

## VR 상에서의 안전한 PIN 입력 방법 제안

김현준<sup>1</sup> · 권혁동<sup>1</sup> · 권용빈<sup>1</sup> · 서화정<sup>2\*</sup>

### Proposal of Safe PIN Input Method on VR

Hyun-jun Kim<sup>1</sup> · Hyeok-dong Kwon<sup>1</sup> · Yong-bin Kwon<sup>1</sup> · Hwa-jeong Seo<sup>2\*</sup>

<sup>1</sup>Graduate Student, Department of IT Engineering, Hansung University, Seoul 02876, Korea

<sup>2\*</sup>Assistant Professor, Department of IT Engineering, Hansung University, Seoul 02876, Korea

#### 요 약

가상현실 속에서 실제와 같은 서비스를 제공하는 기술 VR(Virtual Reality)은 Head Mounted Display(HMD) 기기를 이용하여 실제와 유사한 체험을 제공한다. 최근 VR의 시장은 커졌으나 가상현실에서의 보안에 대한 연구는 다른 분야에 비해 미흡하다. 현재 VR을 활용한 많은 개인화된 서비스들이 진행되고 있는 만큼 안전한 사용자 인증이 중요하다. VR의 HMD 기기를 착용을 하면 주변 환경을 인식하지 못하기에 Personal Identification Number(PIN) 입력 시에 Shoulder Surfing Attack(SSA)으로 사용자의 입력 패턴을 분석이 용이하다. 본 논문에서는 사용자의 편의성은 그대로 유지하면서 해커가 입력 패턴을 분석하더라도 사용자의 비밀 번호를 안전하게 보호할 수 있는 방법에 대해 제안한다. VR 특성에 맞게 기존 직사각형 모양에서 벗어난 새로운 형태의 가상 키패드와 사용자와 직관적인 상호작용을 위해 자물쇠 오브젝트를 최초로 구현 하였다. 또한 VR의 기존 입력 장치들과 동일한 센서를 사용하는 스마트 글러브와 이에 적합한 회전방식의 PIN입력 방식을 구현하였다. 따라서 총 세 가지의 VR 상에서의 안전한 PIN 입력 방법에 대하여 제안하며 실험을 통해 SSA에 대한 안전성을 검증하였다.

#### ABSTRACT

VR(Virtual Reality), which provides realistic services in virtual reality, provides a similar experience using a Head Mounted Display(HMD) device. When the HMD device is worn, it can not recognize the surrounding environment and it is easy to analyze the input pattern of the user with the Shoulder Surfing Attack(SSA) when entering the Personal Identification Number(PIN). In this paper, we propose a method to safeguard the user's password even if the hacker analyzes the input pattern while maintaining the user's convenience. For the first time, we implemented a new type of virtual keypad that deviates from the existing rectangle shape according to the VR characteristics and implemented the lock object for intuitive interaction with the user. In addition, a smart glove using the same sensor as the existing input devices of the VR and a PIN input method suitable for the rotary type are implemented and the safety of the SSA is verified through experiments.

**키워드** : 가상현실, 가상현실 보안, 립모션, 개인 식별 번호, 스마트 장갑

**Keywords** : Virtual Reality(VR), Virtual Reality Security, Leap Motion, Personal Identification Number(PIN), Smart glove

Received 7 March 2019, Revised 18 March 2019, Accepted 2 April 2019

\* Corresponding Author Hwa-jeong Seo(E-mail:hwajeong84@gmail.com, Tel:+82-2-760-8033)

Assistant Professor, Department of Information System Engineering, Han-Sung University, Seoul, 02876 Korea

Open Access <http://doi.org/10.6109/jkiice.2019.23.5.622>

print ISSN: 2234-4772 online ISSN: 2288-4165

©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.  
Copyright © The Korea Institute of Information and Communication Engineering.

