JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 2 : 301~308 Feb. 2017

스마트폰을 이용한 사용자 인증 메커니즘

정필성[1] · 조양현[2*]

User Authentication Mechanism using Smartphone

Pil-seong Jeong[1] · Yang-hyun Cho[2*]

[1]HEART MEDIA Co., Ltd. 461-41, Seogyo-dong, Mapo-gu, Seoul, Korea

[2*]Division of Computer Science, Sahmyook University, Seoul 01795, Korea

요 약

스마트폰의 대중화와 인터넷의 발전으로 많은 사람들이 스마트폰을 이용하여 본인확인 인증절차를 진행한다. 스마트폰을 이용하면 개인용 데스크탑 컴퓨터를 이용하는 상황보다 쉽고 빠르게 인증이 가능하기 때문이다. 하지만 인터넷 해킹 기술과 악성코드 배포 기술이 빠르게 진화하고 공격형태도 더 다양해짐에 따라서 모바일 환경에 적합한 인증방법이 요구되고 있다. 인증방법으로는 소지기반 인증, 지식기반 인증, 생체기반 인증, 패턴기반 인증, 다중요소 인증 등의 방법이 있다. 본 논문에서는 스마트폰을 이용하여 수집 가능한 정보를 인증요소로 활용하는 사용자 인증 메커니즘을 제안한다. 제안 인증 메커니즘을 사용하면 본인의 스마트폰 정보 및 환경정보를 숨김 인증요소로 활용하여 타인에게 노출이 안된 상태에서 인증과정을 진행할 수 있는 장점이 있다. 제안 인증 메커니즘을 이용한 사용자 인증 시스템을 구현하여 적용성, 편의성, 보안성을 기준으로 효용성을 평가하였다.

ABSTRACT

With the popularization of smart phones and the development of the Internet, many people use smart phones to conduct identity verification procedures. smart phones are easier and faster to authenticate than personal desktop computers. However, as Internet hacking technology and malicious code distribution technology rapidly evolve and attack types become more diverse, authentication methods suitable for mobile environment are required. As authentication methods, there are methods such as possessive-based authentication, knowledge-based authentication, biometric-based authentication, pattern-based authentication, and multi-element authentication. In this paper, we propose a user authentication mechanism that uses collected information as authentication factor using smart phone. Using the proposed authentication mechanism, it is possible to use the smart phone information and environment information of the user as a hidden authentication factor, so that the authentication process can be performed without being exposed to others. We implemented the user authentication system using the proposed authentication mechanism and evaluated the effectiveness based on applicability, convenience, and security.

키워드 : 보안요소, 다중인증, 숨김요소, 스마트폰, 스마트 기기

Key word : Hidden Factor, Multi Factor, Security Factor, Smartphone, Smart Device

Received 10 November 2016, **Revised** 11 November 2016, **Accepted** 25 December 2016

* **Corresponding Author** Yang-Hyun Cho((E-mail:yhcho@syu.ac.kr, Tel:+82-2-3399-1787)
Division of Computer Science, Sahmyook Universitiy, Seoul 01795, Korea

Open Access http://doi.org/10.6109/jkiice.2017.21.2.301 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

스마트폰이 대중화되고 실시간 인터넷이 가능해짐에 따라 스마트폰을 이용한 개인 인증 기술 및 개인 정보 보호에 대한 관심이 높아지고 있다. 인증 기술은 임의의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는 것으로 시스템이 접근을 요청한 사용자가 그 본인이 맞는지 확인해 주는 모든 과정을 의미한다. 스마트폰을 이용한 본인 인증 방법으로는 아이디와 비밀번호를 이용한 인증, SMS 인증, 일회용 비밀번호(OTP, One Time Password) 인증, 디지털인증서 등의 인증 기법이 존재한다. 하지만 이러한 인증 기법을 적용한다 하더라도 다양한 방법으로 인증 정보를 해킹하려고 시도하고 있기 때문에 두 개 이상의 단일 인증을 결합한 다중 인증을 권고하고 있다. 하지만 단일 인증에 비해 다중 인증은 시간이 오래 걸리고 복잡하다는 이유로 많은 사람들이 다중 인증의 필요성을 인식하지만 필수적으로 사용하고 있지는 않고 있다[1-3].

