정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

스마트폰 기반 Continuous Authentication 기술 동향

조 금 환*, 김 형 식**

요 약

스마트폰의 잠금을 해제하기 위해 초기에 사용자를 인증하는 과정을 한 번 통과하면 스마트폰의 모든 정보에 접근 가능하다. 현재 스마트폰을 사용하고 있는 사용자가 초기 인증된 사용자인지 아닌지 여부를 판단하지 않기 때문에 인증된 스마트폰에 타인이 접근한다면 모든 정보가 유출될 수 있다. 본 논문에서는 스마트폰 기반 continuous authentication 기술에 대한 연구 동향에 대해 소개하고 현재까지 연구된 기술들을 상용 스마트폰에 적용할 수 없는 한계점에 대해 분석한다.

Ⅰ. 서 론

최신 스마트폰은 PINs, 안드로이드 패턴 락, 패스워드와 같은 knowledge-based 인증 기술과 함께 얼굴인식, 지문인식, 홍채인식, 음성인식 (biometric-based)과 같은 다양한 인증 기술을 제공하고 있다. 이러한 인증 기술은 전통적인 방식의 사용자 인증 기술로 널리 사용되고 있으며, 초기 인증 과정에서 사용자를 한 번(one time) 인증하면 스마트폰의 모든 기능을 사용할 수 있는 “all-or-nothing” 방식을 사용하고 있다. 이러한 방식을 사용하는 경우 현재 스마트폰을 사용하고 있는 사용자가 초기 인증 과정을 통과한 합법적인 사용자인지 아닌지 여부를 판단할 수 없다. 예를 들어 합법적인 사용자가 인증한 스마트폰을 타인 혹은 악의적인 목적을 갖고 있는 사람이 탈취한다면 스마트폰에 저장된 모든 정보에 접근할 수 있다.

이러한 문제점을 해결하기 위해서는 스마트폰을 사용하고 있는 사용자가 합법적인 사용자인지 여부를 판단할 수 있는 정보가 요구되며, 이러한 정보를 통해 합법적인 사용자를 지속적으로 판단할 수 있는 기술이 필요하다. 기존의 “all-or-nothing” 방식의 한계를 극복하기 위해 인증이 성공한 이후 스마트폰을 사용하는 동안 사용자에 의해 발생되는 이벤트를 분석하여 합법적인 사용자가 시스템을 사용하는지 여부를 판단하고 인증할 수 있는 Continuous Authentication (CA)기술이 소개되었다[1].

CA 기술은 스마트폰에 내장된 센서 및 기타 정보(예: 통화기록, 애플리케이션 사용 기록 등)를 활용하여 스마트폰을 사용하고 있는 사용자의 행동 특성을 파악하고, 파악된 정보를 기반으로 합법적인 사용자를 검증하는 과정이다. CA 기술은 사용자가 인증을 위해 필요한 과정을 생략하고 시스템 내부적으로 사용자 인증을 수행하기 때문에 implicit, transparent, progressive authentication 기술이라고도 말한다[2][3].

최근 스마트폰의 컴퓨팅 파워가 지속적으로 증가함에 따라 CA 기술에 대한 연구가 활발히 이루어지고 있으며, 별도의 인증 과정이 요구되지 않기 때문에 사용자에게 편리함을 제공할 수 있는 인증 기술이다. 그러나 시스템이 지속적으로 정보를 수집하고 계산하는 등 스마트폰을 사용하는 주목적이 아닌 이유로 컴퓨팅 파워를 지속적으로 사용하게 되며 그로 인해 배터리 소모가 크다는 문제점을 갖고 있다. 본 논문에서는 다양한 CA 기술을 분류하고, 분류한 각 기술에 대한 최신 연구 동향을 소개하고 각 기술의 한계점에 논의한다.

