핀테크 서비스 기술과 보안동향 분석

문 성 태* 김 기 남*

◈ 목 차 ◈

1. 서 론

11월 29일 한국카카오은행(이하 카카오은행)과 케이(K)뱅크가 국내 첫 인터넷전문은행 예비인가 사업자로 선정됐다.

두 은행 모두 빅데이터를 활용한 새로운 평가, 결재 시스템을 활용하고, 카톡 및 기존의 공중전화 박스를 활용하여 우리에게 새로운 핀테크 서비스를 제공하려한다.

수익 위기에 빠진(매출부진에 따라) 금융사(은행카드사, PG사 등)는 위기를 극복하기 위해 신규 핀테크 사업모델 발굴에 나서고 있다. 또한, IT기업과 인터넷 스타트업도 핀테크를 새로운 먹거리 창출을 위한 블루오션으로 인식하고 다양한 핀테크 서비스를 개발하고 있다. 글로벌 전자결제 시장의 성장에 맞춰 국내 인터넷 쇼핑몰의 불편한 결제시스템을 해외 쇼핑몰과 같이 간편하고 신속한 결제시스템으로 개선해야 한다는 요구가 높아지면서 핀테크 산업에 대한 관심도 높아지고 있다.[1]

항상 새로운 서비스나 시스템이 나오면 보안문제가 이슈가 되었듯이 핀테크 서비스가 안전하게 지속되려면 개인정보, 금융정보등 중요정보에 대한 보안이 우선되야 할 것이다.

올해 4월 발표한 '유진투자증권' 발표자료에 의하면 "미국의 간편 결제 서비스인 '페이팔'의 부정 사용률은 국내 카드업계의 300배에 이른다" 라고 보도 하는 등 보안 취약성을 우려하고 있다.[2]

또한 간편결재 서비스가 늘어나면서 다양한 보안 기술이 주목받고 있다. 금융 보안 기술은 크게 이용자의 본인 인증과 사업자의 서버 보안 등이 있다.

이용자의 본인 인증은 공인인증서, 휴대폰 인증, ARS 인증 등이 대표적인 예다. 올해 9월부터 공인인증서 의무사용 규정이 폐지됨이 따라 대체 수단에 관심을 가지게 된다.

따라서 본 논고에서는 핀테크 서비스의 유형, 서비스 기술, 핀테크 보안 기술 등을 등을 분석하여 보안 문제를 예방할 수 있고, 보안강화를 위한 제언을 하고자 한다.

2. 핀테크 서비스 유형

2.1 결재, 송금 화폐

핀테크 서비스 분야 중 가장 기본적인 '결제/송금' 서비스는 기존의 인증 과정을 최소화·간편화(단순 PIN 번호 입력 등)하여 편리하고 빠른 결제·송금을 가능하게 해준다.

결재/송금화폐는 온라인으로 거래 가능한 가상화폐로 개인, 기업 간 송금 서비스 등도 제공 가능하며 비트코인과 M-Pesa 등이 있다. 비트코인 사용자는 2,500만 명 이상이며, M-Pesa의 거래량은 케냐 GDP의 43%에 이를 만큼 전자화폐의 실물 경제 영향력이 점차 증가하는 추세이다[3]

국내에는 지난해 9월 다음카카오의 카카오페이 출시를 시작으로, LG유플러스의 페이나우(Paynow), KG이니

* 한국정보보호심사원협회

시스의 케이페이(Kpay), SK플래닛의 시럽페이, 옥션·G마켓의 스마일페이, 티켓몬스터와 LG유플러스의 티몬페이, 인터파크의 옐로페이, BC카드의 페이올(Payall), 네이버의 네이버페이, 비바리퍼블리카의 토스·토스페이, 금융결제원과 다음카카오의 뱅크월렛 카카오 등이 간편결제·송금 서비스를 하고 있다. 또한 갤럭시 프리미엄폰에서 이용 가능한 삼성페이도 출시되어 두 달만에 100만명 이상이 이용중이다.(2015년 10월 현재)

서비스	대표사례	기존 금융업
결제/송금	카카오페이, 페이나우	결제, 송금, 외환
인터넷은행	위어바오, 괴도로 은행	은행업무
크라우드펀딩	와디즈, 텀블벅	대출, 투자, 후원
데이터분석	뱅크샐러드, 민트	자산관리, 세무서비스
디지털화폐	코빗, 비트코인	

(그림 1) 핀테크서비스 분류

2.2 인터넷 은행

'인터넷 은행'은 모든 은행 업무(예금, 대출, 송금업 등)가 오프라인 점포없이 온라인(웹, 모바일 등)만을 이용하여 제공되는 은행을 말한다. 점포 운영비 등을 최소화하는 대신 금융소비자에게 더 높은 이자를 제공하고, 365일 24시간 무중지 운영되는 점 등이 기존 은행과의 차별점이다.

내년 하반기부터 영업을 시작하는 카카오뱅크와 K뱅크의 임직원 규모는 300명 이내로 구성된다고 하니 기존 시중은행의 1~2%인력으로 모든 은행업무를 하는 혁신이 일어나게 된다.

인터넷 전문 은행은 오프라인 상에서 보유하던 모든 개인 정보를 저장·관리해야 하므로 금융소비자정보에 대한 고도의 안전한 관리방안을 마련해야 한다.

