고려대학교 KOREA UNIVERSITY

이경호 교수 (고려대학교 정보보호대학원)

# 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체

(기술분류-보안-디지털 취약점 분석·대응)

## 기술성 분석

### 기술 개요

- 본 기술은 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체에 관한 것으로, 모바일 운영체제에서의 데이터 특성을 반영하여 악성 코드를 탐지하며, 알려지지 않은 새로운 모바일 악성 코드인 경우 악성 행위의 유무를 판단할 수 없는 잠재된 악성 코드를 탐지할 수 있어 유리한 효과가 있음
- 또한, 조합 가능한 모든 데이터셋과 기준에 대한 검증으로 탐지율이 가장 높은 조합을 탐지 프로세스로 결정할 수 있어 보다 빠르고 정확하게 탐지할 수 있음

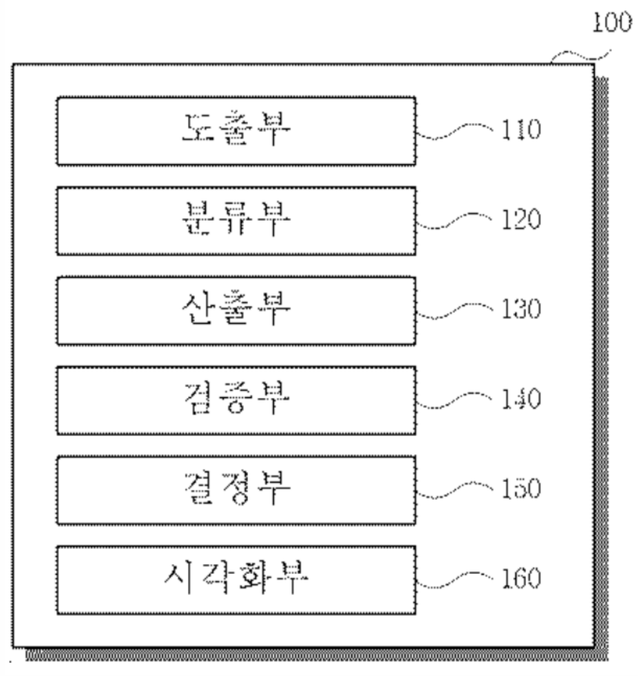
### 미해결 과제(Unmet needs)

- 기존 모바일 악성 코드 탐지 방법의 한계
  - 모바일 환경에서의 악성 코드의 유입은 빠르게 증가하는 추세이며, 이에 따라 금전적 피해를 야기할 수 있는 모바일 환경 하에서의 악성 행위의 탐지와 예측이 중요해지고 있으나, 기존의 모바일 악성 코드 탐지 방법은 규칙 기반이나 블랙리스트 기반이기 때문에 알려진 공격에 대한 탐지만 가능하므로 알려지지 않은 새로운 모바일 공격에 대비할 수 있는 분류 기술이 요구됨

### 기술적 해결수단(발명의 구성)

- 1) 본 발명의 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험 관리 장치의 구성
  - 도출부(110)는 모바일 악성 코드 데이터에 대해 정적 분석 및 가상 환경 하에서 동적 분석을 수행하고, 이를 바탕으로 기존 블랙 리스트를 기반의 모바일 악성 코드 특성을 도출하여 기존 모바일 악성 코드와 관련성이 높은 특성을 선정함
  - 분류부(120)는 선정된 특성들을 활용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류함
  - 산출부(130)는 분류된 악성 행위에 대해 위험도를 산출함
  - 검증부(140)는 모바일 악성 코드 탐지 과정의 효율을 검증함
  - 결정부(150)는 조합 가능한 모든 모바일 데이터 셋과 기준들에 대한 검증부의 검증결과를 기초로, 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정함
  - 시각화부(160)는 위험도를 직관적으로 인식할 수 있도록 비율에 따른 분류, 색상에 따른 분류 및 도표 등으로 나타냄

