Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 1 pp. 32-39, 2017

https://doi.org/10.5762/KAIS.2017.18.1.32
ISSN 1975-4701 / eISSN 2288-4688

모바일 클라우드 환경에서 생체인식을 이용한 사용자 인증 프로토콜 설계

김형욱*, 김범용, 전문석
숭실대학교 컴퓨터학과

A Design of User Authentication Protocol using Biometric in Mobile-cloud Environments

Hyung-Uk Kim*, Bumryong Kim, Moon-Seog Jun
Department of Computer Science and Engineering, Soongsil University

요 약 최근 모바일 클라우드 서비스가 증가하고 있으며, 특히 하나의 클라우드 컴퓨팅 서비스의 제약을 넘어 멀티 클라우드 방식에 관한 연구가 활발하게 진행되고 있다. 멀티 클라우드 환경에서 상호 협약된 서비스 제공자들 간의 추가적인 클라우드 서비스를 이용하기 위해 사용자는 다중 인증이 필요하다. 기존 연구에서 SSO를 이용한 방식은 SSO 서버를 통해 모든 인증이 이루어지기 때문에 악의적인 공격에 의해 SSO 서버의 서비스 불가 시 모든 클라우드 서비스 사용이 불가능하다. 또한 브로커를 이용한 방식에서는 사용자가 가입하지 않은 서비스 제공자에게 인증정보를 노출하게 되는 취약점이 존재한다. 본 논문에서는 추가 클라우드 사용 시 노출이 없는 생체인식을 이용한 안전한 사용자 인증 프로토콜을 제안한다. 제안하는 프로토콜은 멀티 클라우드 환경에서 각각의 클라우드에 인증을 위한 정보를 저장하지 않으며 한 번의 생체인증으로 여러 클라우드를 사용할 수 있다. 키의 안정성 측면에서 키 합의 과정과 키 공간 크기를 통해 안정성을 확보하였으며 중간자 공격, 재생 공격 등의 다양한 공격 방식에 대한 무력화를 통한 안전한 모바일 클라우드 서비스를 제공한다.

Abstract Recently, usage of mobile cloud services has been increasing. In particular, beyond the constraints of a single cloud computing service, studies on the multi-cloud have been actively pursued. A user must authenticate multiple cloud service providers to use additional cloud services in a multi-cloud. In previous studies, an authentication method using single sign-on (SSO) was not available in all cloud services. Cloud services will not be available when the SSO server is not available due to malicious attacks, because all authentication is done via the SSO server. Additionally, using a broker, there is a vulnerability that can expose authentication information for the service provider to a user who did not sign up. In this paper, we propose a secure user authentication protocol using biometric authentication that does not expose user information when using additional cloud services. The proposed protocol can use a single biometric authentication for multi-cloud services without storing authentication information in each cloud service. In terms of key stability (to ensure stability through the key agreement process and the key area), by disabling various attack methods, such as man-in-the-middle attacks and replay attacks, we provide secure mobile cloud services.

Keywords : Authentication, Biometric, Cloud Broker, Mobile-cloud, Multi-cloud

1. 서론

클라우드 라우드 컴퓨팅 서비스는 인터넷 기술과 가상화 기술에 기반을 둔 컴퓨팅 기술로서 IT 자원(프로세싱, 스토리지, 서버, 네트워크, SW 등)을 필요한 만큼 빌려 쓰고, 서비스 부하에 따라 실시간으로 확장할 수 있으

*Corresponding Author : Hyung-Uk Kim(Soongsil University)
Tel: +82-10-5280-3196 email: ddarajaengi@gmail.com
Received September 5, 2016 Revised (1st September 19, 2016, 2nd September 29, 2016)
Accepted January 6, 2017 Published January 31, 2017

며, 사용량에 따라 비용을 내는 컴퓨팅 서비스로 정의된다. 최근 모바일에서 클라우드 서비스를 이용하는 사례가 늘고 있으며, 특히 사용자가 하나의 클라우드 서비스 제공자와 계약을 맺고 이용할 때, 필요에 따라 다른 클라우드 서비스 제공자로부터 추가적인 서비스를 제공 받을 수 있는 멀티 클라우드 환경이 주목받고 있다[1]. 하지만 사용자는 추가적인 다른 클라우드 서비스 제공자에게서 서비스를 받을 때 자신과 계약하지 않은 서비스 제공자에게 직접 접속해야 하므로 안전한 인증정보의 연계와 개인정보의 보호가 필요하다. 그 이유는 여러 클라우드 서비스 제공자에게 개인정보를 제공하였을 때 악의적인 공격자로부터 개인정보가 탈취되어 악용되는 보안 위협이 발생할 가능성이 커지기 때문이다.

