http://dx.doi.org/10.7236/JIWIT.2012.12.3.195
JIWIT 2012-3-25

이중 패스워드 방식을 이용한 스마트폰 뱅킹 관리

A new password authentication scheme using two-way password in Smartphone Banking

송종근*, 김태용**, 이훈재**, 장원태***

Jong-Gun Song, Tae-Yong Kim, Hoon-Jae Lee, Won-Tae Jang

요 약 스마트폰은 사용자들에게 편리함을 제공하지만 분실과 악성코로 인한 보안적인 측면에서 문제점을 이슈가 되고 있다. 본 논문에서는 이중 보안 시스템 환경을 이용하여 기존에 사용되어지고 있는 스마트폰 뱅킹 환경에서의 문제점을 해결하고자 한다. 분실 또는 악성코드를 통해 개인정보 유출, 금전적인 피해를 줄이기 위해서는 스마트폰 뱅킹 서비스 환경에서 개인정보의 통제 및 보호가 보장되는 개인인증 방법을 제공할 필요가 있다. 이를 위해서 기존 ID/Password 방식과 더불어 공인인증서와 함께 스마트폰의 자이로센서를 이용한 이중 패스워드 인증 방식을 제안한다.

Abstract Smart Phone devices offer convenience for users, but present a new set of security issues due to loss or malicious code. In this paper, a mobile cloud system environment is used with existing smart phones in an attempt to solve the problems in a banking environment. In order to prevent financial damages due to loss or personal information leakage by malicious code, a mobile cloud computing service that provides control and protection of personal information in environment that ensures individual authentication is used. Existing ID / Password with certificate, with the way smart phone dual password authentication scheme using the gyro sensors proposed.

Key Words : Smart Phone Banking, Authentication, Gyro Sensor

Ⅰ. 서 론

모바일 단말을 이용한 모든 서비스는 모바일 네트워크 환경이므로 정보보안 및 프라이버시에 대한 취약성이 존재한다. 현재 스마트폰이 제공하는 수많은 기능 중에 커다란 이슈로 주목받는 부분은 인터넷 뱅킹이나 쇼핑몰 결제 등과 같은 모바일을 이용한 금융서비스 분야이다.

이러한 취약성을 극복하기 위하여 기밀성(Confidentiality), 인증성(Authentication), 무결성(Integrity)이 요구 되며 인증 수단으로 공인인증서, OTP, 또는 생체정보를 이용하는 방안이 활발히 적용되고 있다.[1]

이러한 인증수단으로 생체정보를 인증에 활용하는 방안이 활발하게 검토 중이나 실제 사용이 불편한 단점들

*정회원, 동서대학교 유비쿼터스 IT과
**정회원, 동서대학교 정보통신학과
***정회원, 동서대학교 정보통신학과 (교신저자)
접수일자 2012년 05월 30일, 수정완료 2012년 06월 8일
게재확정일자 2012년 6월 8일

Received: 30 May, 2012, Revised: 8 June, 2012
Accepted: 8 June, 2012
*Corresponding Author :jwtway@gdsu.dongseo.ac.kr
Dept. of Computer & Information, Dongseo University, korea

을 가지고 있다. PC에 연결시켜 서명을 받는 방식이나 또는 휴대폰에 센서를 부착해 서명을 하는 3차원 인식하는 기술, 지문센서를 휴대폰에 탑재하여 인식하는 기술 등이 개발되고 있으나 센서를 부착해야 하는 번거로움이 있어 흔히 사용되는 스마트폰의 카메라를 이용하는 인식 방법이 발전되고 있다.

스마트폰 뱅킹 서비스 환경에서 개인정보의 통제 및 보호가 보장되는 개인인증 방법을 제공하기 위해 기존 로그인 방식과 더불어 공인인증서와 스마트폰에 장착된 G센서(Gyro Sensor)을 이용하여 이중 패스워드 인증방식 시스템을 제안한다.

이러한 방법은 모바일 단말기 특성상 정보 입력과 보안을 위한 추가 단말기가 필요하지 않아 비용 없이 시스템을 구축할 수 있으며, 보안에서도 안정적인 인증 서비스를 사용할 수 있다.

