

Security HW SW & AI Research Lab

I. 연구실 구성원

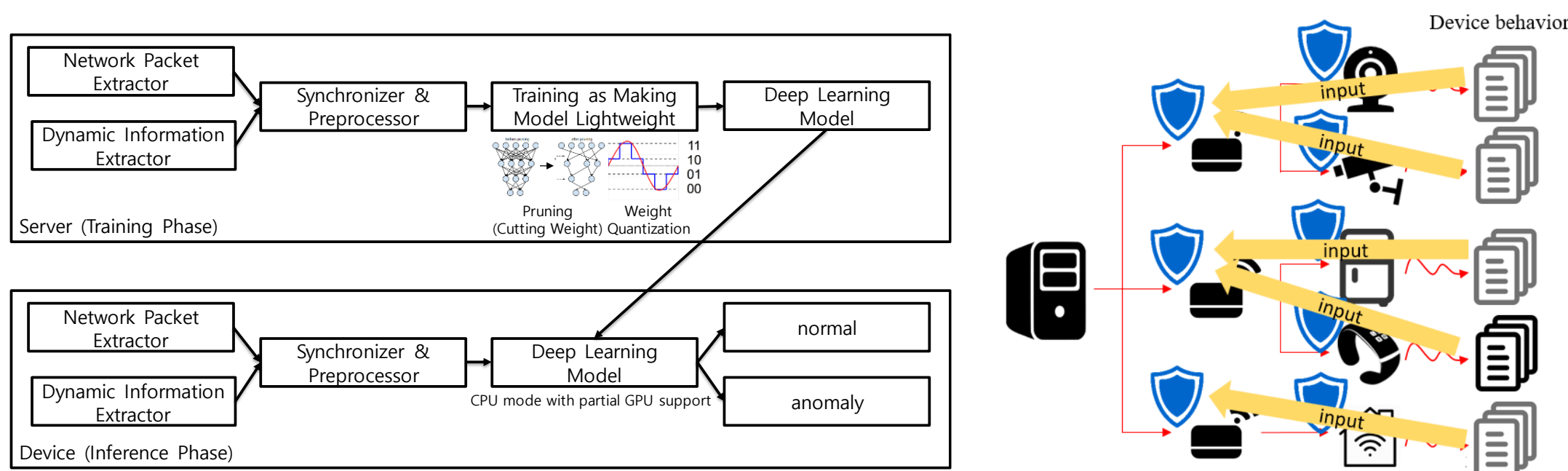
- 지도교수
 - 백윤홍 교수님
- 박사과정
 - 7명
- 석사과정
 - 8명

