Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 3 pp. 41-48, 2017

https://doi.org/10.5762/KAIS.2017.18.3.41
ISSN 1975-4701 / eISSN 2288-4688

시장 경제 활성화를 위한 안전한 모바일 전자결제 방안 연구

김형욱, 정용훈, 전문석*
숭실대학교 컴퓨터학과

A Study on Secure Mobile Payment Service for the Market Economy Revitalization

Hyung-Uk Kim, Yong-Hoon Jung, Moon-Seog Jun*
Department of Computer Science and Engineering, Soongsil University

요 약 최근 핀테크 활성화로 인한 금융 거래 및 결제 관련하여 많은 연구 개발이 활발하게 진행되고 있다. 상품을 구매하고 대금을 지급하는 방법에는 현금, 카드 등 여러 가지 방법으로 결제를 진행하고 있으며, 최근 모바일 카드를 통한 결제 및 휴대폰 간편 결제 등 결제 방식이 빠르고 간편화 되고 있다. 제안하는 모바일 전자결제 방식은 기존 카드 리더기 또는 카드 단말기 없이 사용자의 휴대폰을 이용하여 결제할 수 있는 방법을 제안한다. 결제 시 스마트폰에 내장된 지문인식기를 통해 사용자의 생체정보를 입력받아 본인인증이 먼저 수행되며, 결제 이전 두 사용자의 확인을 위해 인증된 기관에서 부여 받은 인증 코드를 전송하여 이를 검증하고 결제가 이루어진다. 사용자의 생체정보와 결제관련 정보는 스마트폰 내의 안전한 FIDO TEE영역에 저장되어 악의적인 사용자로부터 안전성을 확보하였다. 키의 안전성 측면에서는 모든 키 생성은 FIDO TEE 영역에서 이루어지게 하여 안전성을 확보하였으며, 스니핑, 중간자 공격 등 다양한 공격 방식에 대한 무력화를 통해 안전한 모바일 전자결제 서비스를 제공한다.

Abstract Recently, there has been a lot of ongoing research regarding financial transactions and payments due to the emergence of financial technology (FinTech). Payments have been processed through cash and credit cards, and payment methods have been simplified and are more convenient, with mobile payment via mobile cards and mobile phones. This study offers a new mobile payment method by using a mobile phone instead of a card reader or terminal. For payments, authentication is processed with the user's biometrics and a built-in fingerprint scanner, and the payment is processed after receiving an authentication code issued by the authorizing institution to confirm the user's identity. User biometrics and payment information is secured from any kind of malicious hacker by saving it in a Fast Identity Online (FIDO) Trusted Execution Environment (TEE) section in a smartphone. Regarding key security, every key is securely created in the FIDO TEE section, providing secure mobile payment by neutralizing various malicious attacks, including sniffing and the man-in-the middle attack.

Keywords : Biometrics, Fingerprint, Fintech, FIDO, FIDO TEE

1. 서론

최근 IT 기술의 발달로 금융권에서는 IT기술의 적극적인 활용을 통해 핀테크라는 거대한 혁명이 진행되고 있다. 핀테크는 파이낸셜과 기술의 합성어로 스마트기기를 통해 결제, 예금, 출금, 이체 그리고 자산관리 등 각종 금융 서비스를 IT 기술을 통해 처리하는 산업이다.

세계적인 그룹 페이팔, 알리페이 그리고 한국에서는 카카오페이 등이 결제 서비스와 전자 지갑 형태의 핀테크 기술을 선보이고 있으며, 금융권, 대기업, 중소기업 등에서도 모바일 결제서비스를 선보이고 있다[1].

현재 전통시장은 대형할인업체의 등장으로 그 입지가

*Corresponding Author : Moon-Seog Jun(Soongsil Univ.)
Tel: +82-2-826-6526 email: mjun@ssu.ac.kr
Received December 14, 2016 Revised (1st December 26, 2016, 2nd January 2, 2017)
Accepted March 10, 2017 Published March 31, 2017

현저하게 축소되고 있으며, 이는 지역경제 활성화의 침체 원인이라고 할 수 있다. 최근에는 각급 지방자치단체가 나서 막대한 예산을 투입하여 침체된 전통시장의 활성화를 위해 노력하고 있다. 전통시장을 방문하지 않는 이유로는 대부분 현금 결제만 가능한 이유로 카드 결제 불가능, 주차장 시설 부족, 교환 및 환불의 어려움 등으로 나타났다.

