JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 7 : 1393~1400 Jul. 2017

모바일 환경에서 상호 협력 기반 스마트폰 사용자 인증 알고리즘

정필성[1] · 조양현[2*]

Smartphone User Authentication Algorithm based on Mutual Cooperation in Mobile Environment

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

스마트폰 이용자가 증가함에 따라서 개인정보 보호에 대한 취약점이 증가하고 있다. 개인의 정보를 인터넷에 연결된 여러 서버에 저장하고 동일한 아이디와 비밀번호를 이용하여 인증하는 경우가 많기 때문이다. 전통적인 인증 방식을 해결하기 위해 OTP, FIDO, PIN 코드 등의 인증 방식이 도입되었지만 타 사용자와의 공유가 필요한 인증에는 사용이 제한적이다. 본 논문에서는 병원, 기업과 같이 공용으로 정보를 관리하는 곳에서 필요로 하는 인증방식을 제안하였다. 제안한 알고리즘은 스마트폰 IMEI, QR 코드, BLE, 푸쉬 메시지를 이용하여 같은 장소에 있는 사용자끼리 실시간으로 인증을 진행할 수 있는 알고리즘이다. 스마트폰을 이용하여 상호 협력을 통하여 사용자 인증을 진행할 수 있고, 실시간 인증 취소가 가능한 인증 알고리즘을 제안하고 상호 협력 인증 시스템을 설계 및 구현하였다.

ABSTRACT

As the number of smartphone users increases, vulnerability to privacy protection is increasing. This is because personal information is stored on various servers connected to the Internet and the user is authenticated using the same ID and password. Authentication methods such as OTP, FIDO, and PIN codes have been introduced to solve traditional authentication methods, but their use is limited for authentication that requires sharing with other users. In this paper, we propose the authentication method that is needed for the management of shared information such as hospitals and corporations. The proposed algorithm is an algorithm that can authenticate users in the same place in real time using smart phone IMEI, QR code, BLE, push message. We propose an authentication algorithm that can perform user authentication through mutual cooperation using a smart phone and can cancel realtime authentication. And we designed and implemented a mutual authentication system using proposed algorithm.

키워드 : 보안, 상호 협력, 스마트폰, 인증, 정보보호

Key word : Certification, Information Security, Mutual Cooperation, Security, Smartphone

Received 21 March 2017, **Revised** 24 March 2017, **Accepted** 28 March 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 https://doi.org/10.6109/jkiice.2017.21.7.1393 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

전 세계적으로 스마트폰 이용자수가 증가하고 있으며 Pew Research Center의 발표에 따르면 2015년 3월 기준으로 대한민국은 UAE(90.8%), 싱가포르(87.7%), 사우디 아라비아(86.1%)에 이어 83.0%의 보급률로 4위를 기록하고 있으며, 성인인구 40,879,472명 중 33,929,961명이 스마트폰을 사용하고 있다[1,2].

스마트폰 사용자가 증가함에 따라서 모바일 환경에서 쉽고 편하게 개인 정보에 접근할 수 있게 되었지만 개인정보에 대한 보안이 취약하게 만든 문제점이 발생되었다. 쉽게 편한 인터넷 서비스 가입 및 접근으로 인하여 다양한 서버에 개인정보가 분산되어 저장되어 있으며, 필요할 때 언제나 인터넷에 접근 가능한 환경이 유지되고 있으며, 개인이 여러 개의 인터넷이 가능한 디바이스를 가지고 있는 경우가 많기 때문에 더 많은 정보를 인터넷에 연결된 서버에 저장하고 있다. 또한 대부분의 웹 서비스에 동일한 아이디와 비밀번호를 이용하여 사용자 인증을 하고 있는 경우가 많아 하나의 디바이스가 분실 또는 타 사용자에게 노출되면 많은 정보가 유출되는 사태가 발생할 가능성이 있다[3,4].

