논문 20-45-10-11 The Journal of Korean Institute of Communications and Information Sciences '20-10 Vol.45 No.10
https://doi.org/10.7840/kics.2020.45.10.1720

국내 모바일 간편결제 보안 문제점 개선 방안

이 광 규◆

Improvement of Domestic Mobile Payment Security Problem

Kwang-Kyu Lee◆

요 약

스마트폰의 폭발적 증가로 결제시장에도 새로운 바람이 불고 있다. 최근 금융시장과 IT시장에서는 핀테크(FinTech)기술을 접목한 간편결제 서비스가 국내외적으로 급속히 확산되고 경쟁이 과열되고 있다. 하지만 편리한 만큼 그에 따르는 위험 요소도 있다. 특히, 모바일 간편결제 서비스의 품질 속성 중 보안성과 신뢰성 개선이 무엇보다도 절실함을 보여주고 있다. 이에 본 논문에서는 국내 모바일 간편결제 서비스가 급속히 확산되고 글로벌 인프라를 기반으로 경쟁력을 확보하기 위한 활성화 방안 중에서, 문제가 되는 보안성과 신뢰성 문제를 살펴본다. 이를 통해 해외 주요 사례와의 비교 분석 후 국내 간편결제 서비스 보안 및 신뢰성 발전을 위해 보완해야 될 사항들에 대해 기술하고자 한다.

Key Words : FinTech, Final Technology, Payment, Mobile Pay, Mobile Security

ABSTRACT

With the explosion of smartphones, there is a new wave in the payment market. Recently, in the financial market and IT market, the simple settlement service that incorporates FinTech technology is rapidly spreading domestically and the competition is overheating. However, there are risks as well as convenience. Especially, improvement of security and reliability among the quality attributes of mobile simple settlement service shows the desperation. In this paper, we examine the problem of security and reliability, which is one of the activation methods to secure competitiveness based on global infrastructure and rapid expansion of mobile payment service in Korea. We will describe the issues that need to be supplemented for security and reliability development of domestic simple settlement service after comparing and analyzing with major overseas cases.

Ⅰ. 서 론

최근 IT 세계와 금융권에서 핫이슈가 되고 있는 '핀테크(FinTech)'는 금융을 뜻하는 'Financial'과 기술을 뜻하는 'Technology'의 합성어로 전통적인 금융 시스템에 최신 IT 기술을 결합해 좀 더 편한 금융 서비스를 받게 만드는 것을 의미한다. 다양한 분야에서 O2O(Online to Offline)관련 산업들이 활발해지면서 금융과 ICT에 기반을 둔 핀테크 산업이 새로운 패러다임의 전환을 가져왔다[1]. 이는 ICT의 발전으로 다양한 정보시스템이 구축됨으로써 행정서비스 뿐만 아니라, 금융서비스에 대한 요구를 변화시키고 있다[2]. 핀테크 산업은 크게 송금 분야, 결제 분야,투자분야로 분류되고, 핀테크의 핵심은 사용자들이 좀 더 편리하게 금융서비스에 접근하여 안전하게 결제하고, 송금하고 거래하는 서비스를 말한다[3]. 모바일 간편결제 서비스는 지불 및 송금 분야 핀테크의 핵심적인 기능을 이루고 있다. 현재로서는 국내 전자상거래 결제와 오프라인 결제

※ 본 논문은 2020년도 신한대학교 교내연구비에 의해 연구되었음
◆ First Author : Shinhan University Department of IT Convergence, kklee@shinhan.ac.kr, 정회원
논문번호 : 202006-132-C-RN, Received June 17, 2020; Revised July 18, 2020; Accepted July 21, 2020

