08 초연결네트워크

클라우드 하드웨어 보안 모듈 기술

- **특허명 : Intel SGX 기반 클라우드 HSM 기술**
- **보유기관 : 국가보안기술연구소**
- **상태정보 : 출원예정**

특허원문보기

출원예정

기술개요

· 추가 장비 없이 일반 목적의 클라우드 노드 하드웨어 상에서 클라우드 HSM 기능을 구현
· 보안 솔루션, 암호화 장비, 인증보안 등

기존 문제점

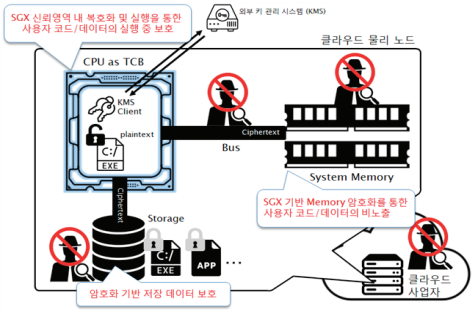
· 클라우드 서비스 제공자(CSP)가 별도의 장비 필요
· 사업자에게 정보 노출
· 하이퍼바이저 또는 OS와 같은 특정 플랫폼 의존

기술 차별점

· 클라우드 사업자 의존 최소화
· 사업자에게 정보를 노출하지 않고 실행 보호 및 데이터 보호 가능
· 실행 중 데이터 탈취 시도 감쇄
· 특정 플랫폼에 의존적이지 않으며, SGX를 지원하는 CPU를 사용하는 Bare Metal 환경에서도 동일 기능 사용

세부내용

· 사용자 코드/데이터의 안전한 암/복호화 및 키 보호를 통한 클라우드 Guest 저장장치 계층에서의 사용자 정보 기밀성 및 무결성 제공
· 클라우드 서비스 제공자(CSP) 및 관리자에게 노출되지 않는 사용자 코드/데이터의 비노출 신뢰실행 기술
· 암호화 및 코드실행보호 등 기밀성 및 무결성이 필요한 프로그램 실행 및 데이터 사용 환경에 적용 가능



기술이전 문의
· 국가보안기술연구소 주익수(042-870-4965, tech@nsr.re.kr)
· 공동마케팅사무국 이가영(042-862-6985, gylee@wips.co.kr)