Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.361

안드로이드에서 앱 사용과 터치 정보를 이용한 행위 기반 사용자 인증 기술 연구*

김 민 우,[1†] 김 승 연,[2] 권 태 경[2‡]
[1]SK 주식회사, [2]연세대학교

A Study of Behavior Based Authentication Using Touch Dynamics and Application Usage on Android*

Minwoo Kim,[1†] Seungyeon Kim,[2] Taekyoung Kwon[2‡]
[1]SK Holdings, [2]Yonsei University

요 약

스마트폰 기기 내에 저장되는 사용자 정보가 다양화되어 개인정보에 대한 위협도 함께 증가하고 있다. 패턴 잠금, 지문 인식 등 다양한 사용자 인증 기술이 스마트폰에 적용되어 있으나 사용자 의존적, 거부감 유발 등의 한계점을 보이고 있다. 최근 주목받고 있는 행위 기반 인증은 기기 사용과 동시에 인증이 가능하여 사용자에게 높은 편의성을 제공하나 타 인증 기술에 비해 정확도가 낮아 이를 개선하기 위한 연구가 꾸준히 수행되고 있다. 본 연구에서는 이전 연구에서 고려되지 않았던 앱 사용 정보를 새로운 인증 요소로 활용하는 방법을 제안한다. 또한 실제 앱 사용 상황을 고려한 데이터 수집 및 분석을 통해 제안 기술의 성능을 상세하게 분석한다.

ABSTRACT

The increase in user data stored in the device implies the increase in threats of users' sensitive data. Currently, smartphone authentication mechanisms such as Pattern Lock, fingerprint recognition are widely used. Although, there exist disadvantages of inconvenience use and dependence that users need to depend on their own memory. User behavior based authentication mechanism have advantages of high convenience by offering continuous authentication when using the mobile device. However, these mechanisms show limitations on low accuracy of authentication and there are researches to improve the accuracy. This paper proposes improved authentication mechanism that uses user's smartphone application usage pattern which has not considered on earlier studies. Also, we analyze performance of proposed mechanism with collected datasets from actual use of smartphone applications.

Keywords: Android, Behavior Based Authentication, Application Usage, Touch Dynamic, Machine Learning

I. 서 론

스마트폰은 전화, 메시지 기능뿐만 아니라 소셜 네트워크, 금융 거래, 네트워크 통신 등 서비스 영역이 확장되어 사용자의 편의성을 증가시키고 있다. 그러나 편의성 증가와 동시에 보안과 개인정보에 대한 위협도 증가하고 있다. 예를 들어 스마트폰을 분실하면 공격자는 기기 내에서 사용자의 다양한 정보를 획득할 수 있게 되었다. 이를 예방하기 위해서는 안전한 사용자 인증 기술을 적용하여 인증된 사람만이 기

Received(02. 27. 2017), Modified(03. 31. 2017), Accepted(03. 31. 2017)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2017-2016-0-00304)
† 주저자, mu.kim@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

기 내 정보에 접근할 수 있도록 해야 한다.

현재 스마트폰에는 PIN, Pattern Lock, OTP 등 다양한 인증 기술이 사용되고 있지만, 안전성을 사용자에게 의존하거나 추가적인 장비를 소지하여야 하는 한계점을 보인다. 생체 인증 기술은 기기에 인증을 위한 추가 장비가 탑재되어야 하며 유출 시 대체가 불가능하다는 점과 사용자의 거부감을 유발할 수 있다는 한계점이 있다[1]. 이러한 한계점을 극복하기 위해 다중요소 인증 기술의 중요성이 부각되고 있으며 대표적인 예로 스마트폰 사용 시 발생하는 가상키보드 입력, 터치 정보 등을 통해 사용자 인증을 수행하는 방법인 행위 기반 인증 기술이 있다.

기존 행위 기반 인증 기술은 터치, 키 스트로크에 초점을 맞추어 요소를 세분화하거나 다양화하는 모습을 보여준다. 그러나 앱 사용 정보 또한 스마트폰 사용 중 수집 가능한 사용자 행위 정보로 인증 요소로써 활용 가능성이 충분하다[2]. 따라서 본 연구에서는 기존 행위 기반 인증 기술의 개선을 위해 앱 사용 정보를 새로운 인증 요소로 활용하는 방법을 제안한다. 또한 사용자들의 실제 앱 사용 경우를 고려한 성능을 상세하게 분석한다. 본 연구를 통해 사용자들의 사생활 침해 방지를 위한 안전하고 사용성 높은 스마트폰 인증 기술을 제안하고 개선하는데 활용될 것으로 기대된다.

II. 관련 연구

2.1 안드로이드 사용자 인증 기술과 한계

안드로이드 환경에서 사용자 인증 기술로 패턴 잠금 시스템과 함께 가장 많이 사용되고 있는 PIN과 패스워드는 PC 환경의 텍스트 기반 패스워드 방식을 그대로 가져와서 사용자들이 친숙하게 사용할 수 있다는 장점이 있다. 그러나 사용 시 대체로 기억에 의존하는 단점 또한 그대로 이어받고 있다.

이를 대체하기 위해 그래픽 패스워드(Graphical Password) 기법들[3][4][5]이 꾸준히 제안되었다. 예를 들어 안드로이드에서 도입한 패턴 잠금 시스템은 9개점을 이용하여 최소 4개 이상의 점을 한 번씩만 지나가는 패턴을 사용하는 방식으로 총 389,112가지의 패턴이 사용 가능하다[6]. 그러나 이 또한 사용자들의 기억에 의존하므로 추측 공격(Guessing Attack)[7], 스머지 공격 (Smudge Attack)[6], 숄더 서핑 공격(Shoulder surfing Attack)[8] 등에 취약하다.

