Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.879

컴플라이언스 기반의 발전된 모바일 기기 생체 인증 모델*

정 용 헌,† 이 경 호‡
고려대학교 정보보호대학원

Advanced Mobile Devices Biometric Authentication Model Based on Compliance*

Yong-hun Jung,† Kyung-ho Lee‡
Graduate School for Information Security, Korea University

요 약

최근 국내외 핀테크의 발전과 더불어 모바일 결제 시장에서 생체 인식 기술을 이용한 FIDO(Fast IDentity Online)가 기존의 패스워드 방식을 대체하며 빠르게 성장하고 있다. 이러한 FIDO 인증은 민감한 생체정보를 처리해야 하므로 반드시 높은 보안성이 요구되는 신뢰할 수 있는 환경에서 처리가 이루어져야 한다. 그러나 이러한 신뢰할 수 있는 환경은 스마트폰의 특정 하드웨어에서 지원하므로 제조사에 의존적일 수밖에 없다. 이에 본 논문에서는 모바일 환경에서 특정 하드웨어가 탑재되지 않아도 보편적으로 안전하게 사용할 수 있는 컴플라이언스 기반의 생체정보의 분산 관리를 이용한 서버 기반의 인증 모델을 제안하고자 한다.

ABSTRACT

Along with the recent worldwide development of fintech, FIDO (Fast IDentity Online) using biometric technology is rapidly growing in the mobile payment market, replacing the existing password system. This FIDO authentication must be processed in a reliable environment that requires high level of security, as sensitive biometrics is being processed. However, this environment is currently dependent on the manufacturer as it is supported by certain hardware on the smartphone. Therefore, this thesis proposes a server-based authentication model using distributed management of compliance based biometric information that can be used universally safely without the need for specific hardware in mobile environments.

Keywords: Fin-tech, FIDO, Biometric authentication, Trusted environment, Distributed management

I. 서 론

미국 시장조사업체 트랙티카에 따르면 생체인식 시장은 2015년 20억 달러(약 2조 2,240억원)에서 25.3%의 연평균 성장률을 보이며 2024년 149억 달러(약 16조 5,680억원)까지 성장할 것이라고 전망했으며, 이 중 모바일 생체인증 기술은 2020년까지 48억대의 스마트 디바이스에 적용 될 것으로 전망했다[29]. 생체인증에 대한 관심이 높아지며 자연스럽게 표준화에 대한 요구가 발생했고, 이러한 관심과 요구가 모아져 인터넷 환경에서도 생체인식 기술을 활용해 안전하게 인증할 수 있는 국제 인증 기술 표준 FIDO 가 생겨났다. FIDO는 기존의 인증 방식과 비교하여 ID와 패스워드를 암기하거나 타이핑

Received(07. 03. 2018), Modified(07. 23. 2018), Accepted(07. 23. 2018)
* 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다 (UD060048AD).
† 주저자, dearyu@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

하는 불편함의 감소와 OTP, 공인인증서 사용을 위한 별도의 인증토큰을 소유하지 않아도 된다는 점에서 편리성이 높고, 사용자의 고유한 신체 정보가 사용되기 때문에 복제가 어렵다는 점에서 높은 보안성의 특징이 있다[2]. 이러한 FIDO의 핵심 기술로 등장한 것이 민감한 데이터를 저장, 처리, 보호하는 기술이 TEE(Trusted Execution Environment) 기술이다. 이 기술은 모바일 기기에 저장된 민감한 개인 정보(바이오 정보, 메시지, 금융 데이터 등)를 불법 유출 목적의 피싱(Phising), 파밍(Pharming), 스미싱(Smishing)을 유발하는 악성코드와 지능화된 해킹 등 다양한 보안 위협으로부터 안전하게 보호해 주는 역할을 한다[7]. 그러나 이러한 TEE 기술은 매우 뛰어난 보안성을 제공하긴 하나, 스마트폰에서 해당 기능을 제공해줘야 하기 때문에 제조사에 매우 의존적이다.

따라서, 본 연구에서는 TEE와 같은 보안 영역을 제공하지 않는 모바일 환경에서도 생체정보의 분산관리를 이용해 서버 기반으로 안전하게 인증을 수행하는 시스템을 설계하고자 한다. 본 연구의 논리적 구성을 위해 2장은 관련 연구로 사용자 정보를 기존의 모바일 저장 방식 및 FIDO를 분석하고, 3장은 FIDO의 보안 영역으로 권장하는 TEE 기술 및 도입 한계에 대해서 제시할 것이고, 4장은 기존 FIDO 방식과의 비교를 통해 새로운 모델을 제시할 것이고, 5장은 바이오 인식의 국제 표준을 토대로 제안 모델에 대한 보안성 평가를 하고, 마지막으로 6장은 내용 정리 및 향후 연구를 제시하고 이 글을 마치도록 한다.

