Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1513

전자금융 불법이체사고 방지를 위한 실시간 이상거래탐지 및 분석 대응 모델 연구

유 시 완†‡
고려대학교 정보보호대학원

Study on a Real Time Based Suspicious Transaction Detection and Analysis Model to Prevent Illegal Money Transfer Through E-Banking Channels

Si-wan Yoo†‡
Center for Information Security Technologies(CIST), Korea University

요 약

금융회사가 전자금융 서비스를 제공하기 시작하면서 전자금융 서비스는 다양화 되었고 전자금융 사용은 지속적으로 증가하고 있다. 이에 금융회사는 안전한 전자금융서비스를 제공하기 위하여 금융 보안정책을 적용하고 있으나 전자금융 사고는 계속해서 지능화되고 증가하고 있는 상황이다. 금융감독기관은 최근 인터넷 전문은행 등장과 핀테크 활성화와 더불어 비대면 실명확인 제도 신설 및 전자금융 거래를 통한 자금이체 시 공인인증서 또는 일회용비밀번호 의무사용 폐지 등의 규정을 개선하여 이용자의 편리함을 추구하는 동시에 금융회사에게는 이상금융거래 탐지 시스템 고도화 및 개선을 통한 불법이체 사고 방지를 권고하고 있다. 본 논문에서는 금융회사 제반 상황에 적합한 블랙리스트기반 자동화 탐지 기법을 제안하고 블랙리스트 정보를 레벨링하여 보안레벨에 따른 블랙리스트기반과 통계모델을 연동한 실시간 이상금융거래 탐지 기법을 제안하며, 기존 전자금융 사고유형 분석을 통한 특징적 패턴에 따른 실시간 이상금융거래 탐지 기법의 대응 모델을 제안하고자 한다.

ABSTRACT

Since finance companies started e-banking services, those services have been diversified and use of them has continued to increase. Finance companies are implementing financial security policy for safe e-banking services, but e-Banking incidents are continuing to increase and becoming more intelligent. Along with the rise of internet banks and boosting Fintech industry, financial supervisory institutes are not only promoting user convenience through improving e-banking regulations such as enforcing Non-face-to-face real name verification policy and abrogating mandatory use of public key certificate or OTP(One time Password) for e-banking transactions, but also recommending the prevention of illegal money transfer incidents through upgrading FDS(Fraud Detection System). In this study, we assessed a blacklist based auto detection method suitable for overall situations for finance company, a real-time based suspicious transaction detection method linking with blacklist statistics model by each security level, and an alternative FDS model responding to typical transaction patterns of which information were collected from previous e-Banking incidents.

Keywords: FDS, Blacklist device information, Auto detection method, Security level, Typical transaction pattern

Received(10. 10. 2016), Modified(11. 16. 2016), Accepted(11. 17. 2016)

† 주저자, hanaysw@hanafos.com
‡ 교신저자, hanaysw@hanafos.com(Corresponding author)

I. 서 론

금융회사가 전자금융 서비스를 제공하기 시작하면서 전자금융서비스 사용이 지속적으로 증가하고 있는 상황이다. 2016년 3월말 국내 인터넷뱅킹 서비스 및 모바일뱅킹 서비스 등록 고객수는 1억 1,977만명으로 전년 말 대비 2.5%가 증가하였으며, 조회서비스, 자금이체서비스, 대출신청 서비스 등 실이용고객수는 5,738만명으로 47.9%를 차지하고 있다. 스마트폰 기반 모바일뱅킹의 경우 전년 말보다 5.0%가 증가하여 6,800만명이 등록하였으며, 이용건수는 전년대비 12.4% 증가하였다. 한편 2011년 이후 정체상태인 PC기반 인터넷뱅킹 이용건수와 달리 모바일뱅킹 이용건수는 지속적으로 증가하여 2014년 4/4분기부터 PC기반 인터넷뱅킹 이용건수보다 우위를 유지하고 있다. 모바일뱅킹 등록고객의 연령대를 보면 10~30대의 사용비율이 높지만 50대 이상도 꾸준히 증가하고 있는 추세이다[1]. 그러나 전자금융서비스 이용이 증가됨에 따라 전자금융 사고 또한 증가하고 있는 상황이다. 한국인터넷진흥원에서 발표하는 인터넷 침해사고 대응통계에 따르면 국내 피싱사이트 차단 현황은 2015년 월평균 1,700건이며, 이는 2014년 월평균 1,200건보다 훨씬 증가한 상황이다[2].

금융기관에서는 전자금융사기예방서비스를 2013년 9월부터 단말기지정서비스 및 공인인증서 (재)발급 시 추가인증(ARS인증, SMS인증 등)을 의무 시행하고 있으며, 단말기기정서비스 가입자가 미 지정 단말에서 이체 거래를 하거나 단말기지정서비스 미가입자가 일정한 금액(1일누적 300만원 이상, 카드3사의 정보유출 사고 후 100만으로 축소) 이상 이체거래 시 추가인증을 반드시 하도록 거래인증을 강화하고 있다[3]. 그리고 전자금융사고를 예방하기 위해 공인인증서, 키보드보안, OTP, ARS인증 등 전자금융 보안대책을 세우고 있으나 지능화된 전자금융사기행위로 계속해서 전자금융 불법이체 사고는 발생하고 있다.

특히 한국인터넷진흥원 2016년 상반기 악성코드 은닉 사이트 탐지 보고서에 의하면 악성코드 유형 중 금융정보 유출관련 건이 73%을 차지할 정도로 전자금융사고에 많은 위협이 노출되어 있다[4].

지능화되고 있는 전자금융 사고를 예방하기 위해 금융위원회는 2013년 7월 제도적, 기술적 보안관리 체계강화에 중점을 두는 '금융전산 보안 강화 종합대책'[5]을 통해 이용자 보호 강화 및 이상금융거래 탐지 시스템(Fraud Detection System) 구축을 권고 하였으며, 금융감독원은 2014년에 금융권 FDS 추진 협의체 출범 및 FDS 고도화 1.0을 통해 2016년까지의 로드 맵을 제시하였다[6]. 2014년에 이상금융거래 탐지 시스템 도입, 2015년 이상금융거래시스템 확대하면서 금융거래정보까지 수집대상 확대, 이상금융거래 분석 및 차단, 이상금융거래 분석 및 상담 전문인력 확보를 추진하고 2016년에는 금융권 공동대응을 추진하는 내용을 발표하였다. 로드 맵 발표 이후 2016년 현재 주요 금융권은 FDS시스템 구축이 완료된 상태이며, 저축은행 및 주요기업에서도 FDS시스템 도입을 검토 중이며 인터넷 전문은행의 등장과 Fin-Tech의 활성화와 더불어 FDS시스템 도입은 확대될 전망이다.

이상금융거래 탐지 시스템은 기존 사고단말 정보를 블랙리스트(blacklist)로 등록하여 실시간 탐지하는 방식 및 금융소비자들의 전자금융거래를 실시간으로 모니터링(monitoring)하여, 정책에 위배된 행위가 발생할 경우 즉각 거래를 중단 시키고 금융기관과 소비자에게 통보하는데 활용된다. 따라서 이상금융거래 탐지 시스템은 무엇보다 블랙리스트 및 전자금융 이상금융거래를 빠르고 정확한 탐지가 매우 중요하다고 할 수 있다.

