클라우드 컴퓨팅 환경에서 안전성이 향상된 사용자 인증 프로토콜

변연상*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : ysbyun@sch.ac.kr, jkwak@sch.ac.kr

User Authentication Protocol with Improved Security in Cloud Computing Environment

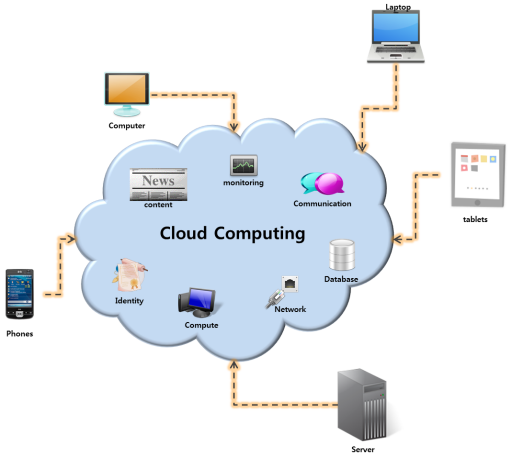
Yun Sang Byun*, Jin Kwak**
*ISAA Lab. Dept. of information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

클라우드 컴퓨팅 환경은 다양한 IT 기술이 융합된 형태로 수많은 사용자들이 같은 인프라를 기반으로 서비스를 제공받는 환경이다. 이렇게 수많은 사용자들이 이용하는 클라우드 컴퓨팅 환경에서는 악성코드 유포, 개인정보 탈취 등과 같은 문제점이 발생할 수 있기 때문에 사용자를 인증할 수 있는 필요성이 대두되었다. 이러한 문제점을 해결할 수 있는 대응 방안이 많이 연구되고 있지만, 클라우드 컴퓨팅 환경의 특징을 고려하지 않고 개발되었기 때문에 적용하기에는 다소 문제점이 있을 것으로 예상된다. 이러한 문제점을 해결하기 위해 Lee 등은 2-factor 인증 기법을 제안하였다. 그러나 Lee 등이 제안한 인증 기법은 무결성, 기밀성을 보장하지 못하며, 도청에 취약한 것으로 분석되었다. 따라서 본 논문에서는 이러한 문제점을 해결할 수 있는 프로토콜을 제안한다.

1. 서론

클라우드 컴퓨팅 환경은 인터넷 기술을 기반으로 하여 다양한 서비스를 제공하는 컴퓨팅 기술로 정의되고 있으며 주요 특징은 소프트웨어 또는 스토리지, 서버 등과 같은 IT 자원을 필요한 만큼 빌려서 사용하고 그에 해당하는 요금을 지급하는 것이다[1,2]. 이러한 특징을 보유한 클라우드 컴퓨팅은 (그림 1)과 같이 표현할 수 있다.



(그림 1) 클라우드 컴퓨팅 개념도

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-010886).

클라우드 컴퓨팅 환경은 다양한 사용자가 동일한 인프라를 기반으로 서비스를 제공받는 형태이다. 다양한 사용자가 하나의 인프라를 이용하기 때문에 악성코드 유포, 개인정보 탈취와 같은 문제점이 발생할 수 있기 때문에 사용자들을 정확하게 판별할 수 있는 인증 기법의 필요성이 대두되었다. 이러한 문제점을 해결하고자 Lee[3] 등은 2010년 2-factor 인증 기법을 제안하였지만, 제안된 인증 기법은 무결성, 기밀성을 보장하지 못하며, 도청에 취약하다.

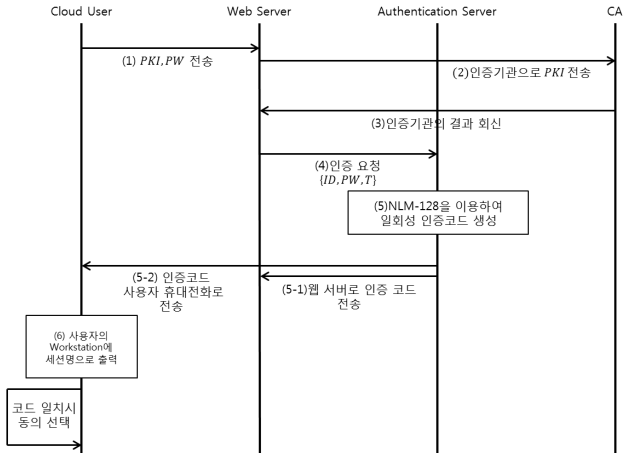
따라서 본 논문에서는 Lee[3] 등이 제안한 인증 기법의 문제점을 해결할 수 있는 사용자 인증 프로토콜을 제안한다.