의 주된 수단은 아직까지 신용카드가 주류를 이루고 있으나 스마트폰이 대중화되면서 모바일 결제 시장에 대한 이동통신회사, 은행, 신용카드회사들의 관심이 집중 되고 있다. IT시대에 맞게 빠르게 움직이고 있는 현대인들은 더 빠르고 편리하며 간편한 것을 원하고 있으며 이러한 기대를 충족시켜주는 기능의 하나가 스마트폰으로 바로 결제가 이루어지는 모바일 간편결제 서비스 또는 모바일 페이다[4]. 간편결제가 각광받고 있지만 보안성에 대한 의문은 존재한다. 간편결제가 편리하다는 장점을 지니고 있지만 동시에 절차가 생략된 만큼 보안사고 우려가 커지는 게 아니냐는 반응이 주를 이룬다. 국내 금융관련서비스, 즉, 인터넷뱅킹에서 송금이나 이체를 한다든지, 아니면 인터넷쇼핑을 통해서 물건을 구매하고 결제를 할 때의 프로세스는 ActiveX, 공인인증서, 키보드 보안 모듈, 암호화 통신 모듈 등 그 외에 여러 모듈들을 설치해야 되기에 사용자는 매우 불편하고, 보안 대책은 여전히 미흡하다. 또한, 편리한 만큼 간편결제 서비스의 보안이 보장되지 않는다면 언제든지 간편결제 과정에서 금융 피해가 발생될 수 있다. 현재 정부가 간편결제를 추진하며 핀테크 산업의 주도적인 위치를 선점하기 위해서는 간편결제 서비스 보안 절차를 소비자의 책임은 최소한으로 제한하되 보호 조직은 강화하는 방향으로 가야 한다. 간편결제 서비스는 간편성과 보안성 두 마리 토끼를 잡아야 하지만, 아직은 간편성에만 초점을 맞춰 진행되는 상황으로, 보안에 대한 심각한 우려가 제기되며, 결제가 확산되더라도 간편함과 안전성 두 가지 모두 조화를 이루어야 할 것이다. 그러나 해외에서는 전자금융거래에 접근하는 방식이 국내와는 다르다. 해외에서는 사용자 편의성을 제공하고 뒷단에서 이상거래탐지시스템(Fraud Detetection System:FDS)을 높이는데 투자를 많이 하지만, 국내는 사용자에게 추가인증을 요구하는 방법으로 이상 거래를 막는다. 즉, 국내에서는 사용자단에 인증작업 등의 보안절차가 진행되는 반면 해외에서는 사용자단 보다는 서버단에서의 인증작업 등의 보안 절차가 이루어지므로 사용자단의 보안 절차가 간소화 되고, 사용자의 PC나 모바일 단말기에 설치되어야 할 모듈들이 줄어들거나 없게 되다보니 절차가 간단해지고 그 기반으로 다양한 서비스들을 만들 수 있다[5]. 이렇게 사용자의 책임은 제한하되 보호 인증 절차는 강화하는 방향으로 가야, 간편결제 서비스의 신뢰성과 안정성을 바탕으로 충분한 사용자를 확보할 수 있는 전략적 요구사항이 되는 것이다. 최근 시대적 흐름에 따라 국내 모바일 간편결제 서비스가 속속 시장에 진출하고 있으나 확산속도는 예상만큼 빠르지 않은 이유는, 사용자들의 개인정보유출 및 보안에 대한 우려, 오프라인 결제 인프라의 부족,각종 규제 등으로 인하여 사용자의 불신 때문이다[6].이와 같은 간편결제 시장 확대를 위해서는 사용자의 철저한 개인정보보호 관리가 지원되고, 보안상의 안정과 신뢰를 사용자에게 인식시키는 것이 무엇보다도 중요하다고 하겠다[7]. 지금까지 국내 모바일 간편결제와 관련된 기존의 연구들은 대다수가 인터넷뱅킹이나 전자상거래 사업 모델을 이용한 보안 절차를 기술하였으며,모바일 결제의 핵심인 보안 문제에 대해서는 구체적인 개선 방안에 관한 연구가 미흡한 편이었다. 이러한 배경에서 본 연구는 국내 모바일 간편결제 서비스의 활성화를 위하여 마케팅 기술의 다양한 보안 기술과 인증제도에 대해 살펴보고 전략적 방향을 제시함으로써 국내 핀테크 산업 발전의 개선방안을 제안하고자 한다.

본 논문 구성은 다음과 같다. 먼저 2장에서 국내외 간편결제 관련연구를 살펴본다. 3장에서는 국내 간편결제 중 가장 시급한 보안 문제를 기술하고, 4장에서는 국내 간편결제 서비스의 보안 문제점을 해외 사례를 통해서 개선 방안에 대해 제언한다. 결론 및 향후 연구 방향은 5장에서 언급한다.

Ⅱ. 관련 연구

2.1 국내 모바일 결제시장 현황

국내 간편결제 서비스는 결제의 편리성과 빠른 결제 처리속도로 인해 이용자가 꾸준히 늘어나고 있으며, 만족도도 전체적으로 높았지만, 서비스 등록 절차 간편화는 개선점으로 지적됐다. 주로 이용하는 장소는 모바일 쇼핑몰(83.6%)이며, PC쇼핑몰(11.6%)과 오프라인 매장(4.8%)이 뒤를 이었다. 그림 1처럼 시장규모는 '16

