46 모바일 엔드 포인트 행동 분석 기반 Policy Engine 구현

소속 정보컴퓨터공학부 분과 D 팀명 KGL 참여학생 권태현, 이승원, 구현서 지도교수 최윤호

과제 개요

과제 배경

- Zero Trust Network Access(ZTNA) 보안 패러다임 확산
- 모바일 디바이스의 행동학적 특성을 활용한 동적 보안 제어 필요
- 기존 NAC 시스템의 정적 인증 방식의 한계

과제 목표

- 다중 모달 데이터 (Touch, Sensor, Network) 실시간 수집
- 하이브리드 ML 모델을 통한 이상 행위 탐지
- 동적 네트워크 접근 및 사용자 피드백 시스템 구축

핵심 기술 및 구현

데이터 수집

- **Touch**: 드래그, 압력 패턴
- **Sensor**: 가속도계, 자이로스코프
- **Network**: GPS(위치), 접속 유형

이상 탐지 모델

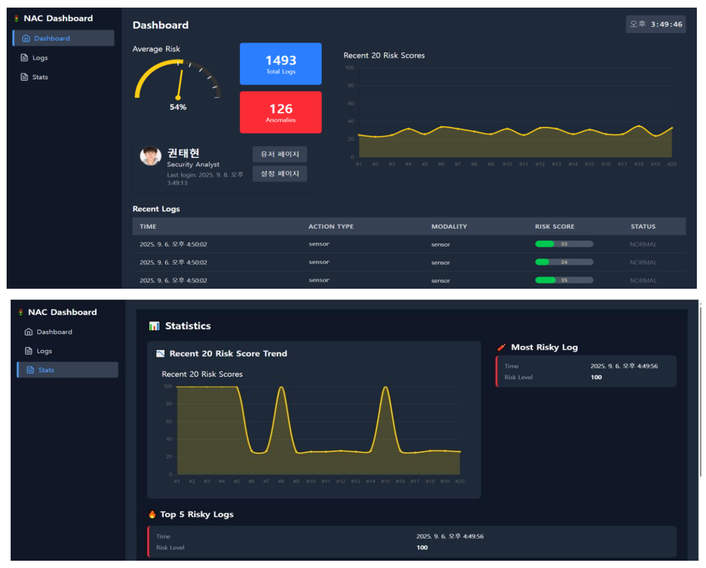
- **Isolation Forest**: 통계적 이상 탐지
- **LSTM AutoEncoder**: 시계열 패턴 분석
- **Hybrid Model**: 두 모델 융합

실시간 대응

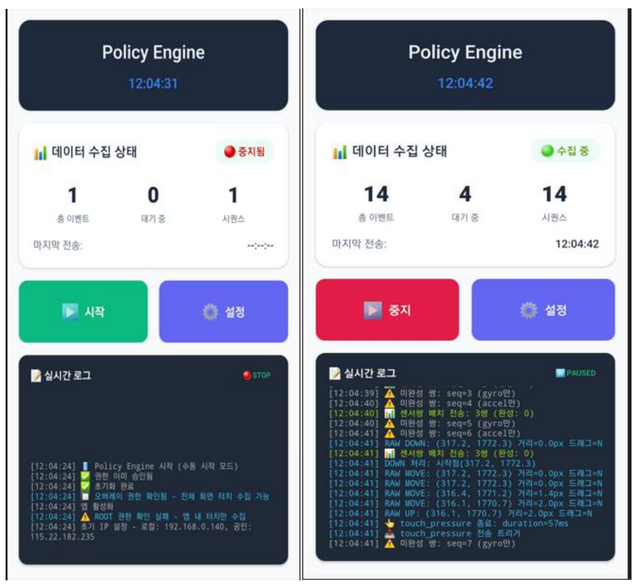
- **네트워크 차단**: 네트워크 연결 모드 전환
- **기기 잠금**: 자동 잠금화면 이동
- **관리자 알림**: 대시보드로 시각화

시스템 아키텍처

대시보드



안드로이드



결론 및 향후 연구 방향

주요 성과 및 성능 평가 결과

```
######################################################
     OVERALL PERFORMANCE SUMMARY (DETECT-STYLE)
######################################################
Model (Mode)          |  F1-Score |  Accuracy |  Precision |     Recall
------------------------------------------------------------------------
Sensor                |    0.9668 |    0.9649 |     0.9915 |     0.9432
Touch Drag            |    0.8748 |    0.8536 |     0.9053 |     0.8463
Touch Pressure        |    0.8468 |    0.8220 |     0.7584 |     0.9585
######################################################

🎯 Average F1-Score: 0.8961
🎯 Average Recall: 0.9160
```

```
======================================================================
요약 결과
======================================================================
| Modality       | Precision | Recall   | F1-Score   | Accuracy |
----------------------------------------------------------------------
| sensor         | 0.8676    | 0.8551   | 0.8613     | 0.9456   |
| touch_drag     | 0.8752    | 0.9484   | 0.9103     | 0.8376   |
| touch_pressure | 0.9182    | 0.8719   | 0.8944     | 0.8211   |
----------------------------------------------------------------------
평가 완료 시간: 2025-09-10 21:49:09
```

- 하이브리드 모델을 통한 안정적 이상 탐지
- 실시간 로그 수집 및 처리 시스템
- 직관적인 관리자 대시 보드 제공 구현

기술 스택

Android, Django, FastAPI, React, TypeScript, PyTorch, scikit-learn, PostgreSQL

향후 연구 방향

- GRU, Transformer 기반 모델 도입
- WebSocket을 활용한 실시간 푸시 알림
- 다중 플랫폼 확장 (IoT, 노트북)