II. 관련 연구

2.1 모바일 정보 저장방식의 종류 및 특징

모바일 정보 저장방식에 따라 보안성, 사용편의성, 비용, 성능 등의 차이가 있다. 현재까지 이러한 모바일 환경에서의 정보 저장방식으로 보편화 된 방법이 SE (Secure Element)와 TPM (Trusted Platofrm Module)과 TEE이다[1][8]. 이번 장에서는 기존 사용하고 있는 모바일 정보 저장방식에 대해서 설명하고 장단점에 대해서 분석하고자 한다.

2.1.1 SE 정보 저장방식

최근 스마트폰에서 가장 널리 사용하는 방식으로 일반 스마트카드와 동일한 기능을 가진 칩이다. 이 칩은 암호화 기능이 있는 애플리케이션의 안전한 실행 및 저장을 담당하는 전용 부품이다. 이러한 SE는 세 가지(Embedded SE, UICC SE 및 Micro SD SE)로 분류된다[1]. 그러나 새로운 애플리케이션을 SE에 저장하려면 SE 발급자와 협의해야 하는 번거로움이 있고, 무엇보다 저장 용량 및 처리가 제한적이라 대규모 배포에는 부적합하다[1].

2.1.2 TPM 정보 저장방식

원래 데스크톱 환경을 위해 설계된 신뢰할 수 있는 플랫폼 모듈이다. TPM은 대칭키 암호화에서 RSA 비대칭키 암호화에 이르기까지 매우 복잡한 암호화 연산을 수행할 수 있는 안전한 마이크로 컨트롤러이다 있다[16]. 그러나 저장 용량이 매우 제한적이라 암호화 작업만 수행하고, 이를 제외한 애플리케이션에서의 모든 조작은 SE에서 수행한다[1].

2.1.3 TEE 정보 저장방식

TEE는 SE의 호환성 부족과 성능 문제를 개선하기 위해 나온 방식이다[1]. 신뢰할 수 있는 격리 환경을 통해 응용프로그램의 무결성 및 기밀성을 제공하는 기술이다[3][6]. 대표적인 기술로는 ARM 사의 TrustZone과 Intel SGX 가 있다[6]. 이들은 각각의 보안 영역 하드웨어를 이용해 일반 OS와 분리된 안전한 환경을 제공한다. Fig 1.은 TEE 아키텍처에 대한 개념도이다.

그러나 TEE 기술은 아직 본격적으로 개화하지 않은 사업으로 국내에서 적용한 대표적인 사례로는 삼성 페이, 삼성 KNOX, 페이팔의 지문 인식 결제

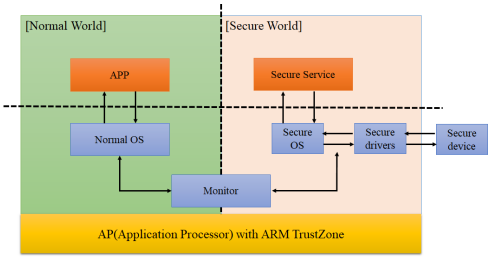

Fig. 1. TEE Architecture

등만 있어 상용화까지는 많은 시간이 필요하다.

2.2 FIDO 기반 인증 기술

FIDO는 2012년 7월에 설립된 글로벌 생체인증 기술 표준 연합회인 FIDO Alliance가 만든 온라인 환경에서의 생체인증 방식의 기술 표준이다. 2014년에 FIDO 1.0 표준이 발표되었고, 2015년에 FIDO 2.0 표준이 발표되었다. FIDO는 크게 UAF (Universal Authentication Framework), U2F (Universal 2nd Factor)로 구분한다. UAF는 온라인 서비스에서 사용하던 패스워드 인증을 사용자의 모바일 인증으로 대신하는 방식이고, U2F는 기존 패스워드 기반 인증과 추가로 USB 등의 별도 기기를 인증하는 방식이다. 핀테크 확산과 더불어 공인인증서 의무 사용이 폐지되며 차세대 인증 방법으로 FIDO 기반 바이오 인증이 부각되었다. FIDO가 각광받는 것은 생체인증 정보를 서버가 아닌 개인이 소유한 기기에서 인증하기 때문이다. 그러나 TEE와 같은 보안영역을 지원하지 않는 모바일 기기의 경우, 정보 유출의 위협이 발생한다. 이에 본 논문에서 제시하는 모델은 개인 기기가 아닌 별도 바이오 서버에서 보안영역에서 수행한 일부 업무를 신속하고 안전하게 수행하고자 한다.

III. FIDO와 TEE

3.1 FIDO와 TEE의 협업 강화

FIDO Alliance와 TEE보안 글로벌 표준 제정을 담당하고 있는 Global Platform은 공식적으로 협업을 강화하고 있으며, FIDO에서 TEE 보안 적용/연계는 의무사항으로 제정하였다. 또한 FIDO Alliance에서 2014년 12월에 발표한 "FIDO UAF Authenticator Commands v1.0"을 내용에서도, Security Guidelines에서 암호화 커널(알고리즘) 및 Matcher, 바이오 정보를 보안 영역(TEE)에서 저장 및 이용할 것을 권장하고 있다[11].

