논문 18-43-10-25 The Journal of Korean Institute of Communications and Information Sciences '18-10 Vol.43 No.10
https://doi.org/10.7840/kics.2018.43.10.1733

금융 서비스를 위한 바이오 인증 개선 방안

정 부 금•, 권 헌 영*, 박 혜 숙**, 임 종 인°

Improvement of Biometric Authentication for Financial Services

Boo-geum Jung•, Hun-yeong Kwon*, Hea-sook Park**, Jong-in Lim°

요 약

금융권에서 본인 인증 수단으로 사용되었던 공인인증서의 의무 사용 폐지 추진과 핀테크 서비스 및 비대면, 온라인, 모바일 거래의 활성화로 생체 정보를 이용한 간편한 바이오 인증이 급격히 적용되고 있다. 그러나 생체 정보사용에 대한 거부감, 유출에 대한 불안감은 새로운 방식의 확산에 장애가 되고 있다. 이에 본 논문에서는 금융 서비스에서 공인인증서를 대체할 기술로 예상되는 바이오 인증의 적용 현황과 정책 현황을 분석하여 각 분야에서의 문제점 및 이슈들을 도출하였다. 이를 바탕으로 보안성과 편의성을 높일 수 있는 개선 방안들을 제안하여, 핀테크 및 금융 서비스를 위한 안전하고 편리한 바이오 인증 기술 개발 및 정책 수립 방향 설정 도움이 되고자 한다.

Key Words : Fintech, Financial Service, Bio Authentication, Bio Template, Bio Distributed Store

ABSTRACT

Easy biometric authentication has been applied and expanded rapidly to the financial services, due to the relax regulation of the mandatory use of the accredited certificate used in the financial sector and the activation of non face-to-face, online, and mobile transactions. However, this new method is not easily accepted because of the reluctance to use personal physical information and anxiety about leakage of sensitive data. But now, biometric authentication is expected to be the best technology to replace credited certificate in financial services. Thus, in this paper, we analyzed the present status of biometric authentication technology, legal system and policy on financial services. And we derived the problems and issues in each field. Based on this, we'd like to propose some enhanced ways to provide safe and convenient biometric authentication for pin-tec and financial services.

Ⅰ. 서 론

비밀번호를 입력하지 않고 지문으로 금융거래를 하고 결재를 하는 것이 더 편리하고 안전한 것일까? 복잡한 공인인증서 비밀번호의 수차례 입력 실패로 불편을 겪은 경우가 누구나 있을 것이다. 또한, 이러한 불편함이 없는 지문인증으로 변경할 수 있음에도 불구하고 등록 절차가 번거롭거나 생체 정보를 등록한다는 것에 대한 불안감으로 아직 생체인증을 적용하지 못하고 있는 경우도 있을 것이다.

공인인증서는 금융거래 및 전자상거래 시 본인의 신원과 문서의 위·변조, 거래사실 부인 방지 등을 위해 사용하는 전자정보로 1999년 전자서명법이 제정되면서 독점적 지위가 부여돼 왔다. 하지만 사용 절차와

◆ First Author : Korea University Department of Information Security & ETRI, bgjung@etri.re.kr, 정회원
° Corresponding Author : Korea University Department of Information Security, jilim@korea.ac.kr, 정회원
* Korea University Department of Information Security, khy0@korea.ac.kr, 정회원
** ETRI Defense & Security ICT Convergence Center, parkhs@etri.re.kr, 정회원
논문번호 : 201807-217-0-SE, Received July 22, 2018; Revised August 13, 2018; Accepted September 21, 2018

관리에 있어 불편함이 점차로 부각되었고, 또한 혁신적인 핀테크 서비스, 비대면, 온라인, 모바일 금융 서비스의 원활한 수용을 위하여 2015년부터 추진되어 드디어 20년 만인 2018년 공인인증서 의무 사용이 폐지될 것으로 보인다.[1)]

공인인증서 의무 사용 폐지 추진에 따라, 생체 정보를 이용한 금융서비스가 활성화 되고 있다. 그러나 생체정보는 한번 유출되면 변경할 수도 없으며 개인의 내적인 정보가 유출되는 것에 대한 두려움으로 적극적인 수용에 문제가 발생하게 된다.

이에 본 논문에서는 향후 공인인증서를 대체할 최고의 기술로 예상되고 있는[2)] 바이오 인증 시스템의 현황을 살펴보고 문제점 및 이슈를 도출하며 이를 개선하기 위한 방안들을 제시하여 바이오 인증 기반의 안전한 금융 서비스 제공을 위한 기술 개발 방향 설정 및 정책 수립에 도움이 되고자 한다. 2장에서는 기술적 현황을 분석하며, 3장에서는 제도적 정책적 현황을 분석하며 4장에서는 이러한 현황 분석을 통하여 도출된 문제점을 해결하기 위한 방안들을 제시하고, 5장에서 결론을 맺는다.

