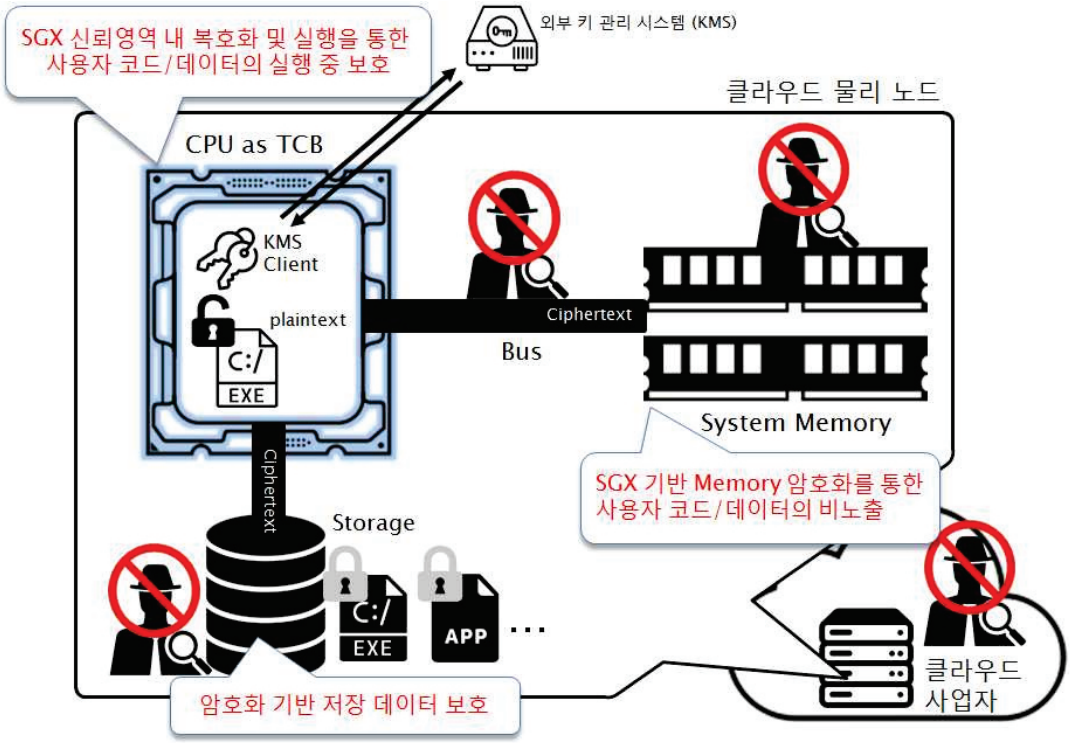
Intel SGX 기반 클라우드 HSM 기술

기술키워드	클라우드 HSM, SGX,								
지식재산권	출원 1건 예정(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	**기능 및 개념검증**	연구실환경 테스트	시제품 제작	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- 추가 장비 없이 일반 목적의 클라우드 노드 하드웨어 상에서 클라우드 HSM 기능을 구현
  - 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

- 기술 개념도



기술성

- 기존의 클라우드 HSM 솔루션들은 클라우드 서비스 제공자(CSP)가 별도의 장비를 갖추고, 서비스를 생성하여 사용자들에게 제공하나 본 기술은 클라우드 사업자 의존을 최소화하여, 사업자에게 정보를 노출하지 않고 실행 보호 및 데이터 보호 가능

- Intel SGX 기술을 기반으로 실행 시 사용되는 데이터를 메모리 상에서 보호하며, 암호화 및 SGX Enclave 내 복호화 및 실행 로직을 기반으로 사용 코드 및 정적 데이터를 보호하여 사용자 응용프로그램 또는 Library의 역공학에 의한 실행 전 분석 방지, 실행 중 데이터 탈취 시도를 감쇄하는 기능을 제공
- 클라우드 호스트의 서비스 구축 환경(VM, Container, Bare metal...) 유형에 따라 응용프로그램 수준에서 서비스 구축도 가능. Microsoft Azure Confidential Computing에서 SGX를 guest에서 사용할 수 있도록 제공하며 Docker 기반 Container는 SGX 사용 가능 (IBM DataShield, Google Asylo 등)

시장성

- HSM (Hardware Security Module) 시장 동향
  - 2016년도 20억 달러 가량의 수익(Revenue) 규모는 2026까지 평균 11.5%의 연성장률(CAGR)을 보이면서 약 59.3억 달러까지 성장할 것으로 예측되고 있으며 중소 규모 기업의 HSM 사용자 대부분이 클라우드 기반 HSM으로의 이동을 적극 고려하고 있는 것으로 보고됨
    (※참고자료: "Hardware Security Module (HSM) Market – Industry Analysis, Size, Share, Growth, Trends and Forecast 2018-2026" Transparency Market Research, May 2018)
  - HP, Utimaco GmbH, Futurex, Thales e-Security, IBM, Ultra Electronics Group, Gemalto NV, SWIFT, Yubico 등의 글로벌 업체가 진출해있음
- 클라우드 환경에서의 HSM
  - 아마존, 마이크로소프트 등의 클라우드 사업자들은 자사의 클라우드 환경에서 사용할 수 있는 HSM 장비들을 도입하여 이미 서비스하고 있음 (AWS Cloud HSM, MS Azure Key Vault 등)
- 본 기술은 클라우드 환경에서 실행되는 응용프로그램 또는 library의 실행 보호를 위한 기술이나 하이퍼바이저 또는 OS와 같이 특정 플랫폼에 크게 의존적이지 않으며 SGX를 지원하는 CPU를 사용하는 Bare Metal 환경에서도 동일한 기능을 사용할 수 있어 가상화 환경, 컨테이너 환경 및 일반 네이티브 컴퓨팅 환경 등에서도 응용프로그램 또는 데이터 보호 등의 목적에 폭넓게 적용할 수 있을 것으로 판단됨

기술 응용 분야

- 암호화 및 코드실행보호 등 기밀성 및 무결성이 필요한 프로그램 실행 및 데이터 사용 환경에 적용 가능
- Authentication, Database Encryption, Document Signing, SSL, Code Signing, PKI/Credential Management, Payments Processing, Application Level Encryption 등의 분야에 활용 가능

기술개발 완료시기

- 2019년 12월 완료 예정

관련 특허 등 지식재산권

- (국내 출원 예정) "(가칭) 상용 CPU를 이용한 클라우드 HSM 기술 및 시스템"