Journal of the Korea Convergence Society
Vol. 10. No. 12, pp. 63-69, 2019

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2019.10.12.063

무작위적인 그래픽 코드를 이용한 인증 알고리즘

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

Authentication Algorithm using Random Graphic Code

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 이용하면 쉽고 빠르게 인증과 결제가 가능하다. 하지만 스마트폰 보안 위협이 다양하고 새로운 해킹 기술로 진화하고 있고 모바일 환경에 특화된 공격 형태로 변화하고 있다. 따라서 모바일 환경에 적합한 인증방법이 요구되고 있다. 현재 지식기반 인증의 보안 취약점을 해결하기 위한 방법으로 금융, 게임, 로그인 등 인증 서비스를 제공하기 위해서 많은 업체에서 일회용 비밀번호(One Time Password)와 같은 2단계 인증 서비스를 제공하고 있다. OTP 서비스는 사용하기 쉽지만 난수표에 대한 복제가 용이하며 제한시간 내에는 유효한 값으로 사용되기 때문에 재사용이 가능한 단점이 존재한다. 본 논문에서는 스마트폰의 전용 애플리케이션을 통해 특수 문자를 인식한 인증 방법을 이용하여 이용자가 높은 보안성을 가지고 쉽고 빠르게 인증을 진행할 수 있는 매커니즘에 대해서 제안한다.

주제어 : 보안요소, 인증 알고리즘, 사용자 인증, 스마트폰, 스마트기기

Abstract Using a smartphone allows quick and easy authentication and payment. However, smartphone security threats are evolving into a variety of new hacking technologies, and are changing to attacks specific to the mobile environment. Therefore, there is a demand for an authentication method suitable for a mobile environment. In order to solve security weaknesses in knowledge-based authentication, many companies provide two-step authentication services such as OTP(One Time Password) to provide authentication services such as finance, games, and login. Although OTP service is easy to use, it is easy to duplicate random number table and has a disadvantage that can be reused because it is used as valid value within time limit. In this paper, we propose a mechanism that enables users to quickly and easily authenticate with high security using the authentication method that recognizes special characters through smartphone's dedicated application.

Key Words : Security Factor, Authentication Algorithm, User Authentication, Smartphone, Smart Device

1. 서론

스마트폰 이용자가 증가함에 따라서 개인정보 보호에 대한 취약점이 증가하고 있다. 인터넷 결제를 진행함에 있어서 데스크톱 컴퓨터에서는 인증을 위한 수단을 지원하기 위한 방안으로 각종 프로그램을 설치해야하는 불편함을 감수해야 하며 특히 공용컴퓨터인 경우 해킹의 위험에 항시 노출이 되어 있을 가능성이 크다. 하지만 스마

*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 November 07, 2019 Revised December 9, 2019
Accepted December 20, 2019 Published December 28, 2019

트폰을 이용하여 결제하는 경우 별도의 프로그램을 설치할 필요가 없으며 클릭 몇 번과 PIN 코드 입력으로 쉽게 결제가 가능하다. 이에 따라서 많은 사람들이 스마트폰을 이용하여 결제 및 개인 인증을 진행하고 있지만 모바일 기기 보안에 대한 인식은 개선되지 않고 있다[1-4].

데스크톱 컴퓨터 환경에서 이루어지던 해킹 기술이 점차적으로 모바일 환경으로 확산되어 가고 있으며 특히 악성코드, 랜섬웨어 및 키로그 등의 진화하고 변질된 보안위협이 스마트폰으로 빠르게 스며들고 있다. 이에 따라 모바일 환경에 맞는 보안인증방법에 대한 연구가 활발하게 진행되고 있다[5-7]. 전통적인 인증 방법인 지식기반 인증의 보안 취약점을 해결하기 위한 방법으로 금융, 게임, 로그인 등 인증 서비스를 제공하기 위해서 많은 업체에서 일회용 비밀번호(One Time Password)와 같은 2단계 인증 서비스를 제공하고 있다. OTP 서비스는 사용하기 쉽지만 난수표에 대한 복제가 용이하며 제한시간 내에는 유효한 값으로 사용되기 때문에 재사용이 가능한 단점이 존재한다. 또한 숫자와 문자를 조합하는 경우가 많아 훔쳐보기 공격이 가능하다[8].