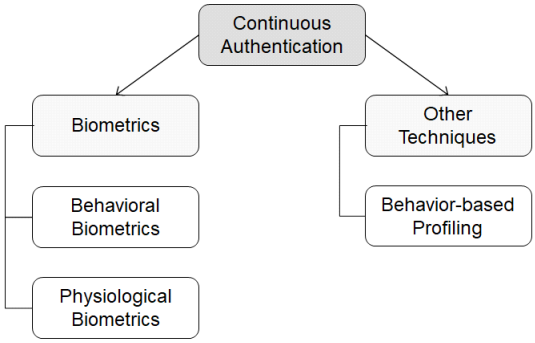
본 논문의 구성은 다음과 같다. Ⅱ장에서는 CA 기술의 유형에 대해 설명하고, Ⅲ, Ⅳ장에서 각각의 CA 기술에 대한 연구 동향에 대해 살펴보고, Ⅴ장에서 본 논문에 대한 결론을 도출할 것이다.

“연구는 과학기술정보통신부 및 한국연구재단 부설 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었음” IITP-2020-2015-0-00742)

* 성균관대학교 정보통신대학 (연구원, geumhwan@skku.edu)
** 교신저자, 성균관대학교 정보통신대학 (교수, hyoung@skku.edu)

Ⅱ. CA 기술 유형

[그림 1]은 CA 기술 분류를 나타내었다. 언급되지 않은 다양한 CA 기술이 연구되고 있지만 상용 스마트폰에 적용이 가능한 기술에 초점을 두고 분류 및 분석하였다. Biometrics를 이용한 기술들이 현재까지 연구된 CA 기술의 대부분이며, 다른 기술의 분류로 user profiling 기술이 연구되고 있다.



〔그림 1〕 CA 기술 분류.

2.1. Biometrics

Biometrics 기반 CA 기술은 다음의 2가지로 분류할 수 있고, 정확도 향상을 위해 각각의 기술을 동시에 사용하는 multimodal biometrics 기술도 연구되고 있다.

- **Behavioral biometrics 기술**: keystroke dynamics, touch dynamics 등과 같이 사람이 하는 행위 방법에 따라 달라질 수 있는 특징을 이용하여 사용자를 인증하는 기술.
- **Physiological biometrics 기술**: physical biometrics 라고도 말하며, 사람이 갖고 있는 인체 부위를 이용한 인증 기술로 얼굴인식, 지문인식 등을 이용하여 사용자를 인증하는 기술.

2.2. Other techniques

본 논문에서 분류하는 other techniques으로 behavior-based profiling 기술을 분석하였고, 이에 속하는 기술로는 location-based 인증기술, application usage를 이용한 인증기술이 연구되고 있다.

Ⅲ. Biometric 기반 CA 기술

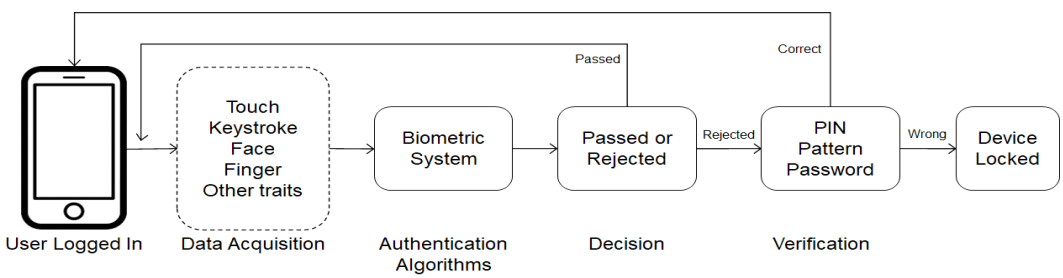
이 장에서는 CA에 사용되는 behavioral biometrics, physiological biometrics 기술에 대한 관련 연구들에 대해 살펴본다.

3.1. Behavioral biometrics

[그림 2]은 biometric 기반 CA 시스템의 프레임워크를 보여준다[4]. Touch, keystroke, face, fingerprint, other traits 등 스마트폰에 내장된 센서 및 사용가능한 기타 정보를 수집한 뒤 인증 알고리즘을 이용하여 합법적인 사용자 여부를 판단한다. 인증에 실패하면 knowledge-based인 PINs, 패턴, 패스워드 등의 인증기술을 이용하여 사용자 인증을 수행한다.

