J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

암호 없는 사용자의 2차 인증용 복합생체 기반의 FIDO 플랫폼☆

FIDO Platform of Passwordless Users based on Multiple Biometrics for Secondary Authentication

강 민 구[1*]
Min-goo Kang

요 약

본 논문에서는 암호 없는(Passwordless) 사용자 환경에서 제로 트러스트(zero trust) 기반 복합 생체 인증을 제안한다. 다양한 FIDO 2.0(Fast Identity Online) 거래 인증 플랫폼 연동을 위한 메타버스와 연계를 설계한다. 특히, 스마트 단말기의 위치정보와 지자기 센서, 가속기 센서 및 복합인증(MFA, Multi-Factor Authentication)을 위한 생체정보 등을 적용한다. 이때, 조도 및 온도/습도 등 상황인식을 바탕으로 2차 인증으로 복잡한 인증을 통해 사용자 환경에 따른 적응형 복합 인증 플랫폼을 제시한다. 그 결과 사용자 환경에 따라 지문인식과 홍채인식, 얼굴인식, 음성 등 행동 패턴으로 다양한 제로 트러스트를 기반으로 2차 사용자 인증이 가능하다. 또한 FIDO 플랫폼의 복합 통합 인증 연계 결과를 확인하고, FIDO2.0을 이용한 거래 인증 연계 플랫폼의 인증 정확도를 개선하고자 한다.

☞ 주제어 : 암호 없는 보안, 복합인자인증(MFA), 제로 트러스트, FIDO 거래, 2차 사용자 인증

ABSTRACT

In this paper, a zero trust-based complex biometric authentication was proposed in a passwordless environment. The linkage of FIDO 2.0 (Fast IDENTITY Online) transaction authentication platforms was designed in conjunction with metaverse. In particular, it was applied with the location information of a smart terminal according to a geomagnetic sensor, an accelerator sensor, and biometric information for multi-factor authentication(MFA). At this time, a FIDO transaction authentication platform was presented for adaptive complex authentication with user's environment through complex authentication with secondary authentication based on situational awareness such as illuminance and temperature/humidity. As a result, it is possible to authenticate secondary users based on zero trust with behavior patterns such as fingerprint recognition, iris recognition, face recognition, and voice according to the environment. In addition, it is intended to check the linkage result of the FIDO platform for complex integrated authentication and improve the authentication accuracy of the linkage platform for transaction authentication using FIDO2.0.

☞ keyword : Passwordless security, Multi-Factor Authentication(MFA), zero trust, FIDO transaction, Secondary user authentication

1. 서 론

최근, 아파트 월 패드와 홈/의료 CCTV의 해킹 등으로 인한 ID/PWD 인증방식의 보완을 위한 복합 생체인증에 의한 사용자 2차 인증의 강화방안이 필요하게 되었다.

기존 SMS 문자인증과 OTP 등의 숫자, 코드 등의 확인 방식도 타인도용 및 유출의 위험이 상존하고 있다. 복합 생체인증 기반 사용자의 신원인증을 위한 지문, 홍채, 얼굴,음성 등 개인의 고유한 생체인증용 정보를 활용한다.

본 논문에서는 제로트러스트(Zero Trust) 기반의 사용자 ID의 2차 인증을 위한 플랫폼의 설계를 제안하고자 한다. 포레스터리서치가 2010년 '아무것도 신뢰하지 않는다'는 제로트러스트를 전제로 기업 내 보안강화 및 액세스 제어에 의한 접근 범위의 최소화를 제시하였다[1].

본 연구에서는 비대면 암호 없는 사용자 정보보호 환경에서 FIDO 기반의 H/W 또는 S/W로 안전영역을 구축하고, 그 안에 개인의 복합 생체인증 정보를 저장한다.

이로서 사용자의 환경에 따른 사용자 인증과 FIDO에 의한 거래인증 플랫폼은 메타버스와 같은 인터넷 환경에서 다양하게 활용될 예정이다[1].

