JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 22, No. 1 : 75~82 Jan. 2018

자동인식 및 데이터 수집을 이용한 사용자 인증 시스템

정필성[1] · 조양현[2*]

User Authentication System based on Auto Identification and Data Collection

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

[1]JNPSOLUTION B1 104, 64, Myeongnyungil, Jongno-gu, Seoul, Korea
[2*]Division of Computer Science, Sahmyook University, Seoul 01795, Korea

요 약

모바일 기기 사용자가 증가함에 따라서 다양한 사용자 인증 방식에 대한 연구가 활발하게 진행되고 있다. 사용자 인증방식에는 사용자 아이디와 비밀번호를 이용하는 지식기반 인증방식, 사용자만이 가지고 있는 특성인 생체기반, 위치기반 등을 이용하는 방법과 OTP(On Time Password)와 같은 2차 인증을 진행하는 인증방식이 사용되고 있다. 본 논문에서는 기존 인증방식의 문제점을 개선하고 사용자가 원하는 방식으로 암호화가 진행될 수 있는 사용자 시스템을 제안한다. 제안한 인증 시스템은 모바일 기기를 이용하여 인증요소를 수집하는 인증요소 수집 모듈, 수집한 인증요소를 조합하여 보안키를 생성하는 보안키 생성 모듈, 생성된 보안키를 이용하여 인증을 진행하는 암호화 및 복호화 모듈로 구성된다.

ABSTRACT

As user of mobile device increases, various user authentication methods are actively researched. The user authentication methods includes a method of using a user ID and a password, a method of using user biometric feature, a method of using location based, and a method of authenticating secondary authentication such as OTP(One Time Password) method is used. In this paper, we propose a user system which improves the problem of existing authentication method and encryption can proceed in a way that user desires. The proposed authentication system is composed of an authentication factor collection module that collects authentication factors using a mobile device, a security key generation module that generates a security key by combining the collected authentication factors, and a module that performs authentication using the generated security key module.

키워드 : 모바일 기기, 보안키, 사용자 인증, 인증요소, 인증 시스템

Key word : Mobile Device, Security Key, User Authentication, Authentication Factors, Authentication System

Received 25 October 2017, **Revised** 01 November 2017, **Accepted** 27 November 2017

* **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.2018.22.1.75 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

스마트폰, 태블릿과 같은 모바일 기기의 보급률이 전 세계적으로 증가하고 있으며 대한민국은 2015년 3월 기준으로 83.0%의 보급률로 성인 40,879,472명 중 33,929,961명이 스마폰을 사용하고 있다[1]. 스마트폰 보급률이 증가함에 따라서 모바일 환경에서 쉽고 편하게 개인 정보를 다룰 수 있는 기술들이 발전되고 있다. 하지만 모바일 기기에서 편하게 개인 정보를 다룰 수 있기 때문에 개인 정보에 대한 보안을 취약하게 만드는 문제점이 제기되고 있으며 이를 위해서 다양한 모바일 기기에서 편리하고 안전하게 사용자 인증을 통해 개인 정보를 보호하는 기술에 대한 연구가 활발하게 진행되고 있다[2-10].

개인 정보는 다양한 방법으로 인증기법을 적용하여 다루게 된다. 사용자를 인증하기 위한 판단 기준이 되는 정보를 인증요소라고 한다. 인증요소는 사용자가 알고 있는 정보를 이용하는 지식기반, SMS나 음성, 이메일 등을 이용하는 소지기반, 질문에 대한 답을 유도하는 특징기반, 사용자가 가진 고유한 생체정보를 이용하는 생체기반 등이 있다. 사용자를 인증하기 위한 가장 쉬운 방법은 아이디와 비밀번호를 사용하는 지식기반 인증 방법이다[2].

지식기반 인증 방법은 구현하기 쉽고 변경이 용이하다는 장점이 있어서 널리 이용되고 있지만 사용자를 인증하기 위한 아이디와 비밀번호를 서버에 저장하기 때문에 보안성 관점에서 부족한 부분이 있다. 또한 대부분의 사용자는 하나의 아이디와 비밀번호를 여러 서버에서 사용자 인증 용도로 사용하고 있기 때문에 타인에게 엿보기 공격(Shoulder Surfing)이나 추측 공격(Guessing Attack) 등을 당할 경우 대다수의 서버에 접속할 수 있는 권한을 넘겨주는 경우가 생길 수 있다[3].