Ⅱ. 금융 서비스를 위한 바이오 인증 기술 현황

바이오인증(생체인증) 기술이란, 개인을 식별할 수 있는 고유의 신체적 또는 행동적 특징(이하 바이오정보, 생체정보)을 통해 신원을 확인하는 방식이다. 특히 생체인증은 비밀번호, 공인인증서 등과 같이 인증정보를 소지하거나 기억할 필요가 없기 때문에 기존 인증방식과 비교하여 편리하며 분실 및 유출 등으로 인한 악용 우려가 적은 안전한 인증방식으로 평가받고 있다. 특히, 최근 모바일 금융거래가 증가하고 핀테크가 활성화되면서 생체인증은 기존의 인증수단을 보완하거나 대체할 수 있는 방식으로 각광 받고 있다. 본 장에서는 바이오인증이 가장 활발히 적용되고 있는 금융권에서의 바이오 인증 수단과 적용 분야에 대해서 분석한다.

2.1 금융권 바이오 인증 수단

생체인증은 본인이 없으면 사용할 수 없는 고정형 정보를 본인만이 사용 할 수 있기 때문에 유일무이한 신원확인의 효력이 있다[1].

지문은 가장 오래되고[3)] 보편적으로 사용되고 있는 인증 수단이다. 지문인식은 보통 지문 융기의 분기점, 끝점 등으로 구성되는 특징 점의 위치와 속성을 추출, 저장, 비교하는 알고리즘을 채용한다.[4)] 지문은 다른 생체인식 기술에 비해 인식장치가 소형화되고 비용이 저렴하며, 사용자에게 친숙하고 편리하다는 점에서 가장 많이 활용되고 있다. 그러나 인식기에 직접 접촉해야하기 때문에 여러 사람이 이용하는 경우 불쾌감이나 위생 문제를 야기할 수 있으며, 불의의 사고나 후천적인 요인으로 지문이 변화하거나 없어질 수 있다. 사진이나 실리콘으로 위조가 가능하며, 생체 정보 유출의 위험이 있다. 또한, 지문은 여러 곳에 남겨질 수 있으므로 정보주체의 지문이 유출되거나 도용될 위험성이 있다.

얼굴 인식은 각 개인 얼굴의 특징을 이용한다. 얼굴 영역을 추출하는 방법으로는 얼굴 영상을 이용하는 방식과 얼굴에서 발생하는 열을 이용하는 방식이 있다. 열상을 이용하는 방식은 적외선 카메라를 사용하여 얼굴 혈관에서 발생하는 열을 촬영한 후 디지털 정보로 변환하여 저장하는 방식인데, 얼굴에 미미한손상이 발생하더라도 본인거부율[5)]이 낮은 장점이 있지만, 영상 획득을 위해 사용하는 적외선 빛에 대해 사람들이 거부감을 가질 수 있다는 단점이 있다. 또한 사진으로도 얼굴로 인식되는 문제점이 있다.[6)]

홍채인식은 안구 중앙의 검은 동공과 흰자위 사이에 있는 도넛 모양의 홍채를 이용한 인증 기술이다. 홍채인식 장치의 적외선 카메라가 홍채를 이미지화한 후, 홍채인식 알고리즘으로 사용자 고유의 홍채 코드를 생성, 등록 후 비교하는 방식이다.[7)] 홍채는 생후 10개월경에 고유한 구조가 형성되어, 후천적인 상처나 질병과 같은 요소를 제외하면 평생 변하지 않는다.

1) 초연결 지능화 규제혁신 추진 방안 http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1373741

2) 보안뉴스>보안 설문조사 (2018-03-20~2018.05-01) http://www.boannews.com/media/poll_02.asp?db=&page=1&gpage=1&idx=177&search=&find=

3) 고대 바빌론 시대부터 신분증명에 이용되었으며, 1684년 영국 왕립협회에서 지문이 사람마다 모두 다르다는 사실을 발견

4) Learn Biometrics, Physiological Modalities, https://www.tutorialspoint.com/biometrics/physiological_modalities.htm

5) 생체 정보의 주인이 인증을 요청했음에도 본인이 아닌 것으로 결과가 나올 확률

6) "얼굴인식 기능 스마트폰, 사진만 대도 잠금 풀려" http://news.mk.co.kr/newsRead.php?year=2017&no=218850

7) "Video Images Fusion to Improve Iris Recognition Accuracy in Unconstrained Environments", https://www.researchgate.net/figure/264825250_fig1_Fig-1-Architecture-for-iris-recognition-system

일란성 쌍둥이도 서로 다른 형태의 홍채를 가지고 있어 개인을 식별하는데 훨씬 정확하다. 본인인증에 실패할 확률이 100만분의 1정도로 정확도가 높을 뿐 아니라, 인식 속도도 빠르다. 홍채 인식은 보통 10cm 정도 거리에서 이루어지는데, 지문과 달리 비접촉 방식이고 콘택트렌즈나 안경을 착용해도 인식이 가능하기 때문에 불쾌감이 낮고 위생적이라는 장점이 있다. 그러나 홍채인식 시스템도 고해상도의 사진을 통해서 우회할 수 있음이 드러난 바 있다.[8] 또한, 홍채인식 장치의 정확도는 특이한 조명 등에 의해 영향을 받을 수 있고, 홍채인식 장치가 눈에서 일정거리 이상 가까워야 하며, 당뇨병 등 질병에 의해 홍채가 변할 수도 있다. 다른 생체인식에 비해 홍채인식 장치는 비싼 단점이 있다.

