산업융합연구 제20권 제11호 pp. 191-196, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.11.191

핀테크 환경에서 보안 키패드와 생체인증을 이용한 1.5-factor 인증 기법

문형진*
성결대학교 정보통신공학과

1.5-factor Authentication Method using Secure Keypads and Biometric Authentication in the Fintech

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

요 약 핀테크 환경에서 스마트 폰을 이용한 금융거래가 활발하게 이루어지고 있다. 안전한 금융거래를 위해 사용자 인증 기술이 필수적이다. 기존 보안 키패드를 통한 PIN 인증은 입력 편리성이 좋지만, 보안성이 떨어지고 취약점이 존재한다. 생체인증 기법은 보안성이 안전하지만 오탐 및 미탐 인증 가능성이 있다. 이를 보완하기 위해 2-factor 인증을 사용한다. 본 논문에서는 생체인증 기법을 적용한 PIN 입력을 통해 편리성과 보안성을 높일 수 있는 1.5-factor 인증을 제안하고자 한다. 지문인증의 안정성과 2~4번의 PIN 입력을 통해 편리성을 제공하여 안전한 금융거래가 가능하다. 제안기법은 PIN 입력 시 생체인증을 동시에 수행하므로 PIN 입력할 때 터치하는 영역에 지문인식을 적용하는 방식이다. 보안이 요구되는 경우 높은 안전성이 요구되는 상황에서는 추가적인 PIN 입력을 통해 입력 편리성을 보장하면서 사용자 인증을 수행하여 안전한 금융거래가 가능하다.

키워드 : 핀테크, 1.5-팩터 인증, 사용자 인증, 보안 키패드, 생체인증, 지문인식, 지문인증

Abstract In the fintech field, financial transactions with smart phones are actively conducted. User authentication technology is essential for safe financial transactions. PIN authentication through the existing security keypads is convenient to input but has weaknesses in security and others. The biometric authentication technique is secure, but there is a possibility of false positive and false negative authentication. To compensate for this, two-factor authentication is used. In this paper, we propose the 1.5-factor authentication that can increase convenience and security through PIN input with biometric authentication. It provides the stability of fingerprint authentication and convenience of two or three PIN inputs, and this makes safe financial transaction possible. Since biometric authentication is performed at the same time when entering PIN, while security is required by applying fingerprint authentication to the area touched while entering PIN. The User authentication is performed while ensuring convenience to input through additional PIN input in situations where high safety is required, and Safe financial transactions are possible.

Key Words : Fintech, 1.5-factor authentication, User authentication, Secure keypads, Biometric authentication, Fingerprint recognition, Fingerprint authentication

1. 서론

ICT 발달로 인해 스마트 폰이 핀테크 환경에서 금융거래에 이용량이 급격하게 증가하고 있다. 안전한 금융거래를 위해 다양한 사용자 인증 기술이 필요하다. 하지만 스마트 폰의 급증으로 SNS의 DM 및 SMS를 통한 피싱이나 스미싱 공격이나 어깨너머 공격(Shoulder surfing attack)과 같은 사회공학기법을 이용한 링크(URL)이나 불법 파일로 인한 멀웨어(Malware) 설치, 키로깅 공격 등의 빈번하게 발생하고 있다[1-4]. 안전한 거래를 위해 다양한 인증 기술이 제안되고 있다. PIN 인증, SMS 문자 기반 인증, FIDO(Fast IDentity Online) 이용한 생체인증을 통해 인증을 수행한다[5].

대표적인 사용자 인증은 보안 키패드를 통한 PIN인증

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received October 4, 2022 Revised October 17, 2022
Accepted November 20, 2022 Published November 28, 2022

으로 편리성이 좋지만, 보안성이 떨어지고 취약점이 존재한다. 보안 키패드를 통해 인증서 비밀번호, 계좌 비밀번호를 입력하지만 자판을 터치스크린에 제시되지만 잘못된 터치가 많고, 키로거 공격을 통해 터치한 위치를 탈취하여 입력된 PIN를 유추가 가능하다[4, 6]. 또한 고해상도의 카메라 촬영이나 어깨 너머 훔쳐보기 공격에 취약점이 존재한다.

FIDO 기반의 생체인증 기법은 보안성이 안전하지만 잘못된 인증 가능성이 존재한다. 본인이 아닌 가족 얼굴을 통해 인증되는 사례가 발생하여 한 번의 인증으로 사용자 인증을 완료하기 어렵다. 이로 인해 2-factor 인증이 수행된 이후 PIN을 입력하거나 또 다른 인증을 요구한다.