3.1.1. Touch dynamics-based

Touch dynamics 기반 인증 기술은 스마트폰의 터치스크린에 입력되는 데이터를 사용한다. 따라서 사용자가 스마트폰을 사용하는 동안 지속적으로 사용자를 인증할 수 있다. 기록된 스크린 터치 데이터에서 동작의



〔그림 2〕 Biometric 기반 CA 프레임워크〔4〕

〔표 1〕 Touch dynamics-based 기술 결과 요약 (AER: Average Error Rate).

Study	Classifier	# Features	Performance (%)
Frank 등[5]	SVM, kNN	27	EER: 0.0-4.0
Zhang 등[6]	Sparsity-based classifiers	27	EER: 0.77
Li 등[7]	SVM	10	EER: 3.0
Feng 등[8]	Random Forset, J48 tree, Bayes' net	53	FAR: 7.5, FRR: 8.0
Zhao 등[9]	L1 distance	100 × 150 image	EER: 6.3-15.4
Meng 등[10]	Classifier 5개 사용	9	AER: 5.01-10.09

feature vector를 추출하고, 추출된 feature를 이용하여 분류기에 트레이닝하여 인증을 한다. Touch dynamics를 이용 시 사용자의 터치 이벤트는 single touch와 multiple touch 두 가지로 분류하여 구분한다. 사용자가 스마트폰을 사용할 때 기본적인 조작은 손가락 한 개를 이용하는 점을 이용하여 single touch 이벤트를 수집하여 사용자 인증을 수행하는 연구들이 진행되었다[5][6][7].

Single touch를 위해 사용된 feature의 개수는 보통 10~27개 정도 사용되고 있다.

그러나 실제 일반적인 상황에서 스마트폰을 사용할 때 많은 사용자들이 두 개 이상의 손가락을 사용하는 경우가 많다(예: zoom in, zoom out). 따라서 좀 더 일반적인 상황을 고려한 multi touch 기반 CA 시스템에 대한 연구가 진행되었다[8].

Zhao 등[9]은 그래픽 터치 제스처 기능을 이용하는 연구를 진행했다. 트레이닝 된 통계적 touch dynamics 이미지를 적용하여 사용자 인증을 위한 성능을 유지하면서 온라인 인증을 수행하는 동안 계산 시간을 단축할 수 있었다. 안드로이드 애플리케이션을 구현하고 제안된 방법의 유용성과 효율성을 100 × 150 image를 feature로 사용하여 평가하였고, 결과는 6.3~15.4%의 EER을 획득 하였다([표 1] 참조).

Meng 등[10]은 cost를 고려하여 사용자 터치 behavioral feature를 개선했다. 5개의 일반적인 classifier(Decision Tree, Naive Bayes, Radial Basis Function Network, Back Propagation Neural Network, SVM)를 이용하여 제안된 방법의 성능을 평가하였다. 60명의 실험참가자를 대상으로 실험한 결과 average error rate가 5.01~10.09%였다.

Touch dynamics를 이용한 인증 기술은 사용자 친화적인 기술로 비교적 인증시간이 빠른 편이지만 상용 스마트폰에 적용할 때 다음과 같은 한계가 존재한다.

- **한계점**: 터치스크린에서 발생되는 이벤트를 사용하기 때문에 터치스크린이 손상된 경우에는 사용할 수 없다. 또한 터치스크린에 입력되는 터치 이벤트가 상황에 따라 터치 압력이나 터치 입력속도 등이 달라질 수 있기 때문에 트레이닝 된 모델과 차이가 발생할 수 있다.

3.1.2. Keystroke dynamics-based

Keystroke dynamics는 모바일 기기 사용자를 지속적으로 인증하는데 널리 사용되는 기술로 cost-effective하고 추가 모듈이 필요 없다는 장점이 있다. Keystroke dynamics 기반 인증 기술의 결과는 [표 2]에 정리하였다. Keystroke dynamics를 이용한 인증 기술은 타이핑 패턴에 따라 사용자를 식별한다. 일반적으로 사용되는 features들은 다음과 같다[11].