최근에는 안드로이드 사용자 인증 기술을 강화하기 위해 생체 인증 기술이 점차 부각되고 있다. 생체 인증 기술은 사용자의 신체적 정보와 행동적 정보를 활용하여 사용자를 인증하는 방법이다. 그 중에서 신체적 정보를 이용한 생체 인증 기술이 최근 스마트폰에 적용되고 있다. 지문 인식 기술은 갤럭시 S5, 아이폰 5S부터 스마트폰에 적용되어 현재 널리 사용되고 있는 생체 인증기술 중 하나이다. 생체 인증 기술은 타 기술에 비해 편리하고 위조가 어렵지만 한번 유출되면 변경이 불가능하다는 문제가 있으며 특정 상황, 예를 들어 지문 인식을 시도할 때 손에 물이 묻은 경우 인증이 제대로 이루어지지 않는다. 또한 홍채나 얼굴 인증의 경우 기기를 사용자 얼굴 정면에 위치시켜야 하는데 공공장소에서 이와 같은 행동을 취하는데 거부감을 가지는 사용자들이 있다[1].

또 다른 생체 인증 기술 중 하나인 행위 기반 인증 기술은 사용자의 행동 정보를 인증 요소로 활용하여 사용자를 인증한다. 스마트폰의 경우 터치 동작, 터치 입력 사이의 간격, 자주 발생하는 터치 오류 등의 터치와 관련된 행위를 기반으로 인증을 수행한다. 행위 기반 인증 기술은 높은 안전성과 더불어 사용자의 기기 사용과 동시에 지속적인 인증을 수행하기 때문에 사용자의 편의성이 높다.

2.2 행위 기반 인증 기술 연구 동향

행위 기반 인증에 대한 연구는 2012년부터 등장하였다. Kolly 등은 사용자들의 버튼 터치 정보를 이용하는 방법을 제안하였다[9]. 데이터 수집은 게임 내에 특정 버튼을 선택하여 총 14,000명에게 데이터를 수집하였으며 그 중 5명만이 정확도 80% 수준으로 인증이 가능하였다. 이후 연구는 인증 요소의 세분화와 다중화에 초점을 맞추어 발전하였다.

2013년 Feng 등은 가상 키보드로 패스워드를 입력하는 특징에 집중하여 TAP(Typing Authentication and Protection)이라는 인증 기술을 제안하였다[11]. 참가자 40명에게 실험한 결과 EER 1% 수준으로 인증이 가능하였다.

2013년 Y. Meng 등은 개별 터치 동작의 터치 타입 별로 데이터를 수집하여 사용자 인증을 수행하였다[10]. 2014년 Y. Meng 등은 2013년 연구에 과도한 특징을 사용하여 프로세싱에 많은 연산이 요구된다는 단점을 해결하는 연구를 수행하였다[12].

특징 데이터를 터치 제스처 관련 8개의 데이터로 축소하여 경량화 된 인증 기법을 제안하였다. 50명의 참가자가 세션마다 120개의 터치 제스처를 입력하도록 하였으며 3일간 25 세션을 진행하여 데이터를 수집하였다. 인공신경망 분류기를 이용하여 분류한 결과 EER 2.46% 수준으로 인증이 가능하였다.

2015년 Shen 등의 연구에서는 싱글 터치 중 슬라이드에만 초점을 맞추어 인증을 수행하였다[13]. 총 51명의 참가자를 대상으로 4 가지의 사용 상황을 가정하여 데이터를 수집하였으며 EER 8% 이하의 수준으로 인증이 가능하였다.

2015년 Lu와 Liu는 터치 행위를 슬라이드와 탭 2가지로 분류하여 특징 데이터로 활용하는 연구를 수행하였다[14]. SFS(Sequential Forward Selection) 알고리즘을 이용하여 슬라이드의 각도와 거리, 탭의 압력만 특징 데이터로 사용하였으며 분류 점수를 향상시킬 수 있는 효율적인 샘플만 추출하여 성능 측정을 수행하였다. 또한, 앉은 상황과 이동 상황을 구분하여 데이터를 수집・분석하였다. 총 60명의 참가자를 대상으로 자연스럽게 기기를 사용하도록 하였으며 SVM 분류기를 이용한 결과 FAR 0.03%, FRR 0.05% 수준으로 인증이 가능하였다.

2015년 Fridman 등은 기존 키스트로크 인증 기술의 확장으로 특징 데이터로 웹 브라우징, 앱 사용, 사용 지역에 대해 추가하여 연구를 진행하였다[15]. 200명의 참가자를 대상으로 30일동안 데이터를 수집하였으며 SVM 분류기를 이용한 결과 EER 5% (사용 후 1분 이내), EER 1%(사용 후 30분 초과) 수준으로 인증이 가능하였다.

2016년 Sitova 등의 연구에서는 키스트로크와 터치 인증 기술에 센서 데이터를 추가하여 연구를 진행하였다[16]. 크게 탭, 키스트로크, 기기를 쥐는 형태로 데이터를 분류하였다. 100명의 참가자를 대상으로 8개 세션을 진행하여 데이터를 수집하였다. 참가자는 세션당 3개의 질문에 대한 답변을 250자 이상으로 입력하였으며 4개의 세션은 앉아서 진행하였고 나머지 4개의 세션은 걸어 다니면서 입력을 진행하였다. One-Class SVM을 이용한 결과 걷는 상황에서 EER 7.16%, 앉아있는 상황에서 10.05% 수준으로 인증이 가능하였다.

