바이오 인증 기술의 활성화에 따른 보안 위험성에 관한 연구

전정훈*

요 약

최근 국내·외 핀테크 관련 산업분야에 대한 많은 관심과 함께 다양한 서비스들이 새로이 등장하고 있으며, 해킹 공격으로부터의 안전을 보장하기 위해, 새롭고 다양한 기술들이 개발되고 있다. 대표적인 기술로는 금융관련 분야에 적용을 고려하고 있는 바이오 인증이 있다. 바이오 인증은 생체의 일부 정보를 인증수단으로 하고 있어, 위· 변조공격으로부터 안전하고 공유 및 저장에 대한 위협들에 대응할 수 있다고 알려져 있다. 그러나 최근 미국 인사관리처(Office of Personnel Management, OPM)의 생체정보(560만 건) 유출사례와 지문위조기술의 등장을 살펴볼 때, 바이오 인증의 안전성을 재고해보아야 하는 상황임을 알 수 있다. 특히, 이미 유출된 생체정보의 도용문제에 대해서 대응방안이 함께 마련되어야 할 것이다. 따라서 본 논문은 여러 산업분야에서의 생체인증기술들과 적용 사례, 취약요인들을 조사해 봄으로써, 향후, 생체인증기술 적용에 따른 침해대응 방안 마련에 활용될 것으로 기대한다.

A Study on Security Risk according to the activation of Bio-Authentication Technology

Jeon Jeong Hoon*

ABSTRACT

In recent years, there is growing interest in 'Fin-tech' in the domestic and international financial sector. And a variety of services in such a situation has emerged. To ensure the safety of from hacking attacks, many new technologies have been developed. These leading technology is the Bio-authentication method that you consider applying to the financial sector. Bio authentication is using biometric information. Also it is known that can cope the threat of fabrication and modifying attacks with shared and stored. However, Recently, When you look at hacking incidents of biometric data(560 million cases) in the United States Office of Personnel Management and advent of the fingerprints counterfeit technology, We can be known that should be reconsidered about the safety of bio-certification. Especially, it should be provided with a response measures for the problem of embezzlement that biometric information already been leaked. Thereby In this paper, by investigating biometric technologies and practices applied and of the vulnerability factor in many industries, it expected to be utilized in the prepared threats countermeasures in accordance with the application of the biometric authentication technology in a future.

Key words : Bio-Authentication, Authentication Technology, Fin-tech, FIDO(Fast IDentity Online), Smart Phone

접수일(2016년 8월 22일), 수정일(1차: 2016년 9월 21일), 게재확정일(2016년 9월 29일)

★ 본 논문은 2015년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교/컴퓨터학과

1. 서 론

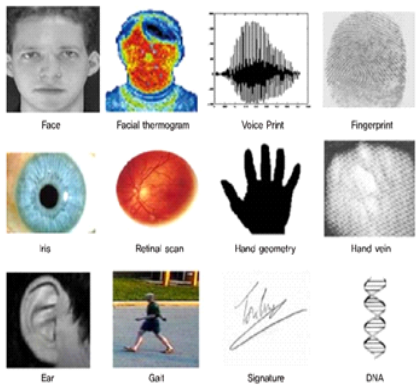
최근 '바이오(bio) 인증'은 '생체인식' 또는 '바이오메트릭스(bio metrics)'라는 명칭으로 여러 산업분야에서 많은 관심이 집중되고 있다. 이러한 배경에는 보안 공격으로부터 보다 안전하고, 편리하며, 신속한 서비스를 제공해주는 새로운 인증기술들이 지속적으로 요구되어 왔기 때문이다. 그러나 최근 FIDO(Fast IDentity Online)는 바이오 인증을 프로토콜(protocol)과 수단으로 분리해 패스워드(password) 없는 방법으로 강도를 높이는 동시에 사용자의 편의성을 향상시키는 방안을 제안함으로써, 국내·외 금융 분야와 스마트 모바일서비스 분야에서 긍정적인 반응을 보이고 있다[1]. 기존 주민번호나 아이디(id), 패스워드, OTP(one time password)를 입력하는 방식은 사용자가 암기 또는 생성기를 휴대해야하고, 인증절차에 적지 않은 시간이 소요되는 단점이 있다. 또한 여러 보안 문제들이 있었으나, 바이오 인증을 통해 해결해 나갈 수 있게 되었다. 이러한 바이오 인증은 사용자들에게 편의성과 신속성을 제공해준다는 장점 때문에 여러 산업분야에서의 활용이 기대된다. 그러나 생체정보의 유출사고 사례들을 살펴볼 때, 예방만이 아니라, 이미 유출된 생체정보의 도용문제에 대한 대응방안도 함께 마련되어야 할 것이다[2].