이러한 문제점을 해결하기 위해 하나의 인증정보를 이용하여 여러 클라우드 서비스를 이용할 수 있는 SSO(Single Sign-On) 기반의 방식, Broker(Cloud Service Broker) 기반의 방식 등이 제안되었다. SSO를 이용한 통합 인증 방식은 SSO 서버가 공격과 같은 문제가 발생하여 정상적으로 작동하지 못하면 그를 이용하는 모든 클라우드 서비스에 접근할 수 없는 문제를 가지고 있다. 한편 브로커 기반의 멀티 클라우드 모델에서는 클라우드 서비스 브로커가 각 클라우드 제공자 사이에서 중개와 인증을 담당하는 역할을 한다[2].

따라서 본 논문에서는 멀티 클라우드 환경에서 생체인식을 사용하는 브로커 기반의 새로운 인증기법을 제안한다. 사용자는 자신이 정당한 사용자임을 증명하기 위해 생체인식을 이용해 인증하게 되며, 기존 클라우드 외에 추가로 사용하는 클라우드들에는 직접적인 인증정보 노출 없이 인증이 가능하도록 하며 사용자와 추가 클라우드의 인증 시 DHP(Diffie-Hellman Problem)[3]를 응용한 안전한 대칭키 합의를 함께 진행한다.

2. 관련 연구

2.1 멀티 클라우드

멀티 클라우드란 하나의 클라우드 서비스를 사용하는 사용자가 필요에 따라 다른 클라우드 서비스를 함께 사용 하는 것을 말한다. 사용자는 하나의 클라우드 서비스에만 가입하였더라도 서비스 제공자 간 협약을 통해 다른 클라우드 서비스를 이용할 수 있게 한다. 이때 클라우드 서비스 브로커라는 TTP(Third Trust Party)를 두고 브로커가 클라우드 간의 자원 혹은 서비스의 공유를 중개한다. 하지만 멀티 클라우드 환경은 서비스가 다양해진 반면 클라우드 간의 연계에 따른 다양한 클라우드의 문제점을 상속하는 등 보안 위협이 크게 증가하였다. 또한, 각 클라우드 간 인증 및 인증정보 공유 시 개인정보 노출의 위협이 존재한다[4].

2.2 SSO(Single Sign-On)

SSO는 사용자측면에서 한 번의 인증 과정으로 생성된 인증정보를 통해 다수의 서비스를 제공받는 통합 인증관리 방식이다. 즉, 사용자는 하나의 인증정보로 접근 권한이 있는 여러 서비스에 자동으로 인증 처리됨으로써 접근할 수 있다[5]. 이 기술을 통해 사용자는 인증 정보를 관리에 대한 부담을 줄일 수 있으며, 재인증 과정 없이 다른 서비스를 이용할 수 있는 편의성을 제공 받을 수 있다. 또한, 서비스 제공자 측면에서는 사용자 인증정보 관리를 위한 비용이 감소하며, 인증과 인증 정보의 집중화를 통한 중앙 관리가 가능하다[6]. 현재 SSO를 지원하기 위한 많은 프로토콜이 있으며 대표적인 방법은 OAuth(Open Authorization), SAML(Security Assertion Markup Language) 등이 있다[7].

2.3 클라우드 서비스 브로커

클라우드 서비스 브로커는 사용자와 클라우드 서비스 제공자 사이에서 클라우드 컴퓨팅 서비스의 부가가치를 창출하기 위해 사용자를 대리하여 일하는 중개자를 의미한다. 즉, 브로커는 사용자와 클라우드 서비스 제공자 사이에서 관계 조율 및 소비자의 요구에 맞는 최적의 클라우드 컴퓨팅 서비스를 제안하고 다양한 클라우드 컴퓨팅 서비스의 전달, 활용, 관리 등의 역할을 수행한다.

Cloud Brokerage 서비스는 클라우드 서비스 제공자 혹은 특정 기업이 서비스를 구성하고 운영할 수 있다. 따라서 브로커 서비스를 구성 및 운영하는 브로커 서비스 제공자에 의해 브로커의 기능 구성이 이루어진다. 브로커 서비스는 서비스 제공 에 따라 서비스 결합 브로커(Service Aggregation Broker), 서비스 차익 브로커(Service Arbitrage Broker), 서비스 중개 브로커(Service Intermediation Broker)로 분류된다[8-9].

