

GCN 기반의 악성코드 탐지 모델과 XAI적용을 통한 악성코드 탐지

스마트 컨트랙트
취약점 분석[illegible]

- 인공지능 기반의 악성코드 연구가 이루어지고 있으나, 악성코드의 특징을 고려한 연구가 부족하며, 탐지 결과에 대한 설명을 제공하기 어려운 문제가 존재함
- XAI 적용을 통해 실제 악성코드 탐지 시, 인공지능이 어떤 부분을 보고 악성코드라고 판별하였는지 파악이 가능하며, 이를 통해 악성코드 탐지 모델의 오탐/미탐 원인 분석 및 성능 개선과 탐지 결과에 대한 신뢰성 제공이 가능함

기존기술

기존의 인공지능 기반 악성코드 탐지 기술
적용 시, 탐지 결과만 제공되며 이에 대한
원인이나 근거를 제시하지 못하는 문제가 존재

- ▶ 단순 이미지 변환 및 Convolutional Neural Network (CNN) 기반의 탐지로 인해, 악성코드 특징 추출이 어려움
- ▶ 탐지 모델만을 제공하여 악성코드 탐지 결과에 대한 설명이 어렵고, 오탐/미탐에 대한 성능 개선이 불가능

기술 차별성

악성코드 탐지 모델의 탐지 결과에 대한
피드백이 가능한 Explainable AI(XAI) 기반
악성코드 탐지 기술 개발

- ▶ Graph Convolutional Neural Network (GCN)
기반의 악성코드를 탐지 통해, 악성코드 공격
분기점 파악에 사용되는 Branch를 파악 가능
- ▶ XAI 기반의 탐지 결과에 대한 설명 제공을 통해
오탐/미탐에 대한 성능개선 가능

발명의 명칭

블록체인 클라이언트 취약점 탐지방법
및 취약점 탐지 장치

출원 번호

10-2022-0097394

출원 일자

2022.08.04