따라서 본 논문은 바이오 인증의 위험요인들을 조사해 봄으로써, 향후 다양한 산업으로의 적용 및 대응기술 개발, 취약성 분석, 기술보완을 위한 연구 자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 바이오 인증기술의 종류와 특징, 표준화, 활성화 동향에 대해 알아보고, 3장은 바이오 인증의 위협요인들을 알아본다. 그리고 4장은 바이오 인증의 취약요인에 따른 대응방안과 마지막 5장에서 결론 부분으로 이글을 마치도록 한다.

2. 관련연구

2.1 바이오 인증 종류 및 특징

바이오 인증은 신체적인 특징과 행동적 특징으로 나누어 볼 수 있는데 이들의 종류를 알아본다[3].



(그림 1) 생체인식의 신체적 방법[4]

신체적 인식방법에는 그림1과 같이 얼굴모양(face)과 열상(thermal image)을 이용한 얼굴인식과 홍채(iris)를 이용한 홍채인식, 정맥(vein)을 이용한 정맥인식, 지문(fingerprint)을 이용한 지문인식이 있으며, 안구의 망막(retina)을 이용한 망막인식, 손 모양(hand geometry)과 장문(palm print) 등이 있다[4]. 그리고 행동적 인식방법에는 걸음걸이와 서명인식, 음성인식 등이 있으며, 최근에는 두 가지 인식방법을 복합 적용하는 기술도 등장하고 있다. 이러한 기술은 인식률과 생성 데이터의 크기에 따라 실용화가 결정된다. 다음은 바이오 인증에 사용되는 생체인식방법들의 특징들에 대해 알아본다.

지문인식은 가장 간편하고, 저렴하여 생성 데이터가 비교적 적으며 신뢰와 안정도에 있어 다른 인식방법 보다 높다. 그러나 손상(상처 및 화상)되거나 지워진 경우, 땀이나 물기 등 이물질로 인식률이 낮아질 우려가 있으며, 여러 사람들이 함께 사용함으로써 위생문제나 지문의 위조, 원격지에서 상대가 살아있는지 여부를 확인하기 어려운 단점들이 있다[5][6][7]. 홍채와 망막인식은 지문인식보다 훨씬 복잡하고, 비접촉 방식이기 때문에 거부감이 없다. 그리고 2초 내 신분확인이 가능하며, 정교하기 때문에 위·변조에 유리하다. 특히, 홍채인식의 경우, 1미터 떨어진 곳에서도 카메라를 이용해 포착이 가능하지만, 높은 비용부담과 사용자 이용에 있어, 다소 불편한 점 등이 단점으로 꼽히고 있다[5][7]. 얼굴인식은 작은 표정의 변화까지 감지할 수 있는 3차원 입체영상의 식별이 가능하기

때문에, 데이터베이스의 연산처리가 빨라야 하는 특징이 있다. 비접촉식으로 자연스럽게 식별이 가능하다는 장점은 있지만, 노화나 변장, 조명, 표정, 사고로 인한 얼굴모양의 변화에는 인식률이 저하되는 단점이 있어, 지문이나 홍채보다도 인식률이 비교적 낮다[5][7]. 음성인식은 물리적인 접촉 없이 자연스럽게 식별이 가능하고, 비용이 매우 저렴할 뿐만 아니라, 원격지에서도 사용이 가능한 장점이 있다. 그러나 다른 인식방법보다도 에러율이 높고, 감기 등의 질병으로 인한 음성변화로 인식률이 저하될 수 있으며, 소음 및 잡음에도 취약한 단점이 있다[5][7]. 정맥인식은 손등이나 손목의 정맥모양을 식별하는 방법으로 인식률이 높으며, 복제가 어려운 장점이 있다. 그러나 하드웨어 구성이 복잡하고, 구축비용이 높아, 활용범위가 제한되는 단점이 있지만, 최근 정맥인식의 높은 편의성과 안전성 등으로 사용이 증가하고 있다[5][7]. 이와 같은 바이오 인증기술은 생체정보의 수집방법 및 특징에 따라 여러 산업현장에 선택적 응용이 가능하고, 최근 핀테크(fin-tech)로 관심이 점차 높아지고 있어 생채인식의 적용사례는 늘어날 것으로 예상된다.

