클라우드 서비스 환경에서 모바일 디바이스의 경량화된 사용자 인증 프로토콜 연구

김정호*, 이아영*, 현영훈**, 전문석*
*숭실대학교 컴퓨터학과
**숭실대학교 정보과학대학원 정보보안학과
e-mail : kimpocjstk1@ssu.ac.kr
aylee@ssu.ac.kr
skellet@ssu.ac.kr
mjun@ssu.ac.kr

A Study on Lightweight User Authentication Protocol for Mobile Device in Cloud Service Environment

Jeong-Ho Kim*, Ah-young Lee*, Young-Hun Hyun**, Moon-Seog Jun*
*Dept of Computer Science and Engineering, Soong-Sil University
**Graduate School of Information Science, Soong-Sil University

요 약

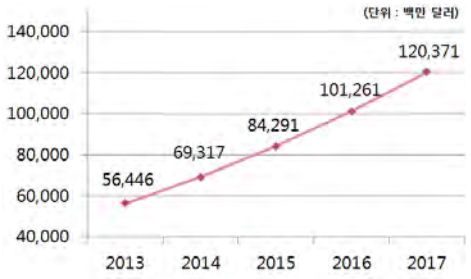
클라우드 시스템은 온라인상에서 사용자가 원하는 형태에 따라 Saas, Paas, Iaas 등의 다양한 방식으로 자원을 할당받아 사용할 수 있는 시스템을 말한다. 또한 모바일 하드웨어의 성능이 나날이 발전함에 따라 클라우드 시스템을 모바일 환경에서 이용하는 것이 가능해졌는데, 모바일 환경에서는 편리한 이동성이라는 장점을 지니고 있지만, 무선의 방식으로 통신하기 때문에 전력 소모량에 대하여 한계점이 있다. 이를 해결하기 위해서 본 논문에서는 모바일 디바이스 이용자들이 클라우드 서비스를 이용하고자 할 때, 전력 소모를 줄인 경량화된 사용자의 인증 프로토콜을 제안하였다.

1. 서론

클라우드는 전 세계적으로 널리 인터넷이 보급됨에 따라 다양한 유·무선 방식의 모바일 디바이스 및 PC에서 인터넷을 통해 언제 어디서든 사용자가 필요로 하는 만큼의 자원을 할당받아 데이터를 저장하거나 서비스를 이용하는 것 인데, 인터넷과 저장 매체 등의 발전에 따라 클라우드 서비스를 공급하는 회사가 생겨나게 되었다. 이는 IT에 관련된 기능들이 회사로부터 서비스 형태로 제공되는 컴퓨팅 스타일로 [그림 1]의 전망과 같이 미래사회의 핵심 기술로 부상하고 있다.

이러한 클라우드 서비스 확산에 대하여 각종 PC 제조업체, Portal, IT 기업 등의 IT 관련 사업자 뿐 아니라, 전 세계 여러 국가들 또한 국가 경쟁력에 큰 척도가 될 수 있는 기술로써 인식하기 시작하면서, 미국이나 EU가 앞다투어 클라우드 서비스를 국가 활성화 전략으로 발표하였으며 우리나라도 이에 발맞추어 정부 차원에서 2014년 클라우드 선진국 도약을 위한 '클라우드 컴퓨팅 활성화 종합계획'을 발표하였다.

점차적으로 영역을 확장해 나가고 있는 클라우드 서비스에서 최근 들어서는 다양한 분야에서 클라우드를 기반으로 하는 서비스가 폭발적으로 성장하고 있는데, 이러한 클라우드 서비스는 스마트폰과 같은 모바일 디바이스의 확산과 더불어 통신에 따른 사용자의 증가에 따라 대용량의 트래픽이 발생하게 되었고, 트래픽 폭주에 대해 유연하게 대처하기 위한 방안이 필요하게 되었다.[1]



[그림 1] 클라우드 컴퓨팅 시장 전망

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해서 기술하고, 3장에서는 클라우드 서비스 환경에서 모바일 디바이스 이용자들의 경량화된 사용자 인증 방식을 제안한다. 마지막으로 4장에서는 결론을 맺는다.

2. 관련 연구

2.1. 클라우드 서비스

클라우드 서비스는 인터넷을 기반으로 하여 자원과 정보

※ 본 논문은 미래창조과학부의 2015년 고용계약형 SW석사과정 지원사업을 지원받아 수행한 결과임

인프라, 그리고 소프트웨어를 제공한다. 이는, 1960년대 존 맥카시가 말한 “컴퓨팅 환경은 전기와 수도 등 공공서비스들을 사용하는 것과도 같다”라는 개념을 제시한 것에서부터 시작하는데, 인터넷을 통한 수요에 의한 제공방식의 서비스다. 클라우드 서비스의 제공자는 다량의 컴퓨터 자원을 분배·가상화하여 각 이용자에게 제공한다. 또한 이용자는 클라우드 서비스를 활용해 자신의 컴퓨터나 모바일 디바이스에 직접적으로 프로그램을 설치하지 않아도 원하는 자원을 이용하고 싶을 때, 이용하고자 하는 만큼, 서비스를 신청하게 되면 인터넷을 통하여 서비스를 받을 수 있다.