Table 1.은 행위 기반 인증 기술의 연구 동향을 정리한 것이다. 각 연구에서 사용한 특징 데이터, 최

Table 1. Previous researches of user behavior based authentication

Research	Feature	Classification Algorithm	Accuracy(%)
Kolley et al. (2012)	Button touch position/time/pressure	Naïve Bayesian	80
Feng et al. (2013)	Keystroke time/pressure	Decision Tree	EER:1
Meng et al. (2013)	Touch type/point/time/direction/number of actions per session under single-touch/ touch-movement/multi-touch	Neural Network	EER:2.92
Meng et al. (2014)	The average time duration/number of touch-movement/single-touch/multi-touch per session, Average speed of Touch-movement, Touch pressure.	Neural Network	EER:2.46
Shen et al. (2015)	Slide position/ length/ angle/ time/ acceleration/ pressure (by 4 direction)	one-class SVM	EER:〈8
Lu and Liu (2015)	Slide (angle, distance), Tap (pressure)	SVM	FAR:0.03 FRR:0.05
Fridman et al. (2015)	Text typed via soft keyboard, Apps visited, Websites visited, Location based on GPS or WiFi	SVM	EER:5 (〈1min) EER:1(〉30min)
Sitova et al. (2016)	Tap (time, size, speed), Keystroke (key hold latency), Grasps (accelerometer, gyroscope, magnetometer)	one-class SVM	EER:7.16 (walking) EER:10.05 (sitting)

고의 성능을 보인 알고리즘, 정확도를 정리하였다.

III. 행위 기반 인증 기술 설계

본 논문에서 제안하는 기술의 구조는 Fig.1.과 같다. 크게 데이터 수집, 특징 추출, 기계학습을 이용한 데이터 학습, 인증 단계로 구분된다.

3.1 데이터 수집 단계

사용자에게 데이터 수집을 위한 추가적인 행위를 요구하지 않도록 백그라운드에서 데이터 수집이 이루어지도록 구현하였다. 데이터 수집기는 접근성 서비스를 이용하여 구현하였으며 백그라운드에서 동작하면서 기기 사용 시 발생하는 터치 정보와 앱 사용 정보를 지속적으로 수집한다.

3.1.1 터치 정보 수집

본 연구에서는 루팅된 기기에 쉘 명령어를 이용하여 터치스크린에서 발생하는 이벤트를 직접 수집하는 앱을 구현하였다. 앱 구현 시 필요한 명령어와 터치 정보를 확인하기 위해 입력 기기와 커널 입력 이벤트를 실시간으로 모니터링이 가능한 getevent 명령어를 이용하였다. 터치스크린 이벤트만 추출하기 위해 터치스크린 입력 기기의 명칭을 확인하려면 adb shell getevent 명령어로 확인 가능하다. 일반적으로 /dev/input/event1이 터치스크린이지만 이는 기기마다 다르므로 반드시 기기별로 확인이 필요하다. 위의 과정에서 찾아낸 정보를 조합하여 adb shell getevent -lt /dev/input/event1 명령어를 입력하면 터치 정보를 수집할 수 있다.

3.1.2 앱 사용 정보 수집

앱 사용 정보는 안드로이드의 접근성 서비스를 이용하여 수집하도록 구현하였다. 안드로이드에는 TalkBack 등 기본 내장 접근성 서비스가 있으며 개발자가 서비스를 만들어 배포할 수도 있다[17].

접근성 서비스는 백그라운드에서 동작하며 사용자 인터페이스에 이벤트가 발생하였을 때 AccessibilityEvent 값을 수신하여 처리하는 과정으로 구성되어 있다. 각 이벤트는 AccessibilityNodeInfo 객체 값을 포함하며 이로부터 화면상의 정보를 수집할 수 있다. 수집 가능한 앱 사용 정보는 패키지명, 클래스명, 뷰 이벤트 타입이 있다.

앱 사용 정보 수집기는 AccessibilityService를 상속받아 백그라운드에서 동작하도록 구현하였다. 수집기 호출 및 데이터 수집은 onServiceConnected() 함수와 onAccessibilityEvent() 함수를 오버라이드하여 구현하였다. 정보 수집은 AccessibilityEvent가 탐지되었을 때 호출되는 onAccessibilityEvent() 함수에 로깅 기술을 구현하여 이벤트 발생 시마다 앱 사용 정보와 터치 정보가 함께 수집되도록 하였다.

3.2 특징 추출 단계

데이터 수집 단계에서 수집한 데이터를 인증 요소로 가공한다. 수집된 데이터들은 기계 학습에 이용하기 위해 벡터화된다. 인증 요소는 총 11 차원의 벡터로 구성되며 패키지명, 클래스명, 뷰 이벤트명, 터치 시작 좌표(x, y), 터치 종료 좌표(x, y), 길이, 각도, 압력, 크기순으로 구성된다. 추출된 인증 요소들은 기계 학습 알고리즘에 학습 모델 생성 또는 분류를 위한 테스트 데이터로 사용된다.

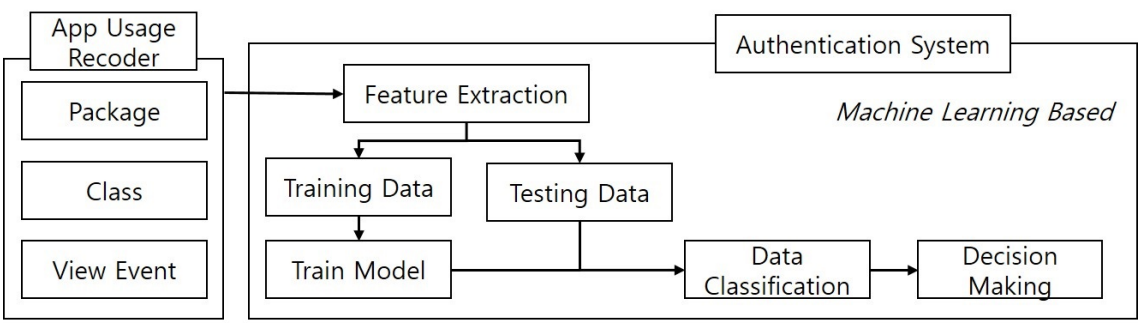


Fig. 1. Mechanism Architecture

3.2.1 터치 정보 추출

수집된 데이터로부터 길이, 각도의 데이터를 추가적으로 연산한다. Fig.2.는 길이와 각도 연산 방법을 도식화한 것이다. 터치 길이 값은 최초 터치가 시작된 점과 종료된 점 사이의 길이를 계산한다. Fig.2.와 같은 경우, 시점 A와 종점 B 사이의 직선거리 계산은 두 점 사이의 거리를 계산하는 식 (1)을 이용한다.