2.2 바이오 인증의 표준화

최근 FIDO(Fast IDentity Online)는 개인정보유출 사고를 최소화하고, 인증체계의 안정성과 보안성, 편의성 등을 높이기 위해 생체정보 등을 활용한 인증기술 분야의 표준화를 주도하고 있다. 2002년 미국의 주도하에 ISO/IEC JTC 1 SC37(Biometrics) 국제 표준화 기구가 설립된 이래로 FIDO의 표준은 지문, 음성, 얼굴 등과 같은 사람의 고유 생체 정보의 인식을 통한 UAF(Universal Authentication Framework)방식과 ID, 비밀번호 방식으로 인증한 후, 보안키를 저장한 동글(dongle) 등을 사용하여 2차 인증을 하는 U2F(Universal 2nd Factor)방식이 있다. 이들의 특징을 살펴보면 다음과 같다. UAF 표준은 공개키 방식을 사용하며, 사용자 디바이스의 FIDO 인증모듈에 사전 Attestation Certificate와 Attestation Private Key가 최소 100,000대 이상의 장비에 사용된다, 그리고 디바이스를 통한 사용자의 유추를 방지하기 위해 새로운 키를 사용하도록 권고하고 있다. 키의 사용은 기존 금융권에서 사용하는 공개키 방식과 차이를 갖으며, FIDO 서버에 사용자의 생체 정보가 전송되지 않도록 하고 있다. U2F 표준 또한 Public Key와 Private Key 쌍을 생성하고 서명에 활용한다는 측면에서 UAF방식과 유사하며, U2F디바이스 등록 및 인증에 자바스크립트 API와 모바일 OS API를 통해 이뤄진다. 그리고 U2F 프로토콜의 암호화 관련 내용을 정의한 상위계층과 디바이스로부터 U2F 디바이스로 USB, NFC, 블루투스 LE 등 암호 메시지 등을 전달하는 하위계층으로 나누어 표준화를 진행하고 있다[8]. 이와 같은 표준화 움직임은 글로벌 시장으로의 확대 적용을 예고하는 것으로, 이에 따른 국내 기반기술 및 제도적 장치의 마련과 관련 분야 산업육성 등 다양한 활성화가 동반되어야 할 것이다.

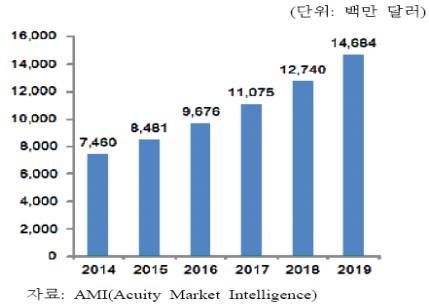
2.3 바이오 인증의 활성화 동향

<표 1> 국내 모바일 간편 결제사업자현황[9]

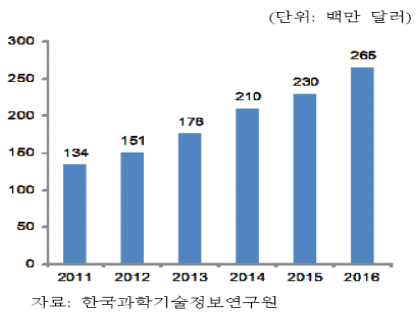
	기업	서비스
플랫폼사	다음카카오	뱅키월렛 카카오
		카카오 간편결제
	SK플래닛	시럽페이
전자결제 대행사	KG 이니시스	케이페이
	엘로페이	후불결제서비스
	페이게이트	간편결제 서비스
이동통신사	LG유플러스	페이나우
	SK텔레콤	페이먼트/BLE전자
	KT	올레앱안심인증
단말제조사	삼성전자	모바일
		삼성페이
	애플	애플페이