II. 관련연구

스마트폰 뱅킹은 언제 어디서든 사용자가 스마트폰이 인터넷만 접속이 가능하다면 거래를 하고 있는 해당 은행의 금융 서비스를 제공 받을 수 있는 것을 말한다. 스마트폰뱅킹이 폭발적인 성장세를 보이고 있는데 2012년 1분기 모바일 뱅킹서비스 일평균 이용건수는 1101만건 가운데 95%이상이 스마트폰을 통한 것으로 나타나고 있다.

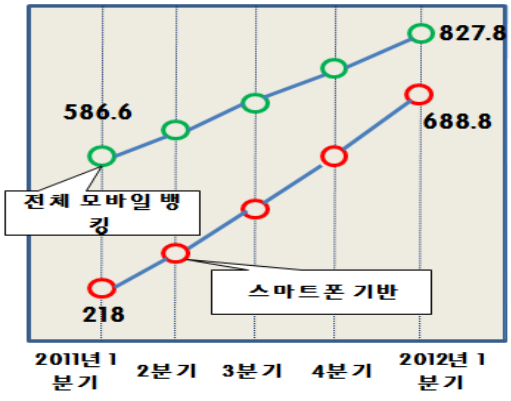

그림 1. 2012년 1분기 일평균 스마트폰 이용
Fig. 1. By the first quarter of 2012 the average day Smart Phone

하지만 스마트폰 뱅킹 애플리케이션은 각 은행마다 공인증서 저장 방식이 다른 방식을 가지며, 공인인증서가 스마트폰에 저장되거나 또한 해당 은행기기 시스템 폴더에 저장하는 방식으로 사용되어 지고 있다.

현재 국내에서는 인터넷 뱅킹을 사용하기 위해서는 액티브X 기반의 공인인증서 방식을 사용하여 전자서명을 해야 뱅킹 서비스 및 금융서비스를 사용할 수 있다.

국내에서는 스마트폰 전자결제 방식으로 공인인증서와 미국과 유럽에서 사용하는 SSL방식과 OTP방식을 적용해 사용하고 있다.[2]

이러한 이유는 사용자가 설치한 애플리케이션을 통해 악성코드가 있는 경우 사용자의 개인정보 유출과 금전적인 피해를 입을 수 있는데 최근 악성코드를 통해 개인정보 유칠과 같은 원하지 않는 서비스를 이용하여 피해를 입은 사례도 등장하면서 각 은행들은 위변조된 애플리케이션을 방지하기 위해 보안업체와 공동으로 솔루션을 개발하고 있다.

또한 패턴인식, 생체인식, 얼굴 인식 등 스마트폰을 통한 애플리케이션이 개발되고 있지만, 이러한 인식 방법들은 도난, 분실, 망각 등의 우려가 없이 안전하게 사용할 수 있는 보안 수단이며, 별도 제작된 센서가 아닌 스마트폰에 장착된 카메라를 통하여 쉽게 이용이 가능하다.

III. 문제점 분석

스마트폰 기반의 금융 거래 서비스의 문제점들이 제기되고 있는데 첫 번째로 공인인증서 관리 문제이다. 스마트폰을 사용하여 금융 거래를 하려면 공인인증서를 필수적으로 요구가 되는데 우리나라의 공인인증 결제 시스템 또는 뱅킹 서비스는 MS의 액티브X라는 프로그램 기반으로 만들어졌지만 모바일 상에서는 액티브X가 제대로 지원되지 않고 있어 금융 기관에서는 새로운 결제방식 도입을 추진하고 있다

이러한 문제점을 대처하기 위해서 각 은행에서는 애플리케이션 통한 뱅킹 서비스를 실시하였는데 하나의 은행 애플리케이션을 설치하여 공인인증서를 사용한다면 다른 은행에서는 이 공인인증서를 접근이 불가하며, 개별 애플리케이션 마다 공인인증서 모듈 및 저장 공간이 필요한 문제점이 제시되었다.

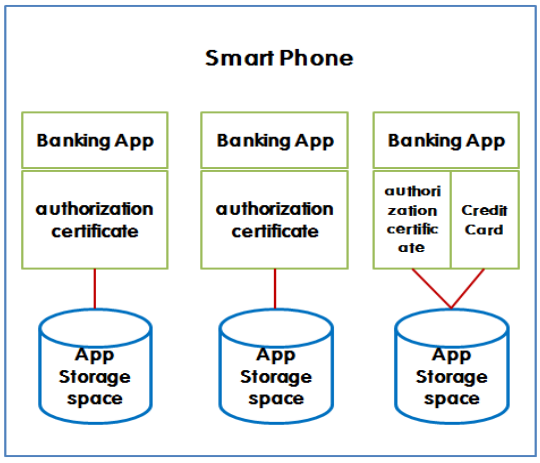

그림 2. 스마트폰 뱅킹 애플리케이션 인증서 저장방식
Fig. 2. Smart Phone Banking application system Certificate Storage

