JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 11 : 2109~2114 Nov. 2017

스마트폰과 스마트워치를 활용한 사용자 인증 기법

서화정*

User Authentication Method Using Smartphone and Smartwatch

Hwa-jeong Seo*

Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

개인 식별 번호는 개인화된 그리고 상업적인 서비스 상에서의 사용자 인증에 가장 보편적으로 사용되는 기술이다. 따라서 사용자는 자신이 사용하고자 하는 서비스에 접근할 때 PIN 정보를 입력하고 사용자 인증을 수행해야 한다. 하지만 개인 식별 번호 입력과정은 사용자가 매번 입력을 해야 하는 부담감을 줄 뿐 아니라 공격자가 어깨너머공격을 시도할 경우 보안이 취약해 지는 문제점을 가지고 있다. 이러한 문제점을 해결하기 위해 스마트폰과 스마트워치를 이용한 인증 기법을 소개한다. 먼저 기존의 기법에서 스마트워치의 센서 정보만을 통해 분석하는 경우의 문제점에 대하여 확인해보았다. 이를 바탕으로 스마트폰과 스마트워치 모두에서 사용자의 센서 정보를 수집하고 이를 통해 인증하는 방법을 제안하였다. 만약 관찰된 가속도 센서 정보가 높은 연관성을 보이게 될 경우 사용자 인증이 성공적으로 이루어지게 된다. 인증 기법에 대한 테스트를 위해 삼성 갤럭시 노트5와 소니 스마트워치2를 사용하였다.

ABSTRACT

Personal Identification Number (PIN) is the most common user-authentication method for the access control of private and commercial applications. The users need to enter PIN information to the applications whenever the users get access to the private services. However, the process imposes a burden on the users and is vulnerable to the potential shoulder-surfing attacks. In order to resolve both problems, we present a continuous authentication method for both smartphone and smartwatch, namely, synchronized authentication. First we analyze the previous smartwatch based authentication and point-out some shortcomings. In the proposed method, we verify the validity of user by analyzing the combined acceleration data of both smartphone and smartwatch. If the monitored sensor data shows the high correlations between them, the user is successfully authenticated. For the authentication test, we used the Samsung Galaxy Note5 and Sony Smartwatch2.

키워드 : 인증, 개인 식별 번호, 가속도 센서, 스마트폰, 스마트워치

Key word : Authentication, Personal Identification Number, Acceleration Sensor, Smartphone, Smartwatch

Received 11 June 2017, **Revised** 15 June 2017, **Accepted** 25 June 2017

* **Corresponding Author** Hwa-jeong Seo(E-mail:hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)
Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.11.2109 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

스마트폰과 스마트워치는 현재 대중적으로 널리 사용되는 IT 기기로써 사용자는 해당 장비를 이용하여 언제 어디서나 인터넷 접근이 가능하다. 사용자는 인터넷을 통해 다양한 서비스를 활용하게 되는데 현재 이러한 서비스는 사용자의 개인적이고 민감한 정보를 포함할 수도 있다. 만약 이러한 정보가 악의적인 공격자에 의해 도청당하고 악용되는 경우 이는 사용자에게 큰 금전적 혹은 정신적 피해를 입힐 수 있다. 따라서 악의적인 공격자에 의해 정보가 누출되는 것을 막기 위해 서비스에 대한 접근은 안전하게 관리되어야 한다. 이러한 서비스 접근에 가장 많이 사용되는 기법은 개인 식별 번호 기반 사용자 인증이다. 사용자는 사용자 인증을 성공하기 위해 숫자로 된 비밀번호를 플랫폼을 통해 전송하게 된다. 사용자가 사용하는 플랫폼의 특징에 따라 다양한 개인 식별 번호 기반 사용자 인증이 제안되고 있다. 전통적으로 개인 식별 번호는 키보드 혹은 마우스를 통해 전달되었다.

하지만 최근에 많이 사용되는 스마트폰과 스마트워치의 경우에는 사용자가 입력에 사용하는 터치 스크린의 크기가 매우 작아서 입력이 어려운 문제점을 가진다. 또한 스마트폰과 스마트워치의 경우 이동형 장비라는 특징 때문에 공공장소에서 사용시 공격자가 어깨너머 공격을 통해 사용자의 비밀번호를 훔쳐볼 수 있는 문제점을 가지고 있다. 따라서 두 장비 상에서 보안성과 편의성을 제공하는 사용자 인증 기법에 대한 연구가 필요하다. 본 논문에서는 스마트폰과 스마트워치가 가지고 있는 가속도 센서를 이용하여 상호간의 동기화된 패턴을 확인하고 이를 이용하여 사용자를 인증하는 방안을 제시 하겠다. 해당 기법의 효용성을 확인해보기 위해 Samsung Galaxy Note5와 Sony Smartwatch2 상의 가속도 정보를 분석하였다.