지식기반 인증 방법의 문제점을 보완하기 위해서 사용자가 소지하고 있는 정보를 이용하는 OTP, 공인인증서, 보안카드, NFC(Near Field Communication) 등의 인증 방식을 지원하거나 비밀번호를 사용하지 않고 사용자의 생체 정보를 인증하는 FIDO(Fast IDentity Online) 기술 기반의 지문인식, 홍체인식 등의 다양한 인증 방식이 사용되고 있다. 하지만 소유기반 인증은 타 인증 방식에 비해서 몇 번의 클릭과 인증 시도가 이루어져야 하며, 항시 소지하고 있지 않다면 인증이 불가능한 단점이 존재한다.

사용자가 항시 휴대하는 스마트 폰과 같은 모바일 기기를 이용하여 위치를 추적하고 이를 통해 인증을 진행하는 위치기반 인증에 대한 연구가 진행되고 있다. 위치 기반 인증으로는 네트워크 기반, 위성신호 기반, AP(Access Point) 기반이 있다. 네트워크 기반 인증은 기지국과 단말기 간의 신호의 방향, 도달시간 등을 기준으로 단말기의 위치를 추적하는 방법으로 오차율이 수백 미터에서 수백 킬로미터로 크기 때문에 보안인증 요소로 활용하기에는 한계점이 존재한다. 위성신호 기반 인증은 인공위성과 단말기까지의 전파 도달시간을 기준으로 위치를 추적하는 방법으로 GPS(Global Positioning System), Galileo, COMPASS 등이 사용된다. 위성신호 기반 기술은 네트워크 기반 기술에 비해서 오차율이 상대적으로 적지만 실내에서 사용이 불가능하다는 점과 수십 미터에서 최대 100여 미터 까지 오차가 생길 수 있어서 보안인증요소로 활용하기에는 활용도가 낮다. AP 기반 인증 기술은 타 위치 기반 기술에 비해서 정확도가 높고 실내외에서 사용 가능한 기술이다. 하지만 MAC 주소 및 SSID(Service Set Identifier)를 흉내 내는 것이 가능하며 스마트폰에서 이루어지는 모든 무선 통신 정보를 해커에게 보여줄 수 있는 치명적인 단점이 존재한다[1].

본 논문에서는 기존의 인증 방식의 한계점을 해결하기 위해서 모바일 기기를 통해 수집가능한 자동식별 정보(NFC 태그, RFID 태그, QR 코드, 바코드 등)와 자동수집 가능한 정보인 IMEI(International Mobile Equipment Identity), WLAN MAC Address, Bluetooth Address, Bluetooth Beacon, 전화번호, 연결된 WiFi SSID, Orientation 센서 정보, 근접 센서 정보, 조도 센서 정보, 음량 정보(진동/무음/벨소리 상태) 등을 수집하는 자동식별 기반 인증 요소 수집 모듈 개발하고 수집한 인증요소를 이용하여 보안키를 생성하고 , 생성한 보안키를 활용하여 사용자 인증 서비스 제공 및 문서나 파일, 데이터를 암호화 및 복호화하는 보안 시스템을 제안한다. 제안 시스템에 적용된 알고리즘은 보안키가 타인에게 노출될 염려가 적으며 노출되더라도 어떤 정보를 사용해서 보안키를 생성하였는지 알 수 있는 방법이 없으므로 안전하고 편리한 인증 방법으로 평가할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 모바일 기

기를 이용한 인증기술에 관하여 알아본다. 3장과 4장에서는 사용자 인증 시스템을 위한 제안 알고리즘과 제안 알고리즘이 적용된 시스템 구현 및 효용성 평가에 대해서 알아본다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 모바일 기기를 이용한 인증 기술

모바일 기기가 발달함에 따라서 모바일 기기에 내장되어 있는 다수의 센서 정보를 활용하는 인증 기법과 같은 모바일 환경에 적합한 인증 기술이 개발되고 있다.

