JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 4, pp. 119-127, April 2026
https://doi.org/10.9708/jksci.2026.31.04.119

A Comprehensive Survey on Behavioral Biometric Authentication

Giluk Kang*

*Ph.D., Dept. of Computer and Information Security, Sejong University, Seoul, Korea

[Abstract]

With the development of information and communication technology (ICT), various ICT-based services are being utilized across society. However, as concerns are raised about the leakage of sensitive information in some services, user authentication is being introduced to prevent this leakage. User authentication is the process of verifying a user's identity when they attempt to access a service or system, and it has recently been studied based on various authentication factors. In particular, biometric authentication is gaining attention as the collection and analysis of high-quality biometric data are enabled by the development of the Internet of Things and artificial intelligence. Therefore, this paper analyzes recent research trends on behavioral biometric authentication, a subfield of biometric authentication. In particular, this paper presents a taxonomy that categorizes authentication factors used in existing studies by authentication device, thereby providing a structured understanding and meaningful insights into the behavioral biometric authentication field. This paper also presents future research directions for behavioral biometric authentication based on the limitations of prior studies, to facilitate the advancement of the field.

▸ **Key words**: User authentication, Behavioral biometric authentication, Internet of things, Artificial intelligence, User's identity

[요 약]

정보통신기술(information and communication technology, ICT)의 발전과 더불어 다양한 ICT 기반 서비스가 사회 전반에서 활용되고 있다. 그러나 일부 서비스에서 민감정보 유출에 대한 우려가 제기됨에 따라, 이를 방지하기 위한 사용자 인증이 도입되고 있다. 사용자 인증은 서비스 또는 시스템에 접근하려는 사용자의 신원을 검증하는 과정으로, 현재 다양한 인증 요소를 기반으로 연구되고 있다. 특히 사물인터넷과 인공지능의 발전으로 고품질 생체 데이터의 수집과 분석이 가능해지면서, 생체기반 인증이 주목받고 있다. 이에, 본 논문에서는 이러한 생체기반 인증의 하위 분야인 행위기반 인증의 최근 연구 동향을 분석하고자 한다. 특히, 기존 연구에서 사용된 인증 요소를 인증 기기별로 정리하여 분류체계를 제시함으로써 행위기반 인증 분야의 체계적인 이해와 의미 있는 통찰을 제공하고자 한다. 또한, 기존 연구들의 한계점을 토대로 행위기반 인증의 향후 연구 방향을 제시하여 해당 분야의 발전을 촉진하고자 한다.

▸ **주제어**: 사용자 인증, 행위기반 인증, 사물인터넷, 인공지능, 사용자 신원

• First Author: Giluk Kang, Corresponding Author: Giluk Kang
*Giluk Kang (giluk1027@sju.ac.kr), Dept. of Computer and Information Security, Sejong University
• Received: 2026. 01. 22, Revised: 2026. 03. 20, Accepted: 2026. 03. 23.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

정보통신기술(information and communication technology, ICT)의 발전과 함께 4차 산업혁명 시대가 도래하면서, 다양한 ICT 기반 서비스가 일상생활과 산업 전반에 도입되어 사회 발전에 이바지하고 있다. 구체적으로, 일상생활에서 사물인터넷(Internet of things, IoT) 기반 서비스가 개인 맞춤형 건강 관리 기능을 제공하여 삶의 질 향상에 기여하고 있다. 또한, 클라우드 기반 서비스는 기업의 비즈니스 전반에 사용되어 각종 시스템 구축 및 운영 비용을 절감시키고 필요한 만큼의 컴퓨팅 자원을 제공하여 자원 활용의 유연성을 보장하고 있다.

이처럼 ICT 기반 서비스의 활용이 증가함에 따라 그 영향력이 점차 확대되고 있으나, 고품질의 서비스를 보장하기 위해 일부 보안이 취약한 IoT 기기를 통해서도 민감 데이터가 무분별하게 수집되면서 데이터 유출에 대한 우려가 제기되고 있다. 특히, 2021년 약 40만 가구의 월패드 카메라 영상이 온라인에 유출되는 사고가 발생하며 이러한 우려가 현실화되기도 했다 [1]. 게다가, 기업이 ICT 기반 서비스를 토대로 디지털 전환을 하는 과정에서 이익과 직결된 기밀정보 또는 사용자 개인정보가 유출되면, 기업에 직접적인 피해를 초래할 수 있어 도입에 앞서 서비스 보안 강화를 요구하고 있다. 이러한 유출 우려와 기업의 요구에 따라, 현재 대부분 ICT 기반 서비스는 사용자 인증 기술이 도입하여 민감정보의 무단 접근 및 의도치 않은 유출을 방지하고자 노력하고 있다.

사용자 인증은 서비스 또는 시스템에 접근하려는 사용자가 정당한 사용자인지를 인증 요소를 토대로 신원 검증하는 과정으로, Fig. 1에서 보듯이 세 가지 인증 방식(지식기반, 소유기반, 생체기반)을 분류된다.

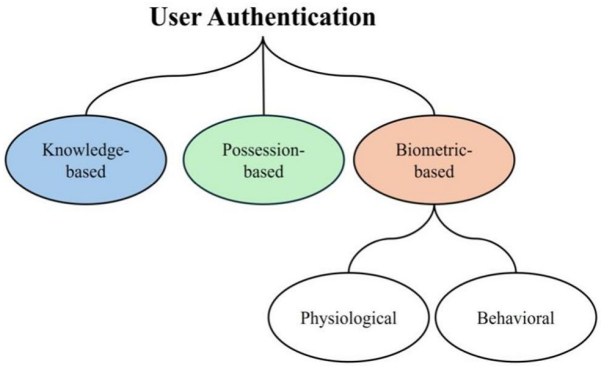

Fig. 1. Classification of User Authentication

여러 인증 방식 중에서도 IoT 기기를 통해 다양하고 고품질의 생체 데이터를 취득할 수 있을 뿐만 아니라 인공지능(artificial intelligence, AI)을 활용한 정밀한 데이터 분류가 가능해짐에 따라 생체기반 인증 연구가 활발히 진행되고 있다. 게다가, 제로 트러스트(zero trust) 보안 모델의 등장과 함께 사용자에 대한 지속 인증의 필요성이 주목받아, 이를 달성할 수 있는 생체기반 인증의 관심이 더욱 증가하는 상황이다.