본 논문에서는 특수 문자를 인증요소로 활용하는 사용자 인증 알고리즘을 제안한다. 스마트폰의 전용 애플리케이션을 통해 특수 문자를 인식한 인증 방법을 이용하게 되면 사용자에게 강화된 보안성과 편리성을 제공할 수 있다. 또한 본 논문에서 제안하는 인증 방식은 키를 생성하는 시스템으로 서버뿐만 아니라 아두이노 기기나 라즈베리 파이와 같은 임베디드 기기를 활용할 수 있다는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 이론으로 인증요소기술에 관하여 알아본다. 3장에서는 제안하는 무작위적 그래픽 코드를 이용한 사용자 인증방법에 대해서 알아본다. 4장에서는 제안한 인증방법을 이용하여 구현된 사용자 인증 시스템에 대해서 알아본다. 마지막으로 5장에서는 결론을 맺는다.

2. 관계 이론

2.1 위치정보 기반 인증

모바일 기기를 이용하면 GPS 또는 AP 정보와 같은 위치정보기반 정보를 인증 요소로 활용하는 것이 가능하다. Feng Zhang외 2명은 GPS와 AP 정보를 이용하여 사용자를 인증하는 방법을 제안하였다[9]. 하지만 실내에서는 GPS 정보를 활용함에 있어서 제약사항이 있으며 정보의 인식 범위가 넓기 때문에 한계성이 존재한다. H. Takamizawa외 1명은 사용자를 인식한 주소지의 GPS 정보 외에 다수의 모바일 기기에서 수집한 GPS 정보를 비교하는 방식을 통해 사용자를 인증하는 기법을 제안하였다[10]. 해당 방식은 실시간으로 변화되는 GPS 정보를 비교함에 있어서 오차율이 크기 때문에 인증 정확도가 감소하는 문제가 발생할 수 있다. W. Jansen외 1명은 주변에 설치한 특정 비콘과의 통신이 가능할 때만 인증이 가능하도록 처리하였다[11]. 하지만 통신 인프라 구축의 범위가 넓기 때문에 비용문제가 발생하여 제한적인 용도로만 사용해야 하는 문제가 발생할 수 있다.

2.2 지자기 센서 기반 인증

H. Ketabdar외 3명은 지자기 센서를 이용하면 사용자의 손 움직임을 추정할 수 있는 원리를 이용하여 사용자가 자성이 있는 펜 또는 반지와 같은 물체를 손에 쥐고 공중에서 글씨를 쓰는 행위를 하면 패턴을 추정하여 인증이 이루어지는 MagiSign 기술을 제안하였다[12]. 사용자 인증을 위해서는 정밀한 값을 읽을 수 있는 특수한 용도의 센서가 필요하며 저가형 모델의 스마트폰의 경우 성능적인 제약사항 때문에 활용 범위가 제한적일 수 있다.

2.3 가속도 센서 기반 인증

J. S. Seo외 1명은 모바일 기기에 내장된 가속도 센서 값을 분석하여 사용자를 인증하는 기법을 제안하였다. 사용자가 모바일 기기를 손에 쥐고 허공에 사용자만이 아는 고유한 패턴을 반복하면 인증이 이루어지는 방법이다[13]. 하지만 모바일 기기의 회전방향과 손에 쥐는 방향 등 고려해야할 요소가 많아서 구현이 어렵고 인증에 실패할 확률이 크다.

2.4 생체 정보 기반 인증

A. Bianchi외 3명은 촉각과 음성으로부터 얻을 수 있는 정보를 분석하여 사용자를 인식하는 이용하여 사용자를 인증하는 방식을 제안하였다[14]. 이 기술은 The Phone Lock이라 부르는데 버튼을 누를 때 마다 고유한 음성과 진동이 발생하도록 하여 사용자가 이 정보를 비밀번호로 사용하는 기술이다. 사용자는 화면에 배치된 버튼을 중앙으로 이동시키는 방식으로 비밀번호를 입력한다. 생체 정보 기반 인증 기술로서 복잡한 패턴을 만들어 낼 수 있지만 훔쳐보기 기술에 노출 될 수 있으며 이용자 또한 불편하게 되는 단점이 존재한다.