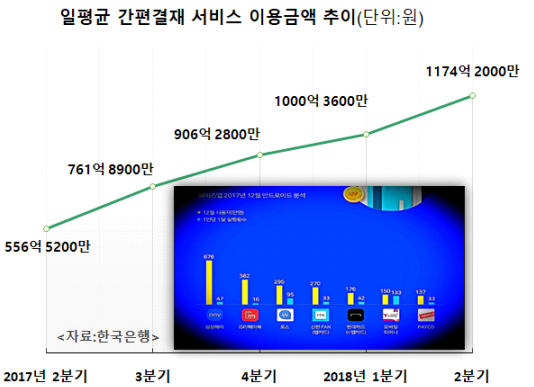

그림 1. 국내 모바일 간편결제 서비스 추이
Fig. 1. Domestic mobile easy payment service trend

표 1. 국내 주요 결제 서비스 및 특징
Table 1. Major domestic payment service and features

명 칭	업체명	주요 특징	가맹점수	출시 시기
네이버페이	네이버	국내 포털사이트 1위, 네이버 회원 누구나 가맹점에서 사용 가능	5.9만	2015. 6
카카오페이	다음카카오	카카오톡 회원 누구나 사용, 메신저를 이용한 선물서비스 강점, 추후 공과금 지불 서비스도 제공	260	2014. 9
케이페이	KG이니시스	전자지불결제 대행서비스업계 1위, 2팩터 인증 '시큐락' 도입 등 보안에 신경	10만	2014. 12
스마일페이	이베이코리아	국내 최대 점유율의 G마켓, 옥션에서 간편하게 결제 가능	G마켓, 옥션	2014. 4
페이나우	LG유플러스	이용자의 휴대폰 번호가 ID역할, 통신 3사 소액 결제 지원, 현대카드 M포인트 결제 서비스 제공	10만	2013. 11
시럽페이	SK플래닛	11번가, 시럽오더 등에서 다양한 상품들 모두 결제 가능, 앱 설치 없이 사용 가능	11번가, 시럽오더	2015. 4
페이올	BC카드	유심(USIM) 방식 사용, 'Token' 방식의 실제 카드번호와 연계된 가상 카드번호로 결제를 진행해 보안에 신경	-	2014. 2
SSG페이	신세계	이마트, 스타벅스 등 신세계 그룹 계열사 9곳에서만 사용 가능한 SSG머니를 충전해 사용하는 방식	신세계 그룹	2015. 7
삼성페이	삼성전자	현재 삼성전자가 출시한 휴대폰 중 갤럭시 S6, S6 엣지, S6엣지+. 갤럭시 노트 등 4종만 사용 가능, 전국 신용카드 가맹점에서 대부분 사용 가능	-	2015. 8

년 11.8조원에서 '17년 40조원 규모로 빠르게 증가하고 있으며, '18년 2분기 이후에도 하루 간편결제 서비스 이용금액이 계속해서 가파르게 증가되는 추세이다[8]. 삼성페이가 기입자 천만 명, 누적 결제금액 18조원('18년 3월 기준)을 넘기며 국내 시장을 주도하고 있으며, 네이버페이, 카카오페이 등이 뒤를 잇는 양상이다[9]. 전체적으로는 시장지배적 사업자가 아직 출현하지 않아 많은 업체들이 다양한 서비스를 내세우며 난립하는 상황이다. 또한, 표 1처럼 회사별로 독자적인 간편결제 서비스를 제공하고 있어 상호 호환이 어려우며, 사장점유율 확대를 위해서는 거액의 마케팅 비용이 소요되므로, 향후 국내 간편결제 서비스 시장은 소수의 지배적인 소수의 사업자 중심으로 재편될 것으로 전망된다[10,11].

2.2 해외 모바일 결제시장 현황

스마트폰의 모바일 간편 결제 서비스란 사용자의 스마트폰 애플리케이션을 이용한 결제서비스로 최초 정보등록 후 모바일 결제 시에 추가정보의 입력 없이 최초 등록한 정보를 이용한 사용자 인증을 통해 안전한 결제를 가능하게 한다[12]. 현재 서비스를 출시하고 있는 회사의 유형으로는 소셜 플랫폼사, 포털사이트, 이동통신사, 은행, 카드사, PG (Payment Gateway)사, 소셜커머스업체 등이, 결제 서비스 기술에는 금융 OTT(Over The Top), P2P 등 이 있다. 이렇듯 모바일 간편결제서비스 시장은 기존 의 금융권뿐만 아니라, 비금융권에서도 적극적으로 참여함으로써 금융거래의 보편화를 앞당기고 있다[13]. 그림2의 시장조사업체인 가트너에 따르면 글로벌 모바일 결제 시장 규모는 2013년 2,400억 달러, 2014년 3,300억 달러, 2015년 4,500억 달러, 2016년 6,200억 달러였으며, 2017년 7,800억 달러(전년대비25.8%증가), 2018년 9,300억 달러(19.2%), 2019년 1조 800억 달러(9.3%)로 2019년까지 연평균 10%씩 성장할 것으로 전망했다[14]. IT 전문 매체인 비즈니스인사이더가 운영하는 BI 인텔리전스 발표 자료에 따르면 미국의 모바일 결제 규모는 오는 2019년까지 5년 동안 연평균 172% 성장하고 결제시장에서 차지하는 모바일 결제의 비중은 2014년 0.1%에서 2015년 1.5%, 2016년 3.8%, 2017년 6.8%, 2018년 10.5%, 2019년 14.8%로 매년 급격히 증가할 것으로 전망된다. 특히 BI 인텔리전스는 애플페이가 초기에 성공을 거두면서 구글월렛 같은 안드로이드 계통 서비스도 동반 상승할 것으로 전망했다. 중국 재정경제부에 따르면, 2010년 4조5000억 위안(약 788조 원)이던 전자상거래 규모는 2014년에 13조 4000억 위안(약 2348조 원)으로 3배 규모로 늘어났다. 매년 30%씩 성장하고 있으며 올해는 15조 위안을 돌파할 것으로 전망된다. 이에 따라 중국의 소매판매액에

