Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1475

거래당사자간 합의에 기반하는 온라인 전자금융 2-WAY 거래인증 모델 제안

이 익 준,† 오 재 섭, 염 흥 열‡
순천향대학교 정보보호학과

Proposal for 2-WAY Trade Verification Model that Based on Consensus between Trading Partners

Ig-jun Lee,† Jae-sub Oh, Heung-youl Youm‡
Department of Information Secuirity Engineering, Soon Chun Hyang University, Korea

요 약

금융 회사 전자금융 거래 시 송금인이 수취인에게 자금을 이체할 경우 송금인은 출금 계좌 번호와 출금 금액 그리고 금융 회사에 사전 등록한 비밀번호 또는 금융 회사가 사전에 배부한 인증 매체에서 제공하는 정보 등 이용자 인증 정보를 입력하여 계좌 이체를 수행한다. 그러나, 현재 이러한 금융 회사와 송금인간 발생하는 이용자 인증 중심의 단방향 거래는 착오 송금 또는 보이스피싱 사기 거래 등 사고 위험에 노출되어 있다. 따라서, 본 연구에서는 송금인과 금융회사 이외 수취인과도 자금 이체 거래 시 거래 내용을 공유하여 수취인이 확인 후 응답하면 이체가 성립될 수 있도록 상호합의가 가능한 온라인 전자금융 2-WAY 거래인증 모델을 제안한다 기존 단방향 전자금융 거래 이체 방법을 양방향 거래 방법으로 개선하여 착오 송금, 보이스피싱 사기 예방 이외 대여금 거래, 계약 거래 등 다양한 용도로 활용하여 금융 회사 계좌이체 거래 이용자의 불편 감소 및 편리성 강화와 금융 회사의 P2P거래 활성화 등의 기대효과를 창출하고자 한다.

ABSTRACT

To verify remitter's identity when the remitter transfers money to a recipient using an electronic financial service provided by the financial institution, the remitter inputs the information; such as the withdrawal account number, the withdrawal amount, the password pre-registered with the financial company, or the information from authenticating medium that is previously distributed by the financial institution. However, the 1-Way transaction between the financial institution and the remitter is exposed to a great risk of accidents such as an anomaly remittance or a voice phishing fraud. Therefore, in this study, we propose a 2-WAY trade verification model for electronic financial transaction that can be mutually agreed by allowing the recipient to share the transaction information with the remitter and the financial company. We have improved the traditional electronic financial transaction's method by replacing it to 2-WAY trade method, and it is used for various purposes; such as preventing an error within the remittance or voice phishing fraud, enhancing loan transaction and contract transaction, etc. Through these variety of applications, we are expecting to reduce the inconveniences while improving the convenience of financial transaction and vitalizing the P2P transaction of financial institution.

Keywords: Authentication, transaction authentication, voice phishing fraud, error remittance

Received(09. 27. 2018), Modified(1st: 10. 19. 2018, 2nd: 11. 15. 2018), Accepted(11. 15. 2018)

† 주저자, leemsjij@gmail.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

I. 서 론

금융 회사에서 사용하는 이용자 인증은 비대면 거래에서 이용자 신원을 확인하는 과정이고, 전자서명 인증은 전자서명법에 근거해 전자문서의 안전성과 신뢰성을 부여하기 위한 제도"라고 정의한다. 그러나, 현재 금융회사의 전자금융거래에서 이용자 인증은 단지, 이용자 시스템 접근권한에 만 중점을 맞춰 거래내용에 대한 확인은 송금인이 모든 책임을 지도록 하는 구조로 되어 있어, 송금인 실수에 의한 착오송금이나 수취인을 사칭한 사기거래에 취약한 단점이 있다. 또한 전자서명인증은 송금인과 금융회사와의 전자금융거래에서 사용되고 있어 거래내용에 대한 확인은 수취인 참여 없이 송금인이 최종 확인하도록 구성되어 있다. 따라서, 본 논문에서는 강력한 이용자인증 또는 전자서명인증으로 막기 어려운 전자금융거래 착오송금 또는 사기거래를 예방할 수 있는 2-WAY 거래인증 방법을 제안함으로써 전자금융거래의 안정성을 높이고자 한다.

II. 관련연구

2.1 전자금융거래 정의

전자금융거래법에서는 전자금융거래를 '이용자가 전자금융업무(금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융 상품 및 서비스를 제공하는 것)를 비대면의 자동화된 방식으로 이용하는 거래'로 정의(제2조제1호)한다. 전자적 장치를 통한다는 말은 금융 상품 및 서비스를 전자적 장치를 통하여 제공한다는 것으로 이용자가 비대면으로 전자적 장치를 통하여 금융상품 및 서비스에 직접 접근할 수 있게 하는 정도에 이르러야 함을 의미한다[1].

또한, 인증(authentication)은 현재 온라인상에서 상대하는 이용자가 그 사람인지를 확인하는 이용자 인증과 메시지의 위변조 및 진위 여부를 확인할 수 있는 메시지 인증으로 구분된다. 먼저, 이용자 인증은 아이디 및 비밀번호, 일회용 비밀번호, 인증서, 생체 인증 등의 다양한 인증 수단으로 구현된다. 메시지 인증은 PKI 인증서를 이용한 전자 서명 수단으로 구현된다.

2.2 이용자 인증 및 거래 인증 기술

전자금융거래에서 사용되는 인증 방법으로 '지식기반 인증', '소지기반 인증' 그리고 '특성 기반 인증'과 '행동 기반 인증' 방법이 있다[2].

2.2.1 지식기반 인증 유형

지식기반 인증방법은 사전에 공유한 정보를 이용자가 발급자에게 제출하고 발급자가 검증함으로써 인증을 수행하는 것이다.

1) 비밀번호
   - ㅇ 이용자와 발급자가 서로 공유한 비밀번호 또는 비밀정보로 인증하는 방법
   - ㅇ 일반적으로 이용자가 비밀번호를 생성하여 발급자에게 등록하고 발급자가 생성한 후 이용자 에게 제공하는 방법이 있음

2) 문답식 인증
   - ㅇ 발급자가 질의 내용을 보여주고, 이용자는 사전에 등록한 질의에 대한 응답 값을 입력하여 인증하는 방법

3) 이미지 인증
   - ㅇ 이용자가 사전에 선택하여 등록한 이미지를 보여주거나, 다수의 이미지 중에 특정 이미지를 선택하도록 하여 인증하는 방법

2.2.2 소지기반 인증 유형

소지 기반 인증 방법은 이용자(금융회사 고객)가 소지하고 있는 인증 디바이스를 활용하여 발급자(금융회사)가 이용자를 인증하는 방법을 의미한다. 보안카드, OTP(One Time Password) 그리고 두 개의 다른 채널을 이용해 서로가 거래사실을 확인하는 OOB(Out Of Band)인증 방법이 있다.