기존 인증 메커니즘인 아이디와 비밀번호를 이용하여 사용자 인증을 진행할 경우 보안에 대한 걱정으로 비밀번호를 길고 복잡하게 입력하게 되는데 오히려 이로 인하여 사용자가 비밀번호를 잊어버리는 경우가 있다. 또한 본인과 연관된 단어나 숫자를 비밀번호에 활용하거나 관리의 어려움 때문에 다른 계정에서 서로 같은 비밀번호를 사용하게 된다. 이로 인하여 인증 정보를 노출하게 되며 개인 정보를 침해당할 수 있다. SMS 인증이나 일회용 비밀번호 인증은 외부의 시스템으로부터 정보를 받아오는 방식이기 때문에 중간에 정보를 가로채기 당해도 알아차리기가 어려운 문제가 존재한다[4,5].

본 논문에서는 위에서 언급한 문제점들을 해결하기 위해서 스마트폰을 이용하여 수집 가능한 상황 정보를 인증 요소로 활용하여 강화된 보안성과 편리성을 제공하는 사용자 인증 메커니즘을 제안한다. 사용자는 인증 과정을 진행할 때 아이디와 비밀번호가 타인에게 쉽게 노출이 될 수 있지만 스마트폰을 이용해 수집한 자동식별 정보를 추가적으로 활용하면 보안성을 강화할 수 있다. 사용자의 스마트폰의 UUID(Universally unique identifier) 및 스마트폰에서 획득한 공유기 ESSID 정보, 블루투스 기기 검색 정보, 스마트폰의 볼륨 정보, 화면 가로, 세로 정보 등을 이용하여 타인에게 쉽게 노출되지 않는 숨김 요소를 인증요소로 함께 활용함으로써 쉽고 간단하게 인증을 강화할 수 있는 사용자 인증 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 인증요소 기술에 관하여 알아본다. 3장과 4장에서는 사용자 인증 시스템을 위한 제안 메커니즘 및 시스템 구현에 대해서 알아보며 5장에서는 효용성에 대해서 평가를 진행한다. 마지막으로 6장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 인증요소 분류

비대면 특징을 가지는 온라인 서비스는 서비스를 받는 사용자가 접근에 대한 권한을 가진 적절한 사용자인지 인증하는 과정이 매우 중요하며 사용자 인증을 통하여 안정성과 신뢰성을 확보하는 것이 필수적으로 선행되어야 한다. 인증 기술을 인증요소에 따라 분류하면 소지기반, 지식기반, 특성기반으로 분류할 수 있다[6,7].

2.1.1. 소지기반 인증

소지기반 인증요소(What you have)는 사용자가 소유하고 있는 요소를 이용하여 사용자를 인증하는 방식이다. 소지기반 인증 요소로 사용되는 대표적인 인증기술로는 OTP(일회용비밀번호), 스마트카드, 보안토큰(HSM) 등이 있다. 인터넷뱅킹에서 자금이체 시 최종사용자 인증수단으로 사용자가 소지하고 있는 OTP를 입력하여 정당한 사용자가 거래를 지시하였음을 확인한다. 일반적으로 소지기반의 인증요소는 보안성으로 인해 대면에 의한 본인확인 후 발급되며, 인증매체의 소지 및 비용 등의 사용자 편의성 이슈가 존재한다.

2.1.2. 지식기반 인증

지식기반 인증요소(What you know)는 사용자가 알고 있는 요소를 통해 사용자를 인증하는 방식이다. 지식기반 인증 요소로 사용되는 인증기술의 예로는 비밀번호, PIN 등이 있다. 사용자가 웹사이트 로그인시 사용자의 ID와 사용자만 알고 있는 비밀번호를 입력하여 인증함으로써 사용자 본임임을 확인한다. 일반적으로 지식기반의 인증요소는 온라인상에서 편리한 사용자 인증기술로 널리 사용되고 있다.

2.1.3. 특성기반 인증

특성기반 인증요소(What you are)는 사용자가 가지고 있는 고유한 특성을 이용하여 사용자를 인증하는 방법이다. 특성기반 인증요소로 사용되는 인증기술의 예로는 지문, 목소리, 홍채 등이 있다. 예를 들어, 비밀금고 출입 시 사용자는 등록한 지문을 입력하여 사용자 본인임을 확인할 수 있다. 특성기반 인증기술은 보안성이 뛰어난 인증기술이기는 하나, 특성정보 노출에 따른 프라이버시 이슈 등으로 인해 접근제어 용으로 주로 사용되고 있다.

