한국경호경비학회 – 제62호(2020): 185–203
https://doi.org/10.36623/KSSR.2020.62.8
투고일 2020. 01. 31 심사일 2020. 03. 08 게재확정일 2020. 03. 12

빅데이터와 FDS를 활용한 보이스피싱 피해 예측 방법 연구

이 승 용 · 이 주 락

빅데이터와 FDS를 활용한 보이스피싱 피해 예측 방법 연구

이 승 용* · 이 주 락**

〈요 약〉

2009년 이후 전체 범죄는 감소하고 있지만, 보이스피싱은 오히려 급증하고 있다. 정부와 학계에서는 이를 근절하기 위해 다양한 대책을 제시하고 연구를 진행해 왔으나 진화하는 보이스피싱을 따라잡기에는 역부족이다.

이 연구에서 연구자들은 범인 검거와 피해회복이 어려운 보이스피싱의 피해 예방에 초점을 두었다. 특히, 피해자가 금융거래행위(계좌이체 등)를 한다는 점이 금융사기(이상거래)와 유사하다는 점에 착안하여, 금융사기 탐지에 활용되고 있는 이상거래탐지시스템(FDS)을 활용한 보이스피싱 예측 방안을 연구하였다. 그 결과 머신러닝 기반의 이상거래탐지시스템(FDS)에 보이스피싱과 관련한 통화내역, 메신저내역, 대포통장, 보이스피싱 유형과 112신고 등 빅데이터를 결합한 방안을 개념적으로 도출하였다.

이 연구에서는 주로 정부 대책과 빅데이터 활용과 관련한 문헌연구를 중심으로 연구를 진행했다. 그러나 데이터 수집의 한계와 FDS의 보안 문제로 구체적인 모델까지를 제시하지는 못하였다. 다만, 관련된 선행연구가 없는 현실에서 머신러닝을 위해 필요한 데이터 종류와 FDS를 융합한 보이스피싱 대응방안의 개념을 최초로 제시했다는 점에 의미가 있다. 향후 이 연구를 바탕으로 '보이스피싱 피해 예측 시스템'이 개발되어 보이스피싱 피해가 근절되기를 기대한다.

주제어 : 보이스피싱, 빅데이터, 머신러닝, 이상거래탐지시스템, FDS.

* 경기대학교 일반대학원 경호보안학과 박사과정 (제1저자)
** 중앙대학교 산업보안학과 교수 (교신저자)

목 차

Ⅰ. 서 론

보이스피싱은 2016년까지 감소하였다가, 2017년부터 다시 증가하고 있다. 2018년 보이스피싱(Voice Phishing, 전화금융사기) 피해액은 전년도보다 82.7%가 증가한 4,440억 원으로 매일 134명이 1인당 9천 1백만 원의 피해를 보고 있는 셈이다(금융감독원, 2019).

2019년 치안정책연구소 치안전망에 따르면, 전체 범죄는 감소하고 있지만, 금융위기 이후 세계적인 경제 침체 속에서 실업률 및 가계부채 증가와 정부의 대출 규제 정책으로 인해 보이스피싱은 계속 증가할 것으로 예상된다.

정부는 이러한 보이스피싱에 대응하기 위해 2011년부터 2018년까지 3차례에 걸쳐 범정부 합동대책[1]을 마련해서 추진해 왔다. 2018년에 경찰은 2017년 25,473명보다 47.7% 증가한 총 37,624명의 보이스피싱 사범을 검거하였다.

이처럼 보이스피싱범죄가 중요한 사회문제가 되자 이와 관련된 많은 연구가 수행되었다. 그동안의 보이스피싱 대응을 위한 연구를 살펴보면, 피해 금액 지급정지 등 특별법 제정, 전담 수사기구 편재와 피해 예방 홍보 및 교육, 보안기술 강화 등의 대응방안을 주로 제시하고 있다. 하지만, 보이스피싱 범죄가 계속 증가하는 추세로

1) 대국민 홍보 강화, 지연 인출 · 이체 등 제도를 정비하고 법적 처벌도 강화

볼 때, 기존의 정부 대책과 선행연구의 대응방안으로는 진화하는 보이스피싱 대응에는 역부족인 것으로 보인다. 따라서 기존 방법과 다른 새로운 관점에서 대응방안을 연구할 필요가 있다.

이 연구에서는 연구자들은 보이스피싱은 피해자가 직접 금융거래를 한다는 특징에 주목하였다. 이러한 특징과 관련 있는 금융사기 탐지에 활용되고 있는 이상거래탐지시스템(FDS)을 활용하는 방안을 검토했다. 그리고 보이스피싱과 관련한 통신사, 금융기관, 경찰범죄정보 등의 빅데이터에 최근 범죄예측에 효과가 있은 것으로 밝혀진 빅데이터 분석기법을 적용해서 보이스피싱을 예측하는 방안에 관해 개념적으로 연구하였다.

다만, 이 연구에서 보이스피싱과 관련한 빅데이터는 통화내역이나 금융정보 같은 개인정보로 확보하기 어려웠고, 금융기관의 FDS는 외부에 공개하지 않기 때문에 실제 모델을 검증하는 단계까지 진행할 수는 없었다. 그러나 빅데이터 분석을 위해 필요한 데이터 종류와 머신러닝 기법을 활용한 모델을 구성하는 단계까지의 연구를 진행할 수 있었다.