## I. 서 론

최근 스마트폰 시장이 포화 상태에 도달함에 따라 IT 기업들은 새로운 기술을 발굴하는 것이 큰 화두가 되었다. 이에 IT기업들이 주목하는 기술이 가상현실이다. 가상현실이란 컴퓨터 등을 사용한 인공적인 기술로 만들어진 실제와 유사하지만 실제가 아닌 어떤 특정한 환경이나 기술 그 자체를 의미한다[1]. 사용자가 Head Mounted Display(HMD) 기기를 이용한다면 HMD 기기는 가상현실 속에서 음성과 영상을 제공하기 때문에 여러 콘텐츠 서비스를 이용할 때 더욱 몰입감 있게 체험할 수 있다. VR은 여러 분야에서 활용이 가능한데 크게 게임, 교육, 의료, 영상 등 분야에 활용이 되고 있다. 구글의 ‘카드보드’와 삼성전자의 ‘기어VR’ 등의 제품들이 VR 관련 콘텐츠를 제공하고 있으며, ‘오culus 리프트(Oculus Rift)’와 HTC 바이브(Vive)와 같은 VR HMD 제품들이 출시가 되고 있다. 하지만 이런 제품들은 비싼 가격과 구축비용으로 인한 단점이 존재한다. 이런 단점을 보완하기 위해 나온 것이 새로운 놀이시설인 VR 체험존이다. VR 체험존은 소비자들이 일정한 비용만 지불하면 자유롭게 VR 경험을 즐길 수 있는 곳으로 점점 사람들의 이용이 늘어나는 추세이다.

VR이 여러 분야에 활용이 되면서 사용자에게 많은 서비스가 제공이 되고 개인화가 이루어지면서 이제는 VR 상에서 사용자에게 대한 인증이 매우 중요해졌다. 현재 VR 상에서 제공하는 Personal Identification Number(PIN)를 사용하게 되면 VR의 특징상 HMD 기기를 착용을 하면 주변 환경을 인식하지 못하는 취약점으로 인해 해커는 사용자의 어깨너머로 훑쳐보는 공격인 Shoulder Surfing Attack(SSA)를 수행하여 사용자의 PIN 입력 패턴을 분석하게 되면 사용자의 PIN은 고스란히 노출이 된다. 따라서 본 논문에서는 립모션과 스마트 글러브를 활용하여 해커의 shoulder surfing attack을 통한 입력 패턴 분석을 방지하면서 사용자의 편의성을 보장하는 새로운 형태의 PIN 입력 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 VR과 립모션, shoulder surfing attack에 관한 관련 연구 동향에 대해 살펴본다. 3장에서는 안전한 PIN 입력을 위해 립모션과 스마트 글러브를 활용한 제안 기법에 대해 설명한다. 4장에서는 제안 기법에 대한 성능 평가를 수행하도록 하며 5장에서는 본 논문의 결론을 맺도록 한다.

## II. 관련 연구 동향

본 장에서는 제안하고자 PIN 입력 패턴 방법 설명에 앞서 VR, 립모션, shoulder surfing attack에 대해 소개하고 관련 연구 동향에 대해서 알아보도록 한다.

### 2.1. Virtual Reality(VR)

최근 VR을 체험할 수 있는 HMD 기기의 성능이 향상되면서 VR에 대한 관심이 증가하고 여러 분야에서 VR을 활용한 다양한 연구가 진행이 되고 있다.

교육 분야에서는 VR을 사용하여 다양한 교육용 시뮬레이션이 제안되고 있다. 소방안전과 같이 사실적 체험이 필요한 경우 VR을 사용하면 가상의 사고 현장에서 능동적인 학습자가 될 수 있다[2]. 현재 다양한 산업현장에서 Programmable Logic Controller(PLC) 기반으로 생산자동화 시스템을 제어하여 제품 양산이 이루어지고 있기 때문에 산업현장에서는 PLC를 능숙하게 사용할 수 있는 전문 인력과 교육 플랫폼이 필요하다. 그렇기 때문에 가상현실을 접목하여 교육용 V-Factory 시스템이 제안되었다[3].

의료 분야에서도 VR을 활용하여 다양한 연구가 진행되고 있다. 특정 장소나 상황을 싫어하는 증상인 공황장애는 보통 노출훈련이라는 치료 방식을 적용한다. 하지만 노출훈련은 비용, 인력, 시간이 많이 소모되기 때문에 VR 기술을 적용한 노출훈련 시스템을 통하여 환자들의 공황장애를 치료하는 방안이 제안되었다[4]. 뿐만 아니라 뇌졸중을 앓고 있는 환자들을 치료하기 위해 VR을 활용하여 개발한 체감형 가상현실 훈련 시스템이 개발되었고 기존의 훈련 시스템과 비교를 하였을 때 집중력과 시각적 작업에 대한 기억에서 더 큰 향상이 있음이 증명되었다[5].

