정 보 보 호 학 회 지
제28권 제1호, 2018. 2

Smart Lock 인증 기법에 대한 연구동향 분석

조 금 환*, 이 승 진*, 김 형 식**

요 약

전통적인 인증 기법(예: 패스워드, PINs, 안드로이드 패턴 락)들은 사용빈도가 많은 모바일 기기의 특성으로 인해 사용자에게 불편함을 가중시킨다. 본 논문에서는 사용성을 고려한 Smart Lock 인증 기법에서 사용되는 요소 기술에 대한 연구동향에 대해 분석하였다. 요소 기술 한 가지를 독립적으로 사용하는 방법보다는 다양한 요소 기술들을 동시에 활용한다면 보안성과 사용성을 모두 만족할 수 있는 인증 기법으로 사용될 것이다.

Ⅰ. 서 론

전통적으로 모바일 기기에서 사용자를 인증하기 위해 패스워드, PINs (Personal Information Numbers), 안드로이드 패턴 락과 같은 인증 기법들이 주로 사용되어 왔다. 그러나 다양한 센서들이 모바일 기기에 내장되면서 지문인식, 홍채인식과 같은 생체 정보 기반의 인증이 가능해졌으며[1,2], 사용하는 비율도 높아지고 있다. 최근 모바일 기기 사용자들은 생체 정보 기반의 인증 기법을 1차 인증 기법으로 사용을 하고 인증에 실패할 경우 대체 인증 기법으로 PINs 또는 안드로이드 패턴 락을 사용하는 방법을 채택하고 있다. 기존 연구결과에 따르면 Apple iPhone의 Touch ID 사용 이유에 대해 90%의 실험참가자가 “편리성” 때문에 사용한다고 답을 하였다[3]. 모바일 기기의 경우 PC나 Laptop에 비해 잠금 해제를 하는 비율이 높기 때문에 어떤 인증 기법이 사용자에게 많은 행위를 요구한다면 더 이상 사용되지 않을 것이다.

따라서 모바일 기기를 위한 보안적인 측면과 사용성 측면을 동시에 고려한 인증 기법이 요구된다. 이러한 요구사항을 반영한 기술로 Smart Lock이 대표적이다. Smart Lock에서는 4가지 기능(On-body detection, Trusted places, Trusted devices, Trusted voice)을 제공하며 이 기능들을 통해 사용자를 인증한다. 예를 들어 사용자가 Trusted places 기능을 사용한다고 하자. 사용자는 A라는 지역을 신뢰할 수 있는 지역으로 설정하고 사용자가 A 지역에 위치한 뒤 스마트폰을 사용한다면 별도의 인증 기법을 요구하지 않고 잠금 해제된 상태에서 바로 사용할 수 있다. Smart Lock의 대표적인 4가지 기능은 다음과 같이 간략하게 설명할 수 있다[4].

- **On-body detection:** 사용자가 스마트폰을 잠금 해제한 뒤 사용은 하고 있지 않지만, 지속적으로 스마트폰을 소유하고 있다고 판단되면 잠금 해제 상태로 유지하는 기법.
- **Trusted places:** 먼저 신뢰할 수 있는 지역을 추가하고, 추후에 해당 지역에서 스마트폰이 위치하면 잠금 해제되는 기법.
- **Trusted devices:** 먼저 신뢰할 수 있는 기기를 등록하고, 스마트폰 주변에 신뢰할 수 있는 기기가 위치하면 잠금 해제 상태로 유지하는 기법.
- **Trusted voices:** “Ok Google” 이라고 사용자가 말을 하면 사용자의 음성을 분석하여 잠금 해제를 수행하는 기법.

따라서 본 논문에서는 사용자 편의성을 고려한 인증 기술인 Smart Lock에서 사용되는 요소 기술에 대한 연구 동향에 대해 살펴본다. 본 논문의 구성은 다음과 같다. Ⅱ~Ⅴ장에서는 On-body detection, Trusted places, Trusted devices, Trusted voices에 사용되는 요소 기술의 연구 동향에 대해 각각 살펴보고, 마지막으로 Ⅵ장에서 본 논문에 대한 결론을 도출할 것이다.