2.1.1. 위치정보 기반 인증

위치정보 기반 인증 기술은 모바일 기기에서 활용 가능한 대표적인 인증 기술이다. Feng Zhang, et al.은 GPS와 AP 정보를 인증요소로 활용하였다[4]. 하지만 사용자의 위치 정보의 범위가 넓고 위치정보에 대한 암호화 과정이 존재하지 않아 위치정보가 노출될 위험이 존재한다. H. Takamizawa, et al. 은 사용자의 실제 주소지의 GPS 정보와 다수의 모바일 기기의 GPS 정보를 비교하여 인증을 진행하는 알고리즘을 제안하였다[5]. 해당 방식은 GPS의 오차율로 인해 인증 정확도가 감소하는 한계점이 존재한다. W. Jansen, et al. 은 주변에 Policy beacon을 설치하여 beacon과 통신이 가능할 때만 인증이 진행되도록 연구를 진행하였다[6]. 하지만 인증이 필요한 지역마다 beacon을 설치해야 하므로 비용적인 측면의 한계가 존재한다.

2.1.2. 지자기 센서 기반 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[7]. 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 범용으로 활용하기에는 제한적이다.

2.1.3. 가속도 센서 기반 인증

T. K. Lee, et al. 은 모바일 기기의 가속도 센서 정보를 수집하여 사용자 인증요소로 활용하였다[8]. 모바일 기기를 손에 쥐고 움직이며 특정 패턴을 반복하면 그에 대한 정보를 분석하여 사용자를 인증하는 방법으로 사용자만의 고유한 움직임에 대한 패턴을 분석한 기술이다. 하지만 모바일 기기의 회전방향과 손에 쥐는 방향을 고려하지 않았기 때문에 인증요소로 사용할 경우 인증 실패할 가능성이 높다.

2.1.4. 생체정보 인증

A. Bianchi, et al. 은 촉각과 음성을 이용하여 인증에 사용하는 The Phone Lock을 제안하였다[9]. 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.

2.1.5. 다중 인증

T. K. Lee, et al. 은 사용자가 위치한 곳의 AP 정보를 1차 인증요소로 활용하고, 2차 인증요소로 생체 정보를 활용하여 사용자를 인증하는 기법을 제안하였다[10]. 하지만 AP 정보는 탈취, 위조, 변조가 쉽다는 단점이 있으며 생체 정보의 경우 날씨, 사용자의 컨디션, 기기 상태에 따라서 인증 성공률이 좌우될 수 있다는 제한사항이 존재한다.

Ⅲ. 제안 사용자 인증 알고리즘

3.1. 제안 모델

제안 사용자 인증 알고리즘을 적용하기 위한 모델은 그림 1과 같다. 제안 모델은 자동인식 및 데이터 수집 기술을 적용한 인증요소 수집 모듈과 수집된 정보를 이용하여 인증요소를 조합하여 보안키를 생성하는 보안키 생성 모듈과 생성한 보안키를 이용하여 암호화 및 복호화를 진행하는 암복호화 모듈로 나누어 구

성된다.

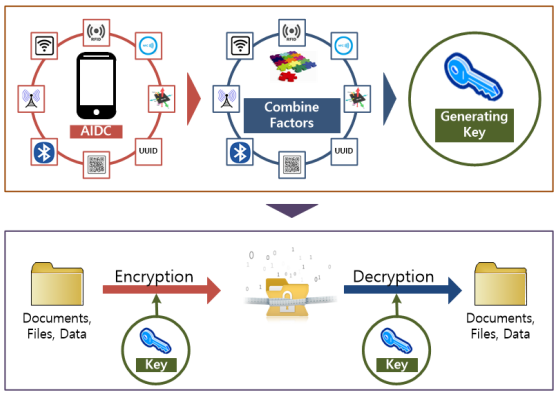

Fig. 1 Proposed Model

3.2. 인증요소 수집 모듈

인증요소 수집 모듈은 자동인식 및 데이터수집 기술을 기반으로 모바일 기기를 이용해서 수집가능한 자동식별 정보인 NFC 태그, RFID 태그, QR 코드, 바코드 등과 자동수집 가능한 정보인 IMEI, WLAN MAC Address, Bluetooth Address, Bluetooth Beacon, 전화번호, 연결된 WiFi SSID, Orientation 센서 정보, 근접 센서 정보, 조도 센서 정보, 음량 정보 등을 수집한다. 그림 2는 수집 가능한 정보를 보여준다.