최근 결제 수단의 변화로 현금, 신용카드, 체크카드, 모바일카드 등 다양한 결제 수단을 제공하고 있다. 그러나 현금, 신용카드, 체크카드는 분실 시 부정사용에 대한 문제점을 가지고 있으며, 모바일카드는 휴대폰 해킹으로 인해 부정사용 될 수 있는 문제점을 가지고 있다.

영국 국제통상기구 MEF(Mobile Ecosystem Forum)은 모바일 결제에 대한 사용자 신뢰도가 낮은 것으로 분석되었다.

기존 신용카드 및 체크카드는 대부분 카드 뒷면의 마그네틱에 정보를 읽어 들여 처리하고 있으며, 복사로 인한 사고가 빈번하게 발생하고 있다. 최근에는 IC 칩이 내장된 카드로 대체되어 복사로 인한 사고를 방지할 수 있다. 또한 모바일에서는 NFC, QR코드, RFID/IrDA 등 무선을 이용하여 카드 정보 등을 전송하여 결제를 진행하고 있으며, 이 모든 결제 수단은 부정사용에 대해 매우 취약하다.

본 논문에서는 지역경제 활성화를 위해 전통시장에서 카드 단말기 없이 스마트폰만을 이용하여 부정사용이 불가능한 간편 결제시스템을 제안하고자 한다. 2장은 관련 연구로서 핀테크 시장에서 사용하는 간편 결제시스템의 기술들을 기술하고, 3장에서는 본인인증이 강화된 모바일 결제시스템을 설계한다. 4장 기존 모바일 결제시스템과 제안하는 시스템을 비교하고, 마지막으로 결론을 맺는다.

2. 관련 연구

2.1 핀테크 기술

2.1.1 금융 시장의 위협

국내 금융에서는 정보통신기술의 발달로 송금, 결제, 자산관리 등 각종 금융 서비스를 PC, 모바일 등에서 이미 제공하고 있었다.

최근 들어 핀테크 산업의 등장으로 글로벌 IT 기업들이 간편하고 다양한 금융서비스 상품을 개발하여 핀테크 시장을 형성해 가고 있다. 해외 IT 기업의 금융업 진출은 전자지갑, 지급결제, 전자화폐 등 모바일 정보기술 환경에 결합하여 금융거래의 확산을 가속화 하고 있다.

Table 1. ICT Companies Financial Service Expansion

Sectors	Enterprise	Contents
Platform	google	Wallet(Google Wallet)
	apple	Wallet(Apple Pay)
SNS	facebook	Wallet
	Tencent	Payments(Tenpay)
Communication Service	verizon	Mobile Payments(ISIS)
	Safaricom	Payments, Electronic cash
electronic commerce	Alibaba	Payments(Alibaba)
	ebay	Payments(Paypal)
	amazon	Payments(Amazon Payments)

해외 IT 기업들은 국내 금융회사와 제휴를 통해 금융서비스를 제공하고 있으며, 이는 IT 기업을 중심으로 한 비금융기관의 금융업종 진입이 기존 금융기업들의 고유 시장의 잠식으로 이어질 때 금융기업 고유 사업에 위협적인 요소가 될 수 있다. 미국의 경우 IT기업 등 비금융사가 2020년에는 기존 금융권 시장의 30%를 잠식 할 것으로 예상하고 있으며, 국내의 경우 비금융기관의 금융업 참여에 대한 규제로 인해 시장 잠식의 속도가 느리며, 소액결제와 송금을 중심으로 비금융사의 시장 확대가 이루어질 것으로 예상된다[2].

2.2.2 국내외 핀테크 사업 동향

최근 화폐제도의 변화로 현금 없는 사회로 변화하고 있으며, IT분야를 선도하는 유럽의 덴마크, 스웨덴, 노르웨이가 현금 없는 사회로 진출하기 위해 발 빠르게 움직이고 있다. 아시아에서는 IT분야를 선도하고 있는 우리나라에서도 현금 없는 사회로 가기 위한 준비를 하고 있다.

유럽의 모바일페이, 우리나라의 삼성페이, 미국의 애플페이, 구글페이는 서로 경쟁하며 시장을 확대해 가고 있으나 결국 이 모든 것을 통합한 전세계 공통 전자결제 시스템이 탄생할 것으로 예상된다. 또한 금융에 한정된 서비스만이 아닌 보험, 증권, 인터넷 전문은행으로 점차 확대되어 사용자의 편의성과 안전성을 중심으로 한 서비스로 사용될 것으로 예상된다[2].