II. 연구 분야

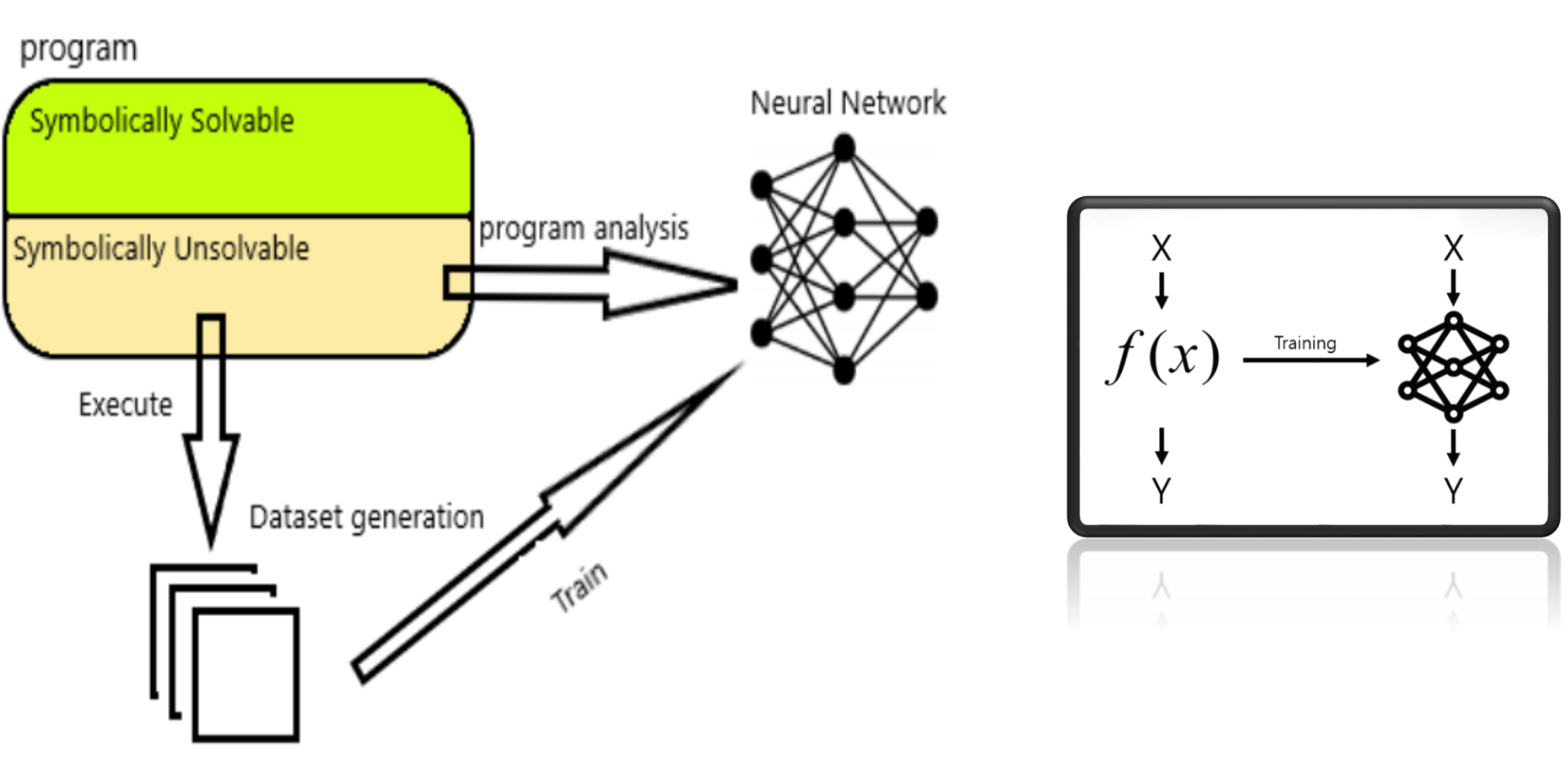
- AI 보안 및 보안 AI 연구
 - 사이버 공격 탐지를 위한 보안 AI 모델
 - AI 모델의 신뢰성 및 강건성(Robustness) 검증
- 보안 하드웨어 설계
 - 하드웨어에 기반한 보안 솔루션
- 보안 소프트웨어 기술
 - 시스템 소프트웨어/컴파일러를 통한 애플리케이션 보호