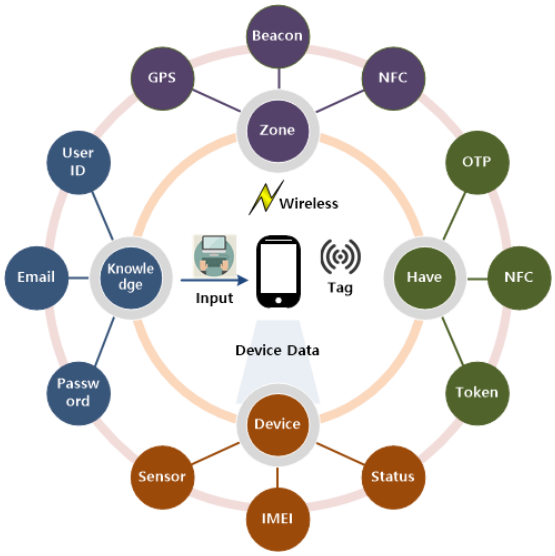

Fig. 2 AIDC-based Authentication Factors

3.3. 보안키 생성 모듈

보안키 생성 모듈은 인증요소 수집 모듈을 통해 수집한 정보를 조합하여 여러 개의 키를 생성한다. 필요에 따라 하나의 키만 사용할 수 있으며 AES(Advanced Encryption Standard) 알고리즘처럼 salt, iv 정보 등이 필요한 경우 각각의 키가 인자로 활용될 수 있다. 보안키 생성 모듈 개념도는 그림 3과 같다.

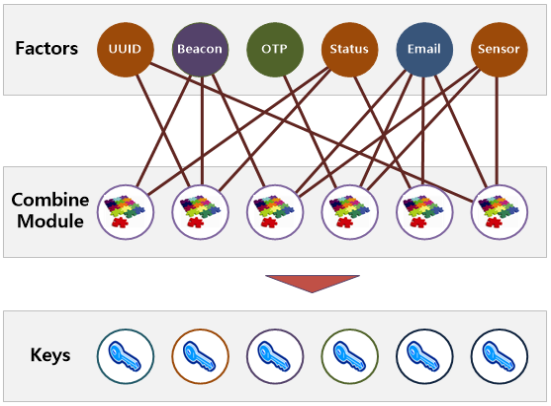

Fig. 3 Generating Authentication Key

그림 4는 보안키를 생성하는 과정을 보여준다.

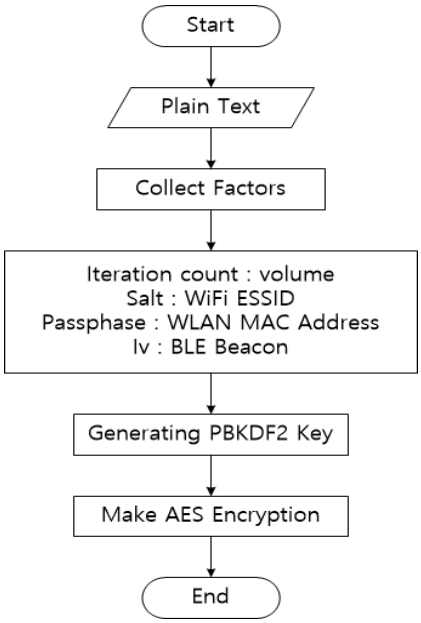

Fig. 4 AES Encryption Process

그림 4에서는 비밀번호를 암호화 하기 위해 수집된 정보 중 음량 정보, WLAN MAC Address, WiFi ESSID, BLE Beacon을 사용하여 iteration count, passphrase, salt, iv로 사용하여 PBKDF2 키를 생성하고 AES 알고리즘을 적용하여 암호화 하는 과정을 보여준다.

3.4. 암복호화 모듈

암복호화 모듈은 생성한 보안키를 이용하여 사용자가 선택한 보안 방식에 맞춰서 암호화를 진행하거나 복호화를 진행하는 모듈로서 인증을 진행할 때 사용한다. 암호화 및 복호화를 진행하는 알고리즘을 수행할 때의 시간은 모바일 기기의 성능에 따라 좌우된다. 때문에 사용자가 선택적 암호화 및 복호화를 할 수 있도록 해야 사용자가 만족하는 시간 내에서 정보를 처리할 수 있다.