정맥인식은 사람마다 고유한 혈관형태를 갖고 있다는 특성을 이용한다. 혈관 인식 위치에 따라 손가락 정맥, 손등 정맥, 손바닥 정맥 등으로 나눌 수 있다. 대부분의 정맥인식 장치는 근적외선이 헤모글로빈에 흡수되는 성질을 이용하여 정맥 이미지를 추출한다. 혈관 분포를 지도의 도로망처럼 단순화한 뒤, 분기점 간 거리나 각도 등 각 분기점 정보를 저장한다.[9] 사람의 혈관은 유전적 형질이 같은 일란성 쌍둥이조차도 형태가 달라 인식 정확도가 높으며, 피부 내에 존재하는 정맥을 이용하기 때문에 외부로의 노출이나 복제가 불가능하며, 비접촉식으로 위생적으로 공공장소에서 사용 가능한 장점이 있다. 그러나 정맥인식 장치의 구조가 소형화하기 어렵고 전체적인 비용이 증가하는 단점이 있다.

음성인식은 사용자의 음성에서 뽑아낸 특징들을 이용하는 인식기술로 비강과 구강의 형태로 인한 특징을 이용한다. 음성의 특징들은 소리의 높낮이에 영향을 받지 않으며 음성의 경우, 코, 입의 형태에 의존하기 때문에 비슷하게 흉내 내려고 해도 똑같이 모사되지 않는다. 음성인식은 단말기에 기본적으로 구비되어 있는 마이크를 인식장치로 이용할 수 있어, 단말기를 새로 설치하거나 구입해야 하는 부담이 적다는 장점이 있다. 원거리에서도 음성 취득이 가능하다. 그러나 주변에 소음이 있거나 음성인식장치의 성능에 따라 인식률이 달라지는 것이 단점이며, 녹음된 음성을 이용한 해킹에도 취약할 수 있다.

2.2 금융권 바이오 인증 적용 분야

인터넷 기술의 발달로 온라인쇼핑과 인터넷뱅킹 등의 서비스도가 활성화된 지 10년이 넘었다[10]. 온라인에서 은행 사이트를 방문할 때마다 보안프로그램들이 PC에 필수적으로 설치되어야 하는 불편함 등을 개선하기 위한 생체인증은 유출되거나 해킹되기가 어렵고 사용이 간편하기 때문에 금융권을 중심으로 급속히 도입되고 있다.

금융분야에서 바이오인증이 제일 많이 활용되는 분야는 ATM으로 미국, 일본 등 다수의 국가에서 생체정보를 이용한 ATM이 운영 중이다. 가장 적극적으로 적용한 국가는 일본으로 주로 손바닥 정맥과 손가락 정맥을 인증수단으로 사용하고 있다. 일본은 지정학적 특수성으로 지진 등 자연재해 시 통장 및 OTP 등을 잃어버린 경우에도 생체정보 만으로 현금인출 및 송금이 가능하도록 시스템을 구축한 것이다.

바이오페이는 'bio'와 'pay'가 결합된 합성어이다. 즉, 생체 정보로 카드 결제가 가능한 거래 방식을 뜻하는 것이다. 롯데월드타워는 세계 최초 무인 스마트 편의점을 선보였다. 이 편의점에서는 카드나 다른 지불 수단이 없어도 물품을 구입할 수 있다. '핸드페이'[11]라는 이 시스템은 사람의 손바닥 정맥 정보를 읽어내어 결제를 가능하게 한다.

모바일결제서비스는 스마트폰 제조 기업을 중심으로 자체적으로 혹은 전자금융기업과 협력으로 바이오인증기술 기반으로 제공하고 있다. 애플, 삼성전자, 등 주요 핸드폰 제조 기업은 애플페이, 삼성페이 등 지문인식 기반의 모바일결제서비스를 활용중이며 스마트폰의 생체 인증 기술의 발전에 따라 홍채, 얼굴, 지문 등 다양한 바이오인식기술을 사용한 서비스가 출시되고 있다.

텔레뱅킹은 전화기를 사용하므로 음성인식 기술을 적용할 수 있으며 등록절차가 간단하고 단말기에 기본으로 탑재되어 있으므로 비용 면에서 다른 바이오인증기술에 비해 유리하다. 통화 연결 시 음성인식 서비스를 이용하여 사용자의 동의를 받고 통화 내용중 음성의 일부를 선택하거나 지정 문장을 읽도록 하여 등록하는 방법을 사용한다.

