Journal of the Korea Convergence Society
Vol. 10. No. 7, pp. 7-14, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.7.007

임베디드 기기를 활용한 다중 방식 인증 시스템

정필성[1], 조양현[2*]
[1]명지전문대학 정보통신공학과 조교수, [2]삼육대학교 컴퓨터·메카트로닉스공학부 교수

Multiple Method Authentication System Using Embedded Device

Pil-Seong Jeong[1], Yang-Hyun Cho[2*]
[1]Professor, Dept. of Information Technology Communication, Myongji College
[2]Professor, Division of Computer & Mechatronics Engineering, Sahmyook University

요 약 스마트폰을 이용하는 사용자는 인증이 필요한 시스템에 접근 권한을 획득하기 위해서 지식기반 인증, 소유기반 인증, 생체기반 인증, 토큰기반 인증 등을 이용하여 인증을 진행한다. 하지만 데스크탑 컴퓨터 사용자는 다양한 인증 방식이 있음에도 불구하고 인증 기기의 제한으로 지식기반 인증 요소인 아이디와 비밀번호를 이용하여 인증하는 방식을 주로 사용하고 있다. 본 논문에서는 사용자가 원하는 방식의 인증 방식을 사용할 수 있는 기능을 제공하는 라즈베리 파이 기반의 다중 방식 인증 시스템을 설계하고 구현하였다. 구현 시스템은 지식기반 인증, 소지기반 인증, 생체기반 인증, 토큰기반 인증 방식을 사용한다. 제안 시스템을 이용하면 경제적인 부담 때문에 별도의 보안 담당자를 두기 어려운 중소기업에서 활용이 가능한 보안 기능을 제공할 수 있다. 구현된 시스템은 개인용뿐만 아니라 기업에서도 사용 가능하며, 금융, 게임 등 다양한 분야에 적용할 수 있다.

주제어 : 사용자 인증, 인증 시스템, 정보보호, 라즈베리 파이, 임베디드 시스템

Abstract Users who use smartphone can using knowledge-based authentication, possession-based authentication, biometric-based authentication, and token-based authentication in order to access rights to systems requiring authentication. However, desktop computer users use method only ID and password, which are knowledge-based authentication factors, due to limitations of authentication devices, despite various authentication methods. In this paper, we designed and implemented a raspberry pi based authentication system that provides multiple authentication method of a user's desired type. The implementation system uses knowledge-based authentication, possessive-based authentication, biometric-based authentication, and token-based authentication. The proposed system can provide a security function that can be used by SMEs, which is difficult to hire a security officer due to the economic burden. The implemented system can be used not only for personal use but also for enterprise, and it can be applied to various fields such as finance and game.

Key Words : User Authentication, Authentication System, Information Security, Raspberry Pi, Embedded System

*This study is supported by Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1A1B03030759)
*Corresponding Author : Yang-Hyun Cho(yhcho@syu.ac.kr)
Received May 13, 2019 Revised June 28, 2019
Accepted July 20, 2019 Published July 28, 2019

1. 서론

정보 기기의 보급화와 정보통신 기술의 발달은 사용자에게 더 많은 정보를 획득하고 정보의 활용 범위를 지역 네트워크에서 클라우드 환경으로 확대할 기회를 제공해 주고 있다. 지역 네트워크 및 클라우드 환경에서 정보를 획득하고 처리하기 위해서 우리는 사용자 인증이라는 절차를 통해 정보를 유통하고 처리한다. 특히 클라우드 서비스가 널리 활성화되어 있고, 클라우드 환경은 다양한 정보 기기와 네트워크 환경에서 접근하기가 쉬우므로 개인정보 유출에 관한 문제점이 많이 제기되고 있으며, 개인 인증 기술 및 정보보호를 위한 연구가 활발하게 논의되고 있다[1-5].

사용자 인증이란 지식기반 인증, 소유기반 인증, 생체기반 인증, 토큰기반 인증 등을 이용하여 사용자가 시스템에 접근 가능한지 여부를 확인하는 절차를 말한다. 인증 시스템은 이러한 인증요소를 이용하여 사용자에게 부여된 접근 권한을 확인할 수 있는 기능을 제공한다. 지식기반 인증이란 전통적인 인증 절차로서 아이디, 비밀번호와 같이 사용자의 지식에 의존하는 정보를 입력하여 사용자를 인증하는 방식이다. 하지만 아이디와 비밀번호는 훔쳐보기 또는 개인 정보를 바탕으로 유추하기 쉽기 때문에 지식기반 인증과 같은 1단계 인증 이후 일회용 비밀번호(One Time Password, OTP)를 통해 추가 인증 절차를 진행하는 토큰기반 인증도 함께 진행하는 하게 되는 경우도 있으며, 금융, 게임 등의 서비스에서 사용자 인증에 많이 활용하고 있다. 생체기반 인증은 개개인이 가진 고유한 생체적 특징인 지문, 홍체, 얼굴 등의 특징을 찾아서 기록된 정보와 비교하여 사용자를 인증하는 서비스로서 스마트폰과 같이 개인용 스마트 기기에서 많이 활용되고 있다[6-9].