또한, 모든 본인인증을 온라인으로 대체해야 하므로 높은 신뢰성을 가진 IT 기반의 본인인증 수단이 필요하다.

2.3 크라우드 펀딩

크라우드 펀딩은 군중을 뜻하는 'Crowd'와 자금조달을 뜻하는 'Funding'의 합성어로 스타트업 기업 같은 신생 기업이 다수의 투자자들에게 소액으로 자금을 조달하는 행위를 의미한다.

크라우드 펀딩법은 후원기부형, 대출형, 투자형 같은 방식으로 스타트업 기업들이 자금을 효율적으로 모을 수 있도록 도움을 주는 법이라고 할 수 있다

즉, 크라우드 펀딩은 아이디어만 있다면 누구든지 온라인으로 다수의 투자자들에게 투자를 받을 수 있으며 소셜 네트워크를 사용한다는 점에 있어서 소셜 펀딩(Social Funding)이라고 말하기도 한다.

대표적인 크라우드 펀딩 사이트로 '텀블벅'이 있다. 텀블벅은 게임 제작, 단행본 제작, 상품 제작, 여행 지원 같은 다양한 형태로 크라우드 펀딩이 진행되고 있다. 크라우드 펀딩을 진행하는 사람은 금액을 모으는 이유, 금액, 모집 날짜를 설정해서 글을 올리고, 지원 금액에 따라 다른 형태로 보상을 받게 된다. 대부분의 크라우드 펀딩 사이트는 '후원, 기부형'의 형태로 이루어진다고 보면 될 것 같다.

크라우드 펀딩 서비스가 확대되기 위해서는 투자금 관리, 이자 배분, 원금 보호 등 펀딩 자금 관리와 관련한 다양한 기준과 모금자·투자자의 개인정보 보호 방안, 거래 무결성 확보 방안 등이 해결되어야 한다.

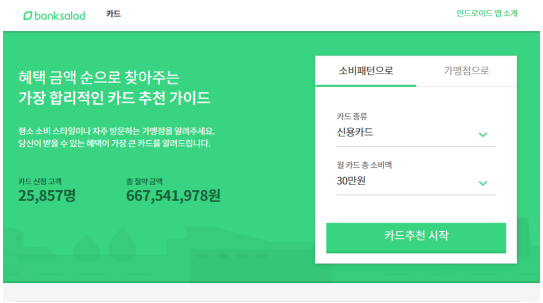
(그림 2) 텀블벅 사이트의 후원현황

2.4 데이터 분석

'금융 데이터 분석' 분야의 핀테크 서비스는 빅데이터(소셜데이터, 소비 패턴 분석, 카드사 혜택 분석, 금융 상품 수익률 등) 분석 기술과 결합하여 개인 자산관리, 신용 리스크 평가, 금융 상품 추천 등을 제공하는 것이다.

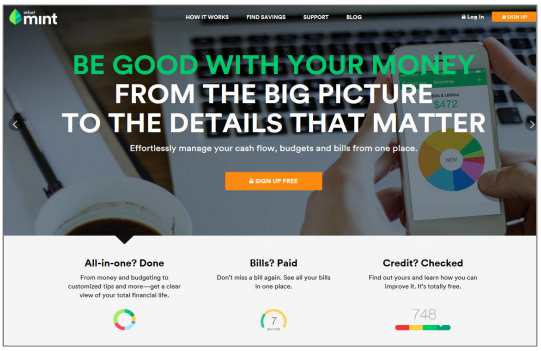
핀테크 벤처기업과 금융권의 상생 모델의 예로 뱅크샐러드라는 사이트가 있다. 개인의 평소 생활 패턴

과 자주 이용하는 상점, 필요한 포인트 혜택, 마일리지 적립 등을 뱅크샐러드 시스템에 입력하면 최적화된 카드가 추천된다



(그림 3) 뱅크샐러드 홈페이지

또한 개인화된 금융 서비스의 성공적인 비즈니스 모델로는 미국의 '민트'가 꼽힌다. 민트는 개인용 금융 계좌 관리 서비스로 사용자가 거래하는 모든 금융 계좌를 한곳에 모아서 관리할 수 있다. 카드사용 내역 등도 취합돼 한 달간 소비가 얼마큼 절약되는 지까지 한눈에 볼 수 있다.



(그림 4) 자산관리 사이트 mint.com

서비스 제공 기업은 금융소비자의 정보를 대용량으로 취급해야 하므로 안전한 정보 관리에 각별한 주의가 필요하다.

3. 핀테크 서비스 기술

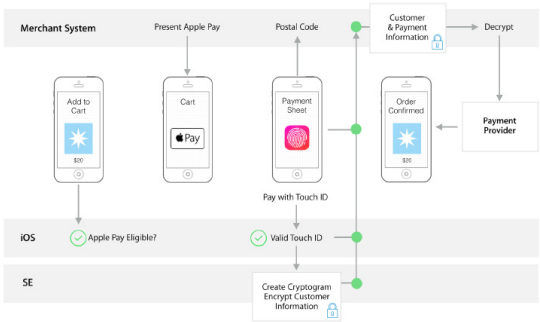
스마트폰과 같이 여러 센서와 통신기술이 탑재된 모바일 기기의 확산으로 인해 다양한 기술을 핀테크 분야에 활용할 수 있는 환경이 마련되면서 각 업체는 시장을 선점하기 위해 다양한 방법과 기술을 도입하여 결제 프로세스를 간소화하고 있다. 대표적으로 NFC, Barcode/QR 코드, Beacon, 모바일 단독카드 등이 있다.