2.5 다중 인증

T. K. Lee외 2명은 1차적으로 사용자가 위치한 곳의 AP 정보를 이용하고, 2차적으로 생체 정보를 이용하여 사용자를 인증하는 기법을 제안하였다[15]. AP 정보를 인증 요소로 이용하게 되면 위조, 변조, 탈취로부터 자유로울 수 없으며, 생체 정보는 사용자의 신체변화, 날씨, 기기 상태에 따라서 다를 수 있기 때문에 완벽한 인식 성공률을 보장하기 어렵다.

3. 제안 시스템

3.1 네트워크 모델

제안 시스템의 네트워크 모델은 Fig. 1과 같다. 제안 시스템 네트워크는 사용자용 PC, 사용자용 스마트폰, 웹 서버, 데이터베이스 서버, 인증키 관리 서버로 구성된다. 사용자가 PC를 통해 로그인을 시도하면 인증키 관리 서버에서 인증키를 생성하여 사용자 웹 브라우저 화면에 보여준다. 사용자는 스마트폰 전용 애플리케이션을 이용하여 인식한 코드를 해석하여 웹 서버로 전송하여 인증을 진행한다. 데이터베이스 서버에는 인증 정보가 보관되어 있다.

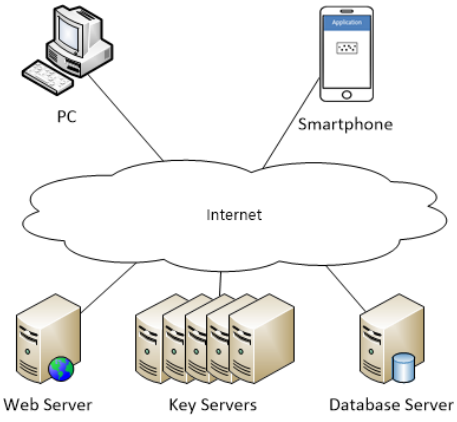

Fig. 1. Network Model

3.2 사용자 등록

Fig. 2는 사용자 등록을 위한 절차를 나타낸다. 사용자는 PC를 이용하여 등록 과정 중에 아이디와 비밀번호 그리고 기타 정보를 웹 브라우저를 이용하여 웹 서버로 전송한다. 웹 서버는 비밀번호를 암호화한 후 데이터베이스 서버에 저장하여 사용자를 등록한다.

① 사용자는 웹 브라우저를 이용하여 사용자 등록을 진행할 웹 서버에 접속한다.
② 사용자는 인증에 사용할 아이디, 비밀번호, 기타 정보를 웹 브라우저에서 입력 후 서버로 전송한다.
③ 인증서버에서 사용자 정보를 확인하여 등록되어 있는 사용자가 아닐 경우 사용자 등록 과정을 진행한다.
④ 아이디, 비밀번호(단방향 해시), 기타 정보를 데이터베이스에 저장하여 등록을 마친다.

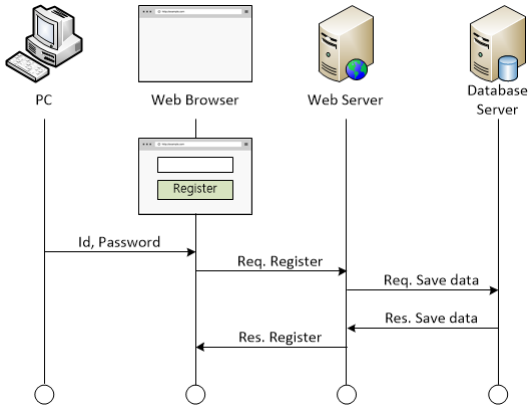

Fig. 2. User Registration

3.3 사용자 인증

Fig. 3은 사용자 인증을 위한 절차를 나타낸다. 사용자는 인증을 위해서 아이디를 웹 서버로 전송한다. 웹 서버는 여러 개의 키 관리 서버들에 인증키를 요청한다. 웹 서버는 각각의 키 관리 서버들이 보내온 무작위적 생성 코드를 조합하여 무작위적 그래픽 코드를 생성한 후 사용자의 웹 브라우저 화면에 출력한다. 사용자는 소지하고 있는 스마트폰의 전용 애플리케이션을 이용하여 웹 브라우저 화면에 출력된 무작위적 코드를 인식하고 인식 정보를 웹 서버로 전송하여 인증을 진행하게 된다. 사용자 인증을 위한 세부 동작은 다음과 같다.

