전의 연구[6, 7, 8, 9, 10]의 좋은 결과에도 불구하고 중앙집권적인 제어기인 키 서버에 문제점이 있다면 전체 그룹은 영향을 받게 된다. 그리고 그룹키 계획안은 비싼 공개키 작동을 사용하고 있다. [11] 연구의 성능 분석과 실험은 트리 기반 그룹 디피 헬먼(tree-based group Diffie-Hellman)으로 가

장 효율적인 제안을 하였지만, 이는 클라우드 환경에 적용하기가 어렵다.

[12]연구에서는 IoT 장치의 낮은 보안 서비스 문제와 위협을 해결하기 위해 어떤 도구에 관하여 언급하였다. 이러한 해결은 전통적인 방법이며 카메라와 같은 모니터링 하는데 사용하는 장치이기 때문에 IoT 특성에 맞지 않았다.

한편, 데이터 손실과 데이터 위반이 2013년의 클라우드 환경에서 가장 큰 위협으로 인식되고 있다[13].

암호화는 대부분의 사람이 이해할 수 없는 복잡한 수학을 포함하고 있는 반면, 키 관리는 기술, 사람, 과정을 포함하므로 더 어렵다. 키 관리는 많은 데이터를 어떻게 보호하느냐를 제한하는 약한 연결이므로 예민한 데이터를 보호하려면 이를 정확하게 이해해야만 한다.

클라우드 컴퓨팅 환경에서 우리는 어디서나 민감한 데이터를 가지고 이러한 데이터 접근이 필요한 응용 능력을 요구한다. 이를 위하여, 우리는 클라우드 환경에서 데이터를 안전하게 보호 유지하기 위한 암호화키와 사용 가능할 데이터를 얻기 위한 복호화 키를 얻을 수 있는 어떤 응용 방법을 필요로 한다.

따라서 본 연구는 IoT 데이터를 위한 클라우드 컴퓨팅에서의 연합 키 관리를 제안한다.

III. 클라우드 IoT 키 관리

연합 키 관리는 다른 컴퓨터 시스템들이 함께 작동할 때 언급이 되며, 이는 다른 응용이 같은 키 서버로부터 키들을 어떻게 얻을 수 있는지를 포함한다. 이는 클라우드의 민감한 데이터를 보호하기 위한 암호화 되기 전에 필요로 하는 키 관리의 중요한 측면이며, 키 연합 능력 부족은 많은 암호와 키 관리의 유용성을 제한한다.

현재 시스템은 연합 키 관리를 실행할 수 없다. 이는 암호화 키들이 어떻게 다루어지는가를 자세히 살펴볼 필요가 있다. 즉 암호화 키는 항상 유일한 식별을 위한 키와 관련된 추가적인 정보를 가진다. 예를 들면, 테이프 구동 장치는 저장된 데이터를 암호화하기 위한 키를 얻을 때, 암호화된 데이터와 함께 저장된 유일한 키 식별자를 얻는다. 암호화된 데이터를 복호화하기 위하여 테이프 구동 장치는 암호화된 데이터와 함께 발견되는 키 식별자와 일치하는 키를 요구한다.

따라서 본 연구는 정확한 키를 얻을 수 있는 키 서버에 관한 정보를 포함하는 키 식별자 대신 클라우드 컴퓨팅에서 프락시 키 서버 기반 연합 키를 고려한다.

3.1 연합키 통신 방식

Fig.1은 데이터 통신 방식인 점대점(point-to-point) 방식과 다대다 방식을 나타내며, 클라우드 환경에서 점대점 방식은 다양한 곳에서 요구하는 데이터를 누가 어떤 데이터를 원하는지, 원하는 데이터를 원하는 곳으로 안전하게 전송할 수 있는 인증 절차가 복잡하며 이에 사용되는 키가 많아 키 관리가 비효율적이다.