$$\overline{AB}=\sqrt{(x_B-x_A)^2+(y_B-y_A)^2} \quad (1)$$

터치 각도는 터치 시작점과 중간점, 중간점과 터치 종점 사이의 각을 계산한다. 중간점은 터치 시작점과 터치 종점 사이 경로상의 최대 및 최소 좌표의 평균값 $((x_{\min}+x_{\max})/2, (y_{\min}+y_{\max})/2)$으로 구성된다. Fig. 2.와 같은 경우, $\overrightarrow{AC}$와 $\overrightarrow{CB}$ 사이의 끼인각($\angle ACB$)을 식 (2)를 통해 계산한다.

$$\cos^{-1}\left(\frac{v_1 \cdot v_2}{\| v_1 \| \| v_2 \|}\right) \quad (2)$$

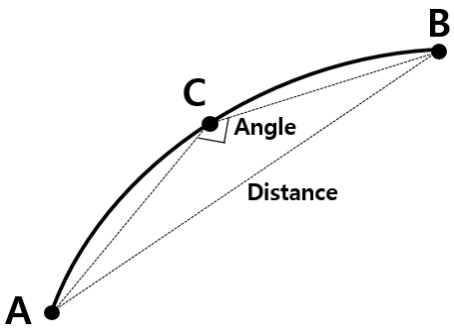


Fig. 2. Illustration of Distance and Angle

3.2.2 앱 사용 정보 추출

추출 단계에서 앱 사용 정보는 수집된 이벤트에서 패키지명, 클래스명, 뷰 이벤트명을 추출한다. 각 정보는 이벤트 타입의 메소드를 이용하여 수집한다. 패키지는 getPackageName(), 클래스는 getClassName(), 뷰 이벤트명은 getEventType() 메소드를 이용한다. 터치 정보와는 다르게 추가적인 연산은 포함하지 않고 문자열 그대로 인증 요소로 사용한다.

3.3 데이터 학습 및 인증 단계

데이터 학습 단계에서는 기계학습 분류 알고리즘을 이용하여 분류 모델을 생성한다. 특징 추출 단계를 거쳐 생성된 인증 요소를 입력 값으로 활용한다. 각 인증 요소는 사용자의 데이터인지 비사용자의 데이터인지 구별 가능한 분류 라벨이 포함된다.

인증 단계에서는 이전 단계에서 생성된 분류 모델에 따라 새로 입력되는 데이터를 사용자의 데이터인지 비사용자의 데이터인지 분류한다. 제안 기술에서 사용되는 인증 요소는 지속적으로 분류가 가능하므로 분류 결과의 라벨과 확률 값을 지속적으로 확인한다.

IV. 실험 방법 및 결과

제안 기술의 성능을 검증하기 위한 방법으로 분류 모델의 정확도 (데이터를 올바르게 분류한 비율)와 에러율 (데이터를 잘못 분류한 비율)을 측정한다.

4.1 실험 환경

본 연구에서는 Lu와 Liu의 연구[14], Fridman 등의 연구[15]에 따라 스마트폰의 대표적인 앱 사용 경우인 소셜 네트워크 앱 사용(SNS), 웹 서핑(WEB), 이미지 브라우징(IMG), 문자 메시지 전송(SMS) 4가지 시나리오를 설정하여 진행하였다.

각 시나리오별 수집 방법은 Teh 등의 연구[1]에 따라 이전 연구의 실험 설계를 활용하였다. 이전 연구들에 따라 본 실험에서도 SNS, WEB, IMG에서는 5분간 앱을 사용하도록 설정하였으며, SMS에서는 10개의 고정된 문장을 입력하도록 하였다.

각 시나리오에서 활용한 앱은 SNS는 페이스북, WEB은 네이버, IMG는 인스타그램, SMS는 안드로이드 기본 문자 메시지 앱을 사용하였다. 페이스북, 네이버의 경우 국내에서 가장 보편적인 소셜 네트워크, 웹 브라우징 앱이므로 실험 앱으로 선정하였다. 인스타그램은 소셜 네트워크 앱이지만 사전 검색 기능만 이용하도록 제한한다면 사진의 랜덤성을 보장하면서 사진 구경을 수행하도록 할 수 있기 때문에 실험 앱으로 선정하였다.

데이터 수집은 실험용 기기를 선정하여 모든 사용자가 동일한 기기를 이용하여 실험을 진행하였다. 실제 사용자의 폰에 데이터 수집 앱 설치 시의 거부감을 해결하고 모든 사용자에게 동일한 실험 환경에서

데이터 수집을 진행하기 위해 실험용 기기로 실험을 진행하였다. 실험용 기기는 넥서스 5를 사용하였으며 화면 크기는 4.95인치, 운영체제는 안드로이드 6.0.1 버전이다. 데이터 수집 시작 전 사용자에게 데이터 수집이 된다는 점을 통지 후 동의를 얻고 실험을 진행하였다. 또한, 실험동안 추가 작업을 요구하지 않고 사용자가 평소 앱을 사용하듯 자연스럽게 사용하도록 유도하였다.

