2021년 IT21
Global Conference
Human in SW, SW in Human
Session 3-6

신뢰 기밀 컴퓨팅 개요(Introduction to Confidential Computing)

강병훈 교수 (KAIST)

신뢰 실행 환경은 많은 보안 공격에 노출되며 취약 할 수 있는 일반 실행 영역으로 부터 주요 코드와 데이타를 안전하게 분리하여 기밀성과 무결성을 보장하면서 수행하는 프로세서 하드웨어 기반의 방어 기술 입니다. 최근 들어서 이러한 신뢰 실행 환경을 Confidential Computing (신뢰 기밀 컴퓨팅) 이라고도 명명 하고 있으며, 클라우드 서버 등에서 개인 정보 보호 요구 등으로 인해 기밀성 이 보장 되어야 하는 데이타와 관련 주요 코드 등에 적용을 할 수 있는 관련 기술 개발이 많이 이루어 지고 있습니다. 본 강연에서는 이러한 신뢰 기밀 컴퓨팅에 대한 개요를 소개 하고 관련 응용 기술 분야들을 살펴 보고자 합니다.

약 력

버클리 대학(University of California at Berkeley)에서 컴퓨터과학(CS) 전공으로 박사학위를 받고, 현재 카이스트 전산학부 교수로 재직중이며, 카이스트 정보보호대학원 책임교수를 역임하였고 사이버 시스템 보안 연구실 CysecLab (Cyber Systems Security Lab, https://cysec.kaist.ac.kr) 지도교수이다.

CysecLab은 보안에 취약할 수 밖에 없는 기존의 컴퓨팅 시스템들이 현재와 미래의 사이버 위협에도 보안성과 안정성을 확보 할 수 있게 하는 시스템 설계 및 방어기술 연구를 목표로 하고 있다. 최근 AI시대의 컴퓨팅 시스템에 대한 보안 위협을 독립된 신뢰 실행 환경의 혁신으로써 방어하는 연구를 주로 수행하고 있다.

주 연구 분야는 Confidential Computing 과 Trusted Execution Environment 설계 및 이를 이용한 안전한 시스템 방어 기술 설계이다. (예, OS 커널 무결성 모니터, 하드웨어 기반 신뢰 실행 환경, 메모리 주소 변환 무결성, 코드 재사용 공격 방어, 고스트 은닉 서버, Dialect Computing). 일부 연구결과는 카이스트 혁신연구(http://breakthroughs.kaist.ac.kr/?post_no=163) 에 소개되었다. 정보보호 고급인재양성을 위한 연구와 교육의 기여로 과학기술정보통신부 정보보호 분야 유공 훈장 장관 표창을 받기도 하였다.

국제 활동으로 정보보호 분야 최상위 학회들인 IEEE Security and Privacy, ACM CCS, USENIX SECURITY, NDSS 에서 Program Committee 직책을 맡고 있고, 최근 CMU CyLab Distinguished Seminar 초청강연도 수행하였다.

신뢰/기밀 컴퓨팅 개요

CySecLab
(Cyber Systems Security Research Lab)

강병훈
Brent ByungHoon Kang, Ph.D.,

May 27, 2021

KAIST CySecLab

Intro. to Confidential Computing based on TEE

CySecLab
(Cyber Systems Security Research Lab)