바이오 인증은 인증정보의 고유성과 편의성 등 장점들을 갖고 있지만, 낮은 인식율과 고가의 비용, 정확성 등의 문제점들로 인해 사용을 꺼려해 왔던 것이 사실이다. 그러나 스마트폰과 같은 사용자 단말기의 휴대성 및 이동성이 향상되고, 다양한 서비스가 제공되고 있는 가운데, 바이오 인증기술의 등장은 매우 시기 적절하다고 할 수 있다. 국내 활성화 움직임의 일환으로 한국인터넷 진흥원은 FIDO와 공인인증서 연

계 기술 개발에 관한 활용기술의 연구를 통해, 간편 결제 활성화를 진행해 왔으며[10], 표1의 현황과 같이 몇몇 모바일 간편 결제 사업자들은 이미 서비스를 제공하고 있다. 모바일 시장은 2015년 대비 해외는 약 76%(5,600억 달러)의 성장세를 보였으며, 국내는 스마트폰을 이용한 결제와 교통카드, 유통매장, 선불카드 등 서비스 확대를 기대하고 있다[9].



(그림 2) 국외 바이오인식 시장규모[11]



(그림 3) 국내 바이오인식 시장규모[11]

아울러 모바일 간편 결제에 바이오 인증 도입에 대한 2015년 우리금융경영연구소의 분석 자료를 살펴보면, 국내·외 바이오 인증시장은 연평균 10%이상의 높은 성장률을 보일 것으로 전망하고 있다. 그리고 그림 2와 같이 2014년 74.6억 달러에서 2019년 146.8억 달러로 14.5%의 성장률을 전망하고 있다. 그리고 국내 시장규모 또한 그림3과 같이 2011년 1.3억 달러에서 2016년 2.7억 달러로 14.6%의 성장이 예상된다[11]. 그러나 KB금융지주 경영연구소의 자료에 따르면, 바이오인증을 활용한 지불결제 기능이 단기적으로 대중화 및 보편화가 이뤄지기는 어려울 것으로 전망하고 있다. 이유로는 220만개 이상이 되는 신용카드 가맹점의 단말기 교체에 따르는 비용과 신용카드사와 VAN사 등의 이해관계자의 추가적인 투자가 필요하며, 고객의 생체 정보를 금융사에 등록해야하는 점 때문에 심리적 거부감과 정보유출에 대한 불안감이 걸림돌이 될 것으로 보고 있다[12].

2.4 개인정보의 침해 동향

신기술들의 등장과 발전을 거듭하면서, 공격기술 또한 함께 진화해 최근 스마트 폰에 대한 공격시도가 증가하고 있다. 이러한 공격들은 표3과 같다[13].

<표 2> 스마트폰 해킹공격 유형[13]

유형	내용
도난/분실	-개인정보유출
악성코드	-과금 유발 : 불특정 다수에 SMS전송 -정보 유출 : 사용자 개인정보외부유출 -장애 유발 : 통화 -배터리 소모
무선랜	-가짜 무선 AP 및 무선 랜 자동접속
스파이앱	-스텔스 모드, 원격전송 -자녀, 직원, 배우자 감시 -통화내역, SMS, 위치정보, 이메일, 접속URL, 사진 유출
스미싱	-앱 설치 권유 메시지 -URL이 포함된 메시지로 유포

표2를 통해 사용자 단말기를 공격목표로 하는 경향이 점차 높아지고 있으며, 이러한 가운데 국·내외 금융 관련 분야의 바이오 인증기술 적용은 새로운 공격기술의 등장을 예고하고 있음을 알 수 있다.

