情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

클라우드 환경을 위한 분산 처리 사용자 인증 프로토콜

정 윤 수,[1†] 이 상 호[2‡]
[1]목원대학교, [2]충북대학교

User Authentication Protocol through Distributed Process for Cloud Environment

Yoon-Su Jeong,[1†] Sang-Ho Lee[2‡]
[1]Mokwon University, [2]Chungbuk National University

요 약

IT 서비스 및 컴퓨팅 자원을 인터넷 기반으로 제공하는 클라우드 컴퓨팅이 최근 주목받고 있다. 그러나 기밀 데이터를 암호화한 후 저장하여도 암호화된 데이터는 클라우드 서버에 저장되기 때문에 기밀 정보가 유출될 수 있다. 본 논문에서는 서로 다른 물리적인 위치에 존재하는 사용자가 기밀 데이터를 안전하게 제공받으면서 임의의 사용자가 기밀 정보를 불법적으로 악용하는 것을 예방하기 위한 사용자 인증 프로토콜을 제안한다. 제안 프로토콜은 임의의 사용자가 원격에서 특정 서버에 접근할 경우 서버에 존재하는 사용자 인증 정보를 일방향 해쉬 함수와 XOR 연산을 사용하여 사용자가 서버로부터 인증을 제공받음으로써 클라우드 컴퓨팅의 사용자 보안 문제를 해결하고 있다.

ABSTRACT

Cloud computing that provides IT service and computer resource based on internet is now getting attention. However, the encrypted data can be exposed because it is saved in cloud server, even though it is saved as an encrypted data. In this paper, user certification protocol is proposed to prevent from illegally using of secret data by others while user who locates different physical position is providing secret data safely. The proposed protocol uses one way hash function and XOR calculation to get user's certification information which is in server when any user approaches to particular server remotely. Also it solves user security problem of cloud.

Keywords: Cloud Computing, User Authentication Protocol, Distribution Process, Certification

I. 서 론

최근 하드웨어・소프트웨어 등의 컴퓨팅 자원을 자신이 필요할 때 사용하고 그에 대한 요금을 지급하는 컴퓨팅 서비스인 클라우드 컴퓨팅이 많은 관심을 받고 있다[1]. 클라우드 컴퓨팅이 널리 사용되는 이유는 서로 다른 물리적인 위치에 존재하는 무형의 형태로 존재하는 하드웨어, 소프트웨어 등의 컴퓨팅 자원을 가상화 기술을 통해 통합할 수 있기 때문이다[15].

클라우드 컴퓨팅 환경에서는 외부 서버에 자료들이 저장되어 있기 때문에 안전하게 자료를 보관할 수 있고, 저장 공간의 제약도 극복할 수 있다. 클라우드 컴퓨팅 환경은 언제 어디서든 자신이 작업한 문서 등을 열람・수정할 수 있는 장점을 가지고 있지만 서버가 해킹당할 경우 개인정보가 유출될 수 있고 서버 장애가 발생하면 자료 이용이 불가능한 단점이 있다. 클라우드 컴퓨팅 환경에서는 서버에 존재하는 데이터를 안전하게 보관하기 위해서 높은 보안성을 보장하는 2-factor 인

접수일(2012년 4월 5일), 수정일(1차: 2012년 5월 24일, 2차: 2012년 6월 11일), 게재확정일(2012년 7월 3일)
† 주저자, bukmunro@mokwon.ac.kr
‡ 교신저자, shlee@cbnu.ac.kr

증 방식이 요구되고 있다. 특히, 기존에 사용되던 패스워드 인증 방식은 낮은 보안성, 비사용, 재사용, 공유, 망각, 도난, 입력 어려움, 키 로깅, 중간자 공격 취약점 등 다양한 보안 문제점이 존재한다[2,3].

클라우드 컴퓨팅에서 보관되는 데이터는 보안이 취약하여 기밀 데이터를 암호화하여 저장하여도 암호화된 데이터는 클라우드 서버에 저장되기 때문에 가상 기기와 클라우드 컴퓨팅 서비스 과정중에 기밀 정보가 유출될 수 있다[4]. 현재까지 클라우드 컴퓨팅 환경에서 사용되고 있는 가상 및 클라우드 플랫폼의 보안 공격은 매우 용이하지만 보호는 매우 어려운 상황이다. 기업이 이를 위한 보안 기술을 수용하게 되면서 기업의 중요한 데이터를 보호해야 하는 IT 관리자는 더 큰 부담을 안고 있다. 엄청난 규모의 가상화 서버에 대한 패칭 작업은 결코 쉬운 일이 아니며 해커들이 서버를 탈취하고 트래픽을 방해하고 취약한 시스템에서 데이터를 훔칠 수 있는 여지를 제공할 수 있다.