III. AI 보안 및 보안 AI 연구

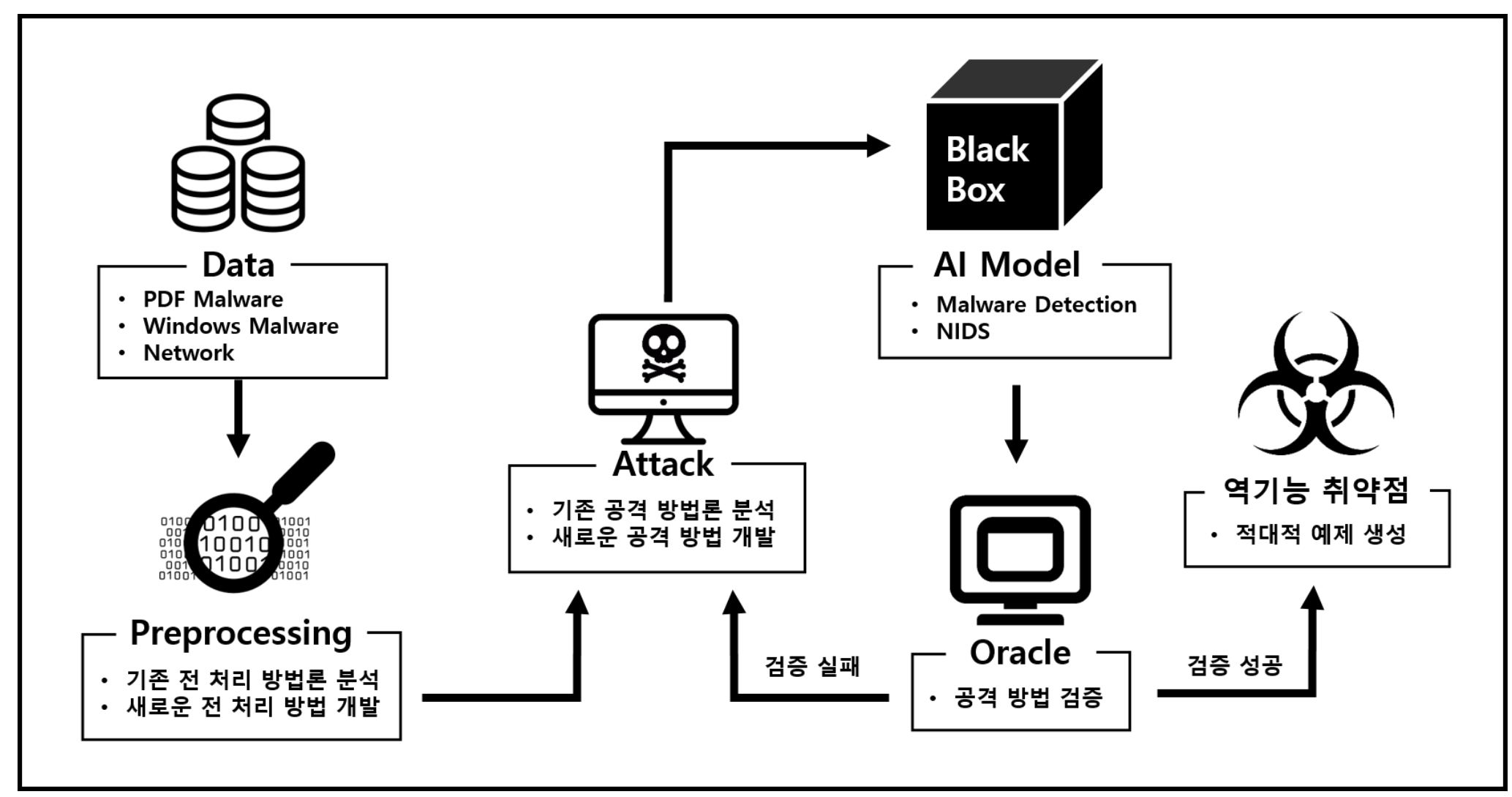
- 사이버 공격 탐지를 위한 보안 AI 모델
 - IoT 및 네트워크 상의 여러 기기를 대상으로 한 공격으로 인한 기기의 비정상 행위를 탐지하기 위한 기계학습 모델 개발