강병훈
Brent ByungHoon Kang, Ph.D.,

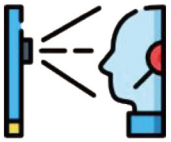
May 27, 2021

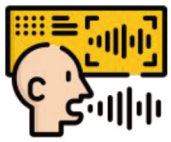
KAIST CySecLab

인공지능 기반 응용 서비스의 기초 요소들

인식

이미지, 얼굴, 언어, 음성





판단/연관/유추

의료 진단, 악성코드공격 판별, 상품 제안

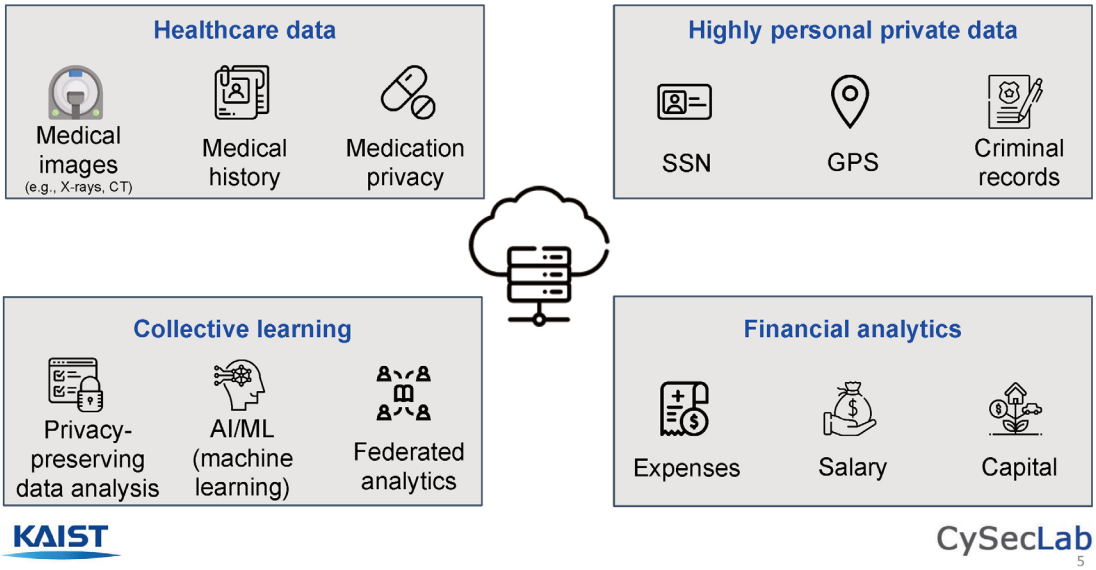
예측

범죄방어, 금융시장, 의료 예측

KAIST

CySecLab

개인정보 데이터에 기반한 인공지능 서비스



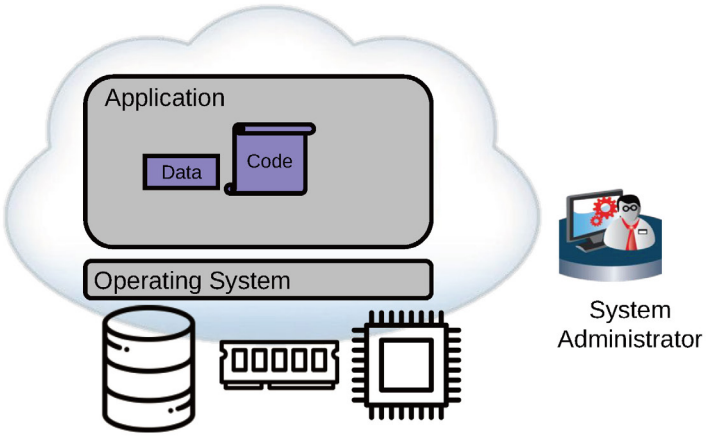
KAIST

CySecLab

인공지능 기반 어플리케이션 및 서비스 시스템

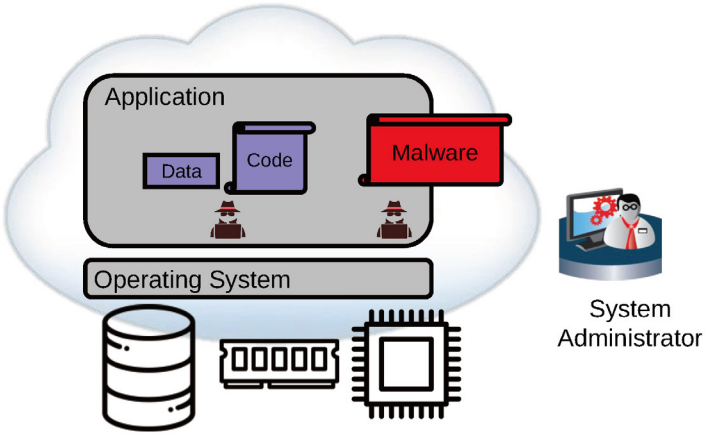
KAIST CySecLab 6

Applications and Platform Systems



KAIST CySecLab 7

Vulnerable Applications and Malwares

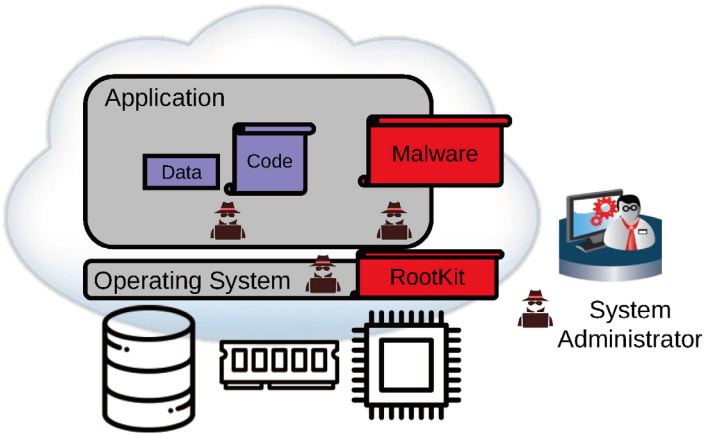