* 성균관대학교 전자전기컴퓨터공학과 (geumhwan@skku.edu, jine33@skku.edu)
** 교신저자, 성균관대학교 전자전기컴퓨터공학과 (hyoung@skku.edu)

Ⅱ. On-body detection 인증 기법

모바일 기기의 가속도 센서, 자이로스코프 센서 등을 통해 사용자가 모바일 기기를 사용하거나 소지한 채 이동할 때의 기기의 움직임에 관련된 정보를 사용자 인증에 활용할 수 있다. 이 장에서는 On-body detection 기술에 필요한 요소 기술에 대해 살펴보고 On-body detection 인증 기법에 대한 기존 연구들에 대해 살펴본다.

2.1. On-body detection을 위한 기계학습 알고리즘

일반적으로 모바일 기기의 센서를 활용한 인증 기법에서는 기기가 인가된 사용자에 대한 특정 센서 값의 패턴을 인지해 암묵적인 인증을 수행해야 한다는 점에서 기계학습 알고리즘이 핵심적인 부분을 담당한다. 가속도 센서와 자이로스코프 센서 등을 활용하는 On-body detection과 같이 시간에 독립적인 데이터의 분류에 활용되는 대표적인 기계학습 알고리즘에는 Random Forest, SVM (Support Vector Machine), Naive Bayes 등이 있다. 특히 SVM은 [그림 2]와 같이 두 클래스를 가지는 데이터를 가장 잘 분류할 수 있는 최적의 초평면을 찾아내고 이 초평면을 통해 클래스를 가지지 않는 데이터를 분류하는 알고리즘으로 다른 알고리즘에 비해 학습 데이터가 적고 목표 클래스의 수가 2개(인가된 사용자, 인가되지 않은 사용자)로 적을 때에도 잘 동작하기 때문에 On-body detection 기반 사용자 인증 시스템에 관련된 많은 연구[5-9]에서 사용되고 있는 알고리즘이다.

2.2. On-body detection 기반 인증 기법

종래에 사용되어 온 인증 기법들은 인증 과정을 이미 수행한 사용자가 지속적으로 기기를 사용하고 있었음에도 상황에 따라 다시 인증 과정을 거쳐야 했다. 인증 과정은 사용자가 기기를 사용하는 주된 목적이 아니기 때문에 빈번한 인증 과정을 빠르게 통과하기 위해 많은 사용자들이 취약한 인증 솔루션을 선택하거나 인증 과정을 생략하게 되었다. On-body detection 기반 인증 기법 은 가속도계, 자이로스코프 등의 모바일 기기에 내장된 움직임 센서를 통해서 모바일 기기의 소프트웨어 키보드를 통해 텍스트를 입력하거나 전화를 받는 등의 자연스러운 사용자 행위 관련 정보를 수집해 사용자를 인증함으로써 종래 인증 기법의 문제점을 완화한다.

Maghsoudi 등[7]은 가속도계와 자이로스코프 센서를 통해 수집된 움직임 데이터를 여러 기계학습 알고리즘에 학습시키고 정확도를 평가함으로써 사용자 인증에서 기기 움직임 데이터의 활용 가능성을 분석했다. 총 60명의 실험 참가자는 모바일 기기를 소지한 채로 1,200 번의 걷기, 달리기, 계단 오르내리기 등의 행위를 수행했으며, 수집된 데이터의 학습에는 Naive Bayes, k-NN (k-Nearest Neighbor), MLP (Multi-Layer Perceptron), SVM의 네 가지 기계학습 분류 알고리즘이 사용되었으며 수집된 데이터는 가공되지 않은 간단한 형태 또는 평균 및 분산이 계산되는 복잡한 형태의 두 가지 방식의 특성 벡터로써 분류기 학습에 사용되었다. 가속도계만 사용했을 때와 가속도계, 자이로스코프의 두 가지 센서를 사용했을 때의 정확도를 비교하였다. 각 알고리즘의 정확도 평가는 10-fold 교차 검증을 사용했으며, 각 기계학습 알고리즘의 정확도 평가 결과는 [표 5]과 같다. 네 가지 기계학습 알고리즘 중 SVM이 가장 좋은 성능을 나타냈으며 일반적으로 가속도계만 사용했을 때보다 자이로스코프를 함께 사용했을 때 더 높은 정확도를 나타냈다.

