모바일 클라우드 환경에서 안전한 인증을 제공하기 위한 상황인식기반 인증기법*

문대호[1†], 은하수[1], 오희국[1], 김상진[2‡]
[1]한양대학교 컴퓨터공학과
[2]한국기술교육대학교 컴퓨터공학과
e-mail: dhmoon@infosec.hanyang.ac.kr

Context-Aware based Certification for Secure Access in Mobile Cloud*

Daehoo Moon[1†], Hasoo Eun[1], Heekuck Oh[1], Sangjin Kim[2‡]
[1]Dept. of Computer Science, Hanyang University
[2]Dept. of Computer Science, Korea University of Technology and Education

요 약

클라우드 컴퓨팅의 개념은 2006년에 처음 나왔다. 이것에 대한 정의는 내려졌지만 서비스 제공자들의 이해에 따라 조금씩 차이가 있다. 현재 아마존과 구글같은 글로벌 기업에서는 클라우드 서비스를 선도하고 있고, 더욱이 모바일 시장이 급성장 하고 있는 현 시대에서 모바일 클라우드는 더욱 앞서나가는 서비스 모델이 될 것으로 전망된다. 하지만 모바일기기는 분실 및 도난의 위험이 높다. 현재 사용 중인 모바일 클라우드의 인증 방법들은 기존 클라우드의 인증방법을 그대로 사용하고 있어서 타인의 모바일 기기를 악의적인 사용자가 습득할 경우 쉽게 인증을 통과 할 수 있다. 따라서 모바일 클라우드 환경에서 사용자의 인증을 더욱 안전하게 할 수 있는 방법이 필요하다. 본 논문에서는 모바일 기기를 이용하여 상황인식을 기반으로 한 인증방법을 제안한다.

1. 서론

2006년 클라우드 컴퓨팅이라는 용어가 처음 생겨난 이래, 스마트폰이 널리 보급되면서 인터넷을 통해 IT인프라를 공유하는 클라우드 컴퓨팅이 기업에서 개인고객으로 확대되었다. 이로 인해 클라우드 컴퓨팅 기반 스마트폰 서비스가 잇달아 등장하면서 모바일 클라우드 서비스가 큰 인기를 모았다. 모바일 클라우드란, 필요한 만큼 사용하고 쓴 만큼 지불하는 클라우드 컴퓨팅과 모바일 서비스를 결합한 것이다. 모바일 클라우드는 현재 클라우드라는 기술과 모바일이라는 인프라가 갖춰진 상황이기 때문에 개념정립과 동시에 서비스 출시가 이루어질 수 있다[1].

클라우드 컴퓨팅에서 가장 중요한 보안기술은 사용자 인증이다. 중앙 집중화된 클라우드 컴퓨팅과 공간을 공동으로 활용하는 멀티테넌시 환경에서 볼 때 암호기술을 적용하여 성능을 하락시키는 것 보다 인증을 강화하는 것이 효율적이기 때문이다[3]. 더욱이 모바일 단말은 분실 및 도난의 위험성이 높기 때문에 모바일 클라우드 환경에서 사용자 인증기술은 매우 중요하다.

현재 모바일 클라우드에서 주로 사용되고 있는 인증기술은 ID/Password 방식이다. 하지만 모바일 기기에서의 인증은 대부분 자동인증기능을 포함하고 있기 때문에 분실 혹은 도난당한 모바일기기는 타인에 의해 악용될 소지가 높다. 이에 대응할 수 있는 기술 중 하나는 상황정보를 인증에 이용하는 것이다. 역할기반 접근제어(RBAC: Role Based Access Control) 에서 확장된 개념인 GRBAC (Generalized Role Based Access Control) 는 접근제어 결정에 사용자 역할, 객체역할, 환경역할을 사용하는 것으로써, 기존의 역할 기반 접근제어에 상황정보를 추가하는 것이다. 따라서 상황정보를 추가하게 되면 더욱 안전하게 인증을 할 수 있다.