2.1.4. 기타 인증요소

위에서 분류하는 세 가지 인증요소 외에 최근에는 전자적인 서명필체, 위치정보 등의 인증기술이 사용되어지고 있다. 사용자 스마트폰의 GPS 기능을 활용하여 사용자의 위치를 확인하여 유효한 경우에만 서비스를 제공하는 등의 방법으로 사용되고 있다. 이러한 인증기술들은 최근 기술의 발달로 소지기반, 지식기반, 특성기반 인증요소 외에 다양하게 사용자를 확인할 수 있는 인증요소가 개발되어 사용하고 있다.

2.2. 다중요소 인증기술

다중요소 인증기술은 각각의 단일요소 인증기술을 두 가지 이상의 인증요소를 결합하여 사용자를 인증하는 방법을 의미한다. 포털, 금융, 게임 사이트 등의 국내 온라인 서비스에서 대표적으로 사용되는 다중요소 인증기술로는 사용자의 지식기반 인증요소인 비밀번호와 소지기반 인증요소인 OTP의 두 가지의 인증요소를 이용하는 것을 예로 들 수 있다. 다중요소 인증기술은 하나의 인증요소가 해킹에 의해 유출 또는 탈취 되더라도 이와 독립적인 다른 인증요소에 의해 안전하게 사용자 인증을 제공할 수 있기 때문에 단일요소 인증에 비하여 보안성을 향상시킬 수 있다.

2.3. 스마트폰을 이용한 인증기술

최근 모바일 기기가 발달함에 따라 모바일 기기를 활용하여 사용자 편의성을 향상시킨 인증기술이 등장하고 있다. 예를 들어, USIM, 현금 IC카드와 NFC기능이 내장된 모바일 기기를 활용한 일회용비밀번호(OTP), 공인인증서 등의 서비스가 이에 속한다. 또한 인터넷뱅킹을 통한 자금이체 시 등록된 휴대폰번호로 전화를 걸어 추가인증을 하는 등의 2채널 인증도 모바일 기기를 활용한 인증기술이다.

2.3.1. 가속도 센서를 이용한 인증

가속도 센서는 스마트폰에서 활용 가능한 대표적인 인증요소이다. J. S. Seo, et al. 은 스마트폰 가속도 센서를 이용하여 사용자의 걸음 패턴(gait)를 분석하여 생체 기반 사용자 인증요소로서 활용하였다[8]. 주성분 분석, 가우시안 혼합 모델링을 통해 얻은 데이터를 학습하고 신뢰구간 검증 방식을 통해서 약 96% 정확도를 가지고 사용자를 구분하였다. 가속도 센서는 사용자의 건강상태 및 환경 조건에 따라서 그 변이가 심하기 때문에 실생활에서 이용하기 위해서는 많은 정보를 수집하고 다양한 학습이 이루어져야 하는 한계점이 존재한다.

2.3.2. 지자기 센서를 이용한 인증

H. Ketabdar, et al. 은 지자기 센서를 이용하여 종이에 펜으로 글씨 쓰듯이 공중에서 자성이 있는 펜이나 반지를 이용하여 사인을 하게 되면 인증이 이루어지는 MagiSign 기술을 제안하였다[9]. 자기장의 변화를 감지하는 도구로는 스마트폰, 특수한 반지, 펜 등의 토큰이 필요하며 복잡한 사인을 인식하기 위해서는 기존의 스마트기기에 탑재된 지자기 센서보다 정밀한 값을 얻을 수 있는 센서가 필요하다. 또한 보급형 스마트폰의 경우 가격을 낮추기 위해서 성능이 제한되어 있는 센서가 사용되는 경우가 있으므로 범용적으로 활용하기에는 한계점이 존재한다.

2.3.3. 촉각과 음성을 이용한 인증

A. Bianchi, et al. 은 촉각과 음성을 이용하여 인증에 사용하는 The Phone Lock을 제안하였다[10]. 화면에 버튼을 위치시키고 각 버튼에 해당하는 음성 및 진동을 통해서 비밀번호로 사용하는 기술로서 사용자가 원하는 타킷 버튼을 중앙으로 드래그하여 등록시킨 후 사용하게 된다. 지식기반 인증을 응용한 기술로서 복잡하게 패턴을 정의할 수 있지만 이는 오히려 사용자가 사용하기 어렵게 할 수 있다는 단점이 존재하며, 다른 사람의 훔쳐보기 공격에 무력화 될 수 있다는 한계점이 존재한다.