스마트 기기의 경우 지식기반 인증, 소유기반 인증, 생체기반 인증, 토큰기반 인증 등의 다양한 인증 방식을 사용가능하도록 개발되어 있으며, 특히 개인용 기기에 특화되어 사용자는 화면 잠금을 해제하거나 결제할 때 생체기반 인증을 활용하는데 어려움이 없도록 개발되어 있다. 하지만 사용자가 모든 정보를 소비하는데 있어서 스마트폰만을 사용하는 것이 아니며, 사용자를 인증하고 권한을 확인하는 다양한 방법이 있음에도 불구하고 범용 컴퓨팅 기기에서는 개인 정보에 접근하기 위해서 아이디, 비밀번호를 입력하는 지식기반 인증 및 일회용 비밀번호를 활용하는 토큰기반 인증에 한정된 인증 서비스를 제공받고 있다. 편리한 정보 접근성을 제공하기 위해서 사용자는 본인이 원하는 방식의 인증 서비스를 받아야만 하며, 평소 자신이 사용하는 인증 방식을 통해 일관된 인증 서비스를 받을 수 있어야만 한다[10].

본 논문에서는 개인용 컴퓨터와 같은 범용 컴퓨팅 기기와 함께 연동하여 다양한 인증 서비스를 제공해줄 수 있도록 임베디드 기기를 활용한 다중 방식 인증 시스템을 제안한다. 사용자는 시리얼 방식 또는 TCP/IP 방식으로 연결한 임베디드 기기를 이용하여 인증을 적용함으로써 지식기반 인증방식과 함께 소유기반 인증, 생체기반 인증, 토큰기반 인증을 함께 진행할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 활용되는 임베디드 기기인 라즈베리 파이와 지식기반 인증, 생체기반 인증, 소유기반 인증, 토큰기반 인증에 관하여 알아본다. 3장에서는 제안 시스템 알고리즘을 알아보며 4장에서는 사용자 인증을 처리하는 시스템 구현에 대해서 알아본다. 5장에서는 효용성에 대해서 평가를 진행하며 마지막으로 6장에서는 결론을 맺는다.

Table 1. Raspberry Pi 3 B+ specifications

Items	Specifications
SoC	Broadcom BCM2837B0 SoC
CPU	1.4GHz ARM Cortex-A53 MP4
GPU	Broadcom VideoCore IV MP2 400 MHz
RAM	1 GB LPDDR2
Wired LAN	10/100/1000 Mbps Gigabit Ethernet
Wireless LAN	802.11b/g/n/ac Dual-Band
Bluetooth	Bluetooth 4.2
Video	HDMI(rev 1.3 & 1.4) DSI
GPIO	40pins
Etc	UART, I²C Bus, CSI, PoE

2. 관련 연구

2.1 라즈베리 파이

라즈베리 파이는 영국의 라즈베리 파이 재단에서 컴퓨팅 기기의 기초교육을 위해서 학교와 개발 도상 국가에서 활용 가능하도록 만든 신용카드 크기의 싱글 보드 컴퓨팅 기기이다. GPIO 핀이 존재하여 다양한 입출력 디바이스를 연결해서 사용할 수 있기 때문에 사물인터넷 환경을 구현하기가 용이하다. 라즈베리 파이는 윈도우10 IoT 코어와 같은 사물인터넷 기기 전용 운영체제가 탑재 가능하며, 공식적인 운영체제로는 데비안 기반의 라즈비

안을 지원하고 있다. Table 1은 본 논문에서 사용된 임베디드 기기인 라즈베리 파이 3 B+의 사양이다[11].

