산업융합연구 제21권 제2호 pp. 117-123, 2023
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2023.21.2.117

모바일 단말기에서 지문 지우기를 활용한 스머지 공격 방지를 위한 보안 키패드 설계

문형진*
성결대학교 정보통신공학과 조교수

Design of a Secure Keypads to prevent Smudge Attack using Fingerprint Erasing in Mobile Devices

Hyung-Jin Mun*
Assistant Professor, Dept. of Information & Communication Engineering, Sungkyul University

요 약 핀테크 환경에서 다양한 서비스를 제공하기 위해 스마트 폰을 대표적으로 사용하고 있다. 또한, 스마트 폰에서의 안전한 서비스를 이용하기 위해 사용자 인증기술이 요구되고 있다. 인증하기 위해 PIN이나 패스워드를 입력하고 완료 버튼을 터치한 순간 서버에 인증정보를 전달하여 인증을 수행한다. 하지만 카메라 등을 이용한 레코딩 공격, 엿보기 공격이 아니더라도 터치스크린 사용 흔적인 스머지가 남게 되어 사후 공격이 가능하다. 스머지 공격을 차단하기 위해 사용자는 인증 후 사용자는 지문을 지워야 한다. 본 연구에서 지문 지우기 여부를 판단할 수 있는 기법을 제안하였다. 제안기법은 PIN를 입력한 다음에 터치한 흔적인 지문 지우기를 수행하고, 지우기 여부를 판단되면 자동으로 입력 완료 버튼 대신에 처리하는 보안 키패드를 설계하였다. 패스워드 입력시 반드시 지문을 지우는 동작을 요구하는 방식이다. 이 기법을 통해 사용자는 반드시 지문 지우기를 해야만 서비스 요청이 완료되어 스머지 공격을 차단할 수 있다.

키워드 : 핀테크, 스머지 공격, 지문 지우기, 보안 키패드, 사용자 인증

Abstract In the fintech environment, Smart phones are mainly used for various service. User authentication technology is required to use safe services. Authentication is performed by transmitting authentication information to the server when the PIN or password is entered and touch the button completing authentication. But A post-attack is possible because the smudge which is the trace of using screen remains instead of recording attack with a camera or SSA(Shoulder Surfing Attack). To prevent smudge attacks, users must erase their fingerprints after authentication. In this study, we proposed a technique to determine whether to erase fingerprints. The proposed method performed erasing fingerprint which is the trace of touching after entering PIN and designed the security keypads that processes instead of entering completion button automatically when determined whether the fingerprint has been erased or not. This method suggests action that must erase the fingerprint when entering password. By this method, A user must erase the fingerprint to complete service request and can block smudge attack.

Key Words : Fintech, Smudge attack, Fingerprint erasing, Secure keypads, User authentication

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received December 28, 2022
Revised January 18, 2023
Accepted February 20, 2023
Published February 28, 2023

1. 서론

스마트 폰의 대중적인 이용으로 인해 핀테크 환경으로 변모하게 되었고, 많은 금융거래에서 스마트 폰을 이용하여 이루어지고 있다. 하지만 스마트 폰이 무선 통신을 이용하고 있고, 스크린의 크기가 작고, 빈번한 금액 거래로 인해 안전성이 큰 이슈가 되고 있다. 스마트 폰을 이용한 안전한 금융거래를 위해 안전한 인증 기술이 요구되고 있다.

핀테크 환경에서 스마트 폰은 SNS의 DM 및 SMS를 통한 피싱(Phishing) 공격이나 스미싱(Smishing) 공격, 엿보기 공격(Shoulder surfing attack)과 같은 사회공학기법에 취약하다. 특히 다양한 공격을 통해 악성코드를 설치하도록 유도하고, 키로깅 공격(Keylogging Attack) 등으로 공격이 빈번하게 발생하고 있다[1-4]. 안전한 거래를 위해 다양한 인증 기술이 제안되고 있다. PIN(Personal Information Number) 및 패스워드 인증, SMS 문자 기반 인증, FIDO(Fast IDentity Online) 이용한 생체인증을 통해 인증을 수행한다[5].