KAIST

CySecLab

8

Vulnerable Applications, Systems and Malwares



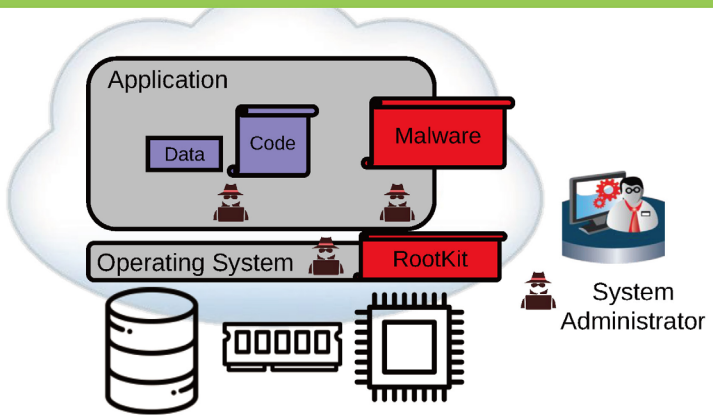
KAIST

CySecLab

9

Vulnerable Applications, Systems and Malwares

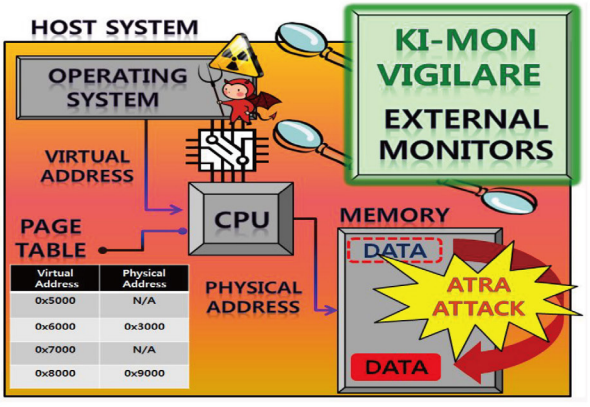
<<궁극의 질문 1.>>
악성코드 없는 세상이 가능할까 ?



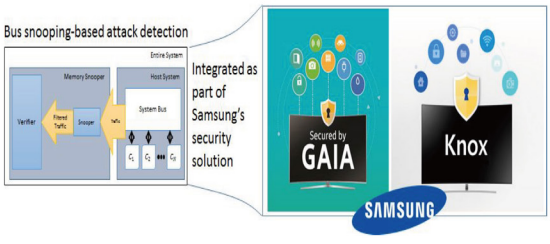
KAIST

CySecLab
10

Platform System Integrity Monitor



- 연구 결과 적용 사례
  - 삼성 스마트 TV 보안 시스템(GAIA)에 연구 결과 적용 및 탑재
  - 삼성 사업부 소프트웨어 보안 솔루션에 Anti-Emulation 탐지 방어기능(2018년), 힙 취약점 공격 방어기술(2017년)



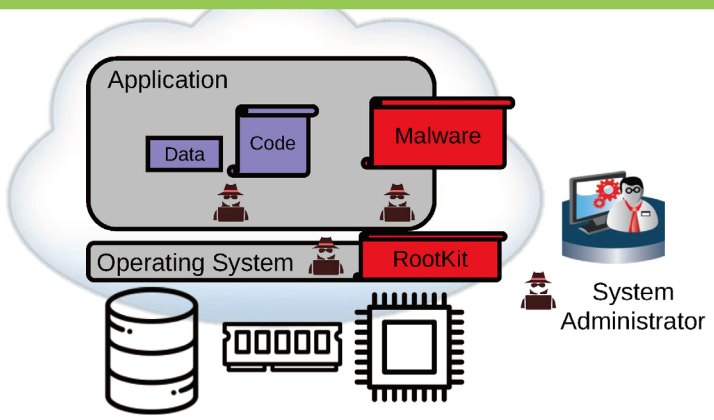
http://breakthroughs.kaist.ac.kr/?post_no=163