2. 복합 생체인식 기반의 사용자 인증 분석

본 절에서는 제로트러스트 기반의 복합생체인증의 활

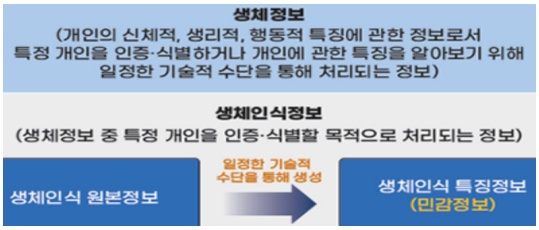
1 Dept. of IT Transmedia Contents, Hanshin Univ., Korea, 18101
* Corresponding author (kangmg@hs.ac.kr)
[Received 29 June 2022, Reviewed 9 July 2022, Accepted 4 August 2022]
☆ This research was supported by a research grant from Hanshin University

용으로 '21년 개인정보위원회 생체정보 보호 가이드라인'에서 생체인식정보 보호 조치를 통해 안전한 사용자 인증과 거래인증 플랫폼의 연계를 제시하고자 한다[2].

2.1 제로트러스트 기반의 복합생체인증 분석/설계

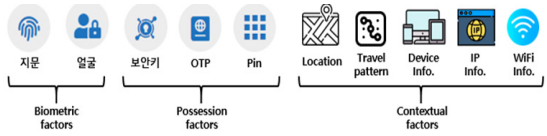
2.1.1 제로트러스트 기반 복합 생체정보 활용 분석

개인정보위원회에서는 생체정보 중 특정 개인을 인증·식별하기 위한 생체정보 보호 가이드라인을 설정하고, 개인정보와 생체정보, 생체인식정보 간의 관계 및 적용하는 규정을 처리하는 정보를 정의하였다.



(그림 1) 개인정보위원회 '생체정보보호 가이드라인'
(Fig. 1) Bio Information Protection Guidelines'[2]

복합인자인증(MFA, Multi-Factor Authentication)는 특징정보인 민감 정보로 분류되기 때문에 다른 개인정보와는 별도로 수집 동의를 받아야 한다.



(그림 2) 사용자인증 분석용 복합생체 인증방식의 분석
(Fig. 2) Multiple biometric platform for the information analysis of user authentication

이를 위한 수집·이용 동의서에 의무적인 포함사항은 ①수집·이용 목적, ②수집 항목, ③보유·이용기간, ④동의를 거부할 권리(이에 따른 불이익의 내용)가 포함된다.

또한, 복합생체정보의 단계에서 생체인식 정보에 대한 통제 수단으로 열람·정정·삭제 등의 통제 수단을 제공해야 한다. 복합 생체인식정보를 전송하는 경우, 암호화 알고리즘으로 전송한다. 전송구간은 SSL(Secure Socket Layer)/TLS(Transport Layer Security), VPN(Virtual Private Network) 등으로 생체정보를 보호해야 한다[2].

2.1.2 제로트러스트 보안분석과 MFA연동 모델

아무 것도 신뢰하지 않는 보안 전략인 제로트러스트는 복합팩터 인증(Multi-Factor Authentication)을 활용한다.

사용자가 내부 통신망에 인가된 사용자에게 권한을 부여한다. 사용자 ID를 검증한 후, 사용자 권한획득 이후에도 사용자의 접근범위를 최소화 하도록 한다[3].

제로트러스트는 한 번에 로그인하는 싱글사인온(SSO, Single Sign On)으로 여러 서비스에 접근할 수 있다. SSO를 도입한 이후 제로트러스트를 준수하려면 사내 방화벽과 VPN이외 새로운 보안 체계가 재구축 되어야 한다.

이는 2021년 미국 행정명령에 의한 이행계획으로 정부기관이 클라우드의 활용 비중을 확대했다. 이로서, 제로트러스트(ZTA Zero Trust Architecture)는 초세분화 적응형 인증 및 컨텍스트(Context) 인식정책을 제시했다[4].

(그림 3) ZTA 연동위한 복합 생체인자 인식모델 분석
(Fig. 3) Multiple biometric information MFA for interlocking ZTNA model

[그림 3]에서 Zero Trust Network Access(ZTNA)가 클라우드 사용자가 원격 접속을 위한 최소한의 액세스만 허용한다. 단말기가 보안 위험에도 공격을 억제할 수 있어야 한다. 이로서, 온프레미스(On-premise)와 프라이빗 클라우드(Private Cloud), 퍼블릭 클라우드(Public Cloud) 기존보안 정책의 갱신(Upgrade)을 추진하도록 해야 한다.

2.1.3 상황 인지기반의 지능형 MFA 생체정보 설계

사이버 보안 솔루션과 플랫폼 연동을 위한 복합 생체인식 기술은 모바일 디바이스 이외에 물리적 인증과 소프트웨어적인 사이버 인증의 경계가 융합된다[5].

