

제목 : ResNet-Variational AutoEncoder기반 변종 악성코드 패밀리 분류

1.제안

도메인 전문가의 개입 없이도 변종 악성코드의 패밀리를 분류할 수 있는 ResNet-Variational AutoEncoder 기반 변종 악성코드 분류 방법을 제안

Variational AutoEncoder (VAE) 네트워크를 활용하여 악성코드를 분류

2.주요 내용 및 기술

- Variational AutoEncoder (VAE):

정규 분포 내에서 새로운 데이터를 생성하는 기계학습 모델

논문에선 VAE의 학습 과정에서 잠재 변수를 추출하여 악성코드의 중요 특징 추출

- 전이 학습 (Transfer Learning):

ImageNet Dataset으로 사전 학습된 ResNet-152 모델의 학습 파라미터를 Encoder Network의 학습 파라미터로 전이하여 훈련 데이터의 특징을 더 잘 학습하고 학습의 효율성을 높임.

- Stacking Classifier를 활용한 앙상블 모델:

변종 악성코드 분류를 위해 Stacking Classifier를 사용하여 앙상블 모델을 구축함.

이 모델은 98.66%의 Accuracy와 98.68의 F1-Score를 달성함.

3.결과 및 기대 효과

전이학습을 수행한 ResNet-Variational AutoEncoder의 경우 기존 Variational AutoEncoder에 비해 높은 성능을 보였으며 학습의 효율을 보임.