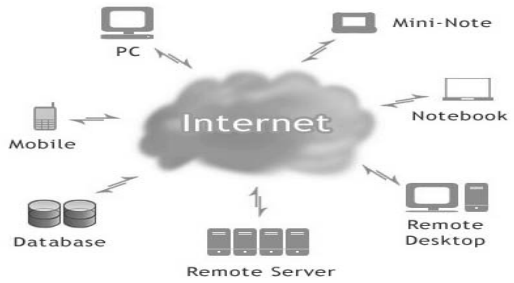
이 논문에서는 물리적, 가상 및 클라우드 환경에서 사용되는 기밀 데이터를 서로 다른 물리적인 위치에 존재하는 사용자가 서비스를 제공받을 경우, 임의의 사용자 기밀 정보를 불법적으로 악용되는 것을 예방하기 위한 인증 프로토콜을 제안한다. 제안 프로토콜은 임의의 사용자가 원격에서 특정 서버에 접근할 경우 서버에 존재하는 서비스를 제공받기 위해서 일방향 해쉬 함수와 XOR 연산을 사용하여 사용자 인증을 제공받는다. 특히, 제안 프로토콜은 서버의 효율성 뿐만 아니라 비용 절감을 위해서 내부 사용자의 인증을 분산 처리하며 외부 사용자는 클라우드 플랫폼이 제공하는 통합 인증 시스템을 이용하여 서버내의 시스템에 접근한다. 또한 제안 프로토콜은 클라우드 컴퓨팅에서 분산 처리된 개인 정보를 모두 중앙에 위치한 서버에 중앙 집중하여 클라우드 컴퓨팅의 사용자 보안 문제를 해결하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅과 클라우드 컴퓨티 보안 연구를 알아본다. 3장에서는 클라우드 컴퓨팅 환경을 위한 분산처리 기반의 사용자 인증 기법을 제안한다. 4장에서는 제안 기법의 보안성을 분석하고 마지막으로 5장에서 결론을 맺는다.

II. 관련연구

2.1 클라우드 컴퓨팅 개요

클라우드 컴퓨팅은 언제, 어디서나 컴퓨팅 자원을 필요에 따라 차용하여 네트워크를 통해 다양한 방식으로 접근하는 서비스를 의미한다[1,2].



[그림 1] 클라우드 컴퓨팅 환경[6]

클라우드 컴퓨팅은 소프트웨어, 스토리지, 네트워크 등 사용 가능한 대부분의 컴퓨팅 자원들을 필요한 만큼 제공받아 사용하고 서비스 종류에 따라 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service) 등으로 사용한다. 클라우드 컴퓨팅은 자원 관리 효율성, 사용자 편의성 등에서 부각되고 있지만 보안성 측면에서 클라우드 컴퓨팅이 갖는 시스템 구조적 특징으로 인해 새로운 형태의 보안 위협에 직면하고 있다[16]. 특히, 클라우드 컴퓨팅에서의 보안 위협은 기존 컴퓨팅 환경과 달리 가상화 엔진 하이퍼바이저에 의한 보안 위협, 관리자에 의한 보안 위협, 네트워크 전송과정에서의 보안 위협 등이 있다[2].

가상화 엔진 하이퍼바이저에 의한 보안 위협은 동시에 복수의 가상머신을 구동하는 하이퍼바이저의 악성코드 감염 시, 동일 하이퍼바이저 상의 가상머신들에 의해 악성코드의 감염 확산이 가능할 뿐만아니라 가상머신의 특정 응용프로그램에 해킹툴 포함 시 다른 가상머신과 하이퍼바이저 등에 대한 공격이 가능하다. 관리자에 의한 보안 위협은 정보 위탁관리로 인하여 사용자의 정보가 복사/이동/수정되어도 사용자의 확인이 불가하고 서비스 제공자의 내부자에 의한 정보유출의 가능성이 존재하고 정보의 소유와 관리 간의 분리로 정보 유출 및 손실 시 책임소재가 불명확한 위협이 존재한다. 네트워크 전송과정에서의 보안 위협은 물리적 자원의 공유 및 집중화로 물리적 자원에 장애 발생 시 해당 자원을 공유하는 모든 사용자의 서비스가 중단될 위협이 존재하며 PC, 스마트폰, 스마트 TV 등 다양한 단말의 접속을 허용하기 때문에 각각의 단말이 갖는 보안위협 뿐만 아니라 모바일 단말의 경우 분실 시 사용자의 정보가 유출 가능성이 존재하는 위협이 존재한다.