Gascon 등[5]은 사용자가 모바일 기기의 소프트웨어 키보드를 통해 텍스트를 입력하는 행위(키 스트로크) 동안의 기기 움직임 패턴을 활용하는 사용자 인증 기법을 제안했다. 제안하는 기법에서는 가속도계, 자이로스코프, 방향 센서를 통해 사용자가 소프트 키보드를 사용하는 동안의 기기 움직임 관련 정보를 수집했으며, 추가적으로 터치 센서를 통해 스크린 터치 행위의 정확한 위치와 세기 등의 키 스트로크 관련 정보도 함께 수집했다. 제안 기법의 정확도 평가를 위해 총 315명의 실험 참가자들이 약 160자 길이의 문장을 모바일 기기의 소프트 키보드를 통해 입력하는 과정을 수행했다. 그 중

〔표 1〕 각 분류 알고리즘의 평가 결과

	Simple (acc)	Simple (both)	Complex (acc)	Complex (both)
N-B	82.7 %	83.2 %	81.1 %	83.6 %
k-NN	86.3 %	87.0 %	88.7 %	89.8 %
MLP	91.4 %	92.5 %	92.9 %	92.7 %
SVM	92.2 %	92.8 %	96.3 %	97.7 %

12명의 수집 데이터가 인가된 사용자의 학습 데이터로 사용되었고 나머지 303명의 수집 데이터는 인가되지 않은 사용자의 학습데이터로 사용되었다. 분류 알고리즘으로는 Linear SVM이 사용되었다. 그 결과, 키 스트로크 과정에서의 모바일 기기 움직임 패턴을 통해 92%의 TPR (True Positive Rate), 1%의 FPR (False Positive Rate)의 정확도로 특정 사용자가 인가된 사용자인지의 여부를 확인할 수 있었다.

Wei-Han Lee 등[9]은 On-body detection 기반의 사용자 인증 시스템의 정확도 향상을 위해 가속도계, 방향 센서를 통해 기기의 움직임 정보를 수집함과 동시에 모바일 기기의 자기계 센서를 통해 사용자와 모바일 기기 주변 환경 정보를 추가적으로 수집했다. 7명의 사용자가 3주 동안 모바일 기기의 여러 가지 센서를 통해 수집한 데이터인 GCU 데이터 셋[10]을 SVM 분류기의 학습에 활용했으며, 10-fold 교차 검증을 분류 알고리즘의 평가에 사용했다. 그 결과, 각 센서 데이터를 5초의 샘플링 레이트로 수집하고 자기계 센서 데이터를 사용하지 않았을 때 96.4%의 정확도로 인가된 사용자를 분류할 수 있었고 추가적으로 자기계 센서를 사용해 데이터를 수집했을 때 97.4%의 정확도로 인가된 사용자를 분류할 수 있었다.

Ⅲ. Trusted places 인증 기법

모바일 기기에서 수집 가능한 위치 정보를 통해 사용자의 정확한 위치를 판단하고 이를 사용자 인증에 활용하는 기법이며 수집된 위치 정보의 정확도가 인증 기법의 보안성에 직결된다. 이 장에서는 사용자 위치 정보를 활용한 인증 기법에 대해 살펴본다.

3.1. 사용자 위치 정보의 활용

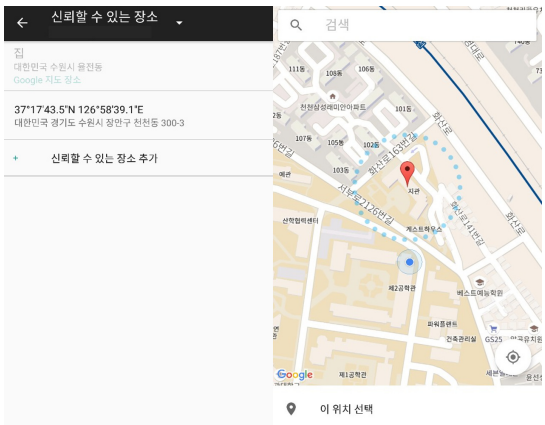
대부분의 모바일 기기에 내장되는 센서 중 하나인 GPS (Global Positioning System) 는 모바일 기기의 현재 위치 정보를 위도, 경도의 값을 가지는 좌표 쌍과 수집된 위치 정보 데이터의 정확도를 나타내는 실수 값을 통해 표현한다. 사용자의 위치 또는 경로 정보는 사용자의 행동 패턴을 나타내는 정보로서, 일반적으로 각 사용자 마다 지니는 행동 패턴이 다르기 때문에 사용자를 구별할 수 있는 특성을 지닌다. 또한 특수한 상황(예: 여행)을 제외하면 사용자는 대부분의 경우 자신에게 익숙한 장소와 경로를 다니며, 따라서 각 사용자의 시간에 따른 위치 또는 경로 패턴의 변화가 크지 않기 때문에 사용자의 위치 또는 경로 정보를 인증에 활용될 수 있다[11,12].