3.2 정보 저장방식 비교를 통한 TEE의 우위

이 장에서는 2장에서 분석한 정보 저장방식인 SE, TPM 및 TEE 간의 주요 차이점에 대해 분석하고자 한다. Table 1.은 안전한 정보 저장에 필요한 각 요소들을 비교한 내용이다.

Table 1. Comparison between the hardware solutions[1]

Criteria	SE	TPM	TEE
Tamper resistance	√	√	
Secure input and display			√
High computation power		√	√
High storage capacity			√
Dependency to manufacturer	√	√	√
Proven security level	√	√	√

SE와 TPM에는 TEE보다 많은 물리적 보안 기능을 갖고 있어 탬퍼링 방지 기술 등을 지원하나, TEE는 안전한 보안 통신 채널을 통해, 대용량의 저장 공간을 기반으로 보다 크고 복잡한 연산을 처리할 능력을 제공 한다. 따라서 FIDO 인증과 같이 높은 보안성과 복잡한 분석 연산이 필요한 프로세스에서는 저장방식으로 TEE가 적합하다.

3.3 FIDO에서 TEE 도입 시 한계

TEE 기술이 FIDO에서의 핵심 기술임에도 불구하고 다음의 이유로 인해 보편화하기에는 분명 한계가 있다. 첫째, TEE 기술은 단말기 제조사에 의존적이고 지원 단말기가 제한적이다. 삼성의 경우 보안 소프트웨어 KNOX가 지원하는 갤럭시 S6 이후 모델, 애플의 경우 보안 영역인 보안 엔클레이브가 장착되어 있는 아이폰 6 이후 모델부터 해당 기술이 적용된다. 즉, TEE를 지원하는 단말기 제조사에서 최근 3년 이내에 출시된 최신 모바일 기기만이 해당 기술을 사용할 수 있어 범용적이진 않다. 둘째, TEE 기술은 단순히 하나의 업체가 보안 서비스를 제공하는 게 아니라, 여러 보안 서비스가 TEE와 연동되는 구조이다. 따라서 아직은 각 분야별 글로벌 보안 업체가 얼라이언스를 구축하는 단계로 이들 업체의 참여 여부에 따라, 성장의 폭이 결정되는 한계가 있다.

IV. 데이터 분산 저장 및 서버 인증 기반 모델

본 장에서는 3장에서 FIDO에서 TEE 도입의 한계로 언급한 TEE를 지원하지 않는 단말기에 대해서

도 안전한 인증 환경을 제공하기 위해, 생체정보의 분산 관리와 서버 기반의 안전한 인증 방식을 통해 FIDO 인증에서 보안성을 높이는 새로운 모델을 제시하려 한다.

4.1 FIDO와 비교한 시스템 구성도

기존 FIDO 시스템 구성과 제안 모델의 시스템 구성의 차이점에 대해 살펴보도록 한다.

Table 2. Difference between old and new model

Division	Old Model	New Model	Improved
Biometric Save and Process	Mobile (TEE)	Bio Server	Universal
Biometric Save unit	Mobile (Whole)	Mobile(Half), Bio Server(Half)	Security

4.1.1 FIDO - 보안영역(TEE) 기반 시스템 구성도

Fig 2.는 보안 영역이 있는(TEE) 클라이언트 측 구성도이다. TEE 환경은 FIDO Alliance의 Security Guidelines에서 보안영역 이용을 권장하는 인증키의 생성 및 관리, 전자서명 및 암호 연산, Matcher 등의 중요한 역할을 하는 인증기(Authenticator)가 보안 영역에서 동작한다[7]. 만약 인증기가 일반영역에 노출되어 있다면 악성코드 및 해킹에 의한 데이터 위·변조는 물론, 중요한 정보 유출로 인해 막대한 피해를 입을 것이다.

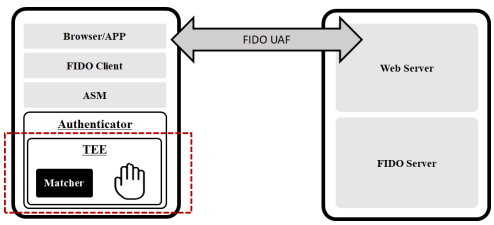

Fig. 2. [Old] TEE Configure

4.1.2 제안 모델의 시스템 구성도

제안 모델은 FIDO의 기본적인 프로세스는 동일하게 진행하되 인증기에서 하는 역할 중 암호화 커널(알고리즘) 및 Matcher, 바이오 정보 관리를 별도

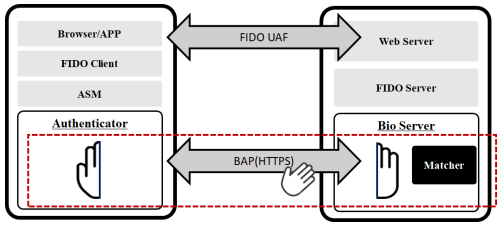

Fig. 3. [New] Proposed Configure

의 바이오 서버에서 수행한다. 여기에 데이터 유출 방지를 위해 제안하는 데이터의 분할 관리 및 저장 역할도 별도 바이오 서버에서 수행한다.