- **Keypress frequency**: 키 누르기 이벤트의 빈도를 계산.
- **Key release frequency**: 키를 해제하는 이벤트의 빈도를 계산.
- **Latency and hold time**: Press to Press(키와 키를 누르는 사이의 시간), Press to Release(키를 누르고 해제하는 사이의 시간) 이벤트의 비율을 계산.
- **Finger's pressure**: 터치스크린을 만지는 동안 가해지는 손가락의 압력.
- **Press area of finger size**: 사용자의 손가락이 터치스크린에 접촉되는 영역.

〔표 2〕 Keystroke dynamics-based 기술 결과 요약 (AER: Average Error Rate).

Study	Classifier	# Participants	Performance (%)
Zahid 등[13]	PSO-GA Fuzzy	25	AER: 2
Urtiga 등[14]	Distance	15	FAR: 12.97, FRR: 2.25
Giuffrida 등[16]	kNN	20	EER: 0.08
Anusas-amornkul등[17]	SVM	5	EER: 5.1

- **Error rate**: 입력된 값을 삭제하는 옵션의 사용빈도를 계산.

모바일 기기 사용자 인증을 위한 그래픽 기반 암호 입력 방식 기반 keystroke dynamics의 사용하는 인증 기술이 제안[12]되었고, Zahid 등[13]은 keystroke dynamics가 스마트폰 사용자를 식별하는데 사용될 수 있음을 증명하였다. 이를 위해 다양한 스마트폰 사용자 25명의 keystroke dynamics 데이터를 수집한 뒤 분석했다. 6개의 구별될 수 있는 keystroke dynamics feature를 발견했고, fuzzy classifier에 적합하다는 것을 보여줬다. 스마트폰의 새로운 keystroke dynamics 기반 PIN 검증 모드를 제공하고 실험결과 제안된 시스템은 average error rate이 2%였다. 사용자가 패스워드를 입력해서 시스템에 액세스하는데 실시간으로 모니터링해서 사용자가 입력할 때 키를 눌렀다가 놓는데 필요한 시간을 캡처해서 feature로 사용하는 연구가 진행되었다[14]. 유클리드 디스턴스를 이용하여 실험한 결과 FAR은 12.97%, FRR은 2.25%를 달성했다.

keystroke를 이용한 인증 기술의 정확도를 향상시키기 위해서 스마트폰에 내장된 센서를 이용한 연구가 진행되었다[16][17].

Giuffrida 등[16]은 센서를 이용한 향상된 keystroke dynamics를 제안하였다. 스마트폰에 내장된 고유한 센서를 통해 사용자의 타이핑 행동의 특징을 찾고 머신러닝 기법에 의존해 사용자 인증을 실시하는 것이 핵심 아이디어다. 제안된 기술의 효율성을 증명하기 위해 안드로이드 프로토타입을 구현했고 20명의 실험참가자를 대상으로 평가하였다. 실험 결과 keystroke에 의한 발생되는 센서 데이터를 이용하는 방법(EER >0.5%)이 keystroke 시간을 측정하는 방법(EER >7%)에 비해 훨씬 더 효과적이었다. 최고 성능을 기준으로 password 입력 시 정확도가 매우 높았다(EER=0.08%).

Keystroke dynamics를 이용한 인증기술은 별도의 장비가 필요 없는 기술로 설치비용이 절감될 수 있고 구현하기 쉽다는 장점이 있지만 다음과 같은 한계점 또한 존재한다.

- **한계점**: keystroke 패턴이 손의 생리적 변화에 따라 달라질 수 있어 정확도에 영향을 미칠 수 있다. 또한 현재까지의 진행된 연구들은 lab study 수준의 연구이기 때문에 실제 사용자가 사용했을 때 타이핑(typing) 패턴이 수시로 변경될 가능성이 있다.

3.2. Physiological biometrics

3.2.1. Face-based

스마트폰을 사용하고 있는 사용자가 합법적인 사용자인지 여부를 얼굴을 이용한 인증 기술들이 연구되고 있다([표 3] 참조).