3.1 NFC 결재

NFC(Near Field Communication)는 RFID의 하나로 13.56Mhz 주파수 대역을 사용하는 비접촉식근거리 무선통신 모듈로 10cm의 가까운 거리에서 단말기 간 데이터를 전송하는 기술이다[4]

이 기술은 현재 데이터 전송뿐만 아니라 결재, 출입통제, 잠금장치 등에서 광범위하게 사용되고 있다.

NFC결재는 2014년 'Apple Pay'를 선보이면서 결제에 널리 활용되기 시작했다.



(그림 5) Apple Pay 결제 흐름도[5]

알리페이(Alipay), 삼성페이 등에서도 NFC결재가 사용 가능하다

3.2 Barcode/QR 코드

카드정보를 PG사에 등록하고 결제 시 사용자 스마트폰으로 바코드(barcode)를 출력하여 제시하거나 QR코드를 읽어 결제가 진행되는 방식이다. 바코드의 경우 소비자가 스마트폰으로 바코드를 출력하여 자신의 카드정보를 제시하면 가맹점은 바코드 리더기를 통해 이를 읽고 카드사에 지급승인을 요청한다. 반면 QR코드방식의 경우 가맹점이 상품 정보를 QR코드를 통해 제시하고 소비자는 스마트폰에 설치된 애플리케이션

을 이용하여 QR코드를 읽고 카드사에 지급승인을 요청한다.

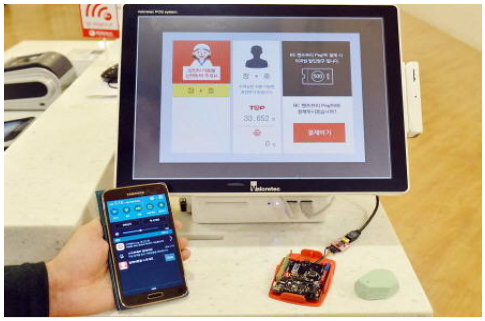
최근에는 스마트워치에 맴버십 카드나, 신용카드를 탑재하여 결재나 포인트 적립등의 서비스로 활용되고 있다.[6]

(그림 6) 스마트 워치의 Barcode

3.3 Beacon

비콘(beacon)은 저전력 블루투스 통신기술을 이용하여 신호를 계속 보내주는 작은 장치이다. 근거리 위치 인식을 적용시킨 무선 감지기다. 카드사들은 고객이 매장에 들어서면 스마트폰에 자동으로 쿠폰이나 할인 정보 등이 뜨게 해 소비를 유도하는 마케팅기법을 도입·추진하고 있다.

하지만 카드사들의 시범사업 결과 블루투스 연동 등 사용자들의 기술적인 경험과 가맹점 단의 인식 부족이 비콘 확산이 지연되고 있다. 혁신적인 서비스의 사용자 경험이 많지 않아 마케팅 기법으로 서비스되고 있지 않다[7]



(그림 7) 카드사 비콘(beacon) 시험서비스 화면

3.4 모바일 단독카드

모바일 신용카드는 유심형(USIM)모바일카드와 앱형 모바일카드 두 가지가 있다. 유심카드는 NFC 기능이 탑재된 안드로이드 OS 전용 단말기에서만 이용할 수있고 앱카드는 안드로이드 OS전용단말기와 애플 IOS전용 단말기에서도 모두 사용할 수 있다. 핀테크의 발달로 대부분의 카드사들은 실물카드를 모바일 기기에 앱을 설치 한 후 서비스를 이용하는 앱카드를 출시하였고. 최근에는 카드사별로 스마트폰으로만 카드결재를 할 수 있는 모바일 단독 카드를 출시하고 있다.[ ]

(그림 8) 모바일단독카드출시현황_아주경제

4. 핀테크 보안 기술

본 절에서는 최근 주목받고 있는 핀테크의 주요 보안기술인 FIDO, FDS, 블록체인 등 핀테크 보안기술 동향에 대해서 알아본다.

〔표 1〕 핀테크 보안기술의 종류

구분	AS-IS	TO-BE
사용자 인증	ID/PW	생체인증 OTP 보안토큰 공인인증서 ICT Tagging FIDO QR코드기반 인증 (위치정보 이용)
결제/뱅킹	ActiveX, Exe	HTML5 등 웹표준 블록체인
모니터링	개별 단위 장비/ESM	FDS
보안인증	-	PCI-DSS ISMS 등

4.1. FIDO

파이도는 아이디와 비밀번호를 입력하는 방식보다 더 강력한 보안성을 제공하면서도 활용하기에 쉬운 인증 서비스다.[9]

온라인 환경에서 생체인식기술을 활용한 인증방식인 FIDO 대한 기술표준을 정하기 위해 2012년 7월 FIDO(Fast IDentity Online) 얼라이언스(Alliance)라는 협회가 설립 되었다. 회원사로 삼성전자, 블랙베리, 크루셜텍, 구글, 레노보, 마스터카드, 마이크로소프트, 페이팔, LG전자 등이 있다.[10]