본 논문에서는 모바일 클라우드 환경에서 기존 ID/Password 자동인증에 추가로 GRBAC기법을 이용하여 상황정보를 정량적인 값으로 변환한 후, Threshold를 통한 (n, t)비밀분배기법으로 사용자를 인증하는 방법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 기술들의 연구동향에 대해 살펴보고 모바일 클라우드의 문제점과 어떠한 보안이슈가 있는지 알아본다. 3장에서는 제안하는 기법을 이해하기 위한 배경지식을 설명하고 안전성을 추가로 제공하는 기법을 제안한다. 4장에서는 제안하는 기법을 모바일 클라우드 환경에 적용한 결과를 분석한다. 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

* "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2012-H0301-12-1002)

2. 동향 및 관련연구

2.1 모바일 클라우드의 동향

모바일 클라우드는 필요할 때마다 사용하고 쓴 만큼 지불하는 클라우드 컴퓨팅과 모바일이 결합된 개념으로 다양한 모바일 기기를 통해 클라우드 컴퓨팅 환경을 제공하는 것이다. 모바일 클라우드는 기존 클라우드 컴퓨팅과 다르게 시간과 공간의 제약 없이 클라우드를 이용할 수 있다. 또한 애플리케이션 개발자는 단말의 사양에 관계없이 하나의 애플리케이션만을 개발하여 모든 단말에 제공할 수 있다. 즉, 애플 앱스토어나 구글 안드로이드 마켓과 같은 특정 플랫폼에 종속되지 않는다는 장점이 있다[2]. 하지만 모바일 클라우드는 아직 연구단계에 있고 현재 사용중인 인증방법은 기존 클라우드의 방법과 같은 ID/Password 방식을 사용한다. 대표적인 모바일 클라우드 서비스인 iCloud나 Dropbox는 모바일 기기에서 최초 인증 후 그 정보가 모바일 기기에 저장된다. 이후에는 자동인증 기능으로 쉽게 접속할 수 있다. 모바일 기기는 개인화된 기기로서 개인정보가 집약되어 있고, 고정된 형태로 물리적인 보호를 받는 PC와 달리 분실, 도난의 위험성이 크다. 모바일 기기를 분실 및 도난을 당할 경우 개인정보 뿐만 아니라 상황에 따라서는 클라우드에 있는 기밀정보의 유출 같은 큰 손실을 입을 수 있다[4]. 따라서 모바일 클라우드에서는 기존의 클라우드 환경보다도 더욱 안전한 사용자 인증이 필요하다.

2.2 모바일 클라우드에서의 보안이슈

모바일 클라우드는 기존 클라우드의 특징과 모바일의 특징을 모두 갖고있다. 따라서 클라우드와 모바일의 보안이슈 또한 함께 갖고 있다. 특히, 자동인증 기능으로 인해 분실이나 악성코드 감염 등으로 모바일 기기의 소유권이 타인에게 넘어갈 경우 개인적 손실 뿐만 아니라 클라우드를 이용하는 집단에게도 손실이 생길 수 있다. 따라서 모바일 클라우드에서는 인증이 매우 중요하다.

2.3 관련연구

2.3.1 상황인식(Context-Aware) 기술

상황인식기술은 변화하는 상황을 분석하여 사용자의 의도와 관련이 있는 정보인지를 판단하고, 유용한 정보이면 상황인식 응용을 위해 정보를 요청하는 기술이다. 상황인식에 대한 정의와 용어들은 1994년 Schilit가 최초로 제안했는데 네트워크 연결성, 통신비용, 통신 대역폭 등의 컴퓨팅 상황정보와 사용자 프로필, 위치 등 현재의 사회적 상황 등의 사용자 상황정보, 그리고 조명, 소음수준, 교통상황 등 물리적 상황정보 이렇게 세 가지 범주로 정의하였다.

2.3.2 RBAC

RBAC기법은 정보에 대한 연산을 수행할 수 있는 접근권한이 사용자에게 직접 할당되지 않고, 역할에 할당되며, 사용자에게 역할이 할당됨으로써 사용자가 접근권한을 획득한다. 사용자가 보호대상의 정보나 자원에 대한 접근권한을 얻기 위해서는 그 권한이 배정된 역할의 구성원이 되어야 한다. 따라서 역할과 객체간의 관계로 접근권한을 관리함으로써 사용자와 객체의 수가 많고 그 구성이 수시로 변할 수 있는 분산 컴퓨팅 환경에서 효율적인 권한부여 및 권한관리가 가능하다. RBAC는 역할 간 계층구조를 통해 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한상속 특징이 있다. 이러한 특징은 권한관리를 단순화 시켜준다. 그리고 이렇게 단순화된 권한관리는 상황정보가 RBAC을 통해 정량적인 값으로 변환될 수 있게 해준다[5].