2.2.3 블록체인과 비트코인

기존 금융기관의 거래를 중앙집중적인 장부에 기반하

기 때문에 높은 비용이 발생하고, 또한 서로 다른 화폐의 단위로 금융회사에서 관리하는 장부 또한 각기 다르므로 높은 비용이 발생한다.

블록체인은 이러한 비효율적인 구조를 혁신하려는 기술이다.

블록체인은 일종의 금융장부로서 비트코인 프로그램을 이용하는 모든 개개인의 P2P 거래내역이 모두 이곳에 기재되고 공유된다.

비트코인은 누구나 P2P 프로그램을 이용하여 돈을 주고받으며, 제3자의 개입 없이 단일 장부에 그 거래 내역이 불변의 기록으로 기입되는 방식으로 거래가 확정된다. 따라서 적은 비용으로 마치 오프라인에서 현금을 주고받듯이 개인 대 개인으로 거래가 가능해진다.

블록체인은 분산데이터베이스의 하나로 P2P 네트워크를 활용하고, 비트코인 사용자 모두의 컴퓨터에 저장할 수 있다.

블록체인 방식은 사용자 과반수의 데이터와 일치하는 거래 내역은 정상 장부로 확인되어 블록으로 묶여 보관된다. 비트코인의 경우 10분 정도마다 사용자들의 거래 장부를 검사해 해당 시간의 거래내역을 한 블록으로 묶는다. 만약 특정 사용자의 장부에 누락 등의 오류가 발생하면, 정상 장부를 복제해 대체하는 방식으로 수정된다[3].

블록체인 기술은 데이터를 공유하는 사용자가 많을수록 보안 안정성은 커진다.

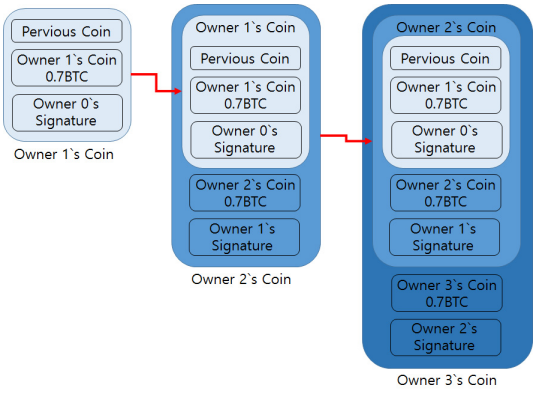

Fig. 1. The Bitcoin network processes

2.2 인증 수단의 변화

기존 본인인증 수단 중 가장 많이 사용되고 있는 방식은 ID/PW로 인증정보 유출 위험이 매우 높고 악의적인 사용자로부터 해킹에 대한 많은 위험에 노출되어 있다. 또한 공인인증서는 대여 및 위임으로 인한 피해사고가 발생 할 수 있으며, 항상 소지해야 한다는 불편함을 가지고 있다.

최근 IT기술의 발달과 IT기기의 발전으로 신기술을 활용한 본인인증 수단이 확대되고 있으며, 금융에서는 바이오 인증기술, 블록체인 등 보안성과 투명성, 비용절감 효과를 볼 수 있어 본인인증 수단으로 주목받고 있다.

바이오 인증기술은 기존 인증 방식과 달리 항상 소지해야 하는 불편함과 기억해야만 한다는 문제점을 해결할 수 있으며, 또한 대여 또는 위임으로 인한 사고를 예방할 수 있다.

2.2.1 SSO(Single Sign-On)

SSO는 사용자측면에서 한 번의 인증 과정으로 생성된 인증정보를 통해 다수의 서비스를 제공받는 통합 인증관리 방식이다. 즉, 사용자는 하나의 인증정보로 접근권한이 있는 여러 서비스에 자동으로 인증 처리됨으로써 접근할 수 있다[4]. 이 기술을 통해 사용자는 인증 정보 관리에 대한 부담을 줄일 수 있으며, 재인증 과정 없이 다른 서비스를 이용할 수 있는 편의성을 제공 받을 수 있다. 또한, 서비스 제공자 측면에서는 사용자 인증정보 관리를 위한 비용이 감소하며, 인증과 인증 정보의 집중화를 통한 중앙 관리가 가능하다[5]. 현재 SSO를 지원하기 위한 많은 프로토콜이 있으며 대표적인 방법은 OAuth(Open Authorization), SAML(Security Assertion Markup Language) 등이 있다[5].