스마트 폰에서 보안 키패드를 통한 PIN 인증이나 패스워드 인증이 편리성으로 인해 보편적으로 사용되고 있지만, 취약점이 존재하여 안전성이 떨어진다[6]. 특히, 보안 키패드를 통해 공동 인증서의 비밀번호, 계좌 비밀번호를 입력시 잘못된 터치가 많고, 키로거 공격으로 터치한 위치를 탈취하여 패스워드 유추가 가능하다[4]. 스마트 폰의 스크린의 크기가 커짐에 따라 사용자가 PIN를 입력하는 과정을 뒤에서 공격자가 엿보기 공격(Shoulder-Surfing Attack)이 가능하다[7].

고해상도의 카메라 등의 녹화 장치를 이용하여 인증하는 과정을 촬영하여 PIN를 알아내는 레코딩 공격(Recording Attack)이 가능하다. 스머지 공격은 스마트 폰에서 패턴 잠금이나 가상 키패드를 이용할 때 손가락의 유분이 터치 스크린에 남아 공격자가 이 흔적을 통해 사용자의 패스워드를 알아내는 것이다. 모바일 단말기에서 인증하는 과정에서 단말기에 남아있는 지문의 흔적은 스머지 공격(Smudge Attack)에 취약하다[8].

본 논문에서는 스마트 폰과 같은 모바일 단말기에서 터치한 흔적 및 지문을 지우는 방식으로 스머지 공격을 차단할 수 있는 기법을 제안한다. 지문을 지울 수 있는 기법을 설계하기 위한 요구사항이 필요하다.

패스워드 입력 후 마지막으로 지문을 지워야 한다.

지문을 지우는 것인지 키패드를 입력하는 것인지 구별할 수 있어야 한다.

사용자로 하여금 지문 지우는 방법을 쉽게 이해할 수 있어야 한다.

2. 관련 연구

2.1 보안 키패드

PC 환경에서 키보드가 아닌 터치가 가능한 디스플레이(모니터)에서 키패드를 보여주고, 터치할 수 있는 키패드를 가상 키패드라고 한다. 간혹 터치가 되지 않은 환경에서도 마우스를 이용하여 터치하는 방식의 가상 키패드를 제시하여 키보드 입력이 아닌 안전한 방식으로 패스워드를 입력한다. 가상 키패드는 키보드 모양과 비슷하게 구성되어 원하는 키패드를 쉽게 찾을 수 있다(Fig. 1).

1	2	3		4	5	6	7	8	9	0
q	w	e	r	t	y		u	i	o	p
a	s		d	f	g	h		j	k	l
↑		z	x	c	v	b	n	m	↵	
#+=			SPACE					OK		

Fig. 1. QWERTY keypads

PC 뿐만 아니라 스마트폰에서도 가상 키패드를 이용할 수 있지만 스마트 폰의 경우 터치한 위치를 알게 되면 터치한 키패드를 유추할 수 있어 스마트 폰의 경우 키패드 사이의 간격을 두어 가상 키패드를 생성한다.

금융기관에서 사용되는 가상 키패드는 QWERTY 방식이다(Fig. 2)[9]. 이 방식에서 왼쪽이나 오른쪽과 같은 측면의 키패드가 고정되고, 나머지 키패드는 1~2 칸만 이동되어 터치한 위치를 활용하면 패스워드를 유추할 수 있다. Fig. 2와 같이 간격을 적절하게 둔 가상 키패드도 넓은 의미의 보안 키패드이다.

2.2 개선된 보안 키패드

2.2.1 테트리스 모양 보안 키패드

금융기관에서 보편적으로 사용하는 기존 보안 키패드는 간격을 1~2칸 이상으로 확보할 수 없는 단점을 가진다. 테트리스는 여러 개가 연결되어 공간을 확보할 수 있는 장점이 있다. 테트리스 모양의 키패드는 기존 키패드와 비교하여 상대적으로 작지만(Fig. 3), 테트리스 게임처럼 이어 붙일 수 있는 장점이 있어 많은 공백을 확보할 수

있어 이를 기반으로 키패드 사이의 공간을 확보하면 위치 기반의 공격으로부터 안전한 키패드이다[9].