전통적인 방식의 인증 방식인 아이디와 비밀번호를 사용하여 인증을 진행하는데서 발생하는 문제점을 해결하고자 비밀번호와 다른 인증요소를 결합하는 형태인 OTP(One Time Password), 공인인증서, 보안카드, NFC 등의 인증 방식을 지원하거나 비밀번호를 사용하지 않고 사용자를 인증하는 FIDO(Fast IDentity Online) 기술 기반의 지문인식, 홍체인식, PIN 코드 인증 등의 다양한 인증 방식이 사용되고 있다[5].

하지만 이러한 인증 방식은 타 사용자와의 공유가 필요한 인증에는 적용이 제한적이며, 특히 병원 또는 기업과 같이 공통체가 협의에 의해서 공용으로 정보를 관리하는 곳에는 그 사용이 바람직하지 않거나 적용이 어려운 경우가 많다. 기업에서는 정보보호를 위해 많은 시간을 할애하고 있지만 여전히 많은 개인 및 사내 정보유출 사례가 있으며, 심지어는 정보에 접근 가능한 권한을 가진 임직원이 퇴사하면서 경쟁사에 정보를 넘겨주는 형태의 산업기밀 유출 사례도 있다. 또한 병원에서는 수평화된 접근 권한을 가진 의료정보 시스템을 이용하여 의사들이 본인의 담당 환자의 정보 이외에도 다른 환자의 정보에 쉽게 접근 가능하며 의료자격이 없는 사무장이 개인정보를 검색하고 유출 또는 삭제가 가능한 심각한 문제점이 존재하고 있다[6,7].

본 논문에서는 개인의 정보 및 기업 정보에 대한 접근 권한에 대한 문제점을 해결하고 개인 또는 다수의 인증을 통해 정보에 접근 가능한 인증이 이루어질 수 있는 모바일 환경에서 스마트폰을 이용하여 상호 협력을 통한 사용자 인증을 진행할 수 있는 인증 시스템을 제안한다. 제안한 시스템에서 사용된 인증 매커니즘은 상호 신뢰를 요구하는 정보에 접근하기 위한 사용자가 인증을 시도할 때 등록된 다른 사용자가 인증을 함께 진행하며 BLE(Bluetooth Low Energy)와 QR 코드를 이용하여 실시간으로 인증 상황을 확인한다. 또한 원할 때는 언제든지 실시간으로 인증을 취소할 수 있는 장점이 있기 때문에 병원의 환자정보, 기업의 비밀정보와 같이 민감한 정보에 접근할 때 스마트폰을 이용하여 쉽고 빠르게 강화된 보안 인증 방식으로 적용할 수 있다는 특징이 있다.

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

Ⅱ. 관련 연구

본장에서는 제안한 모바일 환경에서 스마트폰을 이용하여 상호 협력을 통한 사용자 인증을 진행할 수 있는 인증 매커니즘을 설계 및 구현하는데 필요한 관련 연구에 대해서 설명한다.

2.1. BLE

블루투스 기술은 1998년 Ericsson, Nokia, Tosiba, IBM, Intel 등이 참여한 SIG(Special Interest Group)에 의해 개발되었으며 2010년 6월 30일 기존의 블루투스 Basic Rate(BR) 및 Enhanced data Rate(EDR)보다 전력 소모량을 극소화한 저전력 에너지 기술을 도입하고 이를 포함하는 새로운 표준인 블루투스 4.0을 발표하였다. 표 1은 기존의 블루투스 BR/EDR과 BLE의 특징을 보여준다[8]. BLE는 기존 방식에 비해서 초저전력 대기 상태, 간편한 기기 검색, 다양한 장비로의 데이터 전송, 보안 저전력 전송, 통신거리의 증가, 낮은 duty

cycle 등의 특징들을 가진다. 로우 펄싱(Low Pulsing) 기술을 이용하여 기기 간 연결 유지에 필요한 전력 소모를 줄이는 것이 가능하여 배터리 교환 없이 장기간 사용하는 것이 가능하다. 스타-버스(Star-bus) 토폴로지를 지원하여 다수의 디바이스끼리 통신이 가능하기 때문에 사물인터넷(Internet Of Things) 환경에 적합한 기술로서 평가된다.