Ⅲ. 제안된 사용자 인증 메커니즘

3.1. 제안된 사용자 인증 매커니즘

사용자 인증 메커니즘에 대한 블록 다이어그램은 그림 1과 같다. 사용자는 자신이 소유하고 있는 지식기반 인증요소, 생체기반 인증요소를 이용해서 인증을 시도하며, 인증 시도 과정 중에 스마트폰에서 수집 가능한 스마트폰 고유정보(UUID), 검색된 블루투스 기기 목록, 연결된 와이파이 SSID, 스마트폰 볼륨 정보, 화면 회전 정보를 수집하여 함께 인증요소로 활용한다.

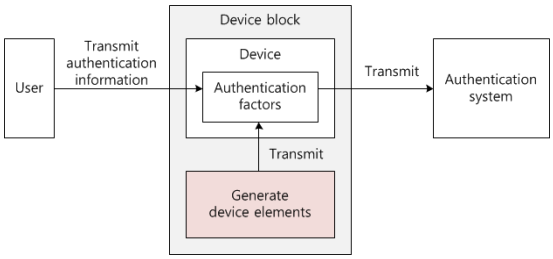

Fig. 1 Proposed Authorization Mechanism

인증요소는 각각의 별도인증요소로 활용할 수도 있지만 다른 인증요소를 암호화 및 복호화하는 암·복호화 키로도 활용이 가능하다. 즉, 사용자는 아이디와 비밀번호를 이용하여 로그인하는 것처럼 사용하지만 실제로는 수집된 자동식별정보를 숨김인증요소로서 이용하여 인증을 시도하는 것이다. 만일 파일 암호화에 사용한다면 해당 기기에서만 열 수 있는 강력한 보안성을 가진 파일을 생성할 수 있다.

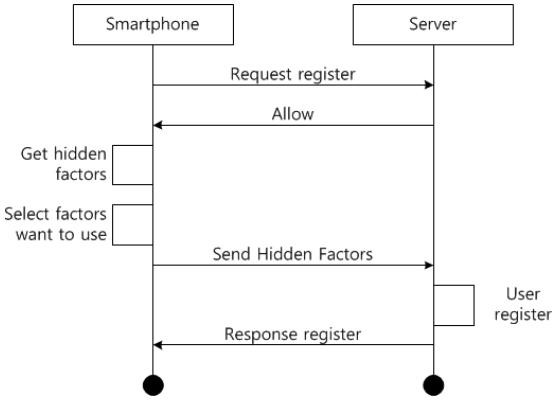

Fig. 2 User Register Flow

사용자는 인증 정보를 스마트폰에 입력하며 가상블록에서 스마트폰 정보를 수집 및 생성하여 인증요소로 포함한다. 디바이스 블록은 가상 블록으로서 스마트폰과 보안요소를 포함하며 인증정보를 서비스 제공자에게 전송하는 역할을 한다. 그림 2는 사용자가 숨김인증요소를 이용하여 사용자 등록하는 과정을 나타낸다.

수집된 정보 중 와이파이 SSID는 사용자의 위치 정보를 이용하여 특정 위치 또는 특정 네트워크에 등록된 경우에만 인증 시도가 이루어지도록 처리하기 위한 목적을 가진다. 블루투스 기기 검색 정보는 위치, 인증시도 전에 사용자 검증 등에 활용할 수 있다. 사용자는 등록을 위해서 숨김인증요소를 수집하고 인증에 사용할 요소를 선별하여 아이디, 비밀번호와 함께 등록에 사용한다. 스마트폰 UUID의 경우 16byte 길이를 가지며, 3×10^{38} 가지의 경우의 수를 가지고 있기 때문에 비밀번호를 암호화하는데 사용되는 SALT로서 활용하고 볼륨 정보는 암호화 반복 횟수(iteration count)에 활용하면 강력한 보안 인증으로 활용할 수 있다. 그림 3은 UUID와 볼륨 정보를 이용하여 암호화를 진행하는 그림이다.

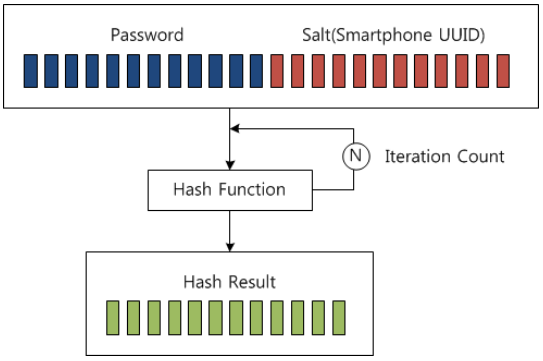

Fig. 3 Make Hash with Salt(Device UUID)

3.2. 데이터 수집

스마트폰에서 인증요소로 활용할 수 있는 정보는 페어링된 블루투스 목록, BLE 정보, 와이파이 SSID, 볼륨 정보, 화면 회전 정보 등이 있다. 그림 4는 인증요소로 활용하기 위해 수집된 블루투스 기기 목록을 보여준다. 블루투스 기기 목록을 활용한 인증은 다른 기기를 추적으로 활용하여 인증에 사용할 수 있기 때문에 소지 기반 인증과 같은 개념으로도 인지할 수 있다.