2.2 클라우드 컴퓨팅을 위한 보안 연구

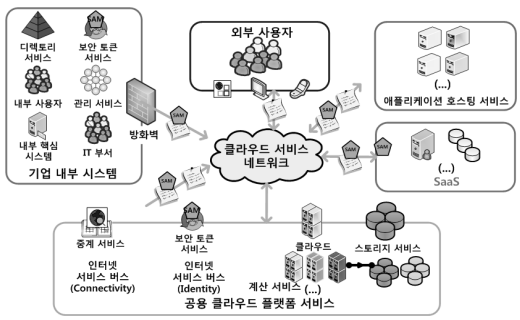
최근까지 IT 기술의 꾸준한 발달로 인하여 클라우드 컴퓨팅을 위한 인증 연구 또한 꾸준히 연구되고 있다[7]. Shoup-Rubin[8]은 3개의 키 분배 프로토콜에 기반한 Bellare-Rogaway 모델[9]을 확장한 기법이다. 이 기법은 스마트카드에서 사용되는 비밀키가 길어 제 3자로부터 스마트카드가 타협(compromised)되지 않는 장점은 있지만 두 객체 중 하나의 객체가 타협되면 안전하지 않은 단점이 있다. Liao et. al. [7] 은 패스워드의 수와 속성에 기반한 스마트카드를 통합하여 인증을 수행하는 기법을 제안하였다. 이 같은 이유는 클라우드 컴퓨팅에서 클라이언트-서버 구조가 다양하여 기존 클라이언트-서버의 인터 네트워크 시스템보다 강한 인증이 필요하기 때문이다. Lee et. al.[10]은 클라우드 컴퓨팅에서 인증을 위한 공개키와 이동 대역폭을 제안하였다. 그러나 이 기법은 인식자(identifier), 패스워드 그리고 PKI 등의 데이터를 평문으로 전달하여 공격자가 데이터를 쉽게 가로챌 수 있는 단점이 있어 실시간 클라우드 컴퓨팅 환경에 부적합하다. Li et. al.[11]는 클라우드 컴퓨팅 시스템이 서비스를 지원하기 위한 신뢰된 플랫폼(trusted platform)과 조합된 이론적 프로토타입 시스템을 제안하였다. Celesti et. al[12]은 클라우드 컴퓨팅을 위한 인식자 관리 문제를 표시하기 위한 참조 구조를 제안하였다. 최근 연구에서는 클라우드 컴퓨팅 환경의 특정 자원을 안전하게 공유하여 사용하는 방법들이 연구되고 있다. 그러나 이 방법들은 특정 자원을 여러 사용자들이 빈번하게 사용할 경우 클라우드 환경의 전체 효율성에 많은 영향을 미칠 수 있는 문제점이 있다. 본 논문에서는 사용자가 보유하고 있는 사용자 정보를 일방향 해쉬 함수와 XOR 연산을 이용하여 물리적 자원에 장애가 발생할 경우 해당 자원을 공유하는 모든 사용자의 서비스가 중단되는 것을 예방함으로써 클라우드 컴퓨팅 환경의 전체 효율성을 유지하는 것을 목적으로 한다.

III. 클라우드 컴퓨팅 환경의 사용자 인증 설계

이 절에서는 클라우드 컴퓨팅 환경에서 사용자의 효율적인 분산 인증을 위해 일방향 해쉬 함수와 XOR 연산을 사용한 사용자 인증 프로토콜을 제안한다. 클라우드 컴퓨팅 환경에서의 보안 위협 중 네트워크 전송과정에서 사용자들이 특정 자원을 빈번하게 사용할 경우 물리적 자원에 장애 발생 시 해당 자원을 공유하는 모든 사용자들이 서비스가 중단될 수 있는 위협을 해소하기 위해서 제안 프로토콜은 사용자의 정보를 일방향 해쉬 함수와 XOR 연산을 사용하여 클라우드 환경의 전체 효율성을 향상시킬 수 있을 뿐만 아니라 제어 집중으로 인한 부하를 낮추고 있다.

3.1 개요

클라우드 컴퓨팅 환경에서 서로 다른 물리적인 위치에 존재하는 사용자가 특정 서버에 존재하는 데이터를 제공 받을 경우 제안 프로토콜에서는 일방향 해쉬 함수와 XOR 연산을 사용하여 인증 서버의 효율성을 높이기 위한 사용자 인증을 수행한다.



[그림 2] 제안 프로토콜의 클라우드 컴퓨팅 환경

그림 2는 제안 프로토콜이 동작되는 클라우드 컴퓨팅 환경을 보여주고 있다. 그림 2에서 제안 프로토콜은 중앙통제의 정도에 따라서 각기 다르게 중앙에서 지원되는 서비스와 데이터베이스에 의해 질적으로 제고된 분산적인 자료처리를 할 수 있다. 그림 2에서 제안 프로토콜은 다른 지역의 프로세스를 사용하고 있는 사용자들에게 또 다른 지역의 프로그램이나 자료를 포함한 유효한 자원을 사용할 수 있도록 인증을 수행한다. 이 때, 자료나 자원에 대한 허가받지 않은 사용자는 접근을 막을 수 있어 옳지 않은 의도로 정보를 수정하려는 제3자를 미연에 방지할 수 있다.

3.2 용어정의

표 1는 제안된 인증 기법에서 사용하는 주요 용어에 대한 설명이다.

〔표 1〕 용어 정의

용어	정 의
U	사용자
AS	인증서버
ID_U	사용자 U의 인식자
PW_U	사용자 U의 패스워드
AS_PU	인증서버의 공개키
AS_PR	인증서버의 개인키
x, y	사용자와 인증서버가 생성한 랜덤값
F_p	유한체
p	유한체 상의 소수
g	원시 소수
SSK	스마트카드의 비밀값
UI	사용자 정보
SI	보안 정보
S_K	세션키
$E_*()$	*의 키를 이용하여 암호화
D_*	*의 키를 이용하여 복호화
$\oplus$	XOR 연산
$\|\|$	연접
$h()$	해쉬 함수