Fig. 2. Secure keypads in the bank

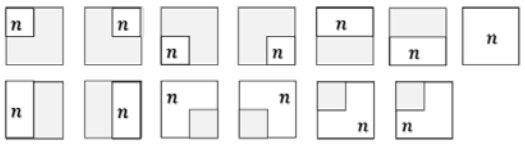


Fig. 3. Type of tetris

키패드는 13개의 종류의 모양을 가지고 있다. Fig. 4는 테트리스 모양의 키패드를 적용한 예시이다. 키패드의 크기가 기존 키패드와 비교할 때 $\frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1$ 이라서 잘못 터치할 가능성이 존재한다[9].

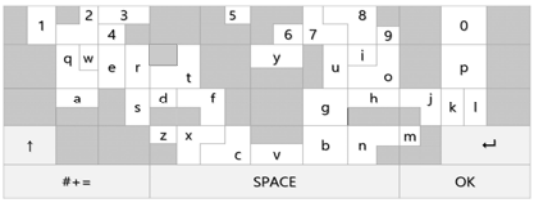


Fig. 4. Example of tetris secure keypad

2.2.2 터치 시간 기반 PIN 보안 키패드

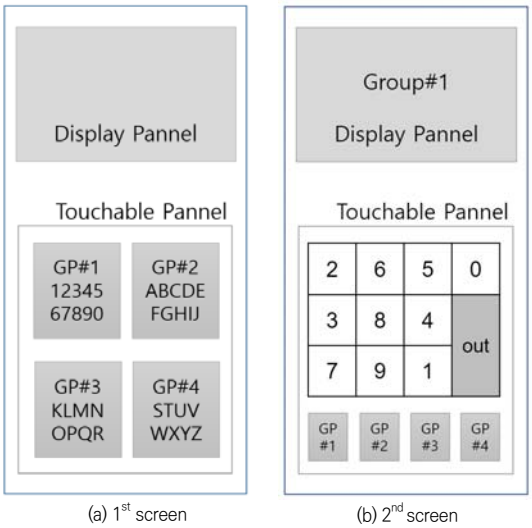
계좌의 패스워드의 경우 숫자로만 구성된다. PIN 보안 키패드는 터치 공간의 제약을 받지 않지만 엿보기, 레코딩 공격에 취약하다. Fig. 5는 터치하는 시간을 기반으로 입력되는 키패드가 결정되는 방식이다[10]. 터치 시간 기반 숫자 보안 키패드는 하나의 키패드에 2개의 숫자(n/M)로 표시되어, 터치하는 시간이 1초 이상이면 왼쪽 숫자(작은 글씨)가 짧으면 오른쪽 숫자(큰 글씨)가 입력되는 방식이다. 이 기법은 엿보기(shoulder surfing attack), 무차별 대입 공격(Brute force attack), 키로깅 공격(keylogging attack)에 안전하지만, PIN 아닌 문자 입력 방식에는 적합하지 않다.

1/5	7/4	9/7
5/8	3/9	2/6
6/1	8/2	0/3
	4/0	OK

Fig. 5. Numeric keypad with long-short touch

2.2.3 이중 터치 가상 보안 키패드

스마트 폰과 같은 모바일 단말기는 터치스크린의 제약으로 인해 숫자 10개와 영문자 26개를 하나의 화면에서 보이기 위해서는 키패드의 크기를 키울 수 없다. 하나의 문자를 입력하기 위해 2번 터치하는 방식의 보안 키패드로 4~5개의 그룹으로 구분하여 첫 화면에는 그룹을 대표



(a) 1st screen (b) 2nd screen

Fig. 6. Double-Touch Secure Keypad Screen

하는 문자를 보여주고 해당 그룹을 선택한 후 그룹 내의 문자를 터치하는 방식의 보안 키패드이다[11]. Fig. 6은 모든 키패드를 4개의 그룹으로 구분하여 제시된 예시이다. 이중 터치 기반 보안 키패드의 첫 화면은 Fig. 6(a)과 같다. 숫자 그룹을 선택하면 해당 그룹의 모든 키패드를 Fig. 6(b)과 같이 제시한다. 사용자는 문자를 터치하면 디스플레이 영역에서 터치한 문자에 매칭된 색을 표시하여 입력된 문자가 맞는지 확인한다. 다음 입력할 문자가 같은 그룹에 있을 경우 현재 키패드에서 터치하고, 같은 그룹에 있지 않은 문자인 경우 첫 화면으로 되돌아 가거나 해당 그룹의 번호를 터치하여 해당 그룹 키패드로 넘어간다.