본 논문에서는 생체인증 기법을 적용한 PIN 입력을 통해 편리성과 보안성을 높일 수 있는 1.5-factor 인증을 제안하고자 한다. 생체인증인 지문을 사용하여 안전성을 보장하면서 2~4번의 PIN 입력을 통해 편리성을 제공할 수 있는 안전한 금융거래가 가능하다.

2-factor 인증이 아닌 편리성을 보장하면서 안전성을 보장하는 기법을 설계하기 위한 요구사항이 필요하다.

- 2-팩터 인증보다 편리성 요구되어야 한다.
- 키로거 공격으로부터 안전한 위치 탈취로 인한 공격으로부터 안전성이 보장되어야 한다.
- 제공된 키패드의 위치가 랜덤하게 제시되고, 쉽게 입력이 가능하고, 터치시 실수가 없도록 키패드의 크기가 보장되어야 한다.
- 훔쳐보기 공격을 차단할 방안이 제시되어야 한다.

2. 관련 연구

2.1 가상 키패드

가상 키패드는 사용자가 스마트 폰에서 비밀번호를 입력할 수 있는 키패드로 PC자판과 비슷하다. 스마트 폰의 터치스크린 영역의 제한으로 PIN 입력시 터치가 쉽지 않다. 금융기관에서 사용되는 가상 키패드는 QWERTY 방식(Fig. 1)과 ABC 방식(Fig. 2)이 있다[7]. ABC 키패드보다 PC자판과 비슷한 QWERTY 키패드 방식을 많이 사용한다. 하지만 왼쪽이나 오른쪽 측면의 키패드가 고정되고, 나머지 키패드는 1~2 칸만 이동되어 터치한 위치를 활용하면 PIN을 유추하거나 일부 알아낸 PIN 정보로 나머지 정보를 유추할 수 있다. 예를 들어, 공격자가 PIN이 “asecgh”를 알아냈다면 사용자의 PIN이 “asdfgh” 으로 유추할 것이다.

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

a		b	c	d	e	f	g		h
	i	j		l	m	n	o	p	q
r	s	t	u		v	w	x	y	z
Shift			?123		←			CLOSE	

Fig. 2. ABC keypads

2.2 보안키패드

2.2.1 시작 위치 랜덤 배치 보안키패드

Fig. 3은 서화정의 보안 키패드는 QWERTY 방식에서 숫자 “1”의 키패드를 임의의 위치에 배치한 변경한 방식이다. PIN 입력할 때 먼저 “1”을 찾은 후, “1”을 기준으로 QWERTY 자판으로 키패드가 배치되어 자판을 기억하지 않을 경우 키패드를 찾기 어렵다[8, 9].

h	j		k	l	z	x		c	v	b
	n	m	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	↵	
#+=			SPACE					OK		

Fig. 3. Seo’ keypads

2.2.2 테트리스 모양 보안 키패드

기존 키패드의 모양은 터치하기 쉽게 직사각형의 형태를 가진다. 하지만 공백을 만들 공간이 부족한 단점이 있어 터치한 위치 취약점이 존재한다. 테트리스 모양의 보안 키패드는 기존 키패드보다 작지만, 테트리스 게임처럼 이어 붙일 수 있는 장점이 있어 빈 공백을 추가로 확보할 수 있는 장점이 있어 위치 취약점에 강점을 가진다. QWERTY 기반으로 키패드 모양을 변경한 보안 키패드이다[9].

테트리스 보안 키패드의 모양은 Fig. 4와 같이 13개의 종류가 존재한다. Fig. 5는 테트리스 모양의 키패드를 적용한 예시이다. 많은 여백이 있어 측면에 키패드가 표시되지 않아서 기존 방식의 측면 터치시 가지는 취약점에 강점이 있다. 하지만 기존 키패드 크기의 $\frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1$ 로 상대적으로 작아 사용자의 잘못된 터치 가능성이 존재한다[9, 10].

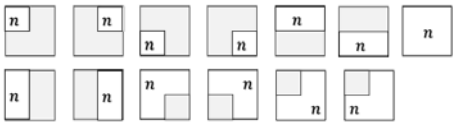


Fig. 4. Type of tetris

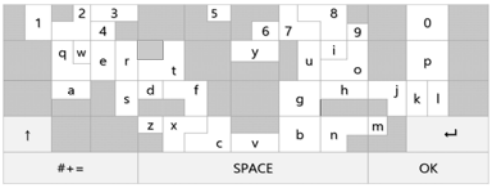


Fig. 5. Example of tetris secure keypad

2.2.3 터치 시간 기반 숫자 보안 키패드

터치 시간 기반 숫자 보안 키패드는 Fig. 6과 같이 하나의 키패드에 2개의 숫자(n/M)로 표시되어, 터치하는 시간에 따라 다르게 입력되는 보안 키패드 방식이다.