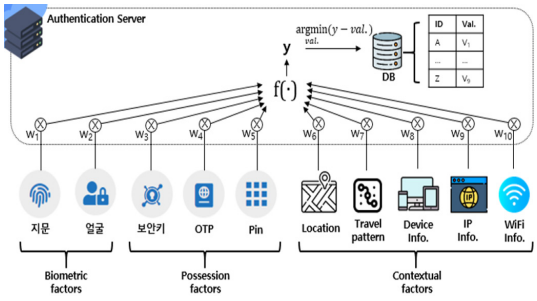
(표 1) 복합 생체인자 인증위한 생체 인식정확도 분석
(Table 1) Accuracy analysis of Multiple biometric MFA

구분	본인 거부률 (FRR : False Rejection Rate)	타인 수락률 (FAR : False Acceptance Rate)
지문	0.1%~0.5%	0.001%~0.01%
얼굴	1%~2.6%	1%~1.3%
홍채	0.0001%~0.1%	0.000083%~0.0001%
손가락 정맥	0.01%~0.3%	0.0001%~0.001%
손바닥 정맥	0.01%~0.1%	0.00008%~0.0001%
음성	1%	0.1%
서명	-	-
손모양	-	-

*출처: 한국은행 금융결제국

이러한 복합생체인증은 출입통제와 사이버 보안 서비스 및 플랫폼으로서 단말기 제조업체, 생체인식 솔루션 업체, 인증관련 분야에서 다양하게 활용되고 있다.

또한, 복합생체정보의 복합인증과 생체정보의 분산저장을 통해 이용률을 높이고 있다. [표 1]은 복합생체인식 MFA 인식정확도에 의한 사용자의 상황에 적합한 최적화된 사용자 ID 인식을 위한 2차 인증방안이 필요하다.



(그림 4) 상황 인지용 지능형 복합인증 연동
(Fig. 4) Intelligent MFA for context-aware authentication

[그림 4]는 사용자의 상황을 인지하는 지능형 사이버 보안과 클라우드 연동 및 5G 연동을 위한 MFA구조이다.

2.2 제로트러스트 보안과 2차 사용자 인증 모델

제로트러스의 보안을 강화하기 위한 사용자 2차 인증인 복합인자인증을 활용한다. 이때, 개인마다 유일하게 소지한 7가지의 고유 특성을 활용해야 한다[5].

(표 2) 복합생체인자(MFA) 활용위한 고유특성 분석
(Table 2) Analysis of unique characteristics for application of multiple biometrics(MFA)

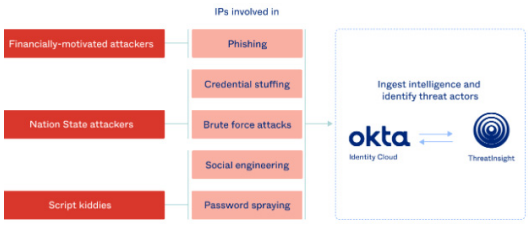
	특성	설명
일반적으로 갖추어야 할 특성	보편성(Universality)	모든 사람이 가지고 있는 생체 특성이어야 함
	유일성(Uniqueness)	같은 특성을 가진 사람이 없어야 함
	영구성(Permanence)	절대 변화하거나 변경되지 않아야 함
	획득성(Collectability)	센서로부터 생체특성정보 추출 및 정량화가 쉬워야 함
신뢰성을 높이기 위한 추가적인 특성	정확도(Performance)	시스템의 정확도, 처리속도, 내구성 등
	수용도(Acceptability)	시스템에 대한 거부감을 느끼지 않는 정도
	기만용이도(Circumvention)	비정상적으로 시스템을 속이기가 쉬운 정도

*출처: 정보통신정책연구원, NICE디앤비

2.2.1 상황 적응형 2차 복합생체인증과 활용분석

사용자의 상황에 따른 빅 데이터와 인공지능에 의한 데이터 처리 속도의 향상과 인식률을 향상되어야 된다.

이로서 암호 없는 사용자 인증의 정확도가 높아지면서 다양한 산업에서 활용될 것이다. 특별히, 스마트 디바이스(폰, 웨어러블 기기 등)와 IoT 기기의 확산으로 금융, 보안, 출입관리, 헬스케어, 검역, 엔터테인먼트 등 점차 많은 분야로 활용사례가 급증하고 있다[6].



