LamGuard: 서버리스 환경을 위한 LLM 기반 동적 검증 프레임워크

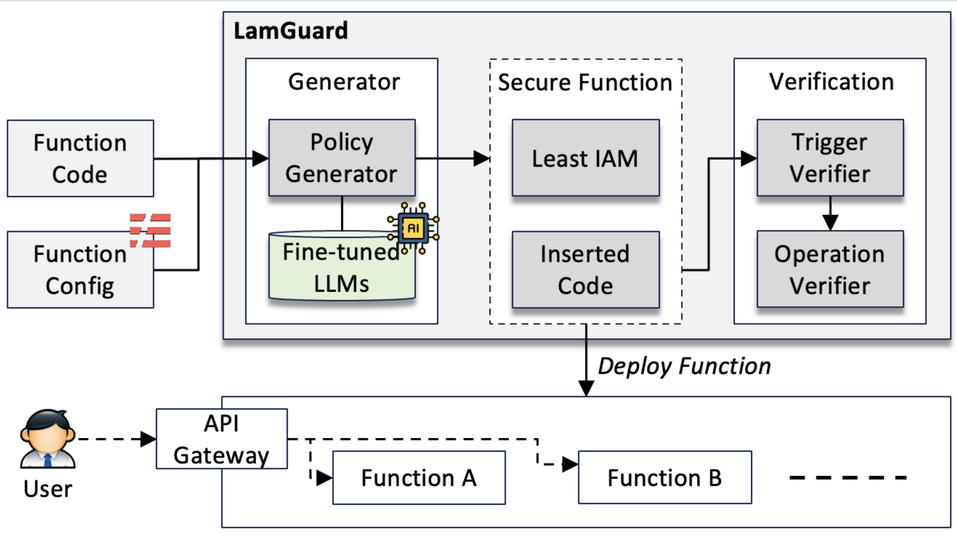
LamGuard: LLM-Based dynamic verification framework for serverless environments

Changhee Shin, Seungsoo Lee
Incheon National University

초 록

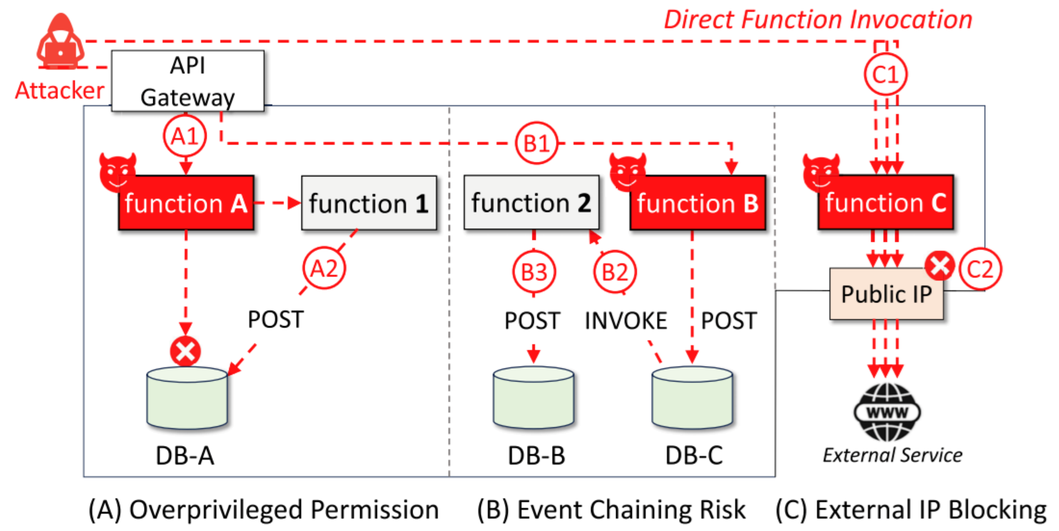
- 서버리스 환경에서는 보안 메커니즘으로 IAM(Identity and Access Management)을 사용.
- IAM의 부적절한 설정은 다른 리소스 접근, DoS(Denial of Service), DoW(Denial of Wallet) 공격으로 이어질 수 있음.
- 최소 권한 원칙을 기반으로 실시간 탐지 및 차단 기능을 제공하는 보안 메커니즘을 소개하며, 적절한 IAM 설정의 중요성을 강조.
- 실험을 통해 LamGuard가 Lambda 함수의 비즈니스 로직에 대해 최소 권한을 효과적으로 추출하고 보안 로직을 삽입하는 방식을 확인.

