중소기업정보기술융합학회논문지 제1권 제1호 pp.29~37, 2011

클라우드 컴퓨팅에서 패스워드기반의 사용자 정보 가상화를 통한 사용자 프라이버시 보장 기법

정윤수[1*], 이상호[2]
[1]한남대학교 산업기술연구소, [2]충북대학교 컴퓨터과학과

A User Privacy Protection Scheme based on Password through User Information Virtuality in Cloud Computing

Yoon-Su Jeong[1] and Sang-Ho Lee[2]
[1]Industrial Technology research Institute, Hannam University
[2]Department of Computer Science, Chungbuk National University

요 약 정보통신 기술의 발달에 따라 정보화 영역이 점차 확대되면서 IT 분야에서는 서버나 스토리지, 네트워크와 같은 인프라 자원들을 언제 어디서나 효율적으로 이용할 수 있는 클라우드 컴퓨팅이 급부상하고 있다. 그러나 클라우드 컴퓨팅 기술을 사용하는 사용자에게는 개인정보 노출, 개인에 대한 감시, 개인 데이터에 대한 상업적 목적의 가공 등의 문제점이 발생할 수 있다. 이 논문은 클라우드 컴퓨팅 환경에서 인프라 자원을 사용하는 사용자 정보를 제3자가 이용할 없도록 가상의 사용자 정보를 생성하여 사용자 프라이버시를 보호하는 기법을 제안한다. 제안 기법은 사용자 정보를 익명의 값으로 가상화하여 제3자가 사용자의 신원을 확인할 수 없도록 사용자에게 부여된 PIN 코드와 조합하여 사용자 익명성을 보장한다. 또한 제안 기법은 클라우드 컴퓨팅에서 중요시 되는 개인 정보를 분산 인증 및 관리할 수 있어 모든 정보가 중앙으로 집중되는 클라우드 컴퓨팅의 사용자 보안 문제를 해결한다. 따라서 열악한 환경의 중소기업 정보화 수준 향상에 클라우드 컴퓨팅 기술의 활용 활성화에도 기여할 수 있다.

키워드 : 사용자 프라이버시, 클라우드 컴퓨팅, 정보 가상화

Abstract As the area of informatization has been expanding followed by the development of information communication technology, cloud computing which can use infra sources like server, storage, and network in IT area as an efficient service whenever and wherever skyrockets. But users who use cloud computing technology may have some problems like exposure personal data, surveillance on person, and process on commercial purpose on their personal data. This paper proposes a security technique which protect user's privacy by creating imaginary user information not to be used by other people. The proposed technique virtualizes user's information as an anonymity value not to let other people know user's identity by combining PIN code with it and guarantees user's anonymity. Also it can manage and certificate personal information that is important in cloud computing, so that it can solve security problem of cloud computing which centers all informations. Therefore this paper can assist upgrading of the level of information of poor SMBs through safe use of cloud computing.

Key Words : User privacy, Cloud computing, Information virtuality

*교신저자(bukmunro@gmail.com)
접수일(2011년 6월 30일), 심사완료일(2011년 9월 21일)

1. 서론

최근 인터넷 기술을 활용하여 정보를 인터넷상의 서버에 영구적으로 저장하고, 데스크톱, 태블릿컴퓨터, 노트북, 넷북, 스마트폰 등의 IT 기기 등과 같은 클라이언트에는 일시적으로 보관되는 컴퓨터 환경인 클라우드 컴퓨팅이 많은 관심을 받고 있다[1]. 클라우드 컴퓨팅이 널리 사용되는 이유는 무형의 형태로 존재하는 하드웨어, 소프트웨어 등의 컴퓨팅 자원을 자신이 필요한 만큼 빌려 쓰고 이에 대한 사용요금을 지급할 수 있고, 서로 다른 물리적인 위치에 존재하는 컴퓨팅 자원을 가상화 기술로 통합할 수 있기 때문이다.

클라우드 컴퓨팅을 도입한 기업 또는 개인은 컴퓨터 시스템을 유지·보수·관리하기 위하여 들어가는 비용과 서버의 구매 및 설치 비용, 업데이트 비용, 소프트웨어 구매 비용 등 엄청난 비용과 시간·인력을 줄일 수 있고, 에너지 절감에도 기여할 수 있어 특히 중소기업의 정보화에 크게 기여할 것으로 예상된다. 사용자가 PC에 자료를 보관할 경우 보통 하드디스크 장애 등으로 인하여 자료가 손실될 수도 있지만 클라우드 컴퓨팅 환경에서는 외부 서버에 자료들이 저장되기 때문에 안전하게 자료를 보관할 수 있고, 저장 공간의 제약도 극복할 수 있으며, 언제 어디서든 자신이 작업한 문서 등을 열람·수정할 수 있다. 하지만 서버가 해킹당할 경우 개인정보가 유출될 수 있고, 서버 장애가 발생하면 자료 이용이 불가능하다는 단점도 있다. 이 같은 결과는 클라우드 컴퓨팅이 제공하는 서비스 구조가 서로 다르기 때문이다[2,3]. 특히, 대용량 데이터의 저장장치인 데이터 센터는 클라우드 컴퓨팅 구조에서 중앙에 위치하고 있으며 데이터를 처리하는 프로세싱은 서버 내에 존재하여 클라이언트에게 데이터 보안과 같은 이용성을 제공하는 역할을 한다.