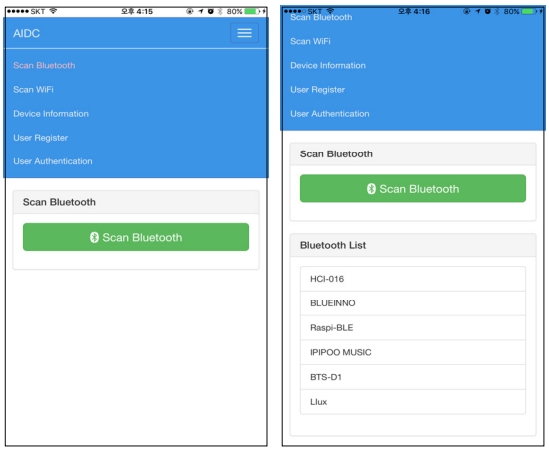

Fig. 4 Scan Bluetooth Devices Screen

그림 5는 인증요소로 활용하기 위해 수집된 와이파이 SSID 목록을 보여준다. 와이파이 SSID 목록은 가장 쉽게 획득할 수 있는 정보로서 네트워크에 연결하지 않고도 활용할 수 있는 정보이다. 다만 순서에 있어서 일정하지 않기 때문에 정확도를 기대하긴 어려울 수 있어서 실내에서 위치 정보를 획득하는데 사용하는 것이 바람직하다.

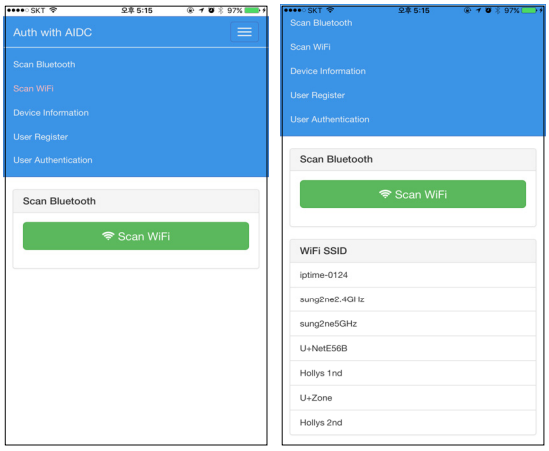

Fig. 5 Scan Wifi SSID Screen

그림 6은 인증요소로 활용하기 위해 수집된 스마트폰 정보를 보여준다. 스마트폰 정보는 복사가 어려운 고유한 정보가 있기 때문에 이를 통해서 아이디, 비밀번호 없이도 기기 인증이 가능하다는 장점을 가지며 추가적으로 정보를 입력하는 방식에 비해서 빠른 인증이 가능하다.

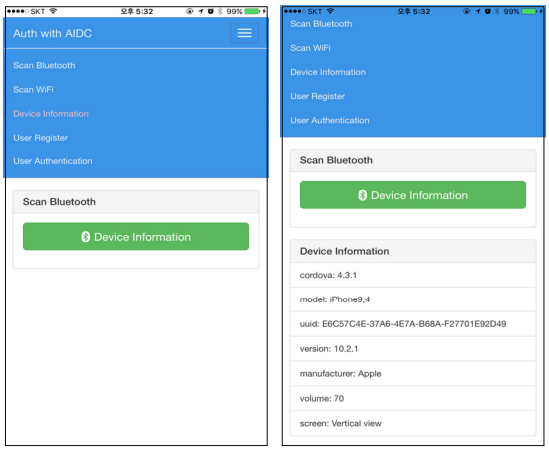

Fig. 6 Smart Device Information Screen

3.3. 제안 시스템 동작

그림 7는 제안하는 시스템에서 사용자 인증을 위한 스마트폰과 인증 서버와의 등록 및 인증 정보 교환 동작을 나타낸다.