2.4 생체인식

FIDO(Fast IDentity Online)는 생체인식을 활용한 인증방식의 기술표준으로 FIDO 얼라이언스(FIDO Alliance)가 제정하였다. FIDO 얼라이언스는 삼성, 레노보 같은 단말기 제조사부터 칩을 제조하는 NXP, 퀄컴 그리고 OS 플랫폼 기업 마이크로소프트, 구글, 금융 서비스기업 알리바바, 페이팔, 비자 등 다양한 기업으로 회원사를 구성되어있다. FIDO는 UAF(Universal Authentication Framework) 그리고 U2F(Universal 2nd Factor) 방식으로 구성된다. UAF는 지문, 성문, 안면, 홍채 등 사용자 고유의 생체정보를 인식해 인증하는 기술이고 U2F는 ID, 비밀번호로 1차 인증한 후 1회성 보안키를 저장하고 있는 동글(Dongle)을 기기에 꽂아 2차 인증하는 방식이다[10-11].

UAF는 기기를 이용해 생체인식을 진행하면 FIDO 서버에 접속하고, 그다음 기기에 저장된 보안 키를 입력하는 순으로 진행된다. FIDO의 기본적인 의미는 사용자 확인(Verification)과 인증(Authentication) 프로토콜 그리고 인증 서버를 분리시키고 다양한 방법으로 사용자 인증을 지원하도록 하는 것이며 크게 등록 절차, 인증 절차, 탈퇴 절차로 구성된다.

2.4.1 FIDO UAF의 등록 프로토콜

(1) 사용자가 응용 앱에서 인증 수단을 패스워드에서 지문 인증으로 변경 요청한다.

(2) 응용 앱은 사용자로부터 패스워드를 입력받아 응용 서버에 전달하면 응용 서버는 패스워드를 확인하고 FIDO 등록 요청 메시지를 FIDO 서버에게 요청한다.

(3) FIDO 서버는 인증정책이 포함된 FIDO 등록 요청 메시지를 생성하여 FIDO 클라이언트에 전달한다. 참고로, 인증정책은 특정 제조사, 특정 모델, 특정 인증수단 등으로 사용할 인증 장치를 제한할 수 있다.

(4) FIDO 클라이언트는 서버 인증정책에 부합하는 지문 인증 장치를 호출하고, 사용자가 지문을 입력하여 사용자 인증에 성공하면, 지문 인증 장치는 공개키 쌍을 생성한다.

(5) 지문 인증 장치는 생성된 공개키와 공개키의 입증 정보가 포함된 FIDO 등록 응답 메시지를 FIDO 서버에 전달한다.

(6) FIDO 서버는 공개키의 입증 정보를 인증 장치 메타데이터를 이용해 확인한 후, 해당 공개키를 FIDO 서버에 저장한다.

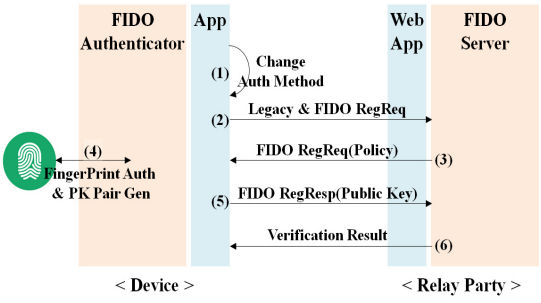

Fig. 1. FIDO UAF Registration Protocol

2.4.2 FIDO UAF의 인증 프로토콜

(1) 응용 앱은 응용 승인에 사용자 인증을 요청한다. 예를 들어, 간편결제 서비스를 이용하기 위해 지문 인증을 요청한다.

(2) 응용 앱은 응용 서버에 FIDO 인증을 요청하면 응용 서버는 FIDO 서버에 FIDO 인증 요청 메시지를 요청한다.

(3) FIDO 서버는 FIDO 인증 요청 메시지를 생성하여 FIDO 클라이언트에 전달한다.