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

Fig. 6. Numeric keypad with long-short touch

키패드를 1초 이상 터치하면 작은 크기의 왼쪽 숫자가 입력되고 1초 미만 터치하면 큰 크기의 오른쪽 숫자가 입력되는 방식이다. 숫자 키패드가 랜덤하게 배치되고, 터치 시간에 따라 다르게 입력되어 보안 키패드의 공격인 어깨너머 공격(shoulder surfing attack), 무차별 대입 공격(Brute force attack), 키로깅 공격(keylogging attack)에 안전하지만 알파벳이 아닌 숫자 키패드만 가능하여 많은 문자입력에 적합하지 않다[11].

2.2.4 이중 터치 가상 보안 키패드

이중 터치 기반 보안 키패드는 4~5개로 그룹핑한 키패드를 제시하여 그룹을 선택한 후 그룹 내의 문자를 터치하는 방식의 보안 키패드이다[10]. Fig. 7은 4개의 그룹으로 구분하여 제시된 보안 키패드의 예시이다. 이중 터치 기반 보안 키패드의 첫 화면은 Fig. 7(a)과 같다. 그룹을 선택하면 해당 그룹의 모든 키패드를 Fig.7(b)과 같이 제시한다. 예를 들어, GP#1를 선택한 경우 "1 2 3 4 5 6 7 8 9 0" 숫자를 한 번에 보여준다. 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.

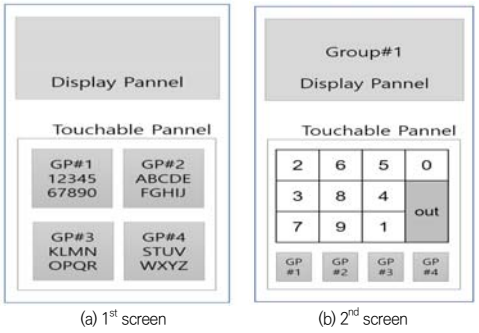


Fig. 7. Double-touch secure keypad screen

첫 화면에서 그룹(GP#2)를 선택한 후, 두 번째 단계 화면에서 해당 그룹의 키패드를 배치하는 방법은 Fig. 8과 같이 다양하다.

- Fig.8(a) 알파벳 순이나 숫자의 오름차순으로 배치
- Fig.8(b) 랜덤하게 배치, 버튼을 자유롭게 배치
- Fig.8(c) PC자판과 같은 방식으로 배치
- Fig.8(d) 영어 사전에 많이 사용된 빈도수에 따라 배치

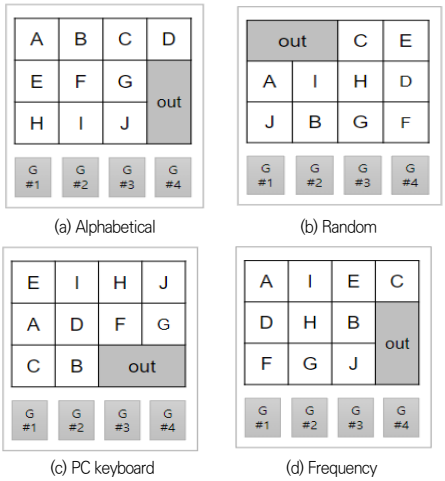


Fig. 8. Method of Keypad Type in the 2nd stage

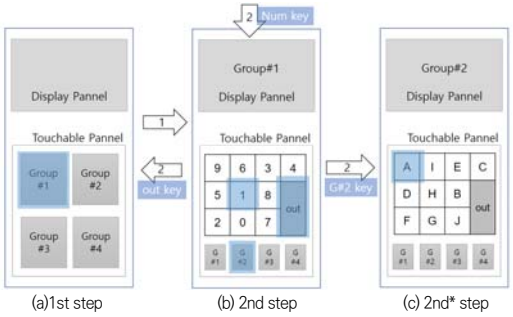


Fig. 9. PIN Input Process

Fig. 9는 숫자를 입력하는 과정을 보여주고 있다.

step 1. 숫자 ⑨를 입력할 때 처음 화면(a)에서 숫자 그룹을 선택한다.