다대다(many-to-many) 방식은 기존의 인터넷과 차세대 인터넷을 하나의 네트워크로 묶어, 마치 하나의 신경조직처럼 작동할 수 있게 제어하는 가상 슈퍼컴퓨터인 그리드(grid)로서 클라우드 컴퓨팅을 지원하는 모델이다.

본 연구는 다대다 방식을 바탕으로 한 IoT 응용 단계의 서비스 활성화를 위한 클라우드 컴퓨팅의 안전한 센서 데이터 지원을 위한 키 설계를 하려고 한다. 센서 데이터 파티별 인증을 위한 다대다 방식은 클라우드 환경의 프락시 키 서버(Proxy Key Server:PKS)를 도입하여 이 서버들의 연합 키로서 파티별 센서 데이터 인증 절차를 시작한다.

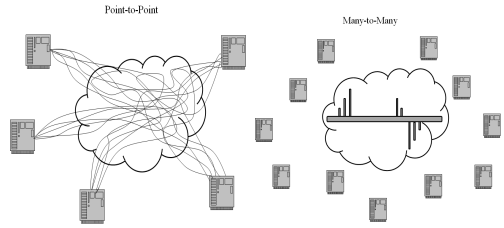

Fig. 1. Point-to-Point vs Many-to-Many in Data Communications

3.2 연합키 생성 과정

IoT 특성을 고려한 연합키는 많은 센서 데이터의 키 추가 및 제거가 용이할 뿐만 아니라 키 생성을 줄이고 통신 오버헤드를 줄일 수 있도록 지원하는 프락시 키 서버에서 진행된다. 클라우드 컴퓨팅 환경에서 적응할 수 있는 프락시 키 서버는 클라우드 마다 하나의 서버를 두어 연합키로서 키 정보를 공유한다.

연합키는 다음과 같은 과정으로 비밀키 s를 공유한다.

1. 다음과 같은 파티 $p_1, \ldots, p_n$ 사이에서 비밀 s를 공유한다.
 -어떤 $t < n/2$ 파티는 s에 대한 어떠한 정보도 가지지 않는다.
 -어떤 t+1 파티의 그룹은 비밀 s를 복구할 수 있다.
2. 신뢰된 중개인은 임의의 다항 a(X)를 선택한다.
 - $a(X) \in F_q[X]$, 차수 t와 $a(0) = s$
3. p_i 에 대하여 $s_i = a(i)$를 공유한다.
4. 주어진 집합 U의 t+1는 비밀 $s = a(0) = \sum_{j \in U} \lambda_j a_j$를 공유, 복구한다.
 - λ_i 는 U에 관한 라그랑즈 계수이다.

Fig.2에서와 같이 클라우드 A의 클라우드 서비스 제공자(Cloud Service Provider:CSP)는 프락시 키 서버 A에게 센서 데이터 파티 인증을 요청하면 프락시 키 서버A는 클라우드 B의 프락시 키 서버 B와 상호 통신하여 연합 키 결과로 센서 데이터 파티를 인증한다.

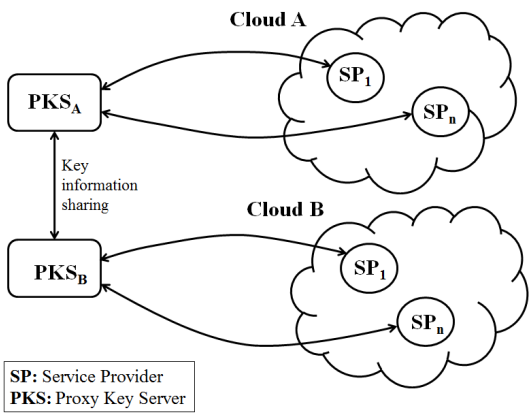

Fig. 2. Key Federation Scheme in Cloud

3.3 클라우드 IoT 서비스

인증 과정을 마치면 Fig.3에서와 같이 웹 서비스는 장치에서 장치로 센서 데이터 이동을 시작한다. 센서 노드들이 랜덤하게 배치되기 때문에 네트워크 토폴로지 정보를 사전에 획득하기 어렵다. 따라서 서비스 브로커가 필요한 서비스의 센서 데이터를 모아 연합키 생성을 프락시 키 서버에게 요청한다. 연합키 생성 요청을 받은 프락시 키 서버A는 연합키를 생성한 후, 다른 클라우드 프락시 키 서버 B와 연합키 정보를 공유한다.

