서울대학교
SEOUL NATIONAL UNIVERSITY

Data

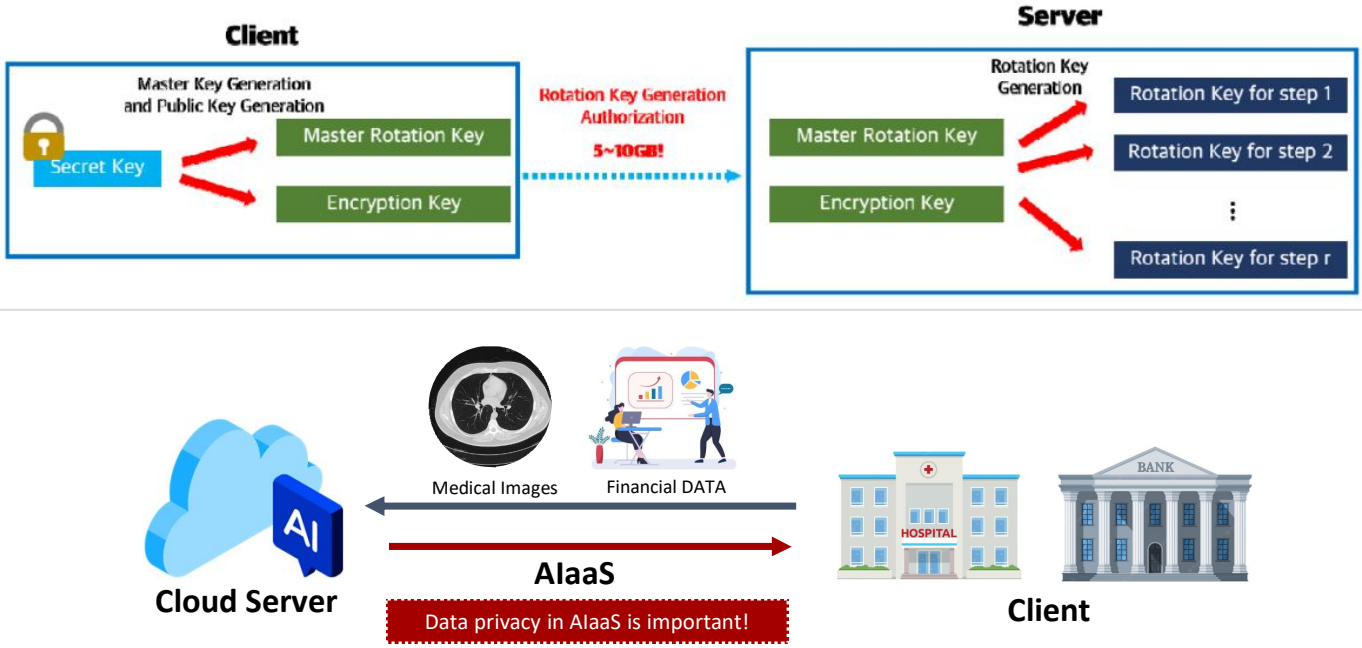
연산량 균형을 이룰 수 있는 동형 회전키 위임 및 관리 기술

서울대학교 공과대학 노종선 교수

기술내용

- 병원의 의료 메디컬 이미지 분석, 금융권 프라이빗 데이터 등 빅데이터 처리에 있어 동형연산이 필요하며, 이는 방대한 연상량과 통신량이 필요함
- 본 기술은, 동형암호를 사용할 때 서버에게 회전 연산키를 생성하는 과정을 위임함으로써 클라이언트의 연산량과 통신량을 줄여줄 수 있음
- 클라이언트가 모든 회전키를 생성하는 것이 아니라 회전키를 생성하는 권한을 위임하는 방법에 대한 기술임

주요도면 및 사진



기술 개발 배경

- 동형연산에는 사용자별로 수GB에서 수백GB까지의 공개키가 필요함
- 해당 키를 생성하고, 저장하고, 연산을 위탁할 서버로 전달하는 모든 일이 큰 문제임
- 특히 스마트폰 등 휴대용 장치에서는 Key Size가 1GB만 하더라도 저장 및 서버로의 전달이 상대적으로 더 큰 비용임
- AI 연산을 대행하는 서버가 하나 이상인 경우, 각 사용자별로 연산에 필요한 키들을 서버 별로 각각 저장하고 있어야 함

특장점(효과)

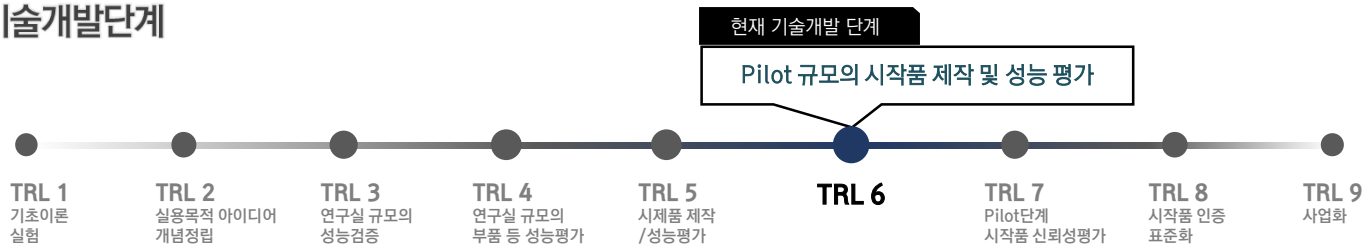
- 회전키를 생성할 수 있는 비교적 적은 종류의 마스터 회전키를 클라이언트가 생성해서 서버에게 보내주면, 이를 사용하여 비밀키에 접근하지 않고도 필요한 이동 정도의 연산키를 생성할 수 있게 됨
- 클라이언트가 소모하는 연산량과 통신량은 마스터 회전키를 생성하고 송신하는 정도만 필요하게 되고, 이후의 연산키를 생성하는데 필요한 연산은 고성능 서버가 담당하게 되어 연산량 균형이 잘 이루어지게 됨
- 또한 서버가 연산키를 스스로 생성하게 됨으로 연산키를 삭제하고 다시 생성하는 일이 가능해져 연산키 메모리 관리가 더욱 수월해지게 됨

기술활용분야

- 클라우드 컴퓨팅, 정보보호 머신러닝, 네트워크 보안, 기타 동형암호 응용 분야 및 인증서비스 등의 암호/보안 기술 분야

응용분야 및 적용제품	관련 업체
• 응용 분야 – 클라우드 서비스 서버 보안 – 네트워크 보안 활용 금융 서비스 플랫폼 서버 보안 – 사물인터넷 서버 보안 • 적용제품 – 클라우드 플랫폼 서비스, 금융 서비스 플랫폼 등 정보 보안이 필요한 서비스 플랫폼 제품	• 서버 보안 전문 기업 • 서버 보안 활용 기업 – Genome analysis – Cancer/tumor detection – Financial analysis – Semiconductor yield analysis – Forensic image recognition – Personalized advertising

기술개발단계



지식재산권 현황

No.	기술명	출원번호	등록번호	국가
1	동형 회전키 생성 권한을 마스터 회전키를 통해 서버에게 위임하는 방법	10-2022-0017596	-	KR
2	동형암호 연산을 위한 키 관리 서버 시스템	10-2022-0017597	-	KR

기술이전 상담 및 문의 : 서울대학교 산학협력단 신양일 변리사 youmei21@snu.ac.kr 02-880-2026