서 차지하는 비중이 2004년 0.1%에서 2013년에는 8.0%로 크게 확대되었다[15]. 중국의 인터넷 이용 인구 6억4900만 명 가운데 5억5700만 명이 모바일을 통해 인터넷에 접속하고 있으며 인민은행에 따르면, 중국의 모바일 결제액은 2014년 9조6500위안(전년대비 317.56%성장), 2015년 22조5900억 위안(약 4000조 원)으로 전년대비 134.3% 증가하였으며 2년 연속 100%이상의 신장세를 보였다.

간편결제 서비스는 미국 대형 온라인 거래사이트 '이베이(e-bay)'에서 '페이팔(Paypal)'이 99년부터 간편결제 및 송금서비스를 제공하면서 본격적으로 확산되었다. 간편결제 서비스는 선구자인 미국보다 중국에서 폭발적으로 확산되고 있으며, 이는 양국 간 금융인프라 차이에 기인하며 중국의 간편결제 서비스 시장규모(거래액 기준)는 '16년 58.8조 위안(원화 9,957조원), '17년 98.7조 위안(원화 1경6,700조원) 규모로서, 미국의 80여배에 달하고 있다. 페이팔은 신용카드 정보를 최초 등록 후 간단한 비밀번호 입력만으로 구매및 송금이 가능하도록 함으로써 사용자 편의를 증진시켰다[16].

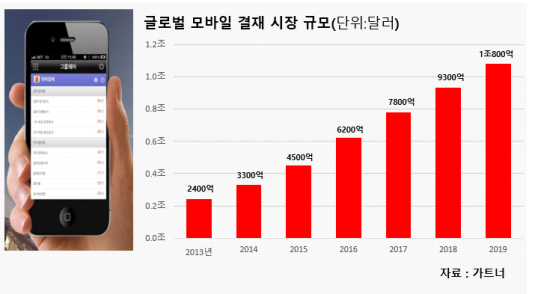

그림 2. 해외 간편결제 서비스 추이
Fig. 2. Overseas Mobile easy payment service trend

Ⅲ. 국내 간편결제 보안 문제점

간편결제의 고속 성장 배경은 결제의 편리성과 처리 속도의 빠름에 있다. 하지만 편리한 만큼 그에 따르는 보안이 보장되지 않는다면, 언제든지 간편결제 과정에서 금융 피해가 발생할 수 있다. 이 장에서는 국내 인터넷 결제 서비스의 복잡성, 오작동 많고 작동 느린 기술적 한계, 사용자에게 책임을 전가하는 국내 금융 시스템, 위조지문 악용 위협에 노출 등 여러 가지 간편결제 서비스 보안 취약사항에 대해 논하고자 한다[17].

① 국내 인터넷 결제 서비스의 복잡성

현재 국내에서 금융관련 서비스, 즉 인터넷뱅킹에서 송금이나 이체를 한다든지, 아니면 인터넷쇼핑을 통해서 물건을 구매하고 결제를 할 때의 사용자 프로세스는 자신의 PC에 여러 개의 ActiveX로 된 보안 모듈을 설치한다. 공인인증서 모듈과 키보드 보안 모듈, 암호화 통신 모듈(보통은 공인인증서 모듈에 포함되어있지만), 그 외에 여러 보안 모듈들이 설치된다. 이들 모듈이 하는 역할은 사용자의 PC와 서비스를 제공하는 서버(인터넷뱅킹, 혹은 인터넷쇼핑 서비스 서버) 사이의 안전한 정보교류를 위한 보안 장치를 맡는 것인데, 해커들이 중간에 데이터를 가로채서 조작한 후 돈이나 배송지를 자신의 계좌나 주소로 바꿀 수 있다. 이는 개인정보보호의 의미도 있지만 해킹으로 인해 내부 정보가 강탈당해도 중요한 카드나 계좌 정보가 노출되지 않도록 하여 2차 피해를 막자는 것도 이유가 되기 때문이다. 해외 서비스의 경우에는 카드 정보를 저장한 다음, 결제를 할 때 이미 저장된 카드 정보를 이용하기 때문에 카드 정보 입력 시 따로 보안을 할 필요가 없다. 하지만 국내는 현행법상으로 이런 보안 장치를 해야 금융관련 서비스를 이용할 수 있다는 것이 사용자 입장에서는 복잡하고 불편하다는 것이다[18,19].