이 연구는 관련 논문, 인터넷, 정부기관 자료와 정책자료 등 문헌연구를 중심으로 진행했다. 특히, 선행연구 중에서 보이스피싱에 대응하기 위해 빅데이터 분석기법을 활용한 연구는 없었기 때문에, 일반적인 범죄예측과 관련한 빅데이터 활용 사례와 금융사기를 탐지하기 위한 여러 연구를 비교 분석하는 방식으로 이 연구를 진행하였다.

Ⅱ. 보이스피싱 사례와 선행연구 검토

1. 보이스피싱 현황 및 유형

2017년부터 급격히 증가하고 있는 보이스피싱은 그 수법과 유형이 진화하고 있다. 금융감독원의 2019년 자료에 따르면, 대출이 어려운 서민들에게 대출할 수 있다고 하거나, 낮은 금리로 대출해 준다고 하며 수수료 등을 편취하는 '대출빙자형' 피해액이 2017년 대비 71.1% 증가한 3,093억 원으로 전체 피해액의 69.7%를 차지하고 있다. 그 외에 검찰이나 경찰 등을 사칭하거나, 불법적으로 수집한 개인정보를 이용해서 카카오톡과 같은 메신저 등을 통해 등록된 지인에게 금전을 요구하는 '사칭형' 피해

액이 2017년 대비 116.4% 증가한 1,346억 원으로 전체 피해액의 30.3%에 해당하는 것으로 확인되었다.

특히, 카카오톡으로 지인을 사칭해서 소액의 금전을 요구하는 사례는 9,601건으로 2017년 1,407건보다 582.4% 급증하였다. 피해액 또한 2017년 58억 원보다 272.1% 증가한 158억 원이었다. 구체적인 피해 유형과 수법은 다음 <표 1>과 같다.

〈표 1〉 보이스피싱 주요 범죄 유형

주요유형	수법
자녀납치 및 사고를 빙자해서 편취	범행 전에 부모와 자녀의 연락처를 확보한 범인이 부모에게 변조한 자녀의 전화번호로 전화를 해서 납치나 사고를 당했다는 식으로 기망해서 계좌이체 등으로 편취
메신저에서 지인을 사칭해서 송금 요구	해킹한 메신저 아이디 계정에 등록된 피해자의 지인과 메신저 대화를 통해 교통사고 등 급하게 돈이 필요하다고 속여서 편취
인터넷 뱅킹을 이용해서 카드론 대금 및 예금 등 편취	피해자가 범죄사건으로 수사 받고 있다는 등으로 속여서 가짜 은행사이트(피싱사이트)에 접속하도록 한 후, 입력한 정보를 통해 알아낸 피해자의 신용카드나 인터넷뱅킹 정보를 이용해서 범인이 피해자인 척 가장해서 피해자의 인터넷뱅킹 등으로 카드론이나 신용대출을 받고 범인의 계좌로 이체
금융회사, 금감원 명의의 허위 긴급공지 문자메시지로 기망, 피싱사이트로 유도해서 예금 등 편취	은행에서 보안승급 내용과 함께 피싱사이트 링크 문자를 받은 피해자가 링크를 클릭해서 피싱사이트(가짜 은행 홈페이지)에 접속, 계좌번호, 공인인증서 정보를 입력하면 범인이 이 정보로 피해자의 계좌에 있는 금액을 이체하거나 대출 등을 받아 편취
전화통화를 통해 텔레뱅킹 이용정보를 알아내어 금전 편취	주로 50대 이상 고령층인 피해자를 대상으로 전화하여 피해자의 계좌가 범죄에 악용되었다는 등으로 현혹시켜 주민등록번호나 보안카드 일련번호 등을 알아내서 피해자의 계좌에 있는 금액 이체
피해자를 기망해서 자동화기기로 유인 편취	경찰이나 검찰을 사칭한 범인이 피해자에게 전화해서 피해자 계좌가 범죄에 악용되어 조치가 필요하다는 등으로 속여서 범인의 계좌로 금전을 이체하게 하거나, 개인정보가 유출됐다고 믿은 피해자에게 금융기관 직원이 개인정보를 유출했다며 직원들 모르게 자동화기기에서 이체하도록 해서 편취
피해자를 기망해서 피해자에게 자금을 이체토록 해서 편취	범인이 경찰이나 검찰을 사칭하며 수사를 위해 피해자 계좌거래내역을 확인해야 한다며 범인의 계좌로 이체하도록 하거나, 국세청 직원이라고 한 후, 미납한 세금을 납부하라고 속여서 범인의 계좌로 송금하도록 해서 편취
신용카드정보 취득 후 ARS를 이용한 카드론 대금 편취	피해자의 신용카드 정보를 알아낸 범인이 ARS로 카드론 대출을 받은 후, 피해자에게 범죄자금이 입금되었다고 속여서 범인의 계좌로 이체하게 한 후 편취

주요유형	수법
상황극 연출을 통한 피해자 기망 편취	피해자에게 전화로 경찰이나 검찰에서 수사하는 상황이 들리도록 하는 방법으로 피해자를 속인 후, 범죄에 악용된 피해자의 계좌 거래내역 확인을 위해 필요하다며 범인 계좌로 자금을 이체하도록 해서 편취
물품대금 오류송금 빙자로 피해자를 기망해서 편취	피해자에게 물품대금 등 허위의 계좌입금 문자를 보낸 후, 잘못된 계좌로 송금했다고 반환을 요구하며 편취