Table. 1 Bluetooth BR/EDR and BLE characteristic comparison

Technology	Bluetooth BR/EDR	BLE
Radio Frequency	2.4GHz	2.4GHz
Range	10 to 100 meters	10 to 100+ meters
Power consumption	15-20mW	1.5-2mW
Latency	100ms	< 3ms
Network topology	Scatternet	Start-bus
Nodes/Active Slaves	7 / 16777184	unlimited

BLE 디바이스는 기본적으로 Advertise 방식을 지원하며 특정 디바이스를 지정하지 않고 주변의 모든 디바이스에게 Non-Connectable Adversing Packet을 일정주기로 전송하는 Advertiser와 Non-Connectable Adversing Packet을 감지하기 위해 주기적으로 스캔하는 디바이스인 Observer로 역할로 구분된다. Advertise 방식은 한 번에 한 개 이상의 디바이스와 통신할 수 있는 방법으로 디바이스가 자신의 존재를 알리거나 31Bytes 이하의 적은 양의 데이터를 보낼 때도 사용된다. 또한 전송할 수 있는 데이터 크기 제한을 보완하기 위해 Scan Request, Scan Response을 이용해서 추가적인 데이터를 주고받을 수 있다.

2.2. QR 코드

QR 코드(Quick Response Code)는 1994년에 일본의 덴소 웨이브(Denso Wave)사에서 개발한 2차원 매트릭스 형태의 바코드로서 빠른 반응(Quick Response)를 위해 기존의 선으로 나열된 1차원 바코드를 격자무늬 정사각형으로 표현한 것이 특징이다. 1차원 바코드는 막대선의 굵기로 정표를 표현하여 20자 내외의 숫자를 표현할 수 있는 것에 반해 QR 코드는 가로, 세로 두 방향으로 정보를 표현하여 한글, 한자, 영자, 숫자 등 다양한 정보를 표현할 수 있으며 최대 2,953바이트 정보를 기록할 수 있다. QR 코드는 3곳의 Finder Pattern이 배치되어 있어 360도 어느 방향에서나 인식이 가능하다. QR 코드는 이미지와 로고를 활용하여 정보를 표현할 수 있는 것이 가능하여 홍보, 마케팅에 널리 활용되고 있다. 또한 생성과 읽기가 쉽기 때문에 다양한 기기에 활용되며, 특히 스마트폰의 카메라를 이용하여 정보를 공유할 때 유용하게 사용될 수 있다[9].

2.3. IMEI

IMEI (International Mobile station Equipment Identities)는 모바일 디바이스 제조사에서 부여하는 고유 코드로서 디바이스의 제조사, 모델, 국적, 단말기 일련번호 등의 정보가 포함된다. 따라서 동일한 종류의 모바일 디바이스라도 고유한 식별 코드를 가지게 되며 이를 이용하여 모바일 디바이스를 구분할 수 있다. 표 2는 IMEI의 구조와 형식을 보여준다[10].

Table. 2 IMEI Structure and Format

Division	Digit	explanation
TAC (Type Allocation Code)	AA(2)	IMEI Certification Authority Number
	BBBBCC(6)	Allocation code
Serial Number	DDDDDD(6)	Device Unique ID
Check Digit	E(1)	EIR registration verification Number

Ⅲ. 제안 사용자 인증 알고리즘

3.1. 네트워크 모델

그림 1은 제안한 사용자 인증 시스템이 운용되는 네트워크 모델을 나타낸다. 모바일 디바이스는 이동통신망 또는 무선 공유기를 이용하여 인증 서버와 상호 통신을 주고받는다. 인증 서버는 사용자의 인증 정보 및 각종 정보들을 안전하게 보관하고 있는 데이터베이스와 네트워크를 통해 연결되어 있다. 모바일 디바이스는 서버와 실시간으로 메시지를 주고받으며, 인증을 필요로 하거나 인증을 받기를 원하는 모바일 디바이스와는 블루투스를 이용하거나 인터넷에 연결된 인증 서버를 이용하여 실시간으로 메시지를 주고받는다. User1은 정보에 접근하기 위해 허가를 요청하는 사용자를 의미하며, User2는 근접된 위치에서 인증을 허가하는 사용자를 의미한다.