3.3 사용자 인증 프로토콜

클라우드 컴퓨팅 환경에서 다수의 사용자가 특정 자원(혹은 데이터 혹은 자료)을 공유해서 사용하는 경우는 빈번하게 발생할 수 있기 때문에 특정 자원의 공유 상태에 따라서 클라우드 환경의 전체 효율성에 많은 영향을 미친다. 제안 프로토콜에서는 특정 서버에 존재하는 자원을 임의의 사용자가 안전하게 서비스 받을 수 있도록 사용자가 보유하고 있는 정보를 이용하여 사용자의 정보를 일방향 해쉬 함수와 XOR 연산을 사용한다. 이 때, 제안 프로토콜은 등록과정, 로그인 과정, 인증과정, 패스워드 교환 과정 등의 4단계 과정를 수행하고, 데이터를 수신하는 지역에서는 인증기관의 역할을 수행하는 서버가 존재한다고 가정한다.

3.3.1 등록 과정

등록과정에서 사용자(User, U)는 사용자의 인식자를 서비스 요청전에 인증서버(Authentication Server, AS)에 등록한다. 등록과정은 7 단계로 동작되며 사용자의 인식자 ID_U와 패스워드 PW_U가 사용되며, 세부적인 동작과정은 다음과 같다.

• 단계 1 : 사용자는 자신이 생성한 랜덤수 x와 패스워드 PW_U를 XOR하여 해쉬함수 $h()$에 삽입하여 (식 1)처럼 계산한다. 이때, 랜덤수 x는 사용자가 인증서버에 접속할 때마다 매번 새롭게 생성된다.

$$Generate\ x,\ h(PW_U \oplus x) \quad \text{(식 1)}$$

• 단계 2 : 사용자와 인증서버 사이에 SSL (Secure Socket Layer) 연결이 확립되면 사용자는 (식 2)를 인증서버에게 전달한다.

$$E_{AS\_PU}(x, ID_U),\ h(PW_U \oplus x),\ h(x \oplus ID_U) \quad \text{(식 2)}$$

• 단계 3 : 인증서버는 사용자로부터 전달받은 정보를 인증서버의 개인키 AS_PR를 이용하여 x와 ID_U을 복호화한 후 사용자 인식자 ID_U를 데이터베이스에서 검색하여 인식자 ID_U가 존재하는지를 체크한 후 정상적인 사용자일 경우 스마트카드에 저장할 정보를 생성하고 그렇지 않을 경우 등록과정을 종료한다.

$$D_{AS\_PR}(x, ID_U) \quad \text{(식 3)}$$

$$Check\ ID_U \stackrel{?}{=} ID_U' \quad \text{(식 4)}$$

• 단계 4 : 인증서버는 인증서버가 생성한 랜덤수 y와 사용자 인식자 ID_U를 연접하여 해쉬함수 $h()$에 적용하여 보안정보 SI를 생성한 후 사용자로부터 전달받은 정보(ID_U, $h(PW_U \oplus x)$, $h(x \oplus ID_U)$)를 XOR하여 사용자 정보 UI를 생성한다.

$$Substitute\ SI = h(ID_U || y) \quad \text{(식 5)}$$

$$Substitute\ UI = h(ID_U \oplus h(PW_U \oplus x) \oplus h(x \oplus ID_U)) \quad \text{(식 6)}$$

• 단계 5 : 인증서버는 보안정보 SI와 사용자 정보 UI를 연접하여 해쉬함수 $h()$에 적용한 값을 $h(x)$ 값과 함께 (식 7)처럼 유한체 F_p상의 소수 p와 원시원소 g를 이용하여 스마트카드의 비밀키 SSK로 사용한다.

$$Substitute\ SSK = g^{h(SI||UI)+h(x)} \bmod p \quad \text{(식 7)}$$

• 단계 6 : 인증서버는 생성된 정보(SI, UI, SSK,

p, g, $h(\bullet)$)를 사용자의 인식자 ID_U와 연계하여 데이터베이스에 저장한 후 사용자에게 생성된 정보(SI, UI, SSK, p, g, $h(\bullet)$)를 전달한다.

$$Transfer\ \ SI,\ UI,\ SSK,\ p,\ g,\ h(\bullet) \qquad \text{(식 8)}$$

• 단계 7 : 사용자는 인증서버로부터 전달받은 스마트카드에 자신이 생성한 랜덤수 x를 입력한다.

3.3.2 로그인 과정

로그인 과정은 사용자가 클라우드 컴퓨팅 환경에 접근하고자 할 때 사용하는 과정으로써 사용자는 이 과정을 통해 정상적인 사용자인지를 검증받는다.

• 단계 1 : 사용자는 스마트카드를 이용하여 클라우드 컴퓨팅 환경에 접속한 후 사용자의 인식자 ID_U와 패스워드 PW_U를 입력한다.