본 논문에서는 현재 금융회사에 구축되어 있는 이상금융거래 탐지 시스템의 현황을 살펴보고, 기존의 블랙리스트 방식에서 고도화된 방식의 블랙리스트기반 자동화 탐지 기법을 제안하고 보안레벨에 따른 블랙리스트 정보와 통계모델을 연동한 실시간 이상금융거래 탐지 기법을 제안하며, 기존 전자금융 사고유형 분석을 통한 특징적 패턴에 따른 실시간 이상금융거래 탐지 기법을 제안하고자 한다.

논문의 구성은 총 5장으로 구성되었다. 2장에서는 이상금융거래 탐지 시스템의 개념 및 구축 현황, 기존 국내외 관련 연구를 살펴보고, 본 연구의 차별성을 밝힌다. 다음으로, 3장에서는 실시간 이상금융거래 탐지 및 분석 대응 모델 세가지 방안에 대하여 제안한다. 다음으로, 4장에서는 제안한 대응 모델을 국내 모 은행에 적용하여 효과성을 검증한다. 마지막으로, 5장에서는 본 논문에 대한 결론과 연구의 한계를 살펴보고 향후 연구에 대한 방향을 제시하고자 한다.

II. 관련연구 및 배경지식

2.1 이상금융거래 탐지 시스템의 개념 및 구축 현황

이상금융거래 탐지 시스템(FDS)에 대한 정의는 금융보안연구원에서 발표한 FDS 기술가이드에서 전자금융거래에 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심거래를 탐지하고 이상금융거래를 차단하는 시스템이라고 정의하고 있다[7]. FDS시스템은 다양하게 수집된 정보를 종합적으로 분석하여 이상금융거래 유무를 판별하는 복합적인 시스템으로 4가지 기능으로 이루어져 있으며 각 기능은 상호 호환 또는 연동되도록 구성된다. 정보수집 기능은 이상금융거래 탐지의 정확성을 위해 크게 이용자 매체 환경 정보와 사고 유형 정보의 수집 기능이며, 분석 탐지 기능은 수집된 정보를 이용자 유형별, 거래 유형별 다양한 상관관계 분석 및 규칙 검사 등을 통해 이상 행위를 탐지하는 기능이다. 또한 대응 기능은 분석된 이상 금융거래 행위에 대한 거래 차단 등의 대응기능이며 모니터링 및 감사 기능은 수집·분석·대응 등의 종합적인 절차를 통합하여 관리하는 모니터링 기능과 해당 탐지 시스템을 침해하는 다양한 유형에 대한 감사기능이다.

금융감독원 발표에 의하면[8] 2016년 상반기 국내 금융회사의 이상금융거래 탐지 시스템 구축 현황은 은행 16개사 및 카드사 8개사가 100% 완료된 상태이며, 증권사 32개사 중 72%에 해당하는 23개사는 구축이 완료된 상태이며, 9개사는 현재 구축이 진행중인 것으로 알 수 있다. Table 1. 은 2016년 상반기 국내 금융회사의 이상금융거래 탐지 시스템 구축 현황을 보여준다.

Table 1. The FDS construction status of Finance company

Category	Completed	Under construction
Commercial Banks	KB, KEB hana, Shinhan, Woori, SC, Citi, Busan, Daegu, JB, Kwang Ju, BNK, Jeju, KDB, IBK, NH, Suhyup	-
Investment Securities	HMC IS, NH IS, Kyobo Secu, Daishin Secu, Mirae Asset Daewoo, Merits Secu, Mirae Asset, Samsung Secu, Shinyoung Secu. Shinhan Inv. Yuanta Secu, Eugene Inv, Kiwoom Secu, Hana FI, Hi IS, Korea IS, Hyundai Secu, Dongbu Secu, Gloden Bridge IS, IBK Secu. E-Bast IS, Hanwha IS, SK Secu	LIG IS, Bookook Secu, Yuwha Secu, Fund Online Korea. KTB IS, Leading IS, Hanyang Secu, BNK Secu, KB IS
Credit cards	BC, Samsung, Hyundai, Lotte, Shinhan, Hana, KB, Woori	-

2.2 이상금융거래 탐지 시스템 기존 연구동향

전자금융사고가 많이 발생을 하면서 이상금융거래 탐지 시스템에 대한 많은 연구가 이루어지고 있다. 금융기업에서 블랙리스트 기반 탐지 시스템을 기본으로 적용하고 있다. 블랙리스트 기반의 이상금융거래 탐지 시스템은 이상금융거래 발생 시 선 차단 후 조치로 운영되고 있으며, 이상금융거래 단말정보를 등록할 시 금융사고처리부서에서 사고신고를 처리하고 분석 후에 이상금융거래 단말정보를 등록하는 절차이다.

블랙리스트기반 탐지는 MAC 주소, HDD S/N, IP 주소, 텔레뱅킹 전화번호, UUID 주소 등 인터넷 뱅킹, 스마트폰뱅킹, 텔레뱅킹을 접속한 단말 정보를 기준으로 탐지한다. Table 2. 은 전자금융 접속채널에 따라 탐지되는 단말정보이다.

블랙리스트로 등록된 단말 정보와 동일한 정보로 인터넷뱅킹, 스마트폰뱅킹, 폰뱅킹에 접속할 경우 탐지시스템에서 탐지하여 전자금융 이용을 제안한다.

박은영[9]의 연구에서는 기존 블랙리스트 패턴기법의 사후 분석기법의 문제점을 도출하고 개선하기 위해 상태전이기법을 적용한 '사전적 사고예방을 위한 이상 금융거래 탐지시스템'을 제시하였다. 정상적인 거래 절차 및 유형을 벗어나는 행위를 식별하여 매체 환경 정보와 거래유형에 대해 프로파일링을 추출하여 프로파일링 패턴변수에 가중치를 부여하고, 프로파일링을 기준으로 프로파일링 그룹을 White

Table 2. Device information by e-banking accessing channel

Channel	Device information
Internet banking	MAC address, HDD S/N, OS, IP address, Gateway MAC, Gateway IP, Proxy, VPN etc.
Smart phone banking	UUID address, IP address, OS, Mobile Model etc.
Tele banking	Telephone number

(정상거래 고객), Gray(사고 가능성 높은 고객), Black(사고가 있는 고객)등으로 Group을 분류하고 세부적인 Rule 패턴을 설정하여 블랙리스트 기반으로 탐지하지 못했던 사고거래 중 58%를 탐지하여, Rule 기반 이상금융거래 탐지를 제안하였다.

Quah[10]의 연구는 실시간 뱅킹 시스템에 인공신경망보다 진보한 자가조직도(self-organization map) 알고리즘을 활용하여 수행속도가 뛰어나고 실시간 학습처리를 통한 통계 분포도 시간에 따라 변화하여 숨겨진 패턴을 감지할 수 있는 방안을 제안하였다. 하지만 많은 입력 데이터가 들어오는 처리 과정이 필요하고 신경망 내부를 추측하기 어려워 결과에 대한 과정 설명이나 추론이 어렵다.

박재훈의[11]의 연구에서는 빠르고 효과적인 이상금융거래 탐지를 위해 고객의 사고사례 패턴을 중심으로 탐지규칙을 설정한 후 의사결정 나무에 의한 정규화를 통해 시스템 효율성 향상과 유지비용 감소 방안을 제시하였다.

최의순[12]의 연구에서는 국내 금융 환경을 반영한 통계적 기법, 빅데이터 분석기법, 매체 정보 중심 탐지기법을 통해서 운영해 본 결과, 이상금융거래 탐지에 필요한 데이터 축적이 미미하여 오탐율이 높아 민원발생 빈도가 높은 것을 확인하였다. 최의순의 연구에서는 실제 사고 내역과 FDS시스템을 통한 사고를 비교·분석하여 False Negative와 False Positive를 감소시키기 위해 사용자 프로파일 구성, 탐지규칙 도출 등을 제시하였다.