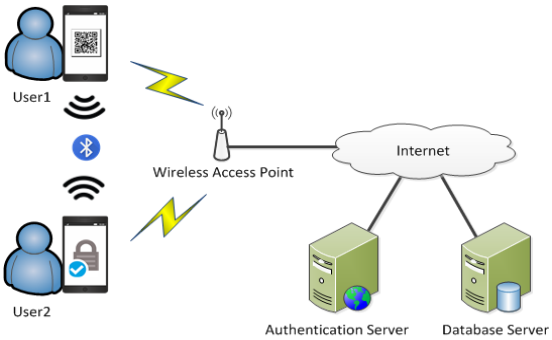

Fig. 1 Proposed Network Model

3.2. 사용자 등록

그림 2는 사용자 등록을 위한 절차를 나타낸다. 사용자는 등록 과정 중에 아이디와 비밀번호를 입력한다. 애플리케이션에서 아이디, IMEI를 이용하여 암호화된 비밀번호, 핸드폰번호를 함께 인증 서버로 전송하여 등록을 진행한다. IMEI와 핸드폰번호를 함께 전송하면 이미 등록된 사용자를 구별할 수 있으며, 인증 기기의 제한 조건을 줄 수 있다는 장점이 있다. 세부 동작은 다음과 같다.

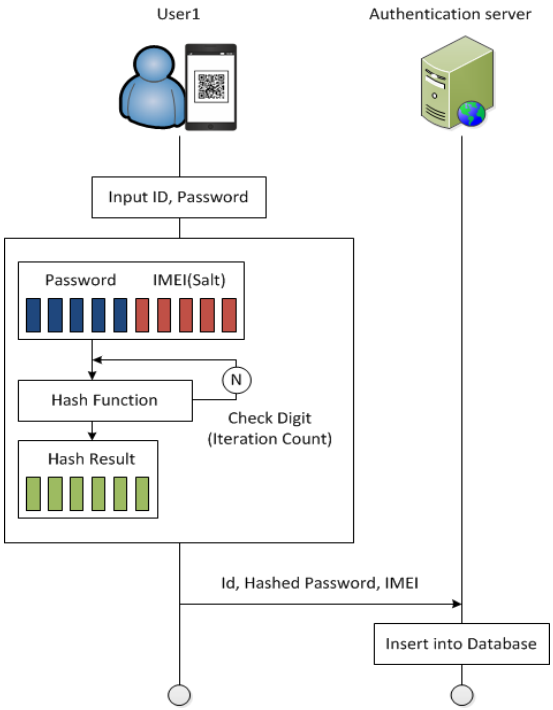

Fig. 2 User Registration Flow

① 사용자는 인증에 사용할 아이디와 비밀번호를 입력한다.

② 전송하기 전에 비밀번호를 IMEI를 SALT로 이용하여 단방향 해시 처리한다. 이때 체크 디지트를 반복 횟수로 지정하며, 체크 디지트가 0일 경우 10으로 처리한다.

③ 아이디, 해시 처리된 비밀번호, IMEI를 인증서버로 전송한다.

④ 인증서버에서 사용자 정보를 확인하여 등록되어 있지 않은 사용자면 데이터베이스 서버로 정보를 저장하여 등록을 마친다.

3.3. 사용자 로그인

본 논문에서 사용되는 인증 절차는 두 개의 인증 절차를 진행한다. 첫 번째 인증 절차는 사용자 로그인 인증 절차로서 접근하고자 하는 정보의 목록을 보거나 본인이 권한을 가지고 있는 정보에 접근하고자 할 때 사용하는 인증 절차이다. 기업이나 병원의 경우 개인의 정보 접근과는 다르게 타인의 정보를 보거나 협업을 해야 하는 경우가 많기 때문에 타인의 정보를 보기 위해서는 첫 번째 인증 절차 이외에 사용자 정보 접근 절차를 진행해야 한다. 그림 3은 사용자 로그인 인증 절차를 나타낸다. 세부 동작은 다음과 같다.