• 단계 2 : 인증서버는 사용자가 입력한 사용자의 인식자 ID_U와 패스워드 PW_U를 이용하여 사용자 정보 $UI' = (ID_U,\ h(PW_U \oplus x),\ h(x \oplus ID_U))$를 계산한 후 인증서버에 저장되어 있는 사용자 정보 UI와 비교하여 사용자를 검증한다.

$$Compare\ \ UI = UI' \qquad \text{(식 9)}$$

• 단계 3 : 인증서버는 사용자로부터 스마트카드에 있는 SI 정보를 요청한다. 인증서버는 요청 정보가 수신되면 (식 10)처럼 SSK'를 계산한다.

$$SSK' = g^{h(SI||UI)+h(x)} \bmod p \qquad \text{(식 10)}$$

• 단계 4 : 인증서버는 인증서버가 생성한 랜덤수 y를 생성하고 ID_U와 연접하여 해쉬함수 $h()$에 적용한다. 그리고, SSK'를 연접하여 해쉬함수 $h()$에 적용한 결과를 $h(y\ ||\ ID_U)$와 XOR하여 SSI로 대체한다. 인증서버는 SSI, 타임스탬프 T, ID_U, ID_{AS} 를 사용자에게 전달한다.

$$Substitute\ \ SSI = h(SSK') \oplus h(y\ ||\ ID_U) \qquad \text{(식 11)}$$

$$Transmit\ \ SSI,\ T,\ ID_U,\ ID_{AS} \qquad \text{(식 12)}$$

• 단계 5 : 사용자는 인증서버로부터 전달받은 정보를 이용하여 $SSK''(=SSK' g^{-h(x)} \bmod p)$, $SKK(=h(SSK''||T)$를 순차적으로 계산한다.

$$Substitute\ \ SSK'' = SSK' g^{-h(x)} \bmod p \qquad \text{(식 13)}$$

$$Substitute\ \ SKK = h(SSK''||T) \qquad \text{(식 14)}$$

• 단계 6 : 로그인 과정이 끝나면 사용자는 인증서버에게 $h(SKK,\ h(SSK''))$, T, SI 를 전달한다.

3.3.3 인증 과정

인증과정은 타임스탬프 T 동안 사용자가 인증 서버에 대한 로그인 과정을 수행하는지에 대한 수행 과정을 처리하는 과정이다.

• 단계 1 : 인증서버는 타임스탬프 T를 체크하여 네트워크 시스템에서 정한 인증 세션의 정상적인 타임스탬프 $\triangle T$ 인지를 확인한다. 여기서 T는 시스템에 처음 접속한 시간을 의미하고, T'는 시스템에 접속한 마지막 시간을 의미한다.

$$Check\ \ T' - T \le \triangle T \qquad \text{(식 15)}$$

• 단계 2 : 인증서버는 사용자를 인증하기 위해서 사용자로부터 전달받은 정보를 이용하여 $new\ SI(=h(ID_U||y))$ 와 $new\ SKK(=h(SSK''||T))$를 계산한다.

$$Generate\ \ \ new\ SI = h(ID_U||y) \qquad \text{(식 16)}$$

$$Generate\ \ \ new\ SKK = h(SSK''||T) \text{(식 17)}$$

• 단계 3 : 인증서버는 생성된 $new\ SI$ 와 $new\ SKK$를 데이터베이스에 사용자 인식자 ID_U와 쌍으로 저장된 SI와 SKK를 비교하여 정상적으로 처리되면 인증서버와 사용자 사이의 세션키 S_K를 생성하여 사용자에게 전달한다.

$$Generate\ \ \ S_K = new\ SI \oplus new\ SKK \text{ (식 18)}$$

$$Transmit\ \ h(S_K\ ||\ ID_U),\ ID_{AS} \qquad \text{(식 19)}$$

• 단계 4 : 사용자는 SI와 SKK를 XOR하여 세션

키 $S_K^{'}$를 생성한 후 인증서버로부터 전달받은 세션키 S_K를 비교하기 위해서 (식 21)처럼 해쉬함수 $h()$에 적용하여 비교한다. 세션키를 비교한 후 정상적이면 인증서버에게 확인 메시지를 보내고 그렇지 않으면 종료한다.

$$Generate\ \ S_K^{'} = SI \oplus SKK \qquad (식\ 20)$$

$$Compare\ \ h(S_K) = h(S_K^{'}) \qquad (식\ 21)$$

3.4 패스워드 교환 과정

패스워드 교환 과정은 사용자의 패스워드 PW_U을 변경하는 과정이다. 이 과정은 서비스를 제공받는 사용자가 임의 시간에 패스워드 PW_U를 변경한다.

• 단계 1 : 사용자는 임의의 클라우드 시스템 환경에서 사용자의 패스워드를 변경하기 위해서 사용자의 인식자 ID_U와 패스워드 PW_U를 선택한다.

$$Select\ \ ID_U,\ PW_U \qquad (식\ 22)$$

• 단계 2 : 사용자는 선택된 사용자의 인식자 ID_U와 패스워드 PW_U를 이용하여 $UI(= h(ID_U \oplus h(PW_U \oplus x) \oplus h(x \oplus ID_U)))$를 계산하여 인증서버에 저장되어 있는 $UI^{'}$와 비교 검토한다. 만약 일치하지 않으면 종료하고 그렇지 않으면 사용자는 임의의 클라우드 시스템 환경에서 사용자의 패스워드를 변경하기 위해서 스마트카드에 있는 패스워드를 선택한다.