실험은 랩 스터디 형태로 10명을 대상으로 진행하였으며 한 사람당 4개의 시나리오를 5번씩 수행하도록 하였다. 그 결과, 총 200회의 실험이 수행되었으며 데이터는 총 375,874개가 수집되었다.

수집된 데이터로부터 추가적으로 계산된(3.2.1절) 각도 속성은 기존 연구들에서 비교적 잘 활용되지 않은 터치 인증 요소였다. 실질적으로 각도가 사용자를 식별하는데 유효한 특징인지 확인하기 위해 수집된 375,874개의 각도 데이터(Fig.3.)에 대해 사용자별로 차이가 있는지 통계적 검증을 시도하였다. 검증 결과 10명의 실험 참가자들 사이에는 수집된 각도 평균에 대해 통계적으로 유의한 차이가 있음이 확인되었으며($ANOVA$, $p<10^{-30}$), 또한 LSD 검증을 통해 2명 단위의 모든(45개) 참가자 조합의 각도 평균의 차이를 분석한 결과 5개 조합을 제외하고 모두 유의 수준(α) 0.1% 이하에서 통계적으로 유의한 차이가 있음이 확인되었다. 비록 몇몇 사용자 간에는 통계적으로 유의한 차이를 발견하지 못하였으나 이는 단순히 평균만을 비교한 결과이므로, 다른 특징과 결합하여 인증 요소로 활용한다면 인증 정확도 향상에 충분히 기여할 수 있을 것으로 판단하였다.

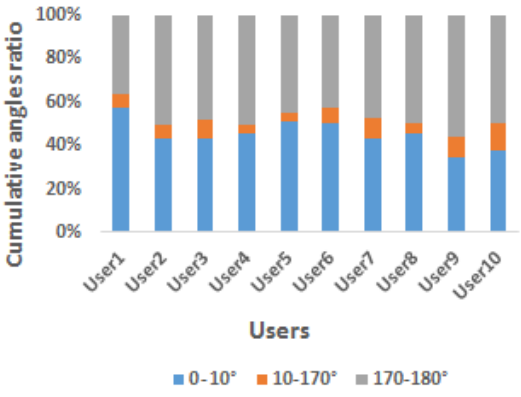


Fig. 3. Distribution of angles

4.2 실험 방법

실험에는 마이크로소프트사에서 제공하는 클라우드 기계학습 플랫폼인 Azure Machine Learning Studio (이하 Azure)에 구현된 기계학습 알고리즘을 이용하였다[18]. 현재 Auzre에는 다양한 이진 분류 알고리즘이 구현되어 있으며 본 실험에서는 Boosted Decision Tree[19], Decision Forest[20], Decision Jungle[21], SVM[22], Locally Deep SVM[23], Neural Network[24] 알고리즘을 사용하였다.

분류 결과의 객관성을 향상시키기 위해 성능 측정은 10-fold cross validation을 이용하였다[25]. 이는 데이터를 총 10개의 조각으로 분류하여 1개의 조각을 테스트 데이터, 나머지 9개 데이터를 학습 데이터로 분류하여 모든 조각에 대해서 분류 정확도를 검증하는 방법이다.

성능 검증의 평가 척도는 Precision, Recall, F-Score, FAR(False Accept Rate), FRR (False Rejection Rate), EER(Equal Error Rate) 값을 이용하고 각각의 의미는 다음과 같다.

- Precision: 참으로 예측된 데이터 중 실제 참인 데이터 비율을 나타낸 값
- Recall: 실제 참인 데이터 중 참으로 예측된 데이터의 비율을 나타낸 값
- F-Score: Precision과 Recall의 중요도를 동일하게 여긴 상태의 조화 평균 값으로 1에 가까울수록 성능이 좋다.
- FAR: 거짓 데이터를 참으로 잘못 분류한 비율
- FRR: 참 데이터를 거짓으로 잘못 분류한 비율
- EER: FAR과 FRR의 값이 동일할 때의 값

성능 검증은 크게 제안 기술에 최적 기계 학습 알고리즘 도출과 기존 기술과의 성능 비교 2가지로 구분된다. 최적 기계 학습 알고리즘 도출 실험에서는 사용된 각 알고리즘의 분류 결과를 평가 척도를 기반으로 비교한다. 이 과정에서 ROC(Receiver Operating Characteristic) 곡선과 AUC(Area Under the Curve) 값[1]을 이용하여 임계값 변화에 따른 분류 성능과 도식화하여 비교한다. 기존 기술과의 분류 모델 성능 비교에서는 FAR, FRR 또는 EER 값을 이용한다. 에러율을 기준으로 비교를

1) ROC 곡선의 밑면적 값, 1에 가까울수록 성능이 좋음

수행하는 이유는 각 연구별로 인증 요소와 적합한 기계 학습 알고리즘, 데이터 집합이 달라 동일한 환경에서 수행된 연구가 아니기 때문이다. 따라서 각 연구에서 수행한 분류 과정에서 발생하는 에러율을 기준으로 성능 비교를 수행한다.

4.3 실험 결과

4.3.1 제안 기술 성능 분석

제안 기술에 가장 적합한 기계학습 알고리즘을 도출하기 위해 시나리오별로 각 알고리즘의 성능을 측정하였다. Fig. 4.는 모든 시나리오를 종합하였을 때 각 알고리즘의 성능 측정 결과를 정리한 것이다. Fig. 4.의 ROC 그래프를 통해 Decision Tree 계열의 알고리즘이 좌측 상단에 가장 근접해 있어 가장 좋은 성능을 보이는 것을 확인할 수 있다. 특히 Boosted Decision Tree와 Decision Forest 알고리즘이 좋은 성능을 보인다. 이에 비해 SVM, LDSVM 알고리즘에서는 낮은 성능을 보인다.