(4) FIDO 클라이언트는 FIDO 인증 요청 메시지에 포함된 정보로 지문 인증 장치를 호출하고, 사용자가 지문을 입력하여 사용자 인증에 성공하면, 지문 인증 장치는 등록 프로토콜을 통해 생성된 개인키를 이용해 전자서명을 생성한다. 전자서명을 생성하기 이전에 거래 정보를 출력하여 사용자로부터 거래 확인을 받는 절차가 추가될 수 있다.

(5) 지문 인증 장치는 전자서명이 포함된 FIDO 인증 응답 메시지를 FIDO 서버에 전달한다.

(6) FIDO 서버는 등록 프로토콜을 통해 등록된 공개키를 이용하여 전자서명을 확인하고 인증 결과를 전달한다[12].

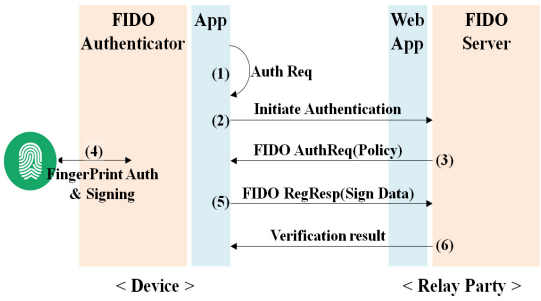

Fig. 2. FIDO UAF Authentication Protocol

3. 제안 프로토콜

3.1 개요

모바일을 통해 이용하는 클라우드 환경에서 안전한 사용자 인증을 위해 생체인식의 인증을 수행하며 생체인증은 FIDO의 UAF를 준용하였다. 특히 하나의 클라우드만을 이용하는 것이 아닌 다수의 클라우드를 함께 이용하는 멀티 클라우드 환경에서 사용할 수 있도록 구성되었으며 통신에 참여하는 개체를 최소한으로 제한하여 인증 과정을 효율을 높일 수 있도록 하였다.

가정사항으로 클라우드 서비스 제공자A(CSP_A)와 클라우드 서비스 브로커(CSB) 그리고 클라우드 서비스 브로커와 클라우드 서비스 제공자B(CSP_B)는 각각 신뢰관계로 대칭 암호화 방식을 이용하기 위한 비밀키(대칭키)를 사전에 공유하고 있어 안전한 통신이 가능하다. CSP_A는 사전 가입과정을 통해 사용자(User)의 공개키와 상호 간의 대칭 암호화를 위한 비밀키를 확보하고 있으며, CSB는 사전 협약과정을 통해 CSP_B의 공개키를 보유하고 있다. 모든 통신 간에는 기본적으로 TimeStamp를 포함하도록 한다.

3.2 인증 과정

이 단계는 사용자(User)가 모바일기기를 이용해 자신이 가입한 클라우드 서비스 제공자(CSP_A)에게 정당한 사용자임을 증명하기 위한 과정이다. 사용자는 자신의 생체인식정보를 이용하고 Relay Party(RP)를 통해 CSP_A에게 사용자 인증을 진행한다.

3.2.1 생체인증 과정

(1) User는 Mobile을 통해 사용자 인증을 위해 RP에게 인증을 진행 준비를 위한 인증초기 메시지(Initiate)를 전송한다.

(2) RP는 User에게 인증을 위한 Challenge를 포함하는 FIDO 인증 요청 메시지(Auth Request)를 전송한다.

(3) User는 RP의 요청에 따라 실제 User의 생체인식(지문, 홍채, 성문, 안면 등)을 통해 생체인증을 한다.

(4) User는 생체인증 이후 자신의 개인키를 이용해 Response를 생성하고, 이를 포함하는 메시지(Auth Response)를 RP에게 전송한다.

(5) RP는 User의 공개키(Pub_U)를 이용해 User의 Response를 검증하고, 이상이 없다면 인증 결과 메시지(Auth Result)를 전송한다.

(6) User는 Auth Result를 확인하고 CSP_A에게 인증정보(Auth Info)와 클라우드 서비스 제공자B의 서비스를 요청하는 메시지(SRV Req)를 User와 CSP_A 간의 대칭키 SK_U-PA로 암호화하고 RP에게 보낸다.

(7) CSP_A는 전송 받은 Auth Info의 진위를 확인하기 위해 RP에 해당 메시지를 전달한다.

(8) RP는 전달 받은 Auth Info를 확인하고, 이상이 없다면 해당 사용자가 정당하다는 결과를 Auth Result에 포함하여 CSP_A에게 전송한다.