최근에는 스마트기기가 발달하면서 등록된 스마트폰 등 스마트 기기를 활용한 소지 기반 인증 기술이 활발히 이용되고 있다.

(1)OOB(Out Of Band) 인증
   - ㅇ 전화 인증: 이용자가 사전에 등록한 전화번호로 전화를 걸어 정당한 이용자임을 발급자에게 인증하는 방법으로, 서비스방식에 따라 거래내용을 통지하고 인증번호를 입력받는 등 다양한 방법으로 구현 가능.

○ 스마트폰 앱 인증: 이용자가 사전 등록한 스마트폰 앱을 통해 정당한 이용자임을 발급자에게 인증하는 방법으로, 서비스 방식에 따라 거래내역을 통지하고 인증번호를 입력받는 등 다양한 방법으로 구현 가능.
○ 이메일 인증: 이용자가 사전에 등록한 이메일을 통해 정당한 이용자임을 발급자에게 인증하는 방법으로, 서비스 방식에 따라 거래내역을 통지하고 인증번호를 입력받는 등 다양한 방법으로 구현 가능.
○ SMS 인증: 이용자가 사전에 등록한 휴대폰에 문자(SMS)로 인증 정보를 전송하면, 이용자는 이를 전자금융 거래화면에 입력하여 정당한 이용자임을 발급자에게 인증하는 방법

(2)OTP(One Time Password) 토큰
○보안카드: 발급자는 비밀번호와 지시자(Index)가 인쇄된 신용카드 크기의 보안카드를 이용자에게 발급하고 이용자는 거래 시 발급자가 요구하는 지시자(index)에 해당하는 비밀번호를 입력하여 인증하는 방법으로 일회용 비밀번호 방식이나 300~350개의 인쇄된 비밀번호 내에서 반복 이용 함.
○비밀 번호 목록: 발급자는 비밀번호를 종이에 인쇄하여 이용자에게 배포하고, 이용자는 비밀번호를 입력하여 인증하는 방법으로 한번 사용된 비밀번호는 재사용되지 않음.
○S/W OTP 발생기: 이용자와 발급자가 서로 공유한 OTP 생성 키를 이용하여 1회만 사용 가능한 비밀번호(OTP)를 생성하고 이를 전자금융거래 시 전달 또는 입력하여 인증하는 소프트웨어 방식의 인증 방법으로 일반 OTP의 거래정보(예: 수취인 계좌번호, 송금금액)와 연계된 거래 연동 OTP로 분류함(거래 연동 OTP는 거래인증 기능 제공).
○H/W OTP 발생기: 이용자와 발급자가 서로 공유한 OTP 생성 키를 이용하여 1회만 사용 가능한 비밀번호를 생성하고 이용 전자금융 거래 시 전달 또는 입력하여 인증하는 하드웨어방식의 인증 방법으로 일반 OTP의 거래정보(예:수취인 계좌번호, 송금금액)와 연계된 거래연동 OTP로 분류(거래 연동 OTP는 거래인증 기능 제공).
○혼합형 OTP 발생기: H/W OTP 발생기와 유사한 방식으로 IC카드 등의 하드웨어 장치에서 안전하게 생성한 OTP를 스마트폰 등을 활용하여 출력하고 인증하는 하드웨어와 소프트웨어 혼합 방식의 인증 방법으로 일반 OTP의 거래 정보(예: 수취인 계좌 번호, 송금금액)와 연계된 거래연동 OTP로 분류(거래연동 OTP는 거래 인증 기능 제공).

(3) PKI(Public Key Infrastructure) 토큰
○일반 저장장치 보관 인증서: 인증기관을 통해 발급된 인증서의 개인키를 소프트웨어 방식으로 PC등에 저장하고 거래 내역에 대해 전자서명하여 인증하는 방법.
○H/W 보안 토큰: 인증기관을 통해 발급된 인증서의 개인 키를 하드웨어방식으로 HSM 등에 저장하고 거래 내역에 대해 전자서명하여 인증하는 방식으로 H/W 보안 토튼과 보안 토큰에 입.출력 장치를 포함한 거래 확인 토큰으로 분류.
○혼합형 보안 토큰: H/W 보안 토큰과 유사한 방식으로 IC 카드 등의 하드웨어 장치에서 안전하게 생성한 전자서명을 스마트폰 등을 활용하여 전달하고 인증하는 하드웨어와 소프트웨어 혼합 방식의 인증 방법.

(4)기타
○IC 카드 인증: 현금카드 등의 IC 카드에 인증을 위한 키를 안전하게 보관하고, 이를 이용하여 이용자를 인증하는 방법으로 거래 정보(예: 수취인 계좌 번호, 송금금액)와 연계되어 인증된 인증 정보 생성 시 거래 인증 기능 제공.
○신용카드 인증: 신용카드 정보(카드번호, 유효 기간, CVC 등)을 이용하여 인증하는 방법으로 주로 전자결제나 온라인 이용자 인증 수단으로 활용.

2.2.3 특성기반 인증 유형

특성 기반 인증 방법은 생체 기반 인증 방법이라고도 하며 이용자의 생체 정보를 활용하여 이용자를 인증하는 방법을 의미 한다. 또한, 생체 인증을 위

해 반드시 다뤄야 하는 기술이 생체 인식 기술이다. 생체인식 기술에서 요구하는 사항은 누구나 가지고 있는 생체의 특성을 이용하여야 한다는 '보편성(universality)'과 각 개인마다 고유한 특성이 있어야 하는 '유일성(uniqueness)' 그리고, 변하지 않고 변경이 불가능해야 하는 '영속성(permanent)'이 있어야 하며, 기술적으로 생체인식 시스템의 센서에 의한 획득과 정량화가 용이해야 하는 '정량성(collectable)'을 필요로 한다. 그리고, 생체 인식 시스템은 데이터 수집 • 전송 • 신호처리 • 데이터 비교 • 의사결정 • 저장을 기본 구성요소로 하고 있다.

(1) 지문/홍채/얼굴/정맥 인식

○ 이용자의 생체 정보(지문, 홍채, 얼굴, 정맥 등)를 추출하여 정보화한 후 등록하고, 이를 이용하여 이용자를 인증하는 방법으로 일반적으로 생체 정보를 이용자단에서 저장.검증하는 로컬 모델과 서버 단에서 자장. 검증하는 센터 모델위주로 사용된다.