2.2 지식기반 인증

지식기반 인증은 사용자가 알고 있는 정보를 인증요소로 활용하는 방법이다. 대표적인 인증요소는 아이디, 이메일, 비밀번호, PIN(Personal Identification Number) 코드 등이 있다. 일반적으로 웹 사이트에서 사용자 맞춤형 정보를 제공받기 위해서 사용자를 인증하는 방법으로서 사용자만이 알고 있는 고유한 정보를 이용하여 인증에 사용하는 방식으로 온라인에서는 가장 널리 사용되는 인증 기술이다[12].

2.3 생체기반 인증

생체기반 인증이 사람마다 고유한 특징을 가지는 생체정보를 인증요소로 활용하는 인증방식이다. 생체기반 인증요소로 활용할 수 있는 정보로는 홍채, 지문, 얼굴 등이 있다. 생체기반 인증요소는 보안요소가 뛰어나지만 개인정보 유출 우려 때문에 개인용 기기인 스마트폰 등에서 활용되거나 외부유출에 대한 책임을 명확하게 명시한 조건에서만 사용 가능하다[13].

2.4 소유기반 인증

사용자가 소유하고 있는 고유한 정보나 도구를 이용하는 방식으로 RFID 기술을 이용한 스마트카드, 블루투스 기기, 초음파 통신기기 등 휴대가 간편하고 사용하기 쉽도록 고안되어 있는 인증 기기들이 존재한다. 특히 스마트카드의 경우 회사 출입문 보안 카드로 널리 사용되며, 최근에는 스마트폰에 내장되어 있는 NFC 모듈을 이용하여 대신하는 경우도 있다[14].

2.5 토큰기반 인증

토큰기반 인증은 사용자가 인증을 요청할 때마다 일시적으로 일화용 비밀번호를 발급하여 인증요소로 사용하는 OTP를 발급하는 OTP 발급기나, 공인인증서와 같은 온라인 신원인증서를 보관하는 용도로 활용하는 보안토큰(Hardware Security Module, HSM)을 이용한 토큰 관리 기반 인증방식이다. 보안성이 높지만 인증이 필요할 때마다 사용자가 실행해야 하며, 토큰을 관리하기 위한 별도의 단말기를 항상 소지해야 한다[15].

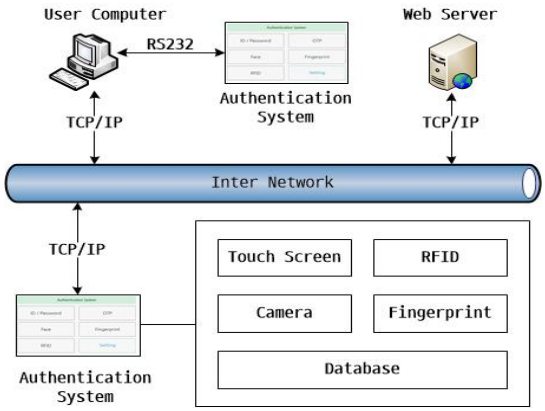

Fig. 1. Proposed system model

3. 제안 인증 시스템

3.1 제안 시스템 모델

제안하는 라즈베리 파이 기반의 다중 방식 인증 시스템 모델은 Fig. 1과 같다. 제안 시스템 모델은 사용자 인증 상태를 출력 및 기능 제어를 위한 터치스크린, 사용자가 입력한 아이디, 비밀번호를 이용하여 사용자 인증을 처리하는 지식기반 인증 모듈, 사용자의 얼굴 특징과 같은 생체 정보를 이용하여 사용자 인증을 처리하는 생체기반 인증 모듈, RFID(Radio Frequency Identification)와 같은 인증에 사용할 수 있는 고유한 소유물을 이용하여 사용자 인증을 처리하는 소유기반 인증 모듈, 일회용 비밀번호(One Time Password, OTP)를 이용하여 사용자 인증을 처리하는 토큰기반 인증 모듈, 인증 제어를 통합적으로 처리하는 라즈베리 파이 시스템으로 구성된다.

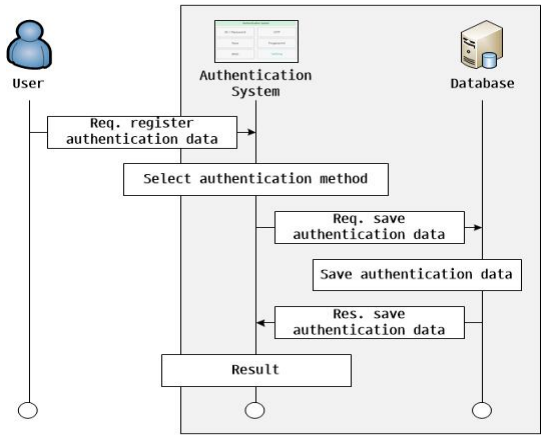

Fig. 2. User registration flow

3.2 사용자 인증 정보 등록

Fig. 2는 사용자 등록을 위한 절차를 나타낸다. 사용자 등록을 위하여 원하는 인증 형태를 선택하고 해당하는 인증 형태에 맞는 사용자 정보를 등록한다.