2.3.3 GRBAC

GRBAC모델은 접근제어 결정에 사용자 역할, 객체 역할, 환경역할을 사용함으로써 기존의 RBAC에 상황정보를 추가한 기법이다. 역할을 사용자, 객체, 환경요소로 구조화하여 RBAC보다 권한관리 측면에서 유연하다. 이 기법은 상황정보를 환경역할로 정의하고, 접근제어 정책에 기술하여 사용자의 접근요청을 처리한다. 그러나 사용자의 상황정보를 환경역할로 정의하면 많은 계층구조가 발생하여 연산량이 많아지고 권한관리에 어려움이 따르는 단점이 있다[6].

2.3.4 (n, t)비밀분배법

(n, t)비밀분배법은 t명의 참여자가 비밀키를 찾으려는 문제이며 t개의 연립합동식의 해를 구하는 문제이다. 아래의 식,

$$f(x) \equiv a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \pmod{p}$$

와 같은 Z_p위에서의 다항식이 있고, 각 참여자 x_i에게 비밀키의 부분키 y_i를 주었다고 한다면, 임의의 t개의 부분집합이 있을 경우 t개의 연립합동식

$$\begin{aligned} a_0 + a_1 x_{i_1} + a_2 x_{i_1}^2 + \cdots + a_{t-1} x_{i_1}^{t-1} &\equiv y_{i_1} \pmod{p} \\ a_0 + a_1 x_{i_2} + a_2 x_{i_2}^2 + \cdots + a_{t-1} x_{i_2}^{t-1} &\equiv y_{i_2} \pmod{p} \\ &\vdots \\ a_0 + a_1 x_{i_t} + a_2 x_{i_t}^2 + \cdots + a_{t-1} x_{i_t}^{t-1} &\equiv y_{i_t} \pmod{p} \end{aligned}$$

을 얻을 수 있다. 그 후 연립합동식을 라그랑주보간법을 이용해 풀어 $f(x)$를 구해 비밀키로 사용할 상수항을 얻을 수 있다.

라그랑주 보간법을 사용하면 좌표평면 위에 주어진 n개의 점 $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$ 을 모두 지나는 다항식을 구할 수 있다. 라그랑주 보간법은 아래와 같은 식으로 나타낼 수 있다.

$$f(x) = \sum_{j=1}^{n} \left(y_j \times \prod_{\substack{i=1 \\ (i \neq j)}}^{n} \left(\frac{x - x_i}{x_j - x_i} \right) \right)$$

이 식을 전개해 보면, 아래와 같다.

$$f(x)=y_1\frac{(x-x_2)(x-x_3)(x-x_4)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)(x_1-x_4)\cdots(x_1-x_n)}+$$
$$y_2\frac{(x-x_1)(x-x_3)(x-x_4)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)(x_2-x_4)\cdots(x_2-x_n)}+\cdots$$

이 전개식을 보면, $x=x_1$을 대입했을 때 첫 번째 항에서 분모, 분자가 같아져서 1이 되고, y_1과 곱해져 결국 y_1이 된다. 나머지 항에서는 $x-x_1$으로 곱하는 부분이 있어서 모두 0이 된다. 결국 $f(x_1)=y_1$이 된다. $x_2, x_3, x_4, \cdots$ 도 모두 마찬가지로 주어진 n개의 점을 지나가는 것을 확인할 수 있다.

