

모션 패스워드 인증방식을 이용한 스마트폰 뱅킹

송중근[○], 장원태^{*}, 이훈재^{**}, 김태용^{**}

^{**}동서대학교 컴퓨터정보공학부, ^{*}교신저자

[○]동서대학교 유비쿼터스IT과

e-mail:jwtway@gdsu.dongseo.ac.kr^{*}, {tykimw2k, hjlee}@gdsu.dongseo.ac.kr^{**}, noname31@nate.com[○]

A Smart Phone Banking using motion password Authentication

Jong-Gun Song[○], Won-Tae Jang^{*}, Tae-Yong^{**}, Hoon-Jae Lee^{**}

^{**}Dept. of Computer & Information Dongseo University

[○]Dept. of Ubiquitous IT, Dongseo University

● 요약 ●

스마트폰은 사용자들에게 편리함을 제공하지만 분실과 악성코드로 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 방식과 더불어 스마트폰의 자이로센서를 이용한 모션 패스워드 인증방식을 제안한다.

키워드: Smart Phone Banking, Smart Phone Authentication, Gyro Sensor

I. 서론

모바일 단말을 이용한 모든 서비스는 모바일 네트워크 환경이므로 정보보안 및 프라이버시에 대한 취약성이 존재한다.

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

인증수단으로 생체정보를 인증에 활용하는 방안이 활발하게 검토 중이나 실제 사용이 불편한 단점들을 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 있다.

스마트폰 뱅킹 서비스 환경에서 개인정보의 통제 및 보호가 보장되는 개인인증 방법을 제공하기 위해 기존 로그인 방식과 더불어 공인인증서와 스마트폰에 장착된 Gyro Sensor를 이용하여 모션 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. 관련 연구

스마트폰 뱅킹은 언제 어디서든 사용자가 스마트폰이 인터넷만 접속이 가능하다. 스마트폰을 통하여 예금조회 및 이체, 신용카드, 지로납부, 부가서비스 등 은행의 전자금융서비스를 이용할 수 있는 시스템이 구축되어 있다.

스마트폰 뱅킹 애플리케이션은 각 은행마다 공인인증서 저장 방식이 다른 방식을 가지며, 공인인증서가 스마트폰에 저장되거나 또한 해당 은행기기 시스템 폴더에 저장하는 방식으로 사용되고 있다.

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

스마트폰이 확산됨에 따라 전자결제를 위한 보안 기술로 기존의 공인인증서를 이용한 전자서명 기술뿐만 아니라 SSL과 OTP를 이용하는 기술을 사용하고 있다[2].

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 banking 서비스는 MS의 액티브X 라는 프로그램 기반으로 만들어졌지만 모바일 상에서는 액티브X 가 제대로 지원되지 않고 있어 금융 기관에서는 새로운 결제방식 도입을 추진하고 있다.

두 번째로 인터넷 banking과 스마트폰 banking의 연동 문제이다. 인터넷 banking을 사용하던 중에 비밀번호를 3회 잘 못 입력해서 계좌가 정지되었는데도 불구하고 스마트폰 banking 앱으로 정지된 계좌로의 이체 서비스가 가능한 등의 문제가 발생하였다.

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

2011년 8월 스마트폰의 유심 카드에 담긴 공인인증서 등 개인 금융정보를 빼돌리는 악성코드가 국내에서 발견되었고, 스마트폰의 '단말기 식별 번호' 정보를 유출하는 악성바이러스도 출현되었다.

IV. 제안사항

제안하는 방식은 기존 로그인 방식, 공인인증서와 함께 스마트폰에 장착되어진 Gyro Sensor를 이용하여 모션 패스워드 인증방식을 제안한다.