KAIST

CySecLab
11

Vulnerable Applications, Systems and Malwares

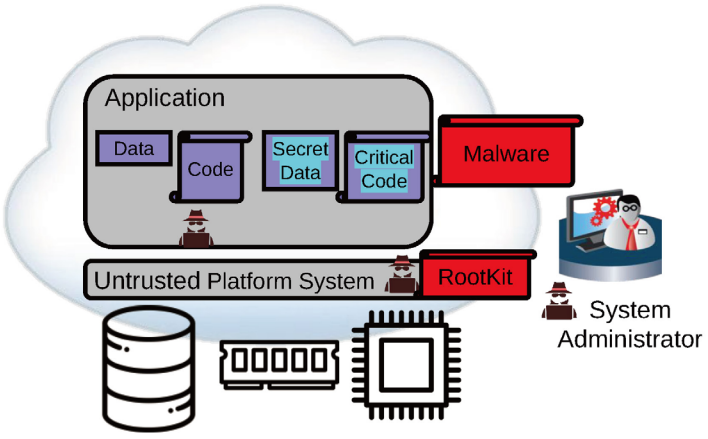
<<궁극의 질문 2.>>
악성코드가 있어도 상관없이 안전한 컴퓨팅 세상이 가능할까 ?



KAIST

CySecLab
12

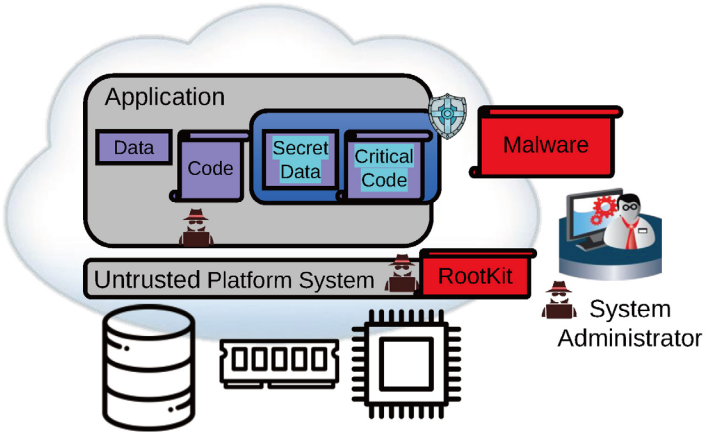
Secure Isolation of Application



KAIST

CySecLab
13

Secure Isolation of Application

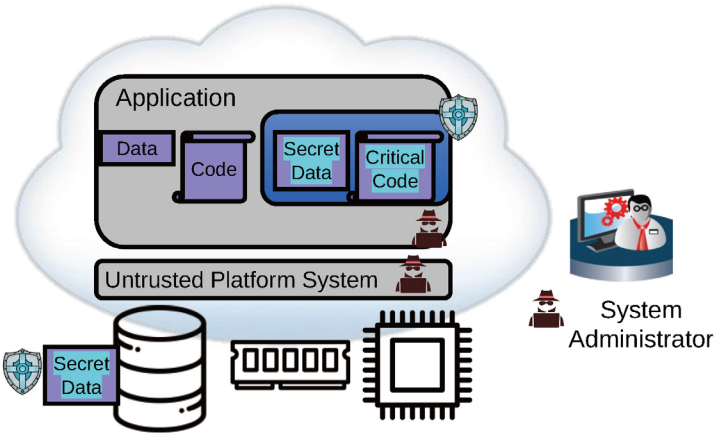


KAIST

CySecLab

14

Data-at-Rest Protection

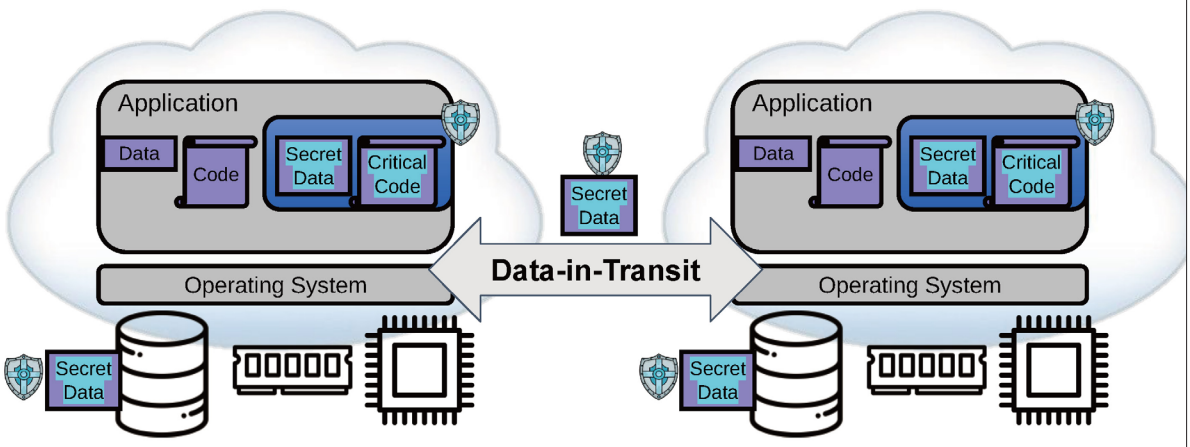


KAIST

CySecLab

15

Data-in-Transit Protection

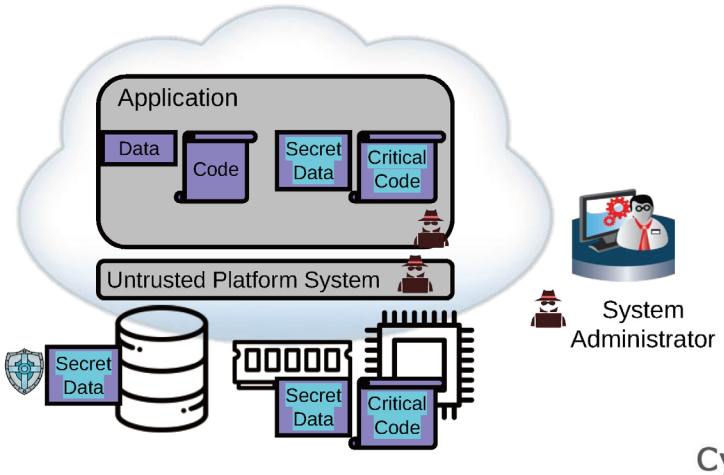


KAIST

CySecLab

16

Data-in-Use Protection