(그림 5) 사용자인증 위한 상황인지 위험감지 사례분석
(Fig. 5) Case analysis of Context-aware threat detections for user authentication

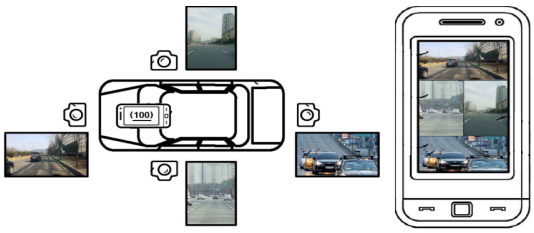
[그림 5]는 상황을 인지하고, 사용자 인증 전에 위협을 감지를 위한 의심스러운 IP 주소의 인증 시도를 기록하고 차단하는 방식이다. 사용자 인증에 관한 위협통찰력(Threat_Insight)은 네트워크의 공격 데이터를 사용하여 악의적인 로그인 시도를 식별하고 차단할 수 있게 된다.

2.2.2 상황적응형 제로트러스 2차 복합생체인증 분석

이러한 ZTNA(Zero Trust Network Access) 사례로 2018년 넷플릭스의 위치 독립적인 보안 액세스(Location Independent Security Access, LISA)이다. 상황 적응형 사용자 인증으로 복합 인자인증(Multi-Factor Authentication)의 특징 정보를 활용한 서비스 접근만 허용할 수 있다.

2.2.3 조도환경 기반의 복합영상 생체인식 설계사례

외부 환경에 노출된 환경에서 조도에 따른 스마트 단말을 활용한 홍채인식, 얼굴인식, 졸음운전 검출 등과 같은 복합 생체인식을 제안하고자 한다[7].



(그림 6) 사용자 조도환경에 따른 복합생체인증 설계
(Fig. 6) Multiple biometric design of lighting environment

[그림 6]은 자동차가 다양한 각도에서 조도여건을 반영한 복합 생체인식을 위한 설계 사례를 제시하고 있다.

외부에 수집되는 카메라 복합영상의 분석을 통해 조도환경을 보상함으로서 생체인식의 성능을 유지할 수 있도록 조도환경에 따른 복합 생체인식을 활용할 수 있다.

3. 암호 없는 2차 사용자 인증 FIDO 플랫폼

본 절에서는 사용자 2차 인증을 위한 상황 인지형 인증(Context-awareness Authentication)위한 FIDO 거래인증 플랫폼을 제안한다. 사용자의 상황 인지는 조도와 소음 등으로 주변 상황을 활용하여 사용자를 인증할 수 있다.

3.1 암호 없는 사용자 생체인증 FIDO플랫폼 연동

최근, 애플도 구글과 마이크로소프트처럼 FIDO와 월드와이드웹(World Wide Web Consortium) 컨소시엄의 암호 없는(Passwordless) 로그인 표준을 지원할 계획이다.

이러한 글로벌 기업의 활동은 인터넷 사용자가 암호 관리 및 레거시 2차 인증으로 정보보안이 개선된 환경에서 안전한 온라인 환경을 제공해야 한다[8].

이로서 FIDO 플랫폼에서 2차 인증은 사용자가 복합 생체인증 기반의 안전한 방식으로 웹사이트 및 앱에서 암호를 입력하지 않고도 로그인할 수 있게 되었다[8].

애플과 구글 및 MS 등 각 기업의 FIDO 플랫폼은 전 세계 수십 억 개의 주요 IoT기기와 스마트 디바이스에 암호 없는 로그인 방식을 구현하고 있다.

암호 없는 로그인 표준 개발자가 사용자의 암호 없는 기능을 확장하기 위해서는 사용자의 복합 생체인증 기반의 원활하고 안전한 다음과 같은 신규 기능이 필요하다.

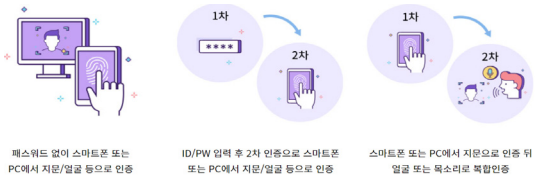
① 사용자가 모든 계정을 다시 등록할 필요 없이 다수의 스마트 기기와 새로 등록된 기기에서 'Pass_Key' FIDO 로그인 계정 자격 증명에 자동으로 접근 가능함.
② 사용자가 실행 중인 OS 플랫폼이나, 웹 브라우저에 무관하게, FIDO 인증을 보유한 스마트 모바일 디바이스 기반의 주변 기기와 연동한 로그인 가능해야 함.