2.3 연구의 차별성

블랙리스트 기반의 이상금융거래 탐지 시스템은 선 차단 후 조치로 운영되고 있으므로 이상금융거래가 발생 한 후 이상금융거래 신고・분석・등록까지의 공백시간이 존재하여, 블랙리스트 탐지 시스템에 단말정보가 등록되기 전까지 동일한 사고의 개연성이 높으며, 신속한 탐지 및 예방이 불가능하다. 프로파일링 및 Rule 기반 탐지시스템은 블랙리스트 기반 탐지시스템에 비해 정탐율은 높으나, 정상적인 거래 절차를 기준으로 행위를 패턴화하여 이상금융거래를 탐지하기 때문에 오탐율도 높을 수 있다. 사고사례를 비교·분석 후 담당자와 FDS시스템 운영과 관련된 주요 이슈에 면담을 실시하여 오탐율과 정탐율의 기준을 설정하여 오탐율을 줄일 수 있으나 전자금융사고의 유형이 빠르게 변화하면서 대응 시간이 현저히 느릴 수 있다. 본 논문에서 이러한 탐지 방식들의 단점을 보완하고자 기존에 운영되고 있는 블랙리스트기반 탐지를 자동화하고, 보안레벨에 따른 블랙리스트 기반과 통계모델을 연동한 탐지기법, 전자금융사고 유형 분석을 통한 특징적 패턴에 따른 탐지기법을 제안하고자 한다.

III. 이상금융거래 탐지기법 분석 및 대응모델 제안

전자금융사고가 지능화 되어 가면서 블랙리스트 기반 탐지기법, Rule 기반 이상금융거래 탐지기법 등 한가지 기법을 통해 탐지하기가 어려워지고 있다. 본 논문에서 제안하는 이상금융거래 탐지기법은 기존의 블랙리스트 방식에서 고도화된 방식의 블랙리스트 기반 탐지 자동화기법, 블랙리스트 보안레벨 기반과 통계모델을 연동한 실시간 탐지 기법, 특징적 패턴에 따른 실시간 탐지기법 세 가지를 제안하고자 한다.

3.1 이상금융거래 탐지 방법 기본정책

Table 3. 과 같이 K은행의 2015년 상반기 금융정보 탈취 유형 별 전자금융 불법이체 사고내역을 조사한 결과 99% 이상 이 파밍 및 보이스피싱을 통하여 고객의 금융정보(이용자비밀번호, 공인인증서, 보안카드, OTP등)를 탈취 후 제3자(범죄자) 단말에서 인터넷뱅킹, 스마트폰뱅킹, 폰뱅킹, 폼뱅킹 등을 통하여 불법이체가 이루어짐을 알 수 있다. 특히 고객의 금융정보 탈취가 기존 일반PC에서 파밍을 통한 탈취 외에 스마트폰 내 악성코드를 실행시켜 파밍 사이트 유도를 통한 탈취와 보이스피싱과 파밍이 결합된 하이브리드 방식을 통한 탈취가 많이 발생하고 있음을 알 수 있다.

Table 3. Illegal money transfer by information hacking type in the 1st half of 2015

Month	Pharming (PC)	Pharming (Smartphone)	Voice Phishing	Voice Phishing + Pharming(PC)	Smishing	Total
Jan.	17	11	3	20	2	53
Feb.	4	6	4	8	2	24
Mar.	12	7	0	10	3	32
Apr.	7	10	1	7	0	25
May	2	20	2	3	0	27
June	1	11	4	3	0	19
Sum	43	65	14	51	7	180

보이스피싱과 파밍이 결합된 하이브리드 방식의 지능화된 방식으로 고객의 금융정보가 탈취 되다 보니 금융권에서 가장 안전한 인증수단으로 이용중인 OTP(One Time Password) 고객에 대해서도 불법이체 사고는 증가하고 있는 추세이다.

Table 4. 는 K은행의 2015년 상반기 보안매체(보안카드, OTP) 이용자 별 불법이체 사고 현황을 나타낸다.

고객정보 탈취 방식은 지능화되고 지속적으로 증가하고 있으며, 이로 인해 다양한 전자금융채널을 통한 불법이체 사고가 발생하고 안전한 인증수단을 소지한 이용자들 또한 불법이체 사고의 피해를 보고 있기에 금융권에서는 더욱더 이상금융거래 탐지 시스템을 통한 효과적인 대응책이 필요하다.

본 논문에서 제안하는 효과적인 이상금융거래 탐지 기법을 위해서는 우선 3가지 기본적인 기준이 바탕이 되어야 한다. 첫째, 이상금융거래 탐지가 되었을 경우 고객번호를 기준으로 거래를 제한한다. 금융보안연구원의 이상금융거래 탐지시스템 기술 가이드는 USER ID를 기준으로 거래를 제한[11]하고 있으나 USER ID로 거래를 제한할 경우는 펌뱅킹(PG거래)을 통한 불법이체사고가 발생할 수 있으며, 계좌번호로 기준을 제한할 경우는 비밀번호가 동일한 다른 계좌번호를 통하여 불법이체사고가 발생할 수 있다. 그러므로 고객번호를 기준으로 거래를 제한함으로서 고객이 소지한 모든 입출금이 자유로운 요구불계좌(전자금융 가능계좌, 전자금융 불가능 계좌)로부터 인터넷 뱅킹, 스마트폰뱅킹, 텔레뱅킹 뿐만 아니라 펌뱅킹 (PG거래) 및 전자지갑 충전 등 다양한 전자금융채널을 통한 불법이체 거래를 예방할 수 있다. Fig. 1. 은 계좌유형 별 자금이 이체될 수 있는 채널 및 채널 별 이체 시 인증수단을 나타낸다. 둘째, 이상금융거래 탐지 시스템에 블랙리스트 단말정보를 등록할 시 보안수준에 따라 레벨링(leveling)하여 등록한다.

Table 4. Illegal money transfer by security tool in the 1st half of 2015

Tool	Security Card	OTP
Jan.	36	17
Feb.	15	9
Mar.	21	11
Apr.	20	5
May	25	2
June	12	7
Sum	129	51

Table 5. 와 같이 HIGH, MIDDLE, LOW로 레벨링을 하여 단말 정보에 따라 이상금융거래 탐지 기법을 다르게 적용하여 오탐율을 줄이고 정탐율을 높이고자 한다. 'HIGH'는 실제 불법이체사고로 이용한 범죄자의 불법단말정보로 FDS시스템 담당자가 확인한 정보로 PC의 MAC 주소, 하드디스크 시리얼번호(HDD S/N), 스마트폰의 UUID 값으로 동일단말로 접속 시 사고 발생 확률이 99% 이상인 것으로 정의하며, 'MIDDLE' 은 실제 불법이체사고로 이용한 범죄자의 불법단말정보로 FDS 담당자가 확인한 정보로 PC의 IP주소, Gateway MAC 주소, Gateway IP 주소, Proxy정보, OS정보, 스마트폰 모델 정보 등으로 동일단말로 접속 시 사고 발생 확률이 70% 이상인 것으로 정의 한다. 'LOW'는 불법이체사고로 이용한 범죄자의 불법단말정보는 아니지만, FDS시스템 담당자가 이상금융거래 분석 시 사고 개연성이 있는 PC의 MAC 주소, 하드디스크 시리얼번호, UUID, 전화번호 등으로 사고 발생 확률이 50% 이상인 것으로 정의 한다.