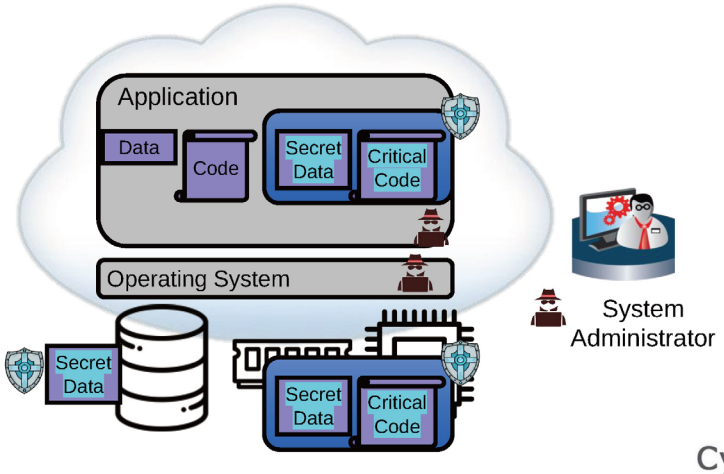


KAIST

CySecLab

17

Data-in-Use Protection: Confidential Computing



KAIST

CySecLab
18

Trusted Confidential Computing (신뢰 기밀 컴퓨팅)

KAIST

CySecLab
19

TEE (Trusted Execution Environment) 하드웨어 아키텍처

❖ **External hardware security module**

- Example: TPM, SIM card or a Smart card
- Advantages
  - ✔ High level of tamper resistance and physical security
- Disadvantages
  - ✔ Power efficiency and performance of the device
  - ✔ Reliant to the less secure software outside of the smartcard
  - ✔ Providing a smart card alongside with the main SoC is expensive