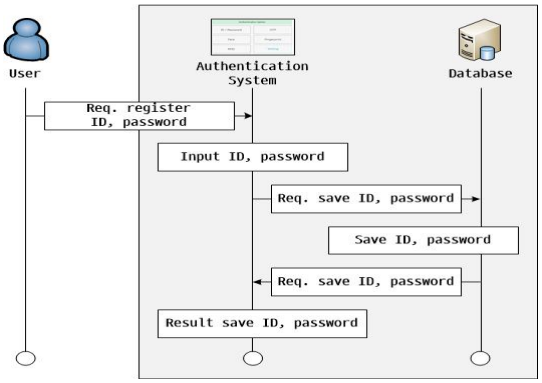

Fig. 3. User Identification, password registration flow

모든 과정에서의 데이터는 암호화하여 데이터베이스에 저장하여 보안기기를 의도적으로 탈취하더라도 데이터 추출이 불가능하도록 처리한다. 본 논문에서는 미국 국가안보국(National Security Agency, NSA)에서 설계한 SHA-2(Secure Hash Algorithm 2) 방식의 SHA 512 알고리즘을 적용한다. Fig. 3은 인증 시스템에서 사용자가 사용할 아이디, 비밀번호를 등록하는 과정을 나타낸다. 사용자는 보안기기의 설정 화면에서 직접 아이디와 비밀번호를 입력하여 사용자를 등록한다. 사용자 비밀번호의 경우 단방향 해시를 적용하여 저장한다.

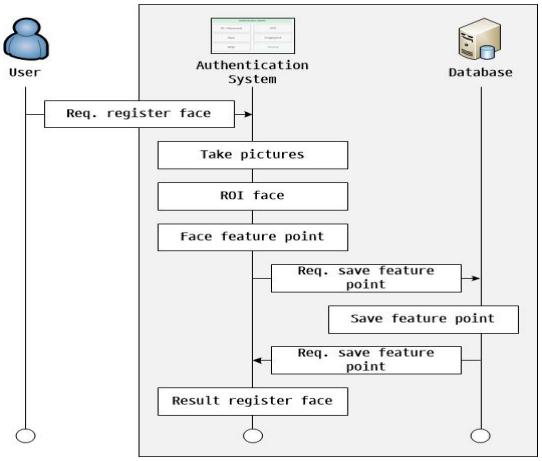

Fig. 4. User face registration flow

Fig. 4는 카메라를 이용하여 얼굴을 인증하기 위해 얼굴을 등록하는 과정을 나타낸다. 얼굴 특징기반 인증방식일 경우 카메라를 이용하여 여러 장의 얼굴 사진을 찍어 등록하는 방식을 진행한다. 얼굴 등록을 진행하기 위해서는 얼굴 검출, 얼굴 정렬, 얼굴 특징점 추출과정을 진행하며 추출된 특징점을 암호화하여 데이터베이스에 저장한다.

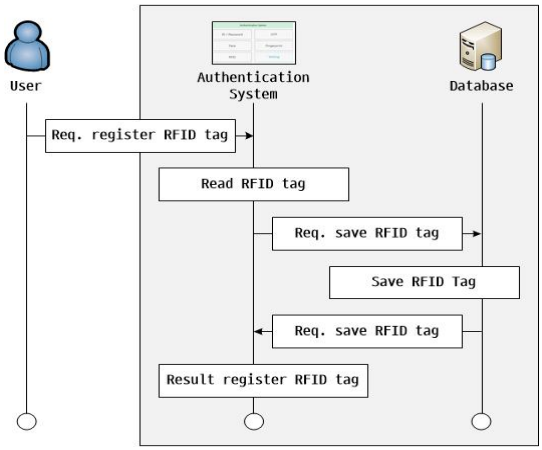

Fig. 5. RFID tag registration flow

Fig. 5는 소유기반 인증을 선택한 경우 RFID 리더에 RFID 태그를 인식시켜서 사용자를 등록한다.

