Journal of KIIT. Vol. 22, No. 5, pp. 23-31, May 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.5.23

어텐션 기반 1D CNN을 활용한 이더리움 온체인 피싱 탐지 방법

강성준*, 정현준**

Ethereum On-chain Phishing Detection Method using Attention-based 1D CNN

Seongjun Kang*, Hyunjun Jung**

이 연구는 정부(과학기술정보통신부)의 재원으로 한국 연구재단의 지원을 받아 수행되고 있습니다.
(No. NRF-2022R1G1A1008493)

요 약

최근 가상화폐의 대중화되면서 이의 특성을 이용한 피싱 및 자금 세탁과 같은 불법 행위가 급증하고 있다. 특히 이더리움을 이용한 온라인 피싱 및 스캠 범죄의 피해가 증가하는 추세이다. 이에 따라, 이더리움 기반 피싱 및 스캠을 효과적으로 탐지할 방법이 필요하다. 이 논문에서는 실시간으로 수집되는 이더리움 온체인 데이터를 활용하여 피싱 활동을 탐지할 수 있는 어텐션 기반 1D CNN을 모델을 제안한다. 본 모델의 핵심적인 특징은 트랜잭션 데이터의 시간 패턴을 인식하여 피싱을 예측하는 어텐션 메커니즘이 결합된 1D CNN 구조에 있다. 모델을 평가하기 위해 기존 딥러닝 모델들과 비교하였으며 비교한 결과 제안된 모델이 정확도와 AUC가 향상되었음을 확인할 수 있었다.

Abstract

The recent popularity of cryptocurrencies has led to a surge in illegal activities such as phishing and money laundering that take advantage of their characteristics. In particular, the number of online phishing and scam crimes using Ethereum is increasing. Therefore, there is a need for an effective way to detect Ethereum-based phishing and scams. In this paper, we propose an attentions-based 1D CNN model that can detect phishing activities by utilizing Ethereum on-chain data collected in real-time. The key feature of our model is the structure of a 1D CNN combined with an attentional mechanism that recognizes temporal patterns in transaction data to predict phishing. To evaluate the model, we compare it with existing deep learning models, and the results show that the proposed model has improved accuracy and AUC.

Keywords
on-chain data, blockchain, attention, 1D CNN, ethereum, cryptocurrency, phishing

* 군산대학교 소프트웨어학부 학사과정
- ORCID: https://orcid.org/0009-0001-0770-2035
** 군산대학교 소프트웨어학부 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-6717-1395

· Received: Mar. 20, 2024, Revised: Apr. 22, 2024, Accepted: Apr. 25, 2024
· Corresponding Author: Hyunjun Jung
Dept. of Software at Kunsan National University, 558, Daehak-ro, Kunsan-si, Jeollabuk-do, Republic of Korea
Tel.: +82-63-469-8917, Email: junghj85@kunsan.ac.kr

Ⅰ. 서 론

가상화폐의 대중화와 더불어 최근 이를 이용한 범죄가 행위가 급격히 증가하고 있다[1]. 특히, 가상 자산 거래의 익명성을 악용한 피싱 사기와 자금 세탁이 범죄 자금의 출처로 사용되고 있다. 이러한 자금은 다양한 범죄 활동에 자금을 제공하고 있어 이와 관련된 대책과 방법들이 논의와 검토를 거치고 있다[2]. 북한은 가상화폐 탈취나 북한 IT 노동자들이 벌어들인 불법 외화벌이 수익금을 가상화폐를 통해 세탁하고 현금화하여 막대한 수익을 벌어들이고 있으며 이러한 수법으로 2022년 3월 액시 인피니티 해킹을 통해 약 6억 2,500만 달러 상당의 가상화폐를 탈취하였다[3]. 북한은 탈취한 가상화폐를 추적하기 어렵게 여러 개로 분산하거나, 다른 가상화폐와 믹싱 방법으로 세탁하여 자금을 만들고 있다고 한다[4].

이렇게 탈취한 가상 자산은 김정은 국무 위원장에게 보고되며, 핵과 탄도 미사일 개발에 악용되는 것으로 분석된다[5]. 국정원은 2017년 북한의 해킹 그룹 라자루스의 악성코드가 국내 가상화폐 거래소를 해킹하여 260억 원 상당의 가상화폐를 탈취했다고 한다[6]. 2024년 2월 한 달 동안 약 4,7000만 달러에 달하는 가상화폐가 도난당했으며, 총 57,066명의 피해자가 가상화폐 관련 피싱 및 스캠 사기를 당한 것으로 분석되었다[7].

보고서에 따르면 이더리움 메인 넷 사용자들이 이러한 공격의 주된 피해자로 나타났다. 공격자들은 다양한 방법을 통해 피싱 및 스캠 범죄를 전략적으로 수행하는 데 온라인을 통해 피해자의 정보를 바탕으로 협박한 뒤, 대가로 가상화폐를 요구하는 범죄가 있으며 새롭게 발행되는 가상화폐를 구매하면 큰 수익을 얻을 수 있다는 식으로 투자자들을 유치하여 금원을 탈취하는 방식이 있다[8].