본 논문의 구성은 다음과 같다. 2장에서는 이전 연구 결과에 대해 확인해 보고 해당 기법들의 특징 및 개선 사항에 대해 알아보도록 한다. 3장에서는 제안하는 기법의 특징에 대해 확인해 보도록 한다. 4장에서는 제안하는 기법을 실제 타겟 플랫폼 상에서 실험한 결과를 확인해 보도록 한다. 마지막으로 5장에서는 해당 논문의 결론을 내린다.

Ⅱ. 관련 연구

스마트 폰 상에서의 안전한 사용자 인증을 위해 오디오 그리고 진동 정보를 기반으로 어깨너머 공격을 방지하는 방안이 제시 되었다 [1]. 해당 기법에서는 화면 상에 10개의 숫자가 표기되고 매 입력 시기마다 무작위로 시작 정보가 결정되고 해당 정보는 오디오 채널을 통해 사용자에게만 안전하게 전달되도록 하였다. 악의적인 공격자는 난수화된 값에 대한 접근이 불가능하기 때문에 시각 정보를 활용한 어깨너머공격을 효과적으로 방어할 수 있는 장점을 가진다.

이후에는 오디오 채널의 정보를 통한 인증 기법을 조금 더 개선하여 최소한의 오디오 채널을 사용자에게 전달해 주고 해당 정보로부터 비밀정보를 이끌어 내는 방법이 제안되었다. 해당 기법은 화면 상에 있는 특정한 문자 혹은 숫자를 비밀정보로 알려주고 해당 정보와 특수한 형식으로 디자인된 키패드를 이용하여 안전하게 비밀 값을 입력하는 방안을 제시 하였다 [2]. 하지만 해당 방식도 사용자의 눈 초점을 분석함으로써 해킹가능하다는 것이 증명되었다 [3]. 이러한 어깨너머 공격을 방지하기 위해 증강현실 플랫폼인 구글 글라스가 최근에 적용 되었다 [4]. 해당 논문에서는 구글 글라스를 착용한 사용자만이 볼 수 있는 비밀정보를 이용하여 효과적으로 어깨너머 공격을 방지하는 방안을 제시 하였다. 최근에는 새로운 IoT 플랫폼인 스마트 워치의 가속도 정보와 스마트 폰의 입력 정보를 기반으로 사용자를 인증하는 방안이 제시 되었다 [5]. 해당 기법에서는 사용자가 화면에 입력하는 값과 연관성이 있는 가속도 패턴이 스마트 워치에서 관찰될 경우 사용자임을 인증하는 기술이 사용되었다.

하지만 해당 논문에서는 사용자가 특정 개인 식별 번호 혹은 입력을 하는 경우에만 사용자 인증이 가능하도록 하였다. 이는 사용자의 다양한 입력 패턴을 고려해야 하기 때문에 실제 사용에는 많은 제약이 따른다. 또한 해당 기법에 대한 실험 결과를 명시적으로 제시하고 있지 않아 장·단점을 도출하는데 어려움이 있다. 따라서 본 논문에서는 사용자가 스마트 워치를 착용하고 스마트폰을 이용할 때 스마트폰과 스마트워치 간에 동기화된 가속도 패턴을 발생시켜 사용자를 간편하게 인증하는 방안에 대해 확인한다. 또한 이전 연구의 결과를 실제로 테스트 해보아 해당 기법과 제안하는 기법의 장

단점에 대해서도 확인한다.

Ⅲ. 제안하는 기법

스마트폰에 정보를 입력 시 우리는 보통 스마트폰 스크린에 나타나는 가상 키보드를 활용하게 된다. 해당 가상키보드를 통해 문자 혹은 숫자를 입력하기 위해서는 해당 값이 위치한 가상키보드를 클릭함으로써 가능하다. 최근에는 이러한 사용자의 입력 방식을 기반으로 사용자의 입력값을 역추적하는 방안이 제시 되었다 [6]. 만약 사용자가 스마트 워치를 착용하고 개인 식별 번호를 입력하는 경우 스마트 워치에서 생성되는 가속도 정보를 해커가 탈취하게 된다면 기존의 암호화 강도가 99.99% 감소하게 됨을 확인할 수 있었다. 본 논문에서는 해당 해킹 기법이 사용하고 있는 스마트 워치와 사용자 인증이 필요한 스마트 폰 상의 가속도 정보를 사용자 인증에 이용하는 방안에 대해 확인한다.