예를 들어보자. $(x_1,y_1)=(-2,4),(x_2,y_2)=(0,2),(x_3,y_3)=(2,8)$와 같은 세 점이 주어졌다. 이 세 점을 위의 라그랑주 보간법 식에 대입하면 아래와 같이 $f(x)$를 구할 수 있다.

$$f(x)=\frac{(x-0)(x-2)}{(-2-0)(-2-2)}4+\frac{(x-(-2))(x-2)}{(0-(-2))(0-2)}2+\frac{(x-(-2))(x-0)}{(2-(-2))(2-0)}8$$
$$=\frac{x(x-2)}{8}4+\frac{(x+2)(x-2)}{-4}2+\frac{x(x+2)}{8}8$$
$$=x^2+x+2$$

이와 같이 라그랑주 보간법을 사용하면 (n, t)비밀분배법에서 쉽게 원래의 함수를 구할 수 있다.

3. 제안하는 기법

3.1 표기법

제안하는 기법은 <표 1>과 같은 표기법을 사용한다.

<표 1> 표기법

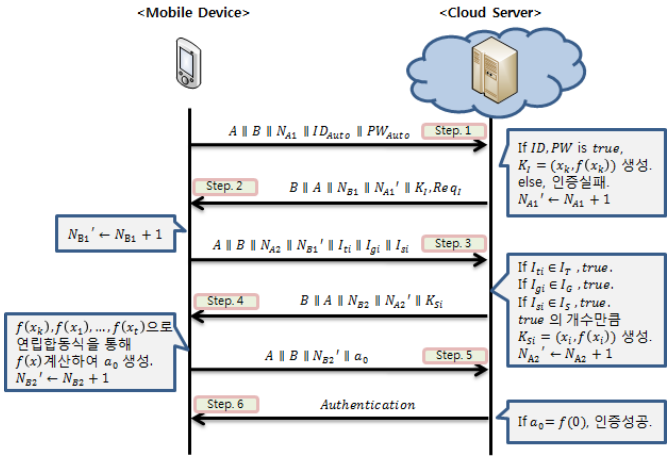
A	모바일 디바이스 식별자
B	클라우드 서버 식별자
N_{Ai}	N_{A1}, N_{A2} 모바일 디바이스의 Nance
N_{Bi}	N_{B1}, N_{B2} 클라우드 서버의 Nance
ID_{Auto}	모바일 단말에서 자동으로 입력하는 ID
PW_{Auto}	모바일 단말에서 자동으로 입력하는 Password
p	클라우드와 모바일 단말이 공유하는 임의의 소수 ($p>t$)
$f(x)$	다항식. $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1} \pmod p$ 계수 $a_1\cdots a_{n-1}$은 클라우드가 Z_p상에서 랜덤하게 선택하여 사용자의 매 인증 시 마다 새로운 $f(x)$를 생성.
a_0	다항식 $f(x)$에서의 상수항. 유한체 $GF(p)$에서의 비밀값. 최종인증값. ($a_0 \in Z_p$)
Req_{IDPW}	클라우드로부터 모바일로의 ID, Pawwsord 요청
Req_I	클라우드로부터 모바일로의 상황정보 요청
ID	사용자가 직접 입력하는 ID
PW	사용자가 직접 입력하는 Password
K_I	Impact Key $K_I=(x_k, f(x_k))$
K_{Si}	비밀정보키 $K_{S1}=(x_1,f(x_1)), K_{S2}=(x_2,f(x_2)), \cdots, K_{St}=(x_t,f(x_t))$
I_{ti}	클라우드 접근당시 시간정보(I_{t1}: 시간, I_{t2}: 요일(날짜))
I_{gi}	클라우드 접근당시 위치정보(I_{g1}: 위치, I_{g2}: 이동방향)
I_{si}	클라우드 접근당시 사용정보(I_{s1}: 사용시간, I_{s2}: 사용빈도)
I_T	클라우드에 미리 설정해 놓은 시간대 범위
I_G	클라우드에 미리 설정해 놓은 위치 범위
I_S	클라우드에 미리 설정해 놓은 Device 사용시간 및 패턴 범위