첫 화면에서 그룹(GP#2)을 선택한 후, 두 번째 단계 화면에서 해당 그룹의 키패드를 배치하는 방법은 Fig. 7과 같이 알파벳 순이나 오름차순으로 배치하거나 PC자판이나 빈도수에 따라 배치할 수 있다.

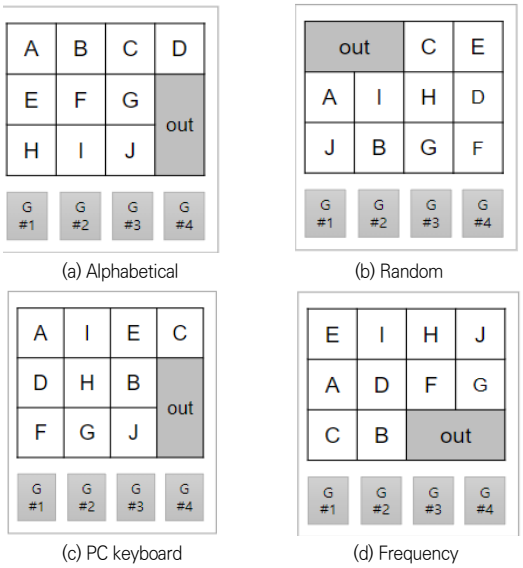


Fig. 7. Method of keypad type in the 2nd stage

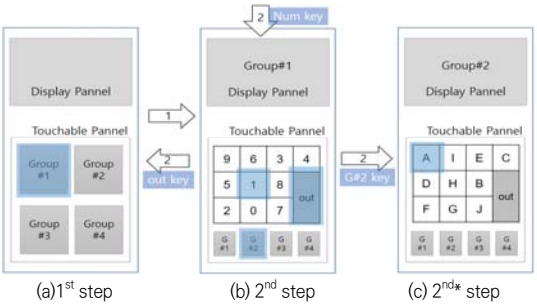


Fig. 8. PIN input process

Fig. 8은 PIN을 입력하는 과정을 보여주고 있다.

step 1. 숫자 ⊡를 입력할 때 처음 화면(a)에서 숫자 그룹을 선택한다.

step 2. 두 번째 단계(b)로 넘어가서 원하는 문자를 입력한다.

step 3-1. 다음 패스워드 문자가 숫자이면 같은 그룹 (b)에서 해당 키패드를 터치한다.

step 3-2. 다음 문자가 해당 그룹에 없을 경우 out 을 터치하여 (a)로 넘어가거나 그룹번호를 알 경우 하단의 해당 그룹을 선택한다. (c)는 하단에 있는 GP#2를 터치했을 때 해당 그룹의 보안키패드 모습이다. 그룹 번호를 모를 때 첫 화면 (a)으로 이동하여 PIN을 입력한다.

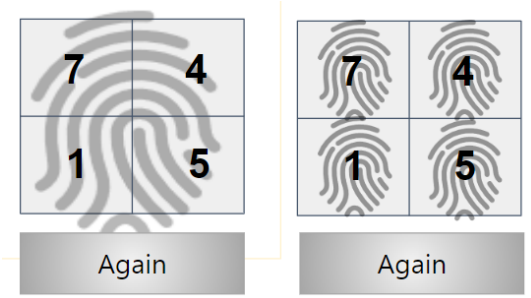
2.4 2팩터 및 1.5 팩터 인증

2-factor 인증은 사용자 인증시 한 개의 인증수단이 아닌 2개의 인증수단을 사용한 것을 의미한다[12]. 인증수단은 패스워드 인증과 같이 사용자가 알고 있는 정보, OTP나 스마트 폰과 같이 사용자가 소지한 기기, 홍채나 지문 같은 사용자의 생체정보가 된다. 안전한 인증을 위해 최근에 스마트폰에서 지문인증후 PIN이나 패스워드 인증하는 2-factor 인증을 수행한다.