② 오작동 많고 작동 느린 기술적 한계

편의성에만 초점을 둔 간편결제는 금융사기와 같은 금융보안사고 발생 시 이용자의 서비스 이용을 불편하게 하는 보안 모듈 설치를 다시 허용하도록 할 수 있으며, 이 경우 'ActiveX'나 공인인증서처럼 현재 지적되는 문제의 악순환이 거듭될 수 있다. 보안 문제가 심각해지는 경우 그간 금융소비자들을 불편하게 했던 복잡한 규제가 다시 생겨나는 악순환이 일어날 수 있다는 것이다. 그동안 국내 소비자들은 온라인으로 상품을 구입할 때 ActiveX 등 이중·삼중의 보안 프로그램을 설치하는 불편을 감수해야 했다. 이에 대한 소비자들의 반감이 크다보니 간편결제 서비스를 도입한 기업들로서는 편의성 강화에 사활을 걸 수밖에 없고, 그러다 보면 동시에 추구하기 쉽지 않은 보안성 강화에는 소홀해지기가 쉽다. 이와 함께 간편결제가 기술적으로도 더 보완돼야 한다는 지적이 나오며, 기술도 오작동이 많거나 느리게 작동하는 등 한계가 있는 것이 사실이다. 또한, 최근 기업들이 지문 인증에 이어 상용화를 준비중인, 목소리·얼굴 인증을 통한 본인 확인으로 보안성 강화에 신중을 기하고 있다[20].

③ 사용자에게 책임을 전가하는 국내 금융 시스템

국내 금융권 시스템을 얘기하면서 해외에서 얘기하는 핀테크는 현재로서는 어렵다고 얘기를 많이 한다. 이유는

현재의 금융 서비스를 사용하는 패턴 및 시스템 구조, 규제 등이 해외의 그것과는 다르기 때문이다. 국내 금융 서비스는 사용자 인증 및 결제에 필요한 정보를 사용자 쪽에서 제공하고 인증하고 검증하고 책임을 지도록 하고 있다. 인터넷뱅킹을 이용할 때나 쇼핑몰 서비스에서 제품을 구매할 때 보면 수많은 보안 관련 솔루션이 설치가 된다. 이것이 의미하는 것은 국내의 경우에는 사용자 인증 및 검증, 결제 시 확인 등을 사용자가 직접 진행하도록 하고 문제가 생겼을 경우에는 사용자가 직접 책임을 지라는 것을 의미한다. 해외의 경우에는 대부분의 인증 및 검증, 확인 절차를 서비스 서버 시스템이 진행을 한다. 공인인증서의 가장 큰 목적이 부인방지인데 이는 내가 인증했고 내가 사용했다는 것을 문제가 생겼을 때 부인하지 못하도록 하는 역할을 한다. 그렇기 때문에 서비스를 제공하는 서비스 업체보다는 서비스를 제공받는 클라이언트에 보안을 더 많이 생각하면서 이것저것 보안 솔루션들을 많이 설치하게 되고 그것으로 인해 다양한 시스템 환경에 대해서 제대로 대응을 할 수 없는 상황에 이르게 되면서 지금의 핀테크 열풍에 뒤쳐질 수밖에 없는 상황에 오게 된 것이다.

④ 위조지문 악용 위협에 노출

주민등록증 뒷면에 노출된 지문은 국내 대표 앱과 인터넷전문은행, 정부가 운영하는 대표 사이트에서 실험 결과, 위조(불법 복제된)지문을 온라인과 모바일에서도 걸러내지 못하는 것으로 입증됐다. 또한, 인터넷전문은행 송금 서비스도 상황은 마찬가지였다. 위조지문 인증에 제약은 없었다. 악용 가능성의 확률, 즉 여러 조건이 갖춰져야 하지만 위조지문 자체를 걸러낼 수 없는 현 보안체계는 마땅히 개선돼야 한다. 공인인증서와 스마트폰 탈취의 제약조건은 남지만, 해커집단이나 사이버테러의 가능성은 충분하다는 게 업계의 중론이다. 이는 결국 언제든지 뚫릴 수 있고, 다른 해킹 수단(공인인증서 탈취 등)과 결합한다면 대형사고로 이어질 가능성이 남아 있는 것이다. 이 모든 문제의 출발점은 주민등록증에 부착된 지문이며, 지문이 악용될 가능성이 있고, 많은 IT기기와 온라인사이트에서 이를 걸러내지 못하고 있는데서 대안을 찾아야 한다.

Ⅳ. 보안 문제점 개선 방안을 위한 제언

간편결제 서비스는 간편성과 보안성 두 마리 토끼를 잡아야 하지만, 아직은 간편성에만 초점을 맞추어 진행되는 상황으로 전자금융거래에 접근하는 방식이 해외와 다른 국내의 경우, 다양한 보안 기술을 통해서 사용자의 정확한 거래를 유지하기 위한 노력이 있어야 한다. 이 장에서는 이와 같은 해외의 차별화된 보안성 강화 기술을 제언한다.