4.2 제안 모델의 주요 프로세스

본 연구에서 제시하는 모델의 주요 프로세스는 Fig 5.와 같다. 크게 등록, 인증, 조회, 삭제 총 4단계의 프로세스로 진행되는데, 등록, 인증 프로세스에 대해서는 주요한 동작이므로 개괄적으로 설명하고, 조회, 탈퇴 프로세스는 간략히 설명하려 한다. Table 3.은 제안 모델의 암호 계수 및 기호를 설명한다.

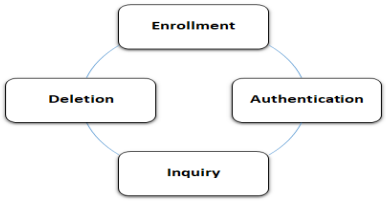

Fig. 4. Proposal Main Process

Table 3. Factors and terms used in the new model

Coefficients	Contents
(n,e)	Public key (RSA)
d	Private key (RSA)
k	Ramdomized symmetric key
p	Extraction Vector value of Biometric
h( )	Hash function
C	Cipher text
E	Encryption
D	Decryption
A+B	Split Encrypted template
S	Electronic Signature
′	Coefficients for Authentication

4.2.1 등록 프로세스

등록 프로세스는 FIDO에서의 등록 프로세스를 부분적으로 따른다. 먼저, 사용자가 응용 앱에서 인증수단을 패스워드에서 생체 인증으로 변경 요청한다[5][9]. 다음으로 모바일 폰이 응용 앱에 로그인(기존 ID/ PW)을 하면 클라이언트는 인증 방식(지문, 정맥 등)을 선택하고, 응용 앱은 FIDO 서버에 등록 요청 메시지를 요청한다[5][9]. FIDO 서버는 인증 정책이 포함된 등록 요청 메시지를 클라이언트인 모바일 폰으로 전달한다[5][9]. 이후 인증기에서 수행해야 되는 사용자 등록 작업을 바이오 인증서버에서 대신 수행한다. 상세한 등록 프로세스 수순은 Fig. 5와 같다. 먼저, 바이오 인증서버에서 생성한 공개키를 전송받고, 랜덤한 대칭키(등록용)를 생성한다. 대칭키를 통해, 생체정보 템플릿을 암호화하고, 식별정보로 사용할 ID도 암호화한다. 그리고 암호화 한 생체정보 템플릿을 해시 함수를 생성하고, 대칭키 또한 공개키로 암호화해, 이 값들을 바이오 인증 서버로 전송한다. 바이오 서버는 먼저 개인키로 대칭키를 복호화 하고, 복호화 한 대칭키로 암호화된 생체정보 템플릿을 해시함수를 적용해서, 전송된 값과 비교하여 무결성을 검증한다. 검증에 이상이 없다면, 암호화된 생체 인식 템플릿을 두 부분으로 나눈다. 또한 대칭키로 식별 정보인 ID를 복호화 한다. 마지막으로 서버는 ID, 암호화된 대칭키, 개인키 그리고 생체 인식 템플릿 일부를 데이터베이스에 저장하고, 나머지 일부 생체 인식 템플릿을 모바일 폰으로 전송 및 저장함으로써 사용자 등록을 종료한다. 그 이후 프로세스는 FIDO와 동일하다.

4.2.2 인증 프로세스

인증 프로세스도 FIDO의 인증 프로세스를 부분적으로 따른다. 상세한 인증 프로세스 수순은 Fig. 6과 같다. 먼저, 응용 앱은 사용자 인증을 위해서 FIDO 서버에 인증 요청 메시지를 요청하고, FIDO 서버는 인증 요청 메시지를 클라이언트인 모바일 폰으로 전달한다[5][9]. 일반적인 FIDO authenticator에서는 생체 템플릿과 알고리즘이 authenticator 내부에 TEE 영역에 저장되어 있기 때문에 내부에서 바이오 인증이 수행되지만, 본 모델에서는 바이오 인증을 위해서 모바일에 저장되어 있