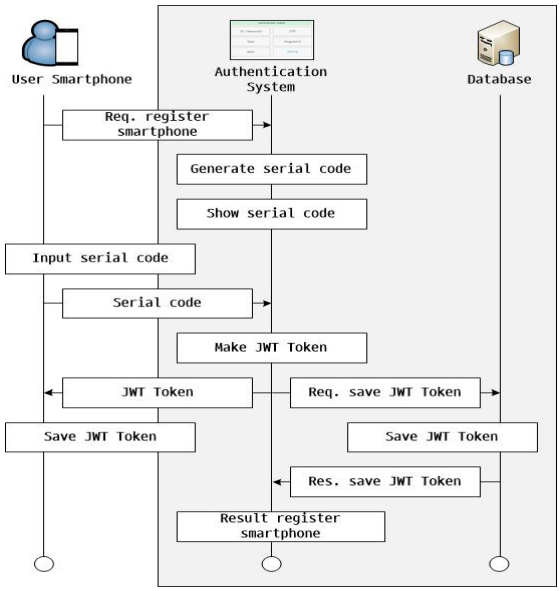

Fig. 6. Smartphone registration flow

Fig. 6은 OTP 코드를 이용하기 위해서는 사용자 스마트폰을 등록하는 과정이다. 보안 기기 터치스크린에 보여지는 시리얼 코드를 사용자 스마트폰 애플리케이션을 이용해서 입력하면 보안 기기에서 JWT 토큰을 생성하여 사용자 스마트폰을 등록한다.

3.3 사용자 인증

Fig. 7은 사용자 인증 과정을 나타낸다. 본 논문에서는 파일 서버를 사용자 인증이 필요한 서버로 정의하였다. 사용자는 원하는 형태의 인증을 선택하고 해당 인증 형태에 맞는 인증요소를 사용하여 인증 절차를 진행한다.

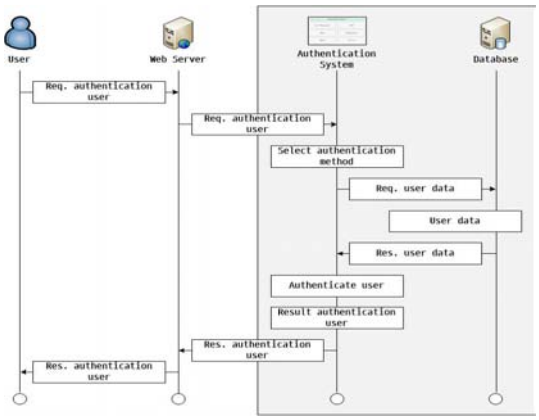

Fig. 7. Possession based authentication method

4. 제안 시스템 구현

제안 다중 방식 인증 시스템을 구현하기 위해서 라즈베리 파이 3 B+를 사용하였다. Fig. 8은 인증요소 수집을 위한 주변 장치들을 라즈베리 파이에 연결하여 시스템을 구성한 사진이다.

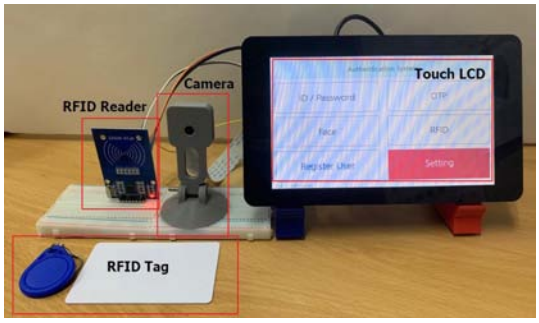

Fig. 8. Proposed system

Table 2는 제안 시스템을 구성하기 위해 사용된 기기와 모듈을 대한 설명이다.

Table 2. Proposed system specifications

Embedded System	Raspberry Pi 3 B+
Touch Screen	7 inch Official Touch Screen
RFID Module	RC522 Chip, 13.56MHz
RFID Tag	ISO14443A 13.56MHz
Camera	PiCamera v2.1

지식기반 인증은 웹 서버를 연동하여 키오스크 형태로 구현하였으며, 인증을 원할 때 터치스크린을 이용하여 아이디와 비밀번호를 입력한다.