오프라인 결제서비스에는 지문, 안면인식, 정맥 등의 인증기술이 사용되고 있다. 결제절차를 간단하게

8) 2014년 독일 해커단체 CCC는 푸틴 러시아 대통령의 고해상도 사진을 이용하여 생체인식 시스템을 우회할 수 있음을 시연한 바 있다. (한국경제, "[Focus] 인증 기술 진화… 비번→패턴→지문→홍채→?", 2016년 8월 12일)

9) IDENTYTECH Solutions, http://www.identytech.com/palm-vein-recognition/

10) www.finda.co.kr/post/financial-product/saving/7934

11) http://news.joins.com/article/21982703, "[디지털 금융] 손바닥 정맥 결제<핸드페이>, 세계 최초 상용화", 2017.09.29.

하고, 결제 지연시간을 단축시키는 등 사용자에게 편의성을 제공하고 있으며 신용카드번호나 계좌번호와 함께 생체정보를 사전에 등록해 두어 물품 결제 시 신용카드를 제시하지 않고 기 등록된 생체정보를 사용하여 결제가 가능하다.

간편결제 서비스는 지문센서가 탑재된 스마트폰을 기반으로 등장했다. 온라인에서는 15만여 개의 온라인 쇼핑몰 가맹점을 확보한 네이버페이가 시장을 주도하고 있다. 오프라인 간편 결제에서는 삼성페이가 앞서가고 있다. 삼성페이는 기존 마그네틱 신용카드 결제기에도 결제가 가능 하도록 하여, 신용카드가 결제 가능 한 모든 곳을 가맹점으로 두고 있다

스마트폰을 이용한 모바일 뱅크 서비스에는 지문홍채 등의 인증기술이 사용되고 있으며 은행, 보험 등의 금융기관에서 운용되고 있다. 공인인증서 및 OTP를 대체하여 생체인증 만으로 간편하게 금융거래가 가능한 간편한 서비스를 제공한다.

2.3 금융권 바이오 인증 방식

바이오정보를 이용하여 본인임을 인증하는 방식에는 바이오정보를 저장하는 위치의 차이로 인하여 서버 저장 방식과 FIDO 방식으로 구분되며, 서버 저장 방식에서는 바이오 정보를 서버에 저장하게 되고, FIDO에서는 생체 인식 단말기에 저장한다.

FIDO(Fast Identity Online)는 모바일 및 인터넷 환경을 위한 바이오인증 방식의 기술 표준으로, 개방된 기술표준 정립을 목적으로 하는 글로벌 바이오인증 기술표준 연합회인 FIDO Alliance에서 만든 것이다. FIDO는 아이디와 패스워드를 입력하는 대신 생체정보를 사용하고, 생체정보를 사용자 단말기에 보존한다. 인증 과정은 단말기 내에서 이루어져 그 결과를 공개키 암호 방식으로 서버에 전달하고 로그인 하는 방식을 사용한다. FIDO는 UAF[12]와 U2F[13] 두 가지 방식이 있다. UAF는 사용자의 단말기에서 제공하는 인증방법을 온라인 서비스와 연동하여 인증하는 기술로 패스워드 없이 생체정보만으로 인증을 완료하는 것을 말하며, U2F는 기존 패스워드를 사용하는 지식기반 인증에서 USB, NFC 보안키, 생체인증 등의 두 번째 인증요소를 추가 하는 것을 의미한다. UAF 방식은 스마트폰과 같은 모바일 환경에 적합한데, 그 이유는 모바일 기기에는 지문 인식 모듈, 홍채 인식 카메라, 얼굴인식 카메라, 마이크 등이 탑재돼 생체 정보를 인식하기 위한 기반이 마련되어 있기 때문이다. 반면 U2F는 기존 PC 기반 온라인 서비스에 적합하다.

서버 저장 방식은, 스마트폰으로 할 수 없는 서비스인, 디지털 키오스크, 홍채인증 ATM 서비스를 대상으로 하며, 개인의 생체정보가 금융회사 서버에 저장되어 있고 생체 인식단말에서 추출한 생체정보를 전송해 서버에서 비교한다는 특징을 갖는다. 정맥, 홍채 등 생체정보에서 개인마다 다른 고유한 특징을 추출해 낸 것을 '템플릿'이라고 부른다. 이러한 템플릿을 자사 서버에 저장한 뒤 인증한다. 이렇게 서버에 저장된 정보는 유출의 위험이 있는데, 미국 연방인사관리처(OPM)는 연방정부 소속 공무원 560만명의 지문을 포함한 생체정보가 유출되는 해킹사건을 겪었다[14]. 우리나라에서도 지문을 포함한 다양한 생체정보가 이전보다 적극적으로 활용될 것으로 예상되는 만큼 이러한 정보를 보다 안전하게 저장하는 방법과 함께 유출된다고 하더라도 유출된 정보를 범죄자들이 재사용하지 못하도록 하는 대책이 함께 마련되어야 할 것이다. 또한 서버로 전송 시 해킹을 통해 탈취될 가능성에 대해서도 대비해야한다.