3. 바이오 인증의 위협요인

3.1 고유성

생체정보는 기존의 인증 정보의 형태와 달리 고유성이 매우 뛰어나다[14]. 이에 대해 [15]는 생체정보의 특성을 고유성과 측정 가능성, 생리적 특성 및 운동적 특성, 자동성, 식별 및 인증으로 정의하고 있으며, [16]

은 영구불변성, 복제가능성의 최소, 도용 위협의 양면성, 비 기억, 비휴대성, 인격권의 직접적인 반영으로 보고하고 있다. 이와 같은 학자들의 견해들을 종합해 보면, 생체정보의 고유성과 영구불변성에 초점을 맞추고 있음을 알 수 있다. 이에 FIDO는 생체정보의 고유성 유지를 위해 사용자 유추 방지와 서버로의 전송 및 저장을 하지 않도록 하였다. 사례로는 Kroger나 West Seattle, Thriftway, Piggly Wiggly 등과 같은 미국의 소매 유통점들은 생체정보를 자사 체인망 내에서만 활용 가능하도록 하고 있다[12]. 그러나 [15]는 생체정보의 고유성을 자물쇠인 동시에 언제든지 침해당할 수 있는 열쇠와도 같은 잠재적 위험성에 대해 언급함으로써 생체정보의 고유성이 오히려 위협요인이 되고 있음을 알 수 있다.

3.2 보편성

최근 핀테크와 바이오 인증에 대한 관심이 높아지고 있는 가운데, 모바일 간편 결제에 바이오 인증의 적용이 시도되고 있다. [17]에 따르면, 국내 여러 사업자들은 락인(lock-in)효과를 보기위해 간편 결제 서비스인 'OO 페이'를 앞 다투어 내놓고 있으며(쿠팡의 로켓페이와 11번가의 시럽페이, 네이버의 네이버 페이, NHN의 페이코), 몇몇 사업자들은 지문 및 홍채인식 기능을 이미 사용 중에 있다. 또한 대부분의 간편 결제 서비스는 스마트폰을 이용하고 있어, 생체인증의 보편화가 급속히 진행될 것으로 예상하고 있다. 그러나 표2와 같이 스마트폰에 대한 공격이 지속될 것으로 예상되고 있는 가운데[13], 생체정보의 보편적 사용은 안정성을 위협하는 요인으로 작용하고 있음을 알 수 있다.

3.3 호환성

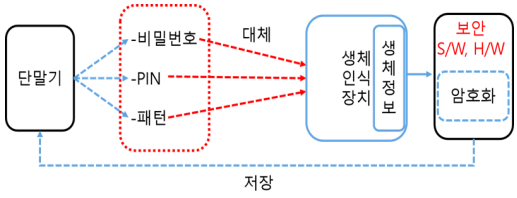
바이오 인증의 특징들을 살펴 볼 때, 글로벌 금융분야 적용은 그림3과 4와 같이 긍정적인 전망이 기된다. 일본의 경우, 해외 관광객을 겨냥한 지문결제 시장을 두고 인프라 구축에 나섰으며, 2020년 올림픽을 겨냥한 지문결제 서비스의 전국 실용화와 해외에서도 이용할 수 있도록 추진하고 있다[18]. 이와 같은 계획에는 생체정보의 호환성 보장이 전제되어야 하는데, 이미 유출된 생체정보[19]나 유출될 경우를 고려해 볼 때, 글로벌한 금융사고로 이어질 수 있어, 매우 치명적인 위협요인이 되고 있음을 알 수 있다.

3.4 범죄 이용 가능성

생체정보는 사람의 신체로부터 얻어지는 정보들로 고유성 및 편의성 등의 장점들을 포함하고 있으나 범죄에 악용될 경우, 상대가 생존하고 있는지 여부를 확인할 수 없는 단점도 포함하고 있다[6]. 이러한 사례로 2015년 미국의 안전관리처(Office of Personnel Management, OPM)는 약 560만 명의 지문인식 정보가 유출되었고[19], 정밀 카메라로 손가락을 촬영해서 인쇄한 종이만으로도 장금 장치가 풀리거나[20], 지문을 본떠 인증을 통과하는 사고사례[20]들이 나타나고 있다. 이러한 상황들을 고려해볼 때, 생체정보를 이용한 범죄는 향후 점차 증가할 것으로 예상되며, 이미 유출되었거나 유출 가능성이 높은 생체정보는 향후 매우 위협적인 요인이 되고 있음을 알 수 있다.