2.3 FIDO(Fast IDentity Online)

FIDO(Fast IDentity Online)는 생체인식을 활용한 인증방식의 기술표준으로 FIDO 얼라이언스(FIDO Alliane)가 제정하였다. FIDO 얼라이언스는 삼성, 레노보 같은 단말기 제조사부터 칩을 제조하는 NXP, 퀄컴 그리고 OS 플랫폼 기업 마이크로소프트, 구글, 금융 서비스기업 알리바바, 페이팔, 비자 등 다양한 기업으로 회원사를 구성하고있다[6].

FIDO는 UAF(Universal Authentication Framework) 그리고 U2F(Universal 2nd Factor) 방식으로 구성된다. UAF는 지문, 성문, 안면, 홍채 등 사용자 고유의 생체정보를 인식해 인증하는 기술이며, U2F는 ID, 비밀번호로

1차 인증한 후 1회성 보안키를 저장하고 있는 동글(Dongle)을 기기에 꽂아 2차 인증하는 방식이다.

UAF는 기기를 이용해 생체인식을 진행하면 FIDO 서버에 접속하고, 그다음 기기에 저장된 보안키를 입력하는 순으로 진행된다. FIDO의 기본적인 의미는 사용자 확인(Verification)과 인증(Authentication) 프로토콜 그리고 인증 서버를 분리시키고 다양한 방법으로 사용자 인증을 지원하도록 하는 것이며 크게 등록 절차, 인증 절차, 탈퇴 절차로 구성된다[7].

2.3.1 FIDO UAF의 등록 프로토콜

(1) 사용자가 응용 앱에서 인증 수단을 패스워드에서 지문 인증으로 변경 요청한다.

(2) 응용 앱은 사용자로부터 패스워드를 입력받아 응용 서버에 전달하면 응용 서버는 패스워드를 확인하고 FIDO 등록 요청 메시지를 FIDO 서버에게 요청한다.

(3) FIDO 서버는 인증정책이 포함된 FIDO 등록 요청 메시지를 생성하여 FIDO 클라이언트에 전달한다. 참고로, 인증정책은 특정 제조사, 특정 모델, 특정 인증수단 등으로 사용할 인증 장치를 제한할 수 있다.

(4) FIDO 클라이언트는 서버 인증정책에 부합하는 지문 인증 장치를 호출하고, 사용자가 지문을 입력하여 사용자 인증에 성공하면, 지문 인증 장치는 공개키 쌍을 생성한다.

(5) 지문 인증 장치는 생성된 공개키와 공개키의 입증 정보가 포함된 FIDO 등록 응답 메시지를 FIDO 서버에 전달한다.

(6) FIDO 서버는 공개키의 입증 정보를 인증 장치 메타데이터를 이용해 확인한 후, 해당 공개키를 FIDO 서버에 저장한다[8].

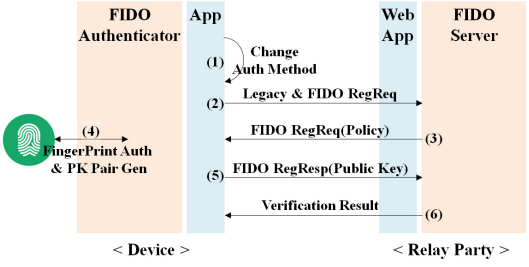

Fig. 2. FIDO UAF Registration Protocol

2.3.2 FIDO UAF의 인증 프로토콜

(1) 응용 앱은 응용 승인에 사용자 인증을 요청한다. 예를 들어, 간편결제 서비스를 이용하기 위해 지문 인증을 요청한다.

(2) 응용 앱은 응용 서버에 FIDO 인증을 요청하면 응용 서버는 FIDO 서버에 FIDO 인증 요청 메시지를 요청한다.

(3) FIDO 서버는 FIDO 인증 요청 메시지를 생성하여 FIDO 클라이언트에 전달한다.

(4) FIDO 클라이언트는 FIDO 인증 요청 메시지에 포함된 정보로 지문 인증 장치를 호출하고, 사용자가 지문을 입력하여 사용자 인증에 성공하면, 지문 인증 장치는 등록 프로토콜을 통해 생성된 개인키를 이용해 전자서명을 생성한다. 전자서명을 생성하기 이전에 거래 정보를 출력하여 사용자로부터 거래 확인을 받는 절차가 추가될 수 있다.

(5) 지문 인증 장치는 전자서명이 포함된 FIDO 인증 응답 메시지를 FIDO 서버에 전달한다.

(6) FIDO 서버는 등록 프로토콜을 통해 등록된 공개키를 이용하여 전자서명을 확인하고 인증 결과를 전달한다[9].