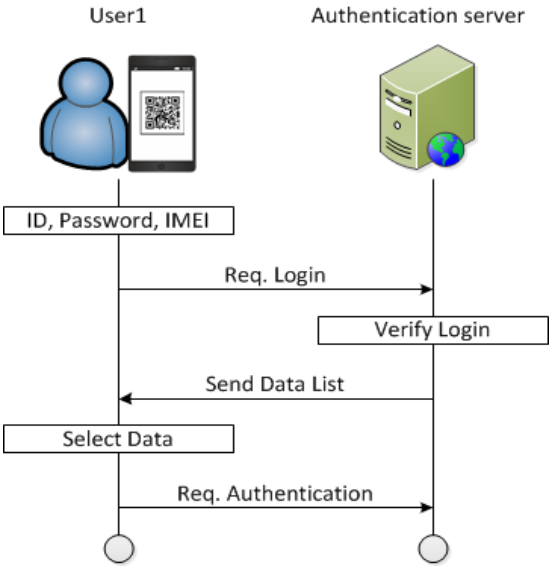

Fig. 3 User Login Flow

① 사용자는 아이디, 비밀번호, IMEI를 이용하여 서버로 로그인 한다. 사용자의 IMEI가 서버에 등록된 정보와 일치하지 않을 경우 로그인을 거부한다.
② 로그인 완료되면 사용자가 요청하는 데이터 리스트를 데이터베이스 서버로부터 받아서 전송한다.
③ 사용자는 데이터 리스트 중에서 본인이 접근하길 원하는 데이터의 인증을 시도하며, 인증 서버에서 해당 정보의 인증 권한을 가진 사람에게 이메일, SMS, 푸시 메시지를 이용하여 메시지를 전송한다.

3.4. 정보 접근 인증

그림 4는 인증 절차를 나타낸다. User1은 인증을 요청하는 사람의 모바일 디바이스이고 User2는 인증을 허가하는 사람의 모바일 디바이스이다. 세부 동작은 다음과 같다.

① User1은 접근하고자 하는 정보를 선택한다.
② 서버에서 User1에게 일회성 임의의 범용 고유 식별자인 UUID(Universally Unique IDentifier)를 생성하여 전송한다. User2에게는 이메일, SMS, 푸시 메시지를 이용하여 인증 요청이 왔음을 알리고 User1에게 전송한 UUID을 알려준다.
③ User1의 화면에 UUID 정보가 들어있는 QR 코드를 생성한다.
④ User2의 카메라를 이용하여 QR 코드를 스캔한 후 스캔된 UUID를 서버로 전송한다.

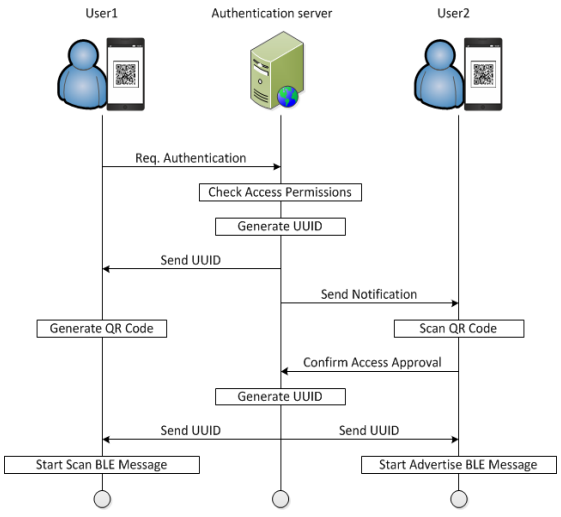

Fig. 4 Document Access Authorization Flow

⑤ 서버에서 User1에 전송한 UUID와 User2에서 받은 UUID가 일치하면 User1에 인증을 허가한다.
⑥ User1의 인증 허가 후 서버에서 새롭게 UUID를 생성하여 User1과 User2에 알린다. 새롭게 생성된 UUID는 인증 유지를 위해서 사용한다.
⑦ User2에서 블루투스를 이용하여 실시간으로 UUID 정보를 광고(Advertising)한다. User1은 User2와의 RSSI 신호를 확인하여 거리가 멀어지거나 신호가 끊어지면 자동으로 인증을 해지한다.
⑧ 만일 User2에서 인증 해지를 요청하면 서버에서 인증을 해지 한다.