일반적으로 사용자 인증에 많이 사용되는 ID/PW이 방식은 지식기반 인증방식으로 구분되는데, 별도의 하드웨어가 필요하지 않지만, 사용자들이 각 서비스들의 ID/PW를 기억해야 하는 전통적인 지식기반 인증방식의 문제점이 있다. 최근에는 사용자가 가진 고유한 형태의 신체구조 또는 행동결과 기반의 생체기반 인증방식이 각광을 받고 있다. 사용자가 별도의 인증 토큰을 소유하거나 기억해야 하는 정보가 없기 때문에 사용자 편의성을 제공한다. 그리고 사용자의 고유한 정보를 사용하기 때문에 보안성도 강하다.

최근에 주목받는 FIDO(Fast Identity Online)인증 기술은 스마트폰, 스마트와치 같은 모바일 기기에서 사용하는 패턴, 지문인식, USIM기반 등의 인증기술을 온라인에 적용하는 것을 기본아이디어로 하고 있다.

FIDO인증기술은 패스워드를 사용하지 않고 기기인증을 이용하여 필요에 따라 여러 인증기술을 선택할 수 있어 편리성과 보안을 동시에 만족하는 간편결제에 적합한 기술이다. FIDO 인증은 (그림 9)와 같이, 패턴, 음성, 지문, USIM기반 인식 등 모바일 기기에서 사용하는 간편하고 보안강도가 높은 인증기술을 온라인에 적용하여 사용자가 결제 시 패스워드를 사용하지 않고 기기인증을 이용하여 편의성을 제공하고, 웹 서비스는 필요에 따라 인증기술을 선택할 수 있다. 마이크로스프트, 애플, 구글, 삼성, 페이팔, ETRI 등 세계의 IT기업과 통신사, 결제회사, 연구원 등이 참여하여 앞으로 핀테크의 사용자 인증에 많이 사용될 전망이다.[11]

FIDO 기술 개념도

(그림 9) 보안에서 본 핀테크, 결제에서 본 핀테크

패스워드 인증은 온라인이나 오프라인 간편결제에 활용하기에는 보안 취약성으로 인해 추가적인 보안이 필요하고 이 또한 취약점으로 작용될 수 있다. 이와 더불어 사용자가 단순한 문자열을 사용하여 발생하는 취약점을 보완하기 위해 비밀번호를 자주 변경하게 하거나 특수문자를 요구하는 것은 편의성에 문제가 될 수 있다. 하지만 FIDO 인증기술이나 생체인증 기반 결제방식은 기존에 스마트 디바이스가 가지고 있는 인증방식을 사용하여 사용자 편의성과 보안성을 제공할 수 있다.[11]

파이도에서 가장 주목받는 인증기술은 바로 바이오인식이다. 내 몸이 곧 인증이 되는 바이오인식은 사용자 편의성을 강화하려는 국내 상황과 인증을 강화하려는 해외 트렌드 모두에 적합하기 때문에 파이도의 메인 이슈로 자리 잡았다. 게다가 파이도는 어떤 인증방식이든 추가가 가능하기 때문에 다양한 바이오인식의 발전에도 큰 역할을 할 것으로 보인다.

이미 보편적인 지문인식은 물론 홍채인식과 얼굴인식 등 우리가 익히 알고 있는 바이오인식 기술이 파이도를 통해 핀테크 분야에 접목됐거나 앞으로 접목될 예정이다. 여기에 뇌파, 음성, 필체, 행위인식 등 다양한 인식이 추가되고 있다.

“파이도의 가장 큰 장점은 단말과 서버만 연결이 됐다면, 단말에서의 인증은 어떤 방식이 됐든 어떤 방식이 추가되던 상관이 없다는 점입니다. 예를 들면, 현재 파이도를 지원하는 갤럭시 S6에 지문인식 말고 얼굴인식이나 홍채인식 기술이 추가되면 그대로 인증수단으로 사용이 가능합니다. 또한, 갤럭시 S6 말고도 추가로 파이도를 지원하는 다른 스마트폰이 나왔을 때 은행이나 카드사에서 이를 추가하면 바로 사용할 수 있습니다.”

무엇보다 파이도는 핀테크 분야의 인증수단뿐만 아니라 포털 등 인터넷의 로그인이나 출입통제 등 오프라인 분야에서도 쉽게 사용이 가능하다는 것에서 크게 각광받고 있다. 식당에서 밥을 먹은 후 내 스마트폰으로 카드를 인증한 후 결제하는 게 가능해진다는 것, 지문이나 홍채, 지정맥 등 신체의 일부를 많은 사람들이 사용하는 단말기에 대는 것에 거부감을 느끼는 사람들에게 파이도는 희소식이 될 것이다.[12]