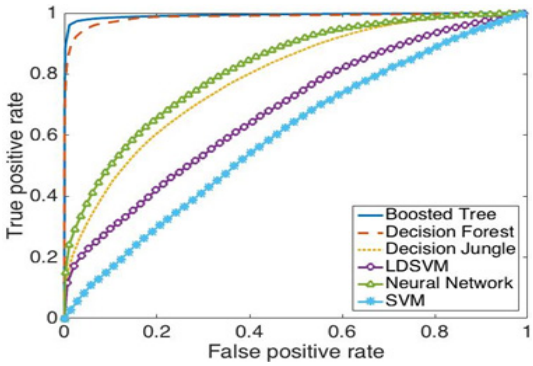


Fig. 4. Machine-learning Algorithms ROC Graph with Pooled Scenario

ROC 그래프에서 확연히 좋은 성능을 보인 Boosted Decision Tree와 Decision Forest 알고리즘의 Precision은 각각 96.52%, 96.36%, Recall은 각각 93.55%, 80%, F-Score는 각각 0.95, 0.87로 타 알고리즘에 비해 뛰어난 성능을 보여준다. 특히 Boosted Decision Tree는 낮은 EER 값으로 실험에 사용된 알고리즘 중 가장 좋은

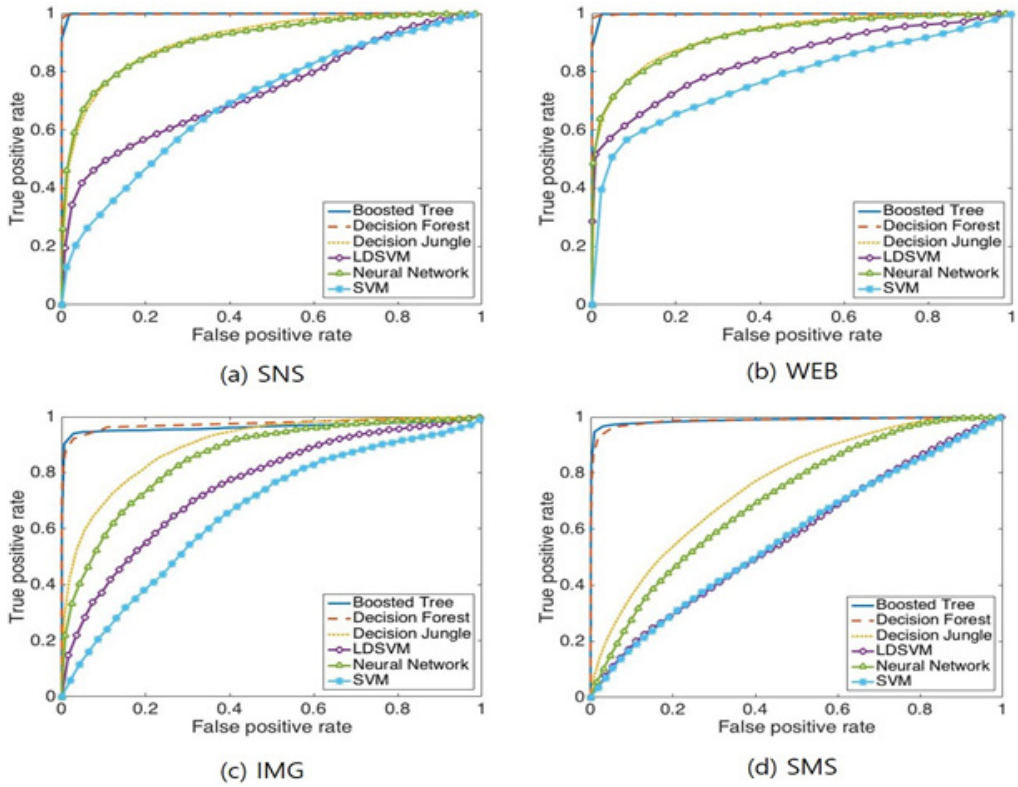


Fig. 5. Machine-learning Algorithms ROC Graphs by Scenario

성능을 보여준다. 그러나 그 외의 알고리즘은 높은 에러율로 제안 기술에 적합하지 않음을 보여준다.

다음으로 제안 기술의 성능을 실험 시나리오별로 측정하였다. Fig.5.는 각 시나리오별 ROC 그래프를 나타낸 것이다. 전체 시나리오와 같이 Boosted Decision Tree와 Decision Forest가 가장 좋은 성능을 보인다. 이 중 Boosted Decision Tree를 제안 기술의 기계학습 알고리즘으로 설정하였다.

각 시나리오별로 성능을 정리하여 비교하였다. Fig.6.는 각 시나리오별 ROC 그래프를 나타낸 것이다. 성능 측정 결과 EER 값을 기준으로 SNS 〉 WEB 〉 ALL 〉 SMS 〉 IMG 순으로 나타났다. 사용자들의 사용 패턴이 다양하게 등장하는 SNS와 WEB에서 각각 EER 0.54%, 0.91%로 낮은 에러율을 보여준다.

Fig. 7.은 각 시나리오별 사용자들의 EER을 비교한 것이다. 모든 시나리오를 종합한 경우, EER 값은 1.1%에서 5.1%로 사용자마다 에러율이 다르게 나타났다. 또한, 시나리오마다 최소의 에러율을 보이는 사용자가 다르게 나타났다. 이는 각 실험 참가자마다 고유의 패턴이 명확하게 나타나는 앱이 다르기 때문이다.