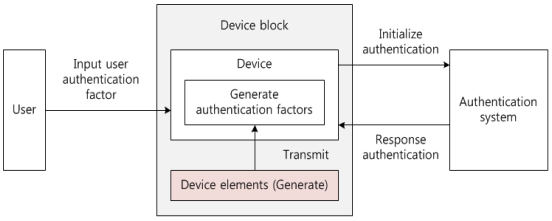

Fig. 7 Proposed System Flow with Authentication Factors

① 사용자 스마트폰에서 사용자가 입력한 인증요소와 스마트폰에서 생성된 인증요소를 함께 인증 서버로 전송하여 등록을 요청한다.

② 인증 서버에서는 등록 요청 정보와 관련된 정책정보를 이용하여 데이터베이스를 구축하고 스마트폰으로 요청 완료를 응답하여 등록 과정을 완료한다.

③ 등록과정 이후 인증을 위해서는 사용자가 인증요소를 입력한다. 이때 등록과정에서 사용한 스마트폰에서 수집 가능한 인증요소가 함께 인증서버로 전송될 수 있도록 동일한 환경을 적용해 주어야 한다. 등록에서 화면을 돌렸다면 동일하게 돌려주어야 하며, 연결된 와이파이 SSID도 동일하게 적용을 해주어야만 인증에 성

공할 수 있다.

④ 인증 서버는 전달된 인증요소를 검증하고 사용자 인증을 수행 후 이에 대한 결과를 응답해 준다.

Ⅳ. 제안된 시스템 구현

제안한 사용자 인증 메커니즘이 적용된 시스템을 구현하기 위해서 파이썬 플라이스 프레임워크를 이용하여 서버를 구현하였다. 사용자 정보 관리를 위한 데이터베이스로는 MySQL 서버를 이용하였으며, 사용자 인증 애플리케이션 구현을 위하여 하이브리드 방식인 Cordova를 이용하였다. 하이브리드 개발방식은 네이티브 개발방식에 비해서 하나의 소스코드로 iOS, Android, Windows Mobile에서 동작 가능하도록 개발이 가능하다는 장점이 있다.

표 1은 사용자 인증을 위해서 사용자 아이디, 비밀번호를 저장하는 테이블을 나타낸다.

Table. 1 USER Table Schema

Field	Type	ETC
IDX	INTEGER	PRIMARY KEY AUTO INCREMENT
USER_ID	VARCHAR(20)	NOT NULL
USER_PW	VARCHAR(255)	NOT NULL

아이디, 비밀번호 이외의 다른 인증요소는 여러 개의 정보를 가질 수 있으므로 표 2과 같이 별도의 테이블을 구성한 후 사용자 아이디를 외래키로 활용하도록 구성하였다. AUTH_FACTOR 테이블은 구분번호, 요소타입, 요소값, 사용자 아이디 필드로 구성하였다.

Table. 2 AUTH_FATOR Table Schema

Field	Type	ETC
IDX	INTEGER	PRIMARY KEY AUTO INCREMENT
FACTOR_TYPE	VARCHAR(255)	NOT NULL
FACTOR_VALUE	VARCHAR(255)	NOT NULL
USER_ID	VARCHAR(20)	FOREIGN KEY

그림 8은 사용자 등록을 진행하는 화면이다. 검색된 와이파이 ESSID와 블루투스 기기 중 인증에 사용할 정보를 선택하고 아이디와 비밀번호를 입력한다. 볼륨 정보와 스마트폰 UUID 정보는 자동으로 습득하기 때문에 사용자가 별도로 선택하지 않고 등록을 진행하며, 진행 과정 중에 자동으로 암호화 처리에 사용된다.

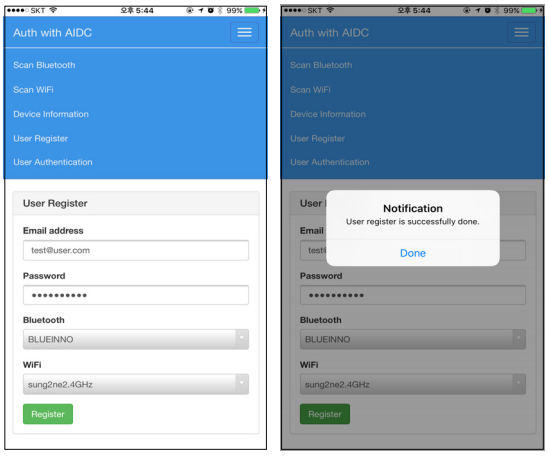

Fig. 8 User Register Screen

그림 9는 사용자 인증 서버에서 사용자를 등록하고 인증을 시도하는 테스트 화면이다. 인증을 위해서 사용자로부터 지식기반 인증요소인 아이디와 비밀번호를 입력받아서 인증을 시도하도록 만들었다. 사용자는 본인의 아이디와 비밀번호만 입력하기 때문에 다른 사람에게 노출이 되더라도 숨겨진 인증요소를 확인할 수 있는 방법은 없으므로 강건한 보안성을 유지할 수 있다.