① 이상금융거래탐지시스템(FDS)

FDS는 지금까지 사용자가 했던 인증 및 검증, 확인 절차를 서비스 서버 시스템이 진행을 하고 본인이 제대로 서비스를 사용하고 있는지에 대한 시스템적 검증 작업을 FDS(Fraud Detection System)가 하도록 한다. 간편결제 시 사기 금융거래나, 이상 금융거래에 관한 데이터나 흐름을 빅데이터로 축적하고 이를 분석하여, 패턴을 추출하고 패턴에서 벗어나는 구매나 결제가 일어났을 경우 해당 구매나 결제를 중지시키고 사용자 인증 작업을 다시 거치게 함으로써 해킹 등으로 탈취당한 계정에 대한이상 거래를 예방하고 서비스의 안정성을 확보 한다. 또한, 금융서비스를 이용할 수 있는 단말과 편리함, 용이성이 높아지면서 자연스럽게 금융거래가 많아지고, 피싱, 파밍, 및 개인정보유출로 인한 이상 전자금융사고 발생률도 더불어서 증가했다. 이를 FDS는 24시간 모니터링을 통해서 사전에 방지하는 보안 시스템이며, 아마존, 알리페이, 페이팔 등에서 딥러닝을 적용한 부정거래탐지시스템으로 사용하고 있다.

② PCI-DSS

우리나라 환경에서는 상당히 불안해 보이는 두 가지 결제 방식이 미국 내에서 널리 사용될 수 있는 이유는 지불결제카드산업(PCI)이 카드회원 정보를 안전하게 취급하기 위해 제시하는 데이터보안표준(DSS)라는 인증 때문이다. 줄여서 PCI-DSS라고 부른다. 아마존 원클릭, 페이팔 등은 모두 PCI-DSS 인증을 통해 정기적으로 보안성에 대한 감사를 받는다. 이를 전제로 간편한 결제 서비스를 구현할 수 있게 한 것이다. PCI-DSS는 일종의 전사적 보안체계로 단순히 ID, 비밀번호를 통한 인증뿐만이 아니라 내부통제, 결제절차가 포함된다. PCI-DSS에 포함된 주요 항목은 보관된 신용카드 정보 암호화, 백신 사용 및 주기적인 업데이트, 단순한 비밀번호 사용금지, 방화벽 구축, 정보접속권한 부여, PC사용자의 개별 ID 및 비밀보호, 신용카드 정보의 물리적 접근 통제, 네트워크 및 신용카드 정보 접속에 대한 체계적인 모니터링, 정기적인 보안시스템 점검 등이다. 또 매년 감사가 이뤄지기 때문에 한번 받고 마는 인증이 아니라 일종의 회계감사 체계와 비슷하며, 페이팔의 경우 자사 서비스에 대한 보안취약점을 알아내 이를 보고했을 경우 보상금을 지급하는 버그바운티 제도도 적용됐다. 원격코드삽입 공격 관련 취약점은 1만 달러, SQL인젝션은 5천달러, 인증우회는 3천달러 식

으로 현상금을 걸어 놓고 있다.

③ SSL(Secure Sockets Layer)

월드 와이드 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 미국 넷스케이프 커뮤니케이션스사가 개발했고, 마이크로소프트사 등 주요 웹 제품 업체가 채택하고 있다. SSL은 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있으며, 인증 암호화 기능이 있다. 인증은 웹 브라우저와 웹 서버 간에 서로 상대의 신원을 확인하는 기능이다. 예를 들면, 웹 브라우저를 사용하는 웹 서버를 사용한 가상 점포의 진위 여부를 조사할 수 있다. 암호화 기능을 사용하면 주고받는 데이터가 인터넷상에서 도청되는 위험성을 줄일 수 있다. SSL 인증서는 클라이언트와 서버간의 통신을 제3자가 보증해주는 전자화된 문서다. 클라이언트가 서버에 접속한 직후에 서버는 클라이언트에게 이 인증서 정보를 전달한다. 클라이언트는 이 인증서 정보가 신뢰할 수 있는 것인지를 검증 한 후에 다음 절차를 수행하게 된다. SSL과 SSL 디지털 인증서를 이용했을 때의 이점은, 통신 내용이 공격자에게 노출되는 것을 막을 수 있으며, 클라이언트가 접속하려는 서버가 신뢰 할 수 있는 서버인지를 판단할 수 있고, 통신 내용의 악의적인 변경을 방지할 수 있다는 것이다.

④ OTP(One Time Password)