Ⅳ. 제안 사용자 인증 시스템 구현

4.1. 시스템 구성

그림 5는 제안한 사용자 인증 시스템 구현을 위한 시스템 구성을 나타낸다. 시스템 구현을 위해 사용자 스마트폰, 인증 서버, 실시간 메시지 전송을 위한 Firebase를 이용하여 시스템을 구성하였다.

본 논문에서 구현된 사용자 인증 시스템은 제안한 알고리즘의 성능을 검증하기 위한 프로토타입으로서 인증서버만 구현하고 실시간 메시지 전송을 위한 서버는 별도로 구현하지 않고 Firebase 모바일 플랫폼을 이용하였다. Firebase 모바일 플랫폼은 서로 다른 플랫폼 간에 안정적인 메시지 교환을 위한 FCM(Firebase Cloud Messaging) 서비스를 지원하고 있으며 안드로이드, iOS 에 맞는 적절할 메시지를 실시간으로 전송할 수 있다는 특징을 이용하여 스마트폰과 인증 서버 간의 접근 인증 허가 메시지 교환을 위해 사용 하였다.

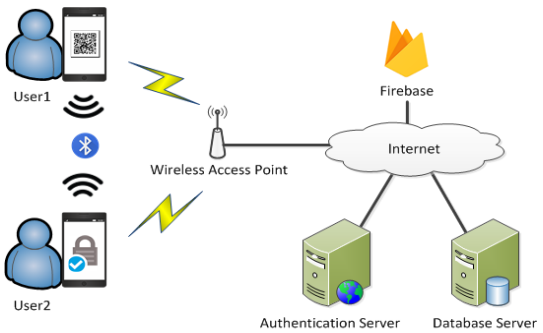

Fig. 5 System based on Proposed Algorithm

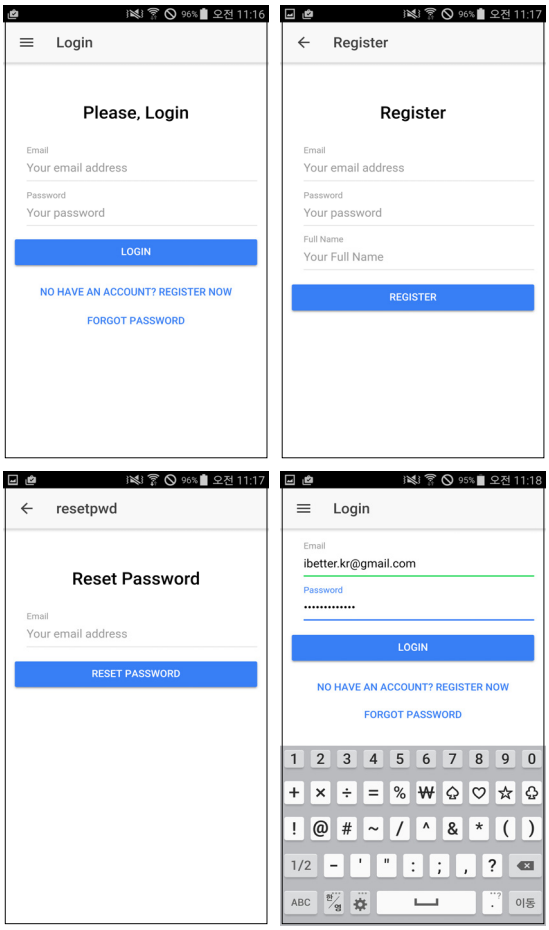

Fig. 6 Login, Register, Reset Password Screen

그림 6은 스마트폰에 구현된 로그인, 회원가입, 비밀번호 찾기 화면이다. 사용자는 회원가입 과정에서 입력한 디바이의 UUID, 이메일, 비밀번호, 이름 등을 이용하여 인증에 활용하게 된다.