일반적으로 얼굴 인식을 이용한 인증 기술 방법은 먼저 스마트폰의 정면 카메라를 이용하여 얼굴을 감지하고 감지된 얼굴에서 특징(feature)을 추출하고 마지막으로 인증을 위해 classifier에게 전달하는 단계로 구성 된다.

Fathy 등[18]은 스마트폰의 전면 카메라가 촬영한 영상을 이용한 active authentication 문제 해결을 위한 자동 얼굴 인식 방법에 대한 연구를 진행하였다. 촬영한 영상 중 얼굴일 가능성이 가장 높은 부분을 찾기 위해 주어진 프레임에서 얼굴 세그먼트를 검출하고 클러스터링 하는 방식을 사용했다.

Crouse 등[19]은 눈에 띄지 않게 작동하는 얼굴 기반 CA 연구를 진행하였다. 모바일 기기에서 얼굴 캡처를 할 때 자이로스코프, 가속도계 및 자력계 센서 데이터를 결합하여 카메라 방향을 수정한다. 이 결과를 기반으로 얼굴 이미지의 방향을 수정할 수 있는 방법을 제안하였

〔표 3〕 Face-based 기술 결과 요약(RR: Recognition Rate, TAR: True Acceptance Rate, FAR: False Acceptance Rate)

Study	Techniques	Features	Performance (%)
Fathy 등[18]	Classifier 9개 사용	mouth, two eyes, nose	RR: 95
Crouse 등[19]	SVM	Biologically inspired model	TAR: 40-50 (FAR: 0.1일 때)
Samangouei 등[20]	Binary attribute	Four types	EER: 13-30
Tsai 등[21]	HAAR classifier	48 × 48 image	Accuracy: 86.88

〔표 4〕 Finger-based 기술 결과 요약

Study	Techniques	Features	Performance (%)
Buduru 등[22]	SVM, kNN	Fingerprint image	Accuracy: 95
Ehatisham-ul-haq 등[23]	Boosted classifier	Fingerprint image	Accuracy: 86.866

다. 실험을 통해 얼굴 방향 보정을 통한 얼굴 인식 정확도의 향상과 CA의 프로타입을 구현하여 유효성을 입증하였다.

시각적인 속성은 기본적으로 외관을 설명하기 위해 이미지에 부여할 수 있는 라벨[15]인 반면 얼굴 속성 기반의 연속 인증 방법이 제안되었다[20]. 이미지에서 눈, 코, 입, 머리카락, 눈&코, 입&코, 눈&코&입, 눈&눈썹, 얼굴전체로 분할해서 총 9개의 얼굴 컴포넌트를 이용하였다. 실험 결과는 13-30%의 EER을 얻었다.

Tsai 등[21]은 얼굴 인식을 위한 interactive artificial bee colony optimization 알고리즘을 이용한 모델을 제안하였다. 실험 결과 실시간 CA 환경에서 정확도를 최대 86.88%까지 얻을 수 있었다. 얼굴 인식을 이용한 인증기술은 스마트폰의 전면 카메라를 이용하기 때문에 별도의 하드웨어 장비가 필요 없다. 상용 스마트폰에 적용할 때 다음과 같은 한계를 극복해야 할 필요가 있다.

- **한계점**: 얼굴인식을 수행하는 과정에서 얼굴의 자세가 변화하는 등의 이유로 정확도가 저하될 수 있다. 예를 들어 조명 조건, 머리 자세, 얼굴 액세서리, 표정, 노화 등은 정확도에 영향을 줄 것이다.

3.2.2. Finger-based

사용자의 finger gesture 또는 지문인식 등을 이용한 인증 방법은 일반적으로 등록, 검색, 확인의 3가지 기능이 이용된다. 등록은 센서에서 지문 이미지를 캡처하는 주요 역할을 한다. 사용자가 지문을 스캔하는 방식에 따라 검증 과정에 영향을 미칠 수 있다. Buduru 등[22]은 Markov 의사결정 과정(MDP)을 결합한 CA 기술을 제안 finger gesture 인증 기술을 제안하여 앞서 언급한 문제를 해결하였다. 제안한 방식은 트레이닝 할 필요는 없지만 메모리와 리소스를 더 많이 소비하게 된다는 단점이 있다. 결과는 [표 4]에 요약되어 있다.