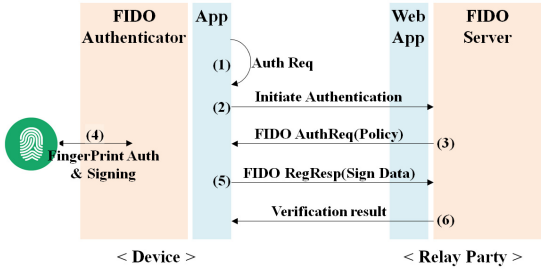

Fig. 3. FIDO UAF Authentication Protocol

2.4 TEE(Trusted Execution Environment)

TEE란 안드로이드 운영체제에서 일반영역(Rich OS)과 별도로 높은 수준의 보안 서비스를 제공하는 독립된 보안 실행 환경을 말한다.

TEE는 안드로이드 환경의 스마트디바이스에서 사용 가능하며 개인정보, 인증서, 콘텐츠 등 강력한 보안이 필요한 데이터 및 App을 독립된 보안영역에서 안전하게 처리 및 실행 가능하게 한다.

TEE는 안드로이드 운영체제가 구동되는 일반영역과 물리적으로 격리되어 있으며, 일반영역에서 TEE 자원에 접근하기 위해서는 TEE Client(TC)와 Trusted Application(TA)간의 인터페이스를 통해 제한적인 자원에 대해서만 접근이 가능하다. TA는 데이터 암호화 및 복호화, 키쌍 생성, 전자서명 생성 등을 수행하는 보안소프트웨어이다[10-11].

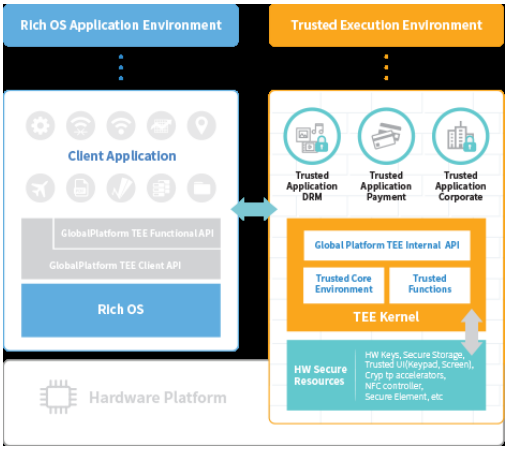

Fig. 4. TEE structure

3. FIDO TEE를 이용한 모바일 결제 시스템

스마트폰을 이용한 결제 환경에서 안전한 사용자 인증 서비스를 제공하기 위해 생체인증을 사용하며, 인증에 사용되는 생체정보, 개인정보, 인증서, 콘텐츠 등은 보안이 강력한 독립된 보안영역에서 안전하게 처리, 보관, 실행된다.

3.1 전체시스템 구성

제안하는 시스템은 카드 단말기 없이 스마트폰을 소지한 사람은 누구나 결제 가능한 시스템을 제안한다. 제안하는 시스템에서는 스마트폰의 NFC 기능을 사용하며 스마트폰과 스마트폰의 접촉만으로 결제가 가능한 시스템이다.

3.1.1 판매자 등록

판매자는 FIDO와 NFC를 지원하는 스마트폰을 보유하고 있으며, 전용 App이 설치되어 있다고 가정한다. 판매자는 최초 1회 은행 창구를 방문하여(대면) 판매자 등록을 해야만 한다.

판매자 등록은 은행에서 신규 통장개설 절차와 유사하다. 본인확인을 위한 신분증(주민번호) 진위확인 후 물품 대금을 받기 위한 신규계좌 개설 또는 기존 계좌 연결, 장치 인증키 생성, 상점코드 생성이 단계별로 진행된다.

장치 인증키는 인가된 기기에서만 사용할 수 있도록 제한하기 위함이며, 은행에서 생성/발급된다. 상점코드 또한 은행에서 생성/발급되며, 이는 판매자 구분과 이를 통해 물품 대금을 지급하기 위해 사용된다.