※ 출처: 금융감독원 보이스피싱 지킴이 홈페이지 – 연구자 재구성

2. 선행연구

보이스피싱과 관련한 선행연구를 살펴보면, 윤해성·곽대경(2009)은 우리나라와 대만·일본 등 외국의 보이스피싱 사례를 연구하며, 보이스피싱 대응을 위해 1) 관련 법률 정비, 2) 전담부서 신설 등 제도 정비, 3) 보안시스템 강화 등 광범위한 대응방안을 제시하였다. 조호대(2012)는 조작·변작 전화번호 발신 차단, 국제 공조수사 강화 등의 방안을 제시했으며, 이범주 외(2016)는 보이스피싱 음원을 분석해서 범죄자의 음원과 대조, 기술적으로 차단하는 애플리케이션 개발을 제안하였다. 이승아(2018)는 보이스피싱 범인의 텍스트 언어학적 분석을 통해 특징을 도출한 연구를 수행하기도 하였다. 김덕용(2018)은 경찰의 광역수사체제 강화와 황금시간대 TV 홍보를 제안하였고, 이기수(2018)는 보이스피싱 단순가담자라도 처벌을 강화하도록 법률 개정 필요성을 제시하였다. 또한, 홍성삼(2019)은 세계 각국의 피싱범죄 대응책을 연구해서 보이스피싱은 법집행기관과 자치단체가 협력해서 단계별로 예방정책을 마련해야 하고, 해외 범죄인 송환을 위한 노력 및 피해구제를 위한 정책도 필요하다는 연구를 하였다. 이상의 연구를 정리하면 아래 <표 2>와 같은데, 선행연구에서 나타나는 법률적, 제도적, 기술적 대응방안은 30분 지연 인출·이체 제도나 지급정지 및 피해자 환수 간소화 등으로 제도화되어 있다. 또한, 수사나 홍보와 같은 정부 기관의 대응도 전담수사팀 운영 및 보이스피싱 홍보 활동 등 강화되었다. 그러나 이러한 선행연구 중 어느 것도 최근 범죄예측과 예방에 효과를 보고 있는 빅데이터를 활용한 방안에 관한 것은 없었다. 최근 급증하고 있는 보이스피싱 추세를 보면, 지금과는 다른 새로운 대응방안에 관한 연구가 필요한 것으로 보인다.

〈표 2〉 보이스피싱 대응을 위한 선행연구

연구자	대응방안
윤해성, 곽대경(2009)	1) 범죄 처벌을 위한 통합 법률 제정 2) 부정계좌 지급정지 제도의 법률적 근거 강화 3) 불법 외국환 송금 처벌 근거 강화 4) 국제 보이스피싱 범죄 처벌 특별법 제정 5) 피해금 회수를 위한 형사소송법 개정 6) 대포통장 관련 법률 제·개정 7) 전담부서 신설 8) 피해 예방 홍보 및 교육 강화 9) 국제 공조수사 확립 및 국제 법규 마련 10) 개인정보보호 대책 마련 11) 정보통신기술과 보안체계 확립 12) 송금 시 음성·문자 알림 서비스 구축 13) 바이오 생체 인식을 통한 송금 차단 14) 인터넷 뱅킹과 모바일 뱅킹의 예방 15) VPN을 통한 차단
조호대(2012)	1) 조작·변작된 발신 번호 차단 시스템 개발 2) 범죄에 사용된 통장 명의인의 다른 통장도 지급정지 3) 경찰 전담 수사부서 구성 4) 경찰 단속 활동 강화, 신속한 수사 착수 5) 인터폴 등을 통한 국제 공조 강화
이범주 외 (2016)	보이스피싱 음원을 분석해서 범죄자의 음성 데이터베이스와 대조하여 기술적으로 차단하는 애플리케이션 개발 제안
이승아(2018)	보이스피싱 범인의 텍스트 구조적 특징과 언어적 특징을 분석한 결과 전문용어나 한자어 등 사용을 통해 사회적 지위를 노출하는 '권력의 원리', '공손의 원리', 특정한 숫자를 사용해서 구체적으로 전달하는 '장면의 원리'가 있다는 것을 밝힘
김덕용(2018)	1) 경찰서와 광역수사체계의 유기적 협조 및 ATM기기 주변 순찰 강화 2) 경찰청, 금융위원회 등 기관 통합 단일 국가기관 신설 후 종합대응 3) 해외발신번호 변작행위 근절 4) 홍보 효과 극대화를 위해 TV 정규뉴스 및 황금시간대 홍보 집중 및 긴급 문자발송 5) 피해회복을 위한 전담센터 설치 및 징벌적 배상제도 도입
이기수(2018)	보이스피싱 단순가담자에 대한 처벌 강화 및 범죄수익 몰수를 위해 관련 법 개정(전자금융거래법, 범죄수익 은닉의 규제 및 처벌 등에 관한 법률)
홍성삼(2019)	Brantingham & Faust(1976)의 범죄예방 3단계 모델을 적용, 인터폴과 미국 등 대응방안을 분석해서 1단계 사례 홍보(자치단체 포함), 2단계 피해 발생 후 대응 강화, 3단계 재범방지를 위한 국제공조 활성화 등을 제시