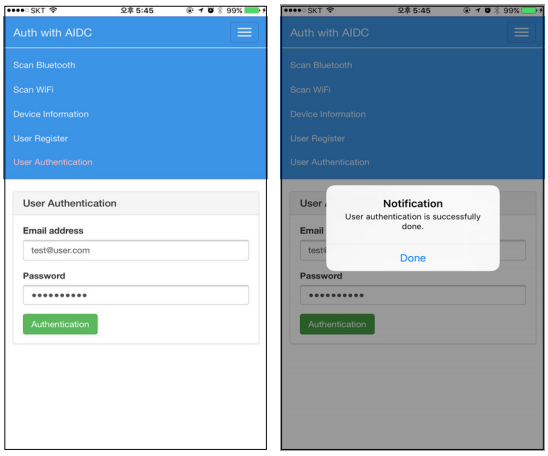

Fig. 9 User Authentication Screen

Ⅴ. 사용자 인증 메커니즘 효용성 분석

사용자 인증을 위한 요소에 있어서 한국인터넷진흥원에서 발표한 본인확인수단의 적합성 기준으로 보편성, 유일성을 갖추어야 하며, 본인확인 기관은 경제성과 법적 타당성(서비스의 명확성)을 고려하여야 하며, 사용자는 대체수단의 범용성 및 본인확인기관에 대한 신뢰성을 고려하여 대체 수단을 선택하여야 한다고 보았다. 이에 따라서 안전성, 편리성, 안정성, 이용성을 본인 확인수단의 적합성 기준으로 제시하였다. 본 논문에서는 인증기술의 기술로 적용성(적용 가능성, 적용 비용, 기술 중립성, 기존인프라 활용성), 편의성(소지사용, 발급, 교육 편의성), 보안성(오프라인 공격대응, 온라인 공격대응, 거래조작 공격대응)을 기준으로 효용성에 대해서 논의 한다.

5.1. 편의성

편의성이란 휴대 및 이용이 간편하고, 언제 어디서든지 쉽게 이용할 수 있는 인증기술인지 여부를 말한다. 본 논문에서 제안하는 스마트폰을 이용해 수집 가능한 정보를 인증 요소로 활용하는 메커니즘을 적용할 경우 항시 휴대하고 다니는 스마트폰을 이용하기 때문에 배터리가 없는 경우를 제외하고 쉽고 빠르게 인증요소를 획득할 수 있다.

5.2. 보안성

보안성이란 지속적으로 발전하는 신규 해킹기술에 대응하여 보정거래 방지의 효과 여부를 말한다. 자신이 가진 고유한 정보를 소유할 수 있고, 또한 인증요소를 다양하게 변화시킬 수 있는 환경적 요인을 적용하면 동일한 장소 및 동일한 기기에서도 여러 권한을 적용하는 것이 가능하며 또한 인증요소가 숨어 있기 때문에 예측이 불가능하여 해킹에 대해서도 상당한 방지효과를 거둘 수 있다.

5.3. 적용성

적용성이란 스마트폰, IPTV 등 새로운 전자금융환경에 적합한 인증기술 인지 여부를 말한다. 제안한 인증 메커니즘은 스마트폰 뿐만 아니라 안드로이드 플랫폼을 이용하여 동작하는 스마트 기기라면 기기정보 및 주변 상황정보를 습득하는 것이 가능하기 때문에 다양한 기기에 적용 가능하다는 특징이 있어 그 활용도가 기대되는 인증기술이다.