클라우드 서비스는 사용자의 필요에 따라 구분을 하게 되는데 대표적으로 SaaS, PasS, IasS로 구분된다.

2.1.1. SaaS(Software as a Service)

SaaS는 애플리케이션을 서비스의 대상으로 제공하는 모델로써, 사업자가 인터넷을 통해 소프트웨어를 제공하게 되면 사용자는 원격으로 접속하면서 일정기간동안 사용할 수 있는 형태의 서비스이다. SaaS의 대표적인 서비스 종류로는 Yahoo Mail, Google Docs, CRM 프로그램을 들 수 있는데 프로그램과 그 안에서 사용되는 데이터가 모두 공급자의 서버에 저장이 되기 때문에 사용자들은 어디서나 웹에 접속해 서비스를 이용할 수 있다.

2.1.2 PaaS(Platform as a Service)

SaaS는 웹상으로 소프트웨어를 제공하던 것이라면, PasS는 개발자들을 위하여 개발이 가능한 플랫폼을 제공하는 서비스를 말한다. 사용자들은 자신이 직접 만든 소스코드를 Service Provider의 클라우드 서버에 업로드해 온라인으로 제공할 수 있는데, 개발만이 아니라 테스트 및 관리, 유지보수 등의 모든 작업들을 제공받은 통합적인 개발환경 안에서 할 수 있기 때문에 기존 방식으로 제공해왔던 서비스보다 훨씬 저렴한 비용으로 프로그램을 개발하고 온라인으로 서비스할 수 있는 장점이 있다.

2.1.3 IaaS(Infrastructure as a Service)

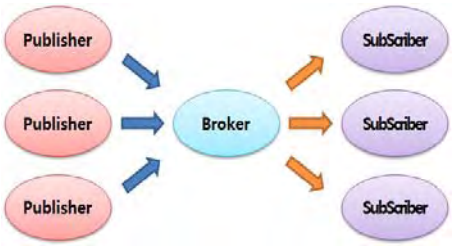
IasS는 컴퓨팅 자원의 아웃소싱이 가능한 하드웨어 환경을 제공하는 서비스를 말하는데, 현재 이렇게 큰 규모의 컴퓨팅 자원에 대해 제공이 가능한 회사는 구글과 IBM, 아마존과 같은 소수 기업에 국한되어 있다. IasS에서는 서비스를 필요로 하는 사용자들이 원하는 시기에 컴퓨팅 자원을 이용할 수 있는 ‘쓴 만큼 지불하는(Pay as you go)’ 모델을 제공하는데 이러한 방식 뒤에는 가상화라는 기술이 있다. 가상화라는 기술은 물리적으로 구성된 서버공간을 온라인을 통해 논리적으로 이용가능한 방법을 말하는데, 이를 이용하면 추가적으로 서버와 각종 하드웨어 장비를 필요로 할 때 저가의 비용으로도 원하는 컴퓨팅자원을 안정적으로 이용할 수 있게 된다.[2]

2.2. MQTT

MQTT(Message Queue Telemetry Transport)는 제한된 자원(CPU, RAM, 배터리 등)을 가진 디바이스를 제한적인 네트워크 상에서 비동기적인 통신을 가능하게 해주는 경량화된 메시징 프로토콜이다. 이름에서 알 수 있듯이, 센서에서 전송되는 데이터와 같은 원격 데이터 전송에 적합하기도 하며 스마트폰의 페이스북 메신저와 같은 어플리케이션에서 클라이언트 간에서 사용되는 메시지 교환을 위해 MQTT 프로토콜을 사용한다.[3]

MQTT는 IBM 및 유로텍에 의해 개발되었으며 개방형 표준 프로토콜로 배포되었으며 2013년 3월 26일에 개최한 첫 번째 기술위원회 회의에서 오아시스에 의해 표준화 되었다. 오아시스는 "구조적 정보 표준의 발전을 위한 조직"의 줄임말이며 개발 및 통합, 채택을 구동하는 글로벌 컨소시엄 개방형 표준이다.