블록체인 데이터 분석 기업 체이널리스의 2024 가상 자산 범죄 보고서에 따르면 이들은 피해자와의 관계 형성을 통해 신뢰를 구축하고, 이를 이용하여 악의적인 가상화폐 거래에 서명하도록 유도 및 피싱 웹 사이트로 유인한 후 사용자들의 지갑을 연결하여 가상화폐를 탈취한 것으로 분석되었다[9]. 탈취한 가상화폐는 자금 세탁 및 다크 넷 시장을 통해 마약, 무기와 같은 범죄 자금으로 사용된다[10]. 이러한 문제를 해결하기 위해 가상화폐의 체계적 조사 방법과 대응책을 마련하고 실질적으로 시행하는 것이 필요하다.

가상화폐는 일반적으로 중앙은행이나 단일 관리 기관의 감독 없이 운영되는 디지털 화폐로, 암호 학적 기술을 활용하여 거래 보안을 강화하고, 이러한 거래들은 온체인(on-chain)이라 불리는 블록체인 기술을 기반으로 분산 원장에 기록된다. 온체인은 블록체인 네트워크 내에서 직접 이루어지고 검증되는 모든 거래 활동을 말한다. 블록체인의 이러한 특성은 각 거래의 연쇄적으로 연결하여 전체 거래의 역사와 현재 상태를 누구나 검증하고 확인할 수 있는 투명성과 확장성을 제공한다[11]. 이러한 가상화폐의 특징인 온체인 데이터 분석을 통해 범죄 행위 탐지에 대한 연구가 필요하다[12].

온체인 데이터는 가상화폐 거래에서 일어나는 트랜잭션에 대한 기록을 의미하며, 이 데이터는 블록체인의 공개적인 원장에 영구적으로 기록되어 누구나 검증할 수 있다[13]. 또한 온체인 데이터는 미가공 데이터로 제공되며 송금자와 수령자의 주소, 전송된 자산의 양, 거래에 부과된 수수료, 거래의 타임스탬프 및 고유한 트랜잭션 해시 값 등으로 구성되어 있다[14].

그림 1은 이더 스캔 API를 통해 북한 해커 라자루스 그룹이 사용한 이더리움 주소를 추적하여 온체인 데이터를 분석한 그림이다.

이 논문에서는 가상화폐의 특성을 이용한 피싱 및 스캠 문제를 해결하기 위해 이더리움 계좌 데이터 기반으로 한 온체인 피싱 탐지 모델을 제안한다. 본 논문에 구성은 다음과 같다. 2장에서는 관련 연구를 통해 기존의 온체인 데이터 분석 기법과 이를 활용한 피싱 탐지 연구의 동향을 살펴보고 3장에서는 제안된 어텐션 기반 1D CNN(Convolutional Neural Network) 모델의 구조와 작동 원리에 대해 상세히 설명한다. 4장에서는 제안한 방법을 실험 및 평가 분석하고, 5장에서는 연구 결과에 대한 종합적인 평가와 향후 연구 방향을 제시한다.

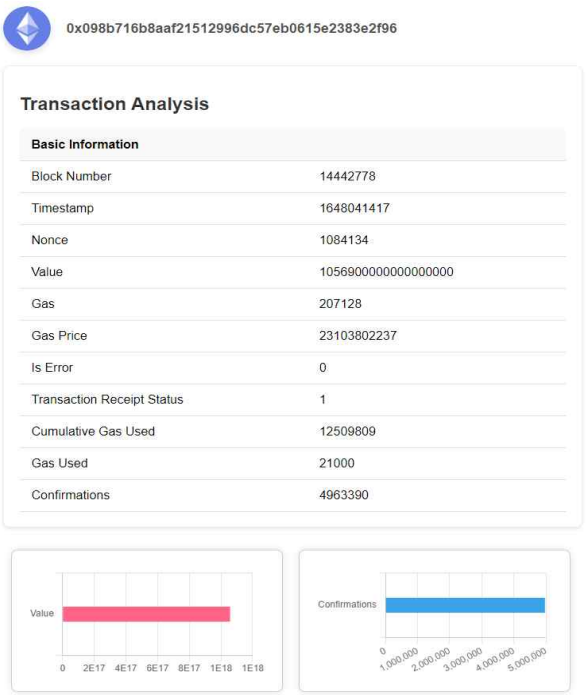

그림 1. 북한 해커 라자루스 온체인 데이터
Fig. 1. Lazarus group onchain data of DPRK hakers

II. 관련 연구

이 장에서는 가상화폐 관련 연구 및 온체인 데이터 분석 연구에 대한 동향을 설명한다.