그림 7은 각각 다른 사용자가 서로간의 스마트폰을 이용하여 로그인을 진행한 후 등록된 글의 목록이 출력되는 화면이다. 본인의 글은 내용이 보이지만 다른 사람의 글은 숨김으로 처리하여 인증을 해야만 접근할 수 있도록 구현하였다. 왼쪽은 안드로이드 폰의 화면이고 오른쪽은 아이폰의 화면이다.

그림 8은 본인의 글과 다른 이의 글에 접근할 때의 메뉴를 보여준다. 본인의 글인 경우 읽기, 수정, 삭제 등의 메뉴가 존재하며, 다른 이의 글을 읽기 위해서는 권한 허가를 요청하는 작업을 진행한다.

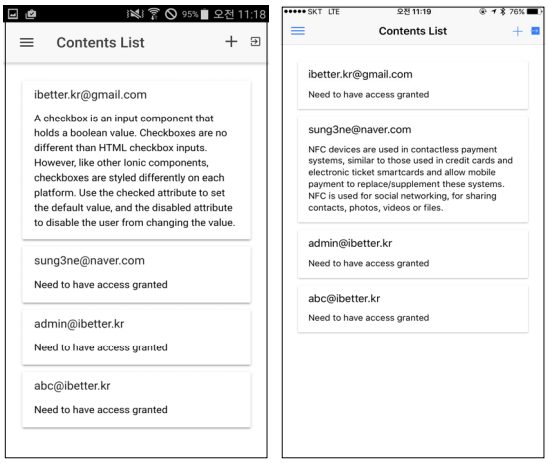

Fig. 7 User Screen with Different Access Granted

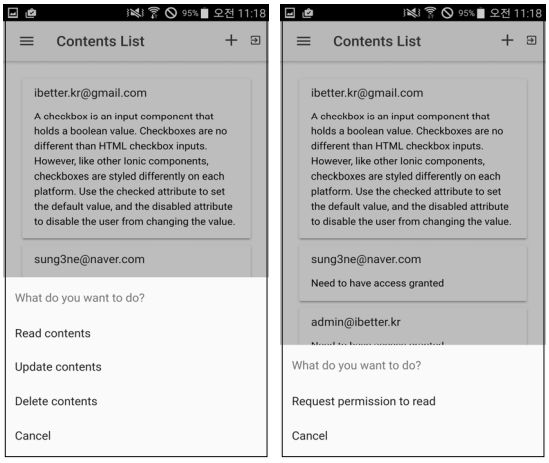

Fig. 8 User Menu with Different Access Granted

그림 9는 다른 이의 글을 읽기 위해서 권한 인증을 획득하는 과정을 보여준다.

① 권한을 획득하기 위해서 User1(안드로이드폰)은 서버에게 해당 문서접근을 위한 인증을 서버에 요청하게 된다.

② 해당 문서의 관리 권한을 가진 User2(아이폰)는 서버로부터 문서 접근에 대한 요청이 왔음을 알리는 메시지를 받게 된다.

③ 인증 허가 버튼을 누를 경우 User1은 서버로부터 인증 UUID를 요청한다.

④ 서버로부터 인증 허가 UUID를 받은 User1의 스마트폰 화면에 인증 QR 코드가 생성된다.

Fig. 9 Authentication Authorization Process Screen

⑤ 인증을 허가하는 User2의 스마트폰으로 QR 코드를 스캔하기 위한 과정을 진행한다.

⑥ 인증이 정상적으로 처리되면 접근을 요청하는 User1의 스마트폰 화면에 글의 내용이 보여 지게 된다. 위의 화면은 인증을 요청하는 안드로이드 폰의 화면이고 아래는 인증을 허가하는 아이폰의 화면이다.

Ⅴ. 결 론

정보기술과 정보통신의 발달로 스마트폰의 이용자가 급속하게 증가하고 있으며 다양한 업무를 스마트폰을 이용해서 진행하는 서비스가 증가하고 있다.

스마트폰을 이용하는 서비스가 증가할수록 보안기술도 함께 발전하고 있지만 인증을 위해 사용되는 아이디와 비밀번호 관리는 개인의 책임 문제이며 여러 개의 서버에서 동일한 계정을 사용하고 있는 문제로 개인정보 유출이라는 문제가 발생하게 된다. 이를 이용하여 타인이 개인의 정보에 접근하고 탈취하는 문제가 발생하고 있다.