$$Select\ \ PW_U \qquad (식\ 23)$$

$$Compute\ \ UI^{'} = h(ID_U \oplus h(PW_U \oplus x) \oplus h(x \oplus ID_U)) \qquad (식\ 24)$$

$$Compare\ \ UI^{'} \stackrel{?}{=} UI \qquad (식\ 25)$$

• 단계 3 : 사용자는 새로운 패스워드를 $PW^{'}$와 사용자가 생성한 랜덤 수 $x^{'}$를 입력하여 $UI^{''}(=h(ID_U \oplus h(PW^{'} \oplus x^{'}) \oplus h(x^{'} \oplus ID_U)))$을 계산하여 인증서버에 저장되어 있는 UI를 $UI^{''}$로 교체하고 사용자가 생성한 랜덤 수 x도 $x^{'}$로 교체한다.

$$Replace\ \ PW = PW^{'}\ \ \text{and}\ \ x = x^{'} \qquad (식\ 26)$$

IV. 평가

이 절에서는 클라우드 컴퓨팅 환경에서 요구되는 보안 요구사항을 기반으로 제안 기법의 안정성을 평가한다.

4.1 보안평가

4.1.1 인식자 관리

서버는 등록자 사용자의 인식자를 모두 테이블로 저장 관리하며 새로운 사용자가 등록하였을 경우 사용자 인식자가 이용가능한지 데이터베이스에 저장되어 있는 테이블을 검색하여 유일한 인식자를 할당 및 관리한다. 제안 프로토콜은 사용자가 서버로부터 인증을 제공받아 분산 처리되고 인증서버가 사용자 정보와 인식자 정보를 처리할 경우 일방향 해쉬함수와 XOR 연산을 통해 처리하기 때문에 제어 집중으로 인한 부하는 높지 않다.

4.1.2 상호 인증

제안 프로토콜은 로그인 과정과 인증 과정에서 $SI \stackrel{?}{=} SI^{'}$와 $UI^{'} \stackrel{?}{=} UI$을 비교하여 인증서버로부터 사용자를 인증한다. 만일 사용자가 생성한 랜덤수 x와 인증 서버가 생성한 랜덤수 y을 SI와 UI에 적용하여 $SSK^{'}(= g^{h(SI||UI)+h(x)} \bmod p)$을 서로 교환함으로써 세션키 S_K을 생성한다. 이때, 세션키 S_K는 인증서버와 사용자만이 알고 있어 제 3자는 알수 없다. 제안 기법에서는 매 통신마다 서로 다른 세션키 S_K을 생성하기 때문에 평문 공격의 암호 알고리즘 공격을 예방한다.

4.1.3 Replay 공격

제안 프로토콜에서는 로그인 과정에서 타임스탬프 T을 사용하여 네트워크 시스템에서 정한 인증 세션의 정상 유·무를 확인하면서 사용자와 인증서버 사이에 세션키 S_K을 공유하여 Replay 공격을 예방한다. 제안 프로토에서는 타임스탬프 T동안 사용자와 인증을 요구할 때마다 매번 서로 다른 세션키 S_K를 생성하여 사용하기 때문에 클라우드 환경처럼 분산 처리를 수행하는 환경에 적합하며 제공되는 서비스 별로 사용자 인증을 개별적으로 수행할 수 있다.

4.1.4 Man in the middle attack 공격

사용자와 인증서버사이에 주고받는 메시지에서 공격자가 SI와 UI을 알고 있다고 가정하면 공격자는 인증서버의 랜덤값 y을 알지 못하기 때문에 SI을 계산할 수 없다. 제안 프로토콜에서 SKK는 $SSK'(=g^{h(SI||UI)+h(x)} \bmod p)$을 이용하여 타임스탬프 T와 연접하여 해쉬함수 $h()$에 적용하여 메시지를 사용자와 인증서버 사이에 전달되는 동안 제3자가 인증서버의 랜덤값 y와 SKK 값을 알지 못하여 SI와 UI을 계산할 수 없다.

4.1.5 Impersonation 공격

제안 프로토콜에서는 사용자의 인식자 ID_U와 패스워드 PW_U를 직접적으로 전달하지 않고 해쉬 함수를 사용하여 사용자와 인증서버 사이에 전달되는 동시에 타임스탬프 T를 사용하여 인증과정을 수행하기 때문에 Impersonation 공격을 예방한다.

4.1.6 패스워드 추측 공격

제안 프로토콜은 일방향 해쉬 함수를 사용하여 패스워드 PW_U를 $h(ID_U \oplus h(PW_U \oplus x) \oplus h(x \oplus ID_U))$처럼 복잡하게 사용한다. 특히, 제안 프로토콜은 사용자와 인증 서버에서 생성한 랜덤값 x,y을 제 3자가 알지 못할 경우 패스워드를 추측하기가 어려워 패스워드 추측 공격을 예방한다.

4.2 성능 평가

해쉬함수의 충돌 확률을 구하기 위해서 성능 평가는 [13]에서 사용된 내용을 기반으로 평가하였으며, 해쉬함수의 충돌 확률을 위해 해쉬 체인에 대한 키 비트 수의 평균 변화, 평균 키 변화 확률, 키 비트 수의 표준 분산 그리고 평균 변화의 분산 확률 등의 (식 27) ~ (식 30)는 [14]에서 계산한 방법을 이용한다.