3.2.2 추가 클라우드 중개 및 키 합의

(9) CSP_A는 RP를 통해 User가 정당한 사용자임을 확인하였고, 이어서 User가 CSP_B의 서비스를 이용하기 위한 SRV Req와, 유저의 공개키 Pub_U를 CSP_A와 CSB 간의 대칭키 SK_PA-B로 암호화하여 전송한다.

(10) CSB는 전달 받은 메시지에 중 SRV Req를 CSB와 CSP_B간의 대칭키SK_B-PB로 암호화하고 CSP_B에게 전송한다.

(11) CSP_B는 전송받은 서비스 요청을 확인하고 서비스 가능에 대한 동의 메시지(Agree)를 CSB에게 전송한다.

(12) CSB는 User가 CSP_B의 서비스를 이용할 때 사용할 대칭키의 재료값으로 소수 p, 정수 g를 선택한다. 단, p는 매우 큰 소수이고, g는 군 $<Z^*_p, x>$의 원소로 위수가 p-1인 생성자다. 그리고 User가 CSP_B의 서비스를 이용할 때 사용할 티

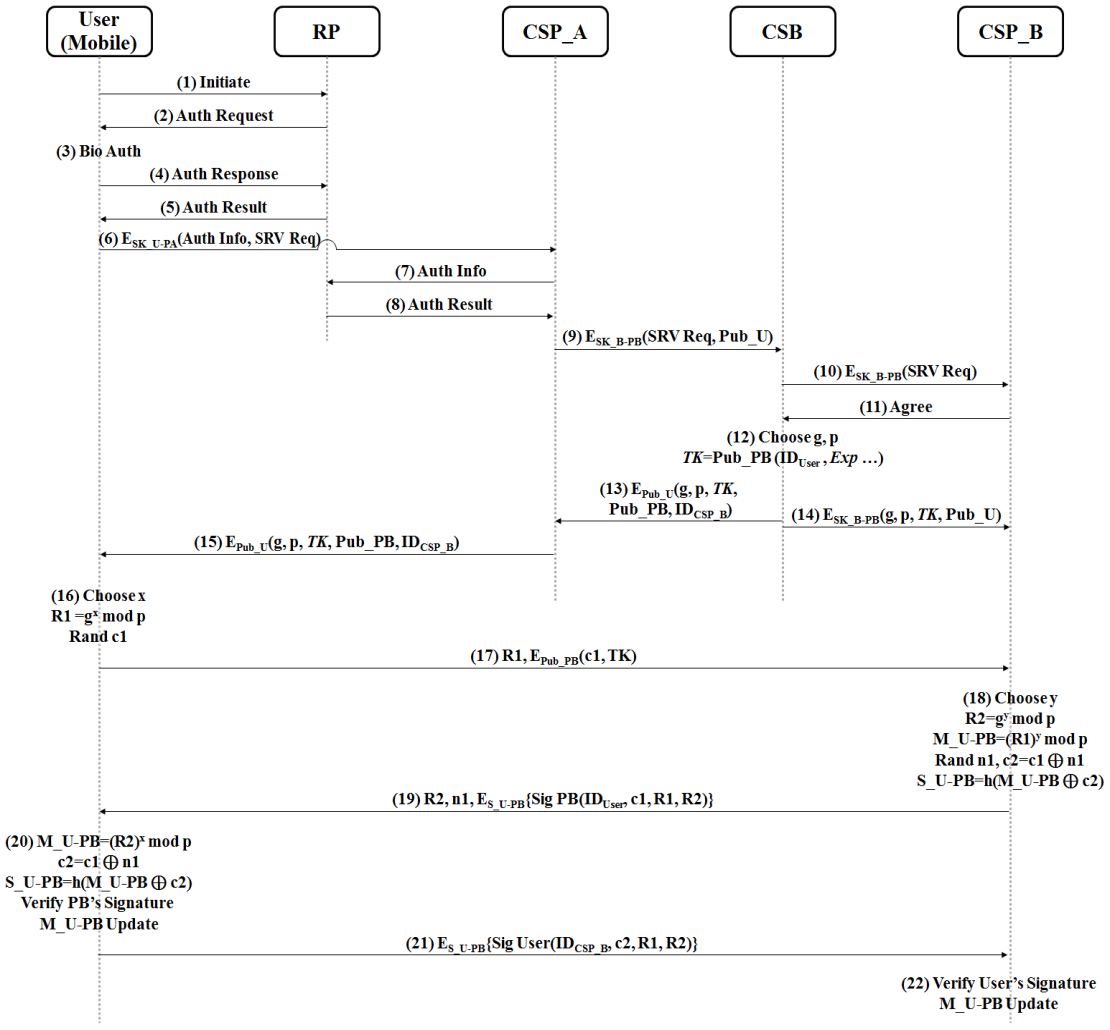

Fig. 3. User Authentication Protocol using Biometric in Mobile-cloud Environments

켓 TK를 생성한다. TK는 User의 식별자(ID_{user}), 사용기한(Exp), 사용할 서비스 등의 정보를 포함한다.