이처럼 현재 VR은 교육, 의료 분야에서 활발하게 연구되고 있으며 해당 분야가 아니더라도 구현된 오브젝트와 상호작용이 가능하다는 장점은 다양한 분야에서 적용이 될 수 있기 때문에 가상현실에 대한 연구는 더욱 활발해질 것이다. 하지만 가상현실에서의 보안에 대한 연구는 아직 다른 분야에 비해 미흡하다. 현재 가상현실 기기와 게임 시스템의 정보보증을 위해 보안 위협을 식별하였고 이를 보호하는 방법이 제안되었지만[6], 가상현실 기술이 보편화되기 위해서는 보안에 대한 연구는 활발히 진행되어야 할 것이다.

## 2.2. 립모션

사람의 움직임을 컴퓨터의 입력으로 사용하려는 다양한 연구는 마우스와 키패드를 입력장치로 사용하였던 GUI(Graphic User Interface)에서 멀티 터치, 3D 모션 인식과 같은 신체를 활용한 NUI(Natural User Interface)로 패러다임의 변화를 이끌었다. NUI 장치의 일종인 립모션은 사용자의 손동작을 3D 정보로 얻어 컴퓨터의 입력으로 활용할 수 있는 대표적인 제품이다. 초 당 200번 씩 사용자의 동작을 인식할 수 있고 손동작의 변화를 0.01mm까지 있기 때문에 립모션은 VR 기술과 함께 다양한 분야에 활용되고 있다[7].

그 예로 의료 분야에서 수술교육은 장소와 시간의 제약이 심하고 인체해부 실습용 시체를 사용하더라도 실제와 다르기 때문에 어려움이 많다. 이러한 문제점의 해결하기 하고 수술교육에서 좋은 효과를 얻기 위해 VR과 립모션을 이용한 수술 시스템이 제안되었다[8]. 뿐만 아니라 게임 분야의 경우 게임의 개발 환경을 제공하는 게임 엔진인 Unity(유니티)에서 립모션을 인터페이스로 활용하여 게임과 사용자 사이의 상호작용을 증진시키려는 연구가 진행되고 있다. 립모션을 사용함으로써 사용자는 마우스나 키패드보다 더 쉽게 조작이 가능하고, 직접 손으로 움직이면서 게임을 진행하기 때문에 좀 더 몰입이 가능하다[9].

## 2.3. Shoulder Surfing Attack(SSA)

Shoulder Surfing Attack(SSA)이란 어떤 사용자가 사무실이나 사람이 공항, 커피숍과 같은 장소에서 사용하고 있는 기기에 대하여 사용자의 인식이 없는 상태에서 로그인이나 민감한 정보를 볼 때 사용자 주변에서 몰래 엿보는 것을 말한다. 이처럼 어깨너머공격은 사용자의 패스워드를 평문 그대로 볼 수 있기 때문에 원시적이면서 효과적인 공격 수단으로써 강력한 공격방법이다[10].

현금 인출기, 휴대전화 도어락 등등 일반적으로 사용되는 PIN(Personal identification number)은 SSA에 취약하다. 그림 1과 같은 VR의 입력과 유사한 입력방식을 사용하는 구글 글라스에서 SSA가 성공적으로 이루어졌고 이를 효과적으로 방어하고 편의성을 함께 제공하는 보안 키패드가 설계되어 제안되었다[11]. VR상에서도 PIN 입력 시 SSA의 공격에 대한 연구가 필요하다.

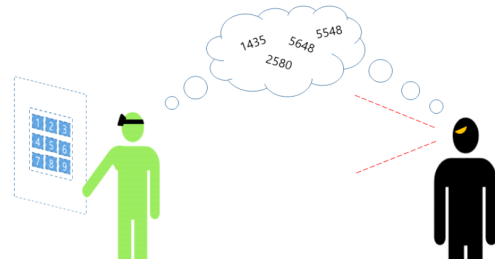


Fig. 1 Hacker doing shoulder surfing attack

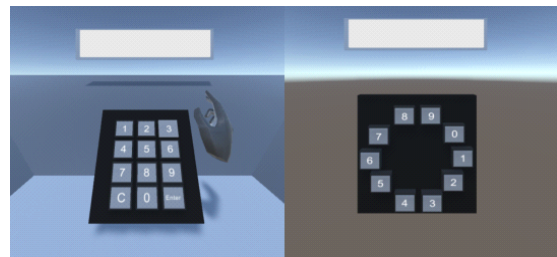


Fig. 2 Left) Traditional keypad Right) keypad to suggest

## III. 제안 기법

본 장에서는 해커가 HMD를 착용하고 있는 사용자를 지켜봐도 사용자의 비밀번호를 알아낼 수 없으며 편의성을 유지하는 기법들에 대하여 소개하고자 한다. 또한 제안 기법에 대한 구현영상<sup>1)</sup>을 Youtube에 올려냈으며, 해당 코드<sup>2)</sup>를 Github에 올려 Open Source화 하였다.