글로벌 표준 기반의 암호 없는 로그인 방식으로 인터넷 서비스 제공업체가 대체 로그인과 계정 복구 등을 통한 암호 없이도 FIDO 자격 증명을 제공할 수 있다.

이때, 복합생체 인증을 암호화할 때 사용한 암호 키는 생성, 이용, 보관, 배포 및 파기 등에 따라 생체인증 정보를 관리해야 한다. 또한, 복합 생체정보에 대한 복합생체 인증정보는 즉시 파기되도록 해야 한다.

3.2 2차 사용자 복합생체인증 FIDO플랫폼 연동

제로트러스트 기반의 암호 없는 2차 사용자 인증을 위한 복합생체 인증기술은 ID/PW 입력 후, 2차 인증으로 스마트 단말용 FIDO 인증 지문 보안키 설계가 필요하다.



(그림 7) 암호 없는 2차 사용자인증용 복합생체 설계
(Fig. 7) Multi-biometric design for passwordless secondary user authentication[9]

(그림 8) 복합생체 기반의 사용자 인증용 FIDO 연동
(Fig. 8) FIDO linkage based on multiple biometrics for user authentication[9]

[그림 7]과 [그림 8]은 하나의 생체인증 장치가 PC로그인 부터 모든 인증이 가능한 FIDO 연동 복합생체의 인증용 플랫폼 설계를 제시하고 있다. 사용자의 2차 인증과 암호화는 MFA를 활용한다. MFA는 암호화 키 정보 등을 외부에서 접근할 수 없는 H/W 보안영역에 저장함으로서 강력한 인증 방식이 될 것이다[9].

4. 1:N 복합생체 기반 FIDO인증 설계/분석

본 절에서는 제로 트러스트 기반 2차 사용자를 인증한다. 이로서, 복합 생체인증과 FIDO 표준이 안전하게 인증하기 위한 복합 인증의 환경요소의 분석하고자 한다.

4.1 FIDO 사용자 2차 인증 분석과 평가방식 제안

MFA(복합인증)에 의한 FIDO 기반의 PC로그인(로컬, AD, VDI) 등의 인증용 평가영역을 분석한다[9][10].

4.1.1 FIDO 사용자 2차 복합 인증용 사용자 환경분석

복합생체 인증 기반의 FIDO 사용자의 2차 인증을 위한 사용자 평가에 대한 규격은 다음과 같다.

- 스마트폰 탑재형 생체인증장치(지문, 안면 등)인증
- 생체인증을 지원하지 않는 FIDO 인증 지원
- USB, NFC, 블루투스형 FIDO 외부인증장치(CTAP)
- 다양한 인증장치(스마트폰 생체인식, PIN, 모바일 OTP, 외부인증장치)의 통합관리 지원
- APP to APP 및 In-APP 형태의 모바일 환경 지원
- 마켓 등록 앱 / SDK / 독립앱 등 고객사 선택 가능한 다양한 방식으로 Android/iOS 클라이언트 제공
- PC연동 위해 Push, QR방식의 모바일 단말기와 연동
- Window Hello 연동 위한 PC 로그인 환경에 적용
- FIDO 표준 브라우저에서는 별도 모듈 없이, FIDO2 WebAuthn인증지원(Edge, Chrome, FireFox, Safari 등)
- 서비스 연동을 위해 RESTApi방식의 연동 규격지원
- 웹기반 관리 기능을 통해, 사용자 및 인증장치, 인증정책에 대한 일원화된 정책관리 기능을 지원
- 사용(등록 사용자, 등록 인증장치, 인증 내역)제공
- 정책(인증장치 허용/차단, 인증 서비스 메뉴별 허용 인증장치, 서비스별 그룹매핑의 인증정책)기능 제공
- 인사정보(계열사/조직) 연동을 위해 LDAP, RDB, Excel, AD를 통한 자동 동기화 지원
- 사용자 본인이 직접 서비스별 인증장치(FIDO, OTP) 등록 및 관리가 가능하도록 셀프서비스의 제안.
- 단말기 미소지 상황을 대응하기 위해 관리자의 승인 기반으로 하는 미소지자 워크플로우 기능 지.
- VPN 접속을 위한 2차 인증을 지원해야 하며, VPN 수정을 최소화하기 위해 RADIUS 프로토콜 지원
- SSO지원여부(ad 연동), VDI 환경 지원 가능(CTRIX)

* FIDO 표준인증 > Passwordless 인증(환경분석)
* 2차사용자인증, 1:1인증방식, 1:N복합인증방식
* 특수 목적 인증 웹 방식 인증
* 앱 방식 인증 스마트폰 지문, 얼굴, PIN, MOTP
* 앱 인증, PC 지문, 지문 보안키 분야 등

4.1.2 FIDO 사용자 2차 복합 인증용 시스템 규격분석

2차 사용자를 인증하고, 복합 생체인증과 FIDO 표준 기반의 복합 인증을 위한 시스템의 규격은 다음과 같다.