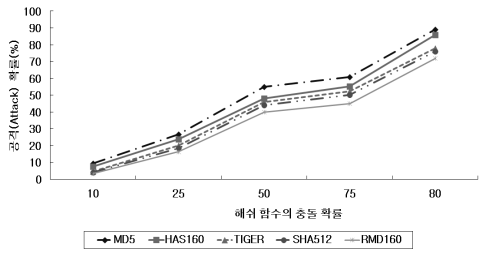
$$\overline{K} = \frac{1}{N}\sum_{i=1}^{N} K_i \quad \text{(식 27)}$$

$$P = \frac{\overline{K}}{128} \times 100\% \quad \text{(식 28)}$$

$$\triangle K = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(K_i - \overline{K})^2} \quad \text{(식 29)}$$

$$\triangle P = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(\frac{K_i}{128} - P)^2} \times 100\% \quad \text{(식 30)}$$

여기서, $\overline{K}$는 해쉬 체인에서 변환된 평균 키 길이 수를 의미하고, K_i는 i번째 해쉬 체인의 키 길이를 의미하고 N은 실험의 반복 횟수를 의미한다. P는 해쉬 체인에서 변환된 평균 키 변화 확률을 의미한다. (식 29)~(식 30)에서 $\triangle K$와 $\triangle P$는 해쉬 체인에서 변환된 키 길이의 표준분산 및 확률을 의미한다.



[그림 3] 해쉬 알고리즘별 해쉬 함수 충돌 확률에 따른 공격확률

[표 2] 제안 프로토콜과 기존 프로토콜의 비교 분석

구분	사용자 인증	권한 인증	바이오 인증	메시지인증	사용자 편의성	효율성
Ipath	ID/Password 기반	접근제어 정책	-	불가능	보통	보통
OpenEMed	인증서 기반	접근제어 정책	-	가능	보통	보통
TeleCardio-FBC	공개키 기반	-	-	불가능	보통	보통
WBASN	ID/Password 기반	-	바이오 인증 사용	불가능	편리	보통
CodeBlue	공개키 기반	-	바이오 인증 사용	가능	편리	보통
Medintegra Web	ID/Password 기반	접근제어 정책	바이오 인증 사용	불가능	편리	보통
[17]	무선 환경을 고려한 인증서기반	무선 환경을 고려한 인증서기반	바이오 인증 사용	가능	편리	높음
제안 프로토콜	일방향 해쉬함수와 XOR연산	접근제어 정책	-	가능	편리	높음

〔그림 3〕은 〔14〕에서 사용한 (식 27) ~ (식 30)을 이용하여 해쉬 알고리즘별로 제안 프로토콜에 적용하였을 경우 해쉬 함수의 충돌 확률별 공격확률을 보여주고 있다. 〔그림 3〕의 결과처럼 해쉬 함수의 충돌 확률이 증가할수록 공격 확률도 비례적으로 증가하였으며, 블록크기 512을 기준으로 알고리즘의 출력길이와 라운드 수가 좋을수록 공격확률이 낮게 나타났다.

〔표 2〕는 원격 의료 시스템의 보안 기술을 분석한 〔17〕을 확장하여 사용자 인증, 권한인증, 바이오 인증, 메시지 인증, 사용자 편의성, 효율성 등 6가지 측면에서 제안 프로토콜과 비교분석하고 있다. 기존 원격의료 시스템은 환자의 프라이버시 및 인증을 기본으로 제공하면서 사용자 인증을 위해 ID, 패스워드, 인증서등을 공개키 기반 및 생체 인증으로 사용하고 있다. 그러나 제안 프로토콜에서는 사용자 인증을 제공하기 위해서 일방향 해쉬 함수와 XOR 연산을 조합하여 연산 효율을 높였다. 또한, 기존 시스템은 ID, 패스워드 그리고 인증서 등을 분실하였을 경우 본인이 아니더라도 인증이 가능하기 때문에 의료 데이터에 대한 무결성을 보장 받지 못하는 문제점이 있지만 제안 프로토콜은 사용자 인증에 필요한 정보를 분실할 필요가 없어 기존 시스템 보다 보안 측면에서 안전하다.

V. 결 론

최근 인터넷 기술을 이용하여 서로 다른 물리적인 위치에 존재하는 자원을 서비스 받는 클라우드 컴퓨팅이 최근 주목받고 있다. 그러나 클라우드 컴퓨팅은 서로 다른 위치에 존재하는 자원을 사용자가 접속하여 사용하기 때문에 사용자가 악의적으로 데이터를 이용할 경우 클라우드 컴퓨팅 서비스를 제공받는 다른 사용자에게 피해를 줄 수 있는 문제점 있다. 본 논문에서는 서로 다른 물리적인 위치에 존재하는 사용자가 기밀 데이터를 안전하게 제공받으면서 임의의 사용자가 기밀 정보를 불법적으로 악용하는 것을 예방하기 위한 사용자 인증 프로토콜을 제안하였다. 제안 프로토콜은 사용자 인증 정보를 일방향 해쉬 함수와 XOR 연산만을 사용하여 인증 서버의 부하를 최소화하였으며, 분산 처리된 개인 인증 정보를 모두 중앙 서버에 집중하여 관리함으로써 클라우드 컴퓨팅의 사용자 보안 문제를 해결하였다. 향후 연구에서는 사용자에게 권한 접근 및 레벨을 부여하여 사용자의 프라이버시를 보장하는 연구를 수행할 계획이다.