가트너 그룹과 ENISA 외에 다수의 자료에서 클라우드 컴퓨팅 환경에서의 관리적 보안의 중요성이 언급되고 있다. 클라우드 컴퓨팅을 통해 데이터가 연동되고 자원을 다양하게 활용하는 것에는 데이터 보호와 자원의 관리정책, 기업 비밀관리나 개인의 프라이버시 측면에서의 문제점도 존재한다.

클라우드 컴퓨팅 환경에서 서버가 다수의 클라이언트를 인증하기 위해서는 수천 비트의 상태 비트 정보가 필요하다[4,5,6]. 여기서 상태 비트 정보란 서버에서 동일한 클라이언트까지 가는 여러 경로 중 연결되어있는 링크(인터페이스)의 상태변화 정보를 의미한다. 현재 가장 보편적으로 이용되고 있는 상태 비트 방식은 OSPF(Open Shortest-Path)이며 이 방식은 네트워크에 특정 변화가 발생할 경우에만 전체 라우팅 테이블이 아닌 해당 변화된 사항만을 선별적으로 교환하여 네트워크의 효율성을 유지할 수 있는 특징이 있다. 기존 기법에서는[7,8,9] 인증 복구 이슈를 명확하게 표시하지 않았을 뿐만 아니라 복구 문제 또한 언급하지 않았다. 반면 [10,11,12]에서는 이동 노드에게 인증서 폐기 목록(CRL, Certificate Revocation List)을 넣기 위해서 프로액티브(proactive) 메커니즘을 적용하고 있지만 프로액티브 삽입 방법은 네트워크 자원을 계속적으로 소비하고 있어 효율성이 떨어지는 단점이 있다.

이 논문에서는 클라우드 컴퓨팅의 기본 요소인 특정 서버에 존재하는 데이터를 서로 다른 물리적인 위치에 존재하는 사용자가 제공받을 경우, 임의의 사용자의 정보가 제3자에 의해 불법적으로 악용되는 것을 예방하기 위하여 가상의 사용자 정보를 생성하여 사용자의 프라이버시를 보호하는 보안 기법을 제안한다. 제안 기법은 사용자 정보를 익명의 값으로 가상화하여 제3자가 사용자의 신원을 확인할 수 없도록 사용자에게 부여된 PIN 코드를 가상화된 사용자 정보와 조합하여 사용자 익명성 코드를 생성한다. 또한 제안 기법은 클라우드 컴퓨팅에서 중요시 되는 개인 정보를 분산 처리할 수 있어 모든 정보가 중앙으로 집중되는 클라우드 컴퓨팅의 사용자 보안 문제를 해결하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 클라우드 컴퓨팅과 클라우드 컴퓨팅 보안 요구사항을 알아본다. 3장에서는 사용자의 익명성을 보장하기 위한 PIN 코드 기반의 사용자 정보 가상화 기법을 제안한다. 4장에서는 제안 기법의 효율성과 보안성을 분석하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 클라우드 컴퓨팅의 개념

클라우드 컴퓨팅은 IT와 관련된 다양한 자원(하드웨어와 플랫폼, 소프트웨어 등)을 웹 형태의 거대한 구름 속에 넣어두고, 이러 자원이 필요한 사용자는 웹을 통해 접속하여 필요한 만큼씩 사용하고 그에 따른 비용을 지불하는 서비스를 의미한다[1,2].

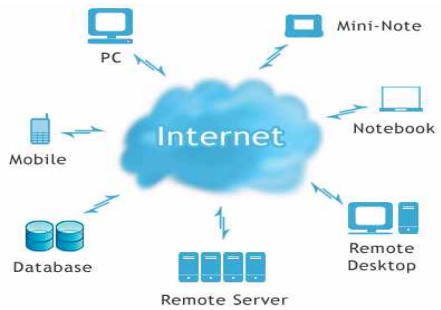

그림 1. 클라우드 컴퓨팅 환경
Fig 1. Cloud computing environment

클라우드 컴퓨팅은 서비스 종류에 따라 SaaS (Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service) 등 3가지로 분류하고 있다. SaaS은 특정 소프트웨어를 필요한 시기에만 웹으로 접속하여 사용하며, 그에 따른 요금을 과금하는 형태의 서비스이다. PaaS은 개발을 위한 플랫폼을 구축할 필요없이 웹에서 빌려쓸 수 있게 만든 방식이다. IaaS은 서버, 스토리지, 네트워크 장비 등의 IT인프라 장비를 가상화 환경으로 구축하여 필요에 따라 빌려 쓰는 방식이다.

클라우드 컴퓨팅 환경을 구축하기 위하여 가장 기본이 되는 가상화 기술은 한 대의 물리적인 장비 중에서 현재 사용되지 않는 부분을 마치 다른 장비 한 대가 추가된 것처럼 인식시켜 업무를 수행하거나 여러 대의 장비를 잠시 동안 연결시켜 고성능, 고용량 장비처럼 활용할 수도 있다[2].