Ⅲ. 금융권 바이오 인증 정책 현황

금융에 IT 기술이 접목되는 편리한 핀테크 서비스의 확산을 위해서 금융위원회에서는 보안성심의 제도, 인증방법평가위원회 제도 폐지로 금융 서비스의 보안 규제방식을 핀테크가 앞선 국가들의 방식과 같이 사전에 실행 하지 못하게 제한하는 것보다 사후에 보안을 강화하는 방향으로 규제의 개념을 개선하고 있다[2].이는, 이러한 정책의 일환으로, 전자금융거래에서도 공인인증서, OTP 등 일회용비밀번호의 의무 사용 완화 추진 등 각종 규제가 순차적으로 완화되고 있다. 특히, 공인인증서의 실제사용 환경에서는 표준이 아닌 기술로 구현되어 있어 추가적인 프로그램을 설치해야 하는 불편함이 따르고, 악성코드로 사용자 단말기에서 공인인증서 탈취가 가능하다는 취약점이 문제점으로 제기되었다[3]. 본 장에서는 바이오 인증 활성화를 위하여 펼쳐지고 있는 제도 및 정책 현황을 분석한다.

3.1 금융 서비스에서 바이오 인증의 법적 근거

전자금융거래법은 컴퓨터, ATM, 전화기 등 전자장치로 이루어지는 금융거래를 규율하고 전자금융업의 운영과 감독에 관한 사업법이다. 기존 전자금융거

12) Universal Authentication Framework
13) Universal 2nd Factor
14) http://news.joins.com/article/18735128

래법 제21조 제3항에서는 “금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자서명법 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다.”고 명시하여 금융 회사들은 공인인증서를 사용할 수밖에 없는 상황이었다. 하지만, 개정된 전자금융거래법에서는 “금융회사 등은 전자금융거래의 안전성 과 신뢰성을 확보할 수 있도록 인증방법에 하여 금융위원회가 정하는 기준 을 준수하여야 한다.”(제21조 제2항)고 하고, “금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제 하여서는 아니 되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.”(제21조제3항)고 개정하였다. 이에 따라 전자금융감독규정 또한 개정이 되었는데, 기존 전자금융감독규정 제37조에서는 “모든 전자금융거래에 있어 전자서명법에 의한 공인인증서는 이와 동등한 수준의 안정성이 인정되는 인증방법을 사용하여야 한다.”는 내용을 개정하여 “전자금융 거래의 종류, 성격, 위험 수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.”라고 명시하면서 공인인증서 의무사용을 폐지하였다. 따라서 생체인증 기반 인증 기술은 공인인증서를 대신하여 전자금융거래에 사용될 수 있는 법적인 근거가 된다.

3.2 비대면 실명 인증

금융위원회에서는 ‘실명확인 방식 합리화 방안’[4]을 발표하여 인터넷전문은행 및 기존 금융회사에서의 비대면 인증을 허용하였다. PC, 스마트폰, ATM 등 디지털 채널을 이용하여 실명확인을 수행하기 때문에 오프라인 지점에 가지 않고도 계좌를 개설하거나 금융거래를 할 수 있는 것이다. 그러나 비대면 인증 기반의 계좌개설은 금융회사 입장에서는 고객층 확장을 위한 새로운 방식이지만 고객입장에서는 개인정보 및 금융자산에 위험을 가져올 수 있는 요인이 되기도 한다. 디지털 채널 등을 이용한 비대면 인증은 편리함이라는 이면에 해킹사고가 발생했을 시 다수의 대포통장 개설 가능성 등의 위협이 존재한다. 디지털 채널만으로 인증을 수행하기 때문에 인증과정에서의 취약점으로 인한 보안사고가 발생할 경우 다수의 피해자를 유발할 수 있어 대면인증보다 위험 영향도가 높을 수밖에 없다.