이에, 본 논문에서는 생체기반 인증 중에서도 행동학적 특성을 활용하는 행위기반 인증 기술의 연구 동향을 분석하여 향후 행위기반 인증 연구의 활성화와 발전의 토대를 제공하고자 한다. 이를 위해, 기존 연구에서 사용된 인증 요소를 인증 기기를 중심으로 정리하여 분류체계를 제시함으로써 해당 연구 분야에 대한 체계적인 이해를 돕고자 한다. 또한, 기존 연구의 한계점을 토대로 향후 해당 분야의 발전을 위한 연구 방향을 구체적인 방법과 함께 제시하고자 한다. 본 논문의 나머지 구성은 다음과 같다. II 장에서는 최근 행위기반 인증 기술을 분류하고 주요 연구를 소개하고 인증 기기를 중심으로 하는 분류체계를 제공한다. III 장에서는 분석된 기존 연구를 토대로 향후 연구 방향을 제시한다. 마지막으로, IV 장에서는 결론을 맺는다.

II. Related Work in Behavioral Biometric Authentication

앞서 언급했듯이, AI의 발전과 제로 트러스트 보안 모델의 등장과 함께 다양한 행위기반 인증 기술이 개발되고 있다. 본 장에서는 이러한 인증 기술의 연구 동향을 사용되는 인증 기기를 중심으로 분류하고 주요 연구를 소개한다.

1. Literature Review Process

다양한 행위기반 인증 기술을 소개하기에 앞서, 본 절에서는 관련 연구를 수집하기 위해 수행한 문헌 수집 절차를 자세히 설명한다.

본 논문은 학술 데이터베이스인 IEEE Xplore를 중심으로 문헌 검색을 수행했다. 구체적으로, 검색 키워드를 “Behavior*” AND “Authentication”으로 설정하고 2019년부터 2025년까지 발표된 Journal 유형의 논문을 대상으로 초기 수집을 진행했다. 초기 수집을 통해 식별된 719편의 논문 중 제목과 초록을 검토하여 12편의 관련 논문을 선별했으며, 이를 인증 기기에 따라 분류했다.

이후, 인증 기기별로 최대한 4~5편 이상의 연구가 포함될 수 있도록 IEEE Xplore 외에도 대표적인 학술 데이터베이스인 ScienceDirect와 SpringerLink를 활용하여 추

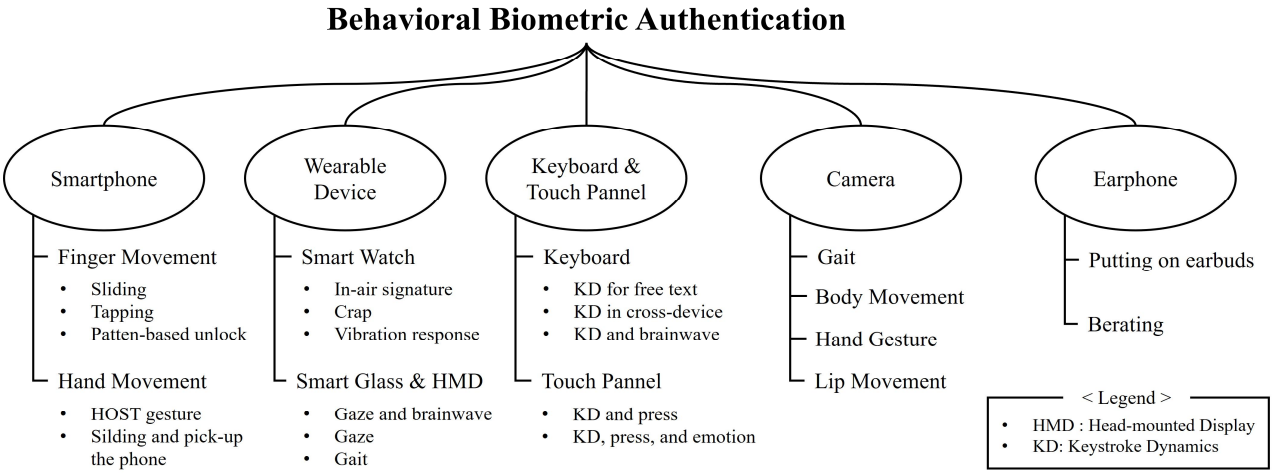

Fig. 2. A taxonomy of behavioral biometric authentication

가 검색을 수행했다. 이때 동일한 분류 조건에서 인증 수단을 기반으로 한 검색 키워드(예: “Behavior” AND “Authentication” AND “Smartphone*”)를 사용했으며, 최종적으로 22편의 대표 논문이 선정됐다. Fig. 2는 이러한 대표 논문을 바탕으로 도출한 인증 기기 중심의 행위기반 인증 요소 분류체계를 나타낸다. 또한, Table 1은 해당 연구들을 간략히 분석하여 정리한 것이다.

2. Smartphone

스마트폰(smartphone)은 다양한 IoT 센서가 탑재된 개인 기기로서 사용자 인증에 여러 이점(예: 다양한 생체 데이터 수집 가능)을 제공하고 있어, 이를 기반으로 한 행위기반 인증 기술이 꾸준히 개발되고 있다. 특히, 사용자가 스마트폰과 상호작용하는 지속시간이 길지 않다는 점으로 인해 사용자 식별에 어려움이 있어 다양한 센싱 데이터(sensing data)를 융합하거나 같이 활용하는 멀티모달(multi-modal) 방식으로 연구가 주로 이뤄지고 있다.