2.2.4 행동기반 인증 유형

행동 기반 인증 방법은 이용자의 행동 패턴(서명, 키보드입력 등)의 특징(압력, 속도 등)을 추출하여 정보화한 후 등록하고, 이를 이용하여 이용자를 인증하는 방법으로 서명 패턴, 키보드 입력 패턴 등이 있다. 이러한 인증 방법의 이용은 인증 정보를 단일로 사용하는지 복합적으로 사용하는 지에 따라 단일 인증(Single Factor Authentication)방법과 다중 인증(Multi Factor Authentication)방법으로 나눈다. 단일 인증은 위에서 정의한 이용자 인증 정보 중에 하나의 인증 정보만으로 이용자를 인증하는 방식이며, 다중 인증은 2가지 이상의 인증 정보를 결합하여 이용자를 인증하는 방법을 말한다. 대부분의 전자금융 거래 서비스 에서는 다중 인증을 선택하고 있다.

마지막으로, 금융 회사에서 주로 사용하는 인증 방법으로 주인증과 추가 인증으로 구분할 수 있다. 주인증 방법은 이용자 인증이나 거래 인증을 하기 위해 주된 방법으로 사용하는 인증으로 전자금융거래에서는 비밀번호, 공인인증서, OTP, 보안카드가 주로 사용되고 있다. 그 외 고액 등 거래에 대한 보조적인 인증방법으로 전화, 이동전화를 이용한 추가 인증 방법이 있다

Table 1. Types of Authentication

Division	Certification Systems	Explanation
Primary Authentication Method	Password	User Authentication with Knowledge-based Password
	PKI Token	User Authentication and Transaction Authentication using Public Key Certificate, a PKI Token
	OTP	Disposable Password Generator of S/W or H/W
	Security Card	List of Passwords printed with a Fixed Number of Passwords
Supplementary Authentication Method	SMS, ARS	Authentication by Phone or Mobile Phone

2.3 전자 서명 인증 기술

전자서명이란 서명자가 해당 전자문서에 서명하였음을 증명하기 위해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말하는데 서명자의 개인 키를 암호화하여 전송함으로써 구현할 수 있다. 개인 키는 본인만이 소유하고 있는 것으로써 개인키와 한 쌍을 이루는 공개 키로만 복호화가 가능하다. 개인 키를 이용해서 암호화 하는 것(전자서명)은 제3자가 데이터를 열지 못하게 하기 위한 방법은 아니며 상대방에게 자신을 가장한 제3자가 아닌 진짜 자신이 보낸 메시지라는 것을 알려주기 위한 방법일 뿐이다. 그리고, 무결성이란 전송된 데이터가 변경/파괴/위조되지 않은 상태를 말하며 공개키 암호 기술에서는 이를 보장하기 위하여 Hash 함수를 이용한다. Hash 함수는 '단방향 함수'로써 원본이 1비트만 변경되어도 2개의 문서는 서로 다른 결과 값을 가진다는 특징을 가지고 있다. 원본 데이터를 Hash 함수를 이용하여 계산하여 나오는 값을 Digest라고 하며 전자서명 시 이용하는 데이터는 '원본 데이터 + Digest'가 된다. 마지막으로, PKI의 주요기능으로 암호화를 통한 정보보호 (비밀유

지)를 하는 기밀성 기능과 선택된 송금인이 정보에 접근할 수 있는 기능인 접근 제어 기능 그리고, 데이터의 위.변조를 방지하는 무결성과 전자 서명 기능을 이용한 인증 및 부인 방지 기능이 있다. 그리고, 이용자는 공개 키 PKI의 최종 이용자로 인증서와 비공개 키를 소지하고 있고, 인증서는 일종의 전자신분증으로 개인을 구별할 수 있는 정보와 공개키 및 부가적인 관리 정보가 포함되어 있다. 이러한 인증서는 HDD, FDD,CD-Key, Smart Card 등에 저장이 가능하다.

공개 키 암호 기술을 기반으로 하는 전자 서명 알고리즘은 안전·신뢰성의 보장을 위해 기본적인 요구사항을 만족해야 한다. 즉, 전자서명 알고리즘은 전자서명 검증에 사용되는 전자서명 검증 키로부터 전자서명 생성에 사용되는 전자 서명 생성 키가 계산되는 것이 실행 불가능해야 하며, 전자 서명은 메시지 내용, 서명자의 전자 서명 검증 키, 그리고 이용자 정보에 의존되어 생성되어야만 한다.

전자 서명은 전자적 거래에 있어서 발생할 수 있는 거래 당사자의 신원 확인, 거래 내용 및 시점의 확인, 송수신 부인방지, 내용의 비밀 보장, 외부의 임의적 접근 제어 등을 가능하게 한다. 즉, 비대면성, 글로벌성, 개방성을 지닌 전자적 거래를 위해서는 거래 참여자간의 신뢰가 전제되어 있어야 하는데 전자서명은 이러한 문제에 대한 해결책을 제시하고 있다. 정보사회에서 익명성이 증가함에 따른 신원 확인을 위한 기술적인 방법이 전자서명인데 전자서명은 서명한 메시지의 송신자 인증 및 서명된 문서의 무결성을 입증할 수 있기 때문에 증가된 익명성에 대응하는 효과적인 기술적 수단이 된다[3].

2.4 착오 송금 사례

전자금융거래를 하는 A씨는 B의 계좌로 송금하려고 ATM기에 계좌번호를 입력하던 중 착오로 이름이 비슷한 B의 계좌로 잘못 입금하였다. 또한, X회사를 운영하는 C는 직원에게 거래처 Y회사에 물품대금 1천만 원을 송금하도록 지시하였으나, 직원이 계좌이체 중 실수로 예정 거래처 Z사의 계좌번호를 입력하여 Z사 계좌로 대금이 입금되었다. 그리고, 휴가철을 맞아 가족들과 여행을 떠난 갑은 토요일 아침, 휴가지로 차를 몰고 가족과 출발하였는데, 예약한 숙박업체로부터 숙박비가 입금되지 않았다는 연락을 받고, 숙박비 자금이체를 잘못한 사실을 인지하였으며, 착오 송금을 어떻게 돌려받을 수 있을지 막막한 상황이며 이러한 송금인에 의한 착오 송금 사례 빈번하게 발생하고 있다.

Table 2. Status of Error Remittance(Amount)

(unit: Transaction, million won, %)

Division		2013	2014	2015	2016	2017	Average
Return charge	Amount	59,958	57,097	61,429	82,942	92,469	70,779
	Price	222,345	145,200	176,134	180,446	238,575	192,540
Not Returned	Amount	29,758	29,323	31,986	47,078	52,105	38,050
	Price	74,152	67,636	90,065	97,412	111,533	88,160

최근 인터넷 뱅킹이나 모바일 뱅킹 등 간편하게 송금할 수 있는 기능이 많이 활용되면서 2017년도 9만2469건(2385억7500만원)이 착오 송금 반환 요청이 있었으며, 이중 5만2105건(56.3%, 1115억3300만원)이 반환되지 않았다. 또한 송금 기능이 있는 금융 회사 전체로 확장할 경우 지난해 총 11만7000여건(2930억원)의 착오 송금이 있었고, 약 6만 건이 반환되지 않은 것으로 조사됐다[4].