본 발명의 악성 코드 행위에 따른 위험 관리 장치의 구성



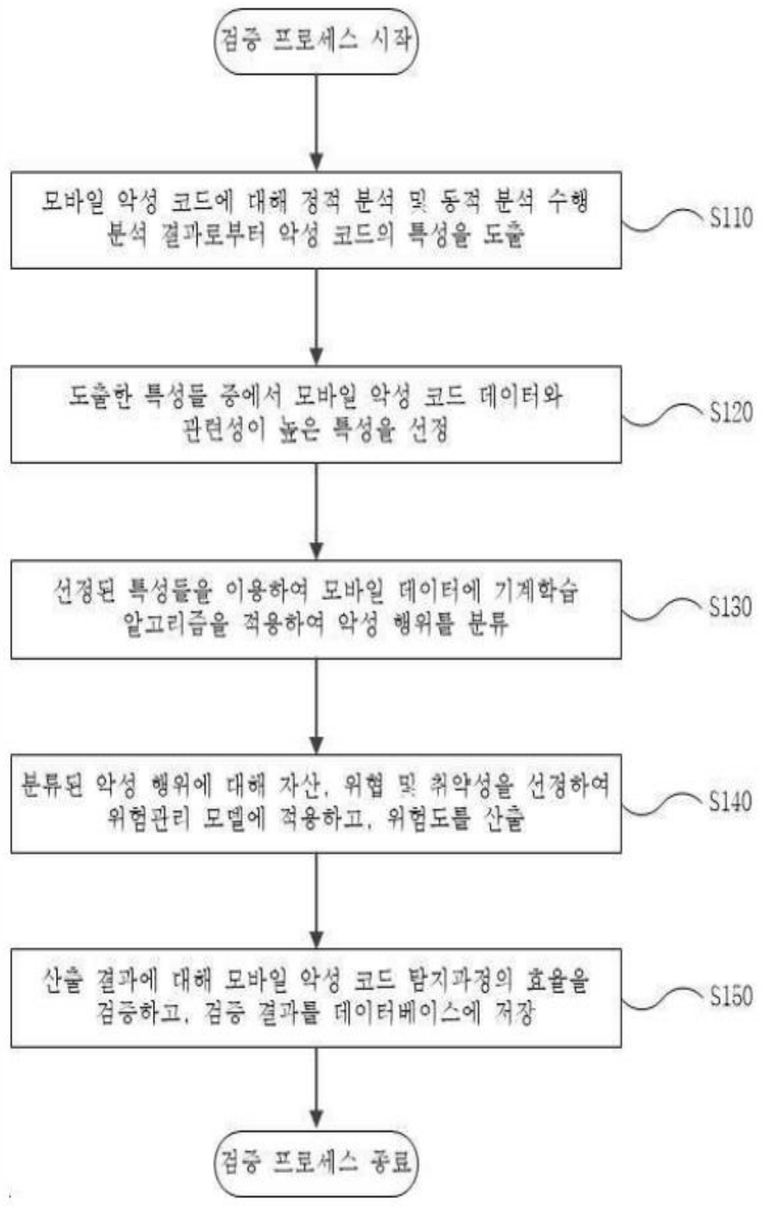
# 본 기술의 우수성 및 파급 효과

## 본 기술의 우수성(효과)

- 악성 행위의 유무 판단을 통한 잠재 악성 코드 탐지
  - 모바일 악성 코드 데이터 셋에 대해 정적 분석 및 가상 환경하에서 동적 분석을 수행하고, 분석 결과를 바탕으로 기존 모바일 악성 코드에서 도출된 침해 지표(IOC, Indicator Of Compromise) 등의 블랙 리스트를 기반으로 하여 모바일 악성 코드의 특성을 도출해 냄
  - 이후 도출된 모바일 악성 코드 데이터에서 기존의 모바일 악성 코드와 관련성이 높은 특성을 선정하고, 이 때 선정된 특성들을 활용하여 모바일 데이터에 기계학습 알고리즘을 적용하여 악성 행위를 분류함으로써 악성 행위의 유무를 판단할 수 없는 잠재된 악성 코드를 탐지할 수 있음

- 빠르고 정확한 악성 코드 탐지
  - 분류된 악성 행위에 대해 자산, 위협 및 취약성을 선정하여 위험관리 모델에 적용하고, 주 위험군과 부 위험군을 분류하여 위험도를 산출함
  - 산출 결과를 기초로 일련의 작업을 수행하는데 소모된 시간, 사용된 리소스, 탐지율 등을 고려하여 모바일 악성 코드 탐지과정의 효율을 검증하고, 데이터베이스에 저장함
  - 조합 가능한 모든 모바일 데이터 셋과 기준들에 대해 검증을 수행하며, 모든 검증 결과를 기초로 탐지율이 가장 높은 조합을 모바일 악성 코드 탐지 프로세스로 결정함으로써 빠르고 정확한 탐지를 가능하게 함

모바일 데이터 셋에 대한 검증 프로세스 수행 과정




## 적용 제품 및 파급 효과

- 악성 코드 탐지 시스템
- 본 기술은 모바일 악성 코드 탐지 효율이 높으면 알려지지 않은 새로운 모바일 악성 코드 공격에 대비할 수 있는 분류 시스템을 제공함으로써 모바일 환경에서 악성 코드로 인한 피해를 줄일 수 있음

## 지식재산권 현황

| 발명의 명칭 | 출원/등록번호 | 출원/등록일자 |
|---|---|---|
| 모바일 운영체제 환경에서 악성 코드 행위에 따른 위험을 관리하는 장치 및 방법, 이 방법을 수행하기 위한 기록 매체 | 10-2046262 | 2019.11.12. |
| **패밀리 특허 현황** | **패밀리 국가** | |
| US11019497 | US | |

문 의 | 고려대학교 산학협력단 기술사업화센터 권성진 02-3290-5832, giannie77@korea.ac.kr