클라우드 서비스 제공자의 센서 데이터 요청에 따라 프락시 키 서버A와 프락시 키 서버 B의 상호 통신으로 연합키 결과를 서비스 인터페이스를 통하여 클라우드 서비스 제공자에게 보낸다. 클라우드 서비스 제공자는 인증된 센서 데이터를 확인 후, 코어 서비스를 진행한다.

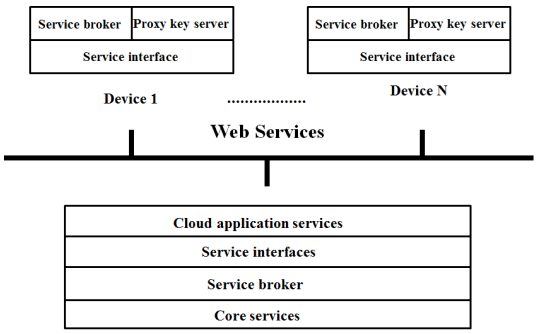

Fig. 3. IoT Web Sevices

IV. 클라우드 컴퓨팅의 연합 키 관리

프락시 키 서버는 두 개체(장치) A와 B 사이 안전한 데이터 통신을 위하여 두 가지 중요한 키 분산을 한다. 하나는 개체 A와 프락시 키 서버에게만 알려진 개체 A에 의해 사용될 새로운 키의 분산이다. 다른 하나는 프락시 키 서버가 개체 A와 B에 의해 사용될 세션 키의 분산이다. 이러한 키 분산은 배타적 논리합(exclusive OR)과 해시 함수 사용을 바탕으로 한다. 개체 A에 대한 새로운 키의 분산은 이러한 목적에만 사용되는 마스터 키를 기반으로 한다. Table 1에서와 같이, 두 개 장치의 응용 서비스를 위한 메시지 암호화에 필요한 새로운 키는 A_k, B_k, 응용 서비스를 위한 프락시 키 서버에 대한 새로운 키는 K_t, 개체 A에 대한 임시값은 A_n, 개체 B에 대한 임시값은 B_n, 프락시 키 서버의 임시값은 K_n으로 표시한다.

Table 1. Notation

Symbol	Description
O_A	Object A
O_B	Object B
A	Message of object A
B	Message of object B
K	Message of PKS
PKS_A	Proxy Key Server of Cloud A
PKS_B	Proxy Key Server of Cloud B
MK	Master Key
SK	Session Key
A_k, B_k	New key of object A, B
K_t	New key of PKS
K_n	Nonce of PKS
A_n	Nonce of object A
B_n	Nonce of object B

4.1 IoT 장치에 대한 키 분산

다음은 개체 A에 대한 응용 서비스를 위한 새로운 키 분산 과정이다.

1. $O_A \rightarrow PKS : A_n$
2. $PKS \rightarrow O_A : K_t, \ A_k \oplus H(MK, A_n, K_t), \ H(A_k, K_t), K_n$
3. $O_A \rightarrow PKS : H(A_k, K_n)$
4. $PKS \rightarrow O_A : H(A_k, A_n)$

위와 같이, 프락시 키 서버는 개체 A에게 전달하기 위해, 마스터 키 MK로 두 개 장치의 응용 서비스를 위한 메시지 암호화에 필요한 새로운 키 A_k, A_t를 생성하고, 임시값을 생성한다. 개체 A는 마스터 키 와 임시값 A_n를 알고 새로운 키 K_t가 주어지기 때문에, $x=H(MK, A_n, K_t)$를 생성할 수 있으며, $x \oplus (A_k \oplus H(MK, A_n, K_t))$로부터 A_k를 복구하기 위해 이를 사용한다. 개체 A는 $A_k \oplus H(MK, A_n, K_t)$를 위해 대체된 무효한 영역이 메시지가 가로채지 않았는지 체크하기 위해 $H(A_k, K_t)$를 사용한다. 즉 A_k이 프락시 키 서버가 보내려는 키인지를 체크하기 위해서이다.