이러한 문제를 해결하기 위해서 OTP, FIDO, PIN 코드와 같은 2차 인증요소를 적용하거나 홍체 인식, 지문인식과 같은 개인이 소유한 고유한 특징을 이용한 생체인식과 다차원 인증 요소를 도입하여 인증을 진행하는 연구가 활발하게 진행되고 있다. 하지만 이러한 인증 방식은 개인을 인증하기 위한 인증 서비스이며 개인적인 서비스에 적용 가능한 인증이 대부분이다.

회사나 병원 같이 여러 사용자들이 정보를 공유해서 사용하는 경우 개인 인증 방식으로는 정보 보호에 한계점이 발생한다. 일례로 무역 회사에서 대외비에 해당되는 제품 수입, 수출 내역을 거래처에서 탈취하거나 퇴사한 사람이 평소 친분이 있던 사람들의 정보를 이용해서 접근할 경우 막대한 손실을 입게 될 수 있다. 병원도 마찬가지로 주치의가 아닌 의료진이 환자 정보에 쉽게 접근한다면 그리고 본인이 그 사실을 모른다면 이 또한 문제가 될 수 있다.

본 논문에서는 공용으로 정보 접근이 가능한 환경에서 사용되는 기존의 개인 인증방식의 문제점을 해결하기 위해서 스마트폰을 이용한 상호 협력 기반 인증 방식을 제안하였다.

인증이 필요한 사용자와 인증을 허가해 주는 사용자가 상호 실시간으로 메시지를 교환하는 형태로 진행하며, QR 코드와 BLE를 이용하여 인증 사태를 유지하거나 종료할 수 있도록 제안하였다. 인증이 필요한 사용자가 IMEI와 UUID를 이용하여 실시간으로 QR 코드를 생성하고 인증을 허가하는 사용자 측에서 스마트폰을 이용하여 QR 코드 정보와 서버 정보를 확인해 주는 동작을 진행하도록 하였다.

제안된 알고리즘은 개인적으로 인증이 필요한 서비스가 아닌 다중 협력 또는 상호 인증이 필요한 환경에서 효율적인 인증 알고리즘으로 제시될 수 있을 것으로 사료된다. 또한 제안한 알고리즘의 효율성을 평가하기 위해서 상호 협력 인증 시스템을 설계 및 구현하였다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1D1B03030759) and the research fund from Sahmyook University, 2016

REFERENCES

[1] Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies [Internet]. Available: http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

[2] 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.

[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] H. T. Chae, and S. J. Lee, “Security Policy Proposals through PC Security Solution Log Analysis - Prevention Leakage of Personal Information,” *Journal of the Korea Institute of Information Security & Cryptology*, vol. 24, no. 5, pp. 961-968, Oct. 2014.

[5] 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.

[6] J. Y. Lee, and S. Y. Kang, “Design and Verification of the Integrated Log Analysis System for Enterprise Information Security,” *Journal of Digital Contents Society*, vol. 9, no. 3, pp. 491-498, Sep. 2008.

[7] Y. J. Jeun, “The Medical Information Protection and major Issues,” *Journal of the Korea Society of Computer and Information*, vol. 17, no. 12, pp. 251-258, Dec. 2012.

[8] U. J. Lee, H. Y. Park, and H. C. Shin, “Implementation of a Bluetooth-LE Based Wireless ECG/EMG/PPG Monitoring Circuit and System,” *Journal of The Institute of Electronics and Information Engineers*, vol. 51, no. 6, pp. 261-268, June 2014.

[9] J. H. Park, “A Research on Expansion of Library Service by Using QR Code,” *Journal of Korean Library and Information Science Society*, vol. 43, no. 1, pp. 321-347, Mar. 2012.

[10] S. J. Kim, “Secure Management Method for Private Key using Smartphon`s Information,” *Journal of the Korean Contents Association*, vol. 16, no. 8, pp. 90-96, Aug. 2016.

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