다양한 연구 중에서도 스마트폰 화면 상 다양한 콘텐츠(content)를 제어하기 위한 손가락 움직임을 토대로 사용자를 인증하는 방식이 주로 다뤄지고 있다. 대표적으로, Xie 외 [2]는 손가락을 화면에 슬라이딩(Sliding)하는 동안 가속도계와 진동 센서를 활용하여 지속 인증을 수행하는 방법을 제안했다. 제안 방법은 스마트폰이 손가락 움직임을 감지하면 진동 센서가 신호를 발생시키고, 이에 따라 생성된 진동 반응을 가속도계를 통해 수집하여 인증 데이터로 활용하는 방식이다. 이 밖에도, 화면을 탭하는 과정에서 발생하는 진동 반응과 탭 위치 좌표, 접촉 면적, 압력, 지속시간 등 다양한 터치(touch) 관련 데이터를 활용하는 멀티모달 기반 인증 기술 [3]과 패턴(patten) 기반 잠금 해제 과정에서 수집된 미끄러질 때 가해지는 압력 데이터와 주변 환경 센서의 데이터(예: 손가락으로 화면을 터치하는 리듬, 손가락 움직임 경로)를 같이 활용하는 암묵적 사용자 인증 방식 [4]도 연구됐다.

한편, 스마트폰과 상호작용하기 위한 손 자체 움직임을 인증에 활용하는 방식도 연구되고 있다. Wu 외 [5]는 Fig. 3(a)와 같이 사용자가 스마트폰을 움켜쥐는 행동을 토대로 사용자 인증을 수행하는 방법을 개발했다. HOST라고 정의된 해당 행동은 Fig. 3(b)에서 보듯이 화면상에 세 손가락을 두고 엄지손가락으로 전원 버튼을 누르면 압력 데이터 외에도 손가락 간의 기하학적 특징(예: 각도, 거리)과 손가락을 대고 떼는 순서 및 유지 시간 등을 수집할 수 있도록 설계됐다.

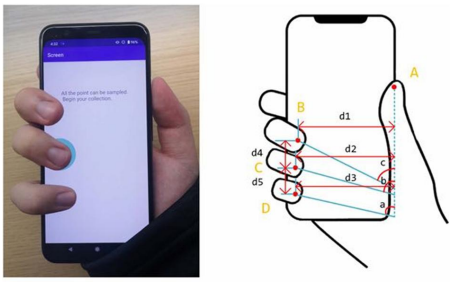

Fig. 3. HOST Gesture [5]

또한, Buriro 외 [6]은 스마트폰으로 전화를 받는 행위를 기반으로 사용자를 인증하는 방법을 제안했다. 해당 방법은 사용자가 앉거나 서거나 걷는 도중 전화가 수신되면, Fig. 4와 같이 화면을 슬라이딩하여 스마트폰 잠금을 해제하고 기기를 귀에 가까이 들어 올리는 과정에서 5가지 센서(예: 가속도계, 자이로스코프)로부터 수집된 데이터를 인증에 활용한다.

Table 1. Summary of related studies on behavioral biometric authentication

Type	Related work	Used sensors or devices	Number of participants	Behavior	Biometric features	ERR (%)	Continuous authentication
Smart phone	[2]	Vibration, Accelerometers	40	Sliding	Duration, Force, Path	-	O
	[3]	Touchscreen, Accelerometers, Gyroscope	40	Tapping	Coordinates, Pressure, Area size, Duration, etc.	2.95	O
	[4]	Barometer, Accelerometers, Gyroscope	23	Patten-based unlock	Finger movement path, Coordinates, Pressure, Drawing rhythm, etc.	0.47	X
	[5]	Touchscreen, Pressure	20	HOST Gesture	Hand geometry, Pressure, Timestamps, etc.	1.25	X
	[6]	Touchscreen, Gravity, Magnetometer, Gyroscope, etc.	85	Sliding and Pick up the phone	Velocity, Acceleration, Pressure, Coordinates etc.	-	X
Wearable device	[7]	Smart watch, Accelerometers, Gyroscope	22	In-air Signature	Velocity, Time consumption, Attitude, etc.	0.83	X
	[8]	Smart watch, Accelerometers, Gyroscope	50	Crap	Electromyography, Arm movements	-	X
	[9]	Smart watch, Vibration, Gyroscope, etc.	20	-	Response vibration's statistical features (e.g, Standard deviation)	2.96	X
	[10]	Eye tracker, EEG headset	30	Visual stimuli	Gaze and Brainwave	0.3	X
	[11]	VR headset	128	Taking	Gaze	-	O
	[12]	AR headset	20	Walking	Head movement	2.9	O
Keyboard & Touch panel	[13]	Keyboard	103	Typing	Standard timing features	7.8	O
	[14]	Keyboard	About 160,000	Typing	Standard timing features, Average keystrokes per minute, etc.	-	O
	[15]	Keyboard	10	Inputting password	Standard timing features, Brainwave	10.47	X
	[16]	Piezoelectric touch panel	10	Inputting password	Frequency domain, Release-press time, etc.	-	X
	[17]	Piezoelectric touch panel	14	Inputting password	Dwell time, Release-press time, Pressure	-	X
Camera	[18]	Camera	10	Gait	Distance among body parts (e.g., nose)	-	O
	[19]	3D motion capture camera, IR-reflective markers	39	Swiping	Marker-based speed, Body part and smartphone distance, etc.	5.4	O
	[20]	RGB camera	50	Hand Gesture	Hand shape, Each finger movement speed, etc.	6.22	X
	[21]	Camera	33	Utterance	Lip appearance, Speech contents, Style of speech	0.35	X
Earphone	[22]	In-ear microphone	35	Breathing during activities	Respiratory tract resonance, Body asymmetry, etc.	3.5	O
	[23]	In-ear microphone	50	Putting on earphone, activities (e.g., walking)	Rubbing, Inner organs' sounds	5	O