3.2 상황정보를 이용한 인증기법

3.2.1 상황정보를 이용하여 사용자를 더욱 정확하게 판단하는 자동인증 기법

본 논문에서 제안하는 기법은 모바일 기기에서 얻을 수 있는 상황정보를 GRBAC를 이용하여 구분 및 정량적인 값으로 변환한다. 이 때, 모바일의 특성을 크게 나타낼 수 있는 위치정보에 가중치를 두어 클라우드 인증 후 차등적인 권한을 줄 수 있다. 기존의 ID/Password와 같은 인증기법은 단순히 사용자를 인증하는데 그치지만 여러 역할들의 값과 GRBAC를 이용하면 역할별 값에 가중치를 부여하여 차등적인 권한을 줄 수 있는 장점이 있다. 예를 들어, 클라우드에 전송된 정보들 중 위치정보가 올바르지 않다면 클라우드 읽기권한만 부여할 수 있다. 또한, 클라우드에 저장되어 있는 데이터를 활용함으로써 클라우드에 접근하는 사용자가 해당 클라우드를 이용하던 사용자라는 것을 인식하고 이것을 인증에 중요한 정보(Impact Key)로 사용할 수 있도록 하였다. 클라우드는 이렇게 모인 정보들을 비교하여 (n,t)비밀분배법을 활용한다. 이 기법을 사용하면 인증을 위해 다수의 정보가 필요하기 때문에 더욱 안전하고, 참된 정보의 개수에 따라 차등적인 권한을 줄 수 있는 장점이 있다. 예를 들어, 2개의 비밀키로는 인증권한을 얻을 수 없고, 3개의 비밀키로 연립합동식을 생성해 알아낸 비밀값으로는 클라우드의 읽기 권한만 부여하며, 5개의 비밀키로 알아낸 비밀값으로는 읽기/쓰기 권한을 부여할 수 있다.

모바일 단말에서의 클라우드 인증과정은 아래 (그림 2)와 같이 진행된다. 클라우드는 높은 컴퓨팅 능력으로 매 인증 시 $f(x)$를 생성한다. 또한 모바일 단말과 클라우드는 인터넷을 통해 데이터를 전송하며, 전송채널은 현재 널리 쓰이고 있는 TLS를 통해 안전하게 보호된다고 가정한다.



(그림 1) 상황정보를 이용한 인증이 성공한 경우

(그림 2)의 자동인증 과정은 아래와 같다.

Step. 1 모바일 단말은 클라우드에 ID/Password를 이용하여 자동인증을 시도한다.

Step. 2 클라우드는 ID/Password를 확인하여 일치하는 경우 Impact Key를 생성하고 그렇지 않은 경우 인증을 중단한다. Impact Key를 생성하면 모바일 단말에 전송하고 상황정보를 요구한다.

Step. 3 모바일 단말은 수집 가능한 상황정보를 전송한다. 이 때, 모바일이 수집할 수 있는 상황정보는 다음과 같다.

- 통신서버 데이터: 시간정보(시간, 요일(날짜))
- GPS 데이터: 위치정보(위치, 이동방향)
- 모바일기기 자체 데이터: 패턴정보(사용시간, 빈도)

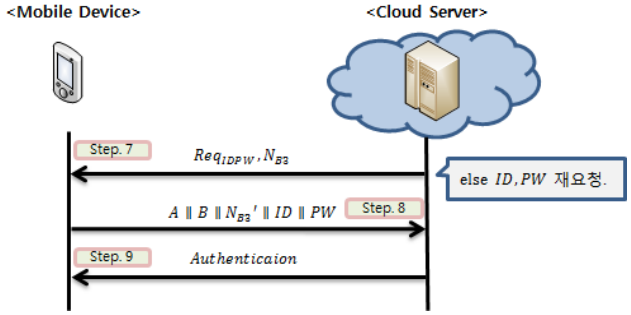
Step. 4 클라우드는 수신한 상황정보를 기존에 저장한 값과 비교하여 참 값에 대응되는 비밀정보키들 $y_i = f(x_i)$을 생성하여 모바일 단말에 전송한다.

Step. 5 모바일 단말은 수신한 비밀정보키들을 이용하여 연립합동식$f(x)$을 계산, 비밀값a_0를 알아낸다.

Step. 6 알아낸 비밀값을 클라우드에 전송하여 인증을 받는다.