① 사용자는 인증에 사용할 아이디를 웹 서버로 전송한다.
② 웹 서버에서 사용자 정보를 확인하여 등록되어 있는 사용자일 경우 키 관리 서버들에게 키 생성을 요청한다.
③ 키 생성 서버에서 사용자 아이디, 인증 시도 날짜, 인증 시도 시간, 웹 서버 식별 번호, 웹 서버 아이피, 주기적 변경이 가능한 고객 식별 번호를 이용하여 무작위 값을 생성하여 웹 서버로 전송한다.

④ 웹 서버에서 무작위 값을 조합하여 무작위적 그래픽 코드를 생성한 후 웹 브라우저 화면에 출력한다.
⑤ 사용자는 소지한 스마트폰의 전용 애플리케이션을 실행한 후 카메라로 읽어 들인 그래픽 코드를 디코딩을 진행한다.
⑥ 스마트폰에서 전용 애플리케이션을 이용하여 디코딩한 정보를 웹 서버로 전송한다.
⑦ 웹 서버에서 제한시간 내에 스마트폰을 이용하여 전송된 디코딩 정보가 맞으면 사용자 인증 기록을 데이터베이스 서버에 저장하고 인증을 진행한다.

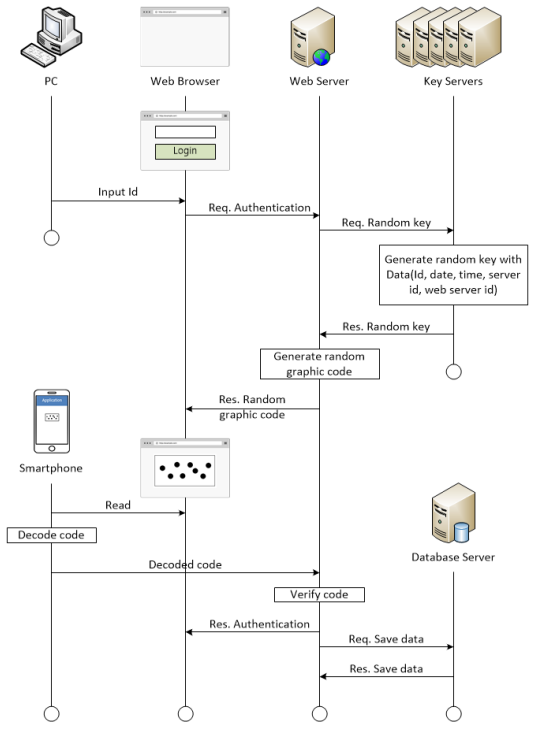

Fig. 3. User Authentication

3.4 그래픽 코드

그래픽 코드 생성을 위해서 ★●◆■▲▼\◀▶♠♥♣▣◈☎♨$&와 같은 특수 문자를 사용한다. 특수 문자는 한글, 한자, 영문, 숫자 등 언어의 표시를 갖는 문자에 속하지 않는 특수한 문자를 의미한다. 키보드의 한글 자음을 누른 다음 '한자' 키를 누르면 다양한 특수 문자를 만들어 낼 수 있다. 특수 문자는 한 번에 쉽게 알아볼 수 있는 문자도 있지만, 자세히 보지 않으면 차이를 알아내기 어려운 문자들도 존재한다. 2,000여 개 이상의 종류가 존재하기 때문에 전용 애플리케이션을 이용하여 인식하지 않으면 인식이 어려울 수 있으며 시간제한이 존재할 경우 제한시간 안에 특수 문자를 키보드를 이용하여 찾아내기 어려우므로 인증요소로 활용할 경우 보안성을 강화할 수 있다. Fig. 4는 특수 문자를 이용하여 생성한 그래픽 코드 예시를 보여준다.