2. Lee 등의 인증 기법 및 안전성 분석

2.1 Lee 등의 인증 기법

2010년 Lee[3] 등이 제안한 인증 기법은 클라우드 컴퓨팅 환경에서 사용자가 *PKI*와 난수 생성기 NLM-128[4]로 생성한 랜덤 넌스 값을 일회성 인증코드로 이용하며, 모바일 단말기와 사용자의 워크스테이션에 동일한 일회성 인증 코드를 전송하여 사용자 인증 과정에 사용한다.

Lee[3] 등의 논문에서는 등록단계와 별도의 인증서 발급 단계는 생략되어 있으며, 클라우드 서비스를 받기 위한 사용자 인증 과정을 수행한다.



(그림 2) Lee 등의 인증 기법

(1) 사용자는 인증을 수행하기 위해 자신의 PKI와 PW_i를 웹 서버로 전송한다.
(2) 웹 서버는 전송받은 PKI의 정당성을 인증받기 위해 인증기관(CA)로 전송한다.
(3) CA는 판별 결과를 회신한다.
(4) 웹 서버는 인증서버로 다시 인증 메시지를 전송한다. (인증 메시지는 사용자ID_i/PW_i로 구성되어 있으며 추가로 타임스탬프 값 T를 전송)
또한 인증서버는 NLM-128을 이용하여 일회성 인증코드를 생성한다.
(5-1) 인증서버는 생성된 인증코드를 웹 서버로 전송한다.
(5-2) 동시에 사용자의 휴대전화로 같은 인증코드를 전송한다.
(5-3) 동일한 코드가 사용자 워크스테이션에 전달되어 세션 명으로 출력된다.
(6) 사용자는 모바일로 전송된 코드와 워크스테이션에 출력된 세션 명으로 출력된 인증코드를 서로 비교한다.
(7) 인증코드가 일치하는 경우 사용자는 연결을 동의하여 연결 세션을 허가한다.
(8) 사용자가 연결을 수락하게 되면 웹서버는 인증 서버에서 받은 인증 코드와 사용자의 코드가 일치하는지 확인하고 서비스를 제공한다.

2.2 Lee 등의 인증 프로토콜의 안전성 분석

Lee 등의 인증 프로토콜은 무결성과 기밀성을 보장하지 못하며, 도청에 취약하다는 문제점을 내포하고 있기 때문에 본 절에서 이러한 문제점들에 대해서 분석한다.

2.2.1 무결성

클라우드 컴퓨팅 환경과 같이 외부에서 내부 데이터에 접근하기 위해 인터넷과 같은 공개된 네트워크를 이용하는 경우가 많다. 이러한 경우 사설망을 이용하여 데이터를 전송하는 경우보다 악의적인 사용자의 접근 및 공격이 용이하기 때문에 해당 데이터의 변경, 파괴 등 가능성이 높아질 가능성이 증가하게 되므로 무결성을 보장해야 한다.

그러나 Lee 등의 제안 기법은 사용자와 웹 서버사이에서 사용자를 검증하기 위해 사용되는 수단인 PKI와 PW_i를 암호화하지 않고 전송한다. 이렇게 전송과정에서 악의적인 사용자가 해당 정보를 탈취하여 변형 등이 가능하기 때문에 데이터의 무결성을 보장하지 못한다.

2.2.2 기밀성

클라우드 컴퓨팅 환경과 같이 막대한 양의 데이터들이 저장된 인프라에서 데이터들의 기밀성이 확보되지 않는다면 악의적인 사용자의 접근이 용이할 뿐만 아니라, 악성코드 유포를 통한 스팸, 피싱과 같은 피해를 발생시킬 수 있다[5]. Lee 등이 제안한 인증 기법에서는 사용자의 로그인 정보를 암호화하지 않고 평문 형태로 전송한다. 따라서 악의적인 사용자가 로그인 정보를 획득하여 데이터를 열람하거나 위·변조시키는 것이 가능하기 때문에 기밀성을 보장하지 못한다.

2.2.3 도청

사용자가 웹 서버로 전송하는 사용자의 PKI와 PW_i를 암호화 과정 없이 평문 형태로 전송된다. 따라서 악의적인 사용자가 일반 사용자의 PKI, PW_i를 도청하는 것이 가능하다.