Table. 1 Encryption Process Time

Device	Processing Time (ms)		
	AES 128	AES 256	AES 512
Galaxy S5	832	1089	2033
Galaxy S6	527	941	1293
Galaxy S8	244	597	1092
Galaxy Note 4	692	1429	1827
Galaxy Note 5	482	870	1594

표 1은 국내 대표적 스마트폰인 갤럭시 5, 갤럭시 노트 4, 갤럭시 노트5, 갤럭시 8의 AES 알고리즘을 처리 시간을 비교한 것이다. 사용된 데이터는 30 Byte 크기의 이메일, 20 Byte 크기의 비밀번호를 포함하는 JSON 구조를 가진다. 표 1의 내용을 통해서 보듯이 최신의 기기일수록 처리 시간이 짧기 때문에 사용자가 숨기려는 정보와 사용 기기에 맞게 알고리즘을 선택적으로 사용 가능하도록 처리해야 한다. 기본적으로는 사용자의 기기 모델을 찾아내고 미리 정해진 규칙에 맞게 기본 값을 설정하고 사용자가 변경하는 방식으로 사용한다. 제안 모듈에서는 아이디, 비밀번호를 이용하는 방식과 API 서비스를 제공하는 웹서버와 스마트폰의 데이터 교환방식에는 빠른 데이터 교환을 위하여 PBKDF2 기반의 AES 128방식을 적용하며, 스마트폰 내부의 데이터 및 폴더를 관리하는 방식에는 분실할 경우 정보 유출로부터 보호하기 위하여 PBKDF2 기반의 AES 256 방식 또는 PBKDF2 기반의 AES 512 방식을 적용한다. 이때 AES 암호화 비트는 스마트폰의 모델명을 가지고 기기의 성능을 기준으로 결정하게 된다.

Ⅳ. 제안 알고리즘 기반 시스템 구현

본 장에서는 제안 알고리즘의 효용성 평가를 위하여 제안 알고리즘을 기반으로 하는 인증 시스템 설계 및 구현에 대해서 설명한다.

4.1. 시스템 구성

본 논문에서 제안한 알고리즘을 기반으로 하는 인증 시스템은 사용자용 스마트폰 애플리케이션, 스프링 프레임워크를 이용하여 개발된 웹 서버, MySQL 데이터베이스 서버, 인증 상태에 대한 정보를 실시간으로 전달할 FCM(Firebase Cloud Messaging) 서버를 이용하여 구현하였다. 제안 알고리즘 기반 시스템 구성은 그림 5와 같다. 구현된 사용자 인증 시스템은 제안한 알고리즘의 성능을 검증하기 위한 프로토타입으로 사용자 계정을 관리하는 웹서버와 데이터베이스를 이용하여 인증서버만 구현하고 실시간 메시지 전송을 위한 서버는 별도로 구현하지 않고 FCM을 이용하였다. FCM을 이용하면 서로 다른 플랫폼 간에 실시간으로 안정적인 메시지 교환을 위한 시스템을 구현하기 용이하다.

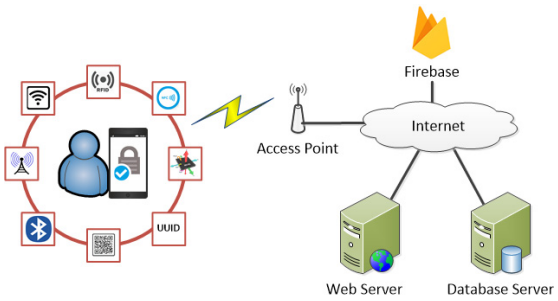

Fig. 5 Proposed Algorithm-based System Model

그림 6은 사용자의 스마트폰에서 수집할 수 있는 정보들을 리스트로 보여주고 암호화 인증키 생성에 사용할 요소들을 고르는 화면과 이를 이용하여 생성한 인증키를 로그로 출력하는 화면이다. 구현된 모바일 기기용

애플리케이션은 다양한 환경에서 여러 개발 언어의 호환성 평가를 위해서 HTML, CSS, 자바스크립트를 이용하는 Framework 7과 자바 언어를 이용하는 안드로이드 플랫폼이 혼합된 형식의 하이브리드 개발 방식으로 개발하였다.