VI. 참고문헌

〔1〕 김학범, 전은정, 김성준, "클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구," 공주대학교 KNU 경영컨설팅 연구소, 경영컨설팅리뷰, 2(1), pp. 127-144, 2011년 2월.

〔2〕 R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, J. Staddon, "Cloud Computing: Outsourcing Computation without Outsourcing Control," Palo Alto Research Center, 2009.

〔3〕 김현승, 박춘식, "클라우드 컴퓨팅과 개인 인증 서비스," 한국정보보호학회지, 20(2), pp. 11-19, 2010년 4월.

〔4〕 김명호, 김재우, 장현춘, "클라우드 컴퓨팅의 오늘과 내일," 한국정보보호학회지, 20(2), pp. 56-64, 2010년 4월.

〔5〕 이경하, 최현식, 정연돈, "클라우드 컴퓨팅에서의 대용량 데이터 처리와 관리 기법에 관한 조사," 한국정보과학회논문지:데이터베이스, 제38권 제2호, pp.104-125, 2011년 4월.

〔6〕 M. Mulazzani, S.Schrittwieser, M. Leithner, M. Huber, E. Weippl, "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space," Proc. of the USENIX Security Symposium, pp.43-54, Aug. 2011.

〔7〕 I-En Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over insecure networks," J. Comput. System Sci. 72(4), pp. 727-740, 2006.

〔8〕 V. Shoup, A. Rubin, "Session key distribution using smartcards," in: Proc. EUROCRYPT 96, in: LNCS., vol 1070, Springer-Verlag, 1996, pp. 321-333, 1996.

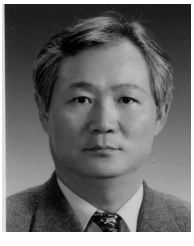
〔9〕 M. Bellare, P. Rogaway, "Provably secure session key distribution-The third party case," in:Proc. 27th ACM Symp. on Theory of Computing, ACM, LAS Vegas, 1995, pp. 57-66, 1995.

〔10〕 S. Lee, I. Ong, H. T. Lim, H. J. Lee, "Two factor authentication for cloud computing," International Journal of KIMICS, vol. 8, pp. 427-432.

〔11〕 Z. Shen, L.Li, F. Yan, X. Wu, "Cloud Computing System Based on Trusted Computing Platform," Intelligent International Conference on, vol. 1, pp.942-945.
〔12〕 A. Celesti, F. Tusa, M. Villari, A Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure," 19th IEEEInternational Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises(WETICE), pp. 263-265, 2010.
〔13〕 D. Xiao, X. F. Liao, and S. J. Deng, "One-way hash function construction based on the chaotic map with changeable-parameter," Chaos, Solitons & Fractals, 2005, vol.24, no. 1, pp. 65-71. 2005.
〔14〕 박길철, 정윤수, 김용태, 이상호, "무선 센서 네트워크에서 데이터 무결성을 보장하기 위한 다중 해쉬 체인 기법," 한국해양정보통신학회논문지, 14(10), pp. 2358-2364, 2010년 10월.
〔15〕 강승석, 손예진, 문은지, "클라우드 컴퓨팅 서비스 구현을 위한 네트워크 가상화 연구," 한국지역정보화학회지, 13(3), pp. 1-17, 2010년 9월.
〔16〕 장은영, 김형종, 박춘식, 김주영, 이재일, "모바일 클라우드 서비스의 보안위협 대응 방안 연구," 정보보호학회논문지, 21(1), pp. 177-186, 2011년 2월.
〔17〕 이유리, 박동규, "WPMI 기반 바이오 인증을 이용한 원격 의료 시스템," 한국정보통신학회논문지, 33(8), pp.279-284. 2008년 8월.

〈著者紹介〉

정 윤 수 (Yoon-Su Jeong) 정회원
1998년 2월: 청주대학교 전자계산학과 학사
2000년 2월: 충북대학교 대학원 전자계산학과 석사
2008년 2월: 충북대학교 대학원 전자계산학과 박사
2008년 3월~2009년 8월: 충북대 및 한남대 시간강사
2009년 9월~2012년 2월:한남대학교 산업기술연구소 전임연구원
2012년 3월~현재: 목원대학교 정보통신공학과 조교수
〈관심분야〉 정보보호, 멀티미디어, 네트워크 보안, 이동통신, 유·무선 통신, 암호이론



이 상 호 (Sang-Ho Lee) 정회원
1976년 2월: 숭실대학교 전자계산학과 학사
1981년 2월: 숭실대학교 대학원 전자계산학과 석사
1989년 2월: 숭실대학교 대학원 전자계산학과 박사
1981년 3월~현재: 충북대학교 전자정보대학 소프트웨어학과 교수
〈관심분야〉 네트워크보안, Protocol Engineering, Network Management