- 모바일 단말 환경 : Android 4.4이상, iOS 9.0 이상
- 서버 지원 환경 : Unix, Linux, Windows server 등 Java 실행환경 지원용 OS
- Java 환경 : JDK 1.8이상 또는 OpenJDK 11이상 지원
- DBMS 환경 : Oracle 11g 이상, MySQL 5.7 이상, MariaDB 10 이상

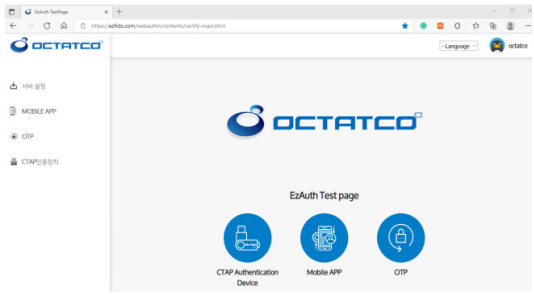
4.1.3 FIDO 2차 사용자용 생체인증 장치 규격분석

제로 트러스트 기반 2차 인증을 위한 복합 생체인증과 생체인증을 위한 개인 FIDO 장치 규격은 다음과 같다.

- 지문인식 카드형 FIDO2 및 NFC 지원 및 인증 획득
- Windows Hello 및 FIDO2 인증 획득 제품
- 전용 H/W 보안칩 Trustzone 내장 제품
- 지문인식 FRR(본인거부율) 1% 이하, FAR(타인인식률) 0.01% 충족제품
- 윈도우 10, 8, 8.1, 7 지원가능, WebauthN 지원제품

4.2 FIDO 인증평가 페이지 설계와 인증 결과분석

FIDO 표준 기반의 2차 사용자의 복합생체를의 인증평가를 실행하는 과정의 페이지 설계와 인증 결과를 분석한다(https://ezfido.com/webauthn/contents/certify-main.html).



(그림 9) FIDO 사용자 인증위한 검증화면 캡쳐 결과
(Fig. 9) Test screen for FIDO user authentication

4.2.1 FIDO 2차 사용자용 생체인증 장치 규격분석

FIDO의 복합생체 인증평가를 위한 페이지 설계에 따른 인증평가 결과를 확인하기 위한으로 분석으로 '인증방법'은 아래와 같은 절차로 진행해야 한다[9][10].

① EzAuth 테스트 페이지(옥타코의 사이트) 접속
② EzAuth App다운로드 (플레이스토어, 앱스토어)
③ EzAuth App 실행
④ PC에서 ezfido.com/webauthn 서버설정 메뉴의 QR을 EzAuth app으로 스캔(EzAuth FIDO 통합인증서버연동)
⑤ 스마트폰 지문인식, PIN, OTP 인증 테스트, PC USB FIDO 지문 보안키 인증 테스트

4.2.2 FIDO 2차 사용자용 생체인증 평가검증 분석

FIDO 생체인증은 각 개발사가 webauthn API를 적용 후, 스마트 폰의 지문인식, PIN, OTP를 인증평가 한다.

① 고객사의 로그인 페이지에서 webauthn API 사용 스마트폰 지문, PIN, OTP인증 테스트(옥타코 사이트)
② EzAuth.com에서 고객사 URL(도메인) 도메인 설정
③ EzAuth.com/webauthn에서 모바일, OTP 등록 후 고객사 로그인 페이지에서 로그인 실행 및 인증평가
④ 고객사 페이지에서 webauthn API인증 로그인 처리
(https://ezfido.com/webauthn/contents/certify-main.html)

(그림 10) FIDO복합인증 위한 사용자 검증용 화면분석
(Fig. 10) Test analysis for FIDO multiple authentication

[그림10]의 (1)~(4)는 사이트 접속후, 암호 없는 사용자가 2차인증을 위한 다양한 복합 생체요소를 활용한 FIDO 플랫폼의 평가과정과 검증내용 및 결과 분석이다.

4.2.3 FIDO 생체인증 윈도우 Demo 동작 결과 분석

FIDO 표준 기반의 2차 사용자를 인증하고, 복합생체용 인증평가인 실행 결과를 분석 한다.