(13) CSB는 p, g와 TK, CSP_B의 공개키(Pub_PB), CSP_B의 식별자(ID_{CSP_B})를 Pub_U로 암호화하고 이를 CSP_A에게 전송한다.

(14) CSB는 p, g와 TK, Pub_U, User의 식별자(ID_{User})를 Pub_PB로 암호화하고 이를 CSP_B에게 전송한다. CSP_B는 해당 메시지의 복호화를 통해 값과 필요정보를 획득한다.

(15) CSP_A는 CSB에게서 전달 받은 메시지를 User에게 전달하고 User는 해당 메시지를 복호화하고 값과 필요정보를 획득한다.

(16) User는 대칭키 생성을 위한 부분키 생성을 위해 x를 선택한다. g^x mod p를 연산을 통해 R1을 생성하고 난수 c1을 생성한다. 단, x는 $0 \leq x \leq p-1$의 조건을 만족하는 수이다.

(17) User는 부분키 R1 그리고 CSP_B의 공개키 Pub_PB로 암호화한 c1, TK를 CSP_B에게 전송한다.

(18) CSP_B는 또 하나의 부분키 생성을 위해 y를 선택하고 g^y mod p를 연산을 통해 R2을 생성한다.

이때 y는 0 ≤ y ≤ p-1의 조건을 만족하는 수이다. 이어서 전송받은 값으로 $(R1)^y$ mod p를 연산해 User와 CSP_B 간의 마스터 대칭키 M_U-PB를 연산한다. 난수 n1을 생성하고 c1과 XOR 연산해 c2를 생성한다. c2와 M_U-PB를 XOR 연산하고 해시(Hash)하여 세션키 S_U-PB를 생성한다.

(19) CSP_B는 R2, n1 그리고 CSP_B의 개인키로 서명한 ID_{User}, c1, R1, R2을 S_U-PB로 암호화하여 전송한다.

(20) User는 전송받은 값을 확인하고 $(R2)^x$ mod p를 계산하여 M_U-PB를 생성한다. 이어서 c1에 n1을 XOR 연산하여 c2를 구한 뒤 M_U-PB에 XOR를 하고 해시하여 S_U-PB를 생성한다. S_U-PB로 암호문을 복호화하고 CSP_B의 공개키로 서명값을 검증한다. 이후 S_U-PB를 M_U-PB 값에 할당하여 마스터 대칭키를 갱신한다.

(21) User는 IDCSP_B, c2, R1, R2를 자신의 개인키로 서명하고 S_U-PB로 암호화하여 CSP_B에게 전송한다.

(22) CSP_B는 전송받은 암호문을 복호화하고 User의 공개키로 서명값을 검증한다. 이상이 없을 경우 마스터 대칭키에 S_U-PB를 할당하여 마스터 대칭키를 갱신한다.

4. 안전성 분석

제안하는 방법의 안전성을 확인하기 위하여 키의 안전성, Mutual Authentication, Man-in the-Middle Attack, Replay Attack, Message Forgery Attack, Snipping 등 다양한 공격 방법에 대해 안전성을 확인 하였으며, 분석된 결과는 다음 표와 같다.

Table 1. Safety Comparison

	SSO	Broker	Proposal
Key Safety	Safety	Safety	Safety
Mutual Authentication	Safety	-	Safety
Man-in the-Middle Attack	-	-	Safety
Replay Attack	-	-	Safety
Message Forgery Attack	Safety	Safety	Safety
Sniffing	Safety	Safety	Safety