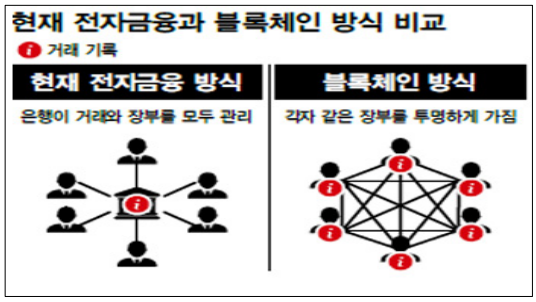
4.2. 블록체인

블록체인은 거래 주체가 일정 시간 단위로 거래정보를 동시에 기록하고 보유하는 네트워크를 뜻한다. 기존에는 금융 거래 시 변동 내역을 금융기관이 승인한 후 금융기관 데이터베이스(DB)에 기록했지만, 블록체인에서는 거래주체들이 내역을 서로 교환해 승인하고 대조하는 방식으로 정보를 확인한다. 중앙 데이터베이스에 거래를 저장할 필요가 없기 때문에 처리속도가 빠르고 비용절감이 가능한 것이 장점이다. 또 모든 승인과정이 자동으로 암호화돼 현존하는 최고의 보안기술로 평가된다.[12]

블록체인은 전세계적으로 통용되는 일종의 공공 거래장부다. 거래가 이뤄질 때마다 블록을 생성해 이를 체인 형태로 정보를 담아 보관하고 저장한다. 특정 서버에 정보가 집중되는 게 아니라 해당 거래를 주고받은 모든 이들에게 거래 정보가 저장되기 때문에 해킹하기 어렵다는 평가를 받고 있다.[13]

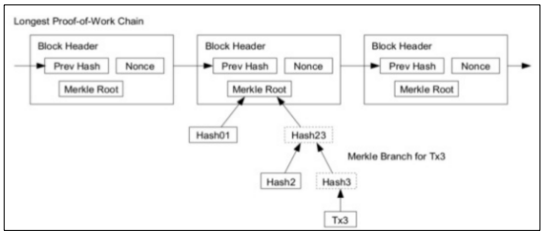
이 기술은 2015년 들어 세계 경제 뉴스에서 자주 등장하고 있다. 세계경제포럼(다보스포럼)은 지난 9월에 기술의 파급효과에 대한 보고서를 발간하면서 블록체인을 앞으로 사회를 뒤바꿀 21개 기술의 반열에 올렸다. 보고서는 “2027년이면 전세계 총생산(GDP)의 10%가 블록체인 기술로 저장될 것”이라고 내다봤다. 또 2023년에는 각국 정부들이 세금을 블록체인 거래로 받기 시작하리라고 봤다. 같은 달 뱅크오브아메리카(BoA), 시티그룹, 모건스탠리, 도이체방크, 홍콩상하이은행(HSBC) 등을 비롯한 22개 세계 은행들은 블록체인 기반 가상화폐 기술을 공동으로 개발하기 위해 ‘R3CEV’라는 벤처기업을 만들었다고 밝혔다.

블록체인이 대체 무엇이기에 이런 관심을 모으는 것일까. 이는 한때 투기 붐까지 불었던 디지털 가상화폐 ‘비트코인’의 핵심 기술로, 이른바 ‘은행 없는 세상’이 오게 할 수 있다는 기대를 모으고 있다. 현재의 금융 시스템에선 사람들이 돈을 주고받으려면 ‘장부’를 기록하고 관리하는 ‘믿을 만한 누군가’가 있어야만 한다. 지금 이런 노릇을 하는 것은 은행을 비롯한 금융기관이다. 은행은 거래의 안전도 보장하고 내용이 기록된 장부도 작성해 보관한다. 이를 위해서 금융거래 정보를 기록하는 거대한 디지털 서버를 관리해야 하고, 해킹 등의 피해를 입지 않게 보안도 유지해야 한다.



(그림 10)현재 전자금융과 블록체인 방식 비교_한겨레

블록체인은 금융거래에서 장부 책임자가 없는 거래 시스템이다. 중앙집권적 은행이 장부를 책임지는 게 아니라 이 거래 시스템에 참여하는 모든 사람들이 같은 장부를 보관하게 된다. 새로운 거래가 발생할 때마다 장부는 이 정보를 별도의 ‘블록’으로 만들고, 이 블록을 기존 장부에 연결한다. 블록이 꼬리에 꼬리를 물게 되니 ‘블록체인’이 된다. 해커가 디지털 장부를 조작하려 해도 이용자가 수천만명, 수억명이라면 흩어져 있는 장부를 한꺼번에 조작할 수 없기 때문에 상대적으로 안전하다. 결국 블록체인 기술이 앞으로 주요 금융시스템으로 자리 잡는다면 은행의 존재가 없어도 개인끼리 스마트폰으로 전자화폐를 주고받는 시대도 상상해볼 수 있다.



(그림 11) 블록 체인의 구조_ETRI

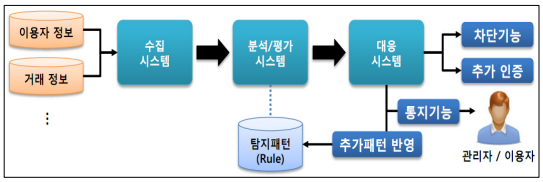
이는 금융시스템이 블록체인을 통해 파격적인 비용 절감을 얻을 수 있다는 얘기가 된다. 현재의 중앙집중적 시스템에선 모든 거래 기록과 개인정보를 저장하고 있는 중앙의 보안이 매우 중요하다. 금융 범죄자들은 이 보안시스템을 뚫기 위해 온갖 신기술을 끊임없이 개발한다. 금융회사들은 이를 방어할 기술에 막대한 비용을 투자하고 있다. 전자상거래가 더욱 확대되고 사물들까지 거래를 주고받는 사물인터넷(IoT) 시대가 다가오면 비용은 더 치솟을 수밖에 없다. 영국 <파이낸셜 타임스>는 블록체인을 적용하면 전자금융 서비스 비용에서 단기적으로 연간 20억달러(약 23조원)를 절감할 수 있으리라고 내다봤다.