① 사전준비 >지문인증 SDK(윈도우/리눅스 라이선스) 의한 윈도우 환경에서 Demo결과를 제시하고자 한다.
- EZF2+지문인식 보안키와 Windows Hello Driver 설치
=>[SW] EzFinger2+(이지핑거2플러스) 드라이버가 자동으로 설치되지 않을 때, 웹사이트 다운로드
- EZF2+ 지문인식기 장치를 PC USB 연결
② x64>Debug>FingerPrint.exe실행(관리자권한 실행)
③ Enrollment Touch 진행 후 Verify Touch 진행
(현재 Enroll Touch 횟수는 3회 고정, 변경 가능)
④ Verify 결과를 확인함(옥타코 사이트 통란 검증)

(그림 11) FIDO생체인증용 윈도우 환경에서 동작분석
(Fig. 11) Window operation analysis of FIDO biometrics

[그림11]은 FIDO 생체인증 기반의 지문인증용 SDK (윈도우/리눅스 라이선스)를 활용한 윈도우 환경에서 동작데모용 결과화면을 표현하고 있다[9].

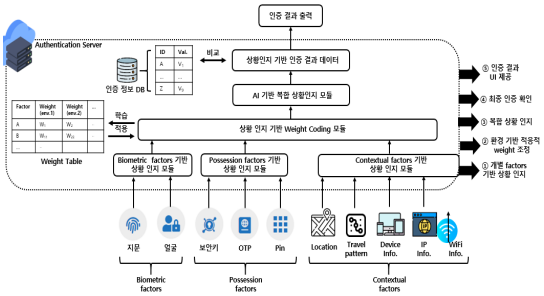
4.3 제로트러스트 기반의 2차 사용자 인증용 복합 생체인증용 상황인지 분석과 평가방식 설계

다양한 사용자 환경에서 제로트러스트 기반 복합 생체인증에 의한 2차 사용자의 보완성 강화하고자 한다[9].

(표 3) 복합 생체인증 수단에 의한 사용자 이용률 분석
(Table 3) Analysis of usage rate by multiple biometrics

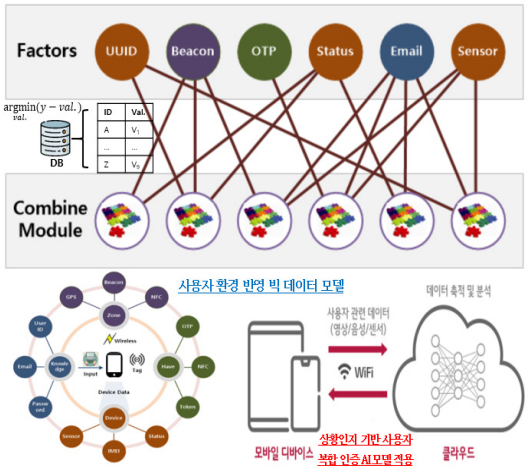
[표 3]은 복합생체 표준에 따른 인증수단 이용률의 결과분석으로 향후 복합인증을 위한 사용자 2차 인증 위한 아래 3가지 요소를 분석하였다[9].

① Customer Identity and Access Management(CIAM)
② Privileged Access Management(PAM)
③ Multi factor Authentication(MFA)



(그림 12) 상황인지 기반의 지능형 생체인증 구조설계
(Fig. 12) Structural diagram of situational wareness-based intelligent multiple biometric recognition

[그림 12]는 사용자의 상황인지에 따른 복합생체 인증의 가중치를 조정하는 지능형 복합생체인식 구조도이다.



(그림 13) 상황 인지 기반 모바일 AI 복합생체인증
(Fig. 13) Mobile AI authentication with context-aware multiple biometrics

[그림13]은 사무실 내 고정형 데스탑의 로그인, 모바일, 이동 중인가를 확인한다. 이때, AI모델의한 FIDO 연동 복합인증의 가중치 조정 방안을 제안하고 있다[11].

이를 위한 스마트 모바일 디바이스 기반의 인증수단의 활용한다. 스마트 폰에 내장된 다수의 센서 정보 기반의 사용자 2차 인식의 정확도를 기대할 수 있다[11][12].

사용자 환경에서 빅데이터 모델과 상황인지 복합인증 모델에 적합하다. 인증 기술의 정확도 분석도 필요하다. 이러한 '인증요소' 가중치의 조절로서 사용자 인식을 위한 사용자 2차 인증의 인식 정확도를 향상할 수 있다[13].