3.2.2 자동인증 실패 시 인증 재시도

만약 올바른 사용자임에도 불구하고 상황정보에 변화(여행, 출장 등)가 있어서 자동인증이 실패하게 되면 (그림 3)의 과정과 같이 추가적인 인증을 요구한다. 이 과정은 위에서 수행한 Step. 6 이후에 추가로 이어진다.



(그림 2) 자동인증 실패 후 추가 프로토콜

Step. 7 클라우드는 사용자에게 ID/Password를 재요청한다.

Step. 8 사용자는 ID/Password를 직접 입력, 전송하여 인증을 받는다.

4. 제안 기법의 분석

ITU-T(International Telecommunications Union - Telecommunication Standardization Sector)가 2006년에 발표한 가이드라인에서는 안전한 패스워드 인증 프로토콜의 요구사항을 나타내고 있으며, 제안된 기법은 해당 요구사항들을 다음과 같이 만족한다.

- 전방향 안전성 제공: 사용자가 인증을 시도할 때마다 $f(x)$를 새로 생성하기 때문에 이전에 사용한 비밀값으로 인증을 시도할 수 없다. 따라서 전방향 안전성을 제공한다.
- 상호인증을 제공: 제안한 프로토콜은 직접적으로 상호인증을 제공하지 않는다. 하지만 TLS를 이용해 안전한 채널을 생성하는 과정에서 인증서 및 서명을 사용해 상대방을 인증한다. 따라서 간접적으로 상호인증을 제공한다.
- 재사용 공격에 안전: TLS에 의해 보호되는 채널이므로 공격자는 메시지의 내용을 수정할 수 없다. 만약 공격자가 Step. 1의 메시지를 가로챘다 하더라도 그것을 다시 Step. 8의 인증에서 재사용을 할 수 없다. 메시지 안의 난스가 다르기 때문이다. 이와 같이 각 메시지 안에 포함된 난스가 모두 다르기 때문에 재사용 공격에 안전하다.
- 누설된 세션키로부터 패스워드 복구불가: 안전하게 보호되는 TLS 전송채널을 사용함으로써 안전하다.

5. 결론 및 향후연구

클라우드 컴퓨팅이 활성화 되고, 스마트폰이 빠르게 보급되면서 모바일 클라우드가 빠르게 확산되고 있다. 하지만 현재 서비스중인 모바일 클라우드는 모바일 기기의 특성을 생각하지 않고 기존 클라우드의 인증시스템을 그대로 사용하고 있다. 따라서 분실하기 쉽고 악용되기 쉬운 모바일 기기의 특성상 모바일 클라우드의 인증시스템을 개선하지 않으면 큰 피해가 발생할 수 있다. 본 논문에서는 상황정보를 이용한 인증을 통해 더욱 안전하게 인증을 제공하는 기법을 제안하였다. 앞으로 모바일 기기에 생체정보 인식모듈 등 더 많은 상황정보를 인식할 수 있는 수단이 증가하면 더욱 안전한 인증을 할 수 있을 것이다. 향후에는 이러한 생체정보와 같은 정보를 정량적인 값으로 변환하는 과정의 복잡함과, 늘어나는 상황정보에 따른 추가적인 연산량 등을 분석할 것이다. 또한 클라우드가 $f(x)$를 생성하는데 드는 비용 또한 신빙성 있게 분석하는 것이 필요하다.

참고문헌

[1] 한국전자통신연구원, “모바일 클라우드 기술 동향,” 모바일 소프트웨어 기술동향 특집, 제25권 제3호, 2010

[2] KT경제경영연구소 보고서, “모바일 클라우드, 모바일의 미래가 될 것인가,” 2010

[3] 디지털데일리, “클라우드 컴퓨팅 핵심 보안과제는 ‘사용자인증’,” 숭실대학교 이정현교수 인터뷰, 2010.

[4] KT경제경영연구소 보고서, “모바일 클라우드 환경에서의 보안 이슈,” 2010.

[5] R. S. Sandhu and E. J. Coyne, "Role-Based Access Control Models", IEEE Computer, Vol.20 No.2, pp. 38-47, 1996

[6] G. Neumann and M. Strembeck, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment" 8th, ACM Symposium on Access Control Models and Technologies(SACMAT2003), pp. 65-79, 2003.