### 3.1. 립모션을 사용한 PIN 입력 방법

립모션을 사용한 첫 번째 방법으로는 키패드 형 PIN 입력 방법이다. 해당 방법에서는 그림 2와 같이 기존의 직사각형 모양의 키패드에서 벗어나 새로운 원 모양의 가상 키패드 입력 방법을 제안하고자 한다.

### 3.2. 스마트 글러브를 사용한 PIN 입력 방법

본 논문에서 사용하기 위해 자체적으로 스마트 글러브를 제작을 하였다. 스마트 글러브는 관성측정장치(Inertial Measurement Unit)와 가변저항방법의 구부림

1) <https://goo.gl/UxAihA>

2) <https://github.com/amdjd/VR-Pin-Input>

센서를 사용하여 손 제스처 데이터를 전송하는 장갑형태의 입력장치이다. IMU 센서를 통해 관성을 측정하여 3차원 공간의 움직임을 사원수(Quaternion)의 형태로 변환하고, 구부림 센서를 통해 각 손가락의 구부림 정도를 각도로 변환하여 블루투스 모듈을 사용하여 정보들을 무선으로 전송하는 장치이다. 구현된 스마트 글러브의 모습은 그림 7과 같으며 사용된 센서들에 대한 설명은 표 1을 통하여 확인할 수 있다.

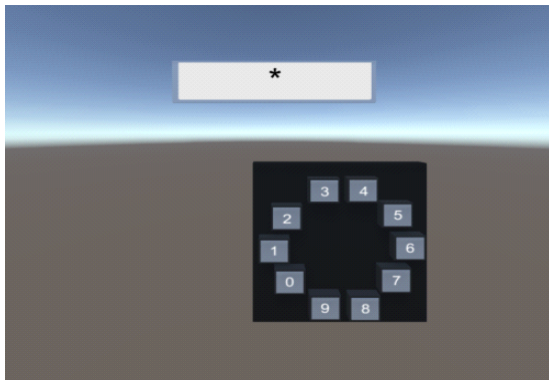


Fig. 3 The location of the keypad and the locations of the numbers are switched when keypad input occurs

제안하는 키패드는 0부터 9까지의 숫자 버튼이 원 모양으로 순차적으로 구성 된다. 초기에 숫자의 배치는 무작위한 순서로 둔다. 사용자가 키패드에 위치한 본인이 입력하고자 하는 숫자를 누르면 그림 3과 같이 키패드의 위치는 사용자가 클릭한 지점을 중심으로 하여 키패드가 다시 배치가 되고 숫자를 무작위하게 회전하여 배치한다. 누르는 지점이 항상 바뀌기 때문에 해커는 입력 패턴을 확인 할 수 없다. 그렇지만 사용자는 숫자가 0부터 9까지 증가하는 패턴은 변하지 않기 때문에 숫자의 위치가 바뀌어도 다음 숫자를 찾기 어렵지 않다.

비밀번호는 관리자의 설정에 따라 4~6자리로 구성이 되며 비밀번호가 일치할 경우에는 패널에 ‘OK’라는 문구가 뜨면서 그림 4의 왼쪽과 같이 인증이 완료되고, 만약 비밀번호가 일치하지 않을 경우에는 패널에 ‘wrong password’라는 문구가 뜨게 되면서 그림 4의 오른쪽과 같이 인증에 실패하게 된다.

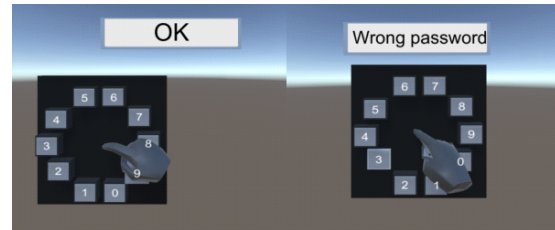


Fig. 4 Left) When a password set by the user is entered, the phrase OK is displayed  
Right) If the password entered is incorrect, the phrase Wrong password is displayed

두 번째 제안하는 방법으로는 현실의 물체인 자물쇠를 구현하여 사용자와 상호작용하는 방법이다. Unity 3D에서 직접 자물쇠 모양의 오브젝트 그림 5와 같이 구현하였다.