지문 인증과 같은 생체인증은 오탐지 및 미탐지 가능성이 높아 2-factor 인증이 요구되지만 2번의 인증절차로 인한 불편함이 있었기 때문에 한 번에 2개인 인증을 수행하는 1.5-factor 인증이 있다[13]. Fig. 9는 스마트폰에 보여지는 1.5 factor 인증 기법의 첫 화면의 예시이다.

Fig. 9. First Screen of 1.5-factor authentication

1.5-factor 인증기법은 Fig. 10에서 보듯이 2가지 방식이 있다. PIN 입력하는 터치스크린 전체가 지문 인식하는 영역(a)과 PIN 입력 영역마다 지문 인식하는 영역(b)으로 나눈다. 인증 시스템에서 2개의 정보인 PIN번호와 지문정보로 인증을 수행하여 PIN이 맞지 않으면 바로 인증실패, 지문이 인증되지 않으면 다시 시도를 요구하는 기법이다.



(a) One fingerprint (b) Partial fingerprint

Fig. 10. Two kinds of fingerprint recognition area

3. 터치 흔적 지우기 기법

지문이나 터치한 흔적을 지우는 방법으로 스머지 공격을 차단하고자 한다. Fig. 11은 PIN를 입력하는 숫자 키패드이다. PIN를 입력한 후에 완료 버튼 대신에 흔적을 지우는 것으로 완료를 대신한다.

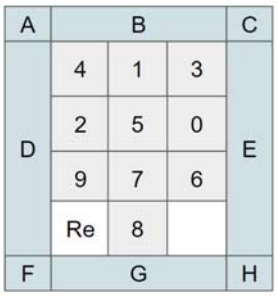


Fig. 11. Touch screen of proposed technique

3.1 지문 지우기 여부 판단 기법

지문을 지우는 것인지 PIN를 입력하는 것인지 판단이 필요하다. 지문을 지우는 방법은 다음과 같다.

좌우 지우기 : 왼쪽 영역(A,D,F)을 터치한 후 숫자 키패드를 지나 오른쪽 영역(C,E,H)을 터치한다. 오른쪽 영역에서 왼쪽 영역으로 지울 수 있다.

상하 지우기 : 위쪽 영역(A,B,C)을 터치하고 숫자 키패드를 지나 아래쪽 영역(F,G,H)을 터치한다. 아래에서 위쪽으로 지울 수 있다.

즉, Fig. 11에서 알파벳(A,B,C,D,E,F,G,H)영역에서 시작되어 숫자를 지나 다시 알파벳 영역을 터치하면 흔적을 지우는 것으로 판단하고 완료를 수행한다. 즉, 알파벳을 터치하면 그 전에 입력한 PIN만 사용자가 입력한 PIN으로 처리한다.

3.2 패스워드 입력시 동작 과정

사용자가 PIN이 아닌 패스워드를 입력할 경우, 보안키패드가 보여지는 공간의 크기가 알파벳 영역으로 약간 줄어든다. Fig. 12는 패스워드가 입력이 가능한 보안 기법이다. 보안키패드 외부의 알파벳 영역에서 지문을 지우는 방식으로 패스워드 입력을 완료로 수행하고, 서버에게 패스워드를 전송한다.