2.2 클라우드 컴퓨팅과 타 컴퓨팅과의 비교

그리드 컴퓨팅은 대용량의 컴퓨팅 리소스를 필요로 하는 문제해결을 위해 인터넷 상에 분산된 컴퓨팅 리소스들을 연결하여 가상의 슈퍼컴퓨터와 같이 사용하는 컴퓨팅 모델로 과학, 수학 등 학술적인 분야에서 활용된다. 클라우드 컴퓨팅은 분산된 IT 자원을 통합하여 사용한다는 차원에서 그리드 컴퓨팅의 분산 컴퓨팅 환경과 유사하지만, 그리드 컴퓨팅은 인터넷을 통해 서버와 PC의 사용하지 않는 자원을 활용하는 것이며, 클라우드 컴퓨팅은 개별적인 서비스 사업자의 가상화된 서버 네트워크를 이용한다는 차원에서 차이가 있다. 즉, 그리드가 인터넷 상의 모든 컴퓨팅 리소스를 연결하는 그물망을 의미하며, 클라우드 컴퓨팅은 사업주체인 서비스 제공자가 제공하는 컴퓨팅 네트워크를 의미한다[2].

유틸리티 컴퓨팅은 사용자가 컴퓨팅 자원을 전기나 수도 등 유틸리티와 같이 필요할 때마다 연결하여 사용하고 사용량에 따라 비용을 지불하는 과금 모형으로 볼 수 있다[4]. 클라우드 컴퓨팅은 인터넷 상의 분산 시스템을 활용하여 컴퓨팅 자원을 서비스로 이용하고, 사용량에 기반하여 비용을 지불한다. 따라서 기술적으로는 그리드의 분산 컴퓨팅을 과금모형으로 유틸리티 컴퓨팅을 택하는 컴퓨팅 개념으로 볼 수 있다. 서버기반 컴퓨팅은 서버에 어플리케이션과 데이터를 두고 필요할 때마다 접속해서 사용하는 방식이다. 데이터의 모든 처리는 서버에서만 이루어지고, 클라이언트는 단순히 입출력만을 처리하는 씬클라이언트의 역할을 담당한다. 클라우드 컴퓨팅이 저사양의 단말기를 통해서도 서버에서 처리되어 제공되는 높은 수준의 서비스를 이용할 수 있다는 차원에서 서버기반 컴퓨팅이 가지는 특성을 포함하고 있다.

그러나 서버기반 컴퓨팅은 사용자를 위한 물리적인 서버가 제공하고 이에 대한 활용의 권한도 사용자가 가진다. 하지만 클라우드 컴퓨팅에서 사용자는 가상화된 서버네트워크를 통해 서비스를 이용할 뿐 물리적인 서버에 대한 정보나 권한을 가지지 못한다.

네트워크 컴퓨팅은 서버에 어플리케이션을 저장하여 사용한다는 점에서 서버기반 컴퓨팅과 비슷하지만, 어플리케이션을 서버로부터 로드하여 로컬에서 실행하기 때문에 자신의 컴퓨팅 자원을 상당부분 사용하게 된다는 점에서 차이가 난다. 클라우드 컴퓨팅은 클라우드 상에서 IT 자원을 서비스로 이용한다는 차원에서 네트워크 컴퓨팅과 구분되어 진다.

2.3 클라우드 컴퓨팅 보안 연구

최근까지 IT 기술의 꾸준한 발달로 인하여 클라우드 컴퓨팅 보안에 관한 연구 또한 꾸준히 연구되고 있다[19]. Rivest et al. 기법[13]은 IPSec과 유사한 독립적인 보안 레이어를 제공하는 프로토콜을 기반으로 HMAC을 생성하며 IP 패킷 전체에 대해 해쉬 다이제스트를 수행한다. 그러나 이 기법은 MITM 공격을 예방하기 위해 IGMP 메시지 인증을 수행할 경우 추가적인 인증 연산 시간에 따른 오버헤드가 발생할 수 있으며 서버의 패킷 처리량이 감소하는 단점이 있다[3,19].

Zhao et al. 기법[14]은 MITM 공격을 예방하기 위해서 의사 난수 생성 함수로써 NIST에서 제안하는 G-DES, G-SHA[15] 등을 사용하여 16비트의 의사 난수를 생성

한다. Zhao et al. 기법은 인증 헤더가 적은 비트수를 차지하는 만큼 헤더의 생성 시간과 인증 시간은 적게 걸리지만 적은 비트 수의 사용으로 인해 무차별 대입 공격에 취약할 수 있고 제 3자가 서버와 사용자 장치 사이에서 패킷을 가로채 의사 난수 필드를 제외한 부분을 수정하여 위조 공격이 일어날 경우 인증 메커니즘을 그대로 통과할 수 있는 단점이 있다[19].

Murph. et al.[16]은 디지털 서명을 통한 라우팅 정보에 대한 무결성과 근원지 인증을 제공하기 위한 인증 메커니즘을 제안하였다. 이 기법은 라우터간 패스워드를 공유하거나 비밀키 공유를 기반으로 MAC(Message Authentication Code) 값을 계산하는 방법을 사용하였으나 비밀키 기반의 MAC도 라우터가 다른 모든 라우터와의 서로 다른 비밀키를 공유하는 것을 전제로 하기 때문에 시스템 운영상 효율성이 떨어지는 문제점이 있다[19].

Cheng[17]는 라우팅 정보를 송신하는 라우터가 자신이 임의로 생성한 비밀키로 먼저 MAC을 계산하여 수신자 라우터에게 보내고, 나중에 그 MAC을 확인할 수 있는 비밀키를 보내는 기법을 제안하였다. 그러나 라우팅 정보를 수신한 라우터가 수신된 라우팅 정보의 인증 확인 작업 없이 라우팅 테이블을 먼저 작성하는 단점이 있다[19].

Zang[18]는 해쉬체인에 기반을 둔 일회용 디지털 서명 방식의 인증 메커니즘을 제안하였다. 그러나 라우팅 정보에 해수함수를 적용해서 나온 각각의 비트에 대해서 일회용 서명을 하는 방식이기 때문에 서명의 길이가 너무 커진다는 단점이 있다[19].

3. PIN 코드를 이용한 사용자 정보의 가상화 기법

이 절에서는 클라우드 컴퓨팅 환경에서 사용자의 익명성을 보장하기 위해서 사용자에게 부여된 PIN 코드를 가상화한 개인정보와 조합함으로써 제3자가 사용자의 정보를 불법적으로 도용하지 못하는 보안 기법을 기술한다.

3.1 개요

특정 서버에 존재하는 데이터를 서로 다른 물리적인 위치에 존재하는 사용자가 서비스를 받을 경우, 임의의 사용자가 원격에서 특정 서버에 존재하는 데이터의 액세스 및 서버의 안전한 인증을 보장하기 위해서 제안 기법은 [그림 1]과 같은 환경에서 PIN 코드를 가상화한 개인정보와 조합하여 익명의 보안 인식자를 생성하여 사용자의 익명성을 보장한다.

그림 2은 제안된 인증 메커니즘의 클라우드 컴퓨팅 환경을 보여주고 있다. 그림 2에서 제안된 기법은 분산된 시스템을 통해 사용자에게 서비스를 제공하여 비용 절감을 가져올 수 있으며 외부 사용자는 클라우드 플랫폼이 제공하는 통합 인증 시스템을 이용하여 서버내의 시스템에 접근할 수 있다.

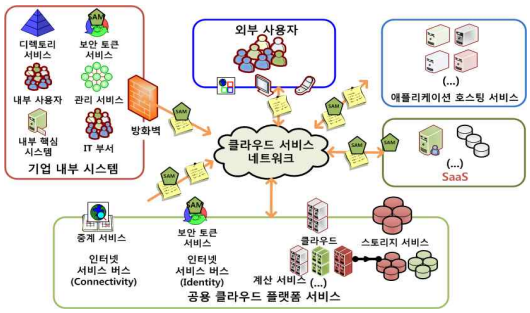

그림 2. 제안 메커니즘의 클라우드 컴퓨팅 환경
Fig 2. Cloud computing environment of proposed mechanism

3.2 용어 정의

표 2는 제안된 인증 메커니즘에서 사용하는 주요 용어에 대한 설명이다.

표 2. 용어 정의
Table 2. Parameter definition

용어	정 의
U	사용자
AS	인증서버
CS	콘텐츠 센터
ID_U	사용자 U의 인식자
PW_U	사용자 U의 패스워드
APW_x	x의 익명 패스워드
RND_x	x가 생성한 랜덤 수
$SK_{U\_AS\_CS}$	사용자, 인증서버, 콘텐츠 서버 간 사전에 안전하게 공유된 공유키
$E(K, Data)$	키 K을 이용하여 $Data$을 암호화
$D(K, Data)$	키 K을 이용하여 $Data$을 복호화
$R\_Message$	서비스 목록 요청 메시지
$Service\_List$	서비스 목록
$A\_Message$	서비스 확인 메시지

3.2 정보 가상화를 이용한 사용자 인증

클라우드 컴퓨팅 환경에서 다수의 사용자가 특정 자원(혹은 데이터 혹은 자료)을 공유해서 사용하는 경우가 빈번하게 발생하기 때문에 특정 자원의 공유 상태에 따라서 클라우드 환경의 전체 효율성에 많은 영향을 미친다. 제안 기법에서는 특정 서버에 존재하는 자원을 임의의 사용자가 안전하게 서비스 받을 수 있도록 사용자가 보유하고 있는 PIN 코드를 이용하여 사용자의 정보를 가상화하여 익명의 보안 인식자를 통해 안정성을 보장한다. 이 때, 제안 기법은 등록과정, 인증과정, 유지보수과정 등의 3단계를 수행하고, 해당 지역에 공개키 기반구조가 존재하여 데이터를 수신하는 지역에서는 인증기관의 역할을 수행하는 서버가 존재한다고 가정한다.