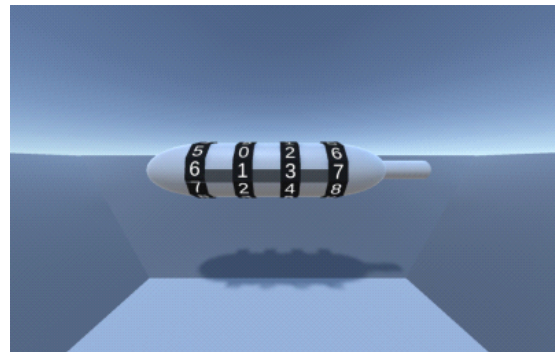
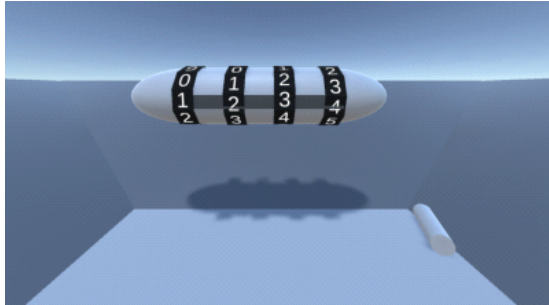


Fig. 5 Implementation of lock object



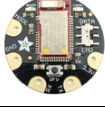
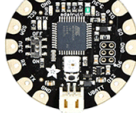
구현된 자물쇠 오브젝트의 초기 숫자들은 무작위하게 위치한다. 사용자는 자물쇠를 돌리는 것처럼 손가락으로 입력하고자하는 숫자를 중앙선에 맞춘다. 숫자의 틀이 동적으로 움직이기 때문에 손의 움직임 정도로는 해커는 숫자를 얼마나 증가 감소시키는지 알 수 없다. 비밀번호와 일치하지 않을 경우 자물쇠는 잠금 상태가 유지되며 비밀번호가 일치할 경우에는 자물쇠의 잠금 상태가 해제되어 그림 6과 같이 사용자는 자신이 입력한 비밀번호가 일치하며 인증이 완료되었음을 확인할 수 있다.





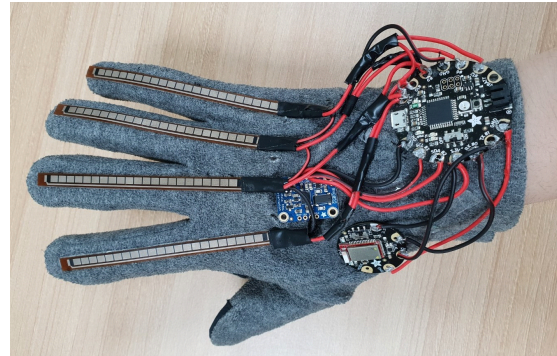
**Fig. 6** If the password set by the user is correct, the lock will open

**Table. 1** Smart gloves implemented using multiple sensors

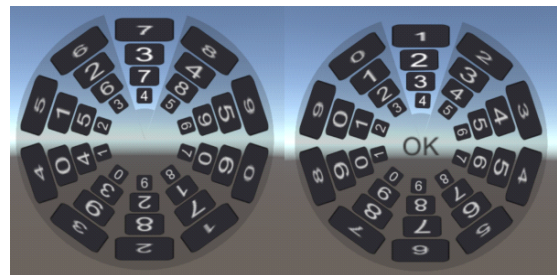
Name	Image	Explanation
IMU sensor		IMU Sensor to measure inertia
Flex sensor		Flex sensor that measures the amount of bend in the finger.
Bluetooth module		Bluetooth Module for wireless communication
Arduino wearable flora		Sensors transmit the measured value to an Arduino wearable flora.

스마트 글러브를 사용하여 PIN을 입력하는 방법에 대해 설명하도록 한다. 그림 8의 왼쪽의 모습처럼 입력틀은 숫자가 0에서 9까지의 순차적으로 위치하고 초기 위치가 무작위한 4개의 원모양의 키패드로 구성된다. 4개의 원 모양의 키패드는 바깥부터 가장 안쪽까지 스마트글러브의 검지에서 소지까지 각각 연결된다. 예를 들어 사용자가 검지를 구부리면 가장 바깥에 있는 원 모양 키패드가 선택되고 다시 펴면 선택이 해제된다. 사용자가 시계 방향 혹은 반시계 방향으로 손을 회전시킬 경우 선택된 모든 키패드는 동일한 방향으로 회전하게 된다. 사용자는 해당 화면에서 12시 방향에 있는 부채꼴 공간 안에 입력하고자 하는 비밀번호를 맞춘다. 원하는 숫자

로 키패드를 이동하고 검지를 뒤로 올리게 되면 입력이 완료된다. 위치된 숫자가 설정한 비밀번호와 일치할 경우 그림 8의 오른쪽과 같이 ‘OK’문구가 가운데 표시되어 인증이 되었음을 확인할 수 있다.