Ⅵ. 결 론

현재 전세계 스마트폰 이용자가 20억명을 넘어설 것으로 예측하고 있으며 PC를 이용한 인터넷 인증보다 스마트폰을 이용한 인터넷 인증이 더 많이 이루어지고 있다. 이에 따라서 기존의 PC 환경을 기준으로 이루어지던 사용자 인증과정에도 변화가 필요하며 모바일 환경을 기준으로 확대하여 새로운 인증요소를 획득 및 활용할 수 있어야 한다. 스마트폰을 이용하면 PC 보다 다양한 인증요소를 획득할 수 있으며 이를 이용하여 더 강력한 보안 체계를 유지할 수 있다. 본 논문에서는 사용자의 스마트폰에서 획득 가능한 와이파이 검색 정보, 블루투스 기기 검색 정보, 스마트폰 볼륨 정보, 화면 가로, 세로 모드 정보, 디바이스 UUID 정보 등을 획득하여 인증요소로서 활용하는 사용자 인증 메커니즘에 대해서 제안하였다. 와이파이와 블루투스 정보의 경우 해당 위치에서만 인증이 이루어지도록 할 수 있는 위치기반 인증요소로서 활용할 수 있다. 스마트폰의 UUID와 화면 정보 및 볼륨 정보를 이용하여 Salt 및 암호화 횟수로 활용하면 숨김요소로서 비밀번호를 암호화 할 수 있는 장점이 있다. 제안된 인증 메커니즘은 아이디와 비밀번호를 이용한 1차원적인 인증에서 다차원적인 인증요소를 활용함으로써 안전성, 보안성을 확보할 수 있으며, 별도의 기기를 사용하는 것이 아닌 항시 휴대하는 스마트폰을 이용하여 인증이 이루어지기 때문에 활용도와 편의성이 높다고 할 수 있다. 본 연구를 초석으로 하여 향후 연구로 사용자 인증뿐만 아니라 파일 암·복호화 기술에도 적용할 수 있도록 연구를 진행하여 문서 및 멀티미디어 동영상이나 음원을 위한 DRM(Digital Rights Management) 적용과 같은 파일보호 분야에 적용이 가능하도록 연구를 진행할 예정이다.

REFERENCES

[1] K. Y. Jin, S. H. Choi, J. W. Seo, and Y. G. Kim, “An Approach to Systems with Multi-Factor Method,” *Journal*

of the Korea Academia-Industrial cooperation Society, vol. 13, no. 2, pp. 842-848, Feb. 2012.

[2] J. Y. Lee, H. S. Shim, K. S. Han, Y. L. Choi, and J. B. Kim, "A Study on the Models of Internal system users Authentication considering Multi Factors," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 9, pp. 2044-2055, Sept. 2015.

[3] C. S. Kim, S. B. Youn, and M. K. Lee, "Shoulder-Surfing Resistant Password Input Method for Mobile Environment," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 20, no. 3, pp. 93-104, June 2010.

[4] S. S. Ji, "The Improved-Scheme of Two Factor Authentication using SMS," *Journal of the Korea Industrial Information Systems Research*, vol. 17, no. 6, pp. 25-30, Dec. 2012.

[5] M. K. Choi, T. C. Kwan, and D. H. Lee, "Analysis of Security Vulnerability in Home Trading System, and its Countermeasure using Cell phone," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 23, no. 1, pp. 19-32, Feb. 2013.

[6] "Standardization trend of non-face authentication technology based on telebio recognition," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 25, no. 4, pp. 43-50, Oct. 2015.

[7] MAS, Internet banking and technology risk management guidelines, Version 3.0, *Monetary Authority of Singapore*, June 2008.

[8] J. S. Seo, and J. S. Moon, "A Study on User Authentication with Smartphone Accelerometer Sensor," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 25, no. 6, pp. 1477-1484, Dec. 2015.

[9] H. Ketabdar, K. A. Yuksel, A. Jahnbekarn, M. Roshandel, and D. Skirop, "MagiSign: User Identifaction /Authetication Based on 3D Around Device Magnetic Signatures," *The Fourth International Conference on Mobile Ubiqutous Computing, Systms, Services and Technologies*, pp. 31-34, 2010.

[10] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices," *TEI`11 Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, pp. 197-200, Jan. 2011.

정필성(Pil-Seong Jeong)

2004년 2월 : 서울과학기술대학교 전자공학과(공학사)
2007년 8월 : 광운대학교 전자통신공학과(공학석사)
2013년 8월 : 광운대학교 전자통신공학과(공학박사)
2016년 8월 ~ 현재 : ㈜하트미디어
※관심분야 : 임베디드 시스템, WSN, WBAN

조양현(Yang-Hyun Cho)

1982년 2월 : 광운대학교 전자통신공학과(공학사)
1985년 2월 : 광운대학교 전자통신공학과(공학석사)
2012년 2월 : 광운대학교 전자통신공학과(공학박사)
1987년 9월 ~ 1997년 8월 : LG정보통신 전송기술개발실 과장
1997년 9월 ~ 현재 : 삼육대학교 컴퓨터학부 교수
※관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS