JPEE 실천공학교육논문지 JOURNAL OF PRACTICAL ENGINEERING EDUCATION

산학연계교육

J. Pract. Eng. Educ. 16(3), 327-332, 2024

사적 영역에 불법 침입 방지를 위한 도어락 방식의 안전한 PIN 인증 기법

Secure PIN Authentication Technique in Door-Lock Method to Prevent Illegal Intrusion into Private Areas

문형진*

성결대학교 정보통신공학과

Hyung-Jin Mun*

Dept. of Information & Communication Engineering, Sungkyul University, Anyang 14097, Korea

[요 약]

스마트 폰의 보급이 사용자에게 다양한 서비스를 제공하여 삶의 편리함을 주고 있다. 특히, 스마트 폰으로 사용자 인증 후에 손쉽게 온라인 금융거래가 이루어지고 있다. 사용자는 PIN을 이용한 인증으로 쉽게 서비스에 접근하지만 그로 인해 훔쳐보기나 레코딩과 같은 사회공학적 공격에 취약하다. 도어락에서 비밀번호 입력 시 허수를 포함하여 인증하는 방법을 스마트 폰에도 적용함으로써 사회공학적 공격에 대한 보안성을 높이고자 한다. 도어락은 PIN을 단말기 내에서 인증을 수행하지만 스마트 폰에서는 PIN 인증이 서버에서 처리하기 때문에 PIN 정보를 안전하게 전달해야 하는 문제가 있다. 제안기법을 통해 허수가 포함된 PIN을 여러 개 생성하여 해시값과 같은 가공값으로 전송하기 때문에 전송의 안정성을 보장하면서, 노출없이 PIN을 입력할 수 있는 기법으로 안전한 사용자 인증이 가능하다.

[Abstract]

The spread of smart phones provides users with a variety of services, making their lives more convenient. In particular, financial transactions can be easily made online after user authentication using a smart phone. Users easily access the service by authenticating using a PIN, but this makes them vulnerable to social engineering attacks such as spying or recording. We aim to increase security against social engineering attacks by applying the authentication method including imaginary numbers when entering a password at the door lock to smart phones. Door locks perform PIN authentication within the terminal, but in smart phones, PIN authentication is handled by the server, so there is a problem in transmitting PIN information safely. Through the proposed technique, multiple PINs containing imaginary numbers are generated and transmitted as processed values such as hash values, thereby ensuring the stability of transmission and enabling safe user authentication through a technique that allows the PIN to be entered without exposure.

Key Words: Smartphone authentication, PIN authentication, Door-lock mechanism, Decoy PIN, Security enhancement

http://dx.doi.org/10.14702/JPEE.2024.327

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 30 April 2024; **Revised** 30 May 2024
Accepted 4 June 2024

***Corresponding Author**
E-mail: jinmun@gmail.com

I. 서 론

ICT의 발전과 스마트 폰의 급격한 보급으로 인해 다양한 분야에서 스마트 폰을 이용한 서비스가 가능해졌다. 정보를 수신하는 단말기에서 정보를 제공하고, 개인별 서비스를 받는 단말기로 발전하면 개인 식별 및 인증이 필수적으로 요구된다. 스마트 폰을 통해 사용자 인증하는 방법은 패턴이나, 생체인증을 비롯한 PIN 입력 등 다양하게 존재한다.

그중에서 가장 간단한 방법은 숫자로 이루어진 키패드로 개인식별번호인 PIN(personal identification number)을 입력하는 방식이 있다[1].

스마트 폰에서 PIN을 통해 인증하는 방법은 통장의 계좌 비밀번호와 같이 4개의 숫자를 입력하는 방식이 대부분이다.

개인 식별 번호(PIN)는 스마트 폰 이외에도 ATM 인출, 온라인 거래, 장치 잠금 해제 등 다양한 목적으로 일상 생활에서 광범위하게 사용된다[2]. 취약한 PIN은 공격자의 표적이 되어 손쉽게 무단 거래, 사용자의 신원 도용, 금전적 손실과 같은 심각한 결과를 초래할 수 있다. ATM 등 실생활에서의 PIN도난을 방지하기 위한 방법 등이 다양하게 존재하고 있다. PIN도난에 취약한 스마트 폰에서의 PIN도난 방지 기법이 더 많이 요구되고 있다.

다음은 ATM 등에서의 PIN도난 기법에 대한 설명이다.

1. **숄더 서핑(shoulder surfing):** 이 공격은 누군가가 어깨너머로 사용자가 스마트 폰으로 PIN을 입력하는 것을 지켜보는 방법이다[3]. 실제 ATM에서 계좌 비밀번호를 훔쳐보는 것을 방지하기 위해 ATM기기의 양 옆에 가림막이 설치되어 있고, 정면에 거울이 배치되어 뒤에 있는 사람이 보고 있는지 확인하도록 되어 있다. 스마트 폰에서는 쉽게 어깨 너머로 쉽게 볼 수 있어 손이나 몸으로 가야야 하지만 이것으로 차단하기 어렵다[3,4].
2. **스키밍(skimming):** 스키밍은 공격자가 신용카드의 띠를 읽기 위해 ATM이나 결제 단말기에 소형 전자 장치를 이용하여 사용자의 카드 정보와 PIN을 모두 획득할 수 있다. 이를 방지하기 위해 은행 내부나 신뢰할 수 있는 장소의 ATM을 사용해야 한다[5].
3. **피싱(phishing):** 사이버 공격에서 사용되는 방법으로 합법적인 이메일이나 문자 메시지로 착각하여 링크를 클릭하여 PIN을 포함한 개인 정보를 요구하는 공격이다. 신뢰할 수 없는 이메일이나 문자 메시지는 차단할 필요가 있다.
4. **사회 공학(social engineering):** 사회적인 관계성을 이용하여 기밀 정보를 알아내는 방법을 의미한다. 공격자가 사용자에게 은행 직원으로 가장하여 보안 검사를 핑계로 사용자의 PIN을 요구할 수 있다. 누구와도 PIN을 공유할 필요가 없다.
5. **취약한 비밀번호(weak password):** 많은 사용자가 PIN생성 시 생년월일이나 전화번호, 연속된 숫자와 같이 추측하기 쉬운 비밀번호를 사용하고 있다. 사용자뿐만 아니라 공격자도 쉽게 PIN을 추측할 수 있다.

실생활에서의 PIN도난을 막는 방법도 중요하지만 다양한 분야에서 사용되는 스마트 폰에서의 PIN 도난을 막는 방법이 요구되고 있다. 스마트 폰에서 인증은 단말기 사용자임을 인증하는 방법과 해당 서비스에서의 사용자 식별과 인증을 하는 방법으로 나눈다[6]. 단말기 사용자임을 확인하기 위해서 패턴이나 생체인증 등을 사용한다. 단말기 사용자임을 확인한 후에 해당 서비스를 제공하는 앱에서의 인증은 보통 ID/PS 기반의 인증이나 신뢰할 수 있는 PASS나 SNS 등을 통한 본인 인증, 문자 기반의 인증, 사전에 등록된 지문정보를 통한 인증이나 PIN과 같은 비밀번호를 기반으로 하는 인증이 존재한다[2,7].

본 연구에서는 가장 편리하고 간단한 PIN인증기법에서 기존의 다양한 공격으로부터 보호받을 수 있는 기법을 제안한다. 사용자가 사전에 등록한 PIN 이외에도 허수를 추가하여 훔쳐보거나 레코딩 공격으로부터 안전한 기법을 제안한다. 도어락에서 이미 사용된 방법이지만 도어락은 자체 단말기에서의 인증이기 때문에 쉽게 적용이 가능하지만 스마트 폰에서는 안전하지 않은 채널로 PIN정보가 전달되어야 하기때문에 보완적인 기술이 요구된다[8].

PIN 인증 시스템 설계를 위해서는 다음과 같은 조건을 만족해야 한다.

- 어깨너머 공격으로 안전하게 인증을 수행할 수 있도록 공격자가 PIN이 무엇인지 확인할 수 없어야 한다.
- 사용자가 입력한 PIN 정보가 안전하게 서버에 전송되어야 한다.
- 사용자가 PIN을 입력하는 방식이 기존 방식과 큰 차이가 없어야 한다.

II. 관련연구

A. 사용자 인증

사용자가 다양한 서비스를 안전하게 받기 위해 사용자 여부를 확인하는 절차인 사용자 인증이 필수적이다. 사용자 인증은 지식기반 인증(what you know), 소유기반 인증(what you have), 객체 특성기반 인증(what you are)으로 구분한다. 본 연

구에서는 지식기반 인증인 PIN의 새로운 접근을 소개한다.

- **소유기반 사용자 인증**(what you have)은 사용자의 소유물을 통해 인증하는 방식으로 인증에 사용되는 소유물은 신분증, 암호화키, 스마트 폰, 신용카드, OTP 등이 있다. 문자서비스를 통해 인증코드를 입력하여 스마트 폰을 소유자임을 증명하거나 사용자의 OTP로 인증코드를 입력하는 방식이 여기에 해당된다.
- **객체인 사용자의 특성기반 인증**(what you are)은 지문이나 홍채 인증이 대표적이다. 지문, 홍채 등의 생체인증은 다른 사용자와 구별되는 특성으로 인증 수단으로 많이 사용된다[6]. 소유기반 인증 방법은 소유물을 분실할 가능성이 있지만 생체인증은 분실의 위험성이 적은 장점이 있다. Face ID를 이용하여 스마트 폰에서 카메라로 사용자의 안면으로 인식하여 인증하기도 한다.
- **지식기반 인증**(what you know)은 사용자만 알고 있는 PIN이나 패스워드 등 사용자의 지식을 기반으로 인증하는 방식이다. ID 인증은 웹사이트에서 ID로 사용자를 식별하고 ID와 짝이 되는 패스워드가 입력되었을 때 인증 여부를 결정한다. 한번 저장되면 사용자가 변경하지 않을 경우 계속 사용되기 때문에 안전하게 보호, 전달할 필요가 있다. 안전한 인증을 위해 클라이언트가 입력한 패스워드를 평문상태가 아닌 해시값을 생성하여 서버에 전송하고 수신받은 해시값과 서버에 저장된 값을 비교하여 인증을 수행한다.

패스워드 기반 인증의 안전성은 1차적으로 패스워드의 길이와 무작위성에 의존한다. 2차적으로는 패스워드가 저장된 테이블의 안전성에 좌우된다. 패스워드의 길이가 짧거나 간단하고, 빈번하게 사용되는 패스워드의 해시값은 역산이 가능하여 패스워드를 알아낼 수 있는 단점이 존재한다[4].

패스워드의 해시값이 저장된 테이블이 유출되고, 레인보우 테이블 공격(Rainbow Table Attack)이 수행될 경우 사용자의 패스워드를 알아낼 수 있다[9]. 패스워드의 안전성을 높이기 위해 안전한 해시함수를 사용하고 패스워드의 길이 및 다양한 형태의 문자를 기반으로 패스워드를 생성해야 한다.

B. 비밀번호 전송 방법

스마트 폰으로 PIN을 통해 사용자 인증을 할 때 전달되는 PIN정보를 안전하게 전송해야 한다. 안전하게 전달하는 방법은 입력된 정보를 암호화하여 서버에 전송하면 서버에서 전송받은 정보를 DB에 저장된 정보와 비교하여 인증을 수행한다. 스마트 폰에서 사용자는 PIN을 입력하면 수식 (1)과 같이 3가지 방식으로 암호화한다.

첫째는 인증시스템이 해시함수를 적용할 경우에는 해시값을 생성해서 서버로 해시값을 전송한다.

둘째는 인증시스템이 대칭키로 데이터 전송을 보호한다면 단말기와 서버가 동일하게 가지고 있는 대칭키로 암호화하여 전송한다.

셋째는 인증시스템이 공개키 방식인 경우 서버의 공개키를 취득하여 공개키로 암호화하고, 서버에 전송한다.

$$E(pin)=\begin{cases} h(pin) & \text{if } h: hash\ function \\ E_{\mathrm{KS}}(pin) & \text{if KS}: symmetric\ key \\ E_{\mathrm{KU}}(pin) & \text{if KU}: public\ key\ of\ Sever \end{cases} \quad (1)$$

$$S_{\mathrm{info.}}=\begin{cases} h(pin) & \text{if } hash\ value \\ pin\|\mathrm{KS} & \text{if KS}: symmetric\ key \\ pin\|\mathrm{KR} & \text{if KR}: private\ key\ of\ Sever \end{cases} \quad (2)$$

각 방법에 따라 서버가 가지고 있는 정보는 수식 (2)와 같이 다른 정보를 가지고 있다.

첫 번째 방식은 서버가 PIN을 가지고 있지 않고, 해시값만 소장하고 있어 전송받은 해시값을 비교하여 같으면 인증이 완료된다. 일반적으로 ID/PS 기반의 인증방식이 이 방식을 사용하고 있다.

두 번째 방식은 서버는 PIN정보를 가지고 있고, 암호문을 복호화할 수 있는 대칭키를 가지고 있어야 한다. 대칭키는 단말기와 서버가 동일한 정보를 가지고 있어야 한다. 서버는 사용자의 수만큼 다른 대칭키를 소유하고 있어야 하고, 사전에 대칭키 분배가 이루어져야 한다.

세 번째 방식은 단말기가 서버의 공개키로 암호화한 정보를 서버가 자신의 가지고 있는 개인키로 복호화하는 방식이다. 복호화하여 얻은 PIN정보가 저장된 PIN 같은 지 확인하여 인증한다. 키교환이 필요 없는 방식이다.

일반적으로 인증시스템은 첫 번째 방식을 주로 사용한다. 서버가 PIN을 가지고 있어야 하고 키 분배에 대한 문제점이 존재한다.

$$E(pin)=\begin{cases} h(pin\|\mathrm{UID}\|etc) \\ E(pin\|\mathrm{UID}\|etc) \\ E(h(pin)\|\mathrm{UID}\|etc) \end{cases} \quad (3)$$

안전한 인증시스템을 적용하기 위해 수식 (3)과 같이 부가적인 정보를 추가할 수 있다. 인증 상대 확인을 위해 UID(식별자) 이외에도 재전송공격을 막기 위해 Timestamp나 난수 등을 추가할 수 있다. 필요에 따라 PIN의 해시값을 암호화하여 전송할 수도 있다.

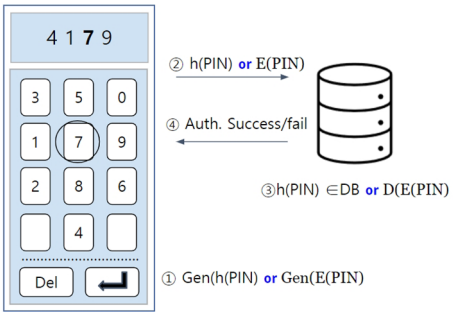

그림 1. PIN으로 인증하는 기존 방식

Fig. 1. Existing method for authentication using PIN.

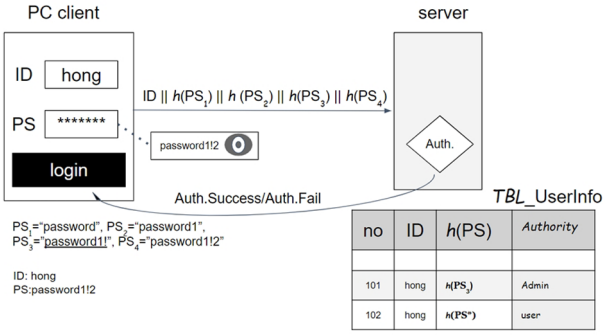

그림 2. 멀티 패스워드 ID 기반 인증

Fig. 2. Mult-password ID-based authentication.

III. 허수가 포함된 PIN기반의 인증기법

비밀번호를 입력하는 도어락은 어깨너머 공격 등의 공격을 막기 위해 실제의 비밀번호 이외의 번호를 추가하여 터치를 통해 도어락을 여는 방식이다. 즉, 도어락의 비밀번호가 "1234"이면 "67123489"를 입력하여 "67"과 "89"를 허수로 취급하고 실제 비밀번호를 확인하는 방식이다.

이 방법은 입력된 정보가 서버로 전달되지 않고 자체에서 인증을 수행하는 도어락에서는 적용하기 쉽다. 따라서 본 논문에서도 도어락과 같은 방식을 스마트 폰에 적용할 수 있는 안전한 PIN기반의 인증 기법을 제안한다.

스마트 폰에서 터치한 PIN을 제 3자가 알 수 없도록 그림 1에서 보듯이 해시값을 생성하거나 암호화한다. 인증하는 방식은 다음과 같은 과정으로 수행한다.

step 1. 입력된 PIN을 공격자가 알 수 없도록 가공한다.

step 2. 안전하지 않은 채널이나 무선으로 서버에 전달한다.

step 3. 수신된 정보를 서버의 DB에 저장된 정보와 확인하여 인증여부를 결정한다.

step 4. 인증결과(인증성공여부)를 스마트 폰으로 전송한다.

이 방식의 문제점은 스마트 폰에서 PIN을 입력하는 과정에서 어깨너머 공격이나 레코딩 공격, 사회공학적 공격을 통해 PIN을 알아내거나 가공된 PIN 값을 전달하는 과정에서 공격자가 계속적으로 수집할 경우 공격 가능성을 찾을 수 있다는 문제점이 있다.

A. 멀티 패스워드 ID기반 인증기법[1]

그림 2는 웹 사이트 등에서 멀티 패스워드를 이용한 인증 및 권한 부여가 가능한 인증기법을 나타낸 것이다[9].

이 방식은 패스워드를 여러 개 생성하여 안전한 인증과 권한 차등 부여와 같은 서비스를 제공할 수 있다. 웹 사이트에서 패스워드를 입력하면 여러 개의 해시값을 생성하여 서버에 전달하고, 인증시스템에 저장된 정보와 비교하여 안전한 인증이 가능하다. 허수가 포함된 패스워드를 입력하면 여러 개의 해시값을 생성하여 전달하기 때문에 훔쳐보기나 레코딩 공격을 차단할 수 있다. 또한 입력된 패스워드에 따라 다양한 권한을 부여할 수 있다. 사용자가 여러 개의 권한을 가질 경우 다수의 계정관리를 해야 하는데 이 방식으로 하나의 계정에 여러 개의 패스워드를 연결하고, 패스워드별로 권한을 부여할 수 있다.

허수가 포함된 다수 해시값 생성 기법은 PC환경에서 키보드를 통해 입력하므로 마지막 문자를 확인 없이 빠르게 인증하는 것이 가능하지만 정확하게 입력하는 것이 어려운 스마트 폰과 같은 환경에서는 바로 적용하기 어렵다. PC와 다르게 스마트 폰에서는 훔쳐보기 및 레코딩 공격에 취약하기 때문에 스마트 폰에 적합한 기법이 필요하다.

B. 단말기에서 허수가 포함된 안전한 인증기법

공격에 취약한 것은 입력한 PIN의 길이가 짧아서 생기는 문제이다. 사용자가 PIN의 길이가 길면 대체적으로 안전하게 인증할 수 있다. 제안 방식은 사용자가 PIN의 길이를 길게 입력할 수 있는 시스템을 설계하고자 한다.

즉, 그림 3에서 보듯이 사용자가 PIN("1234")이외의 가상의 번호를 추가하여 허수가 포함된 새로운 PIN("8912345")의 해시값을 생성하여 서버에 전달하는 방식으로 PIN의 길이를 늘일 수 있다.

그림 3은 허수가 포함된 인증기법을 나타낸 것이고 아래와 같은 단계별 수행을 한다.

step 1. 사용자는 허수를 포함한 새로운 PIN을 입력한다.

step 2. 사용자가 입력한 PIN의 값으로 시스템이 요구한 가공값(해시값이나 암호문)을 생성한다.

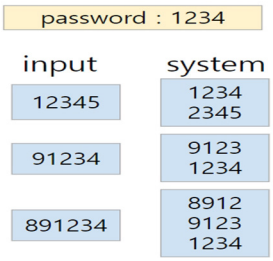

그림 3. 허수가 포함된 인증 기법

Fig. 3. Authentication Method involving imaginary numbers.

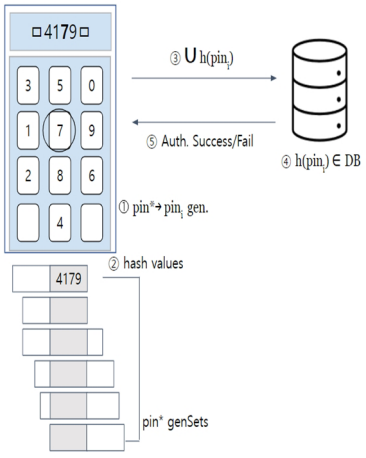

그림 4. PIN 생성 기법

Fig. 4. PIN generation method.

step 3. 다양하게 생성된 PIN의 가공값들을 서버에 전달한다.

step 4. 서버는 입력받은 PIN의 가공값들을 하나씩 DB에 있는 값과 비교한다.

step 5. 모든 가공값과 비교하여 하나라도 같은 것이 있으면 인증 성공, 없으면 인증 실패를 판단하여 사용자에게 인증여부를 전달한다.

제안 방식의 아이디어는 실제 PIN과 가상의 PIN을 구별하고, 가공값을 생성하는 지에 대한 연구이다.

사용자가 입력한 허수가 포함된 PIN*에서 다양한 PINi를 생성한다. 그림 4는 “4179”가 포함된 PINi 생성하고 여러 개 PIN의 가공값으로 인증하는 과정을 나타낸다.

그림 5는 맨 앞자리 부터 하나씩 삭제 해가면서 만든 PIN, 뒷부분 부터 하나씩 삭제하면서 PIN을 생성하는 의사코드이다.

```
def gen(vPIN):
  str=vPIN
  PINs=[]
  for i in range(0,len(vPIN)):
    PIN=str[i:i+size]
    if len(PIN) == size:
      PINs.append(PIN)
  return PINs
```

그림 5. 의사코드

Fig. 5. Pseudocode.

IV. 분석 및 평가

스마트 폰에서 안전하게 PIN을 인증하는 시스템을 설계하기 위해서는 다음과 같은 조건을 만족한다.

첫째, 제안 기법에서 사용자가 PIN을 입력하는 과정에서 어깨너머 공격으로 안전하다. 짧은 PIN 입력 시 공격자가 쉽게 알아내고, 암기할 수 있다. 하지만 제안 기법에서는 긴 PIN을 입력하므로 공격자가 알기 어렵다.

둘째, 현관문에서는 허수를 포함한 번호를 입력하더라도 기기안에서의 인증이므로 추가적인 기술이 요구되지 않는다. 하지만 스마트 폰에서의 인증은 입력된 정보가 서버로 안전하게 전달되어야 인증 여부가 결정된다. 제안 기법에서는 사용자가 입력된 PIN 정보는 단말기에서 여러 개의 정보를 생성하고, 이를 해시값과 같은 암호적 함수값으로 변환하여 전송하므로 서버에 안전하게 전달이 가능하다.

셋째, 제안 기법을 사용 시 시스템을 이해하고 사용에 불편함이 없어야 한다. 현재 도어락에서도 허수를 포함하여 번호를 입력하는 방식이 적용되어 있어 스마트 폰에서 적용 시 사용자가 PIN을 포함하는 긴 정보를 입력하는 번거러움은 있지만 이해 부족으로 인한 어려움은 없다.

IV. 결 론

도어락은 주변서 훔쳐보기가 가능하기 때문에 비밀번호 노출 가능성이 높다. 이 공격을 차단하기 위해 도어락은 허수를 포함한 비밀번호 입력이 가능하다. 입력된 정보로부터 비밀번호가 맞는 지 확인하여 인증을 수행한다.

스마트 폰도 도어락처럼 훔쳐보기나 레코딩 공격에 취약하다. 그럼에도 도어락과 같이 허수를 포함한 PIN인증에 적

용할 수 없었던 이유는 인증 여부를 안전하지 않는 채널을 통해 인증정보가 서버에 전달해야 하기 때문이다.

본 연구에서는 도어락에서 적용이 된 허수가 포함된 PIN 인증이 스마트 폰에서도 가능한 기법을 제안하였다. 향후 연구에서는 제안 기법에서 언급된 허수가 포함된 PIN 입력의 편리성과 안전성이 보장되고, 성능평가 분석이 필요하다.

참고문헌

[1] PIN encryption: Safeguarding Your Personal Identification Number 13 Feb 2024. https://fastercapital.com/content/PIN-encryption--Safeguarding-Your-Personal-Identification-Number.html

[2] H. J. Mun, “Analysis on the trends of PIN input method of mobile device in fintech environment,” *Quality of Life Research,* vol. 1, no. 1, pp. 33-38, April 2023.

[3] S. Schneegass, A. Saad, R. Heger, S. Delgado Rodriguez, R. Poguntke, and F. Alt, “An investigation of shoulder surfing attacks on touch-based unlock events,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. MHCI, pp. 1-14, 2022. https://doi.org/10.1145/3546742

[4] H. J. Mun, “Design of an enhanced group keypad to prevent shoulder- surfing attacks and enable user convenience,” *Journal of Practical Engineering Education,* vol. 15, no. 3, pp. 641-647, December 2023.

[5] https://news.koreadaily.com/2024/02/23/society/ general-society/20240223220404948.html

[6] H. J. Mun, “1.5-factor authentication method using secure keypads and biometric authentication in the fintech,” *Journal of Industrial Convergence*, vol. 20, no. 11, pp. 191-196, 2022.

[7] X. Bultel, J. Dreier, M. Giraud, M. Izaute, T. Kheyrkhah, P. Lafourcade, D. Lakhzoum, V. Marlin, and L. Motá, “Security analysis and psychological study of authentication methods with PIN codes,” In *2018 12th International Conference on Research Challenges in Information Science (RCIS)*, pp. 1-11, May 2018. IEEE. https://doi.org/10.1109/RCIS.2018.8406648

[8] M. H. Lee and H. J. Mun, “Design of an visitor identification system for the front door of an apartment using deep learning,” *Journal of the Korea Convergence Society,* vol. 13, no. 4, pp. 45-51, 2022.

[9] H. J. Mun, S. H Hong, and J. P. Shin, “A novel secure and efficient hash function with extra padding against rainbow table attacks,” *Cluster Computing*, vol. 21, no. 1, pp. 1161-1173, 2018. https://doi.org/10.1007/s10586-017-0886-4.

[10] H. J. Mun, “The secure password authentication method based on multiple hash values that can grant multi-permission to a single account,” *Journal of Industrial Convergence,* vol. 21, no. 9, pp. 49-56, September 2023.

문 형 진 (Hyung-Jin Mun)_종신회원

1996년 2월 : 충남대학교 수학과 졸업
2008년 2월 : 충북대학교 전자계산학(이학박사)
2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
2017년 3월 ~ 현재 : 성결대학교 정보통신공학과 조교수
〈관심분야〉 정보보호, 네트워크 보안, Fintech 보안, 사용자인증