Fig. 4. Authentication sequence based on behavior to answer a call [6]

3. Wearable Device

실생활에서 스마트 워치(smart watch)와 같은 웨어러블 기기(wearable device)가 널리 활용되고 있음에 따라, 이를 활용한 사용자 인증 연구가 활발히 연구되고 있다. 특히, 스마트워치는 사용자 건강 관리를 지원하기 위해 심전도, 혈중산소포화도 등을 측정하는 센서가 탑재되어 있어 생리학적 생체기반 인증 연구가 주로 수행되고 있으나, 가속도계와 자이로스코프 센서를 이용한 행동학적 생체기반 인증 연구도 이뤄지고 있다. 예를 들어, Li와 Sato [7]는 스마트 워치를 착용한 사용자가 공중에 서명하는 과정에서 수집된 손 움직임과 각도 데이터를 토대로 인증하는 방식을 제안했다. 또한, 사용자가 박수를 치는 과정에서 수집된 근전도 및 팔 움직임 데이터를 토대로 사용자를 인증하는 방식 [8]도 개발됐다. 이 밖에도, 스마트폰 기반 인증에서 활용된 진동 센서를 스마트 워치에서도 이용한 도전-응답(challenge-response) 구조의 사용자 인증 방법 [9]도 개발됐다. 해당 방법은 인증 요청이 발생하면 등록 시 사용한 여러 진동 유형 중 무작위로 하나를 발생시키고, 이때 자이로스코프와 가속도계 센서를 통해 수집된 응답 데이터를 토대로 사용자를 인증한다.

지난 몇 년간 코로나19 팬데믹(COVID-19 pandemic)으로 인해 비대면 환경의 필요성이 증가함에 따라, 가상 사무실과 같은 플랫폼이 개발되었으며 이를 위한 사용자 인증 기술이 요구됐다. 이러한 요구에 발맞춰, 많은 연구자가 가상 현실을 위해 사용되는 HMD(head-mounted display) 및 스마트 글라스(smart glasses)와 같은 웨어러블 기기를 기반으로 하는 행위기반 인증 연구를 수행하고 있다. 대표적으로, Fallahi 외 [10]는 뇌파 측정기와 아이트래커(eye tracker)를 결합한 스마트 글라스 형태의 기기를 제작하고, 해당 기기를 착용한 상태에서 수집된 시선 변화 및 뇌파 데이터를 인증에 활용하는 멀티모달 인증 방식을 제안했다. 또한, Fig. 5과 같이 HMD를 착용한 사용자 간 가상 현실에서 대화를 수행하는 과정 중 수집된 시선 데이터를 기반으로 인증을 수행하는 방식 [11]도 개발됐다. 아울러, 사용자가 HMD를 착용한 상태에서 사전 정의된 경로를 따라 보행하는 과정에서 탑재된 관성 측정 장치를 통해 생성된 데이터로 사용자를 인증하는 방법 [12]도 제시됐다.

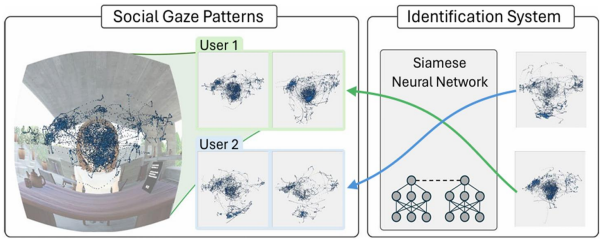

Fig. 5. User authentication method based on social gaze patterns [11]

4. Keyboard and Touch Panel

키스트로크 다이나믹스(keystroke dynamics)라고도 불리는 키보드(keyboard)를 활용한 행위기반 인증 기술은 다양한 인증 수단 중에서도 오랫동안 연구된 분야이다. 본 기술은 사용자마다 서로 다른 키보드 타이핑 패턴(typing pattern)을 보인다는 점을 토대로, Fig. 6과 같이 키 체류 시간인 dwell time 외에도 4가지 표준 타이밍 특징(standard timing features)을 활용하여 사용자를 인증하게 된다.

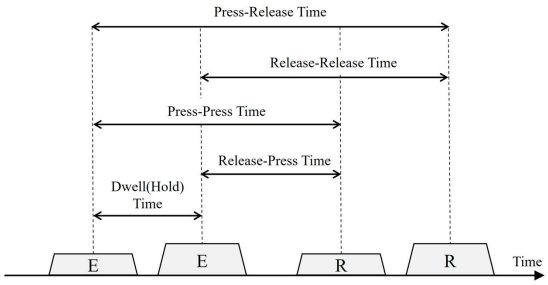

Fig. 6. Keystroke dynamics features

오랫동안 많은 연구가 사용자들이 사전 정의된 문구를 입력하는 과정에서 생성된 인증 데이터를 토대로 사용자 인증 기법을 개발해왔지만, 최근에는 자유로운 텍스트(text)를 입력하는 과정에서 인증을 수행하는 방식으로 발전되고 있다. 예를 들어, Ayotte 외 [13]는 기존 자유 텍스트 기반 인증보다 적은 키 입력 횟수를 토대로 약 2배 이상 빠르게 인증을 수행하는 방식을 제안했다. Yang 외 [14]는 다양한 기기와 키보드 레이아웃(layout)을 사용하는 이질적인 환경에서도 공통된 키스트로크 다이나믹스 특징을 토대로 사용자를 일관되게 인증하는 자유 텍스트

기반 인증 방법을 개발했다. 이 밖에도, 사전 정의된 비밀번호 텍스트를 입력하는 과정에서 수집된 키스트로크 다이나믹스와 뇌파 데이터를 결합한 멀티모달 데이터를 토대로 사용자를 인증하는 방식 [15]도 연구됐다.