먼저 최신 스마트폰과 스마트워치의 경우에는 사용자의 모든 움직임을 확인하는 것이 가능한 다양한 센서들이 탑재되어 있다. 그 중에서도 본 논문에서는 가속도 센서의 특이점을 통해 사용자를 인증한다. 제안하는 사용자 인증 방식은 사용자가 스마트 워치를 착용한 손으로 스마트 폰을 흔들어서 스마트 워치와 스마트 폰 사이에 동일한 가속도 패턴이 발생하도록 하는 것이다. 만약 두 개의 플랫폼 상에서 동일한 가속도 패턴이 일정한 기준 이상으로 나타나는 경우에는 사용자 인증이 되도록 하는 것이다. 여기서 생성되는 가속도 패턴의 경우 X, Y, Z 방향으로 무작위 값이 나타내게 된다. 이는 스마트폰을 흔드는 사용자의 경우 약속되어진 패턴보다는 사용자의 의지에 따라 무작위로 흔들어지게 되고 독특한 패턴이 나타나게 된다. 따라서 X, Y, Z 방향에 따른 패턴에 따라 사용자를 인증하기 보다는 흔들림이 발생할 때 생성되는 가속도 정보를 이용하여 해당 정보가 상호간에 동기화된 경우에만 사용자 인증이 되도록 하였다. 이는 스마트 워치와 스마트 폰의 가속도 센서가 장착된 위치에 따라 가속도의 방향이 서로 바뀌어 나타나는 것을 보완하는 방안이다. 따라서 가속도 각각의 값을 통해 사용자를 인증하는 방안보다는 전체 크기로 현재 패턴을 판단하기 위해 전체 가속도의 합을 다음 $P = \sqrt{x^2 + y^2 + z^2}$ 식으로 계산하여 두 스마트 기기의 패턴을 비교하였다.

여기서 사용자가 스마트워치의 가속도 패턴을 사용자 인증에 사용 가능한 이유는 스마트폰이 스마트워치와 페어링을 하는 경우 상호간에 안전하게 키교환이 이루어 지게 되고 이는 상호간에 안전한 인증을 수행하기 때문에 현재 스마트 워치를 착용한 사람이 사용자임을 확인할 수 있다. 이때 두 플랫폼 상에서 유사한 가속도 패턴이 나오게 되는 경우 이를 이용하여 안전하게 사용자 인증이 가능하다.

Ⅳ. 제안기법 실험

본 논문에서 테스트를 위해 선택한 스마트 폰은 Samsung Galaxy Note5로써 2015년에 출시된 모델이다. 현재 사용가능한 Note 중 진보된 모델 중 하나로써 보편적으로 많이 사용되고 있다. 화면의 크기는 5.7 인치이며 1440X2560 픽셀을 가진다. 제공하는 센서로는 자이로 센서, 근접 센서, 방향 센서, 걸음 센서, 심장박동 센서 그리고 가속도 센서가 있다.

스마트 워치의 경우에는 2014년도에 출시된 Sony SmartWatch2을 사용하였다. 해당 장비의 무게는 76 그램이며 스크린 크기는 1.6인치이다. 해당 스마트 워치는 GPS 센서, 자이로 센서, 방향 센서, 걸음 센서, 그리고 가속도 센서가 장착되어 있다. 안드로이드 웨어를 통해 안드로이드 스마트폰과 페어링이 쉽게 가능하다. 두 장비 상에서의 가속도 센서 정보를 추출하기 위해 안드로이드와 안드로이드 웨어 애플리케이션을 사용하였다. 스마트폰의 가속도의 경우 Sensor Kinetics Pro 프로그램을 통해 정보 추출이 가능하였으며 스마트 워치의 경우에는 SensorRec for Android Wear Pro을 통해 가속도 정보를 추출가능하다.