4. 취약요인에 따른 대응

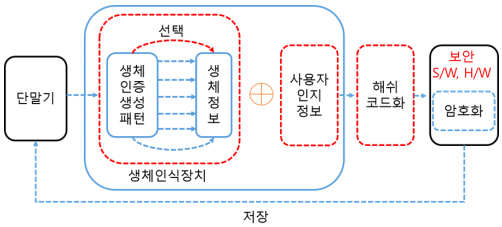
4.1 생체정보 생성의 취약요인에 따른 대응



(그림 4) 생체정보 생성과정

스마트 기기 상의 바이오 인증은 사용자가 일회성 비밀번호나 PIN(personal identification number) 식별번호, 패턴, 인증번호 등을 직접 입력해야하는 번거로움을 개선하거나 신분확인을 위해 생체정보가 이용되고 있다[21][22]. 여기서 그림4의 생체정보 생성과정은 동일 기종의 다른 기기를 사용하여도, 동일한 생체정보를 생성하며, 사용자의 단말기에 암호화된 형태로 보안 소프트웨어에 의해 보호받게 된다. 그러나 보안 소프트웨어에 대한 취약점들로 인해 보안성 보장이 어려운 상태에서 이미 유출된 생체정보의 도용에 대응이

불가하다. 따라서 그림5와 같이 사용자가 여러 생성패턴(생체로부터 정보수집방법 및 생성 알고리즘)을 두고, 사용자가 직접 선택해 사용자만이 인지하고 있는 정보를 생체정보에 추가 삽입하는 방법을 제안한다.



(그림 5) 제안하는 생체정보 생성과정

이와 같은 방법은 유출 시, 생체정보의 재생성으로 호환성과 보편성에 따른 대응이 가능하고, 이미 유출된 생체정보에 대한 범죄이용가능성을 낮출 수 있다. 또한 고유성 유지와 사업자별 운용, 상호 호환이 가능하게 된다.

4.2 생체정보 저장의 취약요인에 따른 대응

간편 결제서비스는 생체정보의 저장여부에 따라 저장형과 비저장형으로 구분되며, 생체정보의 보호방법에 따라 보안 소프트웨어방식과 하드웨어 방식으로 나누어 볼 수 있다[21]. 한편 FIDO는 생체정보를 서비스 사업자가 소유한 서버에 저장하지 않고, 개인이 소유한 스마트 기기에 안전하게 저장하고 관리하도록 권고하고 있어, 향후 비저장형으로 진화할 것으로 예상된다[21]. 그러나 사업자들은 생체정보를 암호화하여 보안 소프트웨어로 보호하도록 하고 있다[8][9]. 대표적으로 삼성의 KNOX는 암호화된 생체정보를 보호하는 보안 소프트웨어 방식으로 보안성에 대해 높은 신뢰를 받지 못하고 있는 상황에서 그림4와 같이 암호화된 생체정보의 저장보다는 그림5와 같이 해쉬 코드(hash code)로 대체함으로써 위협요인이 되고 있는 고유성과 호환성, 범죄 이용 가능성 문제를 해결할 수 있다.

4.3 스마트 기기의 취약요인에 따른 대응

스마트 기기는 앱(app) 설치나 이미지 및 파일을 다운로드 할 경우, 사용자가 공유 항목에 동의하는 순간, 악성 프로그램의 설치 및 동작이 매우 간단해 공격자의 접근이 용이하다[23]. 따라서 스마트 기기에 저장된 생체정보는 유출을 전제로 대응방안이 마련되어야 한다. 따라서 4.1절의 사용자 생성패턴 선택방법과 사용자 정보 추가 삽입 방법을 적용할 경우, 생체정보가 유출되어도 재사용이 불가할 뿐만 아니라, 이미 유출된 생체정보를 도용할 경우에도 대응이 가능하다.