KAIST CySecLab

TEE 하드웨어 아키텍처

❖ **internal hardware security module**

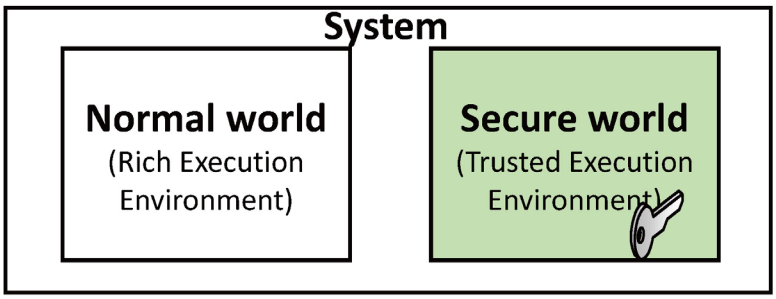
- Example
  - ✔ A hardware block for cryptographic operation and key storage
  - ✔ General-purpose processor dedicated to the security sub-system
- Advantages
  - ✔ Cost reduction (compared to the external)
  - ✔ Performance improvement
- Disadvantages
  - ✔ Restricted perimeter (e.g. only for cryptography)
  - ✔ Less powerful than main processor
  - ✔ Time & energy consuming for inter-processor communication
  - ✔ Complex SoC design

KAIST CySecLab

TEE 하드웨어 아키텍처

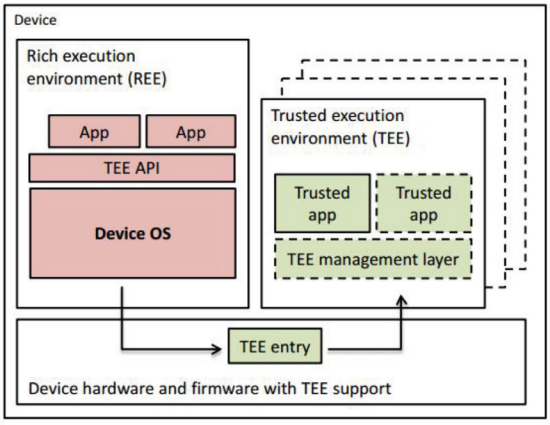
❖ **Processor secure environment**

- ARM TrustZone and Intel SGX
- Countermeasure for
  - Virus and malwares
  - Low-budget hardware attack (e.g. Using a JTAG debugger)



KAIST CySecLab

TEE System Architecture



Architectures with single TEE

- ARM TrustZone
- TI M-Shield
- Smart card
- Crypto co-processor
- TPM

Architectures with multiple TEEs

- Intel SGX
- TPM (and "Late Launch")
- Hypervisor

23

Figure adapted from: Trusted Execution Environments on Mobile Devices. ACM CCS 2013 tutorial.

KAIST CySecLab

TEE Hardware Realizations

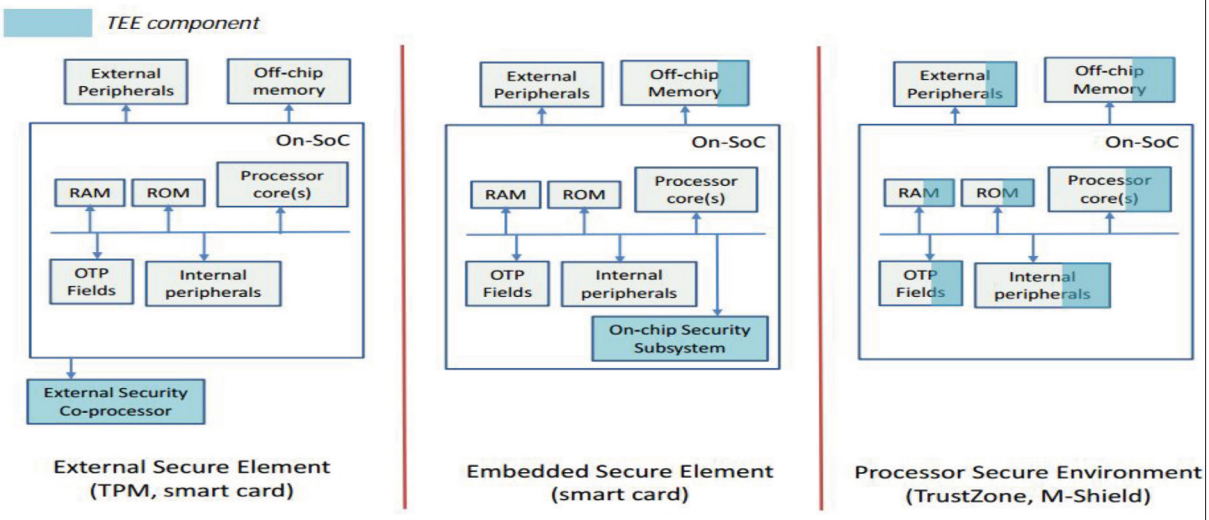