Ⅲ. 빅데이터 활용 범죄예측과 FDS 개관

1. 범죄예방을 위한 빅데이터 분석기법 활용 사례

최근 범죄예방과 예측을 위해 빅데이터를 활용한 분석기법이 활용되고 있다. 빅데이터는 기존의 일반적인 기술로 관리하기 어려운 수십 테라바이트(Terabyte)에서 수 페타바이트(Petabyte)의 데이터를 의미하는데, 그 데이터의 양뿐만 아니라, 데이터 종류가 다양하고, 데이터 생성 속도가 빠르다는 속성을 지닌다.

형사사법 영역에서 빅데이터는 1) 범죄 발생 시기와 지역을 예측하는 범죄예측, 2) 사건 발생 시 관련된 용의자 선정, 3) 증거의 신빙성 판단, 4) 범죄자의 상습성 및 재범 가능성 예측에 활용되고 있다(윤해성 외, 2014).

빅데이터를 활용한 범죄예방시스템 중에서 미국의 프레드폴(Predpol), 파일럿(PILOT: Predictive Intelligence-Led Operational Targeting), 다스(DAS: Domain Awareness System)와 우리나라의 지리적 프로파일링 시스템(GIS: Geographic Information System)에 대해 정리하면 다음 <표 3>과 같다.[2)]

〈표 3〉 빅데이터를 활용한 범죄예방시스템

구분	내용 및 효과	활용기법
프레드폴(PredPol)	- 2011년 미국 산타크루즈 경찰서에서 급증하는 재산범죄 대응을 위해 도입 - 범죄다발지역(핫스팟)에 경찰 우선 배치 - 침입절도 27% 등 최대 29% 범죄 감소	지진 예측 알고리즘에서 시작한 머신러닝
파일럿(PILOT)	- Shreveport 경찰서에서 도입, 범죄정보 외의 지리적, 공간적 정보(수감자, 가석방자 수, 범죄와 무질서 다발지역) 활용 - 범죄다발지역(핫스팟)에 경찰 우선 배치 - 특정지역 재산범죄 40% 감소	로지스틱 회귀분석 등
다스(DAS)	- 뉴욕 경찰청, 실시간 감시와 대응 위주 - 2백대 이상 자동차번호판 탐지기, 3천대 감시카메라, 2천대 방사선 센서, 경찰 데이터베이스 정보 실시간 수집 분석	IBM과 개발한 알고리즘 활용
지리적 프로파일링 시스템(GIS)	- 범죄발생현황, 범죄 다발지역, 112 신고 데이터, 전과자 등 수사대상, 지하철디지털 성범죄, 외국인 등록현황, CCTV - 범죄위험지역 경찰 배치	커널밀도 함수 활용 핫스팟 분석 텍스트마이닝

※ 출처: 탁희성 외(2015) - 연구자 재구성

2) 오요한 · 홍성욱(2018)에 따르면 이러한 방법은 빅데이터를 분석하는 전문 알고리즘으로 운영되고 있는데, 백인보다는 흑인을 잠재적 범죄자로 간주한다든지 하는 편향성의 문제나, 사람이 분석하는 것과 별 차이가 없다는 문제도 있긴 하지만 어느 정도 효과가 있는 것으로 검증되었다고 한다.

2. 빅데이터를 활용한 이상거래탐지시스템(FDS)

신용카드 회사, 은행, 증권회사 등은 금융거래를 통한 사기를 예방하기 위해 2014년부터 이상거래탐지시스템(Fraud Detection System: FDS)을 도입해서 운영하고 있다. 특히, 최근에는 빅데이터 분석기법을 활용한 FDS를 활용하고 있는데, 금융감독원(2017)의 보도자료에 따르면 2017년 3,588건(429.7억 원)을 예방하는 성과가 있었다. 이는 평균 예방률 95.4%로 대부분 금융 이상거래는 탐지되고 피해가 발생하기 전에 예방조치까지 성공적으로 적용된다는 것을 알 수 있다.

국내외 금융회사에서 FDS에 빅데이터 분석기법을 도입해서 활용하는 사례는 아래 <표 4>와 같다.

〈표 4〉 국내외 금융회사의 머신러닝 기반 FDS 활용 사례

구분	금융회사	도입 내용
국외	Papal	딥러닝 기반의 FDS가 금융거래 고객 약 1억 7천만 명이 발생시킨 약 40억 건의 거래정보를 학습하여 사기 탐지를 수행
	Paypal	딥러닝 기반 시스템 사용해서 신용카드 사용과 계좌이체 모니터링, 이상징후 발생 시 해당 고객의 사용자 앱으로 통지
	BillGuard	보험 클레임의 약 20%가 사기, 남용 등에서 비롯된 것을 파악하고, 보험금 지급 및 클레임 과정에서의 정확성, 유효성 등을 확인하고자 딥러닝 기반 시스템을 도입
	Sul America	사기로 인한 은행 손실을 감소시키기 위해 딥러닝 기반 FDS 도입
	D'Oro	금융거래 모니터링을 위해 자기조직화맵 알고리즘 기반의 NetReveal 시스템을 개발하였으며, 유사한 형태가 있는 금융거래 이용자들의 행위를 분류해서 이상 행위를 식별
	US Credit Issuer	랜덤포레스트, 서포트벡터머신 등 여러 머신러닝 알고리즘을 활용한 시스템을 도입하여 이상거래의 탐지율 향상
	US Bank	AML(Anti Money Laundering) 시스템의 오탐률을 낮추고자 비지도 및 지도학습 기반의 머신러닝 솔루션 도입
국내	SK증권	룰 방식(오용탐지)과 딥러닝 방식(이상탐지)이 혼합된 하이브리드(오용+이상 탐지) FDS 도입
	신한은행	딥러닝 기반 FDS의 모형을 구축하고, 개발한 학습 모형 16개에 대해 기존 방식과의 정확도 비교 결과 딥러닝 기반 모형의 우수성 확인
	한국스마트카드	딥러닝 기반 FDS를 구축하였고, 시스템 오류를 이상거래로 탐지하는 등의 오탐이 발견되었으나 실제 이상거래에 대해서는 우수한 탐지 성능을 보임

※ 출처: 금융보안원(2017) - 연구자 재구성

머신러닝(machine learning)은 빅데이터를 활용하는 한 분야로 컴퓨터가 스스로 학습할 수 있도록 하는 알고리즘을 개발하는 것이 핵심이다. 머신러닝은 기존 데이터를 학습시킨 후, 이를 통해 새로운 데이터에 예측값을 찾는 것이 목적이다. 즉, 머신러닝은 확률과 데이터를 기반으로 일정한 결과를 추론하기 위해 스스로 학습하는 알고리즘이라고 할 수 있다(송주영·송태민, 2018).

머신러닝 과정은 1) 데이터 모으기와 준비 과정, 2) 피처 선택(Feature Selection), 3) 알고리즘 고르기(Algorithm Choice), 4) 파라미터와 모델 선택, 5) 트레이닝(학습, 훈련), 6) 평가 단계로 구성된다(Marsland, 2016). 이러한 단계별 세부 내용을 정리하면 다음 <표 5>와 같다.

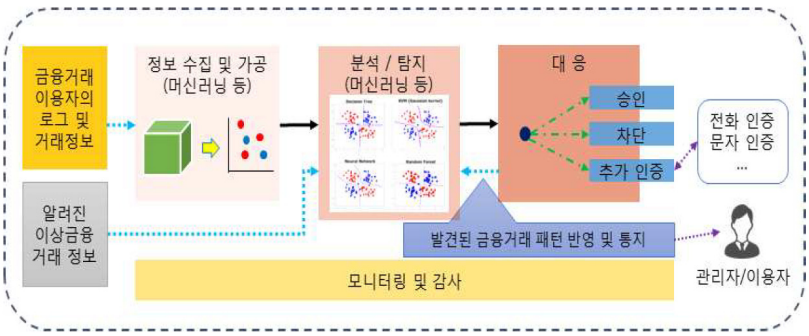
〈표 5〉 머신러닝 개발 단계

단계	내용
데이터 모으기와 준비	데이터 수집 및 가공, 적합한 데이터 선별을 위해 피처 선택 단계 수행 필요, 유용할 것으로 생각되는 피처를 포함한 적당히 작은 데이터를 모으고, 이를 실험해 보고, 최고의 피처를 선택해서 전체 데이터세트를 다시 수집 분석
피처선택(Feature Selection)	직접 실험을 통해 문제에 가장 적합하고 유용한 피처 선별, 어느 정도 문제나 데이터에 관한 사전 지식 요구
알고리즘 고르기(Algorithm Choice)	정확성, 학습시간, 사용 편의성을 고려해서 알고리즘 선택, 알고리즘은 1)지도학습(기존에 이미 분류된 학습용 데이터로 구성된 입력변수와 출력 변수를 활용한 학습), 2)비지도학습(정답이나 목표값이 제공되지 않을 때 사용), 3)강화학습(알고리즘이 출력하는 결괏값에 대해 어느 답이 틀렸다는지 알려 주지만, 어떻게 고쳐야 하는지 알려주지 않아서 알고리즘이 직접 정답을 얻을 때까지 여러 방법을 시도), 4)진화학습(알고리즘에 의해 제출된 답이 얼마나 좋은지에 대한 점수 부여를 통해 학습)으로 분류
파라미터와 모델 선택	대부분 알고리즘은 실험을 통해 적당한 값을 찾아야 하는 파라미터 선택하기 문제를 내포
트레이닝(학습, 훈련)	데이터, 알고리즘, 파라미터가 정해지면 컴퓨터를 사용해서 트레이닝을 하고 모델 생성, 모델은 새로운 데이터에 대해 결괏값을 예측
평가	시스템이 실제로 사용되기 전에 트레이닝 데이터가 아닌 새로운 데이터를 통해 검증하고 평가, 예측값을 실제로 알고 있는 목푯값과 비교

※ 출처: Marsland(2016) - 연구자 재구성

머신러닝을 활용한 FDS 구성은 1) 금융거래 이용자의 금융거래 정보수집 및 가공 단계, 2) 금융거래 정보와 이상금융거래 유형 정보를 머신러닝으로 분석하는 이상거

래 탐지 단계, 3) 이상거래로 탐지된 거래에 대해 추가 인증하거나 차단하는 대응 단계로 이루어져 있다. 이 모든 단계에 대한 모니터링과 개인정보 관리 등에 대한 감사가 병행된다. 이 단계를 도식화하면 다음 <그림 1>과 같다.



※ 출처: 금융보안원(2017)

〈그림 1〉 머신러닝을 활용한 이상거래탐지시스템(FDS) 구성 예시

Ⅳ. 보이스피싱 데이터와 FDS 융합 방안

1. 보이스피싱 연관 데이터

보이스피싱 단계별[3]로 필요한 데이터를 파악해 보면 다음과 같다.

1) 통신사(메신저 업체) 통화내역

보이스피싱은 범행 대상을 선정하든지 아니면 불특정 다수에게 시도하든지 반드

3) 보이스피싱을 단계별로 구분해 보면, 1단계 신용불량자나 노숙자 등을 이용해서 통장(대포통장)을 개설 · 매입하거나 대출 혹은 취업을 미끼로 예금통장을 편취해서 사기이용계좌를 확보하고, 2단계 해외(중국 등)에 본부를 둔 사기단이 금융기관 및 검찰, 경찰, 금융감독원 등 공공기관의 대표전화로 발신자번호를 조작해서 무작위로 국내에 전화나 문자메시지 전송, 3단계 개인정보 유출이나 범죄가 연루되었다는 등의 명목으로 기망해서 피해자의 개인정보나 금융거래정보 탈취 · 기망 · 공갈, 4단계 계좌보호 조치나 범죄혐의 탈피 등 명분으로 사기계좌로 이체를 유도하거나 피해자로부터 편취한 정보로 공인인증서를 재발급 받아 사기범이 직접 이체, 5단계 점조직으로 이루어진 현금인출책이 송금책의 계좌로 입금하면 송금책이 환치기 등의 방법으로 범죄집단 본부로 송금하는 단계로 구성할 수 있다(금융감독원 보이스피싱 지킴이 홈페이지, http://phishing-keeper.fss.or.kr/fss/vstop/main.jsp, 2019. 9. 16.검색)

시 전화나 메신저를 통한 연락을 한다. 대부분 해외에서 연락을 하므로 국제전화를 사용하고, 전화번호를 국내번호와 같이 변조하기도 해서 피해자는 쉽게 식별하기 어렵다.

2) 금융거래 정보(대포통장 등)

대부분 피해자가 범인의 통장으로 계좌이체를 하거나, 현금을 인출해서 직접 전해준다. 일반적으로 거액의 현금을 갖고 직접 거래하는 경우는 거의 없다. 따라서 금융기관에서 거액을 현금으로 인출하는 경우는 정상적이지 않을 수 있다.

피해자가 거래하는 계좌는 평소 거래가 없었던 계좌이고, 소액이 아닌 다액을 이체하거나, 100만 원 이상 이체할 경우 30분 지연 인출되기 때문에 99만 원씩 여러 차례 이체하는 경우가 많다. 특히 이체 받는 계좌는 평소 일상적인 거래가 없고, 범행에 사용되기 직전 1만 원을 이체시키고 인출하는 등 정상적으로 거래가 가능한 계좌인지 확인한다.

3) 보이스피싱 관련 데이터

보이스피싱은 <표 2>의 유형과 같이 자녀납치 및 사고를 빙자해서 편취하거나 금융기관 사칭 등 다양한 방식으로 진화하고 있다. 실시간 범죄 데이터는 자동으로 범죄 패턴을 학습하고 대응할 수 있도록 머신러닝 알고리즘을 고도화시킬 수 있다.

4) 보이스피싱 경찰 112·금융감독원 신고 데이터

보이스피싱 피해를 볼 경우에는 사건 데이터로 남게 된다. 실제 피해까지 진행되지 않았어도 보이스피싱 전화나 메신저를 받은 경우에 경찰 112나 금융감독원에 신고하는 경우가 있다. 경기남부경찰청의 경우만 하더라도 하루 신고가 150여 건이고 이 중에서 10건 정도만 실제 피해를 본다.[4] 범행에 실패한 이러한 데이터는 보이스피싱 패턴 분석에 도움이 될 수 있다.

2. 이상거래탐지시스템(FDS)과 보이스피싱 빅데이터 융합

보이스피싱은 현재 경찰에서 활용하고 있는 지도에 범죄다발지역을 표시하고 경

4) 경기남부경찰청 내부자료

찰력을 집중적으로 배치하는 방식의 범죄예측 빅데이터 기법을 활용하기는 어렵다. 오히려 금융사기 범죄에 대응하기 위해 금융기관에서 활용하고 있는 FDS가 피해자를 예측하는데 더 적합하다.

이 연구에서는 보이스피싱과 관련한 데이터와 머신러닝 기법을 활용한 기존의 FDS를 융합한 모델을 제시한다.[5] FDS에서 활용되는 머신러닝의 구체적인 알고리즘은 보안을 이유로 공개되지 않기 때문에 실증적으로 제시하지는 못했다. 하지만 이러한 '보이스피싱 피해 예측 시스템'을 구성하기 위한 머신러닝을 위해서 필요한 단계 중 1) 데이터 모으기와 준비 과정, 2) 피처 선택(Feature Selection)과 관련한 연구를 진행했다.

보이스피싱 데이터 중에서 피처(Feature) 데이터는 1) 피해자(금융계좌 개설자)의 실시간 통화내역, 2) 피해자의 실시간 해외메신저 내역, 3) 피해자의 실시간 거래내역, 4) 대포통장의 실시간 거래내역이다. 이러한 데이터를 활용해서 예측 알고리즘을 개발하기 위해서는 4) 기존에 알려진 보이스피싱 패턴과 5) 보이스피싱 피해가 발생하지는 않았지만, 전화나 메신저를 받은 범죄시도 신고 데이터가 필요하다. 이상의 데이터와 보관하는 기관을 정리해 보면 아래 <표 6>과 같다.

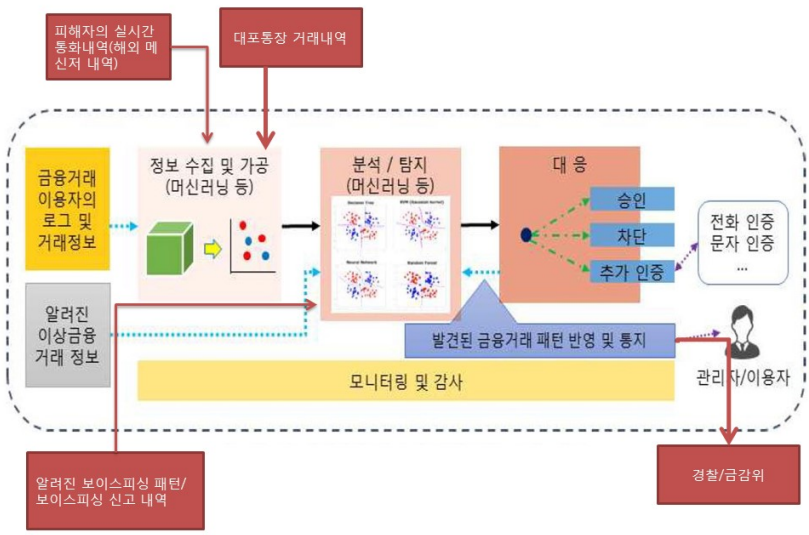
〈표 6〉 '보이스피싱 피해 예측 시스템' 필요 데이터

연번	유형	보유기관
1	통화내역	각 통신사
2	해외메신저 내역	카카오 등
3	금융거래 내역(계좌이체, 인출)	금융기관
4	대포통장 거래내역	금융기관
5	보이스피싱 유형(시나리오)	경찰청, 금감위
6	보이스피싱 신고 내역	경찰청, 금감위

이 데이터를 기존의 FDS에 융합시키면, 정보수집 및 가공 단계에서 기존의 금융거래 이용자의 로그 및 거래정보와 함께 1) 피해자의 실시간 통화내역(해외메신저 내역)과 2) 대포통장 계좌 거래내역 데이터를 같이 가공하고, 분석/탐지

5) 최근 부산은행에서는 빅데이터를 활용한 인공지능기반의 보이스피싱 이상거래 탐지시스템을 운영 1개월간 50여 건, 40억 원 이상의 금융사기를 예방했다고 밝혔다(경남일보, 2019. 7. 3. http://www.gnnews.co.kr).

단계에서 알려진 이상금융 거래정보에 알려진 보이스피싱 패턴과 보이스피싱 신고 내역 데이터를 추가한다. 이상 설명한 모델을 도식화하면 <그림 2>와 같다.



※ 출처: 금융보안원(2017) - 연구자 재구성

〈그림 2〉 보이스피싱 피해 예측 시스템

V. 결 론

보이스피싱은 급격하게 증가하고 있다. 정부와 금융기관은 다양한 대책을 제시하고 있지만 다양한 수법으로 진화하는 보이스피싱은 이제 대상을 가리지 않고 전 국민을 상대로 범행을 계속하고 있다. 게다가 보이스피싱은 대부분 외국에 콜센터가 있고 점조직 형태로 조직화하여 있어 검거로 근절하기는 어렵다. 이렇게 범인을 직접 만나지 않고 속아서 피해를 보는 범죄는 예방이 최선의 대응책이지만, 최근 보이스피싱 피해 추세를 보면 지금의 대응방안으로는 더는 증가하는 보이스피싱을 막을 수는 없는 것으로 보인다. 기존의 대응방안과는 다른 예방을 중심으로 새로운 대책이 필요하다.

최근 범죄예방을 위해 빅데이터 분석기법이 활용되고 있다. 2006년 보이스피싱이 처음 확인된 이후로 10년이 지났고, 다양한 데이터가 축적되어 있으며 이를 분석할 수 있는 기술도 발전했다. 그러나 보이스피싱 대응을 위해 빅데이터를 활용하고자 시도한 연구는 없었다.

이 연구에서는 보이스피싱 대응을 위해 금융사기 적발에 효과가 검증된 머신러닝을 활용한 FDS 시스템을 이용해서 금융기관, 보이스피싱과 관련한 통신사, 경찰의 범죄정보를 접목한 '보이스피싱 피해 예측 시스템'을 개념적으로 제안하였다.