3.2. 사용자 위치 정보를 활용한 인증 기법

현재 상용화된 대표적인 위치 정보 기반 인증 기법으로 Smart Lock[4]에서 제공하는 Trusted places 기능이 있다. Trusted places 기능에서는 [그림 1]과 같이 GPS를 통해 수집한 사용자 위치와 사전에 사용자가 설정한 신뢰할 수 있는 장소들의 위치 정보 값을 비교해 모바일 기기의 잠금 여부를 결정한다. 그러나 GPS의 특성으로 인해 상황에 따라 수집되는 위치 정보의 정확도가 떨어질 수 있고 따라서 신뢰할 수 있는 장소의 범위가 커지기 때문에 사용자 위치 정보를 단일 인자로 인증 시스템에 활용하기에는 보안성이 떨어진다.

여러 종래 연구들[11-13]에서 사용자의 위치 정보를 활용한 인증 기법을 제안했다. 위치 정보가 가지는 한계점 때문에 이러한 연구들에서는 인증기법의 정확도를 높여 보안성을 향상시키기 위해 사용자의 위치 정보에 모바일 기기에서 수집할 수 있는 여러 센서 정보를 결합해 인증 시스템에 활용했다.

Elaine Shi 등[13]은 사용자 행위의 확률 모델링을 통한 인증 시스템을 제안했다. 제안하는 시스템에서는 사용자의 과거 위치, 통화 기록, 문자 기록, 웹 브라우저 사용 등의 행위 정보를 종합해 확률적으로 모델링하고

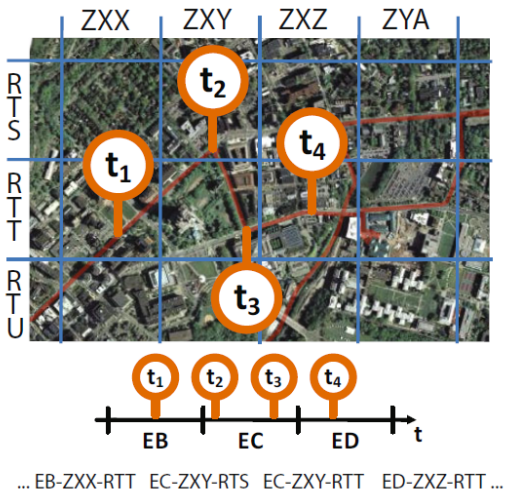


〔그림 1〕 Smart Lock에서 제공하는 Trusted places 기능

현재 수집된 정보들이 인가된 사용자일 확률을 통해 사용자를 인증한다. 사용자의 위치 정보의 경우 GPS 좌표값을 GMM (Gaussian Mixture Model)의 학습 데이터로 활용했으며, GMM 모델의 확률 밀도 함수 값을 통해 인가된 사용자가 특정 시간에 GPS 좌표에 해당하는 위치에 있을 확률을 계산한다. 제안하는 시스템의 사용자 인증 정확도를 평가하기 위해 총 276명의 참가자 중 12일 이상 기간 동안 실험에 참가한 50명의 참가자의 데이터를 통해 인가된 사용자를 모델링했으며, 3일 이상 실험에 참가한 참가자의 데이터를 통해 인가되지 않은 사용자를 모델링했다. 그 결과, 인가되지 않은 사용자가 6번 이하의 사용자 행위(예: 통화, 문자, 웹 브라우저 사용 등)를 발생시켰을 때 기기가 잠길 확률이 75%였으며, 10번 이하의 사용자 행위를 발생시켰을 때 기기가 잠길 확률이 95%였다.