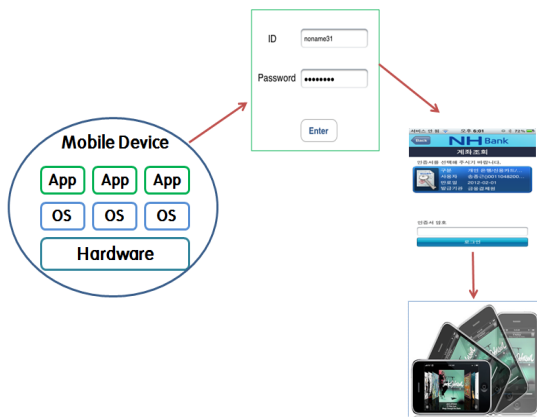


그림 1. 시스템 구조
Fig. 1. System Architecture

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 사용자가 원하는 방향과 설

정 값으로 4자리의 패스워드를 지정하도록 한다.

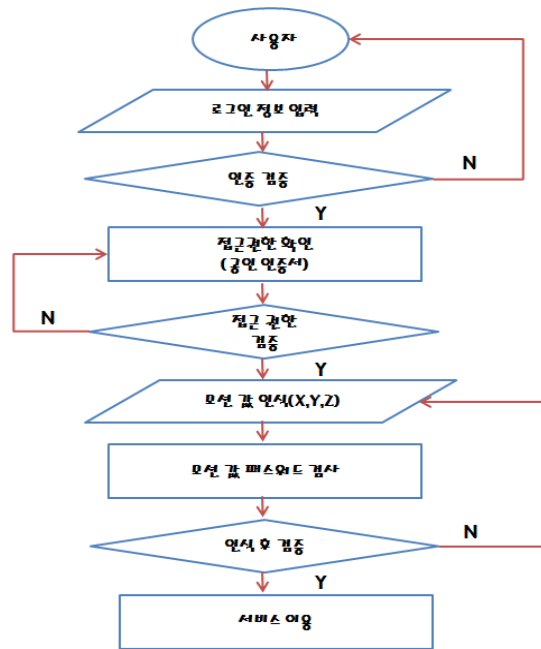


그림 2. 서비스 흐름도
Fig. 2. Service Flowchart

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.

	(x:-0.5 y:0.0 z:0.0)		(x:0.0 y:-1.0 z:0.0)
	(x:-1.0 y:0.0 z:0.0)		(x:0.0 y:1.0 z:0.0)
	(x:0.5 y:0.0 z:0.0)		(x:0.0 y:0.0 z:1.0)
	(x:1.0 y:0.0 z:0.0)		(x:0.0 y:0.0 z:1.0)

그림 3. 모션 패스워드 설정
Fig. 3. Motion password setting

다음 그림3은 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 4자리의 패스워드를 설정 후 사용할 수 있다. 0에서 9까지의 숫자를 모션으로 통해 설정 할 수 있으며, 자신이 원하는 숫자를 입력하고 모션을 설정하면 패스워드를 지정할 수 있다. 단 X, Y, Z축에서 한 축에서는 2개 이상의 숫자를 설정 할 수 없지만 각 축의 -1에서 1사이의 각도에 따라 1에서 최대 60자리 숫자까지 나타낼 수 있다.

V. 결론

2010년부터 시작된 스마트폰의 열풍은 사용자에게 편리함을 제공해 주었지만 분실 또는 악성코드로 인해 보안적인 측면에서 매우 미흡한 상태였다.

본 논문에서는 Gyro Sensor를 이용한 모션 패스워드 방식의 스마트폰 뱅킹 서비스로 보안 위협 및 침해에 대한 대응 방안을 제안하기 위해 기존 방식의 문제점을 분석하고 이를 기반으로 분실과 위협 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 음성

인식과 같은 생체 정보를 통해 인증하는 서비스와 제안한 모션인식 방식과 더불어 패턴인식 등 다양한 인증방식으로 구현될 것이다.

스마트폰을 사용함에 있어 PC와의 연결, 인증되지 않은 어플리케이션 설치 및 분실에 있어 기본 방식만 지켜진다면 뱅킹 서비스를 사용함에 있어 보다 안전한 서비스를 이용할 수 있을 것이다.

참고문헌

- [1] hmjung, and jisun, and kslee, "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] myhwang, and wk, and dblee, and jk, "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] eyjang, and hjkim, and cspark, and jykim, and, jilee, "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] hkkim, and lylee, "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.