한편, 특수 제작된 터치 패널(touch panel) 기반 연구도 수행되고 있다. 대표적으로, Tang 외 [16]는 폴리비닐리덴 플루오라이드(Polyvinylidene Fluoride, PVDF) 소재로 제작된 압전 터치 패널을 통해 7자리 비밀번호 입력하는 과정에서 dwell time, release-press time 외에도 터치 압력을 토대로 사용자를 식별하는 방법을 제시했다. 또한, Jia 외 [17]는 Fig. 7과 같이 감정 상태를 반영하는 인증 방식을 개발했다. 구체적으로 해당 방식은 사용자가 행복, 공포, 슬픔, 혐오를 유발하는 영상을 각각 시청한 뒤 PVDF 기반 터치 패널에 6자리 비밀번호를 입력하는 과정에서 수집된 키스트로크 다이나믹스 특징과 압력 데이터를 인증에 활용한다.

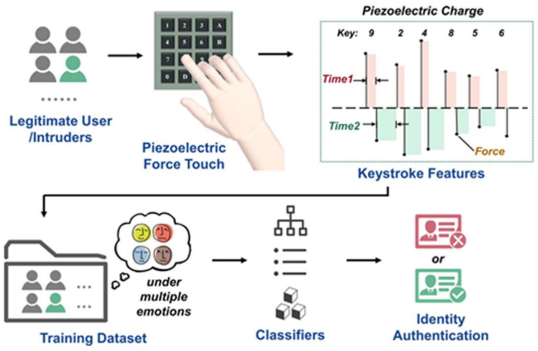

Fig. 7. User authentication method using keystroke dynamics based on emotional responses [17]

5. Camera

카메라(Camera)는 안면 인증 기반 출입 통제와 같은 물리적 보안을 보장하기 위해 주로 사용되는 인증 기기로, 사용자의 행동 이미지를 전체적 또는 부분적으로 획득할 수 있어 행위기반 인증 기술 연구에서 널리 활용되고 있다. 특히, 이러한 연구들은 주로 사용자의 보행, 자세 변화, 손 제스처(gesture)와 같은 행동을 중심으로 인증 기법을 제안하고 있다. 대표적으로, Zhang 외 [18]는 노인과 같은 사회적 취약 계층의 사용자가 돌봄 로봇과 상호작용하기에 앞서, 추가적인 기기 착용이나 인지 능력에 대한 의존 없이 손쉽게 인증되는 방법을 제안했다. 구체적으로, 해당 방법은 눈, 코, 어깨, 팔꿈치와 같은 17개의 신체 관절과 얼굴 위치 데이터를 사용자가 걸어오는 과정에 수집하여 사용자를 인증하게 된다. 이와 유사하게, Cariello 외 [19]는 스마트폰과 상호작용하는 과정에서 3D 모션 캡처(motion capture) 카메라를 통해 수집된 신체 자세 및 움직임 데이터를 기반으로 하는 사용자 인증 방식을 개발했다. 해당 방식은 사용자가 앉거나 걸으면서 스마트폰과 상호작용하는 과정에서 수집된 3D 모션 데이터와 기존 스마트폰 기반 인증 연구에서 널리 활용된 자이로스코프 및 가속도계 데이터를 함께 활용함으로써, 인증 지연 시간을 3~5초 이내로 감소시켰다.

한편, Song 외 [20]는 무작위 손 제스처를 기반으로 한 인증 방법을 제안했다. Fig. 8은 해당 방법의 개요를 나타내며, 기존 연구들과 달리 사용자가 시스템 등록 단계와 인증 단계에서 서로 다른 손 제스처를 사용하더라도 인증이 가능하도록 설계되어 인증용 제스처를 기억할 필요가 없다는 장점이 있으며 모방 공격에 저항성을 가지고 있다.

앞서 살펴본 연구들과 달리, Koch 및 Grbic [21]는 사용자가 말하는 과정에서 수집된 생리학적 데이터와 행동학적 데이터를 함께 활용하는 입술 기반 인증 방식을 개발했다. 해당 방식은 사용자가 특정 인증 문구를 발화할 때 수집된 입술 모양과 음성 스타일(즉, 말투) 외에도 음성 내용을 수집하여 같이 인증 데이터로 활용함으로써 비디오 재생 공격에 저항성을 가진다.

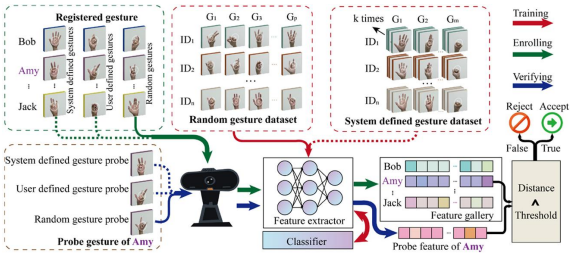

Fig. 8. Hand gesture authentication method using a camera [20]

6. Earphone

이어폰(earphone)은 스마트폰 또는 웨어러블 기기와 연동되어 널리 사용되고 있을 뿐만 아니라 IoT 센서의 발달로 고주파 기반 생리학적 특성을 수집할 수 있음에 따라 생체기반 사용자 인증 수단으로 사용되고 있다. 그러나, 이어폰 기반 생리학적 요소는 청각적 자극으로 인한 사용자 경험 저하, 청력 민감도 차이 등과 같은 한계점을 가지고 있어 행동학적 특성을 함께 활용하는 연구가 수행되고 있다. 예를 들어, Han 외 [22]는 사용자가 호흡하는 과정에서 발생된 호흡음을 토대로 사용자를 인증하는 방식을 개발했다. 특히, Fig. 9에서 보듯이 귓속 호흡음에 포함된 신체 비대칭 특성, 외이도의 기하학적 특성, 호흡기 공명 특성을 고려하여 사용자 인증이 이뤄지게 된다.