Buthpitiya 등[12]은 GPS 센서 기록들을 활용해 사용자의 이동 패턴을 분석하기 위한 n-gram 기반의 사용자 경로 추적 모델을 제안했다. n-gram 모델은 연속되는 데이터를 모델링 할 때 유용한 모델링 기법으로 제안한 기법에서는 특정 시점에서 사용자의 과거 위치 정보를 통해 다음 경로를 예측하기 위해 사용된다. 제안 기법에서는 n-gram 모델의 학습 데이터로 일련의 위치 레이블(geo-label)을 사용했으며, 위치 레이블은 [그림 2]와 같이 GPS를 통해 수집한 위치 정보와 사용자가 해당 위치에 머무른 시간을 통해 구성된다. 제안 기법의 정확도를 판단하기 위해 특정 지역에 거주하는 10명의 사용자 중 8명의 사용자에게는 4주의 기간 동안 기록된 위치 정보를 수집했으며, 2명의 사용자에게는 2주 동안의 위치 정보를 수집했다. 수집된 위치 정보는 위치 레이블의 형태로 n-gram 모델의 학습에 사용되었다. 그 결과, n-gram 모델의 예측 정확도는 86.6%로 Markovian 모델의 정확도 76.8% 보다 10% 가량 향상된 정확도를 보여주었다.

Fridman 등[11]은 사용자 위치 정보와 소프트웨어 키보드를 통해 입력되는 텍스트, 어플리케이션 사용 패턴, 웹 사이트 방문 기록과 같은 행위 정보를 활용한 사용자 인증 시스템을 제안했다. 수집된 위치 정보는 SVM 분류기를 통해 인가된 사용자의 위치 정보 또는 인가되지 않은 사용자의 위치 정보로 이진 분류되었다. 입력되는 텍스트는 *n*-gram 분류기를 통해 이진 분류되었으며, 어플리케이션 사용 패턴과 웹 사이트 방문 기록



〔그림 2〕 GPS 센서 데이터를 통한 geo-label의 구성

은 각각 빈도수 상위 20개의 어플리케이션과 웹 사이트를 기준으로 이진 분류되었다. 각 분류기에서의 예측 결과는 Chair-Varshney optimal fusion rule[14]을 통해 종합되었다. 인증 시스템의 평가를 위해 총 200명의 참가자들에 대해 최소 30일의 기간 동안 누적된 데이터를 수집했으며, 5-fold 교차 검증을 통해 시스템의 정확도를 분석했다. 그 결과, 1분 단위의 사용자 인증에서는 0.05의 EER (Equal Error Rate), 30분 단위의 사용자 인증에서는 0.01의 EER의 성능을 보였다.

Ⅳ. Trusted devices 인증 기법

모바일 기기 인증을 위해 주변의 신뢰할 수 있는 기기를 등록한 뒤 잠금 해제를 수행하는 기법에 대한 연구는 많이 진행되고 있지 않다. 신뢰할 수 있는 기기를 이용한 인증 기술은 보통의 경우 다른 기술의 정확도를 향상시키기 위해 사용되는 경우가 많다.

Agadakos 등[15]은 위치정보의 정확도를 향상시키기 위해 IoT 기기를 사용하는 연구를 진행하였다. 기본적으로 위치정보를 활용하여 사용자 인증을 수행하는 방법을 제안하였으며 스마트폰의 GPS 센서에만 의존하지 않고 획득할 수 있는 주변의 다른 정보들을 통합하여 사용자의 위치정보 획득의 정확도를 향상시켰다.

신뢰할 수 있는 기기를 이용한 기술은 산업계에서 개발되어 사용되고 있다. 삼성의 갤럭시 S8 시리즈부터 해당 기능을 사용하고 있다. 신뢰할 수 있는 기기를 이

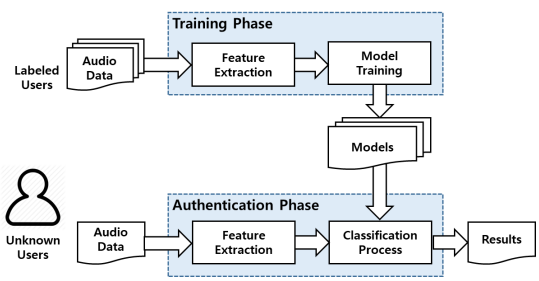
용해서 스마트폰의 잠금을 자동적으로 해제하는 방법이다. 예를 들어 블루투스 기능이 내장된 자동차를 신뢰할 수 있는 기기로 등록을 하면 자동차에 탑승하는 것만으로 잠금 해제가 이루어진다. 그러나 신뢰할 수 있는 기기를 판단하는 기준이 블루투스에 한정되어 있는 점은 블루투스 자체의 보안위협들[16]로 인해 위협이 될 수 있기 때문에 다양한 방법으로 해당 기술을 구현할 수 있는 노력이 필요하다.