[그림 2]는 MQTT의 구조를 나타낸 것인데, Publisher와 Subscriber의 역할을 하는 Client와 Publisher의 정보를 수신하고 Subscriber에게 정보를 전달하는 기능을 가지는 Broker로 이루어져 있다. MQTT의 원리를 살펴보면 정보를 수신하고자 하는 Subscriber인 Client가 자신이 원하는 정보에 대한 토픽을 Broker에게 등록한 후, 정보를 전달하고자 하는 Publisher인 Client가 Broker에게 해당하는 정보를 전달했을 시, Broker는 해당 정보의 토픽을 조회하여 Subscriber가 수신하고자 하는 정보와 일치하는 토픽일 경우 해당 정보를 Subscriber에게 전달한다.[4]



[그림 2] MQTT 구조

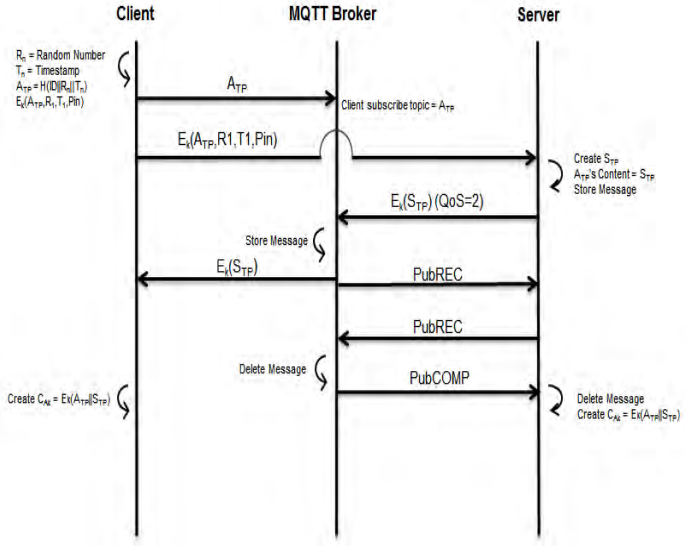
3. 경량화된 사용자 인증 방식 제안

본 논문에서 제안하는 인증 방식은 클라우드 환경에서 MQTT를 활용하여 사용자를 인증하는데 있어 권고되는 사항인 SSL을 사용하지 않고 사용자가 생성하는 난수와 타임스탬프, Pin 정보를 활용하여 사용자만이 사용가능한 토픽을 생성하고 이를 활용하여 사용자를 인증하는 경량화된 사용자 인증 방식이다.

<표 1> 사용자 인증 프로토콜 약어

약어	설명
R_n	Random Number
T_n	Timestamp
$h()$	Hash Function
A_{TP}	Authentication Topic
S_{TP}	Secret Topic
C_{Ak}	Client Access Key

다음 <표 1>은 사용자를 인증하기 위해 사용하는 프로토콜의 약어를 표시한 것이다.



[그림 2] 사용자 인증 프로토콜

첫 째, Client는 고유한 토픽을 생성하기 위해, 난수와 타임스탬프, Pin 정보들을 연접한 후 해시하여 토픽을 생성해 Broker에게 전달한다. 해당 토픽은 Broker에게 등록되고, Client는 Server에 해당 토픽과 난수, 타임스탬프, Pin 정보를 암호화하여 서버에게 전달한다.

둘 째, Server는 Client로부터 전달받은 값을 복호화하여 동일하게 생성하여 값이 동일한지 검증한 후, 사용자가 사용할 수 있도록 비밀 정보를 암호화하여 QoS 2의 방식으로 Broker에게 전달한다.

셋 째, Broker는 이 비밀 정보를 수신하기 위해 토픽을 등록한 Client에게 해당 토픽에 맞는 암호화된 비밀 정보를 전달하게 되고, Client는 전달받은 값을 복호화하여 비밀 정보와 고유한 토픽을 연접해 암호화하여 사용자가 사용할 ID로 생성하여 사용자 등록을 완료한다.

마지막으로, Server에서는 QoS 2의 방식으로 Client가 비밀 정보를 받았다는 확인 메시지를 전달받은 후, 동일하게 고유한 토픽과 비밀 정보를 연접하고 암호화하여 해당하는 사용자의 등록을 완료한다.

4. 결론

본 논문은 기존의 클라우드 서비스에 인증하기 위해 사용했던 https 방식의 메시지 교환과정이 모바일 디바이스를 활용한 사용자 인증 방식에는 전력 소모량에 부담이 있기에, 모바일 디바이스에서 MQTT 프로토콜을 활용하여 고유한 토픽 생성을 통한 전력의 소비를 줄인 사용자 인증 프로토콜을 제안하였다.

향후 제안한 프로토콜은 지속적으로 연구하여 효율성을 높이도록 하고, 나아가 변형을 통해 다양한 상황의 사용자의 인증에도 활용할 수 있도록 해야 할 것이다.

참고문헌

[1] 정성재, “클라우드 보안 위협 요소와 기술 동향 분석”, 2013.

[2] 방송통신위원회, “클라우드 서비스 정보보호 안내서”, 2011

[3] 심승현, “사물인터넷과 MQTT 기술“, 2014.

[4] Bryan Boyd, “MQTT”, 2014