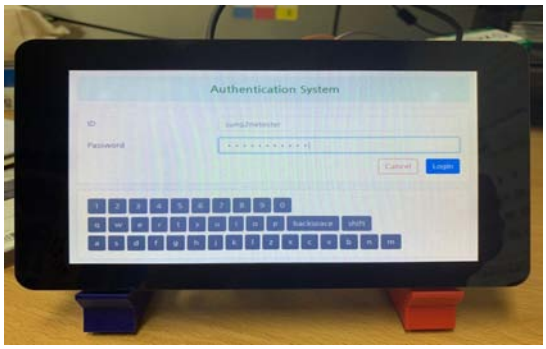

Fig. 9. User authentication using Identification, password

Fig. 9는 사용자가 아이디와 비밀번호를 입력하여 인증을 진행하는 화면이다. 기존 아이디, 비밀번호를 이용한 사용자 등록 방식과는 다르게 보안 기기의 터치스크린을 이용하여 사용자를 등록한다.

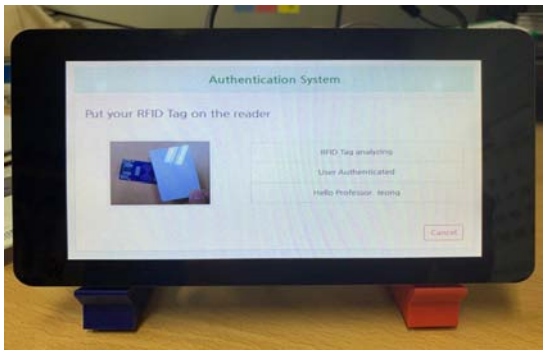

Fig. 10. User authentication using RFID

RFID 기술을 이용한 소유기반 인증요소를 활용하기 위해서 라즈베리 파이 GPIO 핀에 RFID 리더를 연결하여 사용하였다. Fig. 10은 RFID를 이용하여 인증을 진행하는 화면이다.

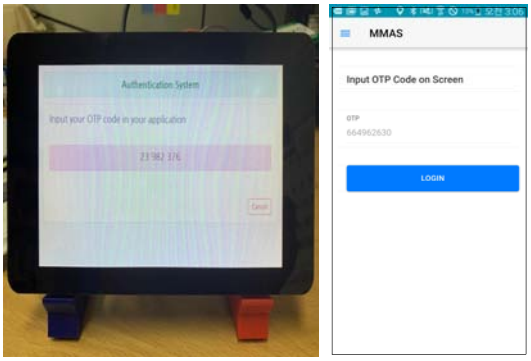

Fig. 11. User authentication using OTP

OTP 토큰을 발행할 때는 사용자의 스마트폰에 푸쉬 메시지 형태로 토큰을 발행하고 터치스크린을 이용하여 입력하도록 처리하였다. Fig. 11은 OTP를 이용하여 인증을 진행하는 화면이다.

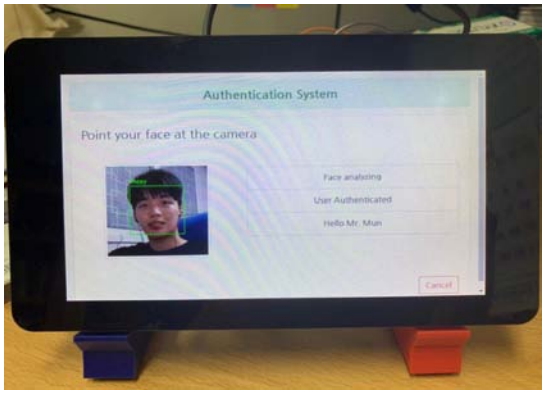

Fig. 12. User authentication using face

생체기반 인증 방식에서는 라즈베리 파이에 연결된 카메라를 이용하여 사용자의 얼굴을 인식하고 인증을 처리하는 방식으로 진행하였다. 얼굴 인식을 위해서는 얼굴 검출, 얼굴 정렬, 얼굴 특징점 추출과정을 진행하며 추출된 특징점을 암호화하여 데이터베이스에 저장한다. 사용자 인증을 위해서는 추출한 특징점과 카메라에서 인식한 얼굴의 추출점을 비교하여 유사도를 검증한다.

본 논문에서는 dlib 라이브러리의 얼굴 특징점 비교 알고리즘(state-of-the-art face recognition)을 이용하였다. 사용한 알고리즘은 Labeled Face in the Wild 에서 제공하는 사진을 이용한 성능평가에서 99.38%의 성능을 보여준다.[16]. Fig.12 는 카메라를 이용한 얼굴 인식 인증을 진행하는 화면이다.