하지만 핀테크 시대의 총아로 떠오른 블록체인에 온통 장점과 장밋빛 미래만 있는 것은 아니다. 올해 1월 정보기술 전문 매체인 <더 버지>와 인터뷰를 했던 마이크로소프트(MS)의 창업자 빌 게이츠는 블록체인 기술을 1차적으로 현실화했던 비트코인에 대해 두가지 문제를 지적했다. 첫째는 잘못된 거래를 되돌리기 어렵다는 점이다. 게이츠는 “사람들은 잘못된 계좌로 돈을 보냈으면 전화를 걸어서 복구해 달라고 하기 마련인데, 이 경우에는 (전화를) 걸 곳이 없다”고 말했다. 장부 책임자가 없는 블록체인 시스템의 약점이다. 다른 하나는 분산형 시스템이 지닌 익명성과 정부 통제의 충돌이다. 그는 “이 거래가 마약 대금인지, 세금을 매겨야 하는 거래인지 등 정부가 알고 싶어하는 것들이 많은데 이를 확인하기 쉽지 않다. 거래량이 임계치를 넘어가면 문제가 될 것”이라고 짚었다.

또 블록체인 기술은 구조적으로 뛰어난 보안성을 보여줬지만, 운용 행태에 따라 빈틈은 발생한다. 2014년 2월 세계 3대 비트코인 거래소로 꼽히던 일본의 마운트곡스(Mt.GOX)가 갑자기 문을 닫는 일이 벌어졌다. 해킹으로 하루아침에 74만4천 비트코인(당시 시세로 약 4128억원)을 잃었기 때문이다. 블록체인 기술을 썼는데 어떻게 이런 일이 벌어졌을까? 전문매체 <테크크런치> 보도를 보면, 공격자는 허브형 거래소인 마운트곡스가 실제 거래 요청에 따라 비트코인 송금을 했는데도 마치 안 된 것처럼 블록체인을 착각하게 만들었다. 결국 이 거래소는 수많은 거래에서 같은 송금을 두차례씩 보내게 되면서 큰 피해를 입게 됐다. 이 회사는 이런 허점에 대비한 자체 확인·회계 시스템을 마련해 두지 않았던 터라 파산에 이르렀다. 결국 2013년 말에 개당 1000달러를 넘었던 비트코인 시세는 이런 사고 등으로 거품이 꺼지면서 2014년 말 400달러 밑으로 곤두박질쳤다. 일본 마운트곡스의 사례는 핀테크의 미래가치에 섣불리 흥분만 하고 근본적인 기술혁신과 보안투자엔 인색한 한국 금융계에도 많은 시사점을 남긴다.[15]

4.3. FDS

FDS는 부정거래탐지 기술로, 카드회사 및 온라인 게임에서 이상거래탐지 및 봇 탐지에 많이 사용됐다. 핀테크 분야에서는 모바일 결제에서 사용자 인증을 간단히하여 사용자의 편의성을 제공하는 대신, 거래의 안전성을 FDS를 이용하여 보장한다. 그리고 온라인 결제에서 사용자의 이체/거래내역이 정상거래인지 부정거래인지를 탐지하는 데 사용하여 피싱/파밍에 대응하고 있다. 국내 금융사들도 작년부터 FDS를 도입해 오고 있으며, 한 금융사는 최근에 FDS로 인해 파밍사기를 탐지하여 부정거래를 사전에 차단할 수 있었다[11]



(그림 12) FDS 구성요소와 주요기능_금융보안원

하지만 FDS도 위협 요소들을 가질 수 있다고 제기되고 있다. 예를 들어, FDS의 구성요소인 사용자 스마트폰의 수집정보를 메모리에서 복제하여 다른 기기에 재사용하여 FDS의 탐지패턴을 우회하거나 피해자가 가해자로 둔갑할 수 있다. FDS의 경우 아직 초기 단계로 운영 및 관리경험이 부족하고 부정거래를 제대로 탐지하는데 많은 시간이 소요되고 취약성 점검 기준 및 시험 방안이 아직 마련되지 않았다. 또한, 부정거래탐지를 위해서는 사용자로부터 여러 정보를 얻어야 하는데, 이때 개인 프라이버시 문제도 고려되어야 할 사항이다.[10]

효율적인 FDS 운영에는 '다양한 패턴 축적'과 오탐율 최소화 '분석 및 운영능력'이 필요하다. 금융업계에 따르면 사기범 범죄수법은 갈수록 진화하고 있어 이를 방어하기 위해서는 다양한 패턴을 통해 사전에 인지하고 막는 것과 분석능력을 강화해 오탐율을 최소화하는 노력이 필요하다는 것.

많은 경험이 필요한 패턴축적은 일개 회사가 '경우의 수'를 확보하기는 쉽지 않아 업계 공유가 꼭 필요한 부분이다. 또한 단말기를 통한 자동화 차단은 탐지율을 강화하는 측면이 있지만, 100% 오탐율을 막는다고 보장할 수 없다. 거래 패턴이 미묘하고, 복잡한 부분이 있어 사람이 개입돼야 하지만, 24시간 365일 모니터링을 하면서 탐지한다는 것이 그렇게 만만치 만은 않은 작업이다.

고객과 직접 접촉하는 FDS는 오탐에 의한 민원이 발생할 소지가 있어 신중하게 접근해야하는 부분이다. 업계에서는 FDS가 활성화되기 위해서는 패턴 공유를 통해 서로간의 시너지를 높이고, 오탐율을 최소화 할 수 있는 분석 능력을 강화하는 것이 필요하다고 강조하고 있다.

주요 증권사의 FDS 도입 예산은 평균 1~3억 수준에서 진행하고 있다<아래 표 참조>.

주요역할/금융기업	KB국민은행	NH투자증권	현대증권
FDS 예산	N/A	2억5천	1억4천 (4월 오픈)
조직및 인원	정보보호본부주관/6명	정보보호본부주관/3명	보안팀/4명
주요업무	1. 기기정보 기반차단 2. 거래행태 분석위한 업그레이드 3. 오탐율 최소화	1. 패턴 설정 및 탐지 2. 다양한 패턴 분석	1. 이체요구 대응위한 개인별 단말정보 실시간 수집 2. 고객별 프로파일링 생성 3. 거래정지문자 실시간확인 4. 이상거래 모니터링
주요 활용분야	1. 고객행태 분석 1. 외부침입시 분석후 임계치를 보고 조치 2. 패턴 정립후 임계치를 넘기면 바로 차단	1. 모니터링 2. 패턴에 의한 이상거래 탐지	1. 이상거래 탐지 및 차단 2. 오탐 방지 위한 전담인력 분석역량 강화
업계 활성화 방안	당장 불편해도 추가 인증불편을 감수할 수 있는 고객인식 제고 필요	사회적 홍보를 통해 FDS로 따른 불편을 이해할수 있는 공감대 형성 필요	업체간 패턴 공유에 따른 시너지 확보 필요
올해 계획	1. 사기거래 판단역량 강화 2. 고도화 및 담당직원 마인드 교육	1. 고도화에 따른 시스템 오픈 2. 최적화 작업 지속 진행	1. 4월 시스템 오픈 2. 패턴 분석 따른 안정화

(그림 13) 주요 금융사 FSD 현황-1

주요역할/금융기업	유안타증권	롯데카드	<요약>
FDS 예산	6억원 미만(솔루션 및 프로젝트 비용포함)	N/A	2억5천~6억원
조직및 인원	보안팀/2명	FDS 전담조직/40명	2~40명
주요업무	1. 이상징후 탐지 2. 징후 발생시 사전정지 3. 징후에 대한 분석	1.FDS 시스템을 통한 부정거래 선별 2. 선별된 거래 모니터링해 회원 본인 사용여부 확인	1. 이상징후 탐지 2. 징후 발생시 차단 3. 이상거래 모니터링 4. 본인여부 확인
주요 활용분야	1. 계좌이체시 실시간 탐지 2. 정상거래 모니터링	1. 부정거래 시도규모 파악 2. 부정거래 차단해 손실방지 3. 온오프라인 금융거래 탐지	1. 모니터링 2. 임계치 설정 3. 오탐방지 위한 분석역량강화 4. 이상거래 탐지
업계 활성화 방안	은행과 증권사간 대포통장 및 부정발급계좌 공유로 위협요소 사전방지 필요	부정거래 정보공유 및 공유된 정보 활용체계 구축 필요	1. 업계간 패턴공유 필요 2. 불편감수하는 사회적 인식 필요
올해 계획	1. FDS 패턴발기 2. FDS 고도화	동업계 공조, 분석역량강화	패턴 최적화 및 고도화추진

(그림 14)주요 금융사 FSD 현황-2

NH투자증권은 2억5천, 현대증권은 1억4천만원 규모이다. 유안타증권은 6억원 규모이다. 솔루션 외에도 프로젝트 비용 부분까지 포함이다. 기업의 규모나 업무 속성, 또는 전담인력 및 비 전담인력의 혼용 등으로 조직의 규모는 보안 팀 소속으로 적게는 2명, 많게는 40명까지이다.

KB국민은행은 정보보호본부 주관 하에 6명이며, NH투자증권은 정보보호부 산하 3명이 관장하고 있다. 현대증권은 보안팀 내에서 4명이다. 유안타증권은 보안팀 소속으로 2명이 관리하고 있다. 통상 30~40명 인원을 갖고 있는 카드사와는 대조적이다.[16]

4.4. 공인인증서 2.0

금융권에서 공인인증서 의무사용이 폐지되면서 사용자들과 관련 업계에서 나오는 반응은 두 가지다. 여러 문제에도 불구하고, 이미 오랫동안 사용돼 온 공인인증서를 보완해서 그대로 사용할 지, 아니면 새로운 인증방식이 등장한다면 이러한 방식을 적극적으로 사용하겠다는 것이다.

최근 한국인터넷진흥원(KISA)과 주요 공인인증서 관리 업체들, 이동통신 3사, 일부 은행들은 공동으로 공인인증서를 안전하게 쓸 수 있는 방법을 안내하는 캠페인을 벌였다. 기존에 보안에 취약하고, 불편한 방식을 개선했다는 뜻에서 공인인증서2.0 혹은 PKI2.0이라 불리는 방식이 그것이다.[8]

이들은 공인인증서를 공개된 NPKI폴더를 사용하지 않과 안전한 저장매체를 사용하도록 다음의 방법을 권고 하고 있다.

1) 보안토큰(HSM)
   별도의 안전한 매체에 공인인증서와 개인키를 저장하고 결과값만 외부에 전송하는 방법, 하지만 별도 매체를 항상 휴대해야 한다
2) 스마트폰 USIM
   USIM칩 내 안전한 저장소에 공인인증서와 개인키를 저장해 보안토큰처럼 활용하는 방식이다. 이동3사가 서비스 중이지만 사용자들은 많지 않다.
3) 은행 OTP
   은행들이 발급하는 OTP카드에 저장한 뒤 스마

트폰의 NFC 기능을 사용해 해당 카드를 터치하는 방법이나 이 역시 활성화는 미비하다

4) 공인인증기관의 안전디스크
공인인증기관에서 제공하는 디스크에 인증서와 개인키를 저장하는 방식이다.

그 외에도 공인인증서를 불러오기 위해 비밀번호를 입력하는 대신 FIDO표준 기반 지문인증을 사용하는 방식을 개발해 내년부터 도입을 검토하고 있다.

5. 결 론

본 기고에서는 현재 서비스되고 있는 핀테크 유형을 결제/송금, 인터넷은행, 크라우드 펀딩, 데이터분석으로 분류하여 설명하였고, 핀테크 기술을 NFC결제, 바코드/QR코드, 비콘, 모바일 단독카드로 나누어 설명하였다

그리고, 핀테크 보안기술에서는 사용자에게 편의성을 제공하는 인증수단으로서 최근 많은 연구와 각광을 받고 있는 FIDO와 비트코인에서 사용하고 있는 현존 최고의 보호기술로 평가되는 블록체인, 부정거래 탐지 기술인 FDS 및 의무사용이 폐지된 공인인증서를 추가 보완하여 사용하는 방법을 설명하였다.

핀테크 보안기술이 계속 발전하고 경쟁에 따른 보안서비스의 변화가 예상되는 만큼 금융, ICT, 정보보호 업체의 발전을 촉발하며 투자 확대를 기대해 볼 수 있겠다.

또한 국내에 핀테크 기술을 활용한 여러 서비스를 제공하여 사용자들에게 편리함을 제공하는 것은 바람직해 보인다. 하지만, 지속적으로 증가하는 보안위협에 적극적으로 대응할 있도록 FIDO 등 위에서 열거한 다양한 보안 기술들을 융합하고 활용하여 금융보안 거버넌스 체계를 구축하는데 필수 요소가 되어야 한다.

참 고 문 헌

[1] 임재석, “핀테크 보안동향 ”, TTA Journal vol.158, 쪽, 2015.

[2] 헤럴드경제, http://news.heraldcorp.com/view.php?ud = 20151112000540&md=20151115003528_BL

[3] 이성훈외, “핀테크 기술 및 보안동향”, 전자통신동향분석, vol 30. No 4, 2015.

[4] 위키백과, https://ko.wikipedia.org/wiki/NFC, 2015.12

[5] Getting Started with Apple Pay, 2014 Apple Inc.

[6] 블로그, 페블 타임(Pebble Time) : 바코드 표시 페블앱, ’Skunk’, 2015.11

[7] 한국금융신문, 우리카드, 비콘 시범사업 실시 2015.07

[8] ZDNetKorea, 공인인증서 2.0 시대, 뭐가달라졌나 2015

[9] ciokorea, 아이디·비번 방식 대안 ’파이도’(FIDO) 규격 확정… ″쉽고 편한 인증 시대 열린다″, 2014.12

[10] 위키백과, FIDO 얼라이언스,

[11] ETRI, 핀테크 기술 및 보안동향, 2015.08

[12] 보안뉴스, 핀테크 보안 등 인증 분야 다크호스, FIDO 기술, 2015.09

[13] 디지털타임스, 금융권 ’블록체인’ 도입 박차, 2015.12

[14] 블로터, 비트코인, 블록체인, 핀테크 기술 한자리에, 2015.12

[15] 한겨레, 세계 금융권력은 왜 ’블록체인’에 열광하나, 2015.12

[16] ciociso매거진, 금융기획|FDS 도입현황과 과제, 2015.03

[17] slideshare, Bitcoin 기술분석, 17쪽, 2013.12

◐ 저 자 소 개 ◑

문 성 태

2009년 고려대학교 컴퓨터정보통신공학과 석사(수료)
2015년 ~ 현재 한국정보보호심사원협회 이사
관심분야 : 정보보호 컴플라이언스, 개인정보보호, ISMS, PIMS, 빅데이터, SIEM

김 기 남

2009년 연세대학교 전산정보학과 석사
2015년 ~ 현재 한국정보보호심사원협회 이사
관심분야 : 보안기술, ISMS, PIMS, 정보보호 관련 법률