Ⅴ. Trusted voices 인증 기법

모바일 기기를 사용하는 사용자의 음성을 인식하여 합법적인 사용자를 인증하는 기법으로 사용자의 음성을 정확하게 인식하는 기술이 요구된다. 이 장에서는 음성 인식 기술에 필요한 요소 기술에 대해 살펴보고 음성 정보 기반 인증 기법에 대한 기존 연구들에 대해 살펴본다.

4.1. 음성 인식을 위한 기계학습 알고리즘

대부분의 음성 인식 기반의 인증 기법은 사용자의 음성 샘플을 트레이닝 하는 부분과 음성 정보를 인식하는 부분이 포함된다[17-20]. 음성 인식 기반 인증 기법은 사람의 목소리 특징이나 문화적인 배경(예: 사용하는 언어) 등에 따라 달라질 수 있기 때문에 매우 엄격한 트레이닝 과정이 수반되어야 한다. 이러한 음성 인식 기반 인증 기법에서 사용되는 대표적인 기계학습 알고리즘으로 MFCC (Mel Frequency Cepstral Coefficients), DTW (Dynamic Time Wrapping)[21], HMM (Hidden Markov Model)[22] 등이 사용된다. 이 중에서 MFCC가 인간의 소리를 인식하는 방법을 보여주는 모델로 가장 많이 사용되는 기계학습 알고리즘이다.



〔그림 3〕 오디오 데이터를 사용한 인증 기법

[그림 3]은 일반적인 오디오 데이터를 사용한 인증 기법의 예이다. 인증 기법을 사용하기 위해 사용자의 음성 정보를 트레이닝을 거치고 앞서 언급한 기계학습 알고리즘을 활용하여 모델링을 한다. 그 후 사용자가 인증을 시도할 때는 Classification Process를 통해 사용자가 인간된 사용자인지를 판단하도록 한다.

4.2. 음성 인식 기반 인증 기법

최근 Alexa, Siri, Google Now와 같은 음성 보조 장치가 다양하게 사용되고 있다. 특히 사용자가 운전 중이거나 운동 중 일 때 또는 터치 인터페이스를 사용하기 어려운 환경에서 사용될 수 있기 때문에 중요성이 더 부각되고 있다. 그러나 음성 인식 채널의 개방된 특성 때문에 안전하게 사용하기 어렵다는 단점이 존재하며, 기존

연구에서 입증된 바와 같이 다양한 위협에 노출되어 있다. 이러한 문제점을 극복하기 위해 다양한 연구들이 진행되고 있다.

Thullier 등[23]은 독립적인 스피커를 기반으로 하는 새로운 모바일 기기 인증 시스템을 제안하였다. 모바일 기기에서 모든 프로세싱이 진행되기 때문에 클라이언트-서버 모델과 같이 많은 비용을 필요로 하지 않는다. 제안하는 시스템은 세 가지 크게 3 가지 과정을 통해 사용자의 음성을 인식한다. 1) 오디오 신호로부터 개별 음성 특징을 추출해서 데이터 셋을 만들고, 2) 해당 데이터 셋을 naive Bayes 분류기를 이용하여 트레이닝 하고, 3) Decision-making 기법을 이용하여 인증 여부를 결정한다. 제안한 시스템의 테스트를 위해 11명의 학생을 모집하여 사용자 스터디를 진행하였다. 그 결과 조용한 환경에서는 91%의 정확도를 보였고, 잡음이 있는 환경에서는 82%의 정확도를 보였다.

Boles 등[24]은 딥러닝을 이용한 음성 인식 기반 인증 시스템을 제안하였다. 오디오 파일로부터 음성 인식이 가능하다는 것을 실험을 통해 확인하였고 제안하는 시스템은 오디오 파일의 상태(quality)와 관계없이 높은 확률로 인식할 수 있다. 오디오 파일을 n 초마다 분리하고 분리된 각각의 오디오에 대해 MFCC 알고리즘을 이용해 계산한 뒤 모델링 과정을 통해 사용자의 음성을 인식한다. 테스트 셋을 사용했을 때 98%의 인식률을 나타냈다. Dovydaitis 등[25]도 유사한 방법을 통한 사

용자 인증 기법을 제안해서 100%의 인식률을 나타냈다. 그러나 위의 연구들은 실시간으로 사용자의 음성을 입력받아 인식하는 방법이 아니기 때문에 실제 모바일 기기에서 사용하는데 한계가 존재한다.