**Fig. 7** Smart gloves implemented using multiple sensors



**Fig. 8** Left) Initial Run Screen  
Right) When user authentication is completed

## IV. 성능 평가

본 장에서는 3장에서 제안한 립모션과 스마트 글러브를 활용한 PIN 입력 방법과 기존의 PIN 입력 방법에 대해 SSA에 대한 안전성을 비교하는 실험을 진행하고 기존 방법과 제안하는 방법에 대한 입력 시간을 측정하고 설문을 통하여서 사용자가 직접 느끼는 편의성을 비교 분석해보도록 한다.

### 4.1. Shoulder Surfing Attack에 대한 안전성

4.1장에서는 기존의 방법과 제안하는 기법이 SSA에 대하여 어느 정도의 안전성을 지니는지 확인하기 위해 각각 기법에 SSA에 안전성 실험을 하였다. 사용자는

HMD를 착용한 상태로 주어진 키패드를 사용하여 비밀번호를 입력하게 된다. 해커는 사용자의 입력 패턴을 분석하여 비밀번호를 도출한다. 해당 실험에서 사용자가 입력하는 비밀번호는 임의로 설정한 비밀번호이며 앞서 설정한 동일한 비밀번호를 입력하는 횟수를 1회부터 5회까지 설정하여 해커가 어느 정도 이상의 횟수 관찰하였을 경우 유사한 비밀번호를 도출할 수 있는지와 도출하였을 경우에 어느 정도의 유사성을 지니는지에 대한 수치적인 평가를 중점으로 실험을 진행하였다. 정확한 내용들은 표 2를 통해 확인하도록 한다.

**Table. 2** Result of shoulder surfing attack on existing virtual keypads

	Password entered by user	Passwords inferred by hackers	Similarity
First Time	4668	5668	75%
Second Time	1680	1580	75%
Third Time	0637	8634	50%
Fourth Time	9542	9542	100%
Fifth Time	3728	3728	100%

**Table. 3** Result of shoulder surfing attack on proposal virtual keypads

	Circul Shape keypad	Lock Object	Smart Glove
First Time	X	X	X
Second Time	X	X	X
Third Time	X	X	X
Fourth Time	X	X	X
Fifth Time	X	X	X

표 2를 통하여 기존의 키패드의 경우에는 1회, 2회 관찰을 통해 사용자의 입력 패턴을 분석하여 비밀번호를 도출하였을 경우에 75%라는 유사성을 보였고 3회 관찰을 통해서 도출한 비밀번호에서는 50%의 유사성을 나타내었다. 또 4회 이상 관찰을 진행하였을 경우에는 도출한 비밀번호에서는 모두 100%의 유사성을 보이는 결과가 나타났다. 이처럼 보안이 적용되지 않은 기존의 키패드의 경우 사용자가 입력한 비밀번호를 유추할 수 있다.

표 3에서 마찬가지로 제안하는 세 가지 방법에도 앞서 수행하였던 실험을 진행해보았다. 하지만 제안한 세 가지 방법 모두 초기에 위치하는 숫자가 무작위하게 주

어지기 때문에 각각의 입력 방법을 분석하더라도 절대 비밀번호를 도출해낼 수 없다. 만약 해커가 비밀번호를 추측하여 맞추려고 한다면 그것은 각 자리 숫자를  $\frac{1}{10}$ 의 확률로 4번이나 맞춰야하는  $(\frac{1}{10})^4$ 의 확률을 가지기 때문에 불가능하다. 만약 관리자가 사용자의 비밀번호를 6자리로 늘린다면 이것은  $(\frac{1}{10})^6$ 의 확률로 늘어나기 때문에 더욱 불가능하게 되어 제안한 기법들은 SSA에 대해 확실한 안전성을 보장한다.