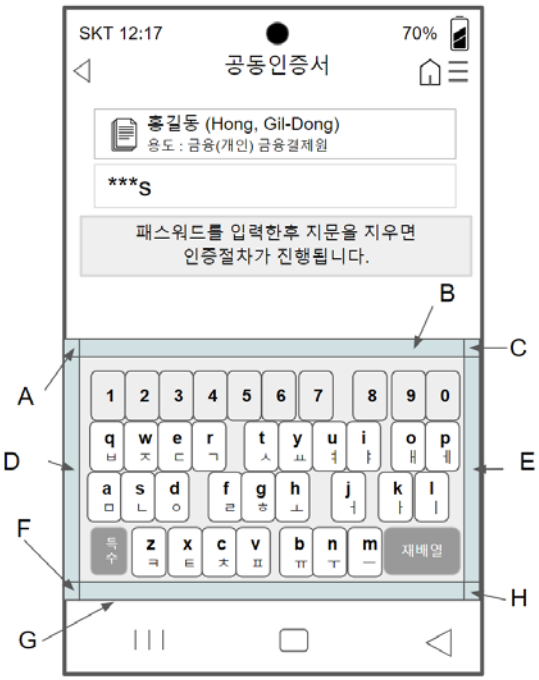


Fig. 12. Proposed Method

4. 분석 및 평가

4.1 제안 기법의 순서도

Fig. 13은 제안 기법의 절차에 대한 순서도이다.

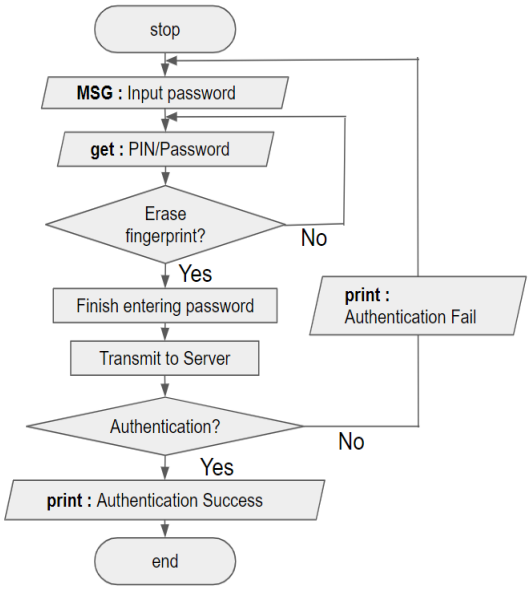


Fig. 13. Flowchart of Proposed Method

step 1. 패스워드 입력 메시지(MSG)가 출력된다.
step 2. 사용자는 패스워드(또는 PIN)를 입력한다.
step 3. 터치가 될 때마다 3.1.1에서 제시된 지문 지우기 여부를 확인한다.
step 4. 시스템은 지문 지우기가 아니면 step 2로 이동하여 추가로 패스워드를 입력받는다. 지문 지우기라면 패스워드 입력이 완료한다.
step 5. 입력된 패스워드를 서버에 전송한다.
step 6. 전송받은 패스워드로 인증 여부를 판단한다. 인증이 실패되면 step 1로 이동한다.
step 7. 인증 성공 메시지를 출력한다.

4.2 제안 기법의 분석 및 평가

터치 스크린을 통해 패스워드를 입력하는 데 흔적으로 인한 공격이 가능하면 흔적을 지우는 것이 필요하다. 모든 패스워드를 입력하고 지문을 지우고, 흔적을 지워야 하지만 사용자가 경각심이 없어 놓치는 경우가 많다. 제안 기법은 모든 패스워드를 입력하고 반드시 지문이나 흔적을 지우는 것을 요구하는 보안 키패드로 스머지 공격에 쉽게 대응할 수 있다.

서론에서 제시된 요구사항을 만족한다. 첫째로 패스워드를 입력하고 지문 지우기가 완료 버튼으로 활용된다. 둘째로, 키패드 입력과 지문 지우기를 구별할 수 있는 판단알고리즘을 제안 기법에 제시하고 있다. 셋째는 패스워드 입력하는 과정에서 디스플레이에서 완료버튼이 없고 지우는 방법을 제시하고 있어 사용법을 쉽게 이해할 수 있다.

5. 결론

다양한 분야에서 사용되는 스마트 폰에서 PIN이나 패스워드 입력을 위해 터치하는 과정에서 흔적인 스머지가 남는데 이를 통해 공격이 빈번하게 이루어지고 있다. 스머지 공격을 차단하기 위해서는 지문이나 터치한 흔적으로 지워야 한다. 하지만 사용자들이 이를 간과하는 경향이 많아 근본적인 해결방법이 필요하다. 본 논문에서는 스마트 폰에서 패스워드나 PIN를 입력하고 모든 입력의 완료하기 위해 지문 지우기 기법을 활용한다. 패스워드를 입력 후 완료 버튼이 아닌 흔적으로 지우는 방법으로 스머지 공격을 차단하는 것이 가능하다.