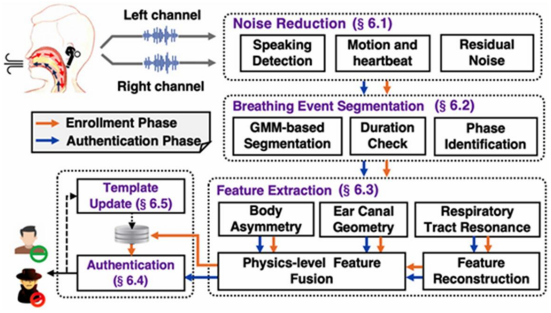

Fig. 9. In-ear breathing-based authentication [22]

Zuo 외 [23]는 이어폰에 내장된 마이크 센서를 통해 수집된 음향 신호를 기반으로 사용자를 인증하는 방법을 제안했다. 제안 방법은 달리기, 걷기, 키보드 입력 등 다양한 움직임 상황에서 이어폰 착용 또는 조정 시 발생하는 마찰로 인한 음향 신호와 신체 기관(예: 심장, 폐)에서 발생하는 생체 음향을 결합하여 사용자를 자연스럽게 인증한다.

III. Further Direction

앞서 행위기반 인증 연구의 동향을 인증 수단을 중심으로 분류하고, 활용된 인증 요소를 토대로 주요 연구를 분석했다. 본 장에서는 분석된 연구를 토대로 향후 행위기반 인증 연구 분야가 나아가야 할 방향을 제시하고자 한다.

1. Development of a Verification Dataset

대부분 연구에서 50명 수준의 참가자를 대상으로 제안한 인증 기술의 유효성을 검증하고 있다. 그러나 사용자 인증 기술은 수백 명의 대규모 환경에서도 신뢰성과 안정성을 유지해야 하므로 더욱 많은 사용자를 대상으로 한 추가 검증이 요구된다. 다만, 인증 방법 제안과 동시에 이를 검증하기 위해 많은 참가자 모집하는 것은 현실적인 한계가 존재하므로, 대규모 공개 데이터세트(dataset)를 구축하는 연구가 별도로 수행될 필요가 있다. 특히, 키스트로크 역학을 제외하고 대부분 연구가 개별적으로 데이터세트를 구축하고 있어 모집군도 다르고 실험 조건도 같지 않아 객관적인 벤치마크 기반 비교평가가 한계가 존재하므로 이러한 연구는 더욱 필요한 상황이다.

대규모 데이터세트 구축 연구는 다양한 연구에서 활용될 수 있도록 범용성을 고려하여 설계될 필요가 있으며, 이를 위해 다음과 같은 설계 전략을 고려해야 한다. 먼저, 인증 수단을 중심으로 최신 연구들을 분석하여 빈번하게 사용되는 행동학적 특성과 센서 종류를 도출하고, 이를 기반으로 행위 프로세스를 구체화할 필요가 있다. 예를 들어, 스마트폰을 이용한 최근 연구들은 대부분 터치 기반 행위(예: 스와이핑, 탭 등)에 중점을 두고 있으므로, 스마트폰 기반 데이터세트를 구축할 때는 이러한 행동을 체계적으로 분류하여 최대한 포함되도록 설계해야 한다.

또한, 실제 상용 시스템은 대규모 환경에서 다양한 사용자를 포함하므로, 이를 반영하여 실험 설계 시 최소 100명 이상의 참가자를 모집하고 성별 및 연령대를 균형 있게 포괄하도록 하는 것이 바람직하다. 특히 다양한 연령대를 포함하는 것은 연령별 인증 기기의 활용 숙련도가 다르므로 범용성을 갖는 인증 기술의 성능을 검증하는 데 중요하다. 마지막으로, 구축된 데이터세트를 사용한 연구 간 성능 비교가 가능하도록 표준화된 평가 프로토콜을 함께 제공할 필요가 있다. 구축된 학습 데이터 규모와 평가 데이터 규모를 명확히 제시하고 FAR(false acceptance rate), FRR(false rejection rate), EER(equal error rate)와 같은 대표적인 성능 지표를 포함한 평가 절차를 명확히 정의함으로써 다양한 연구에서 동일한 기준으로 성능을 검증할 수 있도록 해야 한다. 이와 더불어, 생체 인증 분야에서 중요한 요소인 모방 공격과 같은 공격 모델에 대한 시나리오를 정의하고, 이를 데이터 구축 과정에 반영할 필요가 있다. 앞서 언급한 행위 프로세스처럼 공격 모델도 기존 연구에서 자주 수행된 다양한 공격 시나리오를 분석한 후 이를 기반으로 평가 데이터 세트를 추가 구축하면 더욱 양질의 데이터 세트 구축이 가능할 것이다.

여러 행위기반 인증 분야 중에서도 오랫동안 연구된 키스트로크 다이나믹스 분야에서 이러한 대규모 데이터세트 구축 연구 [24] 가 활발히 이뤄지고 있다. 그러나 해당 분야를 제외하곤 데이터세트 구축에 대한 연구가 부족한 상황이며, 기존 연구들 분석하여 토대로 다양한 행위를 포함하는 데이터세트 구축 연구는 더욱 부족하다. 이에, 제안하는 전략을 고려하여 향후 대규모 공개 데이터세트 구축 연구가 활발히 수행된다면 행위기반 인증 기술의 발전을 가져올 것으로 기대한다. 특히 여러 연구자들이 이러한 데이터세트를 기반으로 제안된 인증 기술을 검증할 경우, 인증 기술 간 비교평가가 가능해져 성능 경쟁이 촉진됨에 따라 해당 분야의 발전이 더욱 가속화될 것으로 예상한다.