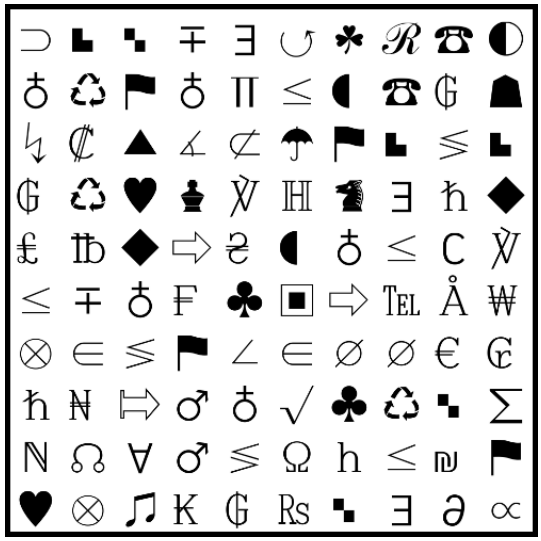

Fig. 4. Graphic Code

4. 제안 시스템 구현

4.1 메시지 구조

그래픽 코드 요청 및 인증을 위해서 사용되는 메시지 구조 형태와 예시는 Table 1과 같다. 인증키 요청시간을 함께 전송하여 메시지를 늦게 받은 서버는 응답을 하지 않도록 처리한다.

Table 1. Request Message Format

Key	Value	Usage
request	request	request api key
request_id	e6e051d8-d458-419a-9b5e-2f78a4a4efe8	unique id that used request key
datetime	2019-11-24 13:27:18	request datetime

인증키 응답 메시지는 구조 형태와 예시는 Table 2와 같다. 인증을 요청하는 서버에서 들어온 인증키를 순서대로 조합하여 그래픽 코드를 만들어낸다.

Table 2. Response Message Format

Key	Value	Usage
request	request	request api key
request_id	e6e051d8-d458-419a-9b5e-2f78a4a4efe8	unique id that used request key
response_id	c10da238-97f8-433d-bedc-33d6e7e6041e	unique id that used response key
datetime	2019-11-24 13:27:20	response datetime

인증키 서버들은 범용PC, 서버, 임베디드 기기(라즈베리파이, 아두이노 등)와 같이 다양한 형태로 존재할 수 있으며, 언제든지 키 생성에 참여할 수도 사라질 수도 있다. 따라서 일정 시간 주기로 존재를 확인해야 할 필요가 있다. 헬로 메시지 구조 형태와 예시는 Table 3와 같으며 응답 메시지는 Table 2와 동일하다.

Table 3. Hello Message Format

Key	Value	Usage
hello	request	request api key
request_id	e6e051d8-d458-419a-9b5e-2f78a4a4efe8	unique id that used hello
datetime	2019-11-24 13:32:37	hello datetime

4.2 시스템 구현

Fig. 5는 그래픽 코드를 인식하기 전 아이디와 비밀번호를 사용하여 로그인 시도를 진행하는 화면이다.

Fig. 5. Login Screen

Fig. 6은 아이디와 비밀번호를 이용하여 1차 인증이 진행된 후 화면에 그래픽 코드를 출력하는 화면이다. Fig 5가 보여진 후 사용자는 스마트폰 애플리케이션을 이용하여 그래픽 코드를 인식하여 2차 인증을 처리하게 된다.

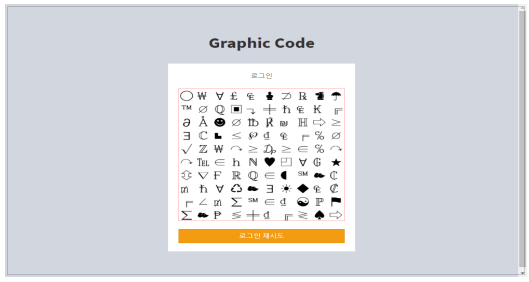

Fig. 6. Graphic Code Screen

Fig. 7은 관리자 페이지에서 사용자 인증을 위해 처리되었던 그래픽 코드를 조회하는 화면이다. 본 화면은 제안 시스템의 올바른 동작을 확인하기 위한 용도로서 실제 서비스에서는 인증된 후 필수적으로 저장되거나 관리될 필요는 없다.

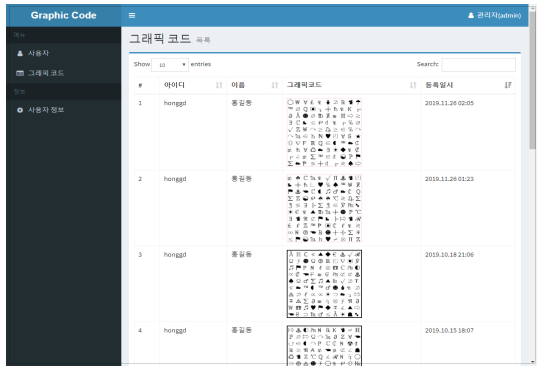

Fig. 7. Graphic Code Log Screen

Fig. 8은 사용자가 애플리케이션을 이용한 인증을 진행하기 위해서 사용자를 등록하고 로그인을 진행하는 스마트폰 애플리케이션 화면이다.

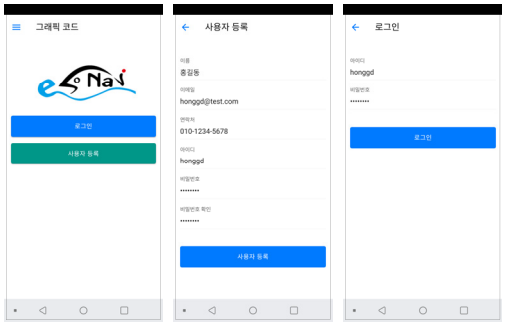

Fig. 8. User Register and Login Screen

Fig. 9는 모니터 화면에 보여지는 그래픽 코드 인증을 시도하기 위해 사용되는 스마트폰 애플리케이션 화면을 보여준다.

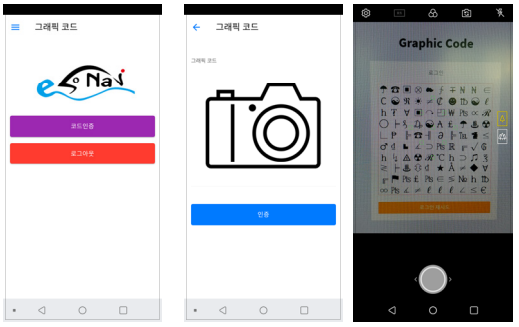

Fig. 9. Graphic Code Authentication Screen

5. 결론

최근 개인정보 대량 유출 사고가 빈번히 발생하고, 개인정보보호법 등 개인정보 관련법이 시행됨에 따라 개인정보 등 중요정보를 안전하게 저장·관리하기 위한 보안기술 도입에 대한 관심이 높아지고 있다. 기업 및 공공기관은 필수적으로 개인정보를 암호화 하여야 하지만 암호화만으로는 개인정보의 안전성을 보장할 수 없다. 암호화된 정보의 안정성은 암호화 알고리즘뿐만 아니라 보안키 관리와도 연관이 있으며, 보안키에 대한 관리 소홀로 보안키가 유출된다면 암호화를 통한 정보보호는 의미가 없기 때문에 보안키를 안전하게 관리하는 것은 매우 중요하다.

사용자 인증기술 평가를 위해서 인터넷진흥원에서 제시하는 적합성 기준으로는 보안성, 편의성, 적용성 등이 있다. 보안성은 진화하고 다양화되는 해킹 기술에 대한 대응력을 말한다. 제안 알고리즘은 기존에 제시되지 않던 새로운 방식의 인증 알고리즘으로서 복제가 어려운 그래픽코드를 사용하였으며 상황에 따라서 키 서버를 추가 및 축소하여 네트워크 구성을 변경하기 용이하도록 구현되어 있기 때문에 해킹에 대해 강건한 특성을 가지고 있다. 편의성은 보편적으로 얼마나 사용하기 편리한가에 대한 논의로서 제안 알고리즘은 그래픽 코드를 인식할 수 있는 애플리케이션과 카메라가 달린 스마트 디바이스만 있으면 필요할 때 언제든지 인증처리가 가능하기 때문에 편의성 요건을 갖추었다고 할 수 있다. 적용성은 최소한의 비용 부담으로 인프라 구축 및 환경 구성이 가능한가를 말한다. 제안 알고리즘에서 사용되는 키 서버는 아두이노, 라즈베리 파이, 테스크톱 컴퓨터, 서버용 컴퓨터, 노트북 등 다양한 컴퓨팅 기기에서 쉽게 구현이 가능하며 전자출결, 금융, 게임 등 다양한 분야에 걸쳐 인증 기술 적용이 가능하다.