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

step 3-1. 만약에 다음 문자가 숫자이면 같은 그룹(b)에 있으면 보여지는 화면에서 해당 키패드를 터치한다.

step 3-2. 같은 그룹에 없을 경우 out 를 터치하여 (a)로 넘어가거나 그룹을 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.

2.3 어깨 너머 공격을 차단 기법

기존의 보안 키패드에서는 사용자가 터치된 문자를 보여주고, 그 다음 문자 입력시 그 전에 있는 문자 대신에 * 로 표시되지만 촬영이나 훔쳐볼 수 있다는 취약점을 가진다.

2.4.1 4색 정리

4가지 색 정리(Four Color Theorem)에 의해 평면에 유한 개의 영역을 다른 색으로 표시가 가능하다. 키패드에 색을 적용하여 모든 키패드로 표현할 수 있다[12]. 사용자가 PIN을 입력할 때 해당 키패드의 색을 화면에 출력하여 터치한 문자가 맞는지 확인할 수 있다.

2.4 2-factor 인증

2-factor 인증은 비밀번호와 같은 사용자가 알고 있는 정보와 OTP나 SMS와 같이 사용자가 소지한 기기, 지문과 같이 사용자의 생체정보 중에서 2가지를 인증에 사용하는 것을 의미한다[13]. 금융기관 앱에 들어갈 때 스마트폰에서 지문으로 인증하고, 거래시 PIN를 입력하는 방식으로 2-factor 인증을 수행한다.

3. 1.5-팩터 인증 기법

3.1 1.5-Factor 인증 설계

생체인증은 단독으로 사용하기 어렵다. 생체인증은 오탐지 가능성이 높기 때문이다. 안면인식기술의 경우 자매나 부자, 모녀, 쌍둥이 등 비슷한 얼굴로 인해 잘못된 인증이 되는 경우가 있다. 미탐지 가능성이 존재한다. 오탐지와 미탐지를 차단하기 위해서 1.5-factor 인증을 설계하고자 한다. Fig. 10은 스마트 폰에 보여지는 제안 기법의 첫 화면의 예시이다.

Fig. 10. Touch screen of proposed technique

Fig. 11는 제안 기법에 대한 플로우 차트를 보여주고 있다.

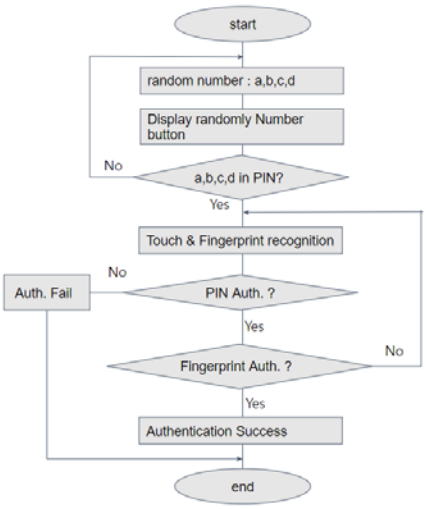
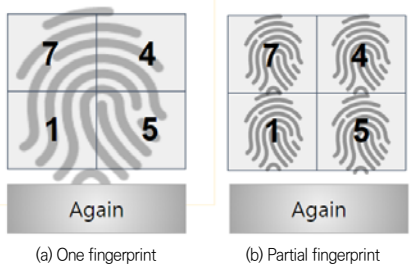


Fig. 11. Flow chart of Proposed Method

- 4개의 버튼을 생성하기 위해 임의의 중복되지 않는 수를 생성하여 화면에 표시한다.
- 만약 사전에 등록된 PIN이 아닌 경우 Again 버튼을 클릭하여 처음에 나오지 않았던 숫자 중심으로 생성하여 표시한다. 최대 3번 이내로 원하는 숫자가 나오도록 생성한다.
- 지문인식을 위해 정확하게 PIN 수에 터치한다. 지문과 PIN을 시스템에 전달하여 인증을 수행한다.
- PIN 인증 실패시 종료를 하고, 지문인증에 실패하면 다시금 지문을 다시 요구한다.
- PIN과 지문 인증에 성공하면 사용자 인증이 완료된다.

3.2 생체인증 영역과 인증 프로토콜

Fig. 12에서 보듯이 지문을 인식하는 영역이 2가지로 PIN 입력하는 전체가 지문 인식하는 영역과 4개의 PIN 입력 영역마다 지문 인식하는 영역으로 나눈다.