2. Consideration of User Acceptability in Behavioral Biometrics

앞서 살펴본 바와 같이, 다양한 행동학적 특성을 기반으로 하는 행위기반 인증 기술이 활발히 연구되고 있다. 그러나 인증에 활용되는 행동학적 특성에 대한 사용자 수용도를 분석한 연구는 매우 부족한 상황이다. 더욱이 제안

방법을 검증하기 위해 참가자를 모집한 후, 데이터 수집하기에 앞서 인증 데이터에 대한 사용자 수용도를 사전에 분석한 연구는 거의 제한적이다. 그러나 지식기반 또는 소유기반 인증 방식과 같은 기존 방식과 달리, 생체기반 인증 방식은 민감한 생체 데이터의 수집 및 저장으로 인해 사용자 거부감을 유발할 수 있다. 특히, 제로 트러스트 보안 모델의 핵심 요구사항인 지속 인증을 달성하기 위해 생체 데이터가 지속적이고 암묵적으로 수집됨에 따라 거부감은 더욱 두드러질 수 있다. 이러한 거부감은 향후 실산업 환경에서 행위기반 인증 기술의 확산을 저해하는 요인이 되어, 관련 연구 분야의 발전을 제한할 가능성이 있다.

따라서, 기존 연구에서 활용된 행동학적 특성에 대해 사용자가 느끼는 거부감을 체계적으로 분석할 필요가 있으며, 향후 수행될 인증 연구들도 수용도 정도를 측정하는 과정을 평가지표로써 제시하여 우수성을 입증해야 한다. 이를 위해, 연구자는 몇 가지 대표적인 연구의 인증 절차를 참가자에게 수행하도록 한 후, 리커트 척도(likert scale)와 같은 심리 검사 기법을 활용하여 체계적으로 분석하는 실험 설계가 요구된다. 특히, 심리 검사 기법을 위한 평가 항목으로 인지적 부담, 편의성, 개인정보 유출 우려 등을 설정하여 사용자 거부감 수준을 다각적으로 분석할 필요가 있으며, 참가자의 성별 및 연령대를 균형 있게 포괄하도록 모집하여 사용자 집단 간 인증 기술에 대한 수용도 차이를 자세히 분석함으로써 실산업에서도 충분히 사용할 수 있다는 점을 입증해야 한다. 또한, SUS(system usability scale)과 같이 다양한 상황에서 제안하는 인증 방법의 사용성을 전반적으로 평가할 수 있는 테스트 방법도 함께 활용하여 이러한 입증이 견고히 할 필요가 있다. 일부 연구 [25]에서 잘 알려진 생체기반 인증 요소를 중심으로 사용자 거부감 분석을 진행하였으나, 향후 행동학적 특성에 중점을 둔 연구가 수행된다면 행위기반 인증 연구 발전을 위한 중요한 토대를 마련할 것으로 기대된다.

IV. Conclusion

최근 ICT 기반 서비스의 활용과 함께, 다양한 IoT 기기를 활용한 AI 기반 사용자 인증 연구가 진행되고 있다. 특히 고품질의 생체 데이터를 처리할 수 있게 됨에 따라, 다양한 인증 기술 중에서도 생체기반 인증 연구가 활발히 이뤄지고 있다. 이에, 본 논문에서는 생체기반 인증의 하위 분야인 행위기반 인증 연구를 인증 기기를 중심으로 분류하여 최근 연구 동향을 제시함으로써 해당 분야에 대한 기초적 이해를 제공했다. 특히, 행위기반 인증 연구의 분류 체계를 제시함으로써 해당 분야를 체계적으로 정리했다. 게다가, 기존 연구의 한계점인 제한된 데이터 세트 규모와 인증 요소에 대한 사용자 수용성 미고려 문제를 해결하기 위한 구체적인 방법을 향후 연구 방향으로 제시함으로써 해당 분야의 발전에 기여할 수 있을 것으로 기대된다.

한편, 개발된 행위기반 인증 기술이 상용 시스템에 적용되기 위해선 다양한 공격 시나리오에 대한 보안성 검증은 매우 중요한 요소이다. 따라서 향후 연구에서는 본 연구를 확장하여 행위기반 인증 기술에서 수행된 위협모델 기반 보안 분석 방법을 체계적으로 조사하여 주요 위협모델을 식별하고, 이를 바탕으로 주요 행위기반 인증 분야별 표준화된 보안 분석 방안을 제안하고자 한다.

REFERENCES

[1] J.B. Lee and I.C. Euom, “A Study on Data Acquisition of IoT Devices Intrusion,” Journal of the Korea Institute of Information Security & Cryptology, Vol. 33, Issue 3, pp. 537-547, June 2023. DOI: 10.13089/JKIISC.2023.33.3.537

[2] Y. Xie, F. Li, and Y. Wang, “FingerSlid: Towards finger-sliding continuous authentication on smart devices via vibration,” IEEE Trans. Mob. Comput., Vol. 23, Issue 5, pp. 6045-6059, May 2023. DOI: 10.1109/TMC.2023.3315291

[3] Y. Chen et al., “TBAuth: A continuous authentication framework based on tap behavior for smartphones,” Expert Syst. App, Vol. 264, No. 125811, pp. 1-14 March 2025. DOI: 10.1109/JIOT.2022.3199657

[4] M. Yao et al., “PresSafe: Barometer-based on-screen pressure-assisted implicit authentication for smartphones,” IEEE Internet of Things J., Vol. 10, Issue 1, pp. 285-302, January 2023. DOI: 10.1109/JIOT.2022.3199657