두 개 장치의 응용 서비스를 위한 메시지 암호화에 필요한 새로운 키 K_t는 두 가지 목적을 제공한다. 첫째는 응용 서비스를 위한 개체 A의 메시지는 K_t없이 $A_k \oplus H(MK)$를 읽을 수 있고, $H(MK)$은 나중에 키들을 복구하기 위해 사용되므로 $H(MK)$을 발견하는 것은 마스터 키를 발견하는 만큼 유용하다. 서로 다른 K_t는 $H(MK, K_t)$를 생성할 때마다 하나의 값을 가지기 때문에 그가 $H(MK, K_t)$를 발견하는 것은 유용하지 않다. 둘째, K_t는 데이터 전송 동안 데이터가 분리되거나 다른 데이터로 대체되지 않게 보호하기 위한 메시지 요소들을 결합하는데 그 목표가 있다.

4.2 IoT 장치의 세션키

개체 A와 프락시 키 서버는 새로운 키를 사용하기 전에 응용 서비스를 위한 메시지 응답을 요구하고, $H(A_k, K_t)$는 제외될 수 있다. A_k에 대한 확인 기능은 응용 서비스를 위한 그 다음 메시지에 내재된다.

IoT 인증은 프락시 키 서버가 두 개체 사이 통신에 사용하는 세션 키를 어떻게 분산하는가를 확인 해준다. IoT의 두 개체 사이 기밀성을 제공하기 위해, 프락시 키 서버는 각 개체에 대한 임시값과 세션 키를 생성한 후, 그 이동은 다음과 같이 진행한다.

1. $O_A \rightarrow O_B : A, H(A_k, B), A_n$
2. $O_B \rightarrow PKS : A, B, H(B_k, A, K, H(A_k, B), A_n), A_n, B_n$
3. $PKS \rightarrow O_B : H(B_k, A, B_n) \oplus SK, H(B_k, A, B_n, SK), H(A_k, B, C) \oplus SK, H(A_k, B, A_n, SK)$
4. $O_B \rightarrow O_A : H(A_k, B, A_n) \oplus SK, H(A_k, B, A_n, SK)$

두 장치 사이의 데이터 기밀성을 위하여, 키 이동 순서는 개체 A에서 개체 B, 개체 B에서 프락시 키 서버로 진행된다. 프락시 키 서버는 개체 A와 B에게 세션 키 SK를 보내야 하며, 응용 서비스를 위한 새로운 키 A_k, B_k는 프락시 키 서버로부터 생성된다. 개체 A와 B는 세션 키를 찾기 위해 $H(A_k, B, A_n)$와 $H(B_k, A, B_n)$를 부호화할 수 있다. $H(A_k, B, A_n, SK)$와 $H(B_k, A, B_n, SK)$는 메시지가 방해받지 않았고, 유효한 세션 키가 복구되었는지 확인하기 위하여 개체 A와 B에 의해 확인될 수 있다. 개체 A와 B는 같은 세션 키를 복구할 수 있으므로 일반적인 세션 키를 가진다.