3.3 생체인식 기반 간편 공인인증

한국인터넷진흥원에서는 금융 서비스 제공자가 전자서명 요구 시, 기존의 비밀번호 입력 없이 지문 등 생체정보로 인증하는 ‘간편 공인인증서 인터페이스 가이드라인[5]’을 제시하였다. 이 가이드라인은 스마트폰의 트러스트존[15], 유심, IC카드 등의 보안매체에 저장된 공인인증서가 사용자 단말에서 부가적인 소프트웨어 설치 없이 사용될 수 있도록 기술적인 요구사항을 담았다. 사용자와 금융서비스 제공자에게 일관성 있는 사용자 경험을 제공하기 위해 요구되는 기본적인 기능과 인터페이스에 관한 것으로 사용자 프로그램 내 간편 인증 저장매체 추가를 위한 요구사항, 간편 인증 UI/UX 최소 요구사항, 간편 인증 서비스 분야 간 상호연동을 위한 규격, 모바일 단말에서 전자서명을 위한 규격 등이다. 또한 스마트폰에서 공인인증서를 대체하여 바이오정보를 사용할 수 있도록 ‘스마트폰 환경에서 바이오 정보 연계 공인인증서 안전 이용 구현 가이드라인[6]’을 배포하였으며, 최근에는 홍채, 얼굴 등 생체인식 스마트폰이 출시되어 금융권은 이 가이드라인에 기반을 두어 ‘지문 및 홍채 기반의 공인인증서비스’를 출시하고 있다.

3.4 바이오정보 분산 관리

한국은행은 금융정보화추진협의회[16]를 통해 바이오정보를 2조각으로 나누어서 한조각은 금융회사 서버에 보관하고 나머지 조각은 외부 서버에 보관하며 금융 거래시 바이오정보 조각을 결합해 인증하는 체계를 표준으로 제정했다[7]. 금융사가 아닌 분산관리를 하는 외부 기관으로서는 금융결제원을 들 수 있다. 바이오정보 분산관리는 금융서버방식과 개인매체방식으로 구분된다. 개인매체방식은 스마트폰에 기본으로 제공되는 센서가 지원하는 인식기술 및 기관별로 제공하는 기술을 활용하는 것으로, 공동 FIDO 이용, 개별 FIDO 연계 업무 중 하나를 선택해 이용한다. 금융서버방식은 금융회사가 제공하는 ATM, 키오스크, 오프라인 창구, 온라인 고객센터에서 손바닥정맥, 지문, 정맥, 얼굴, 홍채 등의 생체인증을 사용한다. 금융서버방식은 자사인증과 위탁인증으로 나뉜다. 자사인증은, 기관에서 바이오정보를 수집하고 이를 분할해 한 조각은 기관에서 저장하고 나머지 한 조각은 분산 관리센터로 보내고, 인증시점에 분산관리센터로부터 조각을 전송받아 기관의 시스템에 보관된 조각과 결합하여 인증하는 방식이다. 위탁인증은 기관에서 수집한 생체정보를 분산관리센터로 전송하고, 센터에서 분할한 후 한 조각을 다시 기관으로 전송해 보관하게 하

15) 트러스트존(TrustZone) : 스마트폰 앱의 안전한 실행환경을 제공하기 위한 스마트폰 내에 존재하는 안전 영역

16) 금융정보화 추진을 위해 국가정보화 기본법 제19조에 의거 설치된 민간기관 등과의 협의체

고, 기관은 인증시점에 보관하고 있던 조각을 분산관리센터로 보내 결합 및 인증 하는 것으로 인증을 외부기관에 위탁하는 방식이다.

Ⅳ. 금융 서비스를 위한 바이오 인증 개선 방안

홍채나 지문, 음성만으로 금융 서비스를 받는 생체인증 시대가 열리고 있지만, 아직은 시작 단계로 개선해야 할 점이 많이 있다. 공인인증서나 보안카드와 같은 별도 소지 수단 없이 간단하게 금융 거래를 할 수 있다는 편리함 이면에는 보안 문제가 내재되어 있기 때문이다. 보안을 강화하다보면 편리함이 떨어질 수 있고 편리함만 생각하게 되면 보안이 약화될 수 있다. 본 장에서는 사용자에게는 최대한 편리함을 제공하면서 내부적으로는 보안을 강화하여 안전함과 간편함의 균형을 이루기 위한 개선 방안을 제시하고자 한다.

4.1 바이오 정보 분산 인증

금융결제원과 금융기관이 생체정보를 나눠서 보관하는 바이오정보 분산관리시스템을 구축했지만 여전히 해킹 공격에서 자유롭지 못한 문제점이 있다. 생체정보를 분산 저장하면 한곳에서 전체를 보관했을 때보다 정보 유출의 위험성을 낮출 수 있다. 그러나 문제는 금융거래시점에 조각났던 정보가 인증 시 온전한 형태로 융합돼 유출 시 악용될 수 있다는 점이다. 자사인증이든 위탁인증이든 분산되어 있던 정보가 한 서버에 모여 결합되어 원래의 완전한 정보의 형태가 되어 인증이 되는데 이렇게 결합된 정보가 유출되게 되면 이는 식별 가능한 형태로 변하기 때문이다. 개인기기가 아닌 외부 시스템으로 보내진 생체정보는 언제든지 유출될 가능성이 있다. 분산 저장에서 한 단계 더 나아가 분산 인증을 하게 되면 분산 저장의 장점을 그대로 살리면서 보안을 강화하는 방안이 될 것이다. 즉, 보관할 당시에 템플릿을 분할했던 방식으로 인증 시 템플릿을 분할하여 금융결제원과 금융회사 각각으로 분산해서 전송하여 각각 인증하고 결과값을 전송받아 두 결과 값이 모두 성공일 경우 정상적인 인증이 완료되도록 하는 방안이다. 이를 구현하기 위해서는 분산 보관을 이용한 분산 인증 기술개발과 정책이 제공되어야 할 것이다.