Ehatisham-ul-haq 등[23]은 터치 기반 제스처 인식 기술을 제안하여 합법적인 사용자의 다른 손가락들이 터치스크린에 사용될 때 사용자를 인증하는 기술을 연구했다. 가속도계 센서를 이용해서 스마트폰의 위치(position)를 파악하고 사용된 손가락을 터치 기반 제스처를 이용해 파악한다. 제안된 기법은 대규모 데이터베이스가 필요하지 않고 공격으로부터 더 정확하고 안전하게 이미지를 분류할 수 있음을 보였다. 지문 인식을 이용한 인증기술은 다음과 같은 한계점이 존재한다.

- **한계점**: 지금까지 연구된 finger-based CA 인증 기술은 touch dynamics와 유사한 기술을 사용해서 인증을 수행하고 있다. 따라서 앞서 언급한 touch dynamics에서 갖고 있는 한계를 동시에 갖고 있다고 볼 수 있다. 또한 touch dynamics에 비해 사용자에게 정확한 터치를 요구할 수 있어 정확도 측면에서 실제 상용화하기에 많은 어려움이 따를 수 있다.

Ⅳ. Other techniques

이 장에서는 biometrics를 사용하지 않는 CA 연구에 대해 살펴본다.

4.1. Behavior-based profiling

Behavior-based profiling 기법은 스마트폰 사용자가 사용하는 애플리케이션이나 서비스 등을 이용하여 사용자를 인증한다. 예를 들어 사용자의 애플리케이션 사용 패턴을 일정 기간 동안 모니터링해서 사용자 프로파일을 생성한 뒤 사용자의 현재 애플리케이션 사용 패턴과 비교한다. 만약 상당한 편차가 발생한다면 합법적이지 않은 사용자가 폰을 사용하고 있다고 판단할 수 있다. 본 논문에서는 대표적으로 사용되는 서비스로 사용자의 위치에 따라 인증을 수행하는 location-based 인증 기술과 애플리케이션 사용패턴에 따라 인증을 수행하는 app usage 인증 기술에 대한 기존 연구에 대해 살펴본다.

4.1.1. Location-based 인증기술

사용자의 현재 위치를 기반으로 사용자를 인증하는 기술들이 연구되고 있다. 스마트폰 잠금 해제를 위한 인증 기술은 아니지만 스마트폰을 이용하여 모바일 거래를 위한 위치 기반 인증 및 허가 기법이 연구되었다[24].

사용자 위치기반 인증 기술의 가능성을 보여준 연구로써 Alawami 등[25]은 실내에서 합법적인 사용자만을 감지해서 안전한 실내 공간을 구축하는 것을 목표로 사용자의 신뢰할 수 있는 작은 영역(2m2) 내에서 사용자의 물리적 존재를 보장하는 fine-grained된 위치 기반 인증 시스템을 제안했다. 스마트폰 애플리케이션을 개발해서 데이터를 수집했다. 실험 결과 실험실에서 7개의 인접한 work cubicle을 구분할 수 있었다. SVM classifier를 이용한 결과 98.37%의 정확도를 얻을 수 있었다([표 4 참조]). 사용자 위치 기반 인증기술은 다음과 같은 한계점이 존재한다.

- **한계점**: GPS를 이용하여 사용자의 위치를 특정 하는 경우 오차로 인해 인증기술의 성능이 감소될 수 있다. 또한 기존연구에서 사용한 Wi-Fi, Bluetooth 등의 경우 지속적인 센싱으로 인해 배터리가 많이 소모되기 때문에 상용 스마트폰에 적용하기 위해서는 이 문제점을 해결해야 한다.

4.1.2. Application usage를 이용한 인증 기술

사용자의 앱 사용 패턴을 이용한 인증 기술 연구는 [표 5]에서 볼 수 있듯이 기존에 잘 알려진 dataset을 이용한 연구들이었다.