이러한 착오 송금을 예방하기 위해 금융감독원에서 제시하는 주요 대책은 다음과 같다.

첫째, 마지막 이체 버튼을 누르기 전에 수취인명과 수취은행, 계좌번호, 금액을 다시 한번 확인한다. 둘째, 자주 이용하는 계좌, 즐겨찾기 계좌 등을 활용하여 이체한다, 셋째, 지연이체 등 송금인이 송금 시 최소 3시간 이후에 수취인 계좌에 일정시간 이후 입금되는 '지연 이체 서비스'를 활용하여 잘못 송금한 경우 취소할 수 있는 시간적 여유를 가질 수 있는 서비스이다.

2.5 보이스피싱 사기 사례

대부분 보이스피싱은 대출빙자형, 정부기관사칭형 또는 가족이나 친구, 직장 동료 등 지인을 사칭한 카카오톡 메신저 피싱과 소액 결제 문자 메시지로 보이스피싱을 유도하는 유형이 있다. 특히, 메신저 피싱 사기범들은 카카오톡, 페이스북 메신저, 네이버 밴드, 네이트온 등 메신저 ID를 도용해 대화창을 통해 지인에게 돈을 요구해 편취하는 수법을 쓰고 있다. 이들 대부분은 급히 거래처에 결제해야 하는데 카드 비밀번호 오류로 보내지지 않는다는 식으로 타인 계좌로 이체를 요청했다.

Table 3. Examples of Voice Phishing Scams

(unit: one hundred million won, person, transaction, %)

Division	2015	2016	2017		2018 first half		Variations(Rate) (B-A)	
				First half (A)	(B)	Day Average		
Amount of damage	2,444	1,924	2,431	1,038	1,802	10.0	764	(73.7)
Number of victims	32,764	27,487	30,919	12,433	21,006	116.1	7,573	(56.4)
Number of damage	57,695	45,921	50,013	22,051	30,996	171.2	8,945	(40.6)

그리고, 2018년 상반기 보이스피싱 피해 금액은 1802억 원으로 지난해 상반기 보다 73.7%(764억 원) 증가했으며 피해자는 2만1006명으로 56.4%(7573명) 늘었고 하루 116명이 10억 원(1인 평균 860만원)의 피해를 입는 상황이다[5].

또한, 경찰청 자료에 따르면 보이스피싱 피해금액과 건수가 증가 추세에 있다. 이러한 보이스피싱 사기를 예방하기 위해 대책으로 금융감독원에서 다음 5가지 대책을 제시하였다. 첫째, 지연이체 등 송금인이 송금 시 최소 3시간 이후에 수취인 계좌에 일정시간 이후 입근되는 '지연이체서비스'를 활용하여 사기로 송금한 경우 취소할 수 있는 시간적 여유를 가질 수 있는 서비스이다. 둘째, 입금 계좌 지정서비스는 미리 지정한 계좌로는 자유롭게 송금이 가능하지만 미지정 계좌로는 1일 1백만 원 이내로 소액 송금만 가능하게 한 서비스 이다. 셋째, 단말기 지정서비스는 봉닝이 미리 지정한 PC, 스마트폰 등에서만 이체 등 주요 전자금융거래가 가능한 서비스이며 넷째, 해외 IP 차단 서비스는 국내 사용 IP 대역이 아닌 경우 이체를 할 수 없도록 차단하는 서비스이다. 다섯째, "가족이나 지인이 메신저로 송금을 요구하면 반드시 전화로 확인하고 통화할 수 없는 상황 등을 들어 본인 확인을 회피하면 응하지 않는 방법이 있다.

III. 선행 연구와의 차이점

이용자 인증이라 함은 누가 어떤 기록에 어떤 조치를 취할 수 있는가를 미리정한 바에 따라, 기록이나 기록 관리 시스템에 접근하는 사람의 접근 자격을 확인하는 절차를 가리킨다. 전자 기록에 대한 허가 받지 않은 접근과 로그인의 전자 기록에 대한 허가받지 않은 접근과 그로 인한 기록의 훼손 · 변조 · 삭제를 막는 무결성 확보 전략 중의 하나이다. '인증(authentication)'은 기록 관리에서는 '진본 확인'이라는 의미를 갖지만, 전산 환경에서는 시스템에 대한 이용자의 접근 권한을 설정하고 접근 자격을 확인한다는 의미로 사용되는 경우가 더 많다. 본 논문은 개인과 금융 회사간의 전자 금융 거래에서 본인 여부 확인 용도로 만 사용되는 이용자인증 수단과 개인과 금융 회사간 송금 거래 내용에 대한 전자서명을 통해 거래내용을 인증하는 전자인증 거래와 같이 송금인에게 일방적인 책임을 묻는 현재의 단방향 거래 방식으로는 착오 송금 또는 보이스피싱 사기 거래를 예방하기에는 한계가 있다.

그리고, 현재 금융 회사에서 이야기하는 거래 인증 유형은 SMS 인증, OTP(S/W, H/W 혼합형)를 이용한 거래 인증과 공인인증서(S/W, H/W 보안 토큰, 혼합형)를 이용한 거래 인증이 있으나, 전자 금융에서 거래 내역 즉, 이용자와 전자 금융 서버 구간에서 처리되는 수취인 이름, 수취인 입금 계좌 번호, 금액에 대해 무결성을 보장하고 부정거래를 방지하기 하여 전자금융 거래사실에 대해서만 부인방지 기능을 제공하고 있다.

따라서, 본 연구에서는 전자금융 거래의 보안을 강화하기 위해 송금인과 금융회사간 거래 내용인 수취인명, 수취인 계좌번호, 금액 이외 송금인과 수취인간의 거래 목적 즉, 계약거래, 대여금거래, 개인간 직거래 등 거래용도를 전자적 수단으로 수취인에게 내용을 알리고 동의를 받는 방식의 2-WAY 거래인증 모델을 제안한다.

IV. 전자금융거래의 2-WAY 거래인증 모델

4.1 2-WAY 거래인증 개념

현재 전자금융거래에서 사용하는 인증방법은 금융회사와 송금인 사이에 금융회사가 사전에 대면으로 확인한 내용과 송금인이 온라인상에서 제시한 내용이 맞는지를 금융회사가 확인하는 송금인과 금융회사간의 인증절차이다. 이러한 인증은 사기 등 위험거래에서 거래의 불법을 확인하는 수단으로 미흡하다. 특히, 대법원판례[6]에서 기존 계좌이체 거래내역 만으로 송금사실은 인증되나 대여사실에 대해서는 인증할 증거가 부족하다는 취지의 원고(송금인)의 상고를 기각한 사례가 있다.