#### 4.2. 실험과 설문을 통한 입력 시간과 편의성 비교

본 논문에서 제시한 3가지 PIN 입력방법과 기존의 방법에 대한 대학생 20명의 집단을 구성하여 실험과 설문을 진행하였다. 실험은 HMD를 착용을 하면 그림 2와 그림 5의 오브젝트가 눈앞에 나와 PIN을 입력하게 되고, 마지막으로 사용자의 스마트 글러브를 착용을 한 상태에서 PIN을 입력하는 것까지 각각 걸리는 시간을 측정하였으며 설문조사는 앞서 실험에서 사용한 제안된 세 가지의 방법들의 보안성과 편의성에 대하여 진행하였다. 측정한 시간의 평균값은 표 4를 통하여서 확인할 수 있다.

**Table. 4** Average input time per keypad

	Basic keypad	Circle shape keypad	Lock Object	Smart Glove
Time	21.08s	14.21s	38.98s	16.37s

표 4를 통해 입력하는데 걸리는 시간들을 확인해보면 원 모양 키패드가 14.21초로 가장 빠른 입력 시간을 보였으며 그 뒤를 이어 스마트 글러브를 통한 입력 속도가 16.37초로 비슷한 시간이 걸리는 것을 확인할 수 있었다. 또 세 번째로는 기존의 키패드가 21.08초가 걸렸으며 마지막으로 자물쇠 오브젝트는 38.98초가 소요되었음을 확인할 수 있다. 해당 실험의 결과를 통하여 기존의 제안되었던 세 가지의 입력 방법 중 원 모양 키패드와 스마트 글러브를 사용한 입력 방식은 기존의 키패드와 비교했을 때 훨씬 더 빠른 입력 속도를 보였다. 하지만 자물쇠 오브젝트의 경우 기존의 키패드와 비교하였을 때 다소 느린 입력 속도를 보여주었다.

**Table. 5** Results of security survey of proposed methods

	very Best	best	so so	worst	very worst
Security	60%	40%	0%	0%	0%

**Table. 6** Results of convenience survey of proposed methods

	YES	NO
Convenience	80%	20%

앞서 언급하였던 대학생 집단에게 진행한 설문조사의 결과는 표 5와 표 6을 통해 확인할 수 있으며 제안된 방식이 기존의 방식과 비교하여 안전하다고 생각하는 지에 대한 질문에서 ‘매우 그렇다’라고 대답한 의견은 60%로 매우 높게 나타났으며 ‘그렇다’라는 의견은 40%로 나타난 것을 통해 보안성의 측면에서도 사용자들에게 긍정적인 평가를 받았음을 알 수 있다. 또한 기존의 방식과 비교하였을 때 제안된 방식이 기존의 방법과 비교하였을 때 편리한지에 대한 질문에서 ‘그렇다’라는 의견은 80%를 차지하였고 ‘아니다’라는 의견은 20%를 차지하였다.

설문과 통하여서 사용자들에게 제안된 기법이 보안성과 편의성에서 기존 방식에 비하여 안전하고 편리하다는 평가를 받았다. 자물쇠 오브젝트 방식은 다른 방식에 비하여 낮은 입력 속도를 통해 편의성이 떨어짐을 보였지만 자물쇠 오브젝트는 시각적인 자극에 민감한 어린 아이들에게 직접 상호작용할 수 있는 교육용 자료로 사용한다면 효과적인 교육을 진행할 수 있을 것이라는 평가가 있었다. 또한 다수의 평가자들로부터 제안한 방법들이 재미있는 놀이 같다는 평가를 받았다.

## V. 결 론

기존의 PIN 입력 방법들은 해커가 SSA를 통해 사용자의 패터를 파악하면 비밀번호가 쉽게 노출된다는 취약점을 가지고 있었다. 이러한 취약점은 본 논문에서 진행한 성능평가에서도 나타났으며 취약점을 보완하기 위해 본 논문에서는 립모션과 Unity 3D를 활용하여 기존의 직사각형 모양에서 벗어난 VR 특성에 맞게 기존의 직사각형 모양에서 벗어난 새로운 형태의 가상 키패드

와 사용자와 직관적인 상호작용을 위해 자물쇠 오브젝트를 최초로 구현 하였다. 또한 VR의 기존 입력 장치들과 동일한 센서를 사용하는 스마트 글러브와 이에 적합한 회전방식의 PIN입력 방식을 구현하였다. 총 세 가지의 VR 상에서의 안전한 PIN 입력 방법에 대하여 제안하였다. 제안한 방법들은 실험을 통해 SSA에 대한 안전함과 설문을 통해 기존 방식보다 보안성과 편의성이 뛰어남을 검증하였다.