Li 등[26]은 MIT Reality 데이터셋을 이용하여 앱 사용 패턴 기반 인증 기술을 연구하였다. 앱 사용 항목이 6개일 때 14일 동안 사용자의 활동에 대해 동적 프로파일 기법을 사용하였으며, 최고 EER은 13.5%였다. 또한 과거 앱 사용 데이터를 이용한 연구도 진행되었다[27]. 규칙 기반 분류기, 동적 프로파일링 기법 및 스무딩 함수의 조합을 사용함으로써 사용자의 전체 앱 사용에 대한 결과는 EER 9.8%였다.

Neal 등[28]은 UND data (200) 데이터셋을 이용하였다. 일주일 동안 앱 사용 데이터를 이용한 결과 79.8%의 평균 recognition rate (RR)를 보였다. Mahbub 등[29]은 UMDAA-02와 Securacy 데이터셋을 이용하였다. Securacy 데이터셋을 이용했을 때 평균 EER이 16.16%였다.

애플리케이션을 이용한 인증기술의 한계점은 다음과 같다.

〔표 5〕 Behavior-based profiling 기법 결과 요약

Study	Behavior	Dataset	Classifier	Performance (%)
Alawami등[25]	Location information	Collected by authors	SVM	Accuracy: 98.37
Li 등[26]	Application usage	MIT Reality	Neural net	EER: 13.5
Li 등[27]	Historical usage data	MIT Reality	Neural net	EER: 9.8
Neal 등[28]	Application usage	UND dataset (200)	Nearest Neighbor	RR: 79.8
Mahbub 등[29]	Application usage	UMDAA-02 dataset, Securacy dataset	Marginally smoothed HMM	Mean EER: 16.16

• **한계점**: 애플리케이션을 사용한 기록이 일정정도 축적되어야 신뢰할 만한 수준의 정확도를 얻을 수 있다. 또한 애플리케이션을 사용하는 패턴이 변경되거나 새로운 애플리케이션이 추가되는 상황에서 정확도의 감소가 발생할 수 있을 것이다.

Ⅴ. 결 론

본 논문에서는 스마트폰에서 사용자를 지속적으로 인증할 수 있는 CA기술에 대한 연구 동향에 대해 알아보았다. 연구 동향에 대해 분석한 결과 각 기술의 특징에 대해 파악할 수 있었고 현재까지 연구들이 상용 스마트폰에 적용되지 못하는 한계가 존재한다는 결론을 얻을 수 있었다. 따라서 향후에는 한계점등을 해결한 솔루션 연구가 필요할 것이다.

참 고 문 헌

[1] K. Niinuma, U. Park, AK. Jain, “Soft Biometric Traits for Continuous User Authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, 2010.

[2] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, “Continuous and transparent multimodal authentication: Reviewing the state of the art,” *Cluster Computing*, vol. 19, no. 1, Mar. 2016.

[3] T. J. Neal and D. L. Woodard, “Surveying biometric authentication for mobile device security,” *Journal of Pattern Recognition Research*, vol. 1, pp. 74 - 110, 2016.

[4] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, “Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data,” *In Proceedings of International Conference on Biometrics*, 2015.

[5] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, “Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, 2013.

[6] H. Zhang, V. M. Patel, M. E. Fathy, and R. Chellappa, “Touch gesture-based active user authentication using dictionaries,” *In Proceedings of IEEE Winter Conference Applications of Computer Vision*, 2015.

[7] L. Li, X. Zhao, and G. Xue, “Unobservable re-authentication for smart phones,” *In Proceedings of 20th Network and Distributed System Security Symposium*, 2014.

[8] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, “Continuous Mobile Authentication using Touchscreen Gestures,” I*n Proceedings of IEEE Conference on Technologies for Homeland Security*, 2012.

[9] X. Zhao, T. Feng, W. Shi, and I. Kakadiaris, “Mobile User Authentication Using Statistical Touch Dynamics Images,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 11, 2014.