4.1 키의 안전성

대칭키 합의, 대칭키 갱신에서 대칭키 암호화 방식인 AES를 사용하며 키의 크기는 256bit이다. AES의 알고리즘은 현재까지 알려진 취약점이 존재하지 않으며, 키 공간이 2^{256}으로 공격자가 키를 찾기 위해서는 2^{256}만큼의 연산이 필요하다. 또한, 매 인증마다 대칭키의 갱신이 이루어지므로 공격자가 키를 찾는 것은 매우 어렵다. 만약 대칭키 합의 과정에서 공개된 값 R1, R2를 탈취하더라도 비대칭 암호화 방식을 함께 사용하고 있으므로 중간자 공격을 방지할 수 있다. 또한, 탈취한 R1, R2의 g^x. g^y으로부터 g^{xy}를 구하는 DHP(Diffie-Hellman Problem)을 해결해야 하지만 현재까지 이 이산 로그 문제를 효율적으로 풀 수 있는 알고리즘이 알려지지 않았다.

4.2 Mutual Authentication

제안하는 프로토콜에서 사전단계의 User-CSP_A, CSP_A-CSB, CSB-CSP_B 각각의 통신구간은 이미 상호인증과 암호학적 안정성이 갖추어진 상태이다. 그 외에 대칭키 합의 과정에서 상호통신 간에 비대칭, 대칭 암호화를 통해 암호화된 메시지를 사용하고 있다. 이때, c1과 c2는 세션키의 재료임과 동시에 시도-응답 인증을 위한 nonce로도 함께 사용되므로 User와 CSP_B는 상호간의 인증이 가능하다. 또한, 세션키 생성 과정에서도 c2 값이 세션키의 재료값으로 사용됨과 동시에 시도-응답 인증을 위한 nonce로도 함께 사용된다.

4.3 Man-in the-Middle Attack

공격자는 User와 CSP_B의 대칭키 합의 과정에서 User와 CSP_B 사이에서 양측과 키 합의를 하여 두 개의 키를 만들어 양측의 메시지를 엿보거나 위조하려고 할 수 있다. 하지만 제안된 프로토콜의 대칭키 합의 과정에서 시도-응답 인증의 요소로 c1 값을 CSP_B의 공개키로 암호화하여 전송하므로 공격자가 중간에서 메시지를 갈취하더라도 c1값을 복호화할 수 없으므로 세션키 생성이 불가능하다. 또한, 사용자에게 R2가 전송될 때에도 CSP_B의 개인키로 생성한 서명값을 생성할 수 없다.

4.4 Replay Attack

Replay Attack은 이전 패킷들을 엿본(eavesdrop) 악의적인 공격자에 의해 시도될 수 있다. 하지만 모든 통신구간의 메시지는 기본적으로 TimeStamp를 요소로 포함

하고 있다. 그 외에 대칭키 합의 과정에서는 매번 값이 달라지는 난수 c1, n1 등을 사용하고 있으므로 공격자가 메시지를 갈취하더라도 더는 사용이 불가능한 무의미한 메시지이다.

4.5 Message Forgery Attack

모든 통신구간에서 보호되어야 할 메시지는 암호학적 안정성을 확보하고 있다. 사전단계에서는 대칭키 혹은 공개키를 이용하여 메시지를 암호화하여 보호하고 있다. 또한, 대칭키 합의, 세션키 생성 각각의 단계에서도 대칭키, 공개키를 이용한 메시지의 암호화가 이루어져 있으므로 공격자가 중간에서 메시지를 갈취하였더라도 암호화된 메시지를 복호화하거나 재암호화 할 수 없으므로 메시지의 위조가 불가능하다.

4.6 Sniffing

모든 통신구간에서 보호되어야 할 메시지는 암호학적 안정성을 확보하고 있다. 각각의 단계에서도 대칭키, 공개키를 이용한 메시지의 암호화가 이루어져 있으므로 공격자가 중간에서 메시지를 엿보더라도 암호화된 메시지를 복호화 할 수 없으므로 그 내용을 확인할 수 없다.