미리 정해진 패스워드가 아닌, 특정한 알고리즘에 따라 수시로 생성되는 비밀번호를 이용하는 보안 시스템으로, 같은 암호를 반복해 사용하다가 위험에 노출되는 사고를 줄이기 위해 고안해 냈다. 은행의 인터넷 뱅킹 안전성을 높이는 도구로 쓰이면서 활성화했다. 거래할 때마다 OTP 생성기로 일회용 암호를 만들어 쓴다. 2012년 8월 말까지 1년 9개월여 만에 OTP가 659만 개나 발급됐다. 2013년부터 은행 · 증권사 · 저축은행 등 금융기업별로 제각각이었던 OTP 발급 방식도 인터넷을 통해 손쉽게 등록할 수 있게 돼 이용이 더욱 늘어날 전망이다. 기업용 OTP 쓰임새도 늘어나는 추세다. 회사 밖에서 그룹웨어 같은 내부 정보망에 접속할 때 OTP를 쓰는 곳이 많아졌다. 특히 클라우드 컴퓨팅 체계가 대중화하면서 OTP 수요는 꾸준히 늘어날 것으로 보인다. 다이렉트 뱅킹은 OTP가 필수다. 웬만한 은행들의 오픈뱅킹은 OTP를 강제하고 있으며, 보안카드는 오픈뱅킹에서 계좌 조회만 가능하다. 사용자가 올바른 OTP를 입력하긴 했는데 여러 가지 방법을 써서 정상적인 로그인 과정을 방해한 뒤 해커의 컴퓨터로 올바르게 입력한 OTP를 보낸 후 해커의 컴퓨터에서 사용자의 OTP를 자동으로 대신 입력해서 해커가 로그인한다. 두 번 입력받게 하면 무력화 된다고 한다.

⑤ PIN(Personal Identification Number)

사용자를 식별하기 위해 사용하는 보통 4자리에서 길게는 8자리의 짧은 숫자만으로 이루어진 비밀번호. 한국어로는 개인식별번호이지만 이미 사람들 사이에서는 '핀번호'라고 부르는 게 흔하며, 외국에서도 마찬가지로 PIN이라고 하면 옷핀 같은 핀을 생각하기 때문에 PIN number라고 불러야 알아듣는다. 그런데 이미 약어인 PIN안에 number가 들어가기 때문에 엄밀히 말하면 핀을 핀넘버라고 부르는 건 역전 앞 같은 겹말이다. 대표적으로 은행에서 통장 또는 카드와 함께 본인임을 확인하기 위해 사용한다. 은행에서 말하는 '비밀번호 4자리'가 바로 PIN. 사실 PIN의 첫 출발이 바로 ATM 기기에서 개인을 식별하기 위해 개발된 것이다. 다만 범죄의 수법이 다양해지다보니 직접 은행까지 행차하는 경우가 아니라면 PIN 뿐만 아니라 보안카드나 OTP 등을 더해서 보안성을 높이고 있다. iOS와 안드로이드에서도 기본적으로 지원하는 잠금 방식이다. 윈도우 운영체제도 사용자 PC 비밀번호를 PIN으로 설정할 수 있으며, 디지털 도어락에서도 사용한다. 지금까지 제언한 해외기업의 보안 인증 기술과 간편결제 현황을 표 2와 그림 3에 정리하였다.

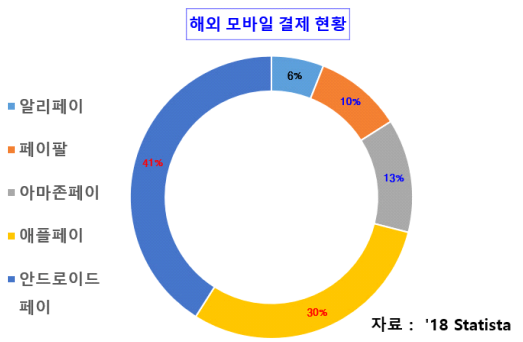

그림 3. 해외 모바일 간편결제 서비스 현황
Fig. 3. Overseas mobile payment service status

표 2. 외국 기업의 다양한 보안 인증 시스템
Table 2. Various security certification system by foreign companies

업체	구글	아마존	알리바바	애플	이베이
서비스명	안드로이드 페이	아마존 페이먼트	알리페이	애플페이	페이팔
결제인증	- 지문인식 - 웹표준 활용(SSL) -PIN 입력	- FDS 실시간 모니터링 - 웹표준 활용(SSL) - id/pwd만 입력하면 원클릭으로 결제 배송 가능	- FDS 실시간 모니터링 (2005~) - PCI-DSS 웹표준 활용(SSL) - OTP 서비스	- 지문인식 - PIN 입력 - NFC로 secure element와 직접통신	- FDS 24시간 모니터링 - PCI-DSS 웹표준 활용(SSL)
출시시기	2015.5	2007.10	2004.10	2014.10	1998.12
특징	- 앱을 통한 실시간 내역 통지 - 결제 데이터 저장 시 최소 2,048bits 암호화 사용 - 미국 시장의 6% 점유	- 모든 정보는 아마존 클라우드 서버에 저장 - 결제 정보 제3자 전달 및 공유하지 않음 - 안면인식 기능 특허 - 미국 시장의 13% 점유	- 제3자 결제 시스템으로 사용자 보호 - 타오바오 등의 자사 대형 유통망 지원 - 신용,보험,자산 관리 서비스 등 제공 - 미국 시장의 41% 점유	- 토큰화 된 결제 정보 보안 요소 - 지문정보 등 보안 구역으로 민감정보 보안 강화 - 애플 스마트폰 사용자가 주로 이용 - 미국 시장의 10% 점유	- 정보유출방지 전담 인력 배치 - 보안과 리스크 관리 인력 배치 전세계 17개 센터 보안 업무 수행 (7,000명) - 피싱사이트 필터링 시스템 운영 - 할부 금융 서비스 제공 - 미국시장의 30% 점유