실제 모바일 기기에서 사용가능한 음성 인식 기반 사용자 인증 기법에 대한 연구들이 진행되었는데, Yan 등[10]은 수동으로 입력할 필요 없는 안전한 음성 인식 인증 시스템을 제안하였다. 개인적인 질문을 통해 사용자 인증의 사용성을 높이고 기존 인증 기법들의 약점을 극복하는 시스템을 목표로 하였다. 인증을 허가하는 시스템에서 사용자가 미리 등록한 다양한 코드(예: 단어)를 말하도록 유도한 뒤 사용자가 관련된 코드를 말하면 시스템에서 사용자 음성 인식과 동시에 코드의 유효성을 검사하는 방식으로 사용자 인증을 수행한다. 제안 시스템의 정확도를 알아보기 위해 15명의 참가자를 모집하여 실험한 결과 평균 80.6%의 인식률을 보였다. Johnson 등[27]은 유사한 방법으로 사용자만이 알 수 있는 답에 대한 질문을 시스템에서 요청하고 사용자는 이에 대한 답을 함으로써 보안성을 더 강화하는 인증 시스템을 제안하였다. 보안성을 고려하여 사용자 지식 기반 인증 기법의 요소를 추가하였지만 이로 인해 정확도가 감소할 수 있다는 단점이 존재한다. 또한 녹음을 한 뒤 재사용하는 공격과 같이 다양한 보안 위협에 대한 요구가 필수적일 것이다.

따라서 실제 모바일 기기에서 높은 정확도 및 강력한 보안을 만족하기 위해서는 정확한 음성 인식 기술 뿐만 아니라 다양한 보안 위협을 고려해야 한다. 예를 들어 앞서 언급한 재사용성 공격의 경우 사람이 직접 말하는 음성이 아니므로 이를 구분할 수 있는 연구가 요구된다.

Ⅵ. 결 론

본 논문에서는 모바일 기기 인증 시 사용자의 편의성을 향상시킬 수 있는 Smart Lock 기능의 요소 기술에 대한 연구 동향을 파악하였다. 연구 동향에 대해 분석한 결과 각 기술의 특징에 대해 파악할 수 있었다. 또한 현재까지 연구결과들은 단일 솔루션으로 인증 기법에 활용하기에는 한계가 존재한다는 결론을 얻을 수 있었다.

따라서 향후에는 단일 솔루션을 이용하는 기술보다는 사용가능한 기술들을 모두 고려하여 인증함으로써 정확도를 더욱 향상 시킬 수 있는 개발이 요구된다.

참 고 문 헌

[1] Apple Touch ID, https://support.apple.com/en-us/HT204587, Accessed: 2018-02-01.

[2] Iris Scanner, http://www.samsung.com/global/galaxy/galaxy-s8/security/ Accessed: 2018-02-01.

[3] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, Konstantin Beznosov, “On the Impact of Touch ID on iPhone Passcodes,” *Usenix Symposium On Usable Privacy and Security*, 2015.

[4] Samsung Smart Lock, https://www.sams ung.com/us/support/answer/ANS00062631/, Accessed: 2018-02-01.

[5] Hugo Gascon, Sebastian Uellenbeck, Christopher Wolf, and Konrad Rieck, “Continuous authentication on mobile devices by analysis of typing motion behavior,” *In Proceedings of GI Conference Sicherheit*, 2014.

[6] Yazan Badin, “Contextual authentication using mobile phone movements to authenticate owners implicitly,” *Master Thesis, University of Twente Department of Computer Science, Enschede*, 2016.

[7] Javid Maghsoudi, and Charles C. Tappert, “A behavioral biometrics user authentication study using motion data from android smartphones,” *European Intelligence and Security Informatics Conference*, IEEE, 2016.

[8] Wei-Han Lee, and Ruby Lee, “Implicit sensor-based authentication of smartphone users with smartwatch,” *In Proceedings of the Hardware and Architectural Support for Security and Privacy*, 2016.

[9] Wei-Han Lee, and Ruby B. Lee, “Multi-sensor authentication to improve smartphone security,” *In Proceedings of International Conference on Information Systems Security and Privacy*, 2017.

[10] Hilmi G. Kayacık, Mike Just, Lynne Baillie, and David Aspinall, “Data driven authentication: On the effectiveness of user behaviour

modelling with mobile device sensors," *Mobile Security Technologies*, 2014.

[11] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam, "Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS Location," *System Journal*, IEEE, 2017.