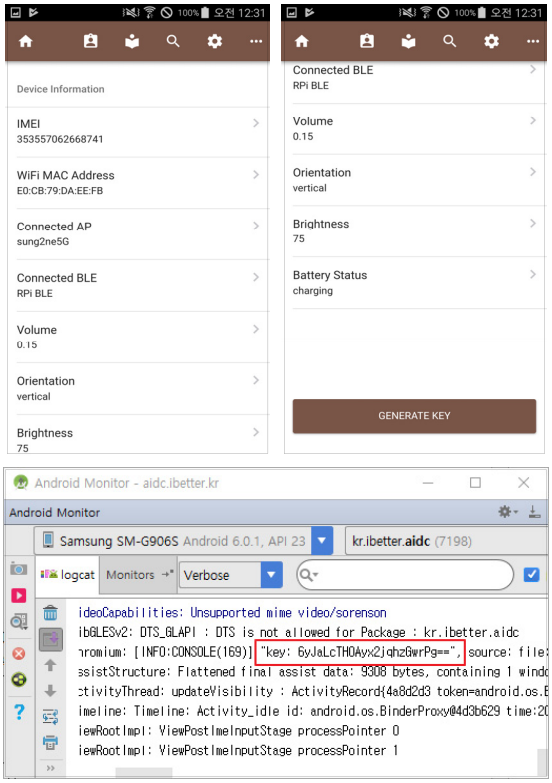

Fig. 6 Smartphone Application Screen

4.2. 효용성 평가

제안 시스템은 사용자가 항상 휴대하고 있는 모바일 기기를 이용하여 개인정보를 보호하고 사용자 인증을 진행할 수 있는 방안을 제시한다. 모바일 기기를 통해 수집가능한 자동식별 정보와 자동수집 가능한 정보를 구분하여 필요에 따라서 사용자가 선택적으로 사용하여 보안키를 생성하며 별도로 보안키를 생성하는 요소를 저장할 필요가 없어 타인에게 보안키 생성 방법을 노출할 염려가 없다. 또한 보안키에 사용하는 정보는 다른 기기에서도 사용하거나 수집 가능한 정보로서 이를 이용하면 타인과의 협조를 통해 보안키를 생성하는 상호 협력기반의 인증키 생성이 가능하다. 본 절에서는 제안 시스템과 기존 시스템과의 비교 분석을 통해 효용성을 논의한다. 표 2는 기존 시스템과의 장점을 객관적으로 분석하여 제시한 내용이다.

Table. 2 Authentication System Comparison

	ID/PW	OTP	Finger print	AP	Proposed
Usability	High	Low	High	Low	High
Feature	Static	Dynamic	Static	Dynamic	Dynamic
Attack	High	Low	Low	High	Low
Portable	High	Low	High	Low	High
Security	Low	High	High	Low	High
Cost	Low	High	High	High	Low

사용성은 알고리즘이 적용된 시스템이 얼마나 사용하기 편리한가에 대한 평가이다. OTP의 경우 토큰을 생성하는 서버와의 동기화 문제, 분실위험성으로 인하여 사용성이 낮다. 제안 알고리즘은 동기화 문제나 소지의 문제를 해결할 수 있으며, 사용자가 이용에 있어서 특별한 작업을 진행해야 하는 것이 아니기 때문에 사용성이 높다고 평가할 수 있다. 지식기반의 아이디, 비밀번호 인증, 지문인증은 정적인 요소를 이용하여 인증을 진행한다. 하지만 제안 알고리즘은 OTP, AP 기반의 인증처럼 인증에 필요한 요소들을 동적으로 변경이 가능하다. 제안 알고리즘은 인증요소가 노출되더라도 어떤 인증요소를 이용하여 암호화를 진행하였는지에 대한 유추가 불가능하여 공격위험에 대한 위험성은 낮고, 보안성은 높다고 평가할 수 있다. 제안 알고리즘은 사용자가 항시 휴대하고 있는 모바일 기기를 이용하여 인증을 진행하기 때문에 휴대성이 높다고 할 수 있다. 비용에 있어서 제안 알고리즘은 별도의 인프라를 구축하지 않아도 되며, 특별한 정보 수집용 기기가 필요 없기 때문에 낮다고 평가할 수 있다.