3.2.1 등록과정

등록과정은 클라우드 컴퓨팅의 서비스를 제공받는 사용자(User, U)가 인증서버(Authentication Server, AS)에게 서비스를 요청하기 전에 사용자의 정보를 인증서버에 등록하는 과정이다. 제안 기법의 등록과정은 4단계로 동작되며 사용자의 인식자 ID_U와 패스워드 PW_U가 필수적이다.

- 단계 1 : 사용자와 인증서버 사이에 SSL (Secure Socket Layer) 연결이 확립되면 사용자는 인식자 ID_U와 패스워드 PW_U를 인증서버에게 전송한다. 인증서버는 전송된 내용을 확인한다.

$$Transfer \quad ID_U,\ PW_U \qquad \text{(식 1)}$$

- 단계 2 : 인증 서버는 전송된 내용을 확인한 후 랜덤 수 RND_{AS}을 생성한다. 인증 서버는 사용자의 인식자 ID_U와 패스워드 $APW_U(=ID_U \bullet g^{PW_U})$를 랜덤 수 RND_{AS}와 함께 해쉬 함수 $H(\bullet)$에 적용하여 익명의 보안 인식자 SID_U를 생성한다. 서버는 생성된 보안 인식자와 인증 서버 자신이 생성한 랜덤 수 RND_{AS}를 쌍으로 데이터베이스에 저장한다.

$$Generate \quad RND_{AS} \qquad \text{(식 2)}$$

$$SID_U = RND_{AS} \oplus H(ID_U,\ APW_U) \qquad \text{(식 3)}$$

- 단계 3 : 인증 서버는 클라우드 컴퓨팅 환경에서 사전에 안전하게 공유된 공유키 $SK_{U_AS_CS}$을 이용

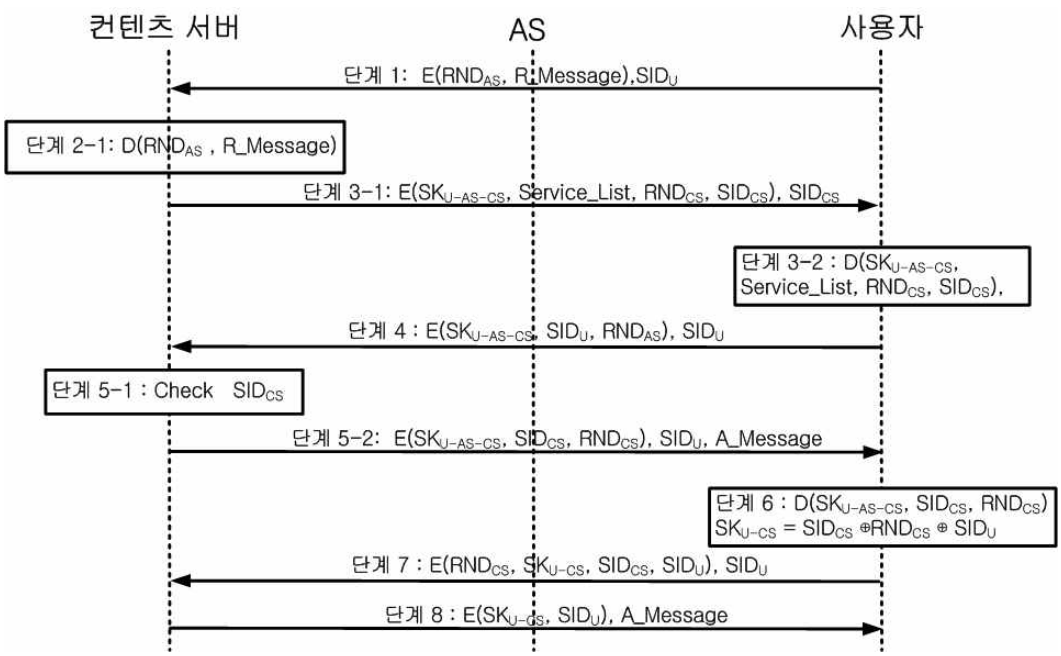

그림 3. Registration 과정
Fig 3. Registration Process

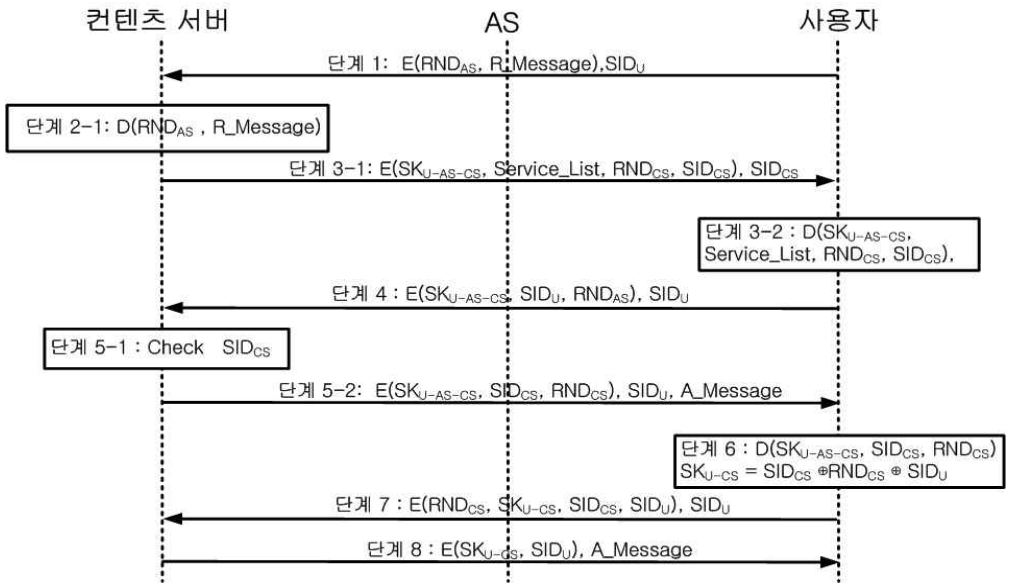

그림 4. 인증 과정
Fig 4. Authentication Process

하여 사용자의 보안 인식자 SID_U와 랜덤 수 RND_{AS}을 사용자와 콘텐츠 서버에게 암호화하여 전송한다.

$$E(SK_{U\_AS\_CS},\ SID_U,\ RND_{AS}) \qquad (식\ 4)$$

- 단계 4 : 인증서버는 랜덤 수 RND_{AS}를 전달한 후 사용자와 인증서버 사이의 SSL 연결을 종료한다.

3.2.2 인증과정

인증과정은 클라우드 컴퓨팅 환경에서 사용자가 서비스를 제공받고자 할 때 인증서버로부터 사용자 인증 유·무를 수행하는 과정이다.

- 단계 1 : 사용자는 인증서버로부터 전달받은 랜덤 수 RND_{AS}를 이용하여 서비스 목록 요청 메시지 $R_Message$를 암호화하여 사용자의 보안 인식자 SID_U와 함께 콘텐츠 서버에게 전달한다.

$$E(RND_{AS},\ R\_Message),\ SID_U \qquad (식\ 5)$$

- 단계 2 : 콘텐츠 서버는 인증서버로부터 전달받은 SID_U와 매칭되는 랜덤수 RND_{AS}를 이용하여 서비스 목록 요청 메시지를 복호화한다.

$$D(RND_{AS},\ R\_Message) \qquad (식\ 6)$$

- 단계 3 : 콘텐츠 서버는 사전에 안전하게 공유된 공유키 $SK_{U_AS_CS}$를 이용하여 서비스 목록 $Service_List$과 자신의 생성한 랜덤 수 RND_{CS} 그리고 인증서버에 사전 등록된 콘텐츠 서버의 보안 인식자 SID_{CS}를 암호화한 (식 7)를 사용자에게 전달한다.

$$E(SK_{U\_AS\_CS},\ Service\_List,\ RND_{CS},\ SID_{CS}),\ SID_{CS} \qquad (식\ 7)$$

- 단계 4 : 사용자는 콘텐츠 서버로부터 전달받은 정보를 복호화한 후 콘텐츠 서버의 보안 인식자 SID_{CS}와 RND_{CS}를 공유키 $SK_{U_AS_CS}$로 암호화한 후 사용자의 보안 인식자 SID_U와 함께 인증 서버에게 전달한다.

$E(SK_{U\_AS\_CS}, SID_{CS}, SID_U, RND_{CS}), SID_U$ (식 8)

- 단계 5 : 인증서버는 사용자로부터 전달받은 정보를 복호화한 후 콘텐츠 서버의 정보를 데이터베이스에 저장되어 있는 정보와 검증한다. 검증이 완료되면 인증 서버는 사용자에게 확인 메시지 $A_Message$를 전달하고 검증이 완료되지 않으면 서비스를 종료한다.

$Check \quad SID_{CS}$ (식 9)

$E(SK_{U\_AS\_CS}, SID_{CS}, RND_{CS}),$
$SID_U, A\_Message$ (식 10)

- 단계 6 : 사용자는 인증서버로부터 전달받은 정보를 복호화한 후 콘텐츠 서버와 사용자 간 공유할 공유키 SK_{U_CS}를 생성한다.

$D(SK_{U\_AS\_CS}, SID_{CS}, RND_{CS})$ (식 11)

$SK_{U\_CS} = SID_{CS} \oplus RND_{CS} \oplus SID_U$ (식 12)

- 단계 7 : 사용자는 콘텐츠 서버의 랜덤 수 RND_{CS}로 사용자와 콘텐츠 서버사이에 공유될 공유키 SK_{U_CS} , 콘텐츠 서버의 보안 인식자 SID_{CS}, 사용자의 보안 인식자 SID_U를 암호화하여 콘텐츠 서버에게 전달한다.

$E(RND_{CS}, SK_{U\_CS}, SID_{CS}, SID_U), SID_U$ (식 13)

- 단계 8 : 콘텐츠 서버는 사용자로부터 전달된 메시지를 RND_{CS}로 복호화한 후 사용자 보안 인식자 SID_U를 SK_{U_CS}로 암호화한 후 확인 메시지와 함께 사용자에게 전달한다.

