인공지능 보안데이터 분석 기술

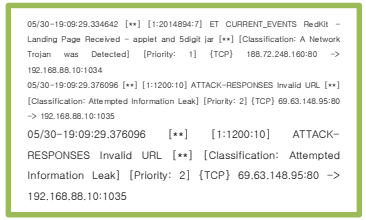
소프트웨어학부 윤명근 교수

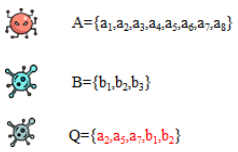
(mkyoon@kookmin.ac.kr)

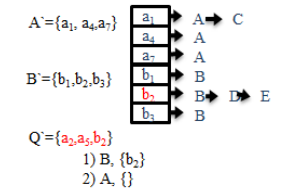
기술 개요

소개기술

- 인공지능 악성코드 탐지 기술
- 인공지능 보안관제 이벤트 분석 기술
- 보안빅데이터 유사도 검색 기술







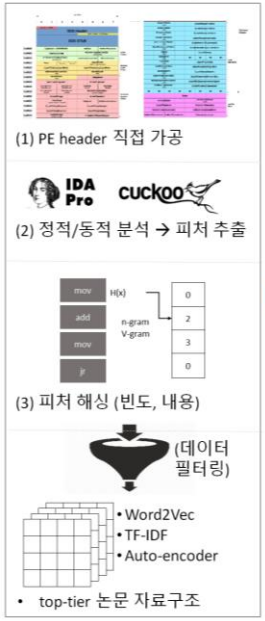
연구배경

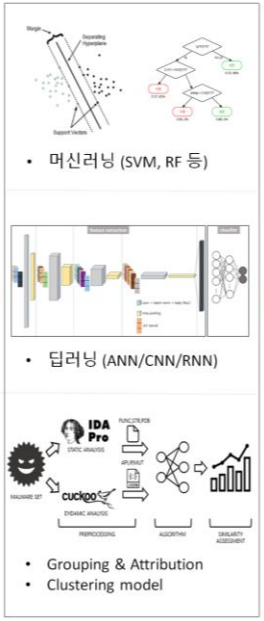
- 악성코드 폭발적 증가에 따른 자동 분석 기술 필요
- 보안관제 이벤트 자동 분석과 공격 대응 기술 필요
- 패킷 레벨의 악성코드 유입 및 내부자료 유출 탐지 기술 필요

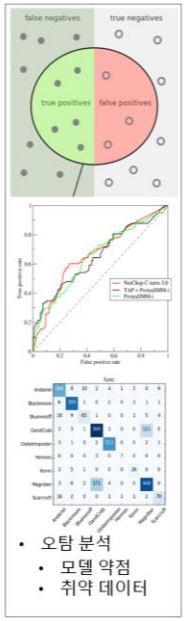
인공지능 악성코드 탐지 기술

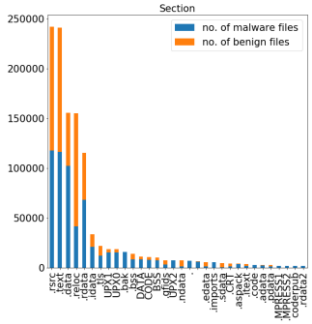
- 변종 악성코드 탐지 기술
  - 정적/동적 분석 기술
- PE/문서형 악성코드 특징 가공 기술
  - **피처해싱 최적화**
  - 정형/비정형 특징 처리
- 머신러닝과 딥러닝 모델 구현 기술
  - 이미지 변환 + CNN 학습
  - **E2E 딥러닝/멀티모달 학습**

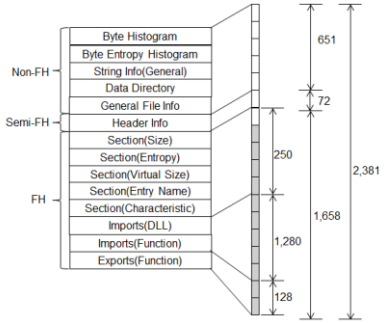
- 특허 출원 및 등록 10건 이상
- 정보보호R&D데이터챌린지 5회 수상
- 국내 시장 1위 기업 기술이전 4건