설문조사의 의견 중 제안한 방법들이 재미있는 놀이 같다는 평가가 있었다. 아직 비밀번호에 대한 중요성을 인지하지 못하는 어린 초등학생들은 개인 정보노출의 위험이 높은 만큼 본 논문에서 제안한 방법들을 교육적인 용도로 활용한다면 어린 아이들의 비밀번호 인식 개선에 크게 도움이 될 것이라고 생각한다. 앞으로 VR 상에서의 보안에 대한 연구가 활발히 진행되기를 기대한다.

## ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017 R1C1B5075742) and was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). This research of Hwajeong Seo was financially supported by Hansung University.

## References

- [1] E. J. Song, "A Study on Training System for Fire Prevention based on Virtual Reality," *Digital Contents Society*, vol. 17, no. 3, pp. 189-195, Jun. 2016.
- [2] Y. K. Chung, "Development of VR Fire-extinguishing Experience Education Contents Using UX Design Methodology," *The Korea contents society*, vol. 17, no. 3, pp. 222-230, Mar. 2017.
- [3] K. J. Seo, J. H. Yun, K. S. Nam, and S. G. Kim, "Development of the Educational V-Factory system

- combining Virtual Reality,” *The Korea Academia-Industrial cooperation Society*, vol. 19, no. 4, pp. 617-622, Apr. 2018.
- [ 4 ] Y. M. Lee, J. A. Park, S. H. Lee, S. J. Kim, and J. K. Lee, “Development of Anxiety Measuring App and VR System for Panic Disorder Exposure Training,” *KIISE Transactions on Computing Practices*, vol. 24, no. 5, pp. 227-233, May. 2018.
- [ 5 ] N. Y. Yang, H. S. Park, T. H. Yoon, and J. H. Moon, “Effectiveness of Motion-Based Virtual Reality Training (Joystim) on Cognitive Function and Activities of Daily Living in Patients with Stroke,” *Rehabilitation Engineering And Assistive Technology Society of Korea*, vol. 12, no. 1, pp. 10-19, Feb. 2018.
- [ 6 ] T. U. Kang, and H. K. Kim, “VR Threat Analysis for Information Assurance of VR Device and Game System,” *Korea Institute of Information Security & Cryptology*, vol. 28, no. 2, pp. 437-447, Apr. 2018.
- [ 7 ] Y. H. Kong, and W. C. Lee, “Motion Control System for a Robotic Manipulator Using Leap Motion,” *Korean Institute of Information Technology*, vol. 14, no. 12, pp. 1-6, Dec. 2016.
- [ 8 ] B. H. Kang, J. S. Kim, and H. W. Kim, “Study for Operation Teaching Machine Using 3D Virtual Reality System,” *Digital Contents Society*, vol. 17, no. 4, pp. 287-293, Aug. 2016.
- [ 9 ] M. J. Kim, J. M. Heo, J. H. Kim, S. Y. Park, and J. H. Chang, “Development and Evaluation of Leapmotion-based Game interface considering Intuitive Hand Gestures,” *The Korean Society for Computer Game*, vol. 27, no. 4, pp.69-75, Dec. 2014.
- [10] S. H. Kim, M. S. Park, and S. J. Kim, “Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes,” *The Korea Institute of Information Security & Cryptology*, vol. 24, no. 6, pp. 1159-1174, Dec. 2014.
- [11] H. J. Seo, and H. W. Kim, “Design of Security Keypad Against Key Stroke Inference Attack,” *The Korean Institute of Information Security & Cryptology*, vol. 26, no. 1, pp. 41-47, Feb. 2016.



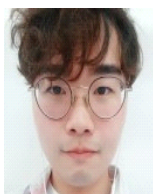
김현준(Hyun-jun Kim)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사  
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정  
※관심분야: 블록체인, 인공지능



권혁동(Hyeok-dong Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사  
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정  
※관심분야: 블록체인, 암호구현



권용빈(Yong-bin Kwon)

2018년 7월: 한성대학교 IT응용시스템공학과 공학 학사  
2018년 8월~현재: 한성대학교 IT융합공학과 석사과정  
※관심분야: 블록체인, 머신러닝



서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업  
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업  
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업  
2016년 1월~2017년 3월: 싱가포르 과학기술청  
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수  
※관심분야: 정보보호, 암호화 구현, IoT