$E(SK_{U\_CS}, SID_U), A\_Message$ (식 14)

3.2.3 유지보수과정

사용자는 등록과정에서 입력한 패스워드 PW_U를 변경할 수 있다. 유지보수 과정은 서비스를 제공받는 사용자가 임의 시간에 패스워드를 변경하는 과정으로써 사용자의 패스워드를 변경하는 과정은 식 (15)와 같다. 식 (15)에서 사용자는 $SID_U^{'}$를 계산한 후 인증서버와 콘텐츠 서버에 저장되어 있는 SID_U를 $SID_U^{'}$로 변경한다.

$SID_U^{'} = RND_{AS} \oplus H(ID_U, APW_U)$ (식 15)

4. 평가

제안 기법의 상호 인증과정을 통해 생성된 세션키 SK는 인증서버와 사용자만이 알고 있는 익명의 정보로써 제 3자는 알 수 없는 값이다. 제안 기법에서는 매 통신마다 서로 다른 세션키 SK가 생성되며 생성된 세션키 SK는 평문(plaintext) 공격의 암호 알고리즘 공격 예방 및 사용자 프라이버시를 보호하고 있다.

제안 기법은 클라우드 환경에서 발생하기 쉬운 cloning 문제를 해결하기 위해 사용자의 인식자 ID_U와 패스워드 $APW_U(=ID_U \bullet g^{PW_U})$를 해쉬 함수 $H(\bullet)$에 적용하여 보안 인식자 $SID_U = RND_{AS} \oplus H(ID_U, APW_U)$ 를 생성함으로써 사용자의 익명성을 보장하면서 사용자 프라이버시를 보호한다. 제안 기법에서 생성되는 사용자의 보안 인식자 SID_U는 수신기마다 서로 다른 보안 인식자 SID_U를 사용하기 때문에 제 3자가 복제된 자신의 정보를 다른 수신기에 적용할 경우 수신기가 사용자를 인식하지 못하여 익명성을 보장받고 있다. 이러한 방법은 수신기에 등록된 사용자의 인식자와 수신기가 해쉬함수에 의해 생성된 인식자 값이 서로 달라 cloning 문제를 예방하고 있다. 따라서 복제된 스마트카드를 사용하는 사용자는 제안 프로토콜의 해쉬 함수에 의해 생성되는 인식자를 판별하기 어려워 제 3자가 자신의 스마트카드를 가지고 다른 수신기를 사용하는 것은 사실상 불가능하다.

불법적인 제3자가 가입자의 인증 정보 및 개인정보를 획득하려고 시도하더라도 제안 기법에서는 메시지를 중간에 가로채더라도 인증서버와 사용자사이에 공유된 세션키 SK을 모르기 때문에 개인정보 유출을 방지한다. 또한 제안 기법은 공격자가 세션을 하이재킹 하더라도 사용자 익명성을 위해 사용하는 보안 인식자 SID_U를 재

사용할 수 없으며, ID기반 공개키/개인키 쌍을 통해 하이재킹으로부터 원천적으로 봉쇄가 가능하다.

제안 기법은 cloning 문제이외에 McCormac Hack 문제 또한 예방하고 있다. McCormac 문제는 제3자가 소유하고 있는 스마트카드를 이용하여 다른 스마트카드가 전송한 메시지를 다른 수신기에게 전달하도록 하는 방법으로써 제안 프로토콜에서는 이 공격을 예방하기 위해 스마트카드와 수신기사이에서 생성된 세션키 정보를 다른 위치에 위치하는 수신기가 알지 못하도록 해쉬 함수와 서명키 기반의 암호 알고리즘을 사용하고 있다. 만일 스마트카드와 수신기 사이의 통신 과정 중에 발생되는 임의의 통신 메시지를 공격자가 스마트카드에 저장하더라도 제안 프로토콜의 세션키 SK는 매 통신마다 서로 다른 세션키가 생성되어 공격자의 스마트카드와 일치하지 않게 된다. 수신기는 공격자가 가지고 있는 스마트카드 내에 저장되어 있는 메시지를 복호화 할 수 없게 되어 서비스를 제공받지 못하게 된다.