두 번째로 악성코드의 위협인데 스마트폰인 일반 휴대폰과 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 인터페이스 제공은 악성코드 전파 경로가 다각화되어 악성코드가 쉽게 퍼지는 결과를 가져왔으며, 내부 인터페이스는 악의적인 개발자가 모바일 애플리케이션에 악성코드를 쉽게 은닉하여 제작할 수 있도록 만들어졌다.[3]

또한 스마트폰 보안에 영향을 주는 구조변경(탈옥, 루팅 등)을 하지 않는 게 좋으며, 무선 랜을 사용하지 말고 이동통신망을 사용하는 게 안전하다.

세 번째로 OTP방식은 사용자 인증을 위해 기존에 구축되어 있는 인증 서버와의 연동이 어려우며, 사용중인 그룹웨어 등 애플리케이션과의 호환성이 떨어진다는 단점을 가지고 있으며, 시스템 관리에 있어서도 시간 동기화방식인 OTP는 인증서버와 OTP 토큰 사이에 시간 정보를 일치시키기 위한 관리자의 노력이 필요하며 사용자가 많은 환경에서는 부담이 될 수 있다.[4]

얼굴인식 또는 패턴인식 같은 경우는 이 또한 문제점을 가지고 있는데 조명이나 카메라와의 거리등에 따른 인식률이 변하며, 얼굴의 각도, 표정에 따른 모양에 대한 문제점과 함께 살이 찌거나 빠졌을 경우 얼굴의 형태가 달라지는 문제점 등으로 인식률에 낮아질 수 있다.

Ⅳ. 제안사항

제안하는 방식은 기존 로그인 방식, 공인인증서와 함께 스마트폰에 장착되어진 Gyro Sensor(3축)를 이용하여 이중 패스워드 인증방식을 제안한다.

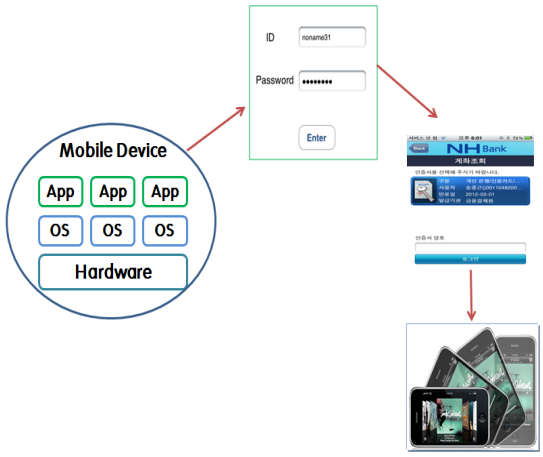

그림 3. 전체 시스템 구성도
Fig. 3. System configuration application

Gyro Sensor는 X, Y, Z벡터 값을 이용하여 움직임을 감지하는 3축 센서로써 스마트폰 단말기 방향에 따라 화면을 전환하는 기능으로 사용되어 지고 있다. 제안한 방식에서는 화면을 전환하지 않고 X, Y, Z축의 통해 0~9까지의 값을 나타내도록 한다.

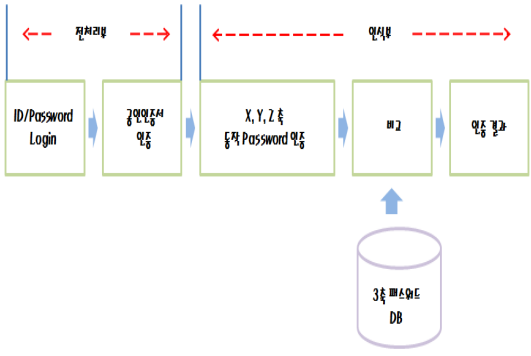

그림 4. 이중 패스워드 인증 처리방식
Fig. 4. Dual-Password authentication processing

전처리부에서는 기존 방식의 로그인방식과 공인인증서 인증을 하는 과정이며, 인식부에서는 사용자가 3축센서 값을 통한 이중 패스워드 모션 값을 4~6자리 설정 후

DB에 저장된 데이터 값과 비교 후 인증이 완료되면 금융 거래 서비스를 시작할 수 있다.