Ⅴ. 결 론

모바일 기기가 다양해지고 모바일 기기를 이용한 인증 기술에 대한 방법들이 다양해짐에 따라서 사용자는 오히려 개인정보보호를 위한 노력을 소홀히 하여 개인정보노출의 위험이 증가하는 문제가 발생하고 있

다. 본 논문에서는 기존에 제시되던 인증방식의 문제점을 해결하기 위해서 자동식별 및 데이터 수집기술을 이용한다. 모바일 기기를 이용하여 식별 가능한 정보와 모바일 기기에서 자동으로 수집할 수 있는 고유한 특성 정보를 바탕으로 암호화를 진행하는 모바일 기기에 적합한 인증 알고리즘 및 시스템을 제안하였다. 제안한 시스템은 별도의 인프라 구축이 필요 없이 기존에 구축된 인프라를 이용하며, 항상 휴대하고 있는 모바일 기기의 정보를 이용하므로 소지의 불편함 없이 개인정보를 안전하게 보호할 수 있는 장점이 있다. 또한 인증을 위한 인증요소 및 보안키가 타인에게 노출될 염려가 적으며 노출되더라도 어떤 정보를 사용해서 보안키를 생성하였는지 알 수 있는 방법이 없으므로 높은 안정성과 공격에 대한 침해가 낮은 인증 방법으로 평가할 수 있다.

향후 연구과제로는 모바일 기기에서 수집된 정보를 기반으로 타인의 인증을 함께 진행하는 공동인증시스템에 대한 연구로 확장하여 회사, 병원, 학교 등 개인정보에 대한 접근이 공동으로 이루어지는 장소에 알맞은 인증 시스템을 연구할 계획이며, 정량적인 평가를 통해 효용성을 입증할 계획이다.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A1B03030759)

REFERENCES

[1] S. J. Oh, “A Cross-cultural Study on the Perception Types of Korean and American Users of Smartphone,” *Journal of the Korean society for Wellness*, vol. 11, no. 3, pp. 1-21, Aug. 2016.

[2] S. R. Cho, D. S. Choi, S. H. Jin, and H. H. Lee, “Passwordless Authentication Technology-FIDO,” *Electronics and Telecommunications Trends*, vol. 29, no. 4, pp. 101-109, Aug. 2014.

[3] S. J. Kim, “Information Security Plan on Cloud Computing - Information Security Management System,” *Korean Review of Management Consulting*, vol. 1, no. 2, pp. 194-208, Aug. 2010.

[4] F. Zhang, A. Kondoro, and S. Muftic, “Location-Based Authentication and Authorization Using Smart Phones,” *2012 IEEE 11th International Conference on Trust, Security, and Policy in Computing and Communications*, pp. 1285-1292, June 2012.

[5] H. Takamizawa, and N. Tanaka, “Authentication system using location information on ipad or smartphone” *International Journal of Computer Theory and Engineering*, vol. 4, no. 2, pp.153-157, April 2012.

[6] W. Jansen, and V. Korolev, “A location-based mechanism for mobile device security,” *Computer Science and Information Engineering, 2009 WRI World Congress on IEEE*, vol. 1, pp. 99-104, March 2009.

[7] H. Ketabdar, K. A. Yuksel, A. Jahnbekarn, M. Roshandel, and D. Skirop, “MagiSign: User Identification /Authentication Based on 3D Around Device Magnetic Signatures,” *The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pp. 31-34, 2010.

[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] 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.

[10] T. K. Lee, Y. H. Kim, and E. G. Im, “Biometric User Authentication Method of Mobile Appilication in Trustable Space,” *Journal of The Korea Institute of Information Security and Cryptology*, vol. 27, no. 2, pp. 201-212, April 2017.

정필성(Pil-Seong Jeong)

2004년 2월 : 서울과학기술대학교 전자공학과(공학사)
2007년 8월 : 광운대학교 전자통신공학과(공학석사)
2013년 8월 : 광운대학교 전자통신공학과(공학박사)
2016년 6월 ~ 현재 : 제이앤피솔루션 기술이사
※관심분야 : 사물인터넷, WSN, 임베디드 시스템

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