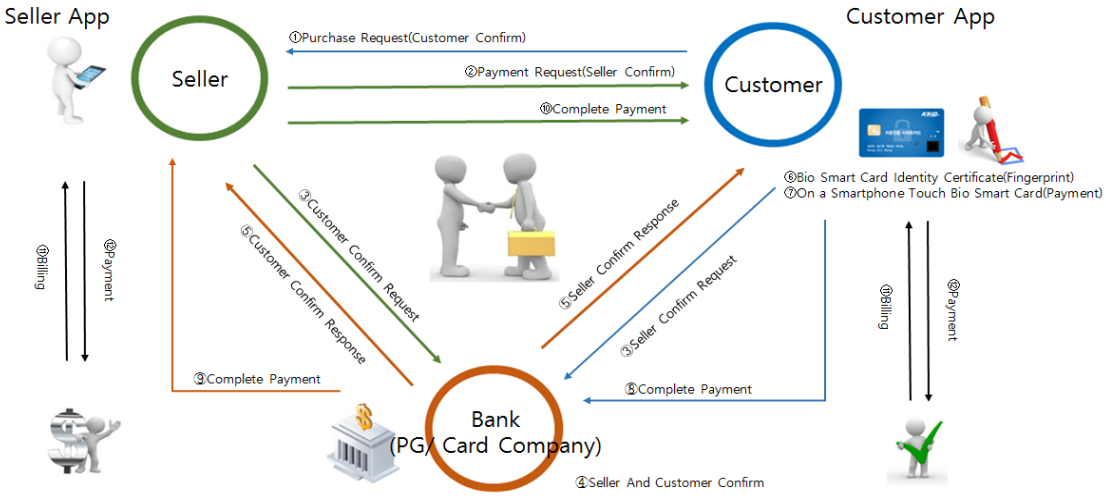

Fig. 5. Suggest system structure

마지막으로 판매자에 대한 지문등록은 위 과정이 모두 완료된 후 판매자 본인의 휴대폰 TEE(Trusted Execution Environment) 영역에 지문을 안전하게 등록/저장하며, 등록된 지문은 본인확인 용도로 사용된다.

3.1.2 구매자 등록

구매자는 FIDO와 NFC를 지원하는 스마트폰을 보유하고 있으며, 전용 App이 설치되어 있다고 가정한다.

구매자는 최초1회 은행을 방문하여(대면) 구매자 등록을 해야만 한다. 은행에서 신분증을 통한 본인확인 후 신청 절차가 진행된다.

본인확인 후 은행에서는 개인의 신용도에 따라 한도가 결정되며, 장치 인증키, 구매자코드가 생성되어 발급된다. 구매자코드는 예를 들어 신용카드는 카드번호가있듯 구매자를 식별하기 위한 고유 값으로 사용된다.

마지막으로 구매자에 대한 지문등록은 위 과정이 모두 완료된 후 구매자 본인의 휴대폰 TEE 영역에 지문을 안전하게 등록/저장하며, 등록된 지문은 본인확인 용도로 사용된다.

3.1.3 통합카드

구매자와 판매자 등록은 신뢰할 수 있는 기관에서 등록한다. 신뢰할 수 있는 기관으로는 은행, 카드사, 인터넷전문은행 등이 될 수 있다.

구매자와 판매자는 여러 개의 카드번호를 등록하여 사용할 수 있다. 등록된 카드는 기관 구분 코드를 이용하여 원하는 카드를 손쉽게 사용할 수 있다.

카드번호와 기관 분류 코드는 TEE 영역에 안전하게 보관되며, 지문인증을 통해 사용자 본인인증 이후 사용가능하다.

Table 2. TEE stored information(example)

	B_code	card_no	PW
Alice	1234	12345678	FIDO Value
Bob	2345	23456789	FIDO Value
Zebra	3456	87654321	FIDO Value

4. 안전성 분석

제안하는 시스템의 안전성을 확인하기 위하여 생체정보의 안전성을 비교하기 위해 다양한 공격 방법에 대한 안전성을 확인하였으며, 분석된 전체적인 결과는 다음 Table 3과 같다.