5. 결론

최근 인터넷 기술을 활용하여 IT 자산을 타 사용자와 공유함으로써 효율성을 증대하여 비용을 절감할 수 있는 클라우드 컴퓨팅 기술이 연구되고 있다. 그러나 클라우드 컴퓨팅은 서버가 해킹당할 경우 개인정보가 유출될 수 있고, 서버 장애가 발생하면 자료 이용이 불가능하다는 단점도 있다. 이 논문에서는 특정 서버에 존재하는 데이터를 서로 다른 물리적인 위치에 존재하는 사용자가 제공받을 경우, 임의의 사용자의 정보가 제3자에 의해 불법적으로 악용되는 것을 예방하기 위하여 가상의 사용자 정보를 생성하여 사용자의 프라이버시를 보호하는 보안 기법을 제안했다. 제안 기법은 사용자 정보를 익명의 값으로 가상화하여 제3자가 사용자의 신원을 확인할 수 없도록 사용자에게 부여된 PIN 코드를 가상화된 사용자 정보와 조합하여 사용자 익명성 코드를 생성하였다. 또한 제안 기법은 클라우드 컴퓨팅에서 중요시 되는 개인 정보를 분산 처리할 수 있어 모든 정보가 중앙으로 집중되는 클라우드 컴퓨팅의 사용자 보안 문제를 해결하였다. 보안 평가 결과 제안 기법은 사용자 요구에 의해 메시지 무결성과 인증을 수행하기 때문에 기존 기법보다 보안 공격에 안전성이 높다. 따라서 열악한 환경의 중소기업들이 클라우드 컴퓨팅의 장점을 안전하게 활용할 수 있어 중소기업의 정보화 수준 향상에 크게 기여할 수 있다. 향후 연구에서는 이동 사용자의 권한 접근 및 레벨을 부여하여 사용자 프라이버시를 보장하는 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

[1] C. S. Lim, “Cloud Computing Security Technology”, Review of KIISC, Vol. 19, No. 3, pp. 14-17, Jun. 2009.

[2] S. K, Un, “Trend of Cloud Computing Security Technology“, Review of KIISC, Vol. 20, No. 2, pp. 27-31, Apr. 2010.

[3] H. S. Kim, C. S. Park, “Cloud Computing and Personal Authentication Service”, Review of KIISC, Vol. 20, No. 2, pp. 11-19, Apr. 2010.

[4] R. Hauser, T. Przygienda, and G. Tsudik, "Reducing the Cost of Security in Link State Routing," Computer Networks and ISDN Systems, vol. 31, no. 8, pp. 885-894, Apr. 1999.

[5] S. Cheng, "An Efficient Message Authentication Scheme for Link State Routing," In Proc. Of the 13th Annual Computer Security Applications Conference, SanDiego, California, pp. 990-998, Dec. 1997.

[6] K. Zhang, "Efficient Protocols for Signing Routing Messages," In Symposium on Network and Distributed Systems Security, San Diego, California, Dec. 1998.

[7] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in Proc. of IEEE WSAAN'03, pp. 342-346, Jul. 2003.

[8] M. Bechler, H. J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A cluster-based security architecture for ad hoc network," in Proc. of IEEE INFOCOM2004, Vol. 4. pp. 2393-2403, Mar. 2004.

[9] A. Weimerskirch and G. Thonet, "A distributed Lightweight authentication model for ad-hoc networks," in Lecture Notes in Computer Science, K. Kim, ed., vol. 2288, Springer-Verlag, pp. 314-324, Nov. 2002.

[10] H. Luo. J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and robust access control for mobile ad-hoc networks,", IEEE/ACM Transaction on Networking, Vol. 12, Issue : 6, pp. 1049-1063, Dec. 2004.

[11] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 2, no. 1, pp. 52-64,

Jan.-March. 2003.
[12] S. Yi an R. Kravets, "MOCA: moblil certificate authority for wireless ad hoc networks," in Proc. of PKI'03, pp.65-79, Sep. 2003.
[13] R. L. Rivest and A. Shamir, "PayWord and MicroMint Two Simple Micropayment Schemes," Proc. of 1996 Int., Workshop on Security Protocols, LNCS 1189, pp. 69-87, Apr., 1996.
[14] F. Zhao, Y. Shin, S. F. Wu, H. Johnson, A. Nilsson, "RBWA: An Efficient Random-bit Window-based Authentication Protocol," GLOBECOM '03, vol. 3, pp. 1379-1383, 2003.
[15] "Random Number Generation and Testing," http://csrc.nist.gov/rng/
[16] S. Murphy and M. Badger, "Digital Signature Protection of the OSPF Routing Protocol" In Proc. of the Symposium on Network and Distributed System Security, pp. 93-102, Feb. 1996.
[17] S. Cheng, "An Efficient Message Authentication Scheme for Link State Routing," In Proc. of the 13th Annual computer Security Applications Conference, San Die해, California, pp. 90-98, Dec. 1997.
[18] M. T. Goodrich, "Efficient and Secure Network Routing Algorithm," provisional patent filing, U.S.A, 2001.
[19] Y. S. Jeong and Y. T. Kim, "An Authentication and Integrity Guarantee Mechanism of Flooding Packet based on Double Hash Chain", Journal of Korean Institute of Information Technology, Vol. 9, No. 1, pp. 147-157, Jan. 31. 2011.

저 자 소 개

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월: 청주대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2009년 9월 ~ 현재 : 한남대학교 산업기술연구소 전임연구원

<관심분야> : 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

이 상 호(Sang-Ho Lee) [정회원]

- 1976년 2월 : 숭실대학교 전자계산학과 학사
- 1981년 2월 : 숭실대학교 전자계산학과 석사
- 1989년 2월 : 숭실대학교 전자계산학과 박사
- 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> : 네트워크보안, Protocol Engineering Network Management,