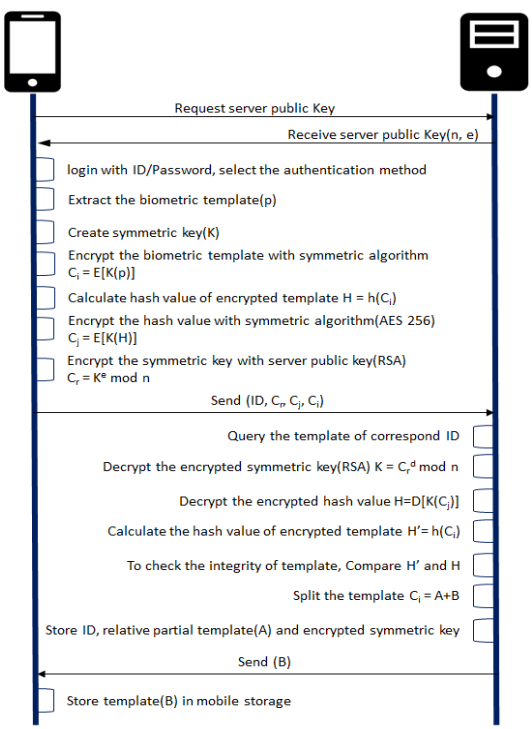

Fig. 5. Enrollment Process

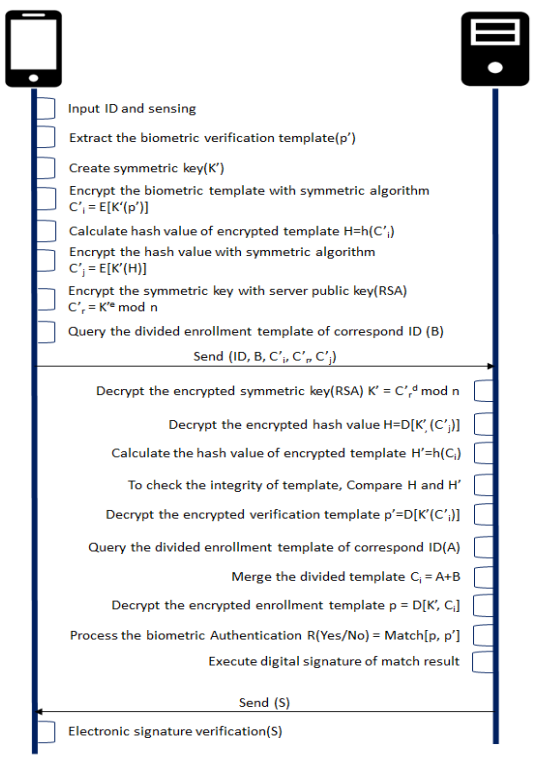

Fig. 6. Authentication Process

는 템플릿 반쪽과 센서로 획득된 인증 템플릿을 서버로 전송한다. 바이오 서버가 수신된 템플릿으로 인증을 수행하고 그 결과를 인증을 요청한 FIDO authenticator에 다시 전송한다. 보다 자세한 내용은 다음과 같다. FIDO authenticator에서는 전송 데이터의 보호를 위한 암호화와 무결성 검증을 위한 해시값 등 다양한 정보를 서버로 전송한다. 먼저 클라이언트에서는 획득된 템플릿의 무결성과 보호를 위해서 등록 프로세스와 동일하게 모바일에서 대칭키를 생성하고 이 키를 이용하여 암호화(AES-256)를 수행한다. 암호화된 인증 템플릿은 위변조를 검증하기 위해서 해시값을 추출한다(SHA- 256). 서버에서는 ID, 암호화된 등록 템플릿, 암호화된 등록 템플릿의 해시값, 분할된 저장 템플릿과 RSA로 암호화된 대칭키를 수신한다. 바이오 서버에서는 단계별로 인증 템플릿 검증, 등록 템플릿 병합, 바이오 인증, 인증 결과 전송의 네 단계를 거치게 된다. 첫째 인증 템플릿 검증 단계는 템플릿을 복호화 하여 해시 검증을 통해서 전송구간 사이에 위·변조를 검증한다. 이와 더불어 기존 인증 템플릿의 해시값을 비교하여 중복성을 체크를 통해서 인증 템플릿 재사용 공격을 감지한다. 두 번째, 등록 템플릿 병합 과정에서는 수신된 템플릿 조각과 서버의 ID에 해당하는 나머지 조각을 병합하고, 병합된 템플릿의 해시값을 검증하여 무결성을 확인한다. 세 번째, 복호화 된 인증 템플릿과 무결성 검증이 완료된 등록 템플릿을 이용하여 바이오 인증을 수행한다. 네 번째, 인증 결과는 바이오 서버에서 전자서명하고 그 결과를 모바일 authenticator에 전송한다. 모바일에서는 미리 수신되어 저장하고 있는 서버의 공개키를 이용하여 전자서명 값을 검증하고 그 결과를 authenticator를 호출한 앱에 전달하여 제안 모델의 사용자 인증을 완료한다.

4.2.3 조회 프로세스

사용자는 자신의 정보가 모바일 인증 서버에 정상적으로 등록되어 있는지 조회할 필요가 있다. 사용자 등록 정보는 등록 시 사용한 식별 정보(ID)를 통해 데이터베이스 검색을 통해 확인한다.

4.2.4 삭제 프로세스

사용자 삭제는 등록 시 사용한 식별 정보(ID)를 조회 후, 이와 연계된 정보 모두를 모바일 서버 데이터베이스에서 삭제한다. 또한 모바일 폰에서도 저장하고 있는 분할 생체 인식 템플릿 일부를 삭제한다.