이 모델의 실현을 위해서는 민감한 개인정보가 포함된 여러 기관의 방대한 데이터를 모아서 관리해야 한다는 어려움이 있다. 그러나 보이스피싱 콜센터가 중국이나 필리핀 등에 있어 범인 검거가 어렵고, 범죄예방 홍보나 지연인출제도와 같은 다양한 정책도 그다지 효과를 보지 못하고 있는 지금의 상황을 보면, 다소 시간과 비용이 필요하더라도 관련된 영역에서 효과가 입증되고 있는 피해 탐지시스템을 구축하는 것이 더 현실적인 대응방안이 될 수 있을 것이다. 또한, 한 번 구축된 머신러닝 기반의 시스템은 실시간으로 데이터 처리가 가능하고 스스로 학습하는 특징이 있으므로 새로운 유형의 보이스피싱에 신속하게 대응할 수 있을 것이다. 향후 이 연구를 바탕으로 '보이스피싱 피해 예측 시스템'이 개발되어 보이스피싱이 근절될 수 있기를 기대한다.

참고문헌

1. 국내외문헌

금융보안원 (2017). **머신러닝 기반의 이상거래 탐지시스템 동향**.

송주영, 송태민 (2018). **(빅데이터를 활용한) 범죄 예측=Crime prediction using big data: 머신러닝을 중심으로**. 서울: 황소걸음아카데미.

오요한, 홍성욱 (2018). 인공지능 알고리즘은 사람을 차별하는가? **과학기술학연구, 18**(3), 153-215.

윤해성, 곽대경 (2009). **보이스피싱의 예방과 대책마련을 위한 연구**. 한국형사사정책연구원.

윤해성, 전현욱, 양천수, 김봉수, 김기범 (2014). **범죄 빅데이터를 활용한 범죄예방시스템 구축을 위한 예비 연구(I)**. 한국형사사정책연구원.

이기수 (2018). 최근 보이스피싱의 범죄수법 동향과 법적 대응방안. **범죄수사학연구, 4**(2), 3-19.

이범주, 조동욱, 정연만, 이상호 (2016). 보이스 피싱 피해 방지를 위한 시스템 구축 방안 제안 및 사례 연구. **한국통신학회 학술대회논문집**, 202-203.

이승아 (2018). 보이스피싱에 대한 텍스트언어학적 연구. **텍스트언어학, 45**, 179-197.

치안정책연구소 (2019). **치안전망2019**.

탁희성, 박준희, 정진성, 윤지원 (2015). **범죄 빅데이터를 활용한 범죄예방시스템 구축을 위한 예비 연구(Ⅱ)**. 한국형사사정책연구원.

홍성삼 (2019). 피싱 사기범죄에 대한 인터폴 및 국가별 대응정책 비교연구. **경찰학논총, 14**(1), 99-130.

Brantingham, P. J., & Faust, F. L. (1976). A Conceptual Model of Crime Prevention. *Crime and Delinquency, 22*(3), 284-295.

Marsland, S. (2016). **알고리즘 중심의 머신 러닝가이드 제2판** (강전형 역). 파주: 제이펍.

2. 기타자료

경남일보 (2019, 7, 2). **부산銀, 보이스피싱 이상거래 탐지시스템 구축**, http://www.gnnews.co.kr/news/articleView.html?idxno=415565, 검색일 2019. 9. 15.

금융감독원 (2018). **2017년 은행 및 증권회사의 이상금융거래탐지시스템 운영 현황 및 감독방향**. [On-line] http://www.fss.or.kr/fss/kr/main.html

금융감독원 (2019). **2018년 보이스피싱 피해액, 역대 최고수준!** [On-line] http://phishing-keep

er.fss.or.kr/
스마트서울경찰 블로그 [On-line] https://smartsmpa.tistory.com/4586, 검색일 2019. 8. 4.
중앙일보 (2017, 12, 9). 미국 프레드폴, 예비 범죄자 잡아내 … 1년 새 강도 27% 줄어. https://news.joins.com/article/22189106#none, 검색일 2019. 8. 4.

【Abstract】

A Study on the Prediction Method of Voice Phishing Damage Using Big Data and FDS

Lee, Seoungyong · Lee, Julak

While overall crime has been on the decline since 2009, voice phishing has rather been on the rise. The government and academia have presented various measures and conducted research to eradicate it, but it is not enough to catch up with evolving voice phishing.

In the study, researchers focused on catching criminals and preventing damage from voice phishing, which is difficult to recover from. In particular, a voice phishing prediction method using the Fraud Detection System (FDS), which is being used to detect financial fraud, was studied based on the fact that the victim engaged in financial transaction activities (such as account transfers). As a result, it was conceptually derived to combine big data such as call details, messenger details, abnormal accounts, voice phishing type and 112 report related to voice phishing in machine learning-based Fraud Detection System(FDS).

In this study, the research focused mainly on government measures and literature research on the use of big data. However, limitations in data collection and security concerns in FDS have not provided a specific model. However, it is meaningful that the concept of voice phishing responses that converge FDS with the types of data needed for machine learning was presented for the first time in the absence of prior research. Based on this research, it is hoped that 'Voice Phishing Damage Prediction System' will be developed to prevent damage from voice phishing.

Keywords: Voice Phishing, Big Data, Machine Learning, Fraud Detection System, Fds