따라서, 금융회사는 이체 거래에서 송금인이 거래

용도 및 조건을 제시하고 거래 당사자인 수취인이 최종 확인하는 거래인증 절차를 통해 송금사실 뿐아니라 이체거래 용도 또는 조건에 대해 증빙력을 갖춘 2-WAY 거래인증을 적용할 필요가 있다.

거래인증에서 전자적 수단을 이용한 '거래행위'에 대한 법률적 정의는 다음과 같다. 전자금융거래법에서는 전자금융거래는 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

전자상거래 등에서의 소비자보호에 관한법률에서는 "전자상거래"란 재화나 용역을 거래할 때 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래방법으로 상행위를 하는 것을 말한다.

또, "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성, 송신·수신 또는 저장된 정보를 말한다. "전자문서는 SMS문자 또는 e-mail 등이 해당 된다. 전자상거래(EC: Electronic Commerce)는 "전자적 방식을 이용하여 전자공간(cyberspace)상에서 이루어지는 거래행위"라고도 정의할 수 있다.

그리고, 전자문서교환, 이미지처리, 바코드사용, 전자우편, PC통신, 업무흐름 관리체제, 전자화폐 및 전자자금이체, 인터넷과 통신망 등 전자적 기술과 수단이 모두 동원될 수 있으며, 이 중에서도 특히 전자문서교환(EDI: Electronic Data Interchange)은 전자상거래를 위한 핵심요소이다.

현재, 전통적인 이체 거래는 송금인의 출금 요청을 금융 회사가 인증 수단을 통해 확인하여 송금인이 요청하는 입금계좌로 입금처리가 되는 금융회사와 송금인간 1-WAY거래 유형이다.

이러한 당사자가 이용자와 금융회사인 일방향(1-WAY)거래 유형으로는 대출 거래 또는 금융상품 가입과 같은 거래가 해당된다.

그러나, 이체거래에서 일방향(1-WAY)거래는 엄밀하게 말하면 '거래행위'로 정의하기에는 부족함이 있다. 그 이유는 이체거래에서 당사자는 송금인과 수취인이므로 당사자간의 전자거래 성립요건을 만족시키기 위해 거래행위 당사자 인적사항, 당사자가 합의 내용대로 합의하였다는 취지의 확인(verification) 내용 등이 포함되어야 한다.

따라서, 송금인과 수취인간 합의가 필요한 이체거래인 경우 전자상거래의 핵심 요소인 전자 문서를 통해 거래 내용을 수취인에게 통지하고 수취인이 거래 내용을 확인한 후 승인 의사를 전자 문서로 회신받을 경우 최종 입금 처리하는 전자금융거래의 확장 유형인 '2-WAY 거래인증'을 제안한다.

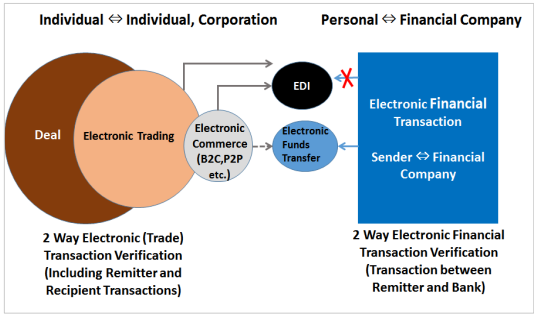

Fig. 1. Comparison of Electronic Financial Transactions and e-Commerce Composition

또한, '2-WAY 거래인증'은 이용자 인증 4대 요구사항인 식별(identification), 인증(authenticatoion), 인가(authorization), 책임추적성(accountability)을 충족한다. 식별(identification)은 시스템에게 주체(subject)의 식별자(ID)를 요청하는 과정으로 각 시스템의 이용자들은 시스템이 확인할 수 있는 유일한 식별자(예, Login ID)를 가져야 하고, 이러한 이용자의 식별자는 각 개인의 신원을 나타내기 때문에 이용자의 책임추적성(accountability) 분석에도 중요한 자료가 된다.

따라서, 개인 식별자는 반드시 유일한 것을 사용해야 하고, 공유되어서는 아니므로, 송금인과 수취인의 전화번호로 식별할 수 있다. 인증 및 인가 단계에서 금융회사와 사전 절차에 따라 등록 및 배부한 접근매체를 통한 인증(authenticatoion)을 수행하고, 송금인 인가(authorization)는 전자 금융거래 원장의 출금 계좌 번호에 접근할 수 있는 주체의 자격을 이름, 아이디, 비밀번호 등으로 검증할 수 있으며, 수취인 인가(authorization)는 거래정보를 전송한 휴대폰에 접근할 수 있는 주체의 자격을 휴대폰 명의 확인 절차로 검증할 수 있다.

그리고, 책임추적성은 송금인의 경우 금융 회사 본인인증 절차를 통과하였으므로 책임추적이 가능하고, 수취인은 본인의 휴대폰으로 문자 통지한 거래내용을 확인 후 본인의 휴대폰 문자로 바로 회신하기 때문에 발신 번호와 회신 번호를 통해 책임추적이 가능하다.

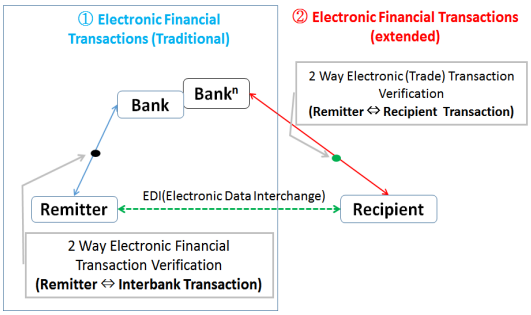

Fig. 2. Concept of 2-WAY Trade Verification

Fig. 2.는 2-WAY 거래인증 개념을 정의한 것이다. ①기존 전자금융거래에서 이체거래는 금융회사가 제공하는 인증수단을 이용하여 송금인을 인증하는 일방향 거래방식이다. 그러나, ②송금인 또는 금융회사에서 수취인 동의 또는 확인이 필요한 거래(조건부 이체, 착오송금예방, 보이스피싱예방 등)에 대해 송금인이 금융회사를 통해 수취인에게 전자문서 형식으로 거래 용도 또는 조건을 안전하게 전달하는 인증 수단인 2-WAY 거래인증을 이용하여 기존 이체거래 영역을 개인간(P2P) 전자거래 영역으로 확대가 필요하다.

4.2 2-WAY 거래인증 시스템 구성

2-WAY 거래인증 시스템 구성은 금융 회사 전자금융 거래 시스템이 구축되어 있는 전산 센터 내에 송금인과 수취인이 거래 내용의 상호합의 프로세스를 처리 하는 2-WAY 거래인증 시스템과 송금인과

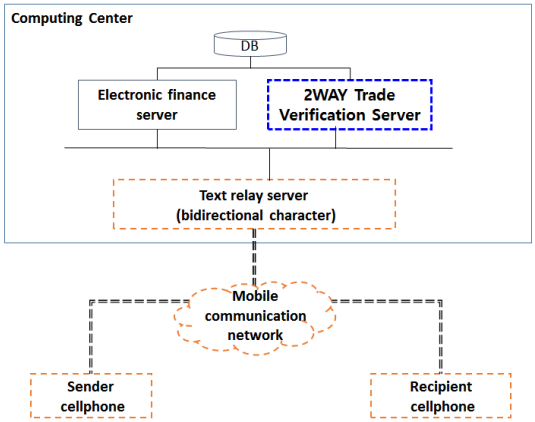

Fig. 3. Diagram of 2-WAY Trade Verification System

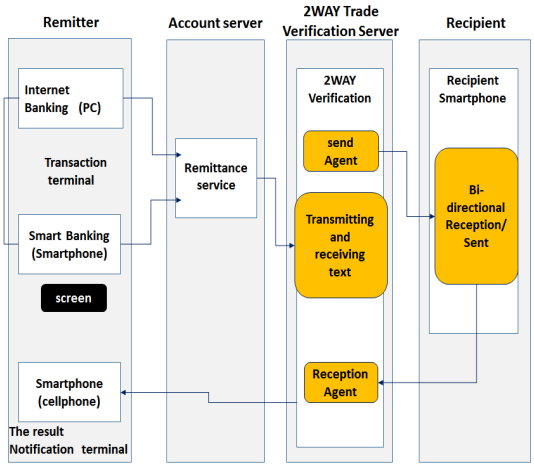

Fig. 4. Interfacre Configuration for 2-WAY Trade Verification

수취인 사이에 전달 수단인 SMS 문자 서비스를 처리하는 SMS 문자 발·수신 시스템으로 구성한다.

또한, 시스템간 인터페이스는 송금인의 거래 단말에서 금융회사로 요청하는 모듈과 금융회사 2 거래인증 서버에서 수취인에게 통지 및 회신 받는 모듈 그리고, 송금인에게 통지하는 모듈을 서로 인터페이스로 연결하여 모듈간 정보의 이동 경로로 활용한다.

4.3 2-WAY 거래인증 처리 절차

2-WAY 거래인증 모델에서 보이스피싱 예방 이체와 송금인과 수취인간 이체거래 내용 상호합의 거래를 처리 위한 절차는 다음과 같다.

첫 번째, 2-WAY 거래인증 주체인 송금인과 금융회사 고유 기능인 이체처리 및 내역을 보관하는 업무서버가 있으며 수취인 전화번호 명의 확인, 양방향 SMS문자 발·수신 프로세스 관리와 거래인증용 일회용번호 생성 및 확인을 수행하는 2-WAY 거래인증 모듈 그리고 수취인과 송금인에게 SMS문자를 통신사로 발송하고 발신 전화번호로 응답처리를 수행하는 문자 발·수신 서버가 있다.

두 번째, 2-WAY 거래인증 상세 처리절차는 다음과 같이 수행하며 Fig. 5에 도식화 하였다.

①(송금인) 이체거래 요청(보이스피싱 예방이체, 수취인거래 내용 확인 이체)

○기본정보 입력:출금계좌번호, 출금비밀번호(지식/소지/특성기반 등), 출금금액,입금

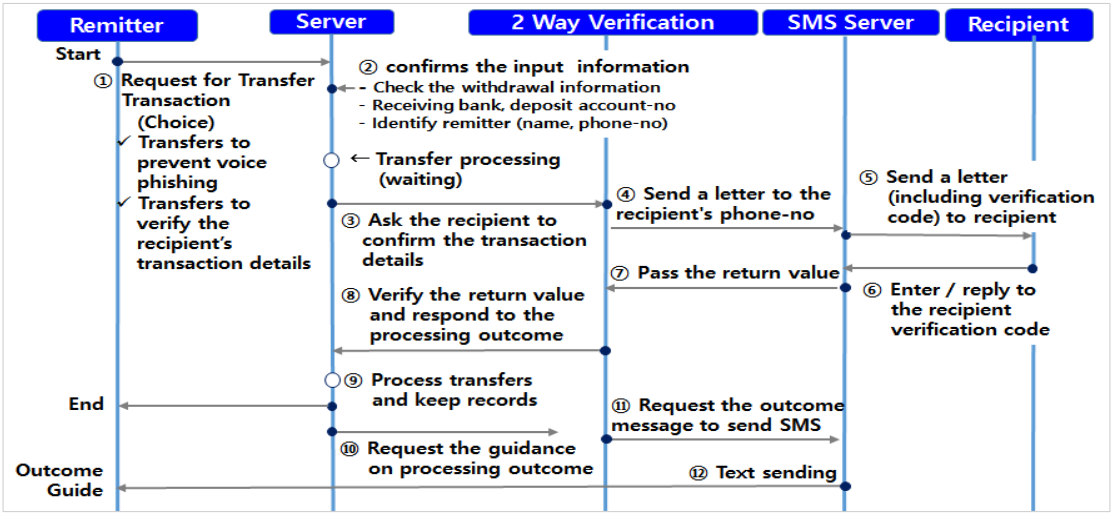

Fig. 5. Process for 2-WAY Trade Verification Procedure

계좌번호,입금은행

○ 2-WAY 거래인증 정보 입력:수취인 전화번호, 이체 용도 및 조건

②(업무서버) 송금인 입력정보 확인

○기본인증 정보: 출금계좌번호, 출금비밀번호, 입금은행,입금계좌번호, 수취인명

○ 2-WAY 거래인증 정보:수취인 전화번호 명의 확인(2-WAY 거래인증 모듈 연계)

③(업무서버->2-WAY 거래인증 모듈)

○ 수취인 전화번호로 송금인 전달내용 문자 발송 요청

④(2-WAY 거래인증 모듈->문자 발·수신 서버)

○ 수취인 전화번호로 SMS 문자 발송 요청 (일회용 인증코드 포함)

⑤(문자 발·수신 서버->수취인)

○ 수취인 전화번호로 SMS 문자 발송

⑥ (수취인) 송금인 전달내용 확인 후 일회용인증코드 입력(SMS문자로 응답)