향후 연구는 지문 지우는 과정에서의 오작동 및 실패율을 줄일 수 있는 방법에 대한 연구가 필요하다.

REFERENCES

[1] B. S. Yu & S. H. Yun. (2011). The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing. *Journal of the Korea Convergence Society,* 2(4), 9-14. DOI : 10.15207/JKCS.2011.2.4.009

[2] D. Y. Kim & S. M. Cho (2015). A Proposal of Smart Phone App for Preventing Smishing Attack. *Journal of Security Engineering,* 12(3), 207-220.

[3] S. H. Kim, M. S. Park. & S. J. Kim. (2014). Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes. *Journal of the Korea Institute of Information Security & Cryptology,* 24(6), 1159-1174. DOI : 10.13089/JKIISC.2014.24.6.1159

[4] I. Y. Choi, J. H. Choi & W. Y. Lee. (2014). A Design and Implementation of a Solution for Real Detection of Information Leakage by Keylogging Attack. Journal of Korea Multimedia Society, 17(10), 1198-1204. DOI : 10.9717/KMMS.2014.17.10.1198

[5] C. J. Chae, H. J. Cho & H. M. Jung. (2018).

Authentication Method using Multiple Biometric Information in FIDO Environment. *Journal of Digital Convergence,* 16(1), 159-164. DOI : 10.14400/JDC.2018.16.1.159

[6] J. S. Song, M. W. Chung, S. H. Seo & S. H. Lee. (2015). Security vulnerability analysis of Simple Mobile Payments Services. *The Korea Information Processing Society Fall Conference,* 22(2), 817-820. DOI : 10.3745/PKIPS.y2015m10a.817

[7] Y. S. Jeoung & D. M. Choi (2017). D-PASS: A Study on User Authentication Method for Smart Devices. The Journal of the Korea Institute of Electronic Communication Sciences, 12(5), 915-922. DOI : 10.13067/JKIECS.2017.12.5.915

[8] H. Lee & T. Kwon (2017). Fingerprint Smudge Attacks Based on Fingerprint Image Reconstruction on Smart Devices. Journal of the Korea Institute of Information Security & Cryptology, 27(2), 233-240. DOI : 10.13089/JKIISC.2017.27.2.233

[9] H. J. Mun, S. Y. Kang & C. Shin.. (2020). Implementation of Secure Keypads based on Tetris-Form Protection for Touch Position in the Fintech. *Journal of Convergence for Information Technology*, 10(8), 144-151. DOI : 10.22156/CS4SMB.2020.10.08.144

[10] J. Song, M. W. Jung, J. I. Choi & S.H. Seo (2018). Proposal and Implementation of Security Keypad with Dual Touch. KIPS Transactions on Computer and Communication Systems, 7(3), 73-80. DOI : 10.3745/KTCCS.2018.7.3.73

[11] H. J. Mun (2022). Design for Position Protection Secure Keypads based on Double-Touch using Grouping in the Fintech. Journal of Convergence for Information Technology, 12(3), 38-45. DOI : 10.22156/CS4SMB.2022.12.03.038

[12] H. J. Mun (2018). Biometric Information and OTP based on Authentication Mechanism using Blockchain. *Journal of Convergence for Information Technology,* 8(3), 85-90. DOI : 10.22156/CS4SMB.2018.8.3.085

[13] H. J. Mun. (2022). 1.5-factor Authentication Method using Secure Keypads and Biometric Authentication in the Fintech. *Journal of Industrial Convergence,* 20(11), 191-196. DOI : 10.22678/JIC.2022.20.11.191

문 형 진(Hyung-Jin Mun) [종신회원]

- 1996년 2월 : 충남대학교 수학과
- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2009년 3월~2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
- 2017년 3월~현재 : 성결대학교 정보통신공학과 조교수
- 관심분야 : 정보보호, Fintech 보안, 사용자 인증
- E-Mail : jinmun@gmail.com