# Confiler: 컨테이너 환경을 위한 지능형 파일 접근 제어 프레임워크

Confiler: An Intelligent File Access Control Framework for Containerized Environments

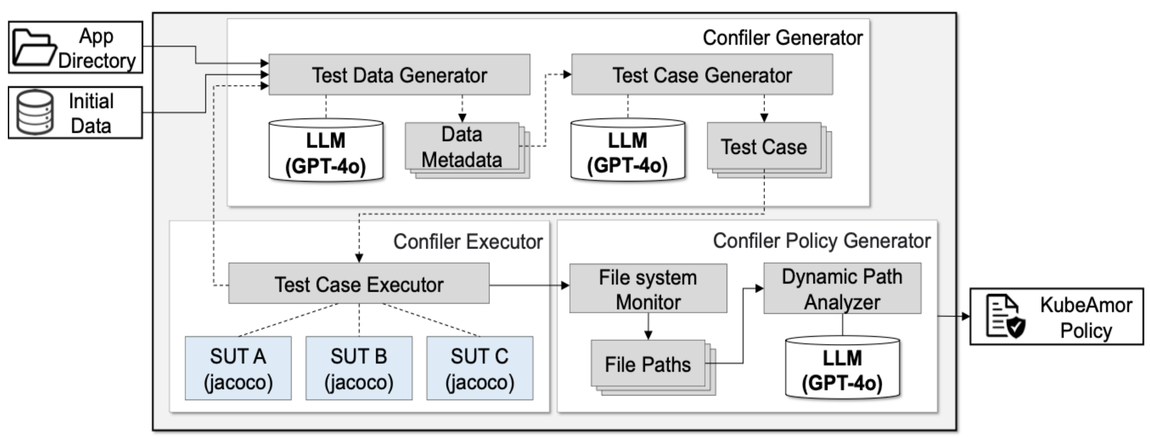
**Hyeonjun Park, Seungsoo Lee**
Incheon National University

## Abstract

● 컨테이너는 경량성과 빠른 실행을 바탕으로 광범위하게 사용되지만, 파일 시스템 접근 제어는 여전히 핵심 취약 지점으로 남아 있다.
● 기존 블랙리스트 정책과 화이트리스트 정책 생성을 위한 테스트 케이스 생성 기법은 Zero-day 공격과 낮은 커버리지 문제를 가진다.
● 동적 파일 경로를 반영하지 못하는 정책은 정상 동작을 방해하거나 공격 표면을 넓히는 위험을 초래한다.
● 본 논문은 **LLM 기반 테스트 케이스 생성을 자동화**하고 파일 접근 로그 분석을 통해 **동적 경로를 자동 식별**하는 Confiler를 제안한다.

## Challenge & Design

● C1) 블랙리스트 정책은 알려진 위협에는 대응할 수 있지만, 새로운 공격이나 **Zero-day 위협**에는 취약하다.
● C2) 화이트리스트 생성을 위해 **충분한 커버리지**가 필요하지만 기존 프레임워크는 SUT Driver 작성 등 **높은 수동 개입**이 필요하다.
● C3) 애플리케이션은 **런타임에 결정되는 파일 경로**를 동적으로 생성한다. 이를 정확히 반영하지 않으면 기능성이 저하된다.




● Confiler Generator
✓ Test Generator는 정적 분석으로 entry point를 식별한다.
✓ **파라미터 흐름을 추적**하여 사용되는 소스코드 파악한다.
✓ LLM을 활용하여 **다양한 분기 조건**을 포괄하는 입력 값과 테스트 케이스 생성한다.
● Confiler Excutor
✓ 생성된 테스트 케이스를 Test Case Executor가 컨테이너에서 실제로 실행한다.
✓ 오류가 발생하면 새로운 입력 데이터를 생성하여 재시도한다.
● Confiler Policy Generator
✓ 성공적으로 실행된 테스트 케이스는 모니터링을 통해 파일 접근 파악한다.
✓ LLM을 활용하여 **동적 경로를 파악**하고 KubeArmor 정책 생성한다.

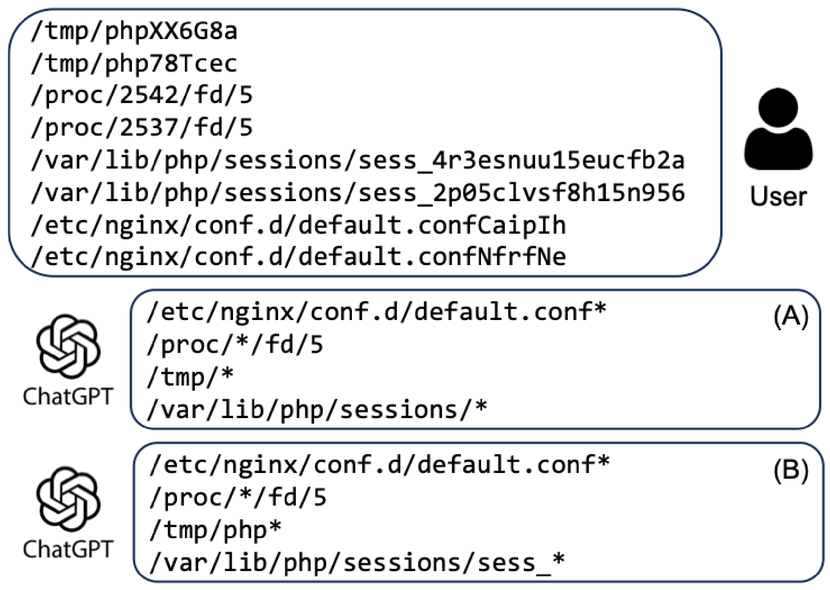
## Evaluation

● 테스트 케이스 커버리지 비교

| | core-banking | fund-transfer | user | utility-payment |
|---|---|---|---|---|
| Evomaster | 2/6 | 2/2 | 1/4 | 1/2 |
| Confiler | **6/6** | 2/2 | **3/4** | **2/2** |

✓ Application : Internet Banking Concept Microservice
▪ Evomaster는 core-banking-service에서 **6개 중 2개의 endpoint**를 커버한 반면, Confiler는 **모든 enpoint** 실행에 성공하였다.
▪ 이 결과는 Confiler의 LLM 기반 테스트 케이스 생성 방식이 더 많은 분기와 코드 경로를 포괄할 수 있음을 보여준다.

● 동적 경로 일반화 효과성




✓ Instruction-only model(A) vs. few-shot model(B)
▪ 모델(A)는 맥락을 이해하지 못해 디렉토리 전부를 **과도하게 일반화**하였다.
▪ 모델(B)는 **의미 있는 패턴을 파악**한 뒤 유지하고 일반화하였다.
▪ 이를 통해 few-shot 학습이 동적 경로 일반화의 성능을 향상시켰다.

## Conclusion

● Confiler는 LLM 기반 테스트 케이스 생성 자동화와 동적 경로 식별을 결합해 효과적인 화이트리스트 정책을 자동 생성한다.
● 평가 결과, 기존 도구 대비 **높은 커버리지를 확보**하며 제안 기법의 효과성을 입증하였다.
● 향후, spring boot framework 뿐만 아니라 gRPC 통신의 서비스 또한 테스트 케이스를 자동 생성하고 정책을 생성하는 연구를 진행할 예정이다.