5. 제안 시스템 효용성 평가

한국인터넷진흥원에서는 사용자 인증 기술에 대한 평가를 위한 적합성 기준으로서 유일성, 보편성을 기준으로 제시하고 있다. 사용자 인증을 위한 시스템을 평가하기 위해서는 시스템을 통해 인증을 진행하기 위한 환경에 대한 경제성과 법적 타당성(서비스의 명확성)에 대한 논의가 필요하며 사용자에게는 대체수단의 신뢰도를 기반으로 범용성에 대한 논의가 이루어져야 한다. 본 장에서는 편의성, 보안성, 적용성을 기준으로 제안 시스템의 효용성에 대해서 평가한다. Table 3은 데스크탑 PC와 인증 방식 지원에 대한 여부를 객관적으로 분석하여 제시한 내용이다.

Table 3. Authentication System Comparison

	PC	Proposed
ID, Password	Applicable	Applicable
RFID	Partial applicable	Applicable
Camera	Applicable	Applicable
OTP	Partial applicable	Applicable

Table 4는 기존 시스템과의 장점을 객관적으로 분석하여 제시한 내용이다.

Table 4. Authentication System Comparison

	PC	Proposed
Usability	Low	High
Attack	Low	High
Portable	Low	High
Security	Dynamic	High
Cost	Low	High

5.1 편의성

편의성은 소지가 간편하고, 배치 등이 편리한가를 말한다. 제안 시스템은 신용카드 크기의 라즈베리 파이와 카메라가 내장된 7인치 터치 LCD, 신용카드 절반 크기

의 RFID 리더를 연결하여 작은 크기로 구성되어 있기 때문에 휴대가 용이하고 네트워크 및 EIA-232D 시리얼 통신을 통해 언제 어디서나 쉽게 인증을 원하는 시스템과 연동이 편리하도록 구현되어 있다.

5.2 적용성

적용성이란 경제적인 비용에 대한 부담이 없으며, 기존 인프라를 활용 가능하며, 다양한 환경에 적용이 가능한지를 말한다. 제안 시스템은 기존 보안 시스템에 비해서 저렴한 비용(10만원 내외)으로 시스템 구현이 가능하며, 스마트폰에서 활용 가능한 대부분의 인증 기술 구현이 가능하기 때문에 사용자는 인증 시스템 사용에 어려움이 없다. 제안 시스템은 사용자 인증 시스템뿐만 아니라 기존에 배치된 출결시스템, POS와 함께 연동하여 결제 시스템으로 확장이 가능하여 쉽게 인증이 이루어질 수 있는 기술로 평가할 수 있다.

5.3 보안성

보안성은 지속적으로 변화하는 해킹 기술에 대한 대응력을 말한다. 제안 시스템은 사용자의 인증을 위한 정보를 취급하고 있지만, 인증에 필요한 최소한의 정보인 암호화되어 있는 해시값만을 보유하고 있기 때문에 사용자의 관리 소홀로 인한 분실사태가 발생하더라도 내부적인 데이터 유출 및 개인 정보 유출에 대한 문제를 야기시키지 않는다.

6. 결론

정보 기술의 발달과 스마트폰의 보급화 덕분에 우리는 스마트폰을 이용해서 사용자를 인증할 때 다양한 인증방식을 선택해서 사용할 수 있게 되었다. 특히, 금융 서비스와 클라우드 서비스를 위해 사용자를 인증하는 경우 지식기반 인증, 소유기반 인증, 생체기반 인증, 토큰기반 인증 등 다양한 방식을 지원하고 있다. 하지만 데스크탑 컴퓨터를 이용하여 사용자를 인증함에 있어서 스마트폰 만큼 자유로운 사용자 인증 방식 선택이 어렵고 제한적인 인증 서비스만을 제공받고 있다.

본 논문에서는 소형 임베디드 기기인 라즈베리 파이를 이용하여 사용자가 아이디, 비밀번호를 입력하는 인증방식 외에 스마트폰에서 제공받는 인증 서비스를 제공받을 수 있도록 다중 방식 인증 시스템을 구현하였다. 본 연구를 토대로 다양화되는 인증 서비스를 사용자에게 제공할 수 있으며, 경제적인 부담 때문에 별도의 보안 담당자를 두기 어려운 중소기업에서 활용이 가능한 보안 시스템을 구성할 수 있다. 제안 인증 시스템은 사용 범위의 제한이 없기 때문에 금융, 게임 등의 다양한 분야에서 활용이 가능한 것으로 평가된다. 향후 본 연구를 기반으로한 사내 보안문서 접근 권한 관리를 위한 인증 서비스에 적용하여 연구를 확장할 계획이다.