V. 제안 모델의 보안성 평가

본 장에서는 3장에서 제시한 제안 모델의 설계가 적정한지에 대한 보안성 검증을 위해 바이오 인식 기술(Biometrics) 관련 국제 표준인 ISO/IEC JTC1 SC 37에서 규정하고 있는 모바일 바이오 인식 표준화 프레임워크의 요구 사항에 충족하는지에 대한 객관적인 보안성 평가를 해당 표준을 기반으로 작성한 국내 표준인 TTA에서 제시한 '생체정보보호를 위한 가이드라인(TTAS.KO-12.0034)'과 최근에 한국인터넷진흥원과 방송통신위원회에서 제시한 "바이오정보 보호 가이드라인"을 토대로 보안성 평가를 하고자 한다.

5.1 '생제정보보호를 위한 가이드라인'에 준한 평가

모바일 생체인식시스템의 표준화 프레임워크에서 각 처리 단계에서 불법접인 외부 공격의 원인으로 인해 취약성이 노출되는 부분을 도식화하면 Fig 7.과 같고[14], 단계별 관련된 국제 표준 규격(ISO/IEC) 내용은 Table 4와 같다.

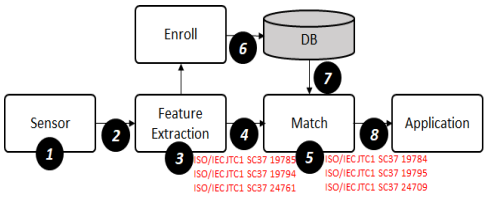

Fig. 7. Vulnerability of biometric system[14][18]

Table 4. Related Standards and contents [18]

ISO/IEC JTC1 SG37	Contents
19785	Common Biometric Exchange Formats
19794	Biometric data interchange formats
24761	Authentication context for biometrics
19784	Application programming interface
19795	Biometric performance testing, reporting
24709	Conformance testing

Fig 7.은 생체인식시스템에서 발생 가능한 각 부분별 취약성을 단계별(①~⑧)로 구분을 했다. 제안 모델에서 단계 ①, ②의 경우, 모바일 폰 자체(제조사)에서 안전하게 보안 기능을 제공한다. 또한 단계 ⑦의 경우는 안전한 바이오 인증 서버 내에서 이루어지는 동작이다. 이러한 3 단계를 제외한 각 단계에서 제안 모델의 보안조치는 Table 5.와 같다.

Table 5. Security evaluation for each stage

	Guide Line	Applied Method	OK
③	-Biometric template encryption required -Monitoring function using system log when performing 1: N search	-Encryption with ra- ndom symmetric key -Log generation and monitoring when perfor- ming search in bio server	O
④	-Extracted biometric template encryption required. Integrity verification through one-way function -The transmission key can be encrypted using a different key each time, or encry- pted using PKI -Validation of transmi- tted data by using hash function	-Application of hash function for biometric template encryption and integrity verifi- cation extracted by symmetric key -The symmetric key to encrypt is generat- ed as a random value Distribution through symmetric key encry- ption with PKI -Ensure the integrity of transmitted data by applying a hash function	O
⑤	-Validation of biom- tric templates requir -ed -Detecting and valida- ting imitation data	-Ensure the integrity of the hash function template -Ensure redundancy and integrity with hash function	O
⑥	-Applying a safe pro- cess for updating bio- metric information. Deletion of existing data	-Biometric informati- on is divided and st- ored in server and mobile phone respec- tively. -DBMS complete delete function	O
⑧	-transmitted through encryption of authenti- cated result values - Authentication result is expressed as Yes / No instead of Score	-Secure VPN or SSL transmission after en- cryption -Reply Yes / No to the authentication result	O

5.2 "바이오정보 보호 가이드 라인"에 준한 평가

생체인식시스템은 바이오정보의 불법 유출, 위·변조 등을 방지하기 위한 기술적·관리적 보호조치를 취해야 한다. Fig 8.의 처리 단계별 개인 정보 침해 위험 요인을 파악하고, 각 단계별 필요한 보호조치를 취하여야 한다. 이와 관련 보안조치는 Table 6.과 같다

해당 제안 모델의 보안 조치는 국제 표준을 기반으로 제시한 정부의 가이드 라인을 충실히 충족하는 다양한 보안 기술들을 적용하고 있다.

Table 6. Security evaluation for each stage

	Guide Line	Applied Method	OK
①	-Measures against collecting and inpu- tting biometrics in- formation -Protect transmission line when collecting and inputting biomet- rics information	-Encryption and hash function redundancy check and integrity guaranteed with sy- mmetric key - A symmetric key that provides Secure Sockets Layer (SSL) and Secure Sockets Layer (VPN)	O
②	-Biometrics infor- mation encryption measures -Safe storage and processing of biome- trics information	-Encryption Set enc- ryption secret key (symmetric key) to PKI Hybrid encryp- tion algorithm -Save security server and security information	O
③	-After creating te- mplate of original information, compl- etely destruction -Keep original infor- mation by legal bas- is / user consent, se- parate from other information	Deletion function in DBMS -Save and manage inf- ormation separately fr- om DBMS	O