[5] C. Wu et al., “It’s all in the touch: Authenticating users with HOST gestures on multi-touch screen devices,” IEEE Trans. Mob. Comput., Vol. 23, Issue 10, pp. 10016-10030, October 2024. DOI: 10.1109/TMC.2024.3371014

[6] A. Buriro, B. Crispo, and M. Conti, “AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones,” J. Inf. Secur. Appl., Vol. 44, pp. 89-103, February 2019. DOI: 10.1016/j.jisa.2018.11.008

[7] G. Li and H. Sato, “Sensing in-air signature motions using smartwatch: A high-precision approach of behavioral authentication,” IEEE Access, Vol. 10, pp. 57865-57879, May 2022. DOI: 10.1109/ACCESS.2022.3177905

[8] A. Buriro et al., “Wearable wisdom: A bi-modal behavioral biometric scheme for smartwatch user authentication,” IEEE

Access, Vol. 12, pp. 61221-61234, April 2024. DOI: 10.1109/ACCESS.2024.3395128

[9] S. Lee, W. Choi, and D. H. Lee, "The vibration knows who you are! A further analysis on usable authentication for smartwatch users," Computers & Security, Vol. 125, No. 103040, pp. 1-15, February 2023. DOI: 10.1016/j.cose.2022.103040

[10] M. Fallahi, P. Arias-Cabarcos, and T. Strufe, "Beyond gaze points: augmenting eye movement with brainwave data for multimodal user authentication in extended reality," Complex Intell. Syst., Vol. 12, No. 39, pp. 1-19, December 2025. DOI: 10.1007/s40747-025-02157-4

[11] M. Rubo and G. Son, "Social gaze fingerprints: identifying social virtual reality users by their eye gaze patterns," Virtual Reality, Vol. 29, No. 144, pp. 1-14, September 2025. DOI: 10.1007/s10055-025-01210-4

[12] Y. Shen et al., "GaitLock: Protect virtual and augmented reality headsets using gait," IEEE Trans. Dependable Secure Comput, Vol. 16, Issue 3, pp. 484-497, June 2019. DOI: 10.1109/TDSC.2018.2800048

[13] B. Ayotte et al., "Fast free-text authentication via instance-based keystroke dynamics," IEEE Trans. Biom. Behav., Vol. 2, Issue 4, pp. 377-387, October 2020. DOI: 10.1109/TBIOM.2020.3003988

[14] Y. Yang et al., "Cross-device free-text keystroke dynamics authentication using federated learning," Pers. Ubiquitous Comput., Vol. 28, pp. 491-505, September 2024. DOI: 10.1007/s00779-024-01832-6

[15] A. Rahman et al., "Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms," IEEE Access, Vol. 9, pp. 94625-94643, June 2021. DOI: 10.1109/ACCESS.2021.3092840

[16] C. Tang et al., "Piezoelectric and machine learning based keystroke dynamics for highly secure user authentication," IEEE Sens. J., Vol. 23, Issue 20, pp. 24070-24077, October 2023. DOI: 10.1109/JSEN.2022.3141872

[17] W. Jia et al., "High security user authentication based on piezoelectric keystroke dynamics applying to multiple emotional responses," IEEE Sens. J., Vol. 22, Issue 3, pp. 2814-2822, February 2022. DOI: 10.1109/JSEN.2021.3136902

[18] R. Zhang et al., "Non-intrusive continuous user verification by care robots: MoveNet gait data," Intelligent Sports and Health, Vol. 1, Issue 3, pp. 160-178, July 2025. DOI: 10.1016/j.ish.2025.06.003

[19] N. Cariello et al., "Posture and body movement effects on behavioral biometrics for continuous smartphone authentication," IEEE Trans. Biom. Behav., Vol. 7, Issue 1, pp. 3-15, January 2025. DOI: 10.1109/TBIOM.2024.3409349

[20] W. Song et al., "Video understanding-based random hand gesture authentication," IEEE Trans. Biom. Behav., Vol. 4, Issue 4, pp. 453-470, October 2022. DOI: 10.1109/TBIOM.2022.3179279

[21] B. Koch and R. Grbić, "One-shot lip-based biometric authentication: Extending behavioral features with authentication phrase information," Image Vis. Comput., Vol. 142, No. 104900, pp. 1-12, February 2024. DOI: 10.1016/j.imavis.2024.104900

[22] F. Han, P. Yang, and Y. Feng, "Exploring earable-based passive user authentication via interpretable in-ear breathing biometrics," IEEE Trans. Mob. Comput., Vol. 23, Issue 12, pp. 15238- 15255, December 2024. DOI: 10.1109/TMC.2024.3453412

[23] Y. Zou et al., "EarPrint: Earphone-based implicit user authentication with behavioral and physiological acoustics," IEEE Internet of Things J., Vol. 11, Issue 19, pp. 31128-31143, October 2024. DOI: 10.1109/JIOT.2024.3417622

[24] I. Tsimperidis et al., "IKDD: A keystroke dynamics dataset for user classification," Information, Vol. 15 Issue 9, No. 50, pp. 1-12, August 2024. DOI: 10.3390/info15090511

[25] R. Alrawili, A.A.S. AlQahtani, and M.K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion" Comput. Electr. Eng., Vol. 119, No. 109485, pp. 1-25, October 2024. DOI: 10.1016/j.compeleceng.2024.109485

Authors

Giluk Kang received the B.E. degree in computer engineering from the Korea National University of Welfare, Pyeongtaek, South Korea, in 2020. He received the Ph.D. degree in computer and information security from Sejong University, Seoul, South Korea, in 2025. His research interests include the Internet of things security, access control, authentication, interoperability on security, the Metaverse, and blockchain.