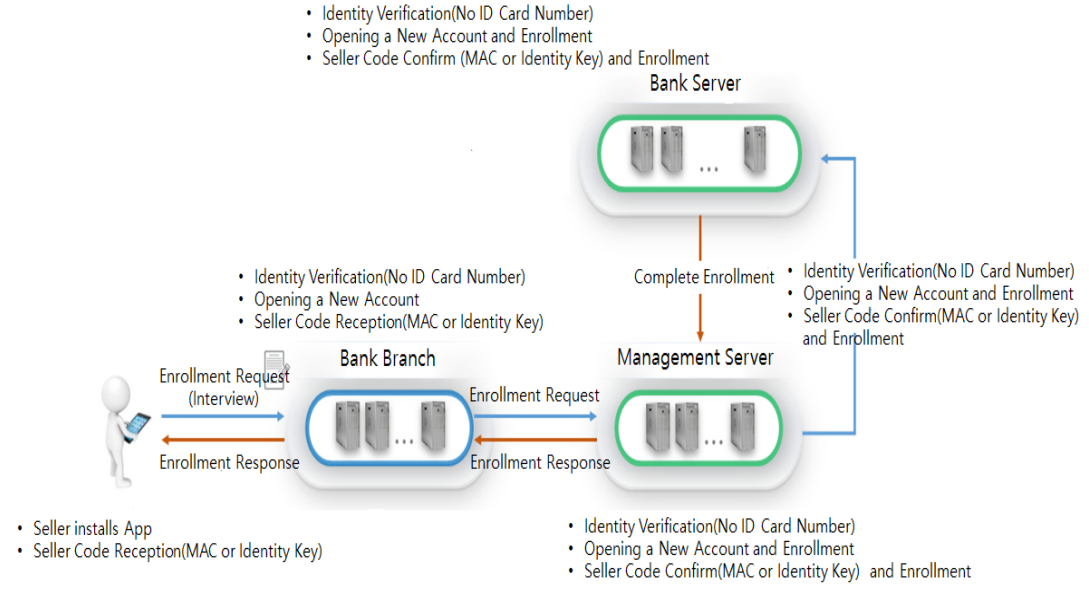

Fig. 6. merchant registration

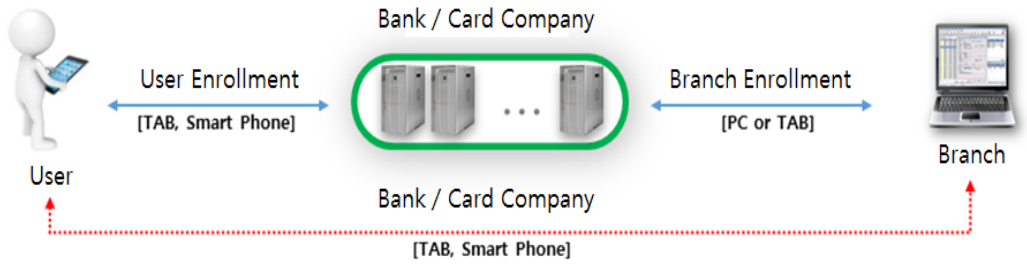

Fig. 7. user registration

Table 3. safety comparison

	SSO	Broker	Proposal System
Safety	Usually	-	Strong
Key Generate	Safety	-	Safety
Sniffing	Safety	Safety	Safety
MITM	-	-	Safety

4.1 생체정보의 안전성

스마트폰에서 생체정보, 개인정보, 인증서 등을 저장하기 위해 사용되는 공간은 일반영역으로 스마트폰에 악성코드가 내포된 앱(App)이 설치되거나 악성코드에 감염되면, 일반영역에 저장된 생체정보(개인정보), 연락처, 사진 등 유출 사고가 발생할 수 있으며, 이러한 유출 사고가 실제 빈번하게 발생하고 있다.

제안하는 시스템에서는 스마트폰 내에 보안영역인 TEE(Trusted Execution Environment)를 사용하여, 안드로이드 환경의 스마트 디바이스에서 생체정보(개인정보), 인증서, 콘텐츠 등 강력한 보안이 필요로 한 데이터 및 App을 독립된 보안영역에서 안전하게 처리 및 실행할 수 있어 안전하다. 또한 TEE 영역에 저장된 생체정보, 인증서 등 외부로 유출이 불가능하므로 안전하다.

4.2 키 생성

기존 시스템은 생체정보, 인증서 등 개인정보를 일반영역에 저장하고 있으며, 암·복호화/검증, 키쌍 생성, 전자서명 생성 등 모든 작업 수행을 일반 영역에서 수행되므로 온라인 공격을 통해 정보 유출이 가능하다.

제안하는 시스템은 보안영역인 TEE영역에서 생체정보의 암·복호화/검증, 키쌍 생성, 전자서명 생성 등 모든 작업 수행을 TEE 내부에서 실행하므로 해킹 또는 정보 유출 등 온라인 공격으로부터 안전하다.

4.3 Sniffing

생체정보(개인정보), 인증서 등은 모든 통신구간에서 암호화되어 전송되거나 전자서명값만 전송되므로 암호학적 안정성을 확보하고 있다. 생체정보의 복호화 및 검증 역시 보안영역인 TEE영역에서 이루어지므로 공격자가 중간에서 데이터를 획득하여도 암호화된 생체정보, 인증서 등을 복호화 할 수 없으므로 유출된 데이터는 무의미한 값이 된다.

4.4 Man-in-the-middle attack

공격자는 생체정보(개인정보)의 암호화, 키쌍 생성 과정에서 임의의 키쌍을 생성하여 양측의 생체정보를 엿보거나 위조하려 할 수 있다.