4.2 바이오 인증 시스템 공유

바이오인증기술은 독자적으로 구축 시 많은 비용이 소요되므로 적극적인 상호 협력이 필요하다. 또한, 등록된 생체정보가 타 금융기관에서 사용할 수 없으면 사용자는 각 개별 금융기관 별로 각각 생체정보를 중복해서 등록해야 하는 불편이 따른다. 공인인증서 및 OTP의 경우 한 금융기관에 등록 하면 타 금융 기관에서도 사용 가능하다. 각 금융기관이 고객의 생체정보를 자사의 서버에 각각 저장하는 경우 유출에 대한 위험부담이 크며, 고객 입장에서도 불안감이 있을 수 있으므로, 신뢰할 수 있는 공인된 외부 기관을 이용하는 방법도 가능할 것이다. 신뢰할 수 있는 외부 공인 기관은 생체정보 관리를 위한 보안강화에 집중하고 각 금융기관은 타 금융기관과 연동한 일관된 서비스 제공이 가능해져 생체인증기술의 안전한 생태계 조성에 유리하다. 다만 생체정보 송수신과 저장이 외부 공인 기관에서 모두 이루어짐에 따라 사이버공격의 표적이 될 수 있어 강력한 보안기술의 적용이 필요할 것이다.

4.3 바이오 정보 단독 인증

현재 금융권은 바이오 정보의 종류 중에서 2개 이상의 정보를 사용하도록 규제하고 있다. 하나의 생체정보로는 본인 인증을 받을 수 없게 되어 있어 또 다른 생체정보를 제공하든지 기존의 핀넘버 또는 ARS, SMS 등의 인증을 추가로 거쳐야 한다. 이는 생체인증으로 금융거래의 편의성과 업무 처리 속도를 높이겠다는 취지와는 거리가 있다. 미국이나 일본 등 해외사례[8]를 참고하여 생체인증 기술의 강화로 기존 공인인증서 하나로 인증한 것과 동일하게 생체인증서 하나로 인증이 가능한 기술적인 보완이 필요하다.

4.4 전자서명으로서의 효력

생체정보는 현재 진행 중인 거래와는 무관한 고정된 정보이므로 전자서명의 효력을 갖기 위해서는 직접 거래정보와 연관된 서명정보를 생성할 수 있는 체계가 필요하다. 「전자서명법」은 '서명 생성정보가 가입자에게 유일하게 속할 것'이라고 정의(제2조 제3호 가항)하고 있는데, 금융기관에 생체 정보를 미리 등록하여 사용할 경우 가입자의 유일한 생체정보를 금융기관에서 똑같이 보유하게 되어(제2조 제3호의 가항을 위배) 전자서명용으로 이용이 어려울 수 있다. 전자서명으로서의 효력을 위해 생체정보를 다른 인증방법들과 같이 해야 할 경우 생체인증의 가장 큰 장점인 간편성은 저해되고 절차와 비용이 추가되는 부작용이 발생하게 되므로, 생체정보만으로 전자서명으로서의 효력이 가능하도록 기술개발 및 법제 개선이 필요하다.

4.5 바이오 정보 변경

생체정보의 특징을 추출하여 바이오인증을 위해 만든 데이터인 템플릿은 유출될 경우 금융사기를 노린 범죄자들에게 다른 용도로 유용될 가능성이 있다. 때문에 사용자가 템플릿 유출이 의심될 경우에는 비밀번호를 변경하는 것과 같이 템플릿을 변경할 수 있도록 해야 할 것이다. 고유의 생체정보는 변경할 수 없지만 템플릿은 생체정보의 특징들 중 몇 가지를 추출하는 것이기 때문에 변경이 가능하도록 기술적, 제도적 지원이 뒷받침되어야 할 것이다.

4.6 윤리적 보안

영화 <쥬라기 월드: 폴른 킹덤(2018)>[17]에서는 DNA를 복원하여 만들어진 공룡을 상업적 이익을 위해 악용하며, 만들어진 동물이라 할지라도 보존과 생명의 권리를 보장해야 하는지의 딜레마에 대한 내용이 나온다. 또한 인간의 DNA를 이용해 새로운 인간이 클론되고 인간과 공룡이 공존하는 세상을 선언하며 마무리된다. 현실 속에서는 1985년 고대 이집트 미이라에서 DNA추출에 성공[9]했고, 매머드 시체에서 DNA를 추출[18]하기도 했다. 1993년에는 1억 3천만 년 된 호박에서 곤충 '바구미'를 발견해서 DNA를 추출[19]하는데 성공했다. 가장 정확하고 민감한 생체정보인 DNA를 추출하고 조작하는 것이 불가능하지만은 않을 것으로 예상되는 상황이다. 그러나, 인간이든 동물이든 모든 생체정보에 대한 조작이나 변형은 어떤 이유로도 행해져서는 안 된다. 생체정보의 비정상적인 유용은 인간의 존엄성을 파괴하는 행위이다. 따라서 바이오인증 산업이 본격화되기 이전에 윤리적 보안에 대한 사회적 여건과 제도적 뒷받침이 조성되어야 할 것이다.