2.1 온체인 데이터 분석 기법 연구

이 연구는 가상화폐 조사를 위한 블록체인 기반의 온체인 데이터 분석 기법에 대한 연구이다. 시간 특정 방식, 그래프 분석 방식 및 이상 징후 탐지 분석 등의 온체인 데이터 분석 기법을 가상화폐 조사를 위한 디지털 포렌식 분야의 조사 방법으로 제시하고, 일부 검증을 위해 pagerank 알고리즘을 사용하여 거래소 및 불법적인 행위와 관련된 가상화폐 주소들을 식별하는 실험을 진행하여 불법적인 행위에 포함된 주소들을 식별할 수 있었다[15].

이 논문에서는 온체인 데이터를 통해 가상화폐에서 발생하는 자금 세탁 및 범죄 자금에 관련된 행위를 탐지하고 추적하기 위해 온체인 데이터 분석 기법에 대한 연구들을 제시한다. 국내에서는 온체인 데이터를 활용한 연구가 상당히 제한적이며 이는 가상화폐 디지털 포렌식 영역에서 온체인 데이터를 활용한 추가적인 실증 연구 및 사례 분석이 필요함을 시사한다.

2.2 온체인 분석 기반 가상화폐 이상탐지

이 연구는 가상화폐 거래소 거래량의 이상 징후 탐지를 위한 프레임워크를 제안한 연구로 온체인 데이터 수집, 상관관계 분석, 딥러닝 기반 이상 탐지로 구성되었다. 이더 스캔 API를 이용해 온체인 데이터를 수집하고 이더리움 계좌 정보를 통합한 뒤, 각 거래소에서 중요하다고 판단되는 요소들을 선정하였다. 선정된 핵심 요인을 분석하고 실험하기 위해, attention과 LSTM(Long Short Time Memory) 모델을 사용하여 다양한 거래소에서 발생하는 거래량에 대한 피팅 곡선을 생성하고, 이 곡선을 이용해 실제 거래량과 피팅 된 거래량을 비교함으로써 이상 거래량을 탐지하였다. 이 과정을 통해 거래소의 일부 비정상적인 거래 금액이 정책 변경과 관련이 있는 것으로 나타났고, 다른 일부는 가상화폐 시장 내 불법 행위 및 자금 세탁과 연관되어 있음을 발견했다[16].

2.3 그래프 임베딩 기반의 이더리움 피싱 탐지

이 연구에서는 가상화폐의 특성을 이용해 피싱 스캠 범죄가 증가하는 현상에 대응하고, 기존 이더리움 네트워크에서 라벨이 지정된 피싱 주소 데이터의 불균형 문제를 해결하기 위해 그래프 임베딩 기술인 trans2vec와 준지도 학습 알고리즘인 tri-training을 결합한 방법을 제안하였다. 제안하는 이더리움 피싱 탐지 모델을 실험 평가를 진행하여 라벨링 된 데이터의 비율이 낮은 조건에서도 대략적인 탐지 결과를 얻을 수 있음을 확인하였다[17].

III. 어텐션을 활용한 1D CNN 기반 이더리움 온체인 피싱 탐지 방법

이 장에서는 이 논문이 제안하는 어텐션 기반 1D CNN 모델을 기반으로 한 온체인 피싱 탐지 프로세스의 모델의 구조와 작동 원리와 모델 실험에 사용한 온체인 데이터의 특성들을 설명한다.

3.1 시스템 프로세스

이 논문에서 제안하는 온체인 피싱 탐지 모델 프로세스는 그림 2와 같다. 피싱 탐지 모델 프로세스는 1번 Phishing Detection Model Train 파트부터 작동한다. 먼저 Kaggle에서 제공하는 이더리움 피싱 계좌 및 정상 데이터를 수집 후 각 데이터를 전처리를 진행한다. 전처리 과정을 거친 데이터는 딥러닝 모델에서 학습을 진행하여 학습 모델을 구성한다. 사용한 이더리움 계좌의 여러 특성을 포함하는 횡단 면적 데이터 학습을 위해 지역적인 패턴 인식에 강인한 1D CNN모델을 사용한다. 1D CNN 모델을 통해 서로 연관된 특성들 사이의 관계를 포착하며 각 특성이 다른 특성들과 어떻게 상호 작용하는지 학습한다. 또한 모델에 셀프 어텐션(Self-Attention)을 사용하여 각 입력 특성의 중요한 정보에 집중할 수 있도록 하며 다양한 유형의 종속성을 포착하고 모델이 다양한 소스의 정보를 결합할 수 있도록 한다. 출력 레이어에서 이진 분류를 통해 클래스를 할당한다. 이후 학습된 모델에 피싱 탐지를 하기 위해 실시간으로 이더리움 계좌 데이터를 수집해야 한다. 2번 On-chain data collection & cleansing 부분에서 실시간으로 이더 스캔 API를 통해 이더리움 블록을 수집하여 계좌 정보 및 트랜잭션 데이터를 전처리 과정을 거친다. 이후 학습된 온체인 피싱 탐지 모델에 이더리움 계좌 데이터들을 입력하여 수집된 계좌 정보가 정상 또는 스캠인지 이진 분류를 통해 예측하는 3번 Phishing Predict Module 과정을 거친다. 이 과정에서는 이더리움 온체인 사이트인 이더 스캔 API를 사용한다. 이더 스캔 API를 통해 이더리움 블록을 수집한다. 수집된 이더리움의 블록에는 수신자 및 송금자의 정보와 이더리움 양의 가격을 알 수 있다. 이렇게 수집된 주소를 다시 이더 스캔에 API를 호출하여 지갑에 대한 거래 정보 및 거래 활동 일수에 대한 정보를 수집 후 전처리 과정을 거친 데이터를 1번 프로세서에서 학습한 온체인 피싱 탐지 모델에 입력하여 주소가 정상 지갑 주소 및 스캠 지갑 주소일 가능성을 알려준다.

3.2 온체인 피싱 탐지 모델 구조

이 절에서는 온체인 피싱 탐지 모델에 대해서 설명한다.

이더리움 피싱 및 정상 계좌 데이터를 읽어와 Dataframe 형태로 저장한다. 저장된 데이터 프레임을 불러와 사기 및 정상 레이블 열을 제외한 데이터를 x로 저장하고 레이블 열은 y로 분리한다.

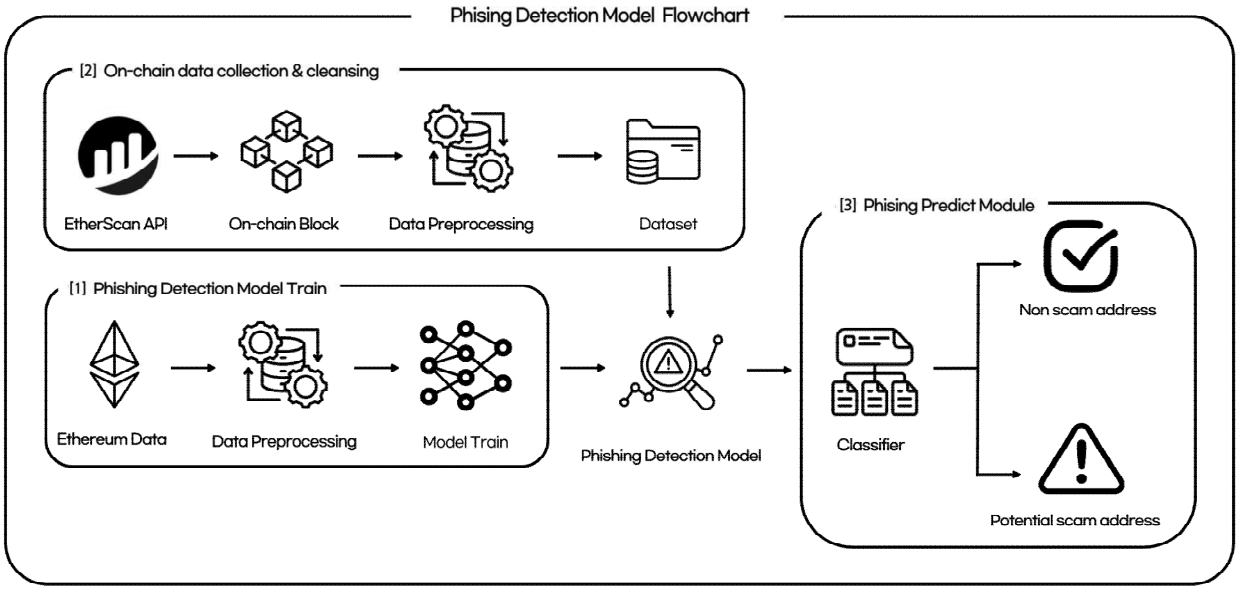

그림 2. 온체인 피싱 탐지 방법
Fig. 2. Onchain phishing detection method

Conv1D는 입력 데이터가 3차원 구조를 갖도록 요구하기 때문에 변환된 데이터 형태에 차원을 확장하여 [sample, x, 1] 형태로 변환된다. 변환된 데이터는 Conv1D 레이어에서 합성곱(Convolution1D)과정에서 필터를 통해 입력 데이터의 가중치를 계산하며 활성화 함수는 복잡한 데이터 패턴을 학습하기 위해 ReLU(Rectified Linear Unit)을 사용한다. 두 번의 합성곱 과정을 거치고 통과된 값을 맥스 풀링(MaxPooling) 과정을 통해 중요한 특성을 유지하도록 출력을 다운 샘플링 한다. 합성곱을 추가적으로 수행 후 셀프 어텐션을 통해 입력된 특성들을 상호 의존성을 파악하여 각 특징들이 전체 패턴에서 어떤 역할을 하는지 잘 이해하여 특징들의 중요성을 파악한다. 추출된 특성들은 평탄화(Flatten) 과정을 통해 다차원 배열을 1차원 벡터로 변환하여 FC(Fully Connected) 레이어로 넘어간다. 모델의 과적합 방지를 위해 드롭아웃(Dropout)의 비율은 0.3으로 설정했다. 최종 출력(Output)은 사기 및 정상 클래스로 분류하기 위해 이진 분류 함수인 시그모이드(Sigmoid) 활성화 함수를 사용하여 0과 1사이의 확률 값으로 계산한다.

3.3 온체인 데이터 수집 및 정제

이 절에서는 이더리움 온체인 데이터 수집과 데이터 정제 과정을 설명한다.

이더리움 온체인 데이터를 수집하고 가공하기 위해서는 가상화폐의 트랜잭션 데이터를 수집하는 과정이 필요하다. 이더리움 온체인 데이터 수집에 있어서, 이더리움의 블록 정보를 쉽게 조회할 수 있는 대표적인 플랫폼인 etherscan.io를 이용해 데이터를 수집한다. 일반적으로 제공하는 온체인 데이터는 원시 데이터의 형태로 제공된다.

이 원시 데이터를 온체인 피싱 탐지 모델에 적합한 형태로 변환하기 위해 수집한 데이터를 정제한다. 데이터 정제 과정은 불필요한 정보의 제거와 필요한 데이터 형식으로 포맷하였다. 이더리움 블록 수집은 etherscan.io에서 수집하였으며 해당 블록 내의 거래 주소를 추적하여 바탕으로 각 주소의 데이터를 수집하였다. 표 2는 이더리움 블록 정보를 수집하기 위한 코드이다. 표 1은 수집한 계좌 온체인 데이터 컬럼이다. 수집한 데이터는 온체인 피싱 탐지 모델에서 활용되는 데이터와 유사한 형태로 구성되어야 한다. 파이썬의 pandas 라이브러리를 활용하여 데이터 전처리 과정을 거쳐 12개의 새로운 컬럼을 만들어 정리했다. 표 3은 이러한 전처리 과정을 통해 만들어진 계좌 데이터의 새로운 컬럼들이다.

표 1. 온체인 계좌 데이터
Table 1. On-chain account data

Column	Type
Txhash	Transaction hash
Method	Contract Call Functions
Blockno	Ethereum block number
DateTime (UTC)	Trading hours (Coordinated Universal Time)
From	Sender address
To	Recipient address
From_Nametag	Sender labeling
To_Nametag	Recipient labeling
Value	Amount of Ethereum
Txn Fee	Transaction fees

표 2. 이더리움 블록 정보 수집 코드
Table 2. Ethereum block information collection code

```
key = "API_KEY_Input“

def fetch_block():
    url_base = "https://api.etherscan.io/api"
    pa1 = {
        'module': 'proxy',
        'action': 'eth_blockNumber',
        'apikey': key
    }
    blk_num_res = requests.get(url_base, pa1).json()
    blk_num = int(blk_num_res['result'], 16)
    pa2 = {
        'module': 'proxy',
        'action': 'eth_getBlockByNumber',
        'tag': hex(blk_num),
        'boolean': 'true',
        'apikey': key
    }
    blk_info_res = requests.get(url_base, pa2).json()
    with open(f"blk_{blk_num}.json", 'w') as f:
        json.dump(blk_info_res, f, indent=4)
    print(f"Saved blk {blk_num} info")

while True:
    fetch_block()
    time.sleep(20)
```

표 3. 전처리한 계좌 데이터
Table 3. Preprocessed account data

Column	Type
AvgRecTnxInterval	Average time interval between incoming transactions
ActivityDays	Days of activity
TotalTransactions	Total number of transactions
AvgValSent	Average Ethereum transfer volume
LifeTime	Account lifetime
NumUniqRecAddress	Number of unique addresses received
NumUniqSetAddress	Number of unique addresses sent
TotalEtherBalance	Number of unique addresses sent
TxFreq	Transaction frequency
AverageActiveHour	Average time of activity
Max Value Sent	Maximum ether transferred
Max Value Received	Maximum ether received

3.4 피싱 예측 탐지

이 절에서는 학습된 온체인 피싱 탐지 모델이 실시간으로 전처리된 계좌 정보를 바탕으로 피싱을 예측하고 탐지하는 방법에 대해 설명한다.

사전에 학습된 온체인 피싱 탐지 모델은 전처리된 계좌 정보 데이터를 입력으로 받아 예측을 수행한다. 예측된 결과는 각 계좌에 대한 피싱 확률을 나타내며, 이 확률의 평균값을 계산하여 임곗값과 비교한다. 식 (1)은 계산된 평균 예측값을 계산하는 수식이다. $\bar{y}$는 평균 피싱 확률을 나타내고 N은 총 계좌 수를 나타내며 yi는 각 계좌의 대한 개별 피싱 확률을 나타낸다.

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} yi \quad \begin{cases} fraud & \text{if } \bar{y} > \theta \\ non\,fraud & \text{if } \bar{y} < \theta \end{cases} \tag{1}$$

$\bar{y}$가 임곗값을 초과하는 경우, 해당 계좌는 피싱으로 분류된다. 해당 과정을 통해 각 계좌에 대한 피싱 예측을 수행할 수 있다.

IV. 실험 및 평가

이 장에서는 본 논문에서 제안하는 온체인 피싱 탐지 모델에 사용한 실험 데이터 수집과 정제 에 대해서 설명하고 모델의 성능 평가를 진행한다.

4.1 실험 환경

모델 실험을 위해 사용한 소프트웨어는 Python 3.9.13, Tensorflow 2.7.0 버전을 사용하였다. 이 실험에서는 Kaggle 및 Github 플랫폼에서 수집한 온체인 이더리움 피싱 주소 데이터를 결합하고, 전처리를 진행했다. 데이터 전처리 후에는 SHAP 라이브러리를 활용하여 피처 선택을 수행한 데이터 바탕으로 모델 학습을 진행하였다.

4.2 실험 데이터 수집 및 정제

이 절에서는 온체인 이더리움 피싱 계좌 주소를 분석하기 위해 Kaggle에서 제공하는 온체인 이더리움 사기 계좌 데이터를 활용하였으며 추가적으로 Github 및 EtherScan을 통해 각 피싱 및 정상 계좌 온체인 데이터를 수집하였다. 이더리움 사기 계좌 데이터는 11,433개 이더리움 정상 계좌 데이터는 14,633개로 이를 통합하면 총 26,066개로 학습 데이터 구성 시 신경망 모델의 견고한 학습 및 공정한 성능 비교가 이루어질 수 있도록 실험을 진행하였다.

표 4. 학습 데이터
Table 4. Training data

Type	Total
Fraud data	11,433
Non fraud data	14,640
ALL	26,073

4.3 실험 결과 및 비교 평가

이 논문에서 제안하는 온체인 피싱 탐지 모델의 성능 평가를 위해 기존 딥러닝 모델과의 성능 비교를 평가한다. Proposed Model V1은 1D CNN 모델이고 Proposed Model V2는 1D CNN 모델에 셀프 어

텐션 레이어를 추가한 모델이다. 이 논문에서는 앞서 설명한 실험 데이터 셋을 각 모델에 사용하여 비교 평가를 진행했다. 표 5는 식 (1)을 적용한 모델의 임계값에 따른 정확도를 평가한 표이다. 이 논문에서 제안하는 온체인 피싱 탐지 모델의 임계치가 0.5일 때 93%의 성능을 보였다. 이진 분류 모델의 성능 평가를 위해 AUC(Area Under the Curve)를 이용하여 평가했다.

표 5. 임계값에 따른 모델 정확도
Table 5. Accuracy of model according to threshold

Threshold value	Model accuracy
0.1	87%
0.2	89%
0.3	92%
0.4	93%
0.5	93%
0.6	91%
0.7	89%
0.8	88%
0.9	85%

그림 3은 실험 데이터 셋을 통해 훈련된 각 모델의 AUC Score를 나타낸 결과이다. 식 (2)는 AUC score를 수식으로 표현한 식이다. 이 논문에서 제안된 온체인 피싱 탐지 모델인 Proposed Model v2는 0.98이며 Proposed Model v1은 어텐션 결합이 없는 1D CNN 모델로 0.96으로 성능이 평가되었다. 평가 결과 제안 모델이 다른 딥러닝 모델에 비해 피싱 탐지 클래스를 분류하는 성능이 우수한 것을 알 수 있었다.

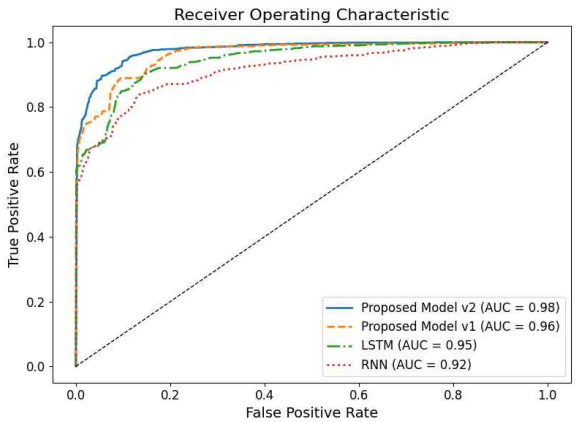

그림 3. 모델 간의 AUC 비교
Fig. 3. AUC comparison between models

그림 4와 표 6은 이 논문에서 제안한 온체인 피싱 탐지 모델과 딥러닝 모델들의 성능을 비교한 결과이며 정확도와 Precision, Recall, F1-score를 측정하였다. 식 (3)과 식 (4)를 통해 정확도 및 F1-score르 계산함으로써, 각 모델의 성능을 정략적으로 평가했다. 이 논문에서 제안한 모델의 정확도는 0.93, F1-score는 0.92로 다른 딥러닝 모델에 비해 성능이 향상되었다.

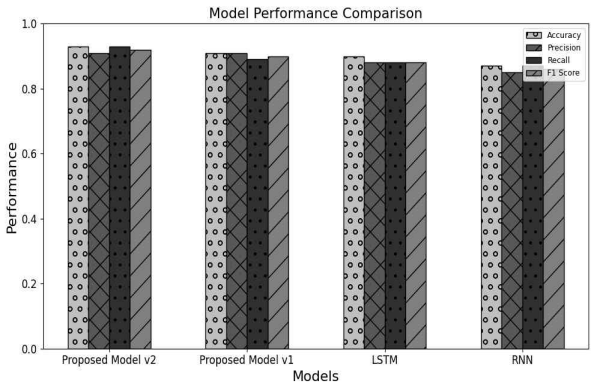

그림 4. 모델간의 성능 비교
Fig. 4. Performance comparison between models

표 6. 성능 비교결과
Table 6. Performance comparison results

Model	Accuracy	Precision	Recall	F1-score
Proposed model v2	0.93	0.91	0.93	0.92
Proposed model v1	0.91	0.91	0.89	0.90
LSTM[18]	0.90	0.88	0.88	0.88
RNN[19]	0.87	0.85	0.87	0.86

$$AUC = \int_0^1 TPR(d)dFPR(d) \tag{2}$$

여기서, TPR은 피싱 주소를 정확하게 예측한 비율이며 FPR은 정상 주소를 피싱으로 분류한 비율이다.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{3}$$

여기서, TP와 TN은 모델이 피싱 주소와 정상 주소를 정확하게 예측한 경우, 예측 FP는 실제 정상이지만 피싱으로 잘못 예측한 경우, FN은 실제 피싱이지만 모델이 정상으로 잘못 예측한 경우다.

$$F1Score = 2 \cdot \frac{\mathrm{Precision} \cdot Recall}{\mathrm{Precision} + Recall} \quad (4)$$

Ⅴ. 결론 및 향후 과제

이 논문에서는 가상화폐를 이용한 피싱 및 스캠을 통한 범죄 자금으로 사용되는 문제를 해결하기 위해 피싱 라벨이 붙여진 가상화폐 주소 기반으로 온체인 데이터를 분석하였으며, 온체인 데이터의 다양한 특징들의 종속성을 포착하기 위해 어텐션과 1D CNN 모델을 사용하여 학습을 진행했다. 실험 평가를 통해 기존 딥러닝 모델보다 어텐션을 결합한 1D CNN 모델이 더 우수한 성능을 보였다. AUC는 0.98로 모델이 피싱 탐지 클래스를 우수하게 분류하였으며, 정확도는 93%로 Proposed Model v1보다 2%의 향상을 보였다. 이 논문에서는 실시간으로 수집되는 온체인 데이터를 처리하고 분석할 수 있는 모델을 제시함으로써 실시간 피싱 및 스캠 탐지의 가능성을 제시했다. 최근 국내 및 전 세계에서 가상화폐를 통한 범죄 행위에 대한 사건들이 빈번히 발생하고 있는 상황에서, 온체인 데이터 분석을 통한 불법 행위의 스캠 및 피싱 계좌 식별은 매우 중요한 과제다. 이러한 배경 하에 이 논문은 온체인 데이터를 효과적으로 활용하여 가상화폐 관련 범죄를 예방하고 탐지하는 기법을 제시함으로써, 해당 분야 연구에 이바지할 것으로 기대된다.

향후 연구에서는 이 논문에서 제시된 온체인 피싱 탐지 모델 프로세스에 실시간 데이터 분석 기능 강화를 통한 온체인 데이터 스트리밍 및 분석 기능을 통합하여 즉각적인 대응 메커니즘을 구축하는 과정이 필요할 것이며 이 논문에서 분석한 이더리움 온체인 데이터뿐만 아니라 다양한 가상화폐 플랫폼으로 확장하여 온체인 피싱 탐지 모델의 범용성을 검증하기 위한 연구를 확장할 것이다.

References

[1] J. Kim, "The Current Status of the Darkweb and Legal Issues in Use", Legal Theory & Practice Review, Vol. 11, No. 3, pp. 181-220, Aug. 2023. https://doi.org/10.30833/LTPR.2023.08.11.3.181.

[2] J. Kim, "A study on the criminal law response to cryptocurrency crimes", Legal Theory and Practice Research, Vol. 11, No. 4, pp.293-316 Nov. 2023. https://doi.org/10.30833/LTPR.2023.11.11.4.293.

[3] J. Kim and K. Lee, "Revisiting International Legal Response to North Korea's Cryptocurrency Heist: Enhancing cyber deterrence through hacking-back", The Quarterly Journal of Defense Policy Studies, Vol. 39, No. 4, pp. 33-63, Jan. 2024. https://doi.org/10.22883/jdps.2024.39.4.002.

[4] W. Jo, G. Kim, S. Heo, and H. Kim, "Trends in the Study of Response Measures for Cryptocurrency Theft and Money Laundering Using Ransomware", Journal of Information Security, Vol. 32, No. 3, pp. 19-26, Jun. 2022.

[5] S. Han and Y. Kim, "A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Korea", Police Science Institute, Vol. 34, No. 2, pp. 319-355, Jan. 2020. https://doi.org/10.35147/knpsi.2020.34.2.319.

[6] D. Yoo, "North Korea's Cyber Threats and Countermeasures", The Journal of Strategic Studies, Vol. 28, No. 3, pp. 7-36, Nov. 2021. https://doi.org/10.46226/jss.2021.11.28.3.7.

[7] Dune, "February 2024 Scam Sniffer Phishing Report", https://dune.com/scam-sniffer/february-2024-scam-sniffer-phishing-report [accessed: Mar. 17, 2024]

[8] J. Jung, "A Study on Pan-governmental and Legislative Controls Related to Cryptocurrency Crime - Focusing on the Amendments to the Specific Financial Information Act", The Journal of Police Science, Vol. 21, No. 1, pp. 61-89, Mar. 2021. https://doi.org/10.22816/POLSCI.2021.21.1.003.

[9] Chainalysis, "The 2024 Crypto Crime Report", https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20Crypto%20Crime%20Report.pdf?version=0 [accessed: Mar. 16, 2024]

[10] S. Lee, "The Trilemma of the Digital Revolution, Underground Finance, and Cybercrime: Countermeasures against Threats, Attacks, and

Crimes Against Crypto Assets", Journal of Payment and Settlement, Vol. 15, No. 1, pp. 169-207, Jun. 2023. https://doi.org/10.22898/kpsakr.2023.15.1.169.

[11] S. Jeong and H. Jung, "Design of Blockchain based Digital Badge Framework for Reliable Career Verification", The Journal of Korean Institute of Information Technology, Vol. 20, No. 9, pp. 147-153, Sep. 2022. http://dx.doi.org/10.14801/jkiit.2022.20.9.147.

[12] J. Jeyong, "A Study on Victimization Factors of Cryptocurrency Crime and its Control Measures: Applying Mixed Methods Research", Journal of the Korean Police Association, Vol. 23, No. 2, pp. 63-92, 2021.

[13] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration", it - Information Technology, Vol. 60, No. 5-6, pp. 283-291, Nov. 2018. https://doi.org/10.1515/itit-2018-0019.

[14] N. Jagannath, et al, "An on-chain analysis-based approach to predict ethereum prices", IEEE Access, Vol. 9, pp. 167972-167989, Dec. 2021. https://doi.org/10.1109/ACCESS.2021.3135620.

[15] S. W. Jeong and B. W. Suh, "A Study of Blockchain-based On-Chain Data Analytics Techniques for Cryptocurrency Investigations", Journal of Digital Forensics, Vol. 17, No. 3, pp. 93-105, Sep. 2023. https://doi.org/10.22798/kdfs.2023.17.3.93.

[16] Z. Gu, D. Lin, and J. Wu, "On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges", Physica A: Statistical Mechanics and its Applications, Vol. 604, Oct. 2022. https://doi.org/10.1016/j.physa.2022.127799.

[17] Y. Cheong, G. Kim, and D. Im, "Ethereum Phishing Scam Detection based on Graph Embedding and Semi-Supervised Learning", KIPS Transactions on Computer and Communication Systems, Vol. 12, No. 5, pp. 165-170, Dec. 2023. https://doi.org/10.3745/KTCCS.2023.12.5.165.

[18] S. Wang, S. Khan, C. Xu, S. Nazir, and A. Hafeez, "Deep learning-based efficient model development for phishing detection using random forest and BLSTM classifiers", Complexity, Vol. 2020, pp. 1-7, Sep. 2020. https://doi.org/10.1155/2020/8694796.

[19] T. Feng and C. Yue, "Visualizing and interpreting RNN models in URL-based phishing detection", In Proc. of the 25th ACM Symposium on Access Control Models and Technologies, Barcelona Spain, pp. 13-24, Jun. 2020. https://doi.org/10.1145/3381991.3395602.

저자소개

강 성 준 (Seongjun Kang)

2018년 3월 ~ 현재 : 군산대학교 소프트웨어학과 학사과정
관심분야 : 클라우드, 블록체인, 웹, 서버, 사물 인터넷

정 현 준 (Hyunjun Jung)

2008년 : 삼육대학교 컴퓨터과학과(학사)
2010년 : 숭실대학교 컴퓨터학과(공학석사)
2010년 : 고려대학교 컴퓨터·전파통신공학과(공학박사)
2017년 8월 ~ 2020년 8월 : 광주과학기술원 블록체인인터넷경제연구센터 연구원
2021년 ~ 현재 : 군산대학교 소프트웨어학과 교수
관심분야 : 블록체인, 데이터 사이언스, 센서 네트워크, 사물인터넷, 머신러닝