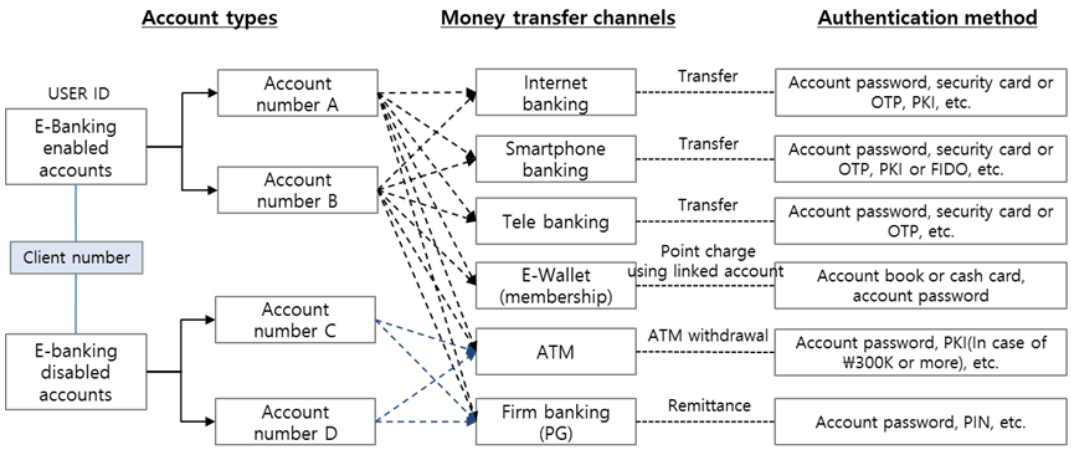

Fig. 1. Money transfer channels and authentication method by account type

셋째, Table 6.과 같이 이상금융거래 탐지 기준을 보안 수준에 따라 지급정지 및 이체정지로 제한을 구분 해야 한다. 이상금융거래 탐지에 정상고객도 탐지될 확률이 있기 때문에 이상금융거래 탐지의 정확률이 90%이상이며, 오탐율이 10% 미만인 탐지 기법은 지급정지 시키도록 한다. 그 외에 탐지 기법은 정상고객이 탐지될 확률이 있으므로 이체정지를 시키고 본인이 거래한 경우에 따라 본인이 추가인증(ARS인증 등)을 통하여 해제하는 프로세스를 도입되어야 한다.

Table 5. Security level of blacklist

Security level	Outline	Blacklist information
HIGH	Device information used for illegal money transfer	MAC address, HDD S/N, UUID
MIDDLE	The suspicious device information	Gateway MAC, Gateway IP, IP address, Proxy, OS, Mobile Model type, etc.
LOW	Device information reported by the 3rd party entities	MAC address, HDD S/N, UUID, Telephone number, etc.

Table 6. Restriction criteria and release procedure

Restriction	Scope	Withdrawal procedure
Prohibition of money transfer	Restrict all e-banking transactions (Internet banking, Smartphone banking, Telebanking, Firm-banking, e-Wallet charging)	In case of self-transactions, additional authentication is required, but in other cases, client should visit branch and update account information.
Suspension of payment	Restrict all e-banking and ATM withdrawal transactions	Clients should visit branch and update account information.

3.2 블랙리스트기반 탐지기법의 자동화

기존방식의 블랙리스트기반 탐지시스템에서 불법사고 단말을 등록하는 절차는 사고 이후 처리 방식으로서, 고객이 불법사고를 콜센터를 통해서 접수할 경우 불법이체 사고처리부서를 통해 사고 분석 후에 블랙리스트 데이터 베이스에 불법사고 단말 정보가 등록된다. 불법이체 사고가 난 후부터 불법사고 단말 정보가 등록되는 동안 위험에 노출되게 된다. 국내 금융회사 중 카드사의 경우는 오래 전부터 카드 부정사용방지를 위하여 24*365 체계가 구축되어 시간에 제약을 받지 않고 사고 접수가 되며, 즉시 사고처리

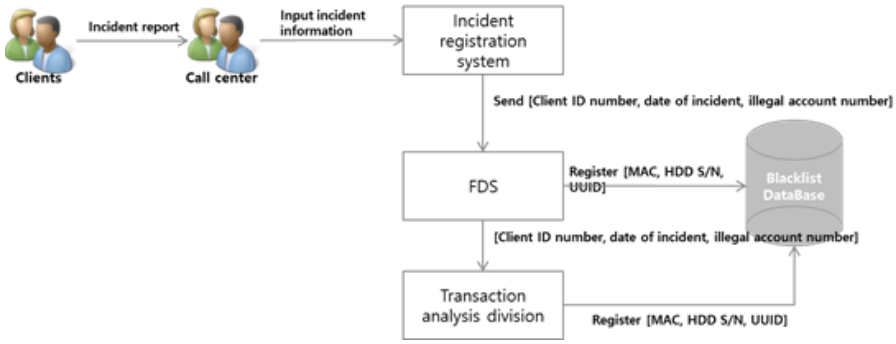

Fig. 2. Workflow of blacklist based auto FDS

부서에서 분석 후 불법단말을 등록한다. 국내 은행의 경우는 FDS시스템을 도입한 기간이 짧고 FDS시스템을 24*365 체계로 전담조직을 운영하는 것이 미미하다. Table 7. 와 같이 2015년 대부분의 은행이 일과시간에는 FDS 전담조직을 운영하고 있으나, 일과시간 이후에는 전자금융 콜센터 상담원을 통하여

Table 7. Exclusive FDS team operation status in 2015

Bank	24*365 operation	Business hour operation
KB	X	O
KEB Hana	X	O
NH	O	O
Shinhan	X	O
Woori	X	O
IBK	X	O

Table 8. The number of e-banking incident by post-incident day in the 1s half of 2015

The incident received	Number of incidents
within 1 day	96
2 days	34
3 days	16
4 days	13
5 days	4
6 days	3
7 days	3
8 days	2
9 days	3
more than 10 days later	6

기본적인 사고접수 및 대응을 하고 있는 추세이다.

Table 8. 은 K은행 2015년 1월부터 6월까지 전자금융사고 발생 후 기간 별 접수 현황을 나타낸다.

고객이 전자금융사고가 발생한 후 사고 신고까지 평균 24시간 이내에 신고를 하며, 53% 가 당일 신고 및 접수를 하고 25% 가 1~2일 이내에 사고 접수가 이루어 지는 등 78% 이상이 2일 이내에 이루어짐을 알 수 있다. 일과시간 이내에 콜센터 상담원을 통해 사고신고 접수 후 FDS 전담조직이 분석 및 사고단말 정보를 블랙리스트로 등록하는데 최소 1 ~ 2시간이 걸린다. 그리고 일과시간 이후에 접수된 사고 건은 대부분의 은행들이 익일 FDS 전담조직에 의해 처리를 하므로 더욱더 많은 시간이 흐른 후 사고단말 정보를 등록함을 알 수 있다. 또한 범죄자들이 동일한 사고단말로 사고 이후에도 다른 사용자 정보로 접속을 시도 하는 것을 확인할 수 있다. 이는 2차 사고의 우려가 있으므로 빠른 조치를 취하는 것이 필요하다.

본 논문에서는 국내은행 FDS 전담조직 운영 제반사항을 고려하여 위험 노출 시간을 줄이는 방안으로 콜센터 상담원을 통해서 불법사고가 사고접수시스템에 접수되면 블랙리스트 데이터베이스에 불법사고 단말 정보 등록을 자동화하여 사고신고가 접수 된 이후 분석과 등록의 시간을 최소화하는 방안이다.

Fig. 2. 은 블랙리스트기반 탐지기법 자동화 흐름도이다. 사고접수 시스템과 FDS시스템을 연동시킴으로써 사고신고 시스템에 불법사고 정보를 등록하면 FDS시스템에 고객번호, 불법이체일자, 불법이체계좌의 정보가 실시간으로 전달되고, FDS 시스템은 전달받은 정보로 거래를 분석 및 검색하여 불법단말 정보가 자동으로 블랙리스트 데이터 베이스에 등록한다. 또한, FDS시스템을 통해 접수 받은 사고신고

정보를 분석부에서 2차적으로 분석함으로써 추가적인 불법단말 정보를 등록하는 시스템을 구축하였다.

불법단말 정보를 등록한 이후 동일 단말정보로 로그인할 경우 사용자는 지급정지에 걸리게 되며, 영업점에 방문하여 금융정보를 바꾼 후에 지급정지가 해제되게 된다. 불법사고 신고가 접수되자 마자 자동으로 블랙리스트 데이터 베이스에 저장되게 함으로서 위험에 노출되는 시간을 최소화하여 2차 사고를 예방할 수 있다.

Table 9.는 불법사고 단말정보를 등록한 후 동일 정보로 로그인 했을 경우 지급정지 걸린 고객의 수를 나타낸다. 이는 사고가 발생한 이후에 동일한 단말을 통해 다른 사용자로 로그인하는 것을 볼 수 있다. 2015년 지급정지를 자동화한 이후에 지급정지 건수가 현저히 늘어남을 알 수 있다. 이렇듯 단말 등록을 자동화 함으로서 동일 단말에 대한 빠른 등록은 전자금융사기 예방에 효과적이다.

Table 9. The suspended transactions due to logon using same illegal device

Month	Number of device	Number of suspended payment
Jan. 2015	216	239
Feb. 2015	89	106
Mar. 2015	269	431
Apr. 2015	161	184
May 2015	119	155
June 2015	140	855

3.3 보안레벨에 따른 블랙리스트 정보와 통계모델을 연동한 실시간 탐지기법

금융보안연구원에서 제안한 이상금융거래 탐지시스템 기술 가이드에서 이상금융거래 탐지를 위한 수집정보는 물리적 MAC, HDD S/N, CPU, 메인보드 정보, 가상화 소프트웨어 사용정보, 브라우저 정보, IP, VPN 정보 등을 수집하여 과거의 접속정보와 거래정보, 현재의 접속정보와 거래정보를 수집하여 Rule 기반 탐지패턴에 적용하도록 제안하고 있다. 다양하게 수집된 정보를 이용하여 복합적으로 활용·분석한 결과를 바탕으로 탐지패턴(Rule)이 생성한다[6]. 본 논문에서는 금융보안연구원에서 제안한 수집정보 외에 Gateway MAC주소와 Gateway IP, VPN, Proxy와 같은 정보를 수집하여 새로운 실시간 탐지기법을 제안하고자 한다. 사용자들은 항상 동일한 패턴과 단말정보를 가지고 전자금융서비스를 이용하지 않기 때문에 Rule 기반 FDS 탐지시스템을 통해서만 이상금융거래를 탐지할 경우 오탐율은 증가하게 된다. 본 논문에서는 금융보안연구원에서 제시한 수집 정보 외에 Gateway MAC 정보와 Gateway IP 정보를 수집하여 FDS 시스템과 연동하는 탐지기법을 제안하고자 한다. Fig. 3. 은 블랙리스트 단말 정보와 FDS 실시간 탐지를 연동한 탐지기법의 흐름도이다. 블랙리스트의 HIGH레벨은 MAC주소, HDD S/N, 전화번호, 불법입금계좌이다. HIGH 레벨 정보로 로그인할 경우 지급정지로 탐지된다. 블랙리스트의 MIDDLE 레벨은 Gateway MAC, Gateway IP, Proxy, OS 등이다. MIDDLE 레벨 정보만으로 이체정지나 지급정

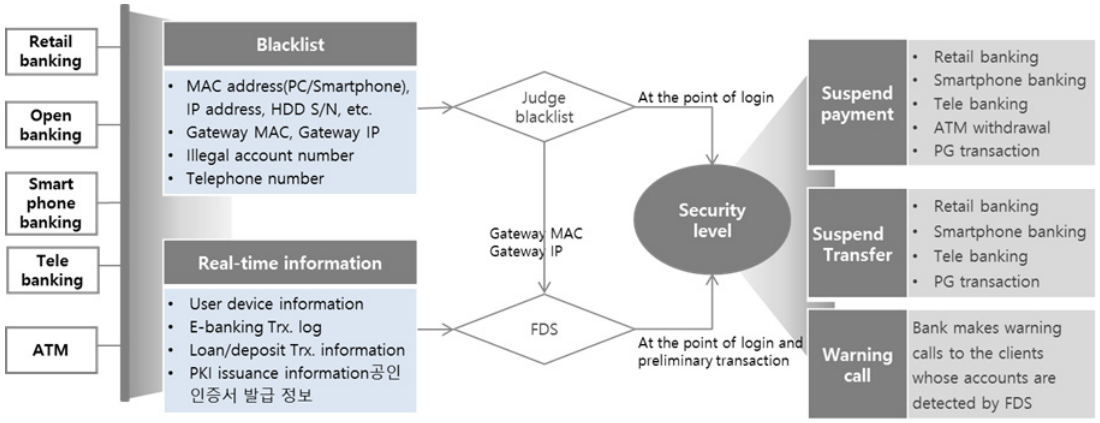

Fig. 3. Workflow using blacklist and FDS

지를 탐지할 경우 오탐율은 높아지게 된다. 오탐율을 낮추기 위해 블랙리스트 MIDDLE 레벨 정보와 FDS 통계모델과 연동한 탐지기법을 사용하도록 한다. 블랙리스트로 등록된 Gateway MAC주소와 Gateway IP로 사용자가 접속을 할 경우 FDS 통계모델을 이용하여 탐지하도록 제안한다. FDS 통계모델은 이용자가 정상적으로 이체를 수행한 과거거래정보를 가지고 접속채널(인터넷뱅킹, 스마트폰뱅킹, 폰뱅킹), 단말정보(MAC 주소, HDD S/N, IP주소), 접속매체정보(Window PC, Mac PC, 안드로이도 폰, 아이폰), 로그인방식(아이디/PW, 공인인증서, 생체인증), 거래금액, 거래시간, 거래계좌, 접속국가 등을 프로파일링(profiling)하여 통계화 시킨 정보를 말한다. 블랙리스트 Gateway MAC 주소 및 Gateway IP주소라 함은 불법단말에서 사용하는 인터넷공유기 또는 네트워크 라우터(router) 및 스위치(switch) 등의 로컬(local) 네트워크장비의 MAC주소 및 IP주소라 할 수 있다.

Table 10. 은 FDS시스템의 일반적인 Rule기반 탐지기법과 블랙리스트 DB정보와 FDS시스템 통계모델과 연동한 탐지기법의 정탐율을 비교한 자료이다. 〔탐지기법 A〕는 수집한 접속정보와 거래정보를 수집하여 Rule 기반 탐지패턴을 이용한 일반적인 탐지기법이며, 〔탐지기법 B〕는 블랙리스트 DB에 등록된 Gateway MAC주소와 Gateway IP주소를 FDS 통계모델과 연동한 실시간 탐지기법이다. Rule 기반 탐지기법보다 블랙리스트 단말정보와 FDS 통계모델을 연동한 실시간 탐지기법의 정탐율이 높은 것을 볼 수 있다.

Table 10. Correct detection rate using blacklist and FDS detection method

Detection method	Mar. 2015	Apr. 2015	May 2015	Correct detection rate
Method A	38 %	11 %	26 %	27 %
Method B	46 %	100 %	78 %	56 %

3.4 특징적 패턴에 따른 실시간 탐지기법

본 논문에서 제안한 블랙리스트 기반 탐지기법의 자동화 방안과 블랙리스트 레벨링 DB 정보를 통한 FDS 통계모델을 연동한 실시간 탐지기법외에 거래정보와 환경매체 정보를 프로파일링 한 후 Rule 패턴을 설정할 때 분석된 새로운 불법이체 사고에 대한 특징적인 패턴을 시스템에 적용하여 오탐율을 줄이고 사고위험을 예방하는 방안을 제안한다. Fig. 4. 는 K은행의 기간별 전자금융 사고에 대한 채널 별 현황과 사고 원인 별 현황을 분석한 자료로 2014년 중반에는 인터넷뱅킹 사고 비중이 높았으며 최근에 스마트폰뱅킹 사고 비중이 높은 것을 볼 수 있다. 즉, 변화하는 사고유형을 신속하고 정확하게 Rule을 구성하여 FDS 시스템에 적용하는 것이 중요하다. 2014년에는 인터넷뱅킹 사고와 스마트폰뱅킹 사고가 비슷한 비율로 발생하였지만, 최근 불법사고가 많이 발생하는 2015년 5월달 전자금융사고 통계를 보면 전체 사고에서 스마트폰 뱅킹 사고가 81%로 높은 비중을 차지하고 있다. 스마트폰 뱅킹 사고에서 아이폰(아이패드 포함)을 이용한 금융사고가 90% 이상 차지하

Month	Internet Banking	Smart phone banking	Tele banking
Jan. 2014	15%	85%	0%
Feb. 2014	29%	64%	7%
Mar. 2014	20%	60%	20%
Apr. 2014	44%	38%	19%
May 2014	43%	53%	4%
June 2014	45%	55%	0%
July 2014	60%	38%	2%
Aug. 2014	52%	43%	5%
Sep. 2014	49%	42%	9%
Oct. 2014	64%	26%	10%
Nov. 2014	67%	27%	6%
Dec. 2014	23%	61%	16%
Jan. 2015	42%	38%	20%
Feb. 2015	27%	58%	15%
Mar. 2015	46%	46%	8%
Apr. 2015	40%	56%	4%
May 2015	11%	81%	7%

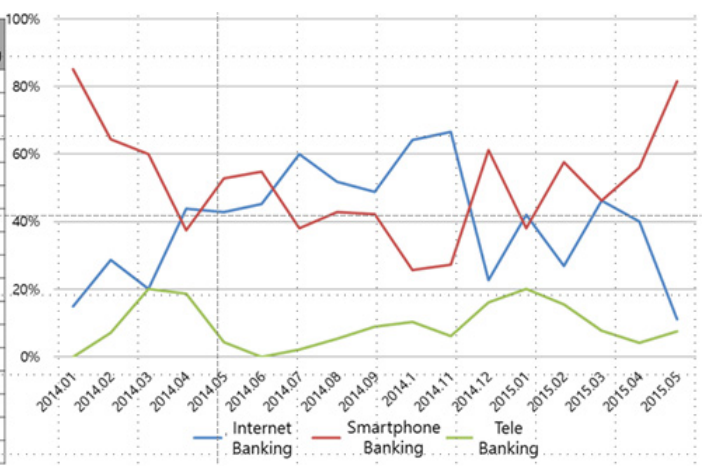

Fig. 4. e-Banking incidents cases by channel in 2014 and 2015

고 있는 상황이다. 아이폰은 단말기 정책상 안드로이드 폰보다 단말기 정보를 수집하는데 제약이 있으며, 그 정책을 악용하여 전자금융 사고가 많이 발생한다. 전자금융 사고 유형은 수시로 변하고 있으며, 빠른 분석을 통해 유형을 적용하는 것이 필요하다. 스마트폰뱅킹 중 아이폰 및 아이패드를 통한 불법이체사고가 증가하기 때문에 아이폰 및 아이패드 사용자를 특징적 패턴으로 분류하여 다른 접속 정보와 비교하여 이상금융거래를 탐지하는 것을 제안한다.

Fig. 5. 는 특징적 패턴 구성도이며 불법사고 특징적 패턴을 일반적 Rule 패턴과 연동하여 탐지할 경우 정탐율을 높일 수 있다. 불법사고 특징적 패턴은 수시로 변경되기 때문에 추가 · 삭제 · 변경이 용이하도록 구성되어야 한다. Table 11. 과 같이 FDS 시스템 내에는 일반적인 Rule 패턴, 사용자 프로파일링, 불법사고 특징적 패턴으로 구별하여 구성해야 한다. 일반적인 Rule 패턴의 경우 모든 전자금융사고에 적용되는 동일한 패턴으로서 사용자가 로그인 또는 예비거래 시 기존에 사용하지 않은 최초 단말 정보일 경우와 예비거래 시 기존에 사용하지 않은 최초 입금계좌가 해당된다. 사용자 프로파일링의 경우 기존에 사용하던 사용자별 전자금융 단말정보 및 전자금융 거래 유형을 말한다. 불법사고 특징적 패턴의 경우는 기간에 따른 사고 유형별 패턴을 말한다.

불법사고 유형을 보면 일반적인 Rule 패턴과 사용자 프로파일링의 패턴은 거의 변화하지 않는다. 그러므로 이상금융거래 탐지 시스템에서 일반적 Rule 패턴과 사용자 프로파일링과 불법사고 특징적 패턴을 신속하고 정확하게 분석하여 적용하도록 한다.

Table 11. FDS rule setting status

Setting type	Summary
Normal rule pattern	Same patterns of all e-banking transactions - The first device and deposit account for preliminary transaction
User profiling	e-Banking device information and transaction type by user - Access device information, access method, logon method, transaction time, access country
Typical illegal incident pattern	Typical pattern by incident - The incidents using I-phone and I-pad smartphone banking are increasing - Multi user logon history using a same device

Fig. 6. 는 특징적 패턴 흐름도를 나타낸다. 사용자가 로그인이나 예비거래를 할 경우 우선 일반적 rule 패턴을 통해 단말정보 및 입금계좌를 확인하고, 특징적 rule 패턴과 사용자 프로파일링을 비교하여 정상고객의 사용 여부를 판단하여 이체정지 및

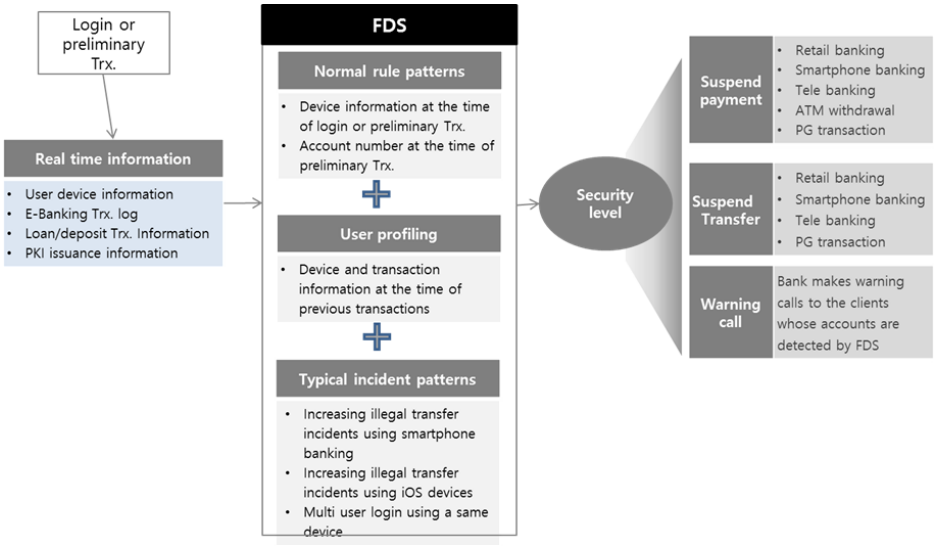

Fig. 5. Diagram of typical pattern method

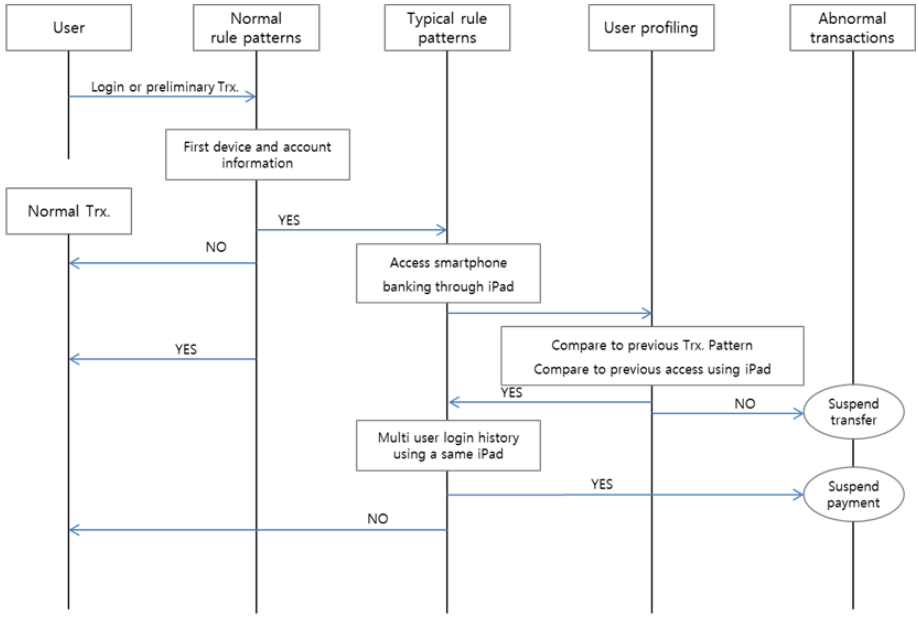

Fig. 6. Workflow of Typical pattern method

지급정지 제한을 두도록 한다.

본 논문에서 일반적 Rule 패턴만 적용한 정탐율과 불법사고 특징적 패턴을 적용한 후의 정탐율을 비교한다. 정탐율은 수식 (1) 과 같이 FDS Detection Number와 Related Accident Number의 비율로 계산한다.

$$\text{정탐율 (\%)} = \frac{\text{Related Accident Number}}{\text{FDS Detection Number}} \times 100 \text{ ---------- 수식(1)}$$

FDS Detection Number는 일반적인 Rule 패턴과 특징적 패턴을 조합하여 적용한 탐지건수이며, Related Accident Number는 FDS시스템 탐지건 중 예방콜(Outbound Call)을 통해 고객이 직접 사고로 확인한 예방 건수이다.

K은행의 2015년 상반기 불법이체사고의 특징적 패턴은 스마트폰뱅킹의 아이폰 및 아이패드(iPad) 단말을 통한 불법이체사고가 지속적으로 발생하는 것으로 2015년 5월 1일부터 5월 31일 한 달간 스마트폰뱅킹 거래에 대하여 일반적인 Rule 패턴과 사용자 프로파일링에 특징적 패턴을 조합하여 이상금융거래 탐지를 적용하였으며, 탐지된 내역을 예방콜을 통하여 30건(Related Accident Number)의 불법이체사고를 예방할 수 있음을 확인하였다.

Table 12. 와 Table 13. 은 K은행의 2015년 5월 1일부터 5월 31일까지 일반적인 Rule 패턴만 적용하여 탐지한 경우와 특징적 패턴을 조합하여 탐지한 경우의 정탐율을 비교한 자료이다. Table 12. 는 일반적인 Rule 패턴으로만 탐지한 경우의 정탐율을 테스트한 것으로 일반적인 Rule 패턴은 스마트폰 뱅킹을 통하여 사용자가 최초단말 및 최초입금계좌로 이체를 시도하는 경우를 탐지한 조건이다. 이유는 범죄자는 탈취한 사용자의 금융정보를 가지고 범죄자 단말에서 범죄자의 대포통장으로 불법이체를 시도하기 때문에 사용자 입장에서는 범죄자의 단말은 최초단말이며, 범죄자의 대포통장은 최초입금계좌로 정의할 수 있다. Table 12.에서 보듯이 일반적인 Rule 패턴으로만 탐지한 경우의 정탐율(0.182%)은 매우 낮다.

Table 13. 은 일반적인 Rule 탐지와 사용자 프로파일링에 불법사고 특징적 패턴을 포함시켜 테스트한 결과이다.

특징적 패턴1(TP1 : Typical Pattern1)은 사용자가 아이폰 및 아이패드로 로그인하여 이체를 시

Table 12. General rule detection

General rule detection	Related accident number	FDS detection number	Correct detection Rate
Case	30	16,404	0.182%

Table 13. Typical pattern detection

Typical pattern detection	Related accident number	FDS detection number	Correct detection Rate
Case TP1	30	367	8.18%
Case TP2	30	41	73.33%

도한 경우의 조건이며, 특징적 패턴2(TP2 : Typical Pattern2)는 사용자가 아이폰 및 아이패드로 이체 시도할 때 동일단말로 다수의 다른 사용자 아이디로 로그인 기록이 있는 경우의 조건이다. Case TP1은 일반적 Rule 패턴(사용자가 최초단말로 최초입금계좌로 이체를 시도한 경우)과 사용자 프로파일링(사용자의 접속채널, 접속단말, 로그인방식, 접속국가, 이체금액 등) 통계정보와 TP1을 조합하여 탐지한 정탐율을 테스트한 것이며, Case TP2는 일반적인 Rule 패턴과 사용자 프로파일링 통계정보와 TP2를 조합하여 탐지한 정탐율을 테스트한 결과이다. 테스트 결과 특징적 패턴을 적용함으로서 정탐율(8.18%)이 증가하였고, TP2 와 같이 특징적 패턴 조건을 구체적으로 정의한 결과에 따라 정탐율(73.33%)이 현저히 증가됨을 확인할 수 있었다. 결론적으로 현재 발생빈도가 높은 전자금융사고의 패턴을 신속히 분석하여 특징적 패턴을 시기 적절하게 변경하여 적용하는 것이 이상금융거래 탐지에 효과적이다.

IV. 적용사례 및 검증

본 논문에서 제안한 블랙리스트기반 탐지기법 자동화, 보안레벨에 따른 블랙리스트 정보와 통계모델을 연동한 실시간 탐지기법, 특징적 패턴에 따른 실시간 탐지기법 방안의 효과성을 검증하기 위해서 K은행의 이상금융거래 탐지 시스템에 실제 적용(2015.07.01 ~ 2016.06.30)하여 전자금융 불법이체사고 현황 및 예방 추이를 연구 하였다.