디자인



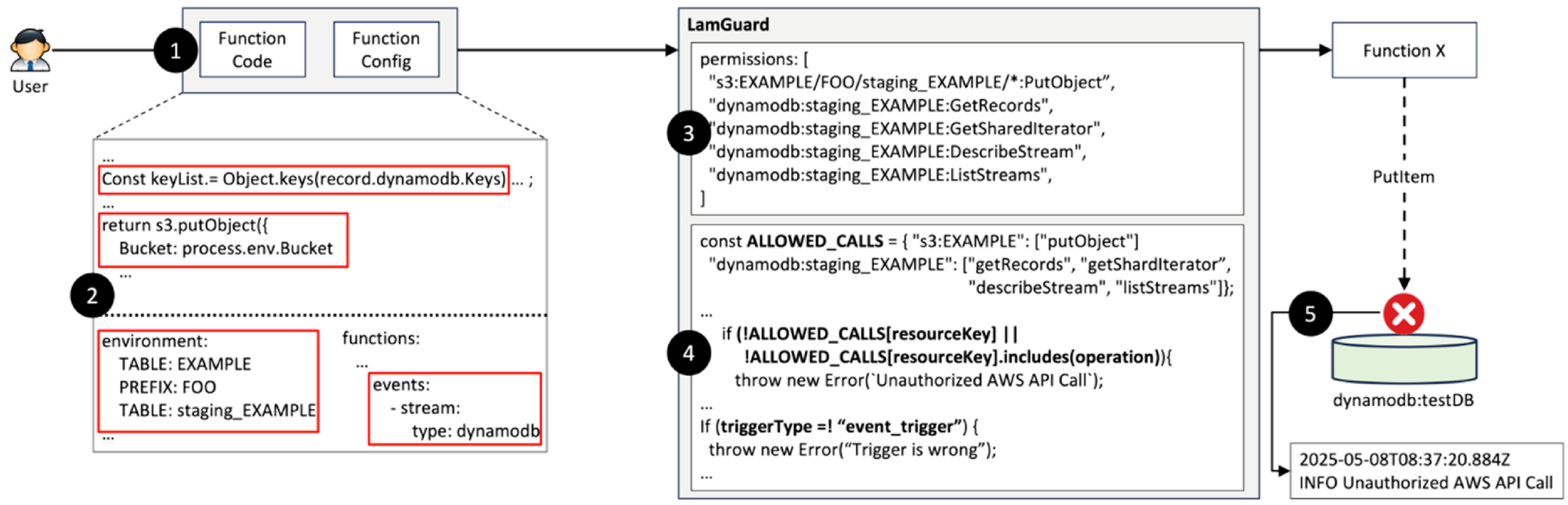
- 함수 코드와 설정(Config)을 입력으로 실행
- 입력을 분석하여 최소 권한 및 함수 트리거 추출
- 추출된 정보 기반 모니터링 및 트리거 검증 로직 생성 후, 자동 삽입

공격 시나리오



- 함수 로직 변경을 통한 리소스 우회 접근
- 함수의 이벤트 조건 악용으로 리소스 우회 접근
- 악성 파라미터 삽입을 통한 DoS공격

평 가



1. 사용자는 함수 코드와 설정을 입력으로 실행
2. LamGuard는 함수의 비즈니스 로직과 설정 코드를 분석
3. 비즈니스 로직에 맞춰 함수에 할당해야 하는 최소 권한 추출
4. 최소 권한 기반 모니터링 코드 및 트리거 검증 코드 자동 삽입
5. 배포된 함수는 실시간으로 함수의 동작을 모니터링하여 부적절한 동작을 차단

결 론

- 본 연구에서 제안하는 LamGuard는 함수 비즈니스 로직에 맞는 최소 권한을 추출하고, 실시간 모니터링 코드 삽입 및 실행이 성공적임을 확인했음.
- 향후 연구에서 LamGuard의 확장을 통해 더 많은 데이터셋을 수집하고, 다양한 벤더와 언어에 대한 확장성을 높이는 연구를 진행할 예정.