- 향상된 딥러닝 기반 기호 실행 연구

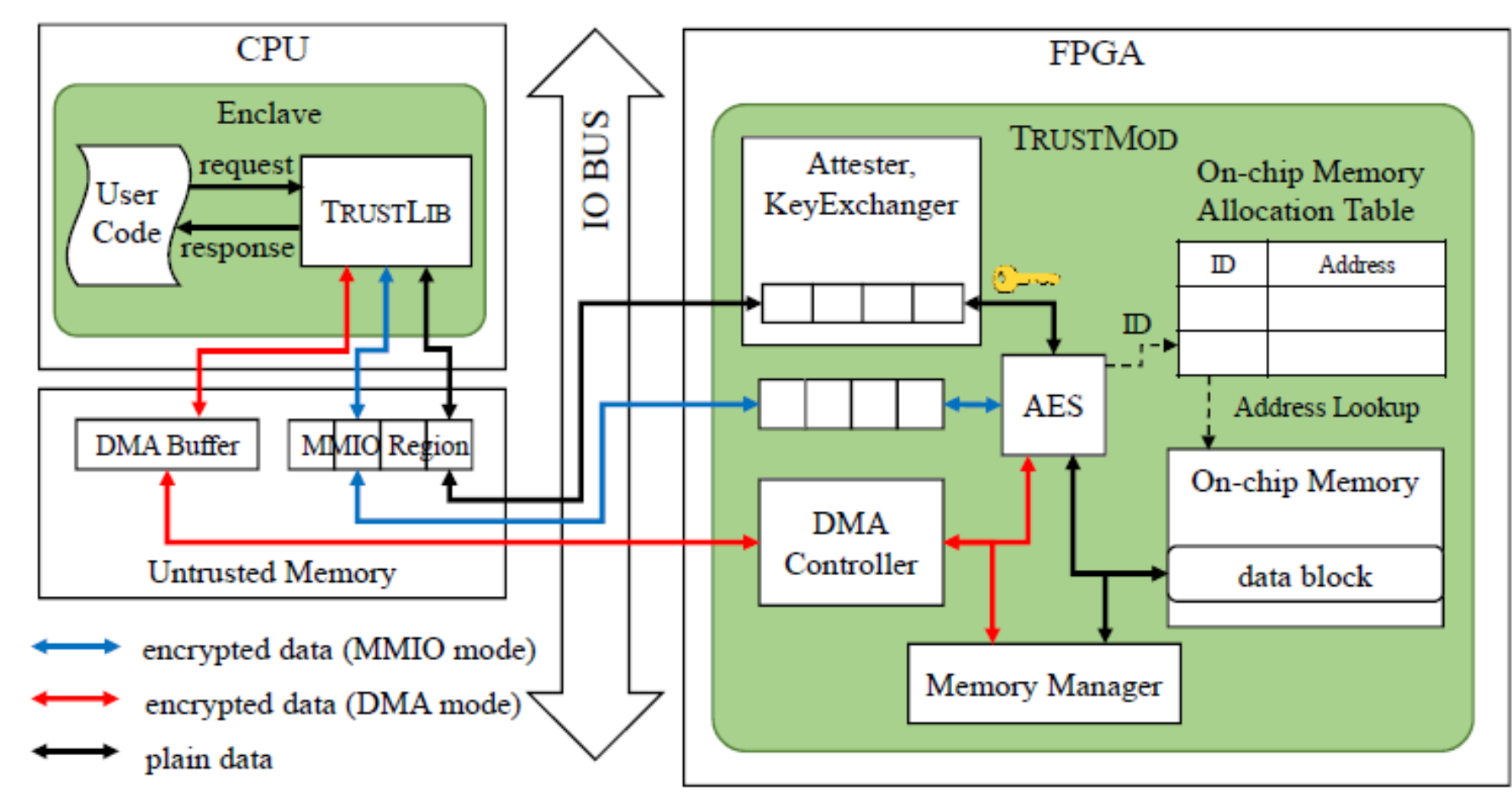


- AI 모델의 신뢰성 및 강건성(Robustness) 검증
 - AI 기반 탐지기를 회피하는 적대적 예제 생성을 통한 신뢰성 검증
 - 적대적 예제 학습을 통한 탐지기 강건성 강화



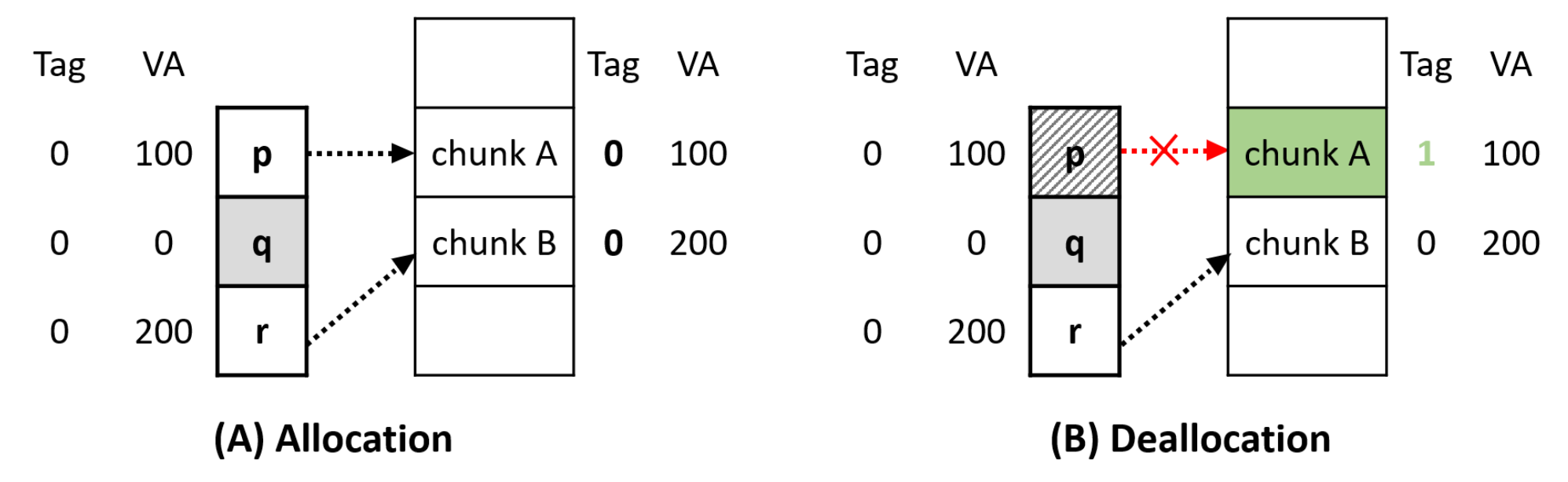
IV. 보안 하드웨어 설계

- 모바일 및 서버급 기기의 보안성 향상을 위한 보안 하드웨어 설계 및 구현
- **Side-Channel Resistant Storage** : 중요한 코드와 데이터의 액세스 패턴을 숨김으로써 안전한 저장장치 제공