위치정보 기반 인증, 지자기 센서 기반 인증, 가속도 센서 기반 인증, 생체정보 인증, 다중 인증 => 센서정보 활용 : 조도, 온/습도 정보 등

5. 결과 고찰 및 결론

본 연구에서는 코로나19 이후 비대면 스마트 워크에서 원격 2차 사용자 인증을 위한 FIDO 복합인증 플랫폼 구축과 거래인증의 검증절차를 분석하였다[14][15].

특별히, FIDO 생체인증 기반의 지문인증용 SDK는 윈도우 환경에서 동작한다. 2차 사용자 인증을 위한 복합생체인증의 검증 결과로 FIDO플랫폼이 활용할 수 있다.

또한, 제안한 상황인지 기반의 제로트러스 사용자 2차 검증에 의한 복합 인증수단을 활용할 수 있다. 이로서,

사용자의 환경에 따른 적응형 AI 복합인증에 의한 FIDO 거래인증 플랫폼의 활용이 가능하게 될 것이다.

또한, 이러한 지능형 위험관리를 위한 기존 취약한 패스워드 시스템은 업무 시간을 감소할 수 있고, 최고의 레벨 보안인증의 서비스가 가능할 것이다.

참고문헌(Reference)

[1] https://www.lgcns.com/blog/cns-tech/31809/?fbclid=IwAR1HjLYnWBhqHdjFq-ai9tG2kmmzjEkKA7hYgmTDMWCKkzH0Fg0Ylx4Jn-w

[2] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRIEi?culture

[3] https://www.lgcns.com/blog/cns-tech/security/31873/?fbclid=IwAR0lbVinAol7pkjT8ofarYfxlzItriOUNH4GIlV7aTF4AtUr4TO6TjipQig

[4] https://www.lgcns.com/blog/cns-tech/31963/?fbclid=IwAR3dJW0L_5Egw8P_5NNWOuwZXMnrhyCeumO5630KrbfeMLmun-oxpbb22UA

[5] https://ssl.pstatic.net/imgstock/upload/research/industry/1627526012944.pdf(2021.07.29.)

[6] https://www.okta.com/security-features/

[7] J.Y.,Lee et al, “biometric processing method using light environment compensation by multi-video analysis of multiple camera videos,” Korea patent #102090332(2020.03.11)

[8] https://www.apple.com/kr/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/

[9] https://octatco.com/

[10] Mingoo, Kang et al, “Application of One ID Certification and FIDO2.0 with Transaction Certification,” Korea Society for Internet and Information, Vol. 20 No. 1, 2019.06.30. https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=JAKO201926072515149

[11] Pil-seong Jeong, Yang-hyun Cho, “User Authentication System based on Auto Identification and Data Collection,”Journal of the Korea Institute of Information and Communication Engineering Vol. 22, No. 1, pp 75~82, Jan. 2018. https://doi.org/10.6109/jkiice.2018.22.1.75

[12] Yook, Moses et al, “User Recognition of Each Personal Identification Technique based on the Biometrics,” The Journal of the Korea Contents Association, Vol. 16, Issue 11, pp. 11-19, Nov. 2016. http://dx.doi.org/10.5392/JKCA.2016.16.11.011

[13] Byungchul Cho, et al “Technology Review on Multimodal Biometric Authentication,” The Journal of Korean Institute of Communications and Information Sciences, Vol. 40 No. 1, Jan. 2015. http://dx.doi.org/10.7840/kics.2015.40.1.132

[14] Cheol-Joo Chae1 et al, “Authentication Method using Multiple Biometric Information in FIDO Environment,” Journal of digital convergence, vol. 16, no. 1, Jan. 2018. http://dx.doi.org/10.14400/JDC.2018.16.1.159

[15] Kyungho Hong et al, “Hand Biometric Information Recognition System of Mobile Phone Image for Mobile Security,” Journal of digital convergence, vol. 12, no. 4, Apr. 2014. http://dx.doi.org/10.14400/JDC.2014.12.4.319

◐ 저 자 소 개 ◑

강 민 구

1986년 연세대학교 전자공학과(공학사)
1989년 연세대학교 전자공학과(공학석사)
1994년 연세대학교 전자공학과(공학박사)
1985～1987년 삼성전자 통신연구소 연구원
1997～1998년 오사카대학교 Post Doc.
2007～2008년 Queens Univ. Visiting Scholar
2000～현재 한신대학교 IT영상콘텐츠학 교수