(a) One fingerprint (b) Partial fingerprint

Fig. 12. Two kinds of fingerprint recognition area

3.3 보안성 강화 기법 및 절차

사용자가 등록한 PIN 번호가 보이지 않을 경우 다시 요청하여 새로운 PIN 번호를 생성하여 화면에 제시하고 PIN 인증실패시 일정 시간 잠긴상태가 되거나 추가 터치를 허용하되, 반복되면 추가적인 인증을 요구한다. 보안 안전성을 높이기 위해 PIN 입력을 2~4회 추가적으로 요구할 수 있다.

4. 분석 및 평가

제안 기법에서 4개 난수를 생성하여 4칸을 생성하여 출력하였지만 스마트 폰의 터치스크린의 크기와 지문인식 영역을 고려하여 Fig. 13과 같이 6개, 9개로 나눌 수 있다. 또한, 제안 기법에서는 PIN을 1회 또는 2~4 번의 최소한 터치로 인해 터치된 숫자를 확인하는 절차가 없이 인증이 수행하기 때문에 어깨 너머 공격에 강하다.

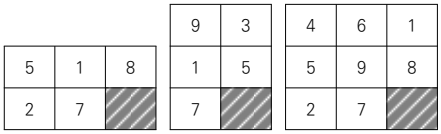


Fig. 13. Kind of PIN touch panel

터치 스크린이 작은 스마트 폰에서는 PIN 입력의 편리성과 생체인증의 안전성을 고려하여 보안 키패드를 설계해야 한다. PIN을 입력하기 위한 키패드의 개수를 4개로 구성하여 사용자의 입력 편리성을 높일 필요가 있다. 또한, 한 번의 터치를 통해 지문인증이 가능하기 때문에 인증하는데 시간을 줄일 수 있어 다양한 공격으로부터 안전하다.

서론에서 제시된 요구사항을 제안 기법에서 만족하고 있다. 첫째, 한번에 PIN입력과 지문인증을 수행하여 입력 편리성이 높아진다. 둘째, 숫자 키패드가 랜덤하게 선택되어 배치되기 때문에 터치되는 위치 탈취로부터 안전하다. 셋째, 디스플레이에 보여지는 키패드 개수가 4, 6, 9개라서 상대적으로 키패드의 크기를 키울 수 있다. 넷째, 지문인증이 포함되어 안전하게 인증되고, 한번의 터치로 훔쳐보기 쉽지 않다.

5. 결론

급격한 스마트 폰의 이용과 ICT 발달로 인해 금융거래에 주로 사용하고 있다. 핀테크 환경에서 스마트 폰을 이용한 금융거래에서 PIN 인증이 일반적이다. 하지만, 스마트 폰에서 PIN 입력시 작은 스크린과 어깨 너머 공격 등의 다양한 취약점을 가진다. 특히 PIN 입력시 터치하는 위치에 따른 PIN 유추가 가능하여 안전한 보안 키패드 기법들이 제안되고 있다.

본 논문에서는 생체인증 기법을 적용한 PIN 입력을 통해 편리성과 보안성을 높일 수 있는 1.5-factor 인증을 제안하고자 한다. 생체인증인 지문을 사용하여 안전성을 보장하면서 2~3번의 PIN 입력으로 편리성을 제공할 수 있는 안전한 금융거래가 가능하다.

향후 연구는 제안기법에서 터치의 횟수에 따른 안전성 척도 측정과 인증시 편리성, 안전성 간의 상관관계 분석에 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] G. O. Baik, C. H. Lim & J. G. Shon. (2010). A Virtual Keyboard System for Preventing Keylogging. *Journal of Security Engineering*, 7(4), 319-334.

[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.

[7] D. H. Lee, D. H. Bae, S. L Yoo, J. Y. Chae, Y. Lee & H. G. Yang. (2011). Analysis of safety in secure keypads for smartphone. *Korea Institute of Information Security and Cryptology(KIISC) review,,* 21(7), 30-37. http://www.earticle.net/Public/View/1/730205

[8] Y. H. Lee. (2013). An Analysis on the Vulnerability of Secure Keypads for Mobile Devices. Journal of Korean Society for Internet Information, 14(3), 15-21.

[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] 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

[11] 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

[12] H. J. Kim, H. J. Seo, Y. C. Lee, T. H. Park & H.W. Kim (2013). Implementation of virtual finace keypads with resistance for shoulder surfing attack. *Korea Institute of Information Security and Cryptology (KIISC) review,* 23(6), 21-29. http://www.earticle.net/Public/View/1/846895

[13] S. H. Lee, H. Kim, & D. H. Lee. (2013). Two-Factor Authentication Scheme based on Mobile Messenger with Improved Usability. *Journal of Security Engineering*, 10(5), 549-566.

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