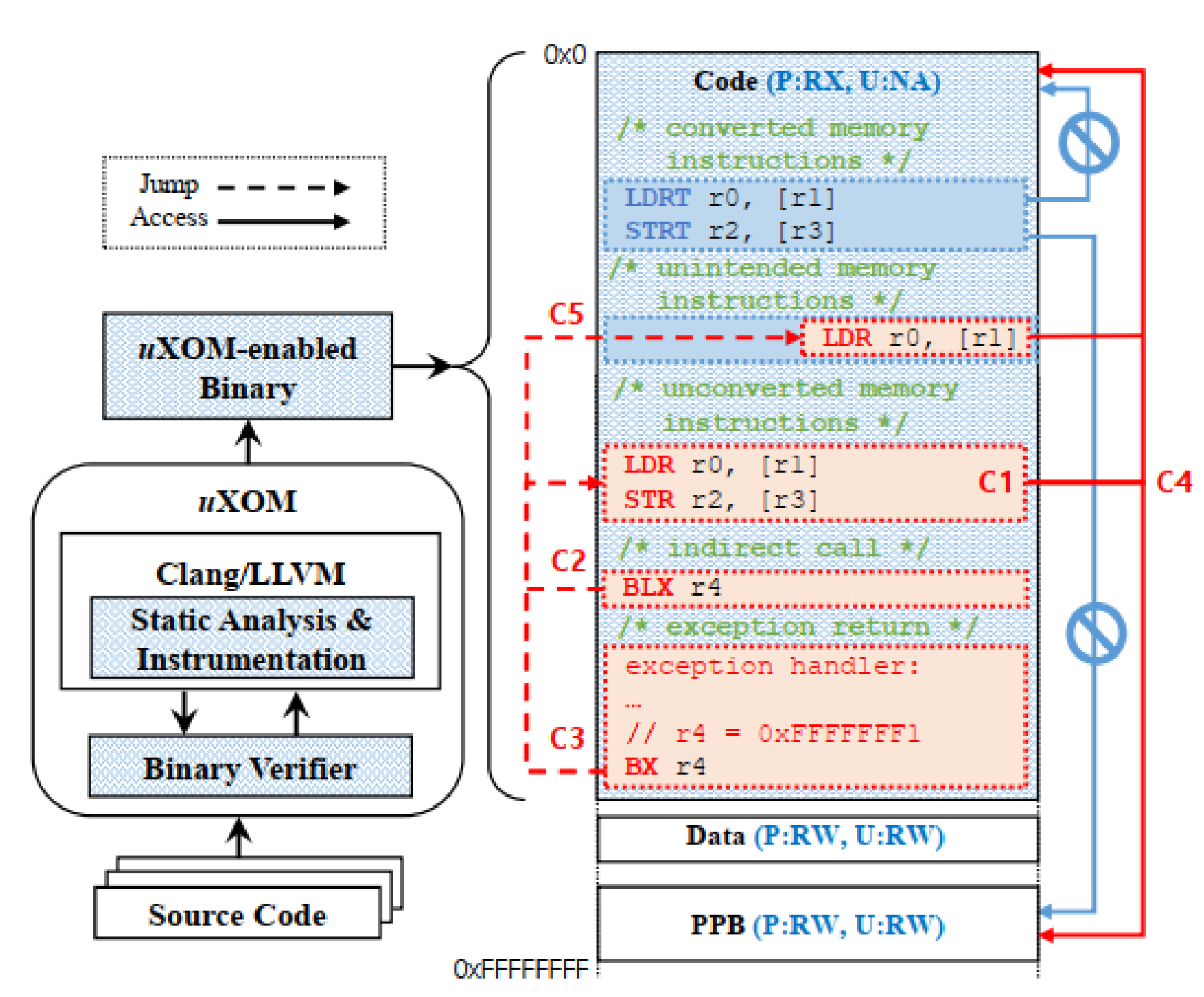


V. 보안 소프트웨어 기술

- Ensuring the **temporal safety** in C/C++ : 새로 제안된 아키텍처의 기능을 이용하여 programming language에 내재한 문제 해결



- **Compiler-based code instrumentation**을 이용하여 소프트웨어 취약점으로부터 애플리케이션을 보호



- Trusted/untrusted module 간 **isolation**을 제공하기 위해 **OS/Hypervisor** 디자인을 제시