[12] Senaka Buthpitiya, Ying Zhang, Anind K. Dey, and Martin Griss, "n-gram geo-trace modeling", International Conference on Pervasive Computing, 2011.

[13] Elain Shi, Yuan Niu, Markus Jakobsson, and Richard Chow, "Implicit authentication through learning user behavior," *In Proceedings of International Conference on Information Security*, 2010.

[14] Z. Chair and P. Varshney, "Optimal data fusion in multiple sensor detection system", *IEEE Transactions on Aerospace and Electronic System*, 1986.

[15] Ioannis Agadakos, Per Hallgren, Dimitrios Damopoulos, Andrei Sabelfeld, and Georgios Portokalidis, "Location-enhanced Authentication using the IoT *Because You Cannot Be in Two Places at Once*," *In Proceedings of Annual Computer Security Applications Conference*, 2016.

[16] John Paul Dunning, "Taming the Blue Beast A Survey of Bluetooth-Based Threats," *IEEE Security & Privacy 8 (2)*, 2010.

[17] Mossab Baloul, Estelle Cherrier, and Christophe Rosenberger, " Challenge based speaker recognition for mobile authentication," *In Proceedings of the International Conference on Biometrics Special Interest Group*, IEEE, 2012.

[18] Cory Cornelius, Zachary Marois, Jacob Sorber, Ron Peterson, Shrirang Mare, and David Kotz, "Vocal resonance as a passive biometric," 2014.

[19] Amitava Das, Ohil K Manyam, Makarand Tapaswi, and Veeresh Taranalli, "Multilingual spoken-password based user authentication in emerging economiesusing cellular phone networks," *In Spoken Language Technology Workshop*, IEEE, 2008.

[20] Max Kunz, Klaus Kasper, Herbert Reininger, Manuel Möbius, and Jonathan Ohms, "Continuous Speaker Verication in Realtime," *In Proceedings of the International Conference on Biometrics Special Interest Group*, IEEE, 2011.

[21] Mumtaj Begam Lindasalwa Muda and I. Elamvazuthi, "Voice Recognition Algorithms using Mel Frequency Cepstral Coecient (MFCC) and Dynamic Time Warping (DTW) Techniques," *Journal Of Computing 2, 3*, *138 – 143*, 2010.

[22] X. D. Huang, Y. Ariki, and M. A. Jack, "Hidden Markov Models for Speech Recognition," 1990.

[23] Florentin Thullier, Bruno Bouchard and Bob-Antoine J. Menelas, "A Text-Independent Speaker Authentication System for Mobile Devices," *cryptography, 1(3), 16*, 2017.

[24] Andrew Boles and Paul Rad, "Voice Biometrics: Deep Learning-based Voiceprint Authentication," *In Proceeding of International Conference on System of Systems Engineering*, 2017.

[25] Laurynas Dovydaitis, Tomas Rasymas, and Vytautas Rudžionis, "Speaker Authentication System Based on Voice Biometrics and Speech Recognition," *In Proceedings of International Conference on Business Information Systems*, 2017.

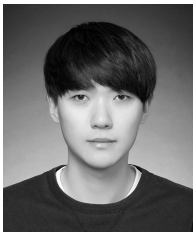
[26] Zheng Yan and Sihui Zhao, "A Usable Authentication System based on Personal Voice Challenge," *In Proceedings of International Conference on Advanced Cloud and Big Data*, 2016.

[27]R.C. Johnson, Terrance E. Boult, and Walter J. Scheirer, "Voice authentication using short phrases: Examining accuracy, security and privacy issues," In Proceedings of IEEE 6th International Conference on Biometric: Theory, Applications and Systems, 2017.

〈저 자 소 개〉

조 금 환 (Geumhwan Cho)
학생회원

2011년 2월 : 청주대학교 정보통신공학과 학사
2013년 2월 : 경희대학교 컴퓨공학과 석사
2014년 9월~현재 : 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : Usable security, 정보보호, 모바일 보안



이 승 진 (Seungjin Lee)
학생회원

2017년 2월 : 성균관대학교 컴퓨터공학과 학사
2017년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 네트워크 보안

김 형 식 (Hyoungshick Kim)
종신회원

1999년 2월 : 성균관대학교 정보공학부 학사
2001년 2월 : KAIST 컴퓨터 과학과 석사
2012년 2월 : University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 조교수
관심분야 : 보안공학, 소셜 컴퓨팅