V. 분 석

제안한 키 관리 시스템은 클라우드 서비스 자원 데이터와 클라우드 프락시 키 서버의 키 데이터 동기화가 가능하며, 제안한 알고리즘의 시뮬레이션을 위해 그 수행은 주기적이다고 가정한다. 본 연구는 클라우드 컴퓨팅에서의 사물인터넷 데이터 보호를 위한 프락시 키 서버 관리를 제안함으로써, 키 관리 효율성을 높이기 위한 클라우드 프락시 키 서버의 연합키를 제안하였다. 클라우드 프락시 키 서버의 연합키 역할 가능성을 Table 2와 같이 분석하였다. Table 2는 클라우드 파운드리[14]에서 본 연구와 J. Park et al.[15]와 R. Hummen et al.[16] 연구들의 공간 복잡도, 키 관리의 확장성, 스케줄링, 키 철회 저항성, 네트워크 안전성을 비교 분석하였다.

공간 복잡도에서 r은 이웃 센서 노드 수, t는 요구된 센서 노드 철회 수행에 필요한 시간으로써 J. Park et al.[15]은 사물인터넷 장치 간 상호 인증을 위한 대칭키 인증과 세션키 합의 동의 시스템이 필요하므로 공간 복잡도가 이웃 센서 노드 수와 센서 노드 철회에 필요한 시간에 비례하므로 $O(r^2 \times t^2)$, R. Hummen et al.[16]은 인증을 위한 게이트웨이의 선 인증, 세션 회수, 핸드셰이크 위임이 필요하므로 $O(r \times t+3t)$, 제안한 계획안은 클라우드 프락시 키 서버의 연합키에 의한 $O(r)$로서 공간 복잡도가 낮음을 알 수 있다. 스케줄링은 클라우드 환경의 프락시 키 서버를 사용함으로써 제안한 계획안은 클라우드 환경이 아닌 [15], [16] 연구보다 우수하다.

[15]는 성능을 개선하기 위해 인증 완료된 장치가 세션키 선 계산을 해야 하므로 키 관리 확장성이 낮으며, [16]은 장치의 인증 오버헤드를 줄이기 위한 게이트웨이에서의 선 인증과 세션 회수로 키 관리 확장성이 낮은 반면, 제안한 계획안은 클라우드 컴퓨팅 프락시 키 서버의 연합키 관리로 키 관리 확장성이 높다는 것을 알 수 있다.

키 철회 저항성에서 제안 연구는 자율적인 프락시 키 서버의 키 관리로 높으며, [15]는 인증을 시도할 때마다 새로운 난수를 생성하여 인증에 사용하므로 낮으며, [16]은 장치의 핸드셰이크 위임으로 적은 자원으로 인증을 하지만 세션 회수로 부담이 있다.

네트워크 안전성에서 [15]는 장치 간 상호 인증과 세션키 동의를 제공하지만, 인증의 참여 장치들이 비밀키를 안전하게 공유하고 있다는 가정이 필요하며, [16]은 인증을 위한 게이트웨이에서의 선 인증, 세션 회수를 하지만 핸드셰이크 위임의 안정성 보장이 미비하다. 하지만 제안 연구는 클라우드 컴퓨팅의 네트워크 연결에서 프락시 키 서버의 능동적인 키 복구와 업데이트로 그 안전성이 보장된다.

Table 2. Analysis Comparison of the Proposed Scheme

Attributes	J. Park et al.[15]	R. Hummen et al.[16]	Our Scheme
Space complexity	$O(r^2 \times t^2)$	$O(r \times t+3t)$	$O(r)$
Key management scalability	low	low	high
Scheduling	low	low	high
Key revocation resistance	low	middle	high
Network security	middle	middle	high

VI. 결 론

본 연구는 IoT 보안의 필요성 부각과 그 데이터의 급성장이 맞물려 그 해결책을 클라우드 컴퓨팅에서 디자인했다. 이는 많은 데이터 처리를 이미 클라우드 컴퓨팅으로 접근하고 있는 현 시점에서 이를 호환할 수 있는 키 관리를 제안하였다. 제안한 프락시 키 서버의 연합 키 관리는 다중 보안 시스템을 통한 중앙 집중식 모니터링에 필요한 서버와 관리를 줄일 수 있다. 그리고 다른 추가적인 키 관련 정보 기술 없이, 보안을 위한 가장 최근 키의 복구와 통합을 업데이트할 수 있다. 이러한 키 관리는 앞으로 급속 성장할 IoT 센서 데이터를 클라우드 컴퓨팅에서 안전하게 처리할 수 있도록 지원한다.