5. 결 론

최근 보안 인증의 취약점들로 인해 바이오 인증에 대한 높은 관심과 함께 금융기관을 비롯한 다양한 분야에 적용을 고려하고 있다. 여러 국가들은 신속성 및 편의성, 정확성 등의 장점들로 인해 금융기관의 검토와 표준화 작업을 진행하고 있지만, 고유정보에 대한 해킹공격이 지속되고 있는 가운데, 이에 대한 대응은 이미 유출된 생체정보 보다는 현 유출을 방지하는데 초점이 맞추어져 있다. 그러므로 유출된 생체정보에 대한 대응방안도 함께 마련되어야 할 것이며, 바이오 인증의 취약성 및 위협요인의 명확한 분석과 이에 따른 대응방안이 함께 마련되어야 할 것이다. 따라서 본 논문은 바이오 인증의 동향과 사고사례를 알아보고, 예상되는 공격유형들과 위험요인에 따른 분석을 통해, 대응방안 마련 및 보안기술의 개발 등에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 바이오 인증의 적용분야에 따른 현 문제점들과 2세대 비저장방식으로의 진화에 따른 취약점 및 위협에 대한 구체적이고 지속적인 연구를 통해, 폭넓은 산업분야에 적용할 수 있는 보안 기술개발이 이뤄져야 할 것이다.

참고문헌

[1] 조상래 외 3인, “패스워드 없는 인증기술-FIDO,” 한국전자통신연구원, 2014.8

[2] 시큐이, “최신 금융회사 해킹 사례 및 보안 동향,” SECUI

[3] 박범근, “생체인식 기술 및 시장동향,” S&T Martket Report, vol.39, 연구성과실용화진흥원,

2016.2
[4] 문기영, “생체인식 기술현황 및 전망,” 한국전자통신연구원(TTA) Journal no.98, pp.38-47, Special Report, 2005.
[5] 정연덕, “생체인식기술(biometrics)의 효과적 활용과 문제점,” 지식재산논단, 2004.
[6] 생체기술의 장점과 한계, http://www.itworld.co.kr/news/77055, 2012.7.30
[7] 생체인식보안, http://www.businesson.co.kr/474, 2014. 4.22
[8] 이동기, “FIDO(Fast IDentity Online)생체 인증 기술 표준화 동향,” TTA Journal(표준 시험인증 기술동향), Vol.157, pp.76-81, 2015.
[9] 백영현, “간편결제에 적용되는 바이오인식 기술 현황,” TTA Journal(바이오인식), Vol.165, pp.47-52, 2016.5.6.
[10] 한국인터넷 진흥원, “KISA 바이오인식 기술 연계한 공인인증 활용 기술 개발 추진,” 보도자료, 창조경제, 2015.5.21.
[11] 김종현, “국내외 생체인식 기술의 도입 현황과 전망,” 우리금융경영연구소 주간 금융경제동향 이슈브리프, Vol.5, No.19, pp.11-14, 2015.7.22
[12] 정훈, “금융산업에서 생체인식 기술의 활용 현황과 전망,” KB금융지주경영연구소, Vol145, No.42, pp.1-5, 2014.6.2
[13] 김성일, 차현나, “스마트폰 해킹의 위험성과 대응 방안,” KT경제경영연구소 ISSUE & TREND, 2013
[14] 박범근, “생체인식기술 및 시장동향,” 연구성과실용화진흥원 S&T Market Report, Vol.39 2016.2
[15] 박영철, “생체정보의 보호.” 헌법학연구, 10(4): 308-311. 2004
[16] 이창범, “생체 프라이버시 보호 원칙에 관한 연구,” 인터넷법률, Vol 31, pp.19-48. 2005
[17] 간편 결제에 지문인식 도입 바람 분다, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160624142015 2016.6.26.일자 ZDNet Korea
[18] 지문결제 도입 한창 한일, 손가락 전쟁, http://www.etnews.com/20160429000272
[19] 해커들 1년전부터 미국비밀정보사용허가 데이터에 접속, http://www.itworld.co.kr/news/94125
[20] 프린터 인쇄한 종이로 스마트폰 지문인식 성공, https://www.hackerslab.org/news/printer/
[21] 카카오, 애플, 삼성 등 간편결제서비스 보안성 비교, http://www.ipnomics.co.kr/?p=37487
[22] 모바일 간편결제 플랫폼의 경쟁 그리고 2세대로의 진화, http://techm.kr/bbs/board.php?bo_table=article&wr_id=2157
[23] 서승현, 전길수, “스마트폰 보안 위협 및 대응전략,” TTA Journal(special theme, 스마트폰 정보보호), Vol.132, pp.44-48

[저 자 소 개]

전 정 훈 (Jeong-hoon Jeon)

2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr