Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.5, Oct. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.5.1089

보이스피싱 심리조작 수법과 소비자 보호 방안: 텍스트 마이닝 기법을 중심으로

한 치 훈,[1†] 김 범 수,[2] 박 재 영[3‡]
[1]한국인터넷기업협회 (주임연구원), [2]연세대학교 정보대학원 (교수),
[3]NH농협금융지주 금융연구소 (책임연구원)

Voice Phishing Scammers' Psychological Manipulation and Consumer Protection Measures

Chihun Han,[1†] Beomsoo Kim,[2] Jaeyoung Park[3‡]
[1]Korea Internet Corporations Association (Assistant Researcher),
[2]Graduate School of Information, Yonsei University (Professor),
[3]Finance Research Institute, Nonghyup(NH) Financial Group (Senior Researcher)

요 약

정부 및 관련 기관에서 보이스피싱을 예방하기 위한 다양한 대책을 마련하고 있음에도 불구하고, 보이스피싱 피해가 계속해서 발생하고 있다. 본 연구는 텍스트 마이닝 기법을 활용하여 보이스피싱 사기범과 잠재 피해자의 실제 대화 448건을 분석하였다. 분석 결과, 보이스피싱 사기범은 지금, 이제, 진행, 오늘, 먼저 등의 한정된 기간을 강조하는 단어를 자주 사용하는 것으로 나타났다. 이것은 사기범들이 특정 단어를 통해 상대방이 합리적인 판단을 하지 못하도록 피해자의 심리를 조작한다는 것을 말해준다. 본 연구의 결과는 정부 및 유관 기관이 효과적인 보이스피싱 예방 및 소비자 보호 정책을 수립하는 데 도움이 된다.

ABSTRACT

Despite various measures being implemented by the government and related institutions to prevent voice phishing, incidents of such fraud continue to occur. This study analyzed 448 actual conversations between voice phishing scammers and potential victims using text mining techniques. The text analysis reveals that voice phishing scammers frequently use words emphasizing limited time frames such as now, soon, in progress, today, first. This indicates that scammers manipulate the victim's psychology through specific words, preventing them from making rational decisions. The results of this study can aid government and related institutions in formulating effective policies for preventing voice phishing and protecting consumers.

Keywords: Text mining, Topic modeling, Voice phishing

I. 서 론

통신 기술의 발전과 인터넷의 보급은 사람들이 언제 어디서나 제약 없이 계좌이체, 증권 등 금융 업무가 가능한 환경을 조성해 주었다. 하지만, 이러한 삶의 변화에 따라서 새로운 금융 범죄들이 발생하였

Received(05. 10. 2024), Modified(1st: 07. 16. 2024, 2nd: 08. 28. 2024), Accepted(08. 28. 2024)
* 본 연구는 한치훈의 석사학위논문을 수정 및 보완하였음

† 주저자, sue_z@naver.com
‡ 교신저자, inyourface33@gmail.com(Corresponding author)

는데 그중 가장 대표적인 예가 보이스피싱이다. 보이스피싱(voice phishing)은 전화를 통하여 신용카드, 계좌번호 등의 개인정보를 불법적으로 알아내어 이를 범죄에 사용하는 전자금융사기를 말한다. 경찰청에 따르면, 국내에서 보이스피싱이 처음 등장한 2006년부터 2021년까지 보이스피싱 누적 발생건수는 약 27만 건이며 누적 피해액은 3조 8681억 원이다[1].

경찰은 보이스피싱을 '서민 경제 침해범죄'로 정의하고 서민 경제의 근간을 위협하고 있다며 해당 범죄에 대한 특별단속을 시행하고 있다. 금융감독원은 '보이스피싱 지킴이' 사이트를 운영하여 보이스피싱 예방법을 제공하고, 〈보이스피싱 체험관〉을 제공하여 사람들이 보이스피싱 음성을 직접 체험하여 예방할 수 있도록 지원하고 있다. 한국인터넷진흥원(KISA)은 '보이스피싱 예방 10계명'을 발표하여 대중들이 보이스피싱에 적절하게 대처할 수 있는 가이드라인을 제시하였다. 하지만 이런 노력에도 불구하고, 보이스피싱 피해는 지속적으로 발생하고 있으며, 점점 진화하는 보이스피싱 수법이 여전히 금융 소비자를 위협하고 있다.

기존 연구는 주로 보이스피싱 사례를 분석하고 그에 대한 법제도적 측면과 대응방안을 검토하는 것에 중점을 두었다. 본 연구는 보이스 피싱 사기범과 피해자의 실제 대화 데이터를 분석하여, 사기범의 심리조작 수법과 이에 따른 피해자의 심리변화를 파악한다. 구체적으로, 보이스피싱 사기범과 피해자가 어떠한 단어를 자주 사용하는지를 분석하여 단어의 어떠한 특성 때문에 피해자가 사기를 당하는지를 설명하고자 한다. 또한, 토픽모델링을 활용하여 보이스 피싱에 대한 주요 토픽을 파악한다. 마지막으로, 감성분석을 통해 보이스피싱 피해자의 감정적 변화를 확인한다. 본 연구는 텍스트마이닝 기법을 활용하여 보이스 피싱 실제 대화를 분석함으로써, 보이스피싱을 예방할 수 있는 방안을 제시한다.

II. 개념적 배경 및 관련 연구

2.1 보이스피싱

보이스피싱(voice phishing)이란 전화를 통하여 신용카드, 계좌번호 등의 개인정보를 불법적으로 알아내어 이를 범죄에 사용하는 신종 사기 수법을 말하며, 전화금융사기로도 불리고 있다. 보이스피싱의 유형을 크게 기관사칭형, 통장매매, 대출사기형, 구직사이트 사칭(취업알선형), 납치 빙자형 등으로 분류할 수 있다. 대출사기형과 기관사칭형에서 보이스피싱 피해가 가장 많이 발생한다는 조사 결과에 따라서 금융감독원은 이러한 유형을 중점적으로 관리하고 있다.

기관사칭형은 크게 금융기관 사칭과 경찰, 검찰 및 금융감독원 등 수사기관 사칭으로 구분할 수 있다. 금융기관 사칭은 주로 은행직원, 제2금융권 직원 등을 사칭하여 저금리 대출 및 대환대출 등을 유도하거나, 개인정보를 편취하기 위하여 사용된다. 수시기관 사칭은 주로 경찰, 검찰 수사관, 검사, 금융감독원 직원 등을 사칭하여, "대포통장이 발견되었다", "범죄에 연루되었다"는 내용의 전화로 피해자를 겁에 질리게 만들어, 대출을 받아 ATM으로 무통장입금을 유도하거나, 피해자의 통장 잔고 및 개인정보 등의 정보를 유출하게 만드는 방법이다.

통장매매는 피해자에게 매력적인 높은 임대료를 제시하여 피해자의 통장을 넘겨받아 범죄의 대포통장으로 활용하는 데에 주로 사용되는 방법이다. 주로 피해자에게 사설도박 사이트나, 용돈벌이식 부업 등의 업체를 사칭하여 높은 통장 임대료를 제시하고, 통장과 현금카드, 체크카드를 택배 등으로 양도받아 보이스피싱의 범죄자금 세탁용 대포통장으로 사용한다.

대출사기형은 주로 금융기관 사칭과 함께 사용되는데, 대출이 필요한 피해자에게 접근하여 선입금 및 수수료 등을 요구하는 방식이다. 주로 낮은 금리를 제시하여 대환대출을 유도하여, "우리 기관의 낮은 금리의 대출 상품을 이용하려면 기존 대출금의 일부를 갚아야 한다"는 명목으로 피해자들에게 돈을 편취한다.

취업알선 및 빙자는 높은 시급으로 일을 할 수 있다며 피해자를 유인하여 계좌번호 등의 개인정보를 편취하는 수법이다. 또한, 대출기관을 사칭하여 보이스피싱 범죄자금의 인출 및 송금책으로 피해자를 활용하여 공범으로 만드는 등의 수법도 존재한다.

납치 빙자형은 자녀나 부모 등 가족을 납치한 것으로 속여 돈을 요구하는 방식이다. 주로 노인들에게 자녀를 납치하였다며 고액의 돈을 입금하라고 협박을 하거나, 아이들이 학원수업 등 전화를 받지 못하는 상황에 부모에게 전화를 하여 "아이를 유괴하였으니 돈을 입금하라, 입금하지 않으면 해를 가하겠다"는 내용으로 협박을 하여 돈을 요구한다. 마지막으로,

노년의 부모를 납치하였다며, 돈을 입금하지 않으면 신체에 해를 가하겠다는 협박을 하는 경우도 존재한다.

금융감독원은 2017년부터 2020년까지 3년간의 보이스피싱 피해자 데이터(135,000명)를 활용하여 사기피해 취약 유형을 살펴보았다[2]. 보이스피싱 피해자 135,000명 중에 76.7%인 104,000명이 '대출빙자형' 보이스피싱에 피해를 입은 것으로 나타났다. 다음으로 '기관사칭형' 보이스피싱 피해자가 31,000명으로 23%를 차지하였다.

또한, 금융감독원은 연령 별 피해 유형을 분석하였는데, 50대가 피해자의 32.9%를 차지하여 보이스피싱에 가장 취약한 것으로 나타났다. 40대가 27.3%, 60대가 15.6% 등으로 뒤를 이었다. 대출빙자형은 50대, 40대, 30대 등의 순으로 취약한 것으로 나타났는데, 이는 40대 및 50대의 자금수요가 많기 때문인 것으로 보인다. 사칭형의 경우에는 50대, 60대, 40대, 20대 순으로 취약한 것으로 확인되었다.

2.2 보이스피싱에 관한 연구

보이스피싱 관련 연구는 크게 세 가지 유형으로 분류할 수 있다. 첫째, 한 시점의 보이스피싱 사례를 분석하고 그에 대한 법제도적 측면과 대응방안을 검토하는 것에 중점을 둔 연구가 존재한다. 예를 들어, 김성언 등[3]은 보이스피싱 피해 사례와 검거된 보이스피싱 조직의 사례에 집중하여 보이스피싱 범죄 집단의 현황을 파악하였으며, 그들이 피해자에게 가하는 심리적 압박감 등을 조사하였다. 이동임[4]과 조호대[5]는 보이스피싱 현황과 사례분석을 통하여 법 및 제도적인 장치를 마련하고 수사기관의 단속 강화 등 효과적인 대응방안을 모색하였다.

둘째, 보이스피싱의 음성에 집중하여 패턴을 파악하고자 하는 연구가 진행된 바 있다. 이범주 등[6]은 보이스피싱 사기범과 일반인들의 음성 패턴을 분석하여 그 차이점을 확인하였다. 분석 결과, 보이스피싱 사기범은 일반인과 비교하여 음성에 실리는 에너지가 낮고 발화속도가 빠른 것으로 나타났다. 도선희[7]는 보이스피싱 사기범의 음성적 특성을 분석하였다. 보이스피싱 사기범의 유형을 대출빙자형, 경찰사칭형, 검찰사칭형 등으로 분류하여 각각의 차이점을 확인하였다. 분석 결과, 대출빙자형은 감정발화와 관련된 피치 값이 대화 전체적으로 낮은 경향을 보이다가 대출 관련 특정 단어에서는 높은 피치 값이 나타난 반면, 경찰 및 검찰사칭형은 전체 발화에서 높은 평균 피치 값을 보였다.

마지막으로, 빅데이터 분석 방법론을 적용하여 보이스피싱 데이터를 분석한 연구가 진행되고 있다. Kim et al.[8]은 보이스피싱이 공격 대상의 개인정보를 수집하여 악용하는 형태로 변화하고 있으며, 이에 따른 공격 패턴을 분석하여 적절한 대응방안을 모색하는 것이 필요하다고 말하였다. 최근에는 스마트폰이 폭발적으로 보급됨에 따라서, 스마트폰을 이용한 보이스피싱을 예방할 방안이 필요하다. 이를 위하여 스마트폰 피싱 앱을 선별할 수 있는 방안을 제시하여 지능화된 보이스피싱에 효과적으로 대응할 수 있는 방안을 검토하였다. 장광호 등[9]은 데이터 기반 수사 기법의 중요성을 강조하면서, 비정형 데이터를 수사에 활용할 수 있는 방안을 검토하였다. 보이스피싱의 실제 비정형 데이터를 수집하여 전화번호, 계좌번호, 범죄 수법 등의 핵심 용어를 추출하여 이를 수사에 활용할 수 있는 방안을 제안하였다.

III. 연구방법

3.1 연구절차

본 연구는 금융감독원에서 제공하는 〈보이스피싱 체험관〉 텍스트 및 음성 데이터를 활용한다. 분석에 사용된 데이터는 2015년부터 2020년까지 업로드된 총 448건의 보이스피싱 음성 및 텍스트 데이터이며, 이 중에서 '대출빙자 및 통장매매'는 174건, '검찰수사관 및 검사 사칭'은 185건, '경찰 및 금감원, 금융회사 사칭'은 47건, '우수 대처'는 42건이다. 448건의 사례 중 남자 사기범은 372건으로 약 83%의 비율을 보이고 있으며, 여성 사기범은 73건으로 약 16%의 비율을 보이고 있다.

본 연구의 분석절차는 Fig. 1.과 같다. 우선 수집된 데이터를 전처리한다. 구체적으로, 음성데이터를 텍스트 데이터로 변환하는 작업을 거친 뒤, 텍스트 토큰화 및 불용어 처리를 진행하며, 텍스트 대화 파일을 사기범의 발화 부분과 잠재 피해자의 발화 부분으로 분류하고, 등록일 기준 연도별로 분류하는 작업을 진행한다. 데이터 전처리 후에 텍스트마이닝 기법을 활용하여 다양한 텍스트 분석을 실시하고, 시사점을 도출한다.

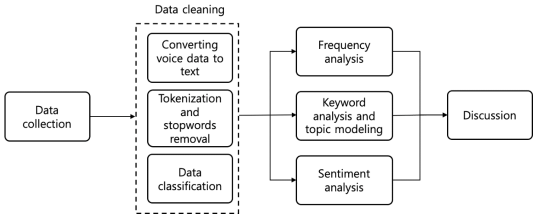

Fig. 1. Research procedure

3.1.1 데이터 변환

텍스트 분석에 앞서, 448건의 보이스피싱 사례 중에서 텍스트 데이터가 없는 경우(300건)에는 음성데이터를 텍스트 데이터로 변환하는 작업을 진행한다. 구글 독스를 활용하여 음성대화를 인식시킨 후, 변환된 텍스트 데이터를 분석에 활용할 수 있는 형태로 변환하는 작업을 진행한다.

3.1.2 토큰화 및 불용어 처리

다음 단계로 형태소 분석(토큰화)과 함께 불용어 처리를 진행한다. 형태소 분석이란, 문장을 문법적이거나 관계적으로 의미를 가지고 있는 각각의 단어로 분류하고, 이에 대한 형태소를 찾아내어 단어의 원형을 복원하는 과정을 말한다. 본 연구에서는 gensim 라이브러리를 사용하여 토큰화 및 형태소 분석을 진행한다. 본 연구에서는 명사와 형용사 형태소가 대화 내에서 가장 중요한 의미를 가지고 있을 것으로 판단하여 해당 형태소들을 추출한다. 명사와 형용사 외의 형태소는 제거를 한 후에, 토픽 모델링에 필요하지 않은 단어들(넌, 월, 일, 안녕하세요 등)에 대한 불용어 처리를 진행하여, 원활한 분석이 가능하도록 한다[10].

3.1.3 데이터 분류

토큰화 및 불용어 처리 과정을 진행하고 난 뒤에는 사기범과 잠재 피해자의 발화를 분류하는 작업을 진행한다. 사기범이 사용하는 단어들의 키워드와 그 빈도를 파악하고, 동시에 잠재 피해자가 사용하는 단어들의 키워드와 그 빈도를 분석하기 위한 절차이다. 사기범과 잠재 피해자의 발화를 분류하는 절차 이외에도, 보이스피싱으로 피해를 입은 것으로 보이는 사례와 보이스피싱 피해를 회피한 사례를 분류하는 작업을 진행한다. 이는 보이스피싱 피해를 입지 않은 피해자가 사용하는 단어의 키워드나 빈도를 확인하고, 그 특성을 분석하기 위함이다.

보이스피싱 피해 회피는 대화 말미에 사기범이 그냥 전화를 끝내거나, 피해자가 관심없다는 의사를 밝히고 통화를 종료하거나, 사기범과 잠재 피해자가 서로 욕설을 하는 등의 특징을 보인다. 즉, 보이스피싱으로 피해를 입은 것으로 보이는 사례와 명확히 구분된다. 본 연구는 전체 데이터를 보이스피싱 피해를 회피한 것으로 보이는 '보이스피싱 회피'와 보이스피싱 피해를 입은 것으로 보이는 '보이스피싱 피해 예상'으로 나눈다.

3.2 분석 기법

3.2.1 빈도분석

본 연구는 토픽 모델링을 빈도분석, 키워드 분석, 토픽 모델링의 순서로 진행한다. 먼저 빈도분석이란, 문서 내의 단어들이 얼마나 나타났는지의 횟수를 파악하여 많은 양의 전체 문서의 내용을 대략적으로 파악할 수 있는 기법이다. 정확한 단어의 출현 횟수를 파악하기 위하여 형태소 분석을 통해 특정한 의미를 지닌 명사나 형용사를 추출하여 분석을 진행하면 더욱 신뢰도 높은 결과물을 얻을 수 있다. 본 연구는 각 문서의 명사 및 형용사를 추출하여 단어의 등장 횟수를 파악한다.

3.2.2 TF-IDF 분석

TF-IDF 키워드 추출 기법은 정보 검색과 텍스트 마이닝에서 이용하는 가중치라고 할 수 있다. 방대한 수량의 문서가 존재할 때, 특정 단어가 문서 내에서 얼마나 중요한 단어인지를 나타내는 수치이다. 즉, 문서 내의 핵심어를 추출할 때 주로 사용하는 방법이다. TF(term frequency)는 단어 빈도로, 특정 단어가 문서 내에 얼마나 자주 등장하는지를 나타낸다. IDF(inverse document frequency)는 역문서 빈도로, 특정 단어가 문서 전체에 많이 나타날수록 값이 작아지고, 특정 문서에 특정 단어가 많이 나타날수록 값이 커진다. TF-IDF는 TF값과 IDF값을 곱한 것으로, 각 단어 별로 가중치를 계산하여 높은 순서대로 키워드를 선정하는 것이다. 즉, 값이 크면 클수록 특정 문서 내에서 중요한 의미를 가지는 단어라고 볼 수 있는 것이다[11].

3.2.3 LDA 토픽모델링

토픽모델링 기법은 문서의 주제를 도출하기 위한 단어 분석 방법론이라고 할 수 있다[12]. 본 연구는 잠재디리클레할당(Latent Dirichlet Allocation; LDA)를 사용한다. LDA는 문서 내 유사한 의미의 단어들을 클러스터링 하여 주제를 추론한다[13]. 즉, 문서가 가지고 있는 잠재 주제에 따라서 특정한 단어가 특정한 주제에 포함될 가능성을 계산하고, 단어 뭉치와 가장 유사한 특정 주제를 찾는다[14].

3.2.4 감성분석

본 연구는 보이스피싱 사기범과 피해자의 감정적인 변화를 파악하기 위하여 감성분석을 진행한다. 초창기 감성분석은 컴퓨터 과학 분야에서 자연어처리 기법의 하나로 연구가 시작되었는데, 현재는 경영학을 포함한 다양한 분야에서 연구가 진행되고 있다[15]. 감성분석은 크게 머신러닝 기반과 규칙 및 어휘(Lexicon)기반의 감성분석으로 분류할 수 있다. 본 연구에서는 규칙 및 어휘(Lexicon)기반의 감성분석을 활용하여 연구를 진행한다. 감성분석에서는 감정을 크게 긍정적 감정과 부정적 감정의 두 가지 감정으로 분류한다. 긍정적 감정에는 흥미, 호감, 기쁨 등의 감정이 포함되며, 부정적 감정에는 통증, 두려움, 분노, 거부감 등이 포함된다.

IV. 연구결과

4.1 빈도분석 결과

보이스피싱 사기범과 보이스피싱 잠재 피해자가 자주 사용한 단어를 빈도분석을 통하여 확인하였다. 먼저, Table 1.을 보면, 보이스피싱 사기범이 가장 많이 사용한 단어는 “고객님, 저희, 지금” 등으로 나타났다. 또한 사기범들은 “지금, 이제, 진행, 일단, 오늘” 등의 한정된 기간을 강조하는 단어를 주로 사용하는 것을 확인할 수 있다. 이와 같은 보이스피싱 사기범의 사기 기법은 제품 판매 및 서비스 경험의 기간을 한정하는 마케팅 기법과 비슷하다. 기업은 종종 ‘지금이 아니면 다시는 살 수 없다’는 심리를 자극하여 소비자의 충동구매를 유도한다[16]. 마찬가지로, 보이스피싱 사기범도 시급함을 유발하는 단어를 사용함으로써, 상대방의 심리를 자극하여 상대방이 합리적인 판단을 하지 못하도록 유도하는 것이라고 볼 수 있다.

Table 1. Frequency analysis (scammer)

rank	word	frequency
1	customer(고객님)	1,995
2	we(저희)	1,043
3	**now(지금)**	994
4	**soon(이제)**	694
5	loan(대출)	544
6	handling(처리)	426
7	**action(진행)**	418
8	words(말씀)	400
9	**once(일단)**	379
10	**today(오늘)**	368

다음으로, Table 2.는 보이스피싱 잠재 피해자 데이터의 빈도분석 결과이다. 본 연구에서는 보이스피싱 피해가 예상되는 사례와 보이스피싱 피해를 회피한 사례로 분류하여 언어 패턴를 비교하였다. 분석 결과, 보이스피싱 피해가 예상되는 사례는 피해자들이 “그럼, 네네, 진행, 그래요” 등과 같은 수동적이고

Table 2. Frequency analysis (victim)

type	rank	word	frequency
success (피해 예상)	1	now(지금)	120
	2	call(전화)	106
	3	**then(그럼)**	86
	4	**yes(네네)**	83
	5	loan(대출)	81
	6	words(말씀)	66
	7	bankbook(통장)	54
	8	account(계좌)	53
	9	**action(진행)**	49
	10	**okay(그래요)**	43
fail (회피)	1	call(전화)	74
	2	no(아니)	68
	3	bank(은행)	55
	4	there(거기)	41
	5	bankbook(통장)	40
	6	**none(없어요)**	36
	7	**report(신고)**	35
	8	**check(확인)**	33
	9	**police(경찰서)**	30
	10	**theft(도용)**	26

순응적인 단어들을 사용하는 것을 확인할 수 있다. 이러한 단어들은 피해자들이 사기범을 의심하지 않은 채로 사기범의 지시를 순순히 따르고, 사기범에 쉽게 설득될 수 있는 상태를 나타낸다.

반면에 보이스피싱 피해를 회피한 사례의 경우에는 "아니, 없어요, 신고, 확인, 경찰서, 도용" 등과 같은 부정적이고 방어적인 단어를 주로 사용한 것을 확인할 수 있다. 이것은 잠재 피해자가 사기범의 공포감 조성이나 호의 제공에 넘어가지 않고 적극적으로 대처하였음을 말해준다.

4.2 토픽모델링 결과

혼잡도(perplexity)를 기준으로 보이스피싱 사기범의 경우 토픽의 개수가 5개, 보이스피싱 잠재 피해자(피해 예상, 회피)의 경우 토픽의 개수가 3개가 적합하다고 판단하였다. 예를 들어, 보이스피싱 피해 예상의 경우, 토픽의 개수를 2개에서 10개까지 모형화한 결과 토픽의 개수가 2개에서 3개로 변할 때 혼잡도(-5.16)가 급격히 감소하였다.

Table 3.은 보이스피싱 사기범의 텍스트 데이터에 대한 토픽모델링을 진행한 결과이다. 금융 사기범이 보편적으로 사용하는 사기 전략으로, 희소가치를 강조하여 투자를 유도하는 것이 있으며, 또한, 사기범은 신뢰성 있는 회사명과 직함을 사칭하여 신뢰성을 강조하고, 공포감을 조성하여 상대방을 설득하고자 한다[17]. 즉, 상대방의 감정적 흥분상태를 유발함으로써, 피해자가 이성적인 판단을 하지 못하는 상태로 만들어서 불합리한 행동을 하도록 유도하는 것이다. 보이스피싱 사기범 역시 비슷한 사기 전략을 사용하는 것으로 나타났다. 사기범들이 주로 "이제, 일단, 그럼, 먼저, 지금, 오늘" 등 피해자를 조급하게 만드는 키워드들을 많이 사용하는 것을 확인할 수 있다. 부록 1에서 희소성을 강조하는 보이스피싱 실제 사례를 확인할 수 있다. 또한, "중고나라, 수사, 검거, 검찰청, 녹취" 등 금융범죄수사와 관련하여 수사기관을 사칭하는 키워드도 확인할 수 있다. 즉 사기범은 메시지 발신원의 신뢰도가 높게 보이도록 위장하고 공포감을 조성하는데, 부록 1에서 실제 사례를 확인할 수 있다.

다음으로는 보이스피싱 잠재 피해자에 대한 토픽모델링을 진행하였는데, 보이스피싱 피해가 예상되는 사례와 보이스피싱 피해를 회피한 사례로 분류하여 분석을 진행하였다. Table 4.를 살펴보면, 보이스피싱 피해 예상은 세 가지의 토픽으로 구분되는데, 먼저, 조급함이 유발된 피해이다. 주요 키워드로 "부족", "여기" 등이 있다. 다음으로, 공포감에 따른 피해이다. 주요 키워드로 "어떡해", "그래요", "똑같네" 등이 있다. 마지막으로, 호의에 의한 피해이다. 주요 키워드로 "그러면", "동의", "보증" 등이 있다.

피해 회피 역시 세 가지의 토픽으로 구분되는데, 첫째, 부정을 통한 회피이다. 주요 키워드로 "아니라", "아니에요" 등이 있다. 둘째, 의심을 통한 회피이다. 주요 키워드로 "진짜", "협박", "일반적" 등이 있다. 마지막으로, 지식에 의한 회피이다. 주요 키워드로 "안되요", "그래", "없어요" 등이 있다.

보이스피싱 수법이 시대적 상황에 따라 변할 수 있다는 점을 고려하여, 추가적으로 연도별 토픽모델링을 진행하였다. 2015년은 두 개의 토픽이 추출되었는데, 첫 번째 토픽은 신용카드, 도용, 대포통장, 신분증, 압수 등 금융범죄수사와 관련된 키워드를 포

Table 3. Results of topic modeling (scammer)

Topic	Keyword
Topic 1	.082*soon(이제), .057*have/has(있는), .055*check(확인), .050*like(같은), .047*possible(가능), .045*then(그러면), .039*overdue(연체), .038*notarization(공증), .035*later(이후), .028*talk(얘기)
Topic 2	.093*simple(간단), .067*at least(최소), .062*once(일단), .060*then(그럼), .059*real(실제), .049*interim(중도), .049*file(서류), .044*guarantee(담보), .042*kakao talk(카톡), .039*receipt(접수)
Topic 3	.139*income(소득), .097*fixed(고정), .063*customer(고객), .058*grant(부여), .049*interest rate(금리), .047*possible(가능), .046*collection(추심), .041*action(진행), .030*result(결과), .029*no(아니)
Topic 4	.119*Mirae asset(미래에셋), .106*Kakao(카카오), .071*method(방법), .065*number(번호), .064*office(사무실), .061*part(부분), .046*picture(사진), .041*none(없으세요), .022*one(하나), .021*yes(네네)
Topic 5	.092*call(전화), .089*Joonggonara(중고나라), .048*investigation(수사), .042*arrest(검거), .037*Shinhan bank(신한은행), .037*related(관련), .034*Prosecutor's office(검찰청), .033*application(신청), .031*explain(설명), .031*record(녹취)

Table 4. Results of topic modeling (victim)

Topic	Keyword
success(피해 예상)	
Topic 1	.094*credit(신용), .074*lack(부족), .041*Woori bank(우리은행), .039*bank(은행), .037*corporate(법인), .032*repayment(상환), .027*different(다른), .026*fund(자금), .025*application(신청), .024*here(여기)
Topic 2	.098*judicial affairs(법무), .076*what(어떡해), .071*yeah(그래요), .055*same(똑같네), .053*go(가면), .032*middle(중간), .024*fund(자금), .022*once(일단), .021*itself(자체), .019*need(필요)
Topic 3	.074*then(그러면), .070*related(관련), .046*part(일부), .046*card(카드), .037*office(사무실), .029*arrangement(배정), .028*parking lot(주차장), .027*situation(상황), .024*agreement(동의), .022*assurance(보증)
fail(회피)	
Topic 1	.096*bank(은행), .070*details(상세), .067*not(아니라), .065*a moment ago(아까), .058*Woori financial group(우리금융), .048*right(그렇죠), .033*Ulsan(울산), .024*capital(캐피탈), .024*open(개설), .022*no(아니에요)
Topic 2	.077*number(번호), .076*sick(아픈), .065*no(아뇨), .041*no(아니), .039*name(성함), .038*head(머리), .028*real(진짜), .024*Hana bank(하나은행), .024*threat(협박), .022*general(일반적)
Topic 3	.080*handling(처리), .060*identification(신분증), .047*transaction(거래), .036*there(거기), .035*confiscation(압수), .027*no way(안되요), .017*okay(그래), .016*perpetrator(가해자), .016*part(부분), .016*have no(없어요)

함한다. 두 번째 토픽은 명의, 본인, 롯데, 농협, 국민 등 명의도용과 관련된 키워드를 포함한다. 이것을 통해 2015년에는 2014년에 발생한 카드 3사 개인정보 유출 사건을 악용한 사례가 다수 발생하였음을 알 수 있다.

2016년은 취업 알선과 관련된 이력서, 알바, 회사, 업체 등의 키워드가 추출되었으며, 2017년과 2018년은 납치 빙자와 대출 빙자와 관련된 키워드가 각각 추출되었다. 납치 빙자는 지하, 짓거리, 데리고, 현찰, 출금, 학원 등의 키워드를 포함하고 대출 빙자는 수수료, 담보, 대출, 금리 등을 포함한다.

4.3 감성분석 결과

본 연구는 추가적으로 감성분석을 진행하여 보이스피싱 사기범과의 대화 내에서 보이스피싱 피해자의 감정적 변화를 확인하였다. 아래 Fig. 2.를 보면, 파란색 선은 사기범의 대화이고, 주황색 선은 피해자의 대화이다. 그래프의 X축은 대화의 흐름이며, 0은 대화의 시작 부분이다. Y축은 감정 점수로, 0은 중립 감정을 의미하고, 1과 가까울수록 긍정적인 감정을 의미하며, -1과 가까울수록 부정적인 감정을 의미한다.