V. 결 론

금융권에서 생체정보의 활용은 편의성과 보안성을 장점으로 하여 적용될 수 있는 분야가 다양하다. 금융사기를 차단하고 투명한 납세는 물론 금융소외계층이나 사회적 취약계층에 대한 금융서비스 지원도 현실화 가능하다. 하지만 생체 정보관리의 중요성을 인지하지 못하거나 빈약한 내부통제로 인한 정보유출, 해킹을 통한 생체 위변조는 심각한 결과를 초래한다. 또한 보안에 대한 우려는 간편하고 확실한 인증 수단인 바이오정보의 활용을 저해하는 요인으로 작용한다. 이에 본 논문에서는 바이오 인증의 보안성과 편의성을 제고할 수 있는 방안들을 제시하였다. 바이오 템플릿의 분산 인증으로 유출로 부터의 안전성을 높이며, 인증 시스템을 공유하여 편의성을 높이고, 생체 인증 단독으로 간편하게 인증과 전자서명이 가능하도록 하며, 정보 유출 시 비밀번호를 변경하는 것과 같이 바이오 템플릿 변경이 가능하도록 해야 한다. 또한, 생체정보에 대한 어떠한 변형이나 악용을 막고 인간의 존엄성을 지킬 수 있는 윤리적 보안이 선행되도록 해야 한다는 것이다. 이러한 개선 방안들을 실현하기 위해서는 기술적 개발 및 정책적인 제도가 마련되어야 하는 문제점이 있으나, 나 자신으로 나 자신임을 확인해 주는 명확한 바이오 인증으로 금융 서비스가 간편하고 안전하게 이루어지도록 하기 위해서는 기술 개발 및 정책의 개선을 늦추어서는 안 될 것이다.

17) http://movie.daum.net/moviedb/main?movieId=108035
18) 4만년전 매머드 DNA 추출 성공…복원 현실화되나 http://hankookilbo.com/v/2d73d81d91a84d7dbb4b88ce43379704
19) http://dl.dongascience.com/magazine/view/S199806N011

References

[1] M. Armstrong, J. Wright, and H. J. Lee, "Biometrics began accelerate in the mobile security authentication means," *Digieco*, pp. 1-10, 2016.

[2] U. Berger, "Access charges in the presence of call externalities," *J. Economic Anal. & Policy*, vol. 3, no. 1, Article 21, 2004.

[3] S. S. Jang, "A study on the effect fintech on the information security industry," *Internet & Security Focus*, pp. 4-32, 2015.

[4] Financial Services Commission, *Rationalization plan on Verifying real name when opening an account*, 2015.

[5] KISA, *Interface Guideline for HTML5 Based PKI Implementation*, 2016.

[6] KISA, *Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smart phone*, 2016.

[7] TTA, *TTAK.KO-12.0302: Biometrics Management Guidelines for the Financial Security*, 2016.

[8] H. M. Kim, "Secure non face-to-face authentication of financial companies," *Electron. Finance and Financial Secur.*, 2016.

[9] S. Pääbo, "Molecular cloning of ancient

egyptian mummy DNA," *Nature*, 1985.

정 부 금 (Boo-geum Jung)

1986년 2월 : 부산대학교 계산통계학과 졸업
1991년 8월 : 숙명여자대학교 전자계산학과 석사
2012년 2월 : 고려대학교 정보보호학과 박사과정 수료
1986년 1월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 바이오정보보호, 신뢰네트워크

권 헌 영 (Hun-yeong Kwon)

1992년 2월 : 연세대학교 법학과 졸업
1998년 2월 : 연세대학교 법학과 석사
2005년 2월 : 연세대학교 법학과 박사
2015년 9월~현재 : 고려대학교 정보보호대학원 부교수
<관심분야> 정보보호법 및 정책, 인터넷규제

박 혜 숙 (Hea-sook Park)

1992년 2월 : 경성대학교 전산통계학과 졸업
1994년 2월 : 부산대학교 이학석사
2005년 8월 : 충남대학교 이학박사
1994년 2월~현재 : 한국전자통신연구원 실장
<관심분야> 고신뢰네트워킹, 특수목적망 설계

임 종 인 (Jong-in Im)

1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
현재 : 고려대학교 정보보호대학원 및 사이버국방학과 교수
<관심분야> 사이버안보, 디지털포렌식, 개인정보보호