⑦ (문자 발·수신 서버->2-WAY 거래인증 모듈)

○ 수취인 회신값 전달

⑧ (2-WAY 거래인증 모듈->업무서버)

○ 수취인 회신값 검증 및 처리결과를 업무서버로 응답

⑨ (업무서버)

○ 이체처리 및 내역(2-WAY 거래인증 처리내용 및 결과 포함)보관

⑩ (업무서버->2-WAY 거래인증 모듈-> 문자 발·수신서버)

○ 처리결과 안내요청

⑪ (2-WAY 거래인증 모듈문자 발·수신 서버)

○ 처리결과 안내문 SMS 발송 요청

⑫(문자 발·수신 서버->송금인)

○ 처리결과 SMS 문자발송

4.4 2-WAY 거래인증 적용 서비스 유형

전통적인 금융회사 전자금융 제공 서비스는 예금조회, 이체, 대출 등의 기본적인 금융 서비스 외에도 계좌 통합 서비스, 기업간 전자상거래(B2B:Business-To-Business) 결제 서비스 등의 금융 서비스도 제공하고 있다. 또한 전통적인 전자 매체에서부터 스마트폰, 태블릿 PC 등 새로운 전자 매체의 등장으로 소액 간편 지급 서비스, 개인간 송금(P2P: Person-to-Person) 등 보다 다양한 금융서비스 제공이 가능하게 되었다. 본 논문에서 제안한 2-WAY 거래인증은 자금이체를 이용한 개인간 송금(P2P) 거래에 가장 적합한 형태로 구성되어있다.

4.5 2-WAY 거래인증 적용 사례

2-WAY 거래인증 모델의 실효성을 확인하기 위해 모 저축은행에서 기존 모바일뱅킹 계좌이체 거래외 보이스피싱 예방이체 거래와 상호합의 이체 거래를 추가하여 시범적으로 적용하여 보았다.

Fig. 6, Fig. 7, Fig. 8 은 지인 사칭 등 보이스피싱 사기를 예방하기 위한 이체 화면으로 절차는 다음과 같다.

첫 번째, 송금인이 계좌이체 시 사기가 의심될 경우 '보이스피싱 예방이체'를 선택하고 수취인의 전화번호를 입력하면,

두 번째, 금융회사에서 수취인에게 전자문서 수단인 SMS 문자를 이용해 동 거래가 보이스피싱 등 사기 거래인 경우 수취인은 형사처벌을 받을 수 있다는 내용을 전달한다.

세번째, SMS문자를 받은 수취인이 사기가 아닌 정상 거래로 동의한 경우 수신 문자에 포함된 일회용 번호를 SMS문자로 발송함으로써 거래 이루어지진다.

만약, 수취인이 사기범인 경우 SMS 문자 발신번호가 금융 회사에 전달됨으로써 사후 추적이 가능한 거래이다. 또한, 본 거래절차는 송금인 실수에 의한 착오송금 예방도 가능하다.

Fig. 9, Fig.10, Fig.11 은 송금인과 수취인 당사자간 자금이체 용도 및 거래 조건에 대해 상호합의가 필요한 경우 2-WAY 거래인증 모델을 이용한 이체화면 이다.

첫 번째, 송금인은 자금이체 용도 및 조건이 대여금 성격인 경우 "상호합의 이체에서 대여금 용도"를 선택하고 수취인에게 전달할 조건과 상환 날짜 및 수취인 전화번호를 입력하면

두 번째, 금융회사에서 전자문서 수단인 SMS 문자를 이용해 동 내용을 수취인에게 전달한다.

세 번째, 수취인이 동 내용에 동의한 경우 합의

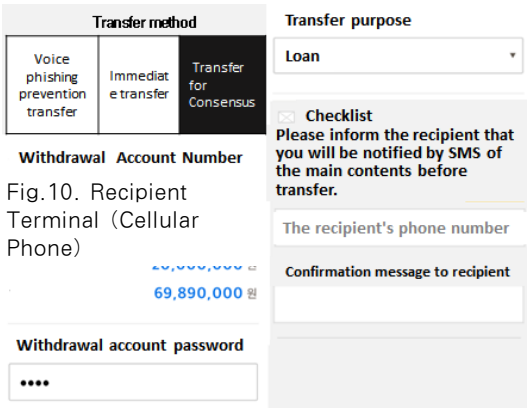

Fig. 6. 2-WAY Trade Verification for Preventing Voice Phishing

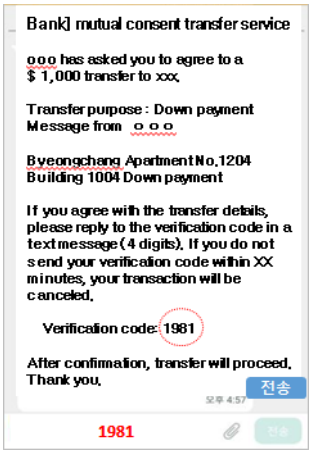

Fig. 7. Recipient Terminal (Cellular Phone)

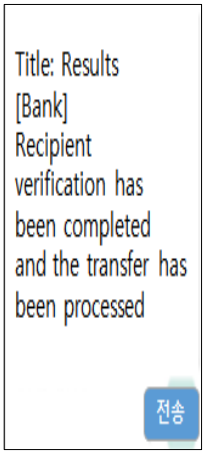

Fig. 8. Remitter Terminal (Cellular Phone)

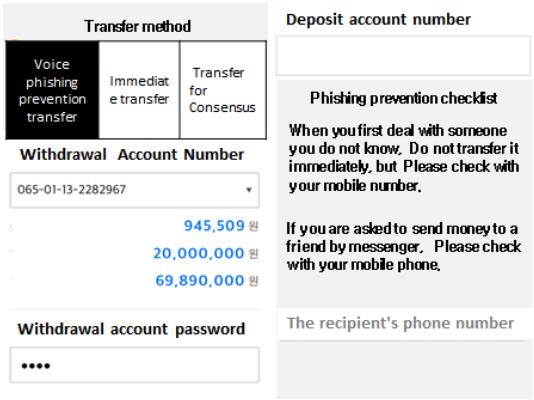

Figure 9. 2-WAY Trade Verification for Consensus (Remitter & Recipicnt)

의미로 수신 문자에 포함된 일회용 번호를 SMS문자로 발송함으로써 개인간 금전대차에 대한 전자거래 계약이 이루어진다.

2018년 6월부터 8월까지 시범 적용한 결과 모바일뱅킹 이체 전체 거래량의 약10%~11%정도 보이스피싱 예방이체 거래로 사용되고 있으며, 약 1%~2.5%정도가 상호합의 이체 거래로 사용되고 있으나, 시간이 지날수록 꾸준한 증가 추세를 보이고 있어 이용자들의 인식의 변화가 긍정적인 것으로 판단된다.

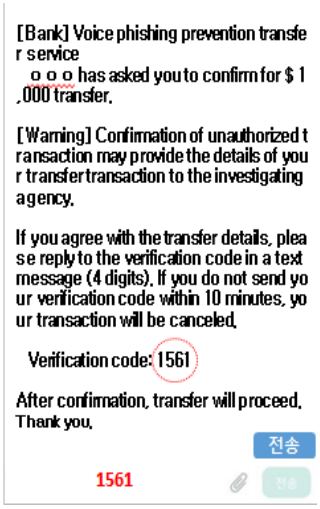

Fig.10. Recipient Terminal (Cellular Phone)

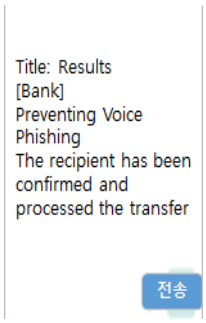

Fig.11. Remitter Terminal (Cellular Phone)

Table 4. Remittance by Mobile Banking (** Savings Bank)

(unit : transaction)

Division	2018.6	2018.7	2018.8	Sum
Basic Remittance	3,333	4,220	2,840	10,393
Preventing Voice Phishing	375 (10%)	480 (10%)	360 (10.9%)	1,215
Consensus (Remitter & Recipicnt)	42 (1.12%)	60 (1.26%)	80 (2.43%)	182
Total	3,750	4,760	3,280	11,790

V. 제안모델 특징 및 기존 인증수단과 기능 비교분석

현재 송금인 중심의 단방향 거래인 전자금융 자금이체 거래는 지인사칭 등 사기공격 또는 송금인에 의한 착오송금과 전자상거래에서 개인 간 계약성 거래 또는 합의가 필요한 서비스를 제공하지 못한다.

따라서, 송금인과 수취인 사이에 양방향 전자 자금이체 거래인 2-WAY 거래인증은 안전한 이동통신사의 양방향 문자서비스를 이용해 전자거래법에서 명시한 전자문서 교환요건을 만족하고, 송금인과 수취인간의 통신채널을 이용해 거래내용 및 용도를 상호 확인한 후 자금이 이체 되므로 모 저축은행처럼 기존 이용자 인증 수단으로 예방이 어려운 착오송금 예방, 지인사칭 보이스피싱 예방 또는 개인간 계약

Table 5. Comparisons of Authentication System and 2-WAY Trade Verification System

Division	Authentication	2-WAY Varification	Remark
Recipient linkage	None	Electronic document agreement transaction	SMS text
Big Data support	None	Separate transaction purpose	Propensity analysis
Electronic Data Interchange	Certificate-based Transaction between Remitter and financial company	- **Remitter** : Authenticated using the authentication method of existing financial company. - **Forwarder** : Sends the input from the remitter directly to the secure mobile network. - **Recipient**: After confirming the contents of received electronic document, reply directly to the received phone number.	Non-repudiation
Preventing the error remittances	The sender only checks the input	The remitter and the recipient confirm the transaction as well as the input	
Preventing the voice phishing	None	Possible to trace the origin of fraudulent (recipient)	Respond with SMS (verification code)

성 거래를 위한 서비스를 2-WAY 거래인증 기능을 이용해 적용할 수 있다.

특히, 지인사칭 보이스피싱의 경우 제 3자(대포통장 제공자 등)가 이미 사기범 일행으로 수취인 확인 문자에 회신을 한 경우라도 수사기관에 발신지 정보를 제공함으로써 범죄행위에 대한 부담과 수사에 도움이 된다.

VI. 결론 및 향후 연구

지속적으로 이슈가 되고 있는 보이스피싱 사기와 착오송금에 대한 예방뿐만 아니라, 향후 금융회사들이 경쟁적으로 제공하는 간편 결제를 이용한 계좌이체 또는 개인간 금전대차거래인 대여금, 각종 계약거래, 개인간 전자상거래인 P2P거래 등 이체 서비스를 본 연구에서 제시한 2-WAY 거래인증 방법을 적용하여 기존 전자금융거래와 전자문서기반의 전자상거래를 연결하는 통로로 활성화되기를 기대한다.

그리고, 본 연구에서 보이스피싱 및 착오 송금에 대한 효과성은 모 저축은행에 적용한 기간(2018.6월~8월)이 짧아 정확한 데이터를 수집하는데 한계가 있어 차후 연구에서 그 효과성 측정을 위한 추가 연구와 향후, 블록체인기술과 연계한 전자금융 P2P 거래를 발굴하기위한 지속적인 연구가 필요하다. 또한, 현금 거래가 대부분인 P2P유형의 개인 간 직접 거래에서도 2-WAY 거래인증 서비스가 적용될 경우 현금 없는 전자금융거래 문화를 만드는 기반이 될 것으로 판단된다.

References

[1] Financial Supervisory Service, "Electronic Financial Supervisory Regulation Commentary", Business Data, pp. 9, May .2017.

[2] Financial Security Institute,"User Authentication Method Evaluation and Selection Guide for Electronic Financial Transactions", The Electronic Finance and Security, pp. 62-66, Oct. 2015.

[3] Chung, So Yoon, "A Study on the Utilization of the Digital Signature and Authentication System through Public Key Infrastructure (PKI)", Master Thesis, The Graduate School Yonsei University, pp. 7-11, Nov. 2001.

[4] Ming Byeong-do, National Assembly room, "Recent 5-year Anomaly Transactions (bank)", Press Releases, pp. 1, Sep. 2018.

[5] Financial Supervisory Service, "Status of Voice Phishing Type in the first half of 2018", Press Releases, pp. 1, Sep.2018.

[6] Supreme Court,"2017 Da 37324 loan, judgment sentence", Supreme Court case, pp1-2, Dec. 2018

〈저자소개〉

이 익 준 (Ig Jun Lee) 정회원
2014년 2월: 동국대학교 국제정보대학원 석사
2016년 3월~2018.8월: 순천향대학교 정보보호대학원 박사과정 수료
2018년~현재: (주)삼위
〈관심분야〉 위험관리, 정보보호관리체계, 보안아키텍쳐

오 재 섭 (Jae Sub Oh) 정회원
2014년: 경희대학교 경영학 박사
2018년~현재: 숙명여대 겸임교수, 유한대 강사, 한국모바일기업진흥협회 기술 이사
〈관심분야〉 블록체인, 비즈니스 모델, 사물인터넷

염 흥 열 (Heung Youl Youm) 종신회원
1990~현재: 순천향대학교 정보보호학과 교수
2011년: 제 16대 한국정보보호학회 회장
2017년: ITU-T SG17 의장