보이스피싱 피해가 예상되는 사례의 경우, 피해자와 사기범 모두 대체로 긍정적인 감정을 공유하고 있는 것을 확인할 수 있다. 즉 피해자가 사기범에 긍정적으로 반응하는 것으로, 사기법의 심리조작에 휘둘

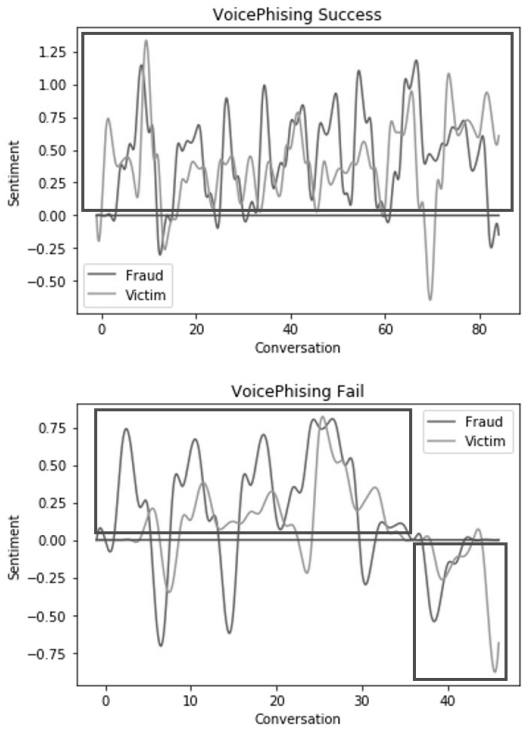

Fig. 2. Results of sentiment analysis

리는 것이다. 한편, 대화 후반에 피해자의 감정이 잠시 부정적으로 변한 것을 볼 수 있는데, 곧바로 긍정적인 감정을 표출한 것으로 보아, 이것은 피해자가 사기범의 심리조작 수법에 당했기 때문인 것으로 추측된다. 다시 말해, 사기범의 속임수에 공포감을 느꼈고, 사기범의 해결방안 제시에 안정감을 찾은 것이다.

반면에 보이스피싱 피해를 회피한 사례의 경우, 대화 초반에는 잠재 피해자가 긍정적인 감정을 느꼈지만, 대화 후반에 사기범을 의심하게 되면서 부정적인 감정을 표출한 것을 확인할 수 있다. 피해 예상 사례와 다른 점으로, 첫째, 사기범의 감정이 부정적으로 자주 변했다는 것이다. 상대방이 본인 뜻대로 반응하지 않자, 사기범이 부정적인 감정을 표출한 것으로 추측된다. 둘째, 대화 후반에 부정적인 감정을 표출한 이후로 통화가 종료될 때까지, 피해 예상과 다르게, 잠재 피해자의 감정이 계속해서 부정적이었다는 것이다. 즉 잠재 피해자가 사기범의 심리조작 수법에 당하지 않은 것이다.

V. 결 론

5.1 연구결과 토의 및 시사점

본 연구는 보이스피싱 실제 데이터를 활용하여 첫째, 보이스피싱 사기범과 보이스피싱 잠재 피해자가 주로 사용하는 단어를 확인하였다. 보이스피싱 사기범은 “지금”, “이제”, “진행”, “오늘”, “먼저” 등의 한정된 기간을 강조하는 단어를 자주 사용하는 것으로 나타났다. 이것은 사기범들이 조급함을 유발하는 특정 단어를 통해 피해자가 합리적인 판단을 하지 못하도록 심리 조작을 시도한다는 것이다. 하지만 모든 사람들이 사기범의 심리조작 수법에 당하는 것은 아니다. 빈도 분석과 토픽모델링 분석을 실시한 결과, 보이스피싱에 당하지 않는 사람들은 주로 방어적인 단어를 사용하는 것으로 드러났다. 즉 사기범의 사기 수법에 빠져들지 않고 저항한 것이다. 다만 본 연구의 결과는 보이스 피싱에 당하지 않는 사람이 특정 단어를 사용하였음을 보여줄 뿐이다. 즉 잠재 피해자의 특정 단어 사용이 보이스 피싱을 막았다고 보기는 어렵다. 향후 연구에서 어떤 특성을 가진 사람들이 사기범에 대항하는 단어를 사용하는지를 살펴볼 수 있다.

보이스피싱 수법은 또한 트렌드를 따라가는 것으로 확인되었다. 예를 들어, 2015년에는 카드 3사 유출 사건을 악용한 사례가 있으며, 2018년에는 비트코인을 악용한 사례가 있다. 또한, 2020년에는 COVID-19을 악용하여 정부지원 대출 상품 가입을 유도한 사례가 있다.

본 연구는 기존 연구의 한계점을 극복하고자, 보이스피싱 범죄 데이터에 대한 텍스트 분석을 진행하였다는 점에서 다음과 같은 학술적 의의를 가진다. 첫째, 기존의 보이스피싱 관련 연구는 각각의 사례를 분석하는 데에 그쳤지만, 본 연구는 보이스피싱의 실제 음성 및 텍스트 데이터를 활용하여 사기범과 피해자가 주로 사용하는 키워드 등을 분석하였다. 또한, 보이스피싱 피해를 회피한 피해자가 사용하는 단어 및 키워드 등을 확인하였다. 둘째, 본 연구는 텍스트 분석을 통해 사람들이 어떻게 보이스피싱에 당하는지 설명하였다. 즉 사기범이 수사관 사칭이나 지금, 이제, 일단은, 바로 등 심리적인 긴장감을 조성하고 조급함을 자극하는 단어를 사용하여, 상대방이 합리적인 판단을 하지 못하게 만든다고 보았다. 마지막으로, 김민정과 김은미[18]는 보이스피싱 피해를 당할 뻔했으나 피해를 모면한 집단에 대해서 지속적인 연구가 필요하다고 말하였다. 이에 본 연구는 주로 보이스피싱 피해자에 초점을 맞춘 기존 연구와 다르게, 보이스피싱에 당하지 않은 집단도 고려함으로써, 보이스피싱에 대한 이해를 확장하였다.

본 연구의 결과는 다음과 같은 시사점을 제시한다. 우선, 관련 기관은 보이스피싱 예방교육에 본 연구의 결과를 반영할 수 있다. 구체적으로, 사기범이 주로 사용하는 단어를 보이스피싱 교육자료에 포함하고 강조함으로써, 보이스피싱에 대한 경계심을 높일 수 있다. 또한, 잠재 피해자가 보이스피싱에 당하는 유형(조급함, 공포감, 호의)과 당하지 않는 유형(부정, 의심, 지식)을 교육자료에 포함함으로써, 보이스피싱을 간단한 방법으로 학습하게 만들 수 있다.

인공지능 기술의 활용범위가 점차 확대되면서, 보이스피싱에도 인공지능 기술이 적용될 수 있다. 최근 관계기관이 “AI · 빅데이터 기반 보이스피싱 예방을 위한 상호 업무협약”을 체결하였다. 이 협약의 주요 내용 중 하나는 보이스피싱 예방 AI를 개발하는 민간 기업에게 보이스피싱 통화 데이터를 제공하는 것이다. 보이스피싱 탐지 · 예방 AI 서비스는 주로 통화 내용의 주요 키워드나 패턴을 탐지하는 방식으로 작동한다. 따라서 본 연구의 결과는 보이스피싱 예방 AI를 개발하는 데 중요한 기초 자료를 제공한다.

보이스피싱 예방을 위한 연구 및 기술 개발에서 가장 중요한 요소는 음성데이터의 축적이다. 현재 관련 연구와 기술 개발에 사용되는 대부분의 데이터는 피해자가 제공한 것이다. 하지만 보이스피싱 발생 건수에 비해 축적된 음성데이터는 매우 부족한 상황이다. 이것은 보이스피싱 전화를 받더라도 녹음까지 고려하지 못하거나 녹음을 하더라도 관련 기관에 제공하지 않기 때문이다. 따라서 정부는 국민에게 보이스피싱 의심 전화를 녹음하도록 적극적으로 안내할 필요가 있으며, 필요시 음성데이터 제공에 대한 적절한 보상도 고려할 수 있다.

다음으로, 소비자의 경우에는 가급적 모르는 전화를 받지 않는 것이 최선의 방안이지만 이것은 현실적으로 불가능하다. 따라서 보이스피싱 사기범이 주로 사용하는 단어를 즉각 알아채서 통화를 중단할 필요가 있다. 예를 들어 “지금”, “이제”, “일단”과 같이 시급함을 강조하는 단어가 있다. 상대방의 심리를 조작하는 이런 단어들은 특히 저금리 대출상품이나 특가 및 할인정보 등을 소개하는 상황에서 자주 사용될 것으로 보인다.

5.2 연구의 한계점 및 향후 연구 방향

본 연구는 다음과 같은 한계점을 가진다. 첫째, 본 연구는 보이스피싱의 텍스트 데이터에 집중하였기 때문에 억양, 사투리 사용 여부, 감정 등 사기범의 음성적인 특성을 고려하지 못하였다. 이범주 등[6]은 보이스피싱 사기범의 음높이, 대역폭, 발화속도, 음색 등을 분석하였는데, 일반인에 비해서 보이스피싱 사기범들의 음성에 실리는 에너지와 발화속도 등에 상대적으로 유의미한 차이가 있음을 확인하였다. 이처럼 보이스피싱은 음성을 통하여 이루어지는 범죄이기 때문에 향후 텍스트 데이터 뿐만 아니라 보이스피싱 사기범의 음성적 특성을 고려한 연구를 진행한다면 의미있는 결과를 얻을 수 있을 것이다. 또한, 본 연구는 보이스피싱 사기범의 심리조작 수법과 잠재 피해자가 그것에 어떻게 반응하는지를 살펴보았는데, 향후 연구에서는 텍스트와 음성적 특성을 모두 고려한 보이스피싱 탐지 서비스를 개발할 수 있다[19].

둘째, 본 연구는 보이스피싱 사기범과 잠재 피해자의 대화 데이터만 사용했다. 즉 피해자의 특성을 고려하지 못하였다. 또한, 사건 피해 규모, 피해 금액, 범인 검거 여부 등 범죄와 관련된 구체적인 정보을 활용하지 못하였다. 위와 같은 데이터들을 추가적으로 고려하여 연구를 진행한다면 더욱 의미있는 결과를 도출할 수 있을 것이다.

마지막으로, 본 연구는 보이스피싱 데이터만을 사용하였기 때문에 스마트폰 앱, 몸캠 피싱, 메신저피싱 등 최근 새로운 형태로 발생하고 있는 피싱 범죄에 대한 분석을 진행하지 못하였다. 최근에는 스마트폰 보급이 활성화되면서, 스마트폰 앱을 활용한 피싱 피해 사례가 발생하고 있다. 저금리를 내세운 보이스피싱을 통하여 피해자의 스마트폰에 피싱 앱을 설치하게 부추겨 개인정보를 편취하는 새로운 형태의 금융사기가 발생하거나, 음성 및 화상 채팅을 하자고 피해자를 유혹하여 특정 앱을 설치하도록 부추겨, 피해자의 스마트폰을 해킹하여 협박을 하는 몸캠 피싱 등의 범죄가 새로이 등장하고 있다. 추후에 진행될 연구에서는 위와 같이 새로운 형태의 피싱 범죄와 관련된 데이터를 분석하여 이에 대한 예방 및 탐지에 기여할 수 있는 연구를 진행할 필요가 있다.

부록. 보이스피싱 실제 사례

표 1. 희소성 강조 사례

사기범 : 정상적으로 계약 만료가 되셔야지 신용평점이 올라가시거든요 피해자 : 네 사기범 : 예 근데 그거를 하루만에 보완을 하셔야 되서 저희가 우회적인 방법으로 그 평점 보완을 해드릴건데요 피해자 : 네 사기범 : 예 하루만에 하실수 있는, 여보세요? 피해자 : 네 사기범 : 네 하루만에 해드릴 수 있는 방법중에 가장 확실한 방법이 강제 상환 방식이라는게 있습니다. 피해자 : 네 사기범 : 이 부분은 저희 국민은행에서 뭐 임의로 처리를 할 수 있는 내용이 아니라 저희가 이제 정부지원 상품으로 나오신 부분이라서 그 은행연합회, 은행상위기관인 고객들 신용정보관리하는 은행연합회 쪽에다가 협조요청을 해드릴 수 있는 권한이 있습니다. 피해자 : 네 사기범 : 네 협조요청을 하게 되면은 강제상환이

라는 걸 이용하게끔 도와 드릴건데요. 피해자 : 네 사기범 : 강제상환을 한다고 바로 평점이 올라가시는 게 아니라 이제 그 실제로 고객님께서 대출받고 나면 자금 잘 못 받거나 또는 계약 내용상에 문제가 있으면 그 대출을 사용하면 안되지 않습니까? 피해자 : 네 사기범 : 예 그럴때에 은행연합회 쪽에 이제 클레임을 걸면은 그 고객님께서 시간이 좀 지났더라도 이자나 중도상환 수수료 없이 그 고객님 신용상의 불이익 없이 상환처리 시켜주는게 강제상환입니다

표 2. 기관 사칭 및 공포감 조성 사례

사기범 : 네 저는 서울중앙지검 첨단범죄수사 1팀 김진우 수사관입니다 피해자 : 네 사기범 : 네 그 다름이 아니고 oo씨가 그 연루되어있는 명의도용사건 때문 에 몇 가지 확인차 연락 드렸거든요 피해자 : 어 그게 무슨소리세요? 사기범 : 아 명의도용사건 때문에 본인이 연루된 것 때문에 몇가지 확인하려고 그 연락 드렸는데 혹시 김승우라고 알고 계십니까? 피해자 : 아니요. 그런 사람 모르는데 사기범 : 아 그러세요? 다름이 아니고 지금 뭐 개인정보유출 사건 때 그 유출 되면서 도용 당하신 피해자인지 그 몇가지 확인차 연락드린건데 피해자 : 어 저 잘못한거 없는데?

References

[1] Edaily, "Status of voice phishing", https://www.edaily.co.kr/News/Read?newsId=02132006632558192&mediaCodeNo=257, 2024.09.19.

[2] Seoul Finance, "Status of voice phishing victims by types", https://www.seoulfn.com/news/articleView.html?idxno=391552, 2024.09.19.

[3] Seong Eon Kim and Young Jin Yang, "The evolution of tele-financial fraud: an analysis of offender victim interaction structures and respondence to 'voice phishing'," Korean Journal of Public Safety and Criminal Justice, 17(3), pp. 101-149, Jan. 2008

[4] Dong Im Lee, "Recovery of revival from damage caused by voice phishing crime," Korean Journal of Victimology, 18(2), pp. 263-284, Oct. 2010

[5] Ho-Dae Cho, "Voice phishing occurrence and counterplan," The Journal of the Korea Contents Association, 12(7), pp. 176-182, July 2012

[6] Bum Joo Lee, Dong Uk Cho, and Yeon Man Jeong, "Identification of voice features for recently voice fishing by voice analysis," The Journal of Korean Institute of Communications and Information Sciences, 41(10), pp. 1276-1283, Oct. 2016

[7] Seon Hui Do, "A study on the phonetics of voice phishing," Criminal Investigation Studies, 4(1), pp. 67-90, June 2018

[8] Jung-Hoon Kim, Jun-Young Go, and Keun-Ho Lee, "A scheme of social engineering attacks and countermeasures using big data based conversion voice phishing," Journal of the Korea Convergence Society, 6(1), pp. 85-91, Feb. 2015

[9] Kwang Ho Jang and Hee Doo Kim, "Research of investigation technology to create a network using unstructured data: focusing on voice phishing response support," The Journal of Police Science, 20(2), pp. 93-117, June 2020

[10] Seung-Joon Yang, Bo-Yeon Lee, and Hee-Woong Kim, "A topic modeling approach to the analysis of happiness and unhappiness," Knowledge Management Research, 17(2), pp. 165-185, Jan. 2016

[11] S. Robertson, "Understanding inverse document frequency: on theoretical arguments for IDF," Journal of Documentation, vol. 60, no. 5, pp. 503-520, Oct. 2004.
[12] T.K. Landauer, D.S. McNamara, S. Dennis, and W. Kintsch, Handbook of latent semantic analysis, 1st Ed., Psychology Press, Feb. 2007.
[13] D.M. Blei, A.Y. Ng, and M.I. Jordan, "Latent dirichlet allocation," Journal of Machine Learning Research, vol. 3, pp. 993-1022, Jan. 2003.
[14] D.M. Blei and J.D. Lafferty, Text mining, 1st Ed., Chapman and Hall/CRC, June 2009.
[15] Yuyoung Kim and Min Song, "A study on analyzing sentiments on movie reviews by multi-level sentiment classifier," Journal of Intelligence and Information Systems, 22(3), pp. 71-89. Sep. 2016
[16] J.J. Inman, A.C. Peter, and P. Raghubir, "Framing the deal: the role of restrictions in accentuating deal value," Journal of Consumer Research, vol. 24, no. 1, pp. 68-79. June 1997.
[17] Minjung Kim and Eunmi Kim, "The types of the financial fraud and characteristics of victims focused on the middle-aged and elderly consumers," Journal of Consumer Policy Studies, 45(2), pp. 23-46. Aug. 2014
[18] Minjung Kim and Eunmi Kim, "Analysis of voice phishing damage experiences and influencing factors," Journal of Consumer Policy Studies, 52(1), pp. 52-71. April 2021
[19] Jihoon Yang, Choonghoon Lee, and Seong Baeg Kim, "Development and utilization of voice phishing prevention service through KoBERT-based voice call analysis," KIISE Transactions on Computing Practices, 29(5), pp. 205-213, May 2023

〈저자소개〉

한 치 훈 (Chihun Han) 정회원
2016년 8월: 한국외국어대학교 경영정보학 학사
2021년 2월: 연세대학교 정보대학원 정보시스템학 석사
2023년 7월~현재: 한국인터넷기업협회 정책2실 주임연구원
〈관심분야〉 프라이버시, 개인정보보호, 인공지능

김 범 수 (Beomsoo Kim) 종신회원
1990년 2월: 서울대학교 경영학 학사
1992년 2월: 서울대학교 경영학 석사
1999년 2월: University of Texas at Austin 경영학 박사
1999년~2002년: University of Illinois at Chicago 조교수
2002년~현재: 연세대학교 정보대학원 교수
〈관심분야〉 ICT의 효과적 활용, 데이터 거버넌스, 프라이버시, 개인정보보호

박 재 영 (Jaeyoung Park) 정회원
2012년 8월: 숭실대학교 정보통신전자공학부
2017년 2월: 연세대학교 정보대학원 정보시스템학 석사
2021년 8월: 연세대학교 정보대학원 정보시스템학 박사
2021년 9월~2022년 7월: 연세대학교 정보대학원 박사후 연구원
2023년 6월~현재: NH농협금융지주 금융연구소 책임연구원
〈관심분야〉 프라이버시, 개인정보보호, 디지털 금융