Table 14. 는 K은행에 본 연구에서 제안한 탐지기법을 적용 전과 적용 후의 전자금융채널 유형 별 불법이체 사고내역을 나타낸다. 제안한 탐지기법 적

Table 14. Illegal transaction incidents of K bank

Time	Year	Month	Internet banking	Smartphone banking	Tele banking	Sum
Before implementation	2015	Jan.	23	20	10	53
		Feb.	8	12	4	24
		Mar.	17	13	2	32
		Apr.	10	14	1	25
		May	3	22	2	27
		June	6	13	0	19
	Total (Mon Avg)					**180 (30)**
After implementation	2015	July	3	1	1	5
		Aug.	4	1	0	5
		Sep.	1	1	0	2
		Oct.	1	1	1	3
		Nov.	1	2	0	3
		Dec.	0	1	0	1
	2016	Jan.	6	0	0	6
		Feb.	0	1	0	1
		Mar.	2	2	0	4
		Apr.	2	3	0	5
		May	2	1	0	3
	Total (Mon Avg)					**38 (3.5)**

용 전에는 월 평균 30건의 불법이체 사고가 발생하였으나, 적용 후에는 월 평균 3.5건 정도로 약 88%의 불법이체 사고가 감소함을 알 수 있다.

Table 15. 는 K은행에 본 연구에서 제안한 탐지기법을 적용 전과 적용 후의 예방율을 나타낸다. 예방율은 수식 (2) 와 같이 사고건수와 예방건수의 합과 예방건수의 비율로 계산한다.

$$\text{예방율}(\%) = \frac{\text{예방건수}}{(\text{사고건수} + \text{예방건수})} \quad \text{---- 수식(2)}$$

사고건수는 고객이 은행에 불법이체사고로 신고한 건수이며, 예방건수는 은행이 탐지된 이상금융거래에 대하여 고객에게 직접 예방콜을 통하여 사고를 예방한 건수이다. 제안한 탐지기법을 적용 전에는 예방율이 69% 이나, 적용 후에는 예방율이 87% 로 증가함을 확인할 수 있다. 특히 적용 후(11개월간) 예방건수 총 261건에 2,773백만원을 예방 하였다. 이는 제안한 세 가지 탐지기법이 이상금융거래 탐지 시스템에 효과적으로 응용되어 이상금융거래를 실시간으로 탐지함으로써 불법이체사고 예방에 효율적인 대안임을 알 수 있다.

결과적으로 제안한 블랙리스트기반 탐지기법 자동화를 통하여 동일한 불법단말에서의 추가 사고 발생을 차단함으로써 2차 피해를 최소화 할 수 있었으며, 보안레벨에 따른 블랙리스트 정보와 통계모델을 연동한 실시간 탐지기법을 통하여 불법단말의 Gateway MAC주소와 Gateway IP주소의 통계모델를 연동한 탐지기법을 활용하여 인터넷뱅킹을 통한 불법이체 사고를 사전에 예방 할 수 있었다. 마지막으로 특징적 패턴에 따른 실시간 탐지기법을 신속하게 적용하여 스마트폰뱅킹을 통한 불법이체 사고를 효과적으로 대응 할 수 있었다.

Table 15. Prevention rate of K bank

Time	Number of incidents	Number of prevention	Prevention rate
Before	180	398	69%
After	38	261	87%

V. 결론 및 향후 연구과제

전자금융서비스가 증가함에 따라 고객의 금융자산 탈취 행위는 점점 고도화 되고 있으며 탈취한 정보를 가지고 다양한 전자금융채널을 통하여 불법이체 시도가 끊임없이 발생하고 있다. 금융회사는 끊임없이 발생하고 있는 불법이체 시도를 예방하기 위하여 이상금융거래 탐지 시스템을 구축 운영 중에 있다. 본 논문에서는 국내은행의 전자금융 이상금융거래 탐지 시스템 운영 환경에 적합한 세가지 탐지기법과 대응모델을 제안하였다. 제안한 탐지기법인 블랙리스트기반 탐지기법 자동화, 보안레벨에 따른 블랙리스트 정보와 통계모델을 연동한 실시간 탐지기법, 특징적 패턴에 따른 실시간 탐지기법을 K은행 FDS 시스템 운영환경에 실제 적용하여 적용 전과 적용 후의 불법이체 사고 추이를 비교 분석하였다. 제안한 탐지기법을 적용한 결과 실제 FDS 시스템에서 정확한 이상금융거래 사전 탐지를 통하여 불법이체 사고를 88% 정도 감소시키는 효과를 검증 하였다. 그러나 특징적 패턴에 따른 실시간 탐지기법은 불법이체 사고 이후 종합 분석을 통하여 특징적 패턴을 얼마나 신속하고 정확하게 적용하는지에 따라 정탐율이 높아지는 등 FDS 시스템 사고분석 담당자들의 분석 능력에 따라 탐지율의 차이가 날 수 있는 한계를 가지고 있음을 알 수 있었다. 하지만 본 논문에서 제시한 세가지 탐지기법 및 대응모델을 국내 금융회사의 이상금융거래 탐지 시스템에 적용한다면 지능화된 전자금융 불법이체 시도로부터 신속하게 대처함으로써 사고를 예방할 수 있을 거라 확신한다.

향후에는 이상금융거래 탐지 시스템의 미탐율을 최소화할 수 있으며, 사고분석 담당자들의 분석 능력에 상관없이 FDS 시스템에서 상관관계를 자동분류하며 사전적 대응이 가능하며 가설 없이 다차원 분석이 가능한 딥러닝(deep learning) 기반의 탐지기법을 연구하여 효율적인 이상금융거래 탐지 대응방안을 제시하고자 한다.

References

[1] Internet banking service use status in the 1st quarter of 2016,The Bank of Korea, May. 2016.

[2] Statistics about responding against internet hacking incidents, KISA(Korea Internet and Security Agency), Mar. 2015.

[3] Guideline to fully implement e-banking

fraud detection service, FSS(Financial Supervisory Service), May. 2013.
〔4〕 Trends report on detecting malware concealing sites, KISA(Korea Internet and Security Agency), July. 2016.
〔5〕 Financial Security Comprehensive Plan, FSC(Financial Services Commission), Nov. 2013.
〔6〕 FDS upgrade Roadmap for financial industry, FSS(Financial Supervisory Service), Dec. 2014.
〔7〕 FDS technology guide, FSI(Financial Security Institute), Aug. 2014.
〔8〕 e-Banking transactions will be safer and more convenient, FSS(Financial Supervisory Service), Aug. 2016.
〔9〕 Eun Young Park, Ji Won Yoon, "A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking," Journal of Society for e-Business Studies VOL. 19, NO. 4, Nov. 2014.
〔10〕 J.T.S. Quah and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence," Expert systems with applications VOL. 35, NO. 4, pp. 1721-1732, Dec. 2007.
〔11〕 Jae Hoon Park, Huy Kang Kim, Eunjin Kim, "Effective Normalization Method for Fraud Detection Using a Decision Tree ," Journal of The Korea Institute of Information Security & Cryptology VOL.25, NO.1, Feb. 2015.
〔12〕 Eui Soon Choi, "A Study on Improvement of Effectiveness Using Anomaly Analysis rule modification in Electronic Finance Trading," Graduate School of Korea University, June. 2014.

〈저자소개〉

유 시 완 (Si-wan Yoo) 정회원
1988년 2월: 고려대학교 수학과 졸업
1990년 9월~현재: 한국투자금융입사 및 KEB하나은행 IT그룹 전무
2014년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호 정책 및 제도, 전자금융보안, 생체보안