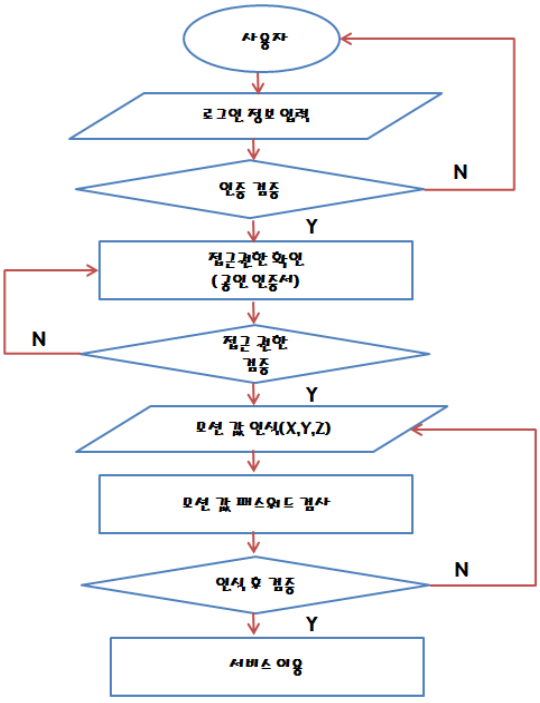

그림 5. 서비스 흐름도
Fig. 5. Service Flowchart

그림5의 서비스 흐름도는 사용자에서 공인인증서를 통한 접근 권한 검증까지는 일반적인 인증방식인 로그인과 함께 공인인증서를 통해 접근 하게 된다.

다음으로 모션 값을 통해 좌, 우의 값은 X축을 통해 -1부터 1까지 총 4자리 숫자로 나타내며, Y축도 마찬가지로 -1부터 1까지 축의 값을 통해 4자리 숫자로 나타낸다. Z축은 2자리 숫자로 나타내 총 10자리 중 지정한 4~6자리를 인식 후 검증을 마치면 서비스를 이용할 수 있다.

현재 사용되어 지고 있는 시스템 방식은 로그인방식과 더불어 공인인증서, 또는 OTP 시스템을 이용한 뱅킹 서비스이다.

다음 그림6은 공인인증서와 OTP 시스템을 이용한 방식이다. OTP시스템을 통해 모바일 뱅킹서비스를 이용하는 어플리케이션은 공인인증서 확인 후 스마트폰으로 싱크 코드 3자리가 푸시알림을 통해 전송되어진다. 싱크 코드 입력 후 6자리의 랜덤코드가 발생하여 OTP 시스템을 사용하게 된다.

그림 6. 기존 모바일 뱅킹 어플리케이션
Fig. 6. Existing Mobile Banking application

다음 그림7은 본 논문에서 제안한 방식으로 기존의 공인인증서 접속 방식까지는 같지만 gyro sensor의 X, Y, Z축을 통해 모션 패스워드를 입력하는 방식이다.

애플리케이션 설정에서 자신이 원하는 모션을 선택하여 4~6자리의 패스워드를 설정 후 사용할 수 있다. 0에서 9까지의 숫자를 모션으로 통해 설정 할 수 있는데 각 X, Y, Z축의 지정 번호가 아닌 자신의 원하는 모션과 숫자를 지정하여 사용할 수 있는 시스템 방식이다.

그림 7. 0~9까지 패스워드 모션 방식
Fig. 7. 0~9 to the password motion system

기존에 사용되던 로그인방식과 공인인증서, OTP 방식의 시스템은 휴대폰 분실과 개인정보 유출 시 쉽게 타인에 의해서 사용되어 질 수 있다. 하지만 제안한 모션을

이용한 패스워드 방식은 해킹 또는 분실에 있어 보안 적으로 안정적이며, 각 방향마다 지정 번호가 아닌 자신이 직접 방향과 그 번호를 지정함으로 있어 최대한 안전하다고 할 수 있다.

단 제안한 방식은 숫자 이외의 문자를 설정할 수 없는 단점을 가지고 있지만 언제든지 설정을 통해서 자신만의 모션 패스워드를 변경하여 보다 안전하게 사용할 수 있다.