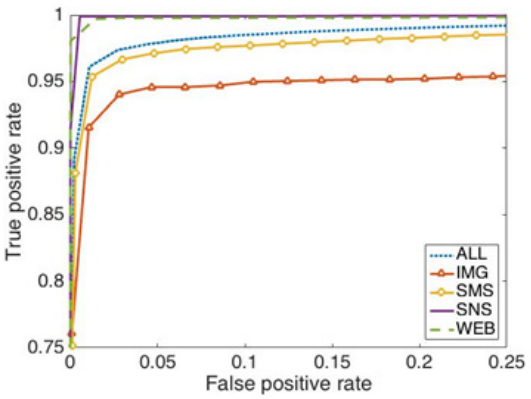


Fig. 6. Boosted Decision Tree ROC Graph by Scenario

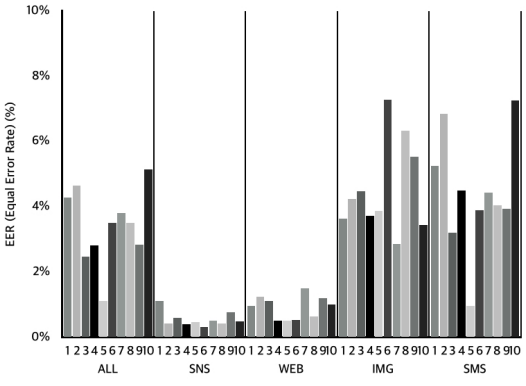


Fig. 7. EER Distribution of 10 Participants by Scenario

4.3.2 이전 연구와의 성능 비교

본 연구의 제안 기술은 Shen 등의 연구, Sitova 등, Fridman 등의 연구보다 낮은 에러율을 보여준다(Table 2.). 그러나 Lu and Liu의 연구보다는 낮은 성능을 보인다. Lu and Liu의 연구에서는 분류 성능을 향상시킬 수 있는 효율적인 샘플만 이용하여 성능 측정을 수행한 결과이다. 따라서 데이터 클리닝을 추가적으로 수행해야 한다는 단점이 있으며 효율적인 데이터가 충분히 모이기까지의 소요 시간이 불분명하여 실제 환경에서는 성능이 저하될 수 있다.

본 연구와 기존 연구의 차이점은 기존 연구에서 이용되었던 터치 정보에 앱 사용 정보를 결합하여 인증 요소로 활용한다는 점이다. 이를 통해 앱마다 분류 모델을 생성하여 인증이 가능하다. 또한 제안 기술의 성능 측정 결과를 보면 앱마다 성능이 상이하게 나타난다. 즉, 앱의 성격에 따라 임계값을 다르게 설정한다면 사용성을 더욱 향상시킬 수 있을 것이다.

Table 2. Performance Comparison with Previous Researches

Research	Error(%)
This work	EER: 3.41,FAR: 0.37 FRR: 6.45
Shen et al. (2015)	EER:〈8
Lu and Liu (2015)	FAR:0.03, FRR:0.05
Fridman et al. (2015)	EER:5(〈1min) EER:1(〉30min)
Sitova et al. (2016)	EER:7.16(walking) EER:10.05(sitting)

4.4 연구 한계점

본 논문에서는 앱 사용 정보와 터치 정보를 활용하는 행위 기반 인증 기술에 대해 연구하였다. 그러나 제한된 환경에서 실험을 진행하여 본 연구에는 다음과 같은 한계점이 있다.

첫째, 데이터 일반화의 어려움이다. 본 연구에서는 10명의 실험 참가자 중 한명을 사용자, 그 외 나머지 실험자를 비사용자로 분류하여 성능 측정을 수행하였다. 그러나 비사용자로 분류된 실험자들의 데이터가 일반적인 공격자의 사용 패턴이라 일반화하기에는 어려움이 많다. 이를 해결하기 위해 필드 스터디로의 확장을 통해 충분한 표본을 확보함과 동시에 단일 클래스로 모델을 생성하고 분류하는 알고리즘 활용에 대한 고려가 필요하다.

둘째, 데이터 수집의 한계이다. 본 연구에서 사용하는 터치 정보 수집기는 정책의 한계로 인해 루팅이 요구되어 실험 환경이 제한된다. 또한, 실제 사용자 기기에 행위 정보 수집기를 설치하는 것에 대한 거부감으로 인해 실제 사용 데이터를 수집하기 어렵다. 따라서 사전 동의 후 실험 진행이 가능하도록 다양한 방법으로 실험자를 모집하거나 사용 시나리오, 실험 기기의 세분화에 대한 고려가 필요하다.

셋째, 제안 기술의 실험 측정 결과 기존보다 개선된 모습을 보여주었으나 유럽 생체 인증 기술 성능 상용화 기준[26]에는 미달되는 성능을 보인다. 유럽 생체 인증 기술 성능 상용화 기준은 FRR 1%, FAR 0.001%인 반면 제안 기술의 성능은 FRR 6.45%, FAR은 0.37%로 개선이 요구된다. 따라서 임계값 조절과 인증 요소 추출 방법 개선으로 FAR, FRR을 감소시키기 위한 연구가 필요하다.

V. 결 론

본 논문에서는 기존 행위 기반 인증 기술에서 인증 요소로 활용되는 터치 정보에 앱 사용 정보를 새로운 인증 요소로서 활용하는 방법을 제안하였다. 성능 측정 결과 모든 시나리오를 종합한 결과에서 EER 3.41% (FAR 0.37%, FRR 6.45%)로 기존 연구보다 좋은 성능 측정 결과를 보여주었다. 에러율을 기준으로 시나리오별 성능을 비교한 결과 앱 사용 패턴이 다양하고 명확하게 나타날 여지가 많은 SNS, WEB에서 가장 좋은 성능을 보여주었다. 본 연구의 방법에 기반 하여 앱 중요도에 따라 일부 앱에서만 활용하는 등의 방법으로 기존 행위 기반 인증 기술의 성능 개선에 이바지 할 수 있다.

References

[1] P.S. Teh, N. Zhang, A.B.J Teoh, and K. Chen, "A survey on touch dynamics authentication in mobile devices," Computers & Security, Vol. 59, pp. 210-235, 2016.

[2] A. Alzubaidi and J. Kalita, "Authentication of Smartphone Users Using Behavioral Biometrics," IEEE Communications Surveys & Tutorials, Vol. 18, No. 3, pp. 1998-2026, 2016.

[3] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," In USENIX Security Symposium, 2004.

[4] H. Gao, X. Guo, X. Chen, L.Wang, and X. Liu, "Yagp: Yet another graphical password strategy," Annual Computer Security Applications Conference (ACSAC'08), pp. 121 - 129, 2008.

[5] K. Renaud and A. D. Angeli, "Visual passwords: Cure-all or snake-oil?," Communications of the ACM, pp. 135 - 140, 2009.

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," In Proc. of the 4th USENIX Conference on Offensive Technologies (WOOT'10), pp. 1-7, 2010.

[7] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks," In Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec'13), pp. 1-6, 2013.

[8] A.H. Lashkari, S. Farmand, O.B. Zakaria, and R. Saleh "Shoulder surfing attack in graphical password authentication." arXiv preprint arXiv:0912.0951 (2009).

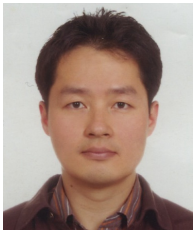
[9] S.M. Kolly, R. Wattenhofer, and S. Welten, "A personal touch: Recognizing users based on touch screen behavior," Proceedings of the Third International

Workshop on Sensing Applications on Mobile Phones, ACM, 2012.
[10] Y. Meng, D.S. Wong, and R. Schlegel, "Touch gestures based biometric authentication scheme for touchscreen mobile phones." International Conference on Information Security and Cryptology. Springer Berlin Heidelberg, 2012.
[11] T. Feng, X. Zhao, B. Carbunar, and W. Shi, "Continuous mobile authentication using virtual key typing biometrics." 12th International Conference on Trust, Security and Privacy in Computing and Comm- unications. IEEE, pp.1547-1552, 2013.
[12] Y. Meng, and D.S. Wong, "Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones," Proceedings of the 29th Annual ACM Symposium on Applied Computing. ACM, pp.1680-1687, 2014.
[13] C. Shen, Y. Zhang, Z. Cai, T. Yu, and X. Guan, "Touch-interaction behavior for continuous user authentication on smartphones," 2015 International Conference on Biom- etrics (ICB), IEEE, pp.157-162 2015.
[14] L. Lu, and Y. Liu, "Safeguard: User Reauthentication on Smartphones via Behavioral Biometrics," IEEE Trans- actions on Computational Social Syst- ems, Vol. 2, No. 3, pp. 53-64, 2015.
[15] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location." IEEE Systems Journal , vol.PP, no.99, pp.1-9, 2015.
[16] Z. Sitová, J. Šeďenka, Q. Yang, G. Peng, and G. Zhou, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users." IEEE Transactions on Information Forensics and Security, Vol. 11, No. 5, pp. 877-892, 2016.
[17] Android Developers, "Building Accessibility Services," available at https://developer.android.com/guide/topics/ui/accessibility/index.html
[18] Microsoft Azure Machine Learning Studio, available at https://studio.azureml.net/
[19] J.H. Friedman, "Greedy function approximation: a gradient boosting machine," Annals of statistics, pp. 1189-1232, 2001.
[20] A. Criminisi and J. Shotton, "Decision forests for computer vision and medical image analysis," Springer Science & Business Media, 2013.
[21] J. Shotton, T. Sharp, P. Kohli, S. Nowozin, J. Winn, and A. Criminisi, "Decision jungles: Compact and rich models for classification," Advances in Neural Information Processing Systems. pp.234-242, 2013.
[22] C. Cortes and V. Vapnik. "Support-vector networks," Machine learning, Vol.20, No.3, pp.273-297, 1995.
[23] C. Jose, P. Goyal, and P. Aggrwal, "Local deep kernel learning for efficient non-linear svm prediction." Proceedings of the 30th international conference on machine learning (ICML-13), 2013.
[24] S. Haykin, "Neuronal Networks-A comprehension Foundation," 1999.
[25] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in Proc. Int. Joint Conf. Artificial, Vol. 14, No. 2, pp.1137-1145, 1995.
[26] "European Standard EN 50133-1: Alarm systems. Access control systems for use in security applications," Technical Body CLC/TC 79, European Committee for Electrotechnical Standardization, 2002.

〈저자소개〉

김 민 우 (Minwoo Kim) 학생회원
2015년: 세종대학교 컴퓨터공학과 학사
2017년: 연세대학교 정보대학원 석사
2017년 1월~현재: SK 주식회사
〈관심분야〉 암호 프로토콜, 네트워크 보안, 스마트폰 보안 등

김 승 연 (Seungyeon Kim) 학생회원
2015년 2월: 세종대학교 응용통계학 및 컴퓨터공학 학사 (자연과학대학 수석졸업)
2015년 3월~현재: 연세대학교 정보대학원 석박통합과정
〈관심분야〉 Usable Security, Social Engineering, 스마트폰 보안, 인증 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년 Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 인증, Usable Security, 사물인터넷 보안, 소프트웨어 보안, 펌웨어 보안 등