References

[1] A Sajid, H Abbas, and K Saleem, "Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges," IEEE Access, vol. 4 pp. 1375~1384, Mar. 2016.

[2] Atzori, Luigi, Antonio Iera, and Giacomo Morabito, "The internet of things: A sur-

vey," Science Direct journal of Computer Networks, vol.54, no.15, pp.2787 - 2805, May 2010.
〔3〕 Yinghui H. and Guanyu L., "Descriptive models for internet of things," IEEE International Conference on Intelligent Control and Information Processing, pp. 483- 486, Aug. 2010.
〔4〕 Yuxi Liu and Guohui Zhou, "Key technologies and applications of internet of things," IEEE Fifth International Conference on Intelligent Computation Technology and Automation, pp. 197-200, Jan. 2012.
〔5〕 Huansheng N. and Ziou Wang, "Future internet of things architecture: Like mankind neural system or social organization framework?," IEEE Communication Letters, vol. 15, no. 4, pp. 461-463, Apr. 2011.
〔6〕 A. Perrig, D. Song, and J.D. Tygar. "ELK, A new protocol for efficient large-group key distribution," in Proceeding of the IEEE Symposium on Security and Privacy (IEEE S&P), pp. 247-262, 2001.
〔7〕 S. Setia, S. Koussih, S. Jajodia, and E. Harder, "Kronos: a scal-able group re-keying approach for secure multicast," in Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P), pp. 215 - 228, Jan. 2000.
〔8〕 A. T. Sherman and D. A. Mcgrew, "Key establish-ment in large dynamic groups using one-way function trees," IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444-458, May 2003.
〔9〕 Y. R. Yang, X. S. Li, X. B. Zhang, and S. S. Lam, "Reliable group rekeying: a performance analysis," in Proceeding of ACM SIGCOMM'01, pp. 27-38, Aug. 2001.
〔10〕 X. B. Zhang, S. S. Lam, D. Y. Lee, and Y. R. Yang, "Protocol design for scalable and reliable group rekeying," IEEE/ACM Transactions on Net-working, vol. 11, no. 6, pp. 908-922, Dec. 2003.
〔11〕 Y. Kim. A. Perrigm, and G. Tsudik. "Simple and fault-tolerant key agreement for dynamic collaborative groups," in 7th ACM Conference on Computer and Communications Security (CCS'00), pp. 235-24, Nov. 2004.
〔12〕 Arijit Ukil, Jaydip Sen, and Sripad Koilakonda, "Embedded security for internet of things," IEEE International Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp 1-6, Apr. 2011.
〔13〕 Top Threats Working Group, "The notorious nine: cloud computing top threats in 2013," https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
〔14〕 https://www.cloudfoundry.org/future-network-security-cloud-foundry/
〔15〕 J. Park, S. Shin, and N. Kang, "Mutual authentication and key agreement scheme between lightweight devices in internet of things," The Journal of Korean Institute of Communications and Information Sciences, 38(9), pp. 707-714, Sept. 2013.
〔16〕 R. Hummen et al., "Towards viable certificate-based authentication for the internet of things," WISEC'13 Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 37-42, Apr. 2013.

〈저 자 소 개〉

성 순 화 (Soon-hwa Sung) 종신회원
2005년: 충남대학교 컴퓨터공학과 박사
2006년~2010년: 충남대학교 차세대통신인력양성사업단 BK전임교수
2011년: 충남대학교 공학교육혁신센터 초빙교수
2012년: 충북대학교 소프트웨어학과 초빙교수
2014년~현재: 충남대학교 소프트웨어 연구소
〈관심분야〉 사용자 인증, 키 관리, 모바일 결제 시스템, IoT(Internet of Things) 보안, 클라우드 보안