예를 들어 악의적인 사용자가 사전에 클라우드 서버에 정당한 사용자로 등록을 하고, 사용자와 서버사이에서 도청을 통해 PKI, PW_i를 전송받고 본인의 PKI', PW_i'를 전송하여 사용자 인증 과정을 수행한다. 공격자가 정당한 사용자에게는 악성코드가 감염된 사이트로 접속을 유도하거나, 사용자의 개인정보를 이용한 스팸메일, 문자 전송 등 악성 행위를 하는 것이 가능해 진다.

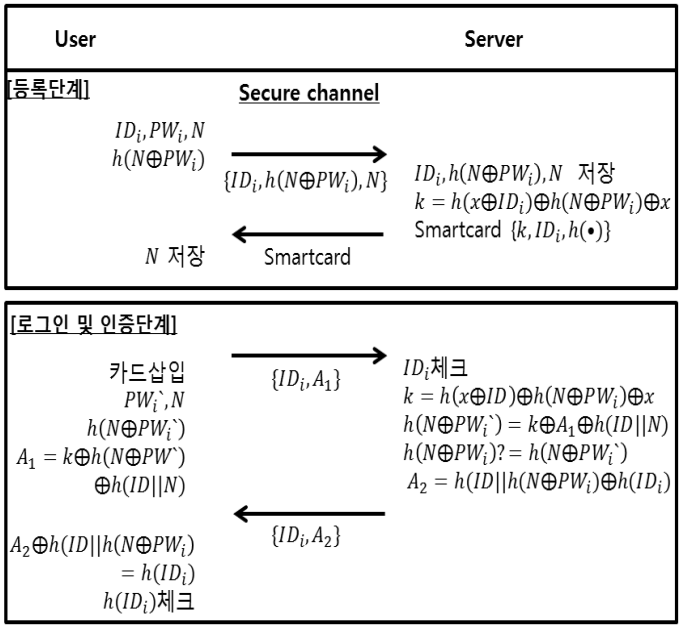
3. 제안 프로토콜

본 논문에서는 앞에서 분석한 문제점을 기반으로 클라우드 컴퓨팅 환경을 위한 스마트카드 기반의 사용자 인증 프로토콜을 제안한다.

3.1 용어 정의

<표 1> 파라미터

분류	내용
$User$	사용자
$Server$	서버
ID_i	사용자 식별자
PW_i	사용자의 패스워드
N	랜덤 넌스 값
x	서버의 비밀 값
$h(\cdot)$	일 방향 해쉬 함수
$\oplus$	XOR 연산



(그림 3) 제안 프로토콜

3.2 등록단계

본 단계는 사용자들이 서비스 이용을 위해 등록하는 단계이며 안전한 채널을 통해 다음과 같이 진행된다.

① 사용자는 등록을 위해 안전한 채널을 통해 사용자의 ID_i, PW_i를 생성하고, 랜덤 넌스 N을 생성한다. 그 후 패스워드 검증자 $h(N \oplus PW_i)$를 생성하여 함께 서버로 전송한다.

② 서버는 사용자의 ID_i를 체크하고, 전송받은 패스워드 검증자 $h(N \oplus PW_i)$와 넌스 값 N과 함께 서버에 저장한다.

③ 저장된 패스워드 검증자와 사용자의 식별자인 ID_i, 서버의 비밀 키 값 x를 해쉬 연산과 XOR 연산을 통하여 $k = h(x \oplus ID_i) \oplus h(N \oplus PW_i) \oplus x$를 생성하고, 스마트카드에 저장하여 사용자에게 발급한다.
(이때 스마트카드에 저장된 인자 값은 $ID_i, k, h(\cdot)$)

④ 스마트카드를 발급받은 사용자는 앞서 생성한 랜덤 넌스 값 N을 자신의 스마트카드에 저장한다.

3.3 로그인 및 인증 단계

본 단계는 사용자의 로그인 정보를 전송받은 서버가 사용자에 대한 인증 과정을 수행하는 단계로 자세한 설명은 다음과 같다.

① 사용자는 자신이 발급받은 스마트카드를 리더기에 삽입하고 패스워드 PW_i'를 입력하고 N을 이용하여 패스워드 검증자 $h(N \oplus PW_i')$를 생성한다. 패스워드 검증자과 k를 이용하여 A_1을 생성한 다음 ID_i와 함께 서버로 전송한다.