제안하는 시스템에서는 생체정보의 암호화, 키쌍 생성은 보안영역인 TEE 내부에서 생성되고 관리된다. 공격자가 중간에서 암호화된 데이터를 갈취하여 복호화를 시도할 경우 TEE 내부에서 생성/관리되는 키를 획득할 수 없으므로 복호화는 불가능하다. 또한 개인키를 이용한 전자서명값을 생성할 수 없다.

5. 결론

최근 핀테크 기술의 발달로 다양한 분야에서 모바일을 통한 서비스를 제공하고 있다. 특히 금융권에서는 모바일에서 생체정보를 이용한 비대면 본인확인, 간편 결제 등에 사용되고 있으며, 생체정보를 이용한 비대면 본인확인 및 전자서명에 적용되고 있다.

본 논문에서는 사용자가 모바일 환경에서 생체정보(개인정보), 인증서, 콘텐츠 등을 안전하게 저장/관리할 수 있으며, 생체정보를 이용한 사용자 인증 및 결제 방법

을 제안하고 있다. 제안하는 사용자 인증 기법은 생체정보를 이용하여 위임 또는 대여로 인한 사고를 예방할 수 있다. 또한 결제 시스템에서는 안전한 사용자 인증 기법과 금융 관련 정보를 안전하게 관리하여 안전한 금융 거래를 제공한다. 앞으로 다양한 전자화폐와 모바일 전자결제서비스가 나타날 것이며, 이에 따라 모바일에서 간편성, 편의성, 안전성이 강조된 사용자 인증 방법과 기타 민감 정보 보호에 대한 연구가 필요할 것이다.

References

[1] Korea Internet & Security Agency, Excavating research areas of FinTech through the analysis of its relevant technologies and policy trends at home and abroad, Feb. 2016.

[2] jeongkook park, “Fintech and information security”, 2015 korean institute of information scientists and engineers. pp.23-32, May, 2015.

[3] Inyeob Ji, Kwang Myung Chun, “Digital Currency and Inflation Hedge: Evidence from Bitcoin” Korea Association for Telecommunications Policies. pp31~51. 2016.

[4] Pratap Murukutla, K. C. Shet, "Single Sign on for Cloud.", *2012 International Conference on Computing Sciences. IEEE*, pp. 176-179, Sept, 2012. DOI: https://doi.org/10.1109/ICCS.2012.66

[5] Wanpeng Li, Chris J. Mitchell, "Security issues in OAuth 2.0 SSO implementations.", *International Conference on Information Security. Springer International Publishing*, pp. 529-541, Oct. 2014. DOI: https://doi.org/10.1007/978-3-319-13257-0_34

[6] Hyung-woo Lee, Yeong-Joon Park, “A Design and Implementation of User Authentication System using Biometric Information”, Korea Academia-Industrial cooperation Society, pp.3548-3557, Sept. 2010. DOI: http://doi.org/10.5762/KAIS.2010.11.9.3548

[7] Jeong-Hyo Park, " A Non-Password Secure Biometric Digital Signature Method for Mobile Device", Soongsil University Graduate School, 2016.

[8] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, "Universal 2nd factor (U2F) overview", FIDO Alliance Proposed Standard, 2015.

[9] Rolf Lindemann, Davit Baghdasaryan, Eric Tiffany, "FIDO UAF Protocol Specification v1.0", FIDO Alliance Proposed Standard, 2014.

[10] FIDO TEE, www.emobileid.co.kr

[11] KISA, “Implementation guideline for safe usage of accredited certificate bio information in smart phone”, Sept. 2016.

김 형 욱(Hyung-Uk Kim) **[정회원]**

- 2012년 2월 : 숭실대학교 정보보안학과 (공학석사)
- 2012년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 (박사수료)
- 2006년 9월 ~ 현재 : 한국전자인증 기술연구소 책임연구원

<관심분야>
PKI, 생체인증, IoT

정 용 훈(Yong-Hoon Jung) **[정회원]**

- 2006년 8월 : 숭실대학교 컴퓨터공학 (공학석사)
- 2010년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2011년 3월 ~ 2014년2월 : 서일대학교 조교수
- 2016년 6월 ~ 현재 : 한국스마트아이디 사업기획부장

<관심분야>
생체인증, IoT, 네트워크 보안

전 문 석(Moon-Seog Jun) **[종신회원]**

- 1989년 2월 : University of Maryland Comuter Science (공학박사)
- 1989년 3월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

<관심분야>
네트워크 보안, 생체인증, IoT