5. 결론

언제 어디서나 접속하고 이용할 수 있는 클라우드 컴퓨팅 서비스는 다양한 환경에서 서비스되고 있다. 특히 모바일을 통해 이용하는 클라우드 서비스가 주목받고 있으며, 두 개 이상의 클라우드 서비스를 함께 이용하는 멀티 클라우드 기술에 관한 많은 연구가 진행되고 있다. 본 논문에서는 사용자가 모바일을 이용해 멀티 클라우드 컴퓨팅 서비스를 이용하고자 할 때 클라우드 간의 상호작용을 위한 생체인증을 이용한 사용자 인증 기법을 제안하였다. 제안하는 인증기법은 서비스 이용을 위한 사용자의 생체인증 한 번으로 다수의 클라우드를 이용할 수 있게 하였다. 또한, 대칭키 합의, 대칭키 갱신 과정에서 통신에 참여하는 개체를 최소화하였으며, 사용자와 추가 서비스를 제공하는 제공자 간의 1:1로 그 작업을 수행함으로써 인증과정의 복잡함과 악의적인 공격자로부터 일어날 수 있는 다양한 문제를 사전에 방지할 수 있도록 설계하였다. 모바일을 이용하는 클라우드 서비스와 멀티 클라우드 서비스의 안전한 서비스를 기대하며 지속적인 연구가 필요할 것이다.

References

[1] Mohammed A. AlZain,Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-clouds.", *2012 45th Hawaii International Conference on System Sciences. IEEE*, pp. 5490-5499, Jan, 2012.
DOI: http://dx.doi.org/10.1109/HICSS.2012.153

[2] Jaekyung Lee, Junggab Son, Hunmin Kim, Heekuck Oh, "An Authentication Scheme for Providing to User Service Transparency in Multicloud Environment.", *Journal of The Korea Institute of Information Security & Cryptology*, vol. 23, no. 6, pp. 1131-1141, Dec, 2013.
DOI: http://dx.doi.org/10.13089/JKIISC.2013.23.6.1131

[3] Dan Boneh, "The decision diffie-hellman problem.", *International Algorithmic Number Theory Symposium. Springer Berlin Heidelberg,* vol. 1423, pp. 48-63, June, 1998.
DOI: http://dx.doi.org/10.1007/bfb0054851

[4] Yukyeong Wi, Jun Kwak, "OpenID based User Authentication Scheme for Multi-clouds Environment.", *The Journal of Digital Policy&Management*, vol. 11, no. 7, pp. 215-223, Jul, 2013.

[5] Pratap Murukutla, K. C. Shet, "Single Sign on for Cloud.", *2012 International Conference on Computing Sciences. IEEE*, pp. 176-179, Sept. 2012.
DOI: http://dx.doi.org/10.1109/ICCS.2012.66

[6] Wanpeng Li, Chris J. Mitchell, "Security issues in OAuth 2.0 SSO implementations.", *International Conference on Information Security. Springer International Publishing*, pp. 529-541, Oct. 2014.
DOI: http://dx.doi.org/10.1007/978-3-319-13257-0_34

[7] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Llanos Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps.", *Proceedings of the 6th ACM workshop on Formal methods in security engineering. ACM*, pp. 1-10, Oct. 2008.
DOI: http://dx.doi.org/10.1145/1456396.1456397

[8] Eunhye Kim, "Cloud Service Brokerage.", *Internet&Security Issue*, pp. 27-32, Korea Internet&Security Agency, 2011.

[9] Emiliano Casalicchio, Monica Palmirani, "A Cloud Service Broker with Legal-Rule Compliance Checking and Quality Assurance Capabilities.", *Procedia Computer Science*, vol. 68, pp. 136-150, Sept. 2015.
DOI: http://dx.doi.org/10.1016/j.procs.2015.09.230

[10] Jeong-Hyo Park, " A Non-Password Secure Biometric Digital Signature Method for Mobile Device", Soongsil University Graduate School, 2016.

[11] Rolf Lindemann, Davit Baghdasaryan, Eric Tiffany, "FIDO UAF Protocol Specification v1.0", FIDO Alliance Proposed Standard, 2014.

[12] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, "Universal 2nd factor (U2F) overview", FIDO Alliance Proposed Standard, 2015.

김 형 욱(Hyung-Uk Kim) [정회원]

- 2012년 2월 : 숭실대학교 정보보안학과 (공학석사)
- 2012년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 (박사수료)
- 2006년 9월 ~ 현재 : 한국전자인증 기술연구소 책임연구원

<관심분야>
PKI, 생체인증, IoT

김 범 용(Bumryong Kim) [정회원]

- 2014년 8월 : 국가평생교육진흥원 컴퓨터공학 (공학사)
- 2016년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2016년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 (박사과정)

<관심분야>
생체인증, 헬스케어. 네트워크 보안

전 문 석(Moon-Seog Jun) [종신회원]

- 1989년 2월 : University of Maryland Comuter Science (공학박사)
- 1989년 3월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 2091년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

<관심분야>
네트워크 보안, 생체인증, IoT