② 전송받은 서버는 전송받은 ID_i를 체크하고 전송받은 값과 저장된 패스워드 검증자 및 자신의 비밀 키 x를 이용하여 k값을 생성한다.

③ 패스워드 검증자 값을 확인하기 위해 k값과 전송받은 A_1값, $h(ID_i||N)$을 XOR 연산을 통해 검증자 값을 확인한다.

④ 또한 서버는 $A_2 = h(ID||h(N \oplus PW_i) \oplus h(ID_i)$를 계산하여 사용자의 ID_i와 A_2값을 사용자에게 전송한다.

⑤ 사용자는 전송받은 A_2값과 패스워드 검증자를 기반으로 하여 $h(ID_i)$값을 계산하고, 자신의 스마트카드를 이용하여 $h(ID_i)$값을 생성하여 비교한다.

4. 안전성 분석

4.1 무결성

본 논문에서 제안한 프로토콜은 스마트카드를 기반으로 사용자 인증 과정을 수행한다. 등록과정은 안전한 채널에서 진행하며 사용자가 임의의 난수를 생성하여 패스워드 검증자를 생성한다. 또한 생성된 패스워드 검증자 $h(N \oplus PW_i)$를 스마트카드에 저장하여 로그인 및 인증단계에서 사용한다. 이를 통해 공격자가 손쉽게 로그인 정보를 획득하는 것이 불가능하며, 임의의 난수로 생성한 패스워드 검증자를 생성할 수 없다. 따라서 제안된 프로토콜은 무결성을 보장할 수 있다.

4.2 기밀성

제안 프로토콜에서는 기본적으로 로그인 정보를 스마트카드에 저장하여 이용한다. 또한 PW_i를 해쉬 연산과 XOR연산을 통해 검증자 $h(N \oplus PW_i)$로 변환하여 이용하기 때문에 로그인 정보를 알아내기 어렵다. 만약 PW_i가 노출되더라도 사용자가 임의로 생성한 넌스 값 N을 알 수 없기 때문에 기밀성을 보장할 수 있다.

4.3 도청

기존의 Lee 등의 인증 기법은 정당한 사용자로 인증받기 위해 ID, PW_i, PKI등을 이용한다. 하지만 이러한 인자 값들을 암호화 과정 없이 평문 형태로 서버에 전송하기 때문에 손쉽게 도청이 가능했다.

본 논문에서 제안한 프로토콜은 안전한 채널을 통해서 사용자의 ID_i와 패스워드 검증자 $h(N \oplus PW_i)$를 전송하여 k값을 패스워드 검증자 및 비밀키 값을 생성하고 스마트카드에 저장하여 사용된다. 이를 통해 악의적인 사용자가 전송되는 파라미터들을 획득할 수 있는 도청에 안전하다.

<표 2> 안전성 분석

구분	Lee 등의 프로토콜	제안 프로토콜
무결성	x	O
기밀성	x	O
도청	x	O

5. 결론

본 논문에서는 Lee 등이 제안한 인증 기법이 무결성, 기밀성을 보장하지 못하며 도청에 취약하다는 것을 분석하였으며, 이를 해결할 수 있는 스마트카드 기반의 사용자 인증 프로토콜을 제안하였다. 본 논문에서 제안한 인증 프로토콜은 Lee 등이 제안한 인증 기법과는 다르게 안전한 채널에서 등록과정을 수행하며 Lee 등의 제안한 인증 기법의 문제점인 무결성, 기밀성을 보장하면서 도청에 안전한 프로토콜을 제안하였다.

참고문헌

[1] M. Armbrust, A. fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, “Above the Clouds: A Berkely view of Cloud Computing” Technical Report No. UCB/EECS-2009-28.

[2] John W.Rittinghouse and James F.Randsome, “Cloud Computing Implementation,Management and Security ” in CRC Press, pp. 153-154, [Online] 2010,

[3] S. Lee, I. Ong, H. T. Lim, H. J Lee, "Two Factor Authentication for Cloud Computing", INTERNATIONAL JOURNAL OF KIMICS, VOL. 8, NO. 4, AUGUST 2010

[4] Hoon Jae Lee and Sang Jae Moon, "On an improved summation generator with 2-bit memory," in ACM of Signal Processing, vol. 80, pp.211-217, Jan 2000.

[5] 한국정보통신기술협회, “공공 부분 데스크탑 클라우드 도입 가이드라인”, 2011