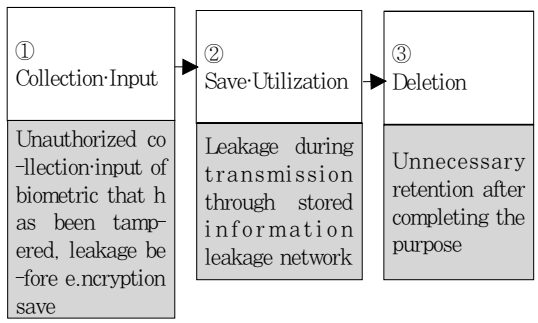

Fig. 8. Risk Factors of Biometric at Each stage[15]

5.3 기존 연구와의 비교 분석

FIDO에서 TEE와 연계된 연구들은 현재까지 많이 진행되어 왔다. 이 장에서는 TEE 관련 다양한 연구들과 본 연구와의 차이점에 대해 살펴보려고 한다.

전정훈 님은 유출된 생체정보의 도용 문제에 대한 대응 모델을 제시했고, 본 논문에서도 유출된 생체정보의 도용 대응을 위해, 랜덤으로 생성되는 대칭키 및 해시 함수를 통해 대응했다. 또한, H.Nishimura 님은 TEE를 통해 기기 간의 키 공유에 보안을 강화했다면, 본 논문은 TEE가 없는 환경에서의 암호화된 프로토콜 및 키 분배로 보안을 강화했다. Prathame- sh Raut 님은 TEE에서 안전하게 지문인식을 이용해 사용자 등록하는 연구를 했다면, 본 논문은 TEE가 없는 환경에서 다양한 바이오 인식을 이용해 안전하게 사용자 등록하는 방식을 제안했다. 끝으로 GeonLyang Kim 님은 TEE 기반의 가상화 기술을 통해 소프트웨어로 TEE와 유사한 환경을 제공한다면 본 논문은 별도 모바일 서버를 통해 하드웨어 및 독자적인 암호화 프로토콜 방식으로 TEE와 유사한 환경을 제시한다.

Table 7. Comparative analysis with existing research

Title	Author	Point
A Study on Security Risk according to the activation of Bio Authentication Technology[20]	Jeon Jeong Hoon	Proposal of Best model against leakage of biom etric
Secure authentication key sharing between mobile devices based on owner identity[30]	H. Nishim ura	Using TEE, key sharing between devices via 3rd authentication system
Device Fingerprinting for Secure User Enrollment using TEE[2]	Pratha mesh Raut	Secure user enrollment through fingerprint recognition at TEE
Secure user authentication based on the trusted platform for mobile devices[7]	Geon Lyang Kim	Proposal of TEE -based virtual platform TMZ systems

VI. 결 론

시장조사업체 TNS, KT 경제경영연구소에 따르면 2017년 3월 기준으로 국내 스마트폰 보급률은 91%에 이른다고 한다. 이와 같이 급격히 증가하는 스마트폰 이용자 수에 따라, 모바일 보안 위협 또한 급격히 증가하고 있다[2]. 이에 삼성은 작년 7월 ARM 사의 TrustZone을 이용한 보안장치 녹스(Knox)를 개발해 안전한 저장 영역을 제공하고 있다. 그러나 해당 제조사에 국한된 장치로 누구나 이용할 수 있는 기술은 아니다. 삼성뿐만 아니라 TEE를 지원하는 모든 업체들은 하드웨어 종속적일 수밖에 없다. 이에, 본 연구에서는 TEE가 없는 모바일 환경에서도 생체정보의 분산 저장을 통해 컴플라이언스 기반의 안전한 서버 기반 인증 시스템을 설계했다. 향후 연구에서는 실제 다양한 외부 보안 공격에 대해 제안 모델이 얼마만큼 효용성이 있는지에 대해 연구해 보고자 한다. 본 연구에서 제시된 방법이 실 서비스에 적용되어 비대면 전자거래에서 바이오 인증 이용 환경이 더 안전하고 보편화되길 기대해 본다.

References

[1] Bouazzouni Mohamed Amine, Peyrard Fabrice ,Conchon Emmanuel, "Trusted mobile computing: An overview of existing solutions," *FUTURE GENERATION COMPUTER SYSTEMS THE INTERNATIONAL JOURNAL OF ESCIENCE*, 80, pp. 596-612, Mar. 2018.

[2] Prathamesh Raut and Bhushan Patil, "Device Fingerprinting for Secure User Enrollment using TEE," *International Journal of Science and Research*, vol. 6, no. 3, pp. 1410-1412, Mar. 2017.

[3] Hang Jiang1, Rui Chang, Lu Ren1, Weiyu Dong, Liehui Jiang, and Shuiqiao Yang, "An Effective Authentication for Client Application Using ARM TrustZone," Information Security Practice and Experience - 13th International Conference, LNCS 10701, pp.