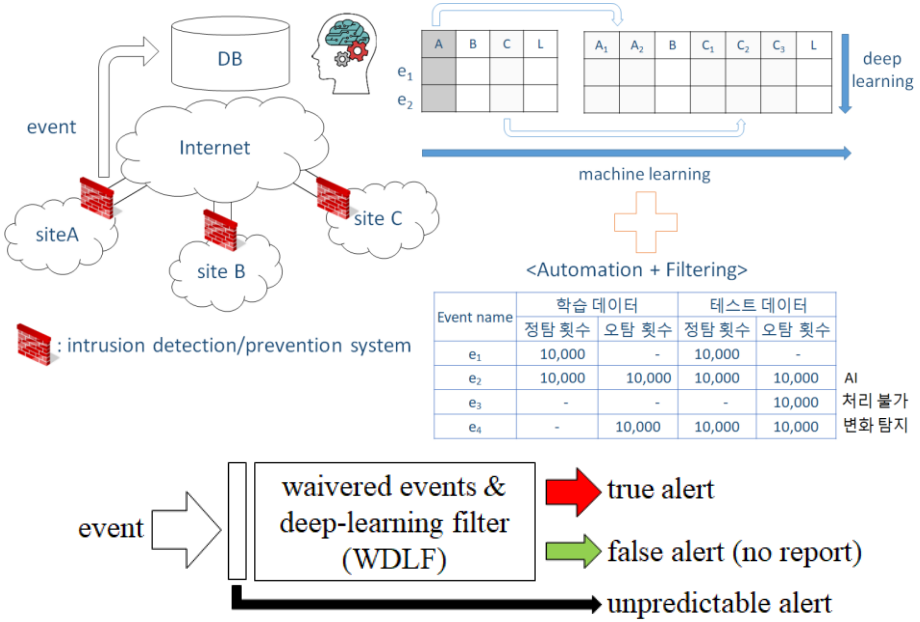




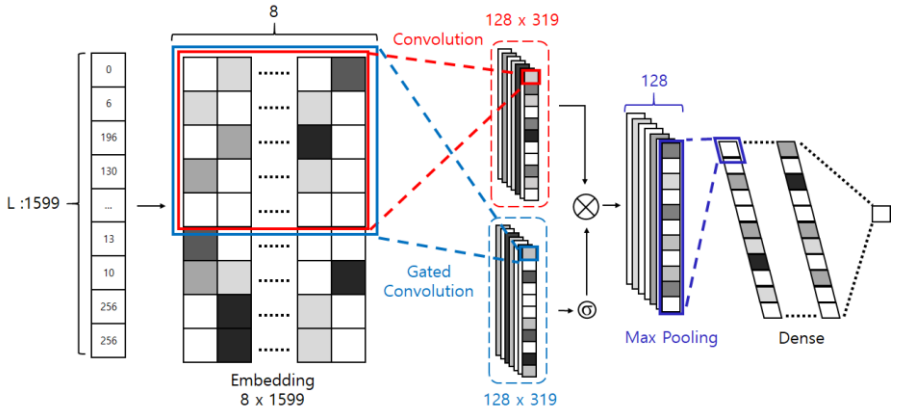
인공지능 보안관제 이벤트 분석 기술

- 보안관제 이벤트 특징 추출 기술
  - 정형/비정형 특징 처리
- 정오탐 자동 분류 및 공격 탐지 기술
  - **이벤트 내부 정보 활용**
  - **이벤트 상호 연계 정보 활용**
- 머신러닝과 딥러닝 모델 구현 기술
  - **1DConv 기반 패킷 러닝 기술**
  - E2E 딥러닝/멀티모달 학습