[10] W. Meng, W. Li, and D.S. Wong, “Enhancing touch behavioral authentication via costbased intelligent mechanism on smartphones,” *Multimedia Tools and Applications*, vol. 77, 2018.

[11] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, “Sensor-based Continuous Authentication of Smartphones’ Users Using Behavioral Biometrics: A Contemporary Survey,” *IEEE Transactions on Internet of Things Journal*, 2020.

[12] T. Y. Chang, C. J. Tsai, and J. H. Lin, “A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices,” *Journal of Systems and Software*, vol. 85, no. 5, 2012.

[13] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, “Keystroke-based User Identification on Smart Phones,” *In Proceedings of International Workshop on Recent advances in intrusion detection*, 2009.

[14] E. V. C. Urtiga and E. D. Moreno, “Keystroke-based biometric authentication in mobile devices,” *IEEE Latin America Transactions*, vol. 9, no. 3, 2011.

[15] N. Kumar, A. Berg, P. Belhumeur, and S. Nayar, “Describable visual attributes for face verification and image search,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 10, 2011.

[16] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, “I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics,” *In Proceedings of International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2014.

[17] T. Anusas-amornkul, “Strengthening password authentication using keystroke dynamics and smartphone sensors,” *In Proceedings of ACM International Conference on Information Communication and Management*, 2019.

[18] M. E. Fathy, V. M. Patel, and R. Chellappa, “Face-based active authentication on mobile devices,” *In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, 2015.

[19] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, “Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data,” *In Proceedings of International Conference on Biometrics*, 2015.

[20] P. Samangouei, V. M. Patel, and R. Chellappa, “Attribute-based continuous user authentication on mobile devices,” *In Proceedings of IEEE International Conference on Biometrics Theory, Applications and Systems*, 2015.

[21] P.W. Tsai, M.K. Khan, J.S. Pan, and B.Y. Liao, “Interactive Artificial Bee Colony Supported Passive Continuous Authentication System”, *IEEE Systems Journal*, vol. 8, no. 2, 2014.

[22] A.B. Buduru and S.S. Yau, “An effective approach to continuous user authentication for touch screen smart devices,” *In Proceedings of IEEE International Conference on Software Quality, Reliability and Security*, 2015.

[23] M. Ehatisham-ul-haq, M.A. Azam, U. Naeem, and J. Loo, “Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing,” *Journal of Network and Computer Applications*, vol. 109, no. C, 2018.

[24] F. Zhang, A. Kondoro, S. Muftic, “Location-based authentication and authorization using smart phones,” *In Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[25] M. A. Alawami, H. Kim, “LocAuth: A fine-grained indoor location-based authentication system using wireless networks characteristics,” *Computers & Security,* vol. 89, 2020.

[26] F. Li, N. Clarke, M. Papadaki, and P. Dowland, “Behaviour profiling for transparent authentication for mobile devices,” *In Proceedings of European Conference on Information Warfare and Security*, 2011.

[27] F. Li, N. Clarke, M. Papadaki, and P. Dowland, “Active authentication for mobile devices utilising behaviour profiling,” *International Journal of Information Security*, vol. 13, no. 3, 2014.

[28] T. Neal, D. Woodard, and A. Striegel, “Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits,” *In Proceedings of IEEE International Conference on Biometrics Theory, Applications and Systems*, 2015.

[29] U. Mahbub, J. Komulainen, D. Ferreira, R. Chellappa, “Continuous authentication of smartphones based on application usage,” *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 3, 2019.

〈저 자 소 개〉

조 금 환 (Geumhwan Cho)

2011년 2월 : 청주대학교 정보통신공학과 학사
2013년 2월 : 경희대학교 컴퓨터공학과 석사
2020년 8월 : 성균관대학교 컴퓨터공학과 박사
2020년 9월~현재 : 성균관대학교 정보통신대학 박사후연구원
<관심분야> Usable security, AI/ML security, 정보보호, 모바일 보안

김 형 식 (Hyoungshick Kim)

종신회원

1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 교수
<관심분야> 보안공학, 소셜 컴퓨팅