802-813, 2017.
〔4〕 Cui Jinhua, Cai, Zhiping, Zhang Yuanyuan, Liu Anfeng, and Li Yangyang, "Securing Display Path for Security-Sensitive Applications on Mobile Devices," Computers, Materials & Con -ua, vol. 55, no. 1, pp. 17-35, Apr. 2018.
〔5〕 Hwa-Gun Cho and Hae-Sool Yang, "A Methodology for the Improvement of Accredited Digital Certificate Integrating FIDO Biometric Technology and TrustZone," Journal of Digital Convergence, 15(8), pp. 183-193, Aug. 2017.
〔6〕 Sanggi Jeon, Changjun Choi, and Jong-Hyouk Lee ,"A Survey of Components and Application Technologies of the Trusted Execution Environment," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 65-66, Nov. 2017.
〔7〕 Kim GeonLyang, Lim JaeDeok, and Kim JeongNyeo ,"Secure user authentication based on the trusted platform for mobile devices," EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, 15p, Sep. 2016.
〔8〕 Jong-Moon Yoon, "A Status and prospect of mobile payment technology," KISDI Research Report, 27(22), pp. 24-40, Dec. 2015.
〔9〕 Su-Hyeong Kim, "FIDO standard technology trend," TTA Journal, pp. 70-75, Mar. 2016.
〔10〕 Lee Donghun, "A first course in Modern Cryptography," Korea University, pp. 283-286, 345-349, Feb. 2012.
〔11〕 FIDO alliance, "FIDO UAF Authenticator Commands v1.0," https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-authnr-cmds-v1.0-ps-20141208.html, Jun. 2018.
〔12〕 Jong-Seon Park and Byeong-Hwa Han, "Next Generation Certified FIDO and Biometrics," Eugemef Journal, Oct. 2016.
〔13〕 FIDO alliance, "A Guideline for Telebiometric Protection," Telecommunications Technology Association, Dec. 2005.
〔14〕 Telecommunications Technology Association, "A Guideline for Telebiometric Protection," Dec. 2005.
〔15〕 Korea Communications commission, Korea Internet & Security Agency , "A Guideline for the protection of Biometric," Dec. 2017.
〔16〕 Saurabh Kulkarni, "Analyzing Trusted Elements in Mobile Devices," Deparmtent of Mathematics and Computer Science, Nov. 2015.
〔17〕 Security Research Department Security Technology Team, "Detailed analysis of the latest Android TrustZone vulnerability," Financial Security Institute, Oct. 2015.
〔18〕 Jason Kim, "K-NBTC International Standard Activities & Test Services," Korea Internet & Security Agency, 2015
〔19〕 ARM, White Paper, R Coombs, "Securing the Future of Authentication with ARM Trust Zone-based Trusted Execution Environment and Fast Identity Online (FIDO)", 2015.
〔20〕 Jeon Jeong Hoon, "A Study on Security Risk according to the activation of Bio-Authentication Technology," Convergence security journal, 16(5), pp. 57-63, Aug. 2016.
〔21〕 Byoungcheon Lee, "Certified Key Management in Multi K-FIDO Device Environment," Journal of the Korean Institute of Information Security and Cryptology, 27(2), pp. 293-303, Apr. 2017.

[22] Hyeonjong Ki, "ISO/IEC JTC1/SC37 Biometrics WG," The monthly technology & standards, pp. 46-50, Feb. 2007.
[23] Dr Stephen Elliott , "JTC 1 SC 37 - 'Biometrics' International Standards," Purdue University, Feb. 2007.
[24] FIDO alliance, "2017 State of authentication report,", 2010.
[25] Kai Fan, Hui Li, Wei Jiang, Chengsheng Xiao, and Yintang Yang, "U2F based Secure Mutual Authentication Protocol for Mobile Payment," IACM International Conference Proceeding Series, May. 2017.
[26] Jang J and Kang B.B., "URetrofitting the Partially Privileged Mode for TEE Communication Channel Protection," IEEE Transactions on Dependable and Secure Computing, May. 2018.
[27] Aravind Machiry, Eric Gustafson, Chad Spensky, Chris Salls, and Nick Stephens, "BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments," Network and Distributed System Security Symposium , Mar. 2017.
[28] Togan M, Chifor B.-C, Florea I., and Gugulea G, "A smart-phone based privacy-preserving security framework for IOT devices," Institute of Electrical and Electronics Engineers Inc, Dec. 2017.
[29] Boannews, "Biometrics Global Certification FIDO, Domestic Business Activity Report," https://www.boannews.com/media/view.asp?idx=69879, Jun. 2018.
[30] H.Nishimura, "Secure authentication key sharing between mobile devices based on owner identity," 2018 Fourth International Conference on Mobile and Secure Services, Feb, 2018.

〈저자소개〉

정 용 헌 (Yong-hun Jung) 정회원
2006년 2월: 광운대학교 전자정보공과대학 컴퓨터공학부 학사
2016년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2006년 1월~현재: 한국후지쯔 플랫폼 시니어 매니저
〈관심분야〉 (클라우드) 시스템 아키텍처, IT 인프라 컨설팅, 정보보호
E-mail: dearyu@korea.ac.kr

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월: 삼성그룹 네이버주, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책
E-mail: kevinlee@korea.ac.kr