먼저 [1]에서 제안된 사용자 인증 기법을 본 실험환경에서 테스트하였다. 해당 테스트를 위해 사용자가 스마트 워치를 착용하고 있고 스마트 폰으로는 특정한 값을 입력하고 있다고 가정하였다. 만약 스마트 워치에서 스마트폰에 값을 입력하는 가속도 패턴이 관찰되고 스마트폰이 입력을 받고 있다면 적법한 사용자가 스마트폰을 사용하고 있음을 확인할 수 있다. 해당 사용자 인증 기법은 스마트워치를 착용한 손목과 스마트폰을 들고 있는 손의 위치에 따라 총 4가지 시나리오로 생각해

볼 수 있다. 그림 1에는 가능한 4가지 시나리오를 나타내고 있다. 먼저 (a)의 경우에는 오른손으로 스마트폰을 잡고 있고 스마트워치를 착용한 왼손으로 스마트폰에 입력을 하는 경우를 나타낸다. (b)의 경우에는 반대로 오른손으로 스마트폰을 잡고 있고 왼손 손목에 스마트 워치를 착용하고 스마트폰에 입력을 하는 경우를 나타낸다. 나머지 (c)와 (d)의 경우 한손으로 스마트폰을 잡고 입력을 하는 경우를 나타내고 있다. 차이점은 (c)의 경우 스마트 워치를 착용하지 않은 손으로 스마트폰에 입력을 하는 경우이며 (d)의 경우 스마트 워치를 착용한 손으로 입력을 하는 경우를 나타낸다. 총 4가지 시나리오 중 사용자 인증이 어려운 경우는 (c)에 해당한다. 그 이유는 스마트 워치를 착용한 손에서 입력과 관련된 가속도 정보를 받아올 수 없기 때문이다.

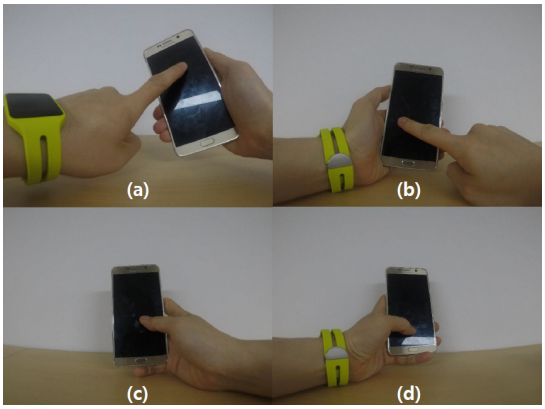

Fig. 1 Four typing scenarios with smartphone and smartwatch

그림 2에는 스마트 폰에 값을 입력하는 순간에 스마트 워치에서 감지되는 가속도 패턴을 나타내고 있다. 첫 번째 경우에는 스마트 워치를 착용한 손을 통해 스마트 폰에 직접 입력을 하게 되는 것을 나타내고 있다. 스마트폰에 입력을 하기 위해 스마트 워치를 착용한 손이 상하좌우로 움직이기 때문에 가속도들의 변동폭이 크게 나타난다. 두 번째 패턴의 경우에는 스마트 워치를 착용한 손으로 스마트폰을 들고 있는 경우를 나타낸다. 해당 경우에는 스마트 폰이 눌려지는 순간에 간접적인 입력 진동이 스마트워치를 착용한 손에 전달되고 해당 정보가 기록되는 방식으로 측정되었다. 하지만 첫 번째 경우에 비해 가속도의 변동폭이 작게 나타나는데 그 이유는 스마트폰이 움직이지 않도록 손으로 고정하고 있는 상황에서 전달되는 가속도 패턴이 작게 나타나기 때문이다. 마지막으로 스마트 워치를 착용한 손으로 스마트폰을 조작하는 경우를 나타낸다. 해당 경우에는 입력을 하기 위해 스마트 워치를 착용한 손을 움직여야 하기 때문에 해당 변동값이 가속도 그래프에 나타나게 된다.

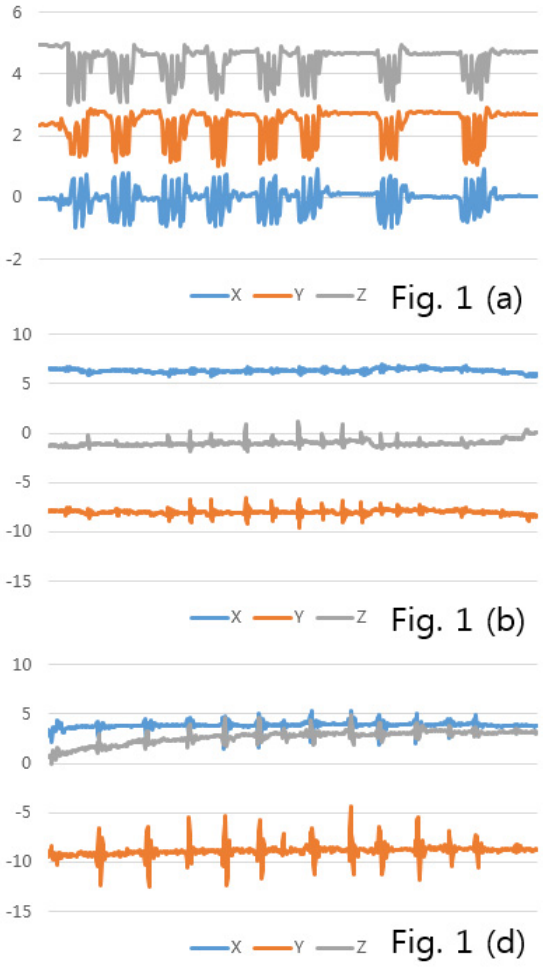

Fig. 2 Accelerometer pattern in smartwatch when the user entered the input to the smartphone

그림 3에서는 본 논문에서 제안하는 기법으로써 스마트 워치를 착용한 손으로 스마트폰을 쥐고 흔들어서 가속도 패턴을 생성하게 된다. 해당 경우에는 스마트폰

과 스마트워치에서 비슷한 가속도 크기의 패턴이 관찰됨을 확인하는 방식으로 사용자를 인증하게 된다.

Fig. 3 Synchronized moving

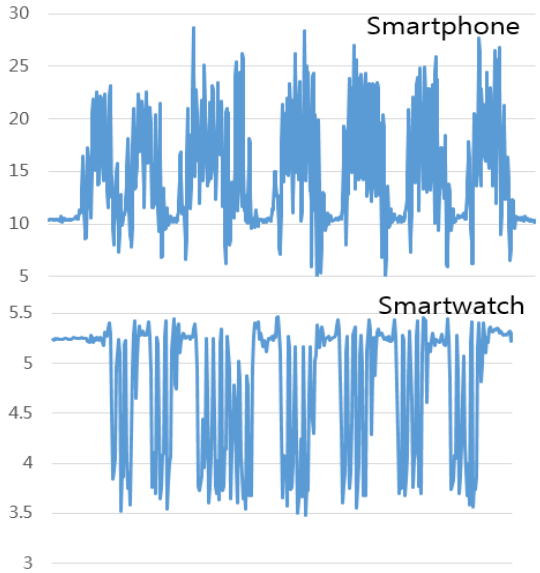

Fig. 4 Accelerometer pattern in smartphone and smartwatch when the user shake the smartphone

그림 4에서는 제안하는 방식을 통해 도출된 가속도 값의 변동추이를 나타내고 있다. 그림 2에서 이전 연구 결과에 대한 가속도의 변동폭과 비교해 볼 때 제안하는 방안의 경우에는 보다 쉽게 입력 패턴에 대한 구별이 가능하다. 변동폭이 짧은 경우에는 사용자의 가속도 정보를 통해 사용자 인증 시 잘못된 판단으로 사용자를 인증하게 되는 문제를 발생시킬 수 있다. 반면에 제안하는 기법은 보다 명확하게 패턴 확인이 가능하다.

표 1에서는 스마트 워치 상에서 관찰되는 가속도 패턴의 크기에 대해 비교하여 나타내고 있다. 특히 크기가 약 2 이상 차이가 나게 되는 경우에 대해서는 가속도 패턴이 잘 관찰된다고 판단하여 High로 정의하였으며 그렇지 않은 경우에는 Low로 정의하여 나타내었다. 먼저 입력 패턴을 이용하여 사용자를 인증하는 이전 기법의 경우에는 스마트워치를 착용한 손으로 스마트 폰을 입력하는 경우에 가장 패턴이 잘 나타났다. 그리고 스마트 워치를 착용한 손이 아무런 가속도 정보를 받을 수 없는 그림 1의 (c) 경우에는 가속도 패턴을 확인할 수 없다. 이는 가속도 패턴을 추출할 수 있는 방안이 없기 때문이다. 그 외에 그림 1의 (b)의 경우와 그림 1의 (d)의 경우에는 간접적으로 스마트워치에서 입력되는 패턴을 찾을 수 있었지만 그 값이 사용자 인증에 사용하기에는 미약하다는 것을 확인할 수 있었다. 반면에 제안하는 가속도합의 패턴 동기화 기반 사용자 인증의 경우, 스마트 워치와 스마트 폰 모두에서 선명하게 가속도 패턴이 관찰된다. 따라서 해당 기법은 사용자 인증에 사용 시 보다 낮은 오차율을 제공한다. 그 이유는 가속도 패턴의 크기의 대비가 모다 명확히 제시되고 있기 때문이다.

Table. 1 Observation of accelerometer pattern in smartwatch

Method	Accelerometer pattern
Fig. 1 (a)	High
Fig. 1 (b)	Low
Fig. 1 (c)	None
Fig. 1 (d)	Low
Fig. 3	High

본 논문에서 제안된 기법은 기존의 사용자 인증 기법과 혼용하여 사용함으로써 사용자 편의성을 증대시키는 방향으로 발전시킬 수 있다. 최근에 발표된 논문에서는 사용자가 접근하는 정보의 민감도에 따라 사용자 인증 과정을 다르게 하여 사용자 편의성을 높이는 방안이 제시되었다 [7]. 이처럼 본 논문에서 이전 스마트워치 기반 사용자 인증 기법을 지속적인 인증 기법으로 적용을 하다가 사용자가 정말 민감한 정보에 접근하는 시도가 발생하는 경우 패턴이 명확하게 나타나는 제안하는 방안을 적용하게 된다면 편의성과 보안성

모두를 향상시킬 수 있다. 추후 연구로는 제안된 안전한 사용자 인증 기법을 실제 서비스 시스템에 접목하는 것이다 [8].

Ⅴ. 결 론

본 논문에서는 스마트폰과 스마트워치 상의 가속도 정보를 활용한 사용자 인증 기법에 대해 확인해 보았다. 먼저 사용자가 입력하는 행위가 스마트폰과 스마트워치에서 동기화되어 나타나는 특징을 이용한 이전 방안의 특징에 대해 확인해 보았다.

이를 바탕으로 제안된 기법에서는 스마트워치를 착용한 손으로 스마트폰을 잡고 흔들어 동기화된 가속도 패턴을 생성해 냄으로써 인증하도록 하였다. 해당 기법은 실제 디바이스 상에서 실험되었으며 그 실효성에 대해 확인해 볼 수 있었다. 추후 연구로는 생성되는 가속도 정보를 대량으로 수집하여 해당 빅데이터에 대한 머신러닝을 통해서 정확히 상황을 판단해 내는 방안에 대해 확인해 볼 예정이다.

ACKNOWLEDGMENTS

"This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2014-0-00743) supervised by the IITP(Institute for Information & communications Technology Promotion)"

REFERENCES

[1] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: audio and haptic shoulder-surng resistant PIN entry methods for mobile devices," *In Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, Funchal, pp. 197-200, 2011.

[2] M. Lee, H. Nam, and D. Kim, "Secure bimodal PIN-entry method using audio signals," *Computers & Security*, vol. 56, pp. 140-150, Feb. 2016.

[3] H. Seo and H. Kim, "Hidden Indicator Based PIN-Entry Method Using Audio Signals," *Journal of information and communication convergence engineering*, vol. 15, no. 2, pp. 91-96, June 2017.

[4] H. Seo, Z. Liu, J. Kim, and H. Kim, "Personal identification number entry for Google glass," *Computers & Electrical Engineering*, vol. 63, pp.160-167, May 2017.

[5] J. Ranjan and K. Whitehouse, "Automatic authentication of smartphone touch interactions using smartwatch," *In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, Heidelberg, pp. 361-364, 2016.

[6] H. Seo, Z. Liu, G. Seo, T. Park, J. Choi, and H. Kim, "Open sesame! hacking the password," *In International Workshop on Information Security Applications*, Jeju, pp. 215-226, 2015.

[7] D. Buschek, F. Hartmann, E. Von Zezschwitz, A. De Luca, and F. Alt, "Snapapp: Reducing authentication overhead with a time-constrained fast unlock option," *In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose, pp. 3736-3747, 2016.

[8] Y. Zhong, B. Bhargava, Y. Lu, P. Angin, "A Computational Dynamic Trust Model for User Authorization," *Asia-pacific Journal of Convergent Research Interchange, HSST*, vol. 1, no. 4, pp. 1-6, Dec. 2015.

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