V. 결론

2010년부터 시작된 스마트폰의 열풍은 사용자에게 편리함을 제공해 주었지만 분실 또는 악성코드로 인해 보안적인 측면에서 매우 미흡한 상태였다. 현재 스마트폰 뱅킹에 필요한 스마트폰 공인인증서에 대한 연구와 더불어 통합은행 애플리케이션 뱅킹 서비스도 이루어지고 있다.

본 논문에서는 Gyro Sensor를 이용한 이중 패스워드 방식의 스마트폰 뱅킹 서비스로 보안 위협 및 침해에 대한 대응 방안을 제안하기 위해 기존 방식의 문제점을 분석하고 이를 기반으로 분실과 위험 요소에서 좀 더 안전하기 위한 방법을 제안하였다.

제안한 방식은 스마트폰 기기의 장점을 이용하여 모션 인증 방식을 채용하고 스마트폰 분실 또는 보안의 취약성, 악성코드에서 안전하다.

향후 스마트폰 기기의 기능의 확대됨에 따라 지문인식, 또는 음성인식과 같은 생체 정보를 통해 인증하는 서비스와 제안한 모션인식방식과 더불어 패턴인식 등 다양한 인증방식으로 구현될 것이다. 안전한 인증방식을 위해 정확한 인식률 향상과 빠른 비교, 분석을 위한 연산 능력이 필요할 것이다.

참고문헌

[1] H. M. Jung, J. I. Sin, K. S. Lee, “Design of User Authentication Method in Mobile Cloud Computing,” 2010 Fall Conference of Korea Multimedia Society, Vol.13, No.2, pp. 516~519, November 2010

[2] M. Y. Hwang, W. K, D. B. Lee, J. K, “Certificate Management Plan in Smart Phone Banking using the Mobile Cloud Computing,” The Institute of Electronics Engineers Summer Conference Article, Vol.33, No.1, pp.1873~1876, June 2010

[3] E. Y. Jang, H. J. Kim, C. S. Park, J. Y. Kim, J. I. Lee, “The study on a threat countermeasure of mobile cloud services,” Korea Institute of Information Security 2011, Vol.21, No.1, pp. 177~186, Feb. 2011

[4] H. K. Kim, L. Y. Lee, “A Study on One-Time Password Authentication Scheme in Mobile Environment,” Journal of Korea Multimedia Society, Vol.14, No.6, pp.785~793, June 2011

[5] J. C. Park, “Design of A One-time Password Generator on A Mobile Phone Providing An Additional Authentication for A Particular Transaction,” Journal of KIISE , Vol.36, No.6, pp.552~557, December 2009

[6] H. N. You, J. S. Lee, J. J. Kim, J. P. Park, M. S. Jun, “A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment,” Journal of KICS , Vol.36, No.8, pp.939~946, August 2011

※ 본 연구는 지식경제부에서 지원하는 동서대학교 유비쿼터스 어플라이언스 지역혁신센터에서 지원받았음(과제번호. B0008352).

저자 소개

송 종 근(정회원)

- 2009년 동서대학교 정보네트워크학과 학사 졸업.
- 2011년 동서대학교 유비쿼터스 IT과 석사 졸업.
- 2012년 동서대학교 유비쿼터스 IT과 박사 과정 중.

<관심분야 : Smart Phone, Remote Control, Vehicle, authentication>

김 태 용(정회원)

- 1995년 Okayama Univ.(Electrical and Electronic of Eng)
- 1997년 Okayama Univ.(Electrical and Electronic of Eng), MS
- 1997년 Okayama Univ.(Electrical and Electronic of Eng), Ph.D.
- 2002년~현재 : 동서대학교 정보통신학과 부교수

<관심분야 : 무선통신, 미들웨어 응용, 수치해석>

이 훈 재(정회원)

- 1985년 경북대학교 전자공학과 (공학사)
- 1987년 경북대학교 전자공학과 정보통신전공(공학석사)
- 1998년 경북대학교 전자공학과 정보통신전공(공학박사)
- 2002년~현재 : 동서대학교 정보통신학과 정교수

<관심분야 : 정보보안, 네트워크 보안, 데이터통신 >

장 원 태(정회원) 교신저자

- 1985년 Electronics Engineering, SungKyunkwan Univ.
- 1995년 Graduate School of Engineering of Seoul Univ. MS
- 1989년~2000년 Korea Telecom International Vertech Solution Inc
- 2002년~현재 : 동서대학교 정보통신학과 부교수

<관심분야 : Remote Control, Microprocessor, Mobile >