- 특허 출원 및 등록 3건 이상



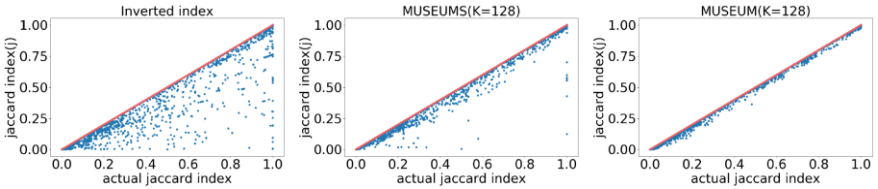
Event name	학습 데이터		테스트 데이터		
	정탐 횟수	오탐 횟수	정탐 횟수	오탐 횟수	
e_1	10,000	-	10,000	-	
e_2	10,000	10,000	10,000	10,000	AI
e_3	-	-	-	10,000	처리 불가
e_4	-	10,000	10,000	10,000	변화 탐지

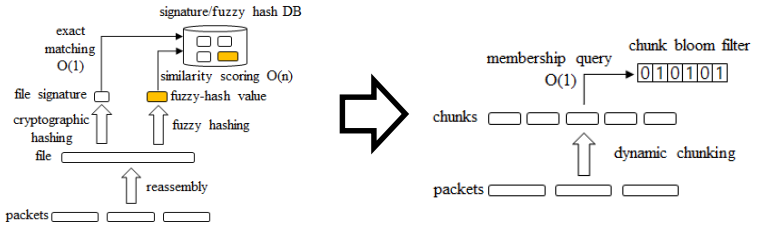


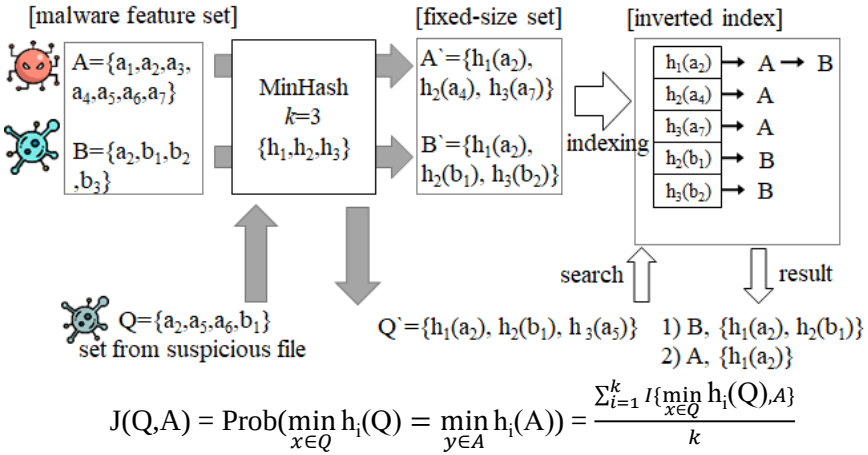
보안빅데이터 유사도 검색 기술

- 고정 크기 샘플링 이론 증명 및 구현
  - **MinHash 이론 활용**
  - **원본 크기 무관 64개 샘플 추출**
- Elasticsearch 플랫폼 구현 완료
  - 천만 개 이상 악성코드 실험 성공
  - **기존 기술 대비 처리속도, 저장공간 6배 이상 향상**
- **원본 패킷에서 내부 정보 유출 탐지**

- 특허 출원 및 등록 다수(국제특허 포함)







$$J(Q,A) = \text{Prob}(\min_{x \in Q} h_i(Q) = \min_{y \in A} h_i(A)) = \frac{\sum_{i=1}^{k} I\{\min_{x \in Q} h_i(Q), A\}}{k}$$

응용 분야

응용시장

△보안 제품 제조 산업 (악성코드, 침입방지, 문서보안)
△보안 서비스 산업 (사이버보안센터, 보안관제)
△빅데이터 검색 산업 (포털사이트, 검색엔진 개발)