V. 결론 및 향후 연구방향

최근 스마트폰을 이용한 새로운 모바일 결제방식이 등장하고 지급결제를 편리하게 하기 위한 모바일 간편결제 수단의 중요성은 더욱 증가하고 있다. 하지만 새롭게 진화하는 해킹기술의 대응 미비, 고객에 대한 신뢰성 및 안정성 보장 결여, 국내 인터넷 이용환경의 제도적인 특수성, 사용자들의 개인정보유출이나 결제 인프라 부족 등으로 여러 가지 대응 보안 기술들이 미흡한 실정이다. 현재 국내에서도 간편결제 보안기술이 적용되고 있으나, 여러 개인정보를 입력해야하는 불편함이 사용자를 외면하고 있다. 본 연구에서는 핀테크 서비스 간편결제의 정보보호의 필요성과 FDS, PCI-DSS, SSL, OTP, PIN등 다양한 보안 인증제도를 비교 제언하였다. 본 연구에서 제언한 보안 인증제도가 정책적인 간편결제 활성화 방안과 기업들의 전략적 대안을 제시하는데 가이드라인을 제시함으로써 핀테크산업 활성화에 실질적인 도움을 줄 수 있을 것으로 기대한다. 향후 연구방향으로는 개인정보를 블록체인에 암호화하여 데이터 관리에 무결성을 보장하는 영지식 증명방법(Zero-Knowledge Proof)을 연구한다. 이 방법은 개인정보의 신원을 노출하지 않고 개인정보를 제공할 수 있는 기술로서, 논문에서 언급한 보안 결제인증 방식에 적용하여, 간편결제 보안 기술의 성능을 실험할 것이다.

References

[1] KTFC, "*Major issues and service outlook in the mobile payment market such as biometric recognition,*" 2014.

[2] K. C. Nam, "Case study of EA implementation in the korean public sector: Guidelines, lessons, and future research model," *Informatization Policy*, vol. 22, no. 4, 2015.

[3] S. H. Noh and T. K. Kwan, "A comparative study on the domestic mobile environment simple payment service," *KSMIS,* 2014.

[4] Y. K. Noh, "*Recent Trends and Future Prospects of Simple Payment Service*," KDB Future Strategy Research Institute, Apr. 2018.

[5] I. S. Bae, "*China's rapidly growing mobile payment market reached 4,000 trillion won last year*," Asian state economy, Feb. 2015.

[6] J. H. Suk and S. H. Mun, "Service quality evaluation and improvement plan for mobile

simple payment service," Kyungpook National University Graduate School, Jul. 2016.

[7] J. M. Suk and B. Y. Jung, "Mobile payment security trends and implications," *KSIDI*, vol. 26, Nov. 2014.

[8] J. K. Ahn, "Analysis of domestic fintech trends and mobile payment services: Using text mining techniques," *NIA*, Sep. 2016.

[9] Y. Oh and T. S. Kim, "A study on security and usage intention of mobile simple payment," in *Proc. KICS Winter Conf.*, pp. 54-55, 2015.

[10] J. G. Lee, "Partial revised bill of the Electronic Financial Transactions Act," *Bill Information*, Feb. 2015.

[11] C. K. Lee, "The limitation of simple payment is inconvenient payment if security problems cannot be overcome," *Jmagazine*, Aug. 2015.

[12] H. J. Lee, "Fintech seen as the difference between domestic and international financial security technologies," *Startup's Story Platform*, Jan. 2015.

[13] S. S. Jang, "A study on the impact of fintech on the information security industry," *Internet & Secur. Focus*, 2015.

[14] Etnews, "*Simple payment government website brings fake fingerprints,*" Apr. 2018.

[15] Etnews, "*Comparing the security of major simple payment services,*" Jan. 2016.

[16] K. S. Jung, "A study on activation measures of local mobile easy-to-use payment," *Convergence Secur. J.*, vol. 15, no. 4, pp. 73-82, 2015.

[17] Y. S. Jung, "*Fintech is the future... 8 questions about Samsung Pay,*" *CNBNews*, Apr. 2015.

[18] Chosunbiz, "*Last year, online transactions exceeded KRW 45 trillion,*" Jan. 2015.

[19] Y. Y. Cho and H. W. Kim, "Fintech mobile simple payment service activation plan," *Information Policy Winter*, pp. 22-44, 2015.

[20] Y. W. Choo, "Current status of domestic internet payment service and improvement plan," *KISA*, Mar. 2017.

이 광 규 (Kwang-Kyu Lee)

1985년 2월 : 동국대학교 수학과 학사

1991년 2월 : 동국대학교 수학과 이학석사

2002년 8월 : 충북대학교 전산과 이학박사

1996년~현재 : 신한대학교 IT융합공학부 교수

<관심분야> 인공지능, 정보보안, 빅데이터, 블록체인

[ORCID:0000-0003-0357-9356]