본 논문에서는 아이디, 비밀번호 입력 후 사용되는 2차 인증 과정에서 무작위적 그래픽 코드를 이용하여 인증을 진행하는 기법에 대해서 제안하고, 제안된 기법을 이용하여 인증 시스템을 구현하였다. 제안 기법은 확장 가능한 여러 대의 키 생성 서버를 사용하며 상황에 따라서 서버용 컴퓨터, 범용적인 개인용 컴퓨터, 임베디드 기기(라즈베리 파이와 같은 싱글 보드 컴퓨터 등), 스마트폰 등 다양한 기기를 사용하는 것이 가능한 차세대 인증 보안 시스템 기술로서 생성 서버를 일시적으로 확장 가능하기 때문에 보안적인 측면에서 키를 예측할 수 없는 차세대 인증기술로 평가할 수 있다. 다만 그래픽 코드를 인식할 수 있는 애플리케이션이 설치되어 있어야 하고 카메라가 사용가능한 스마트 기기가 필요하다는 점에서 사용 환경에 대한 한계점이 명확하다고 할 수 있다.

향후 아이디, 비밀번호 입력 후 추가인증을 진행하는 시스템, 전자출결시스템 등에 제안 알고리즘을 적용하여 각 상황에서 고려되어야할 요구조건과 적용한계점 등을 분석하고 이를 개선하는 추가 연구를 진행할 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] Y. Ko, J. Choi & B. Kim. (2012). Protecting Individuals from Secondary Privacy Loss using Breached Personal Data Information Center, *Journal of the Korea Institute of Information Security & Cryptology, 22(2),* 391-400.

[6] J. H. Kim, J. Y. Go & K. H. Lee. (2015). A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing, *Journal of the Korea Convergence Society, 6(1),* 85-91.
DOI : 10.15207/JKCS.2015.6.1.085

[7] T. H. Park, G. R. Lee & H. W. Kim. (2017). Survey and Prospective on Privacy Protection Methods on Cloud Platform Environment, *Journal of the Korea Institute of Information Security & Cryptology, 27(5),* 1149-1155.
DOI : 10.13089/JKIISC.2017.27.5.1149

[8] H. J. Mum. (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain, *Journal of Convergence for Information Technology, 8(3),* 85-90.

[9] F. Zhang, A. Kondoro & S. Muftic. (2012). Location-Based Authentication and Authorization Using Smart Phones, *TRUSTCOM '12 Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,* 1285-1292.
DOI : 10.1109/TrustCom.2012.198

[10] H. Takamizawa & N. Tanaka. (2012). Authentication system using location information on ipad or smartphone, *International Journal of Computer Theory and Engineering, 4(2),* 153-157.

[11] W. Jansen & V. Korolev. (2009). A location-based mechanism for mobile device security, *Computer Science and Information Engineering, 2009 WRI World Congress on IEEE, 1,* 99-104.
DOI : 10.9723/jksiis.2012.17.6.025

[12] H. Ketabdar, K. A. Yuksel, A. Jahnbekarn, M. Roshandel & D. Skirop. (2010). MagiSign: User Identification/Authentication Based on 3D Around Device Magnetic Signatures, *Proc. Of UBICOMM'10,* 31-34.

[13] J. S. Seo & J. S. Moon. (2015). A Study on User Authentication with Smartphone Accelerometer Sensor, *Journal of The Korea Institute of Information Security and Cryptology, 25(2),* 1477-1484.

[14] A. Bianchi, I. Oakley, V. Kostakos & D. S. Kwon. (2011). 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,* 197- 200.

[15] 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.

정 필 성(Pil-Seong Jeong) [정회원]

· 2014년 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