REFERENCES

[1] J. W. Jung, J. D. Kim, M. G. Song & C. G. Jin. (2015). A study on Development of Certification Schemes for Cloud Security, *The Journal of digital policy & management, 13(8),* 43-49.
DOI: 10.14400/JDC.2015.13.8.43

[2] S. H. Hong. (2012). New Authentication Methods based on User's Behavior Big Data Analysis on Cloud, *Journal of Convergence for Information Technology, 2(2),* 35-41.
DOI: 10.22156/CS4SMB.2016.6.4.031

[3] M. K. Choi, T. C. Kwan & D. H. Lee. (2013). Analysis of Security Vulnerability in Home Trading System, and its Countermeasure using Cell phone, *Journal of The Korea Institute of Information Security and Cryptology, 23(1),* 19-32.
DOI: 10.13089/jkiisc.2013.23.1.019

[4] S. J. Kim. (2010). Information Security Plan on Cloud Computing - Information Security Management System, *Korean Review of Management Consulting, 1(2),* 194- 208.

[5] H. T. Chae & S. J. Lee. (2014). Security Policy Proposals through PC Security Solution Log Analysis - Prevention Leakage of Personal Information, *Journal of the Korea Institute of Information Security & Cryptology, 24(5),* 961-968.
DOI: 10.13089/jkiisc.2014.24.5.961

[6] D. R. Kim. (2015). A Study on the OTP Generation Algorithm for User Authentication, *The Journal of digital policy & management, 13(1),* 283-288.
DOI: 10.14400/JDC.2015.13.1.283

[7] S. H. Lee. (2014). User Authentication Using Biometrics and OTP in Mobile Device, *Journal of Convergence for Information Technology, 4(3),* 85-90.

[8] T. K. Lee, Y. H. Kim & E. G. Im. (2017). Biometric User Authentication Method of Mobile Appilication in Trustable Space, *Journal of The Korea Institute of Information Security and Cryptology, 27(2),* 201-212.
DOI: 10.13089/jkiisc.2017.27.2.201

[9] J. S. Kim, S. J. Lee, B. S. Kim & S. W. Lee. (2015). Standardization trend of non-face authentication

technology based on telebio recognition, *Journal of The Korea Institute of Information Security and Cryptology, 25(4)*, 43-50.

[10] Y. J. Lee, Y. E. Ku & T. K. Kwon. (2019). A Study of User Perception on Features Used in Behavior-Based Authentication, *Journal of the Korea Institute of Information Security & Cryptology, 29(1)*, 127-137.

[11] Raspberry Pi Foundation. (2019). *Raspberry Pi. Raspberry Pi* [Online]. https://www.raspberrypi.org

[12] Y. J. Shin. (2017). A Study on the Personal Information Protection for Improvement of Personal Identification - Focusing on the Alternative Means of Resident Number for Users, *Journal of Korean Associastion for Regional Information Society, 20(2)*, 1-24.

[13] S. H. Yun. (2016). The Biometric Authentication based Dynamic Group Signature Scheme, *Journal of the Korea Convergence Society, 7(1)*, 49-55.
DOI: 10.15207/jkcs.2016.7.1.049

[14] M. G. Lee, Do. W. Kim & J. S. Shon. (2012). Active Authentication Method using NFC, *The Journal of Korean Institute of Communications and Information Sciences, 37(2)*, 140-156.

[15] C. O. Kang, J. J. Won, S. J. Park & J. C. Ryou. (2013). Efficient File System Level Encryption Mechanism Using HSM, *Journal of the Korea Institute of Information Security and Cryptology, 23(5)*, 849-858.
DOI: 10.13089/jkiisc.2013.23.5.849

[16] S. Balaban. (2015). Deep learning and face recognition: the state of the art, *Biometric and Surveillance Technology for Human and Activity Identification XII*, 1-9
DOI: 10.1117/12.2181526

정 필 성(Pil-Seong Jeong) [정회원]

· 2004년 2월 : 서울과학기술대학교 전자공학과(공학사)
· 2007년 8월 : 광운대학교 전자통신공학과(공학석사)
· 2013년 8월 : 광운대학교 전자통신공학과(공학박사)
· 2018년 3월 ~ 현재 : 명지전문대학 정보통신공학과 조교수
· 관심분야 : 사물인터넷, WSN, 임베디드 시스템
· E-Mail : ibetter.kr@gmail.com

조 양 현(Yang-Hyun Cho) [정회원]

· 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 컴퓨터·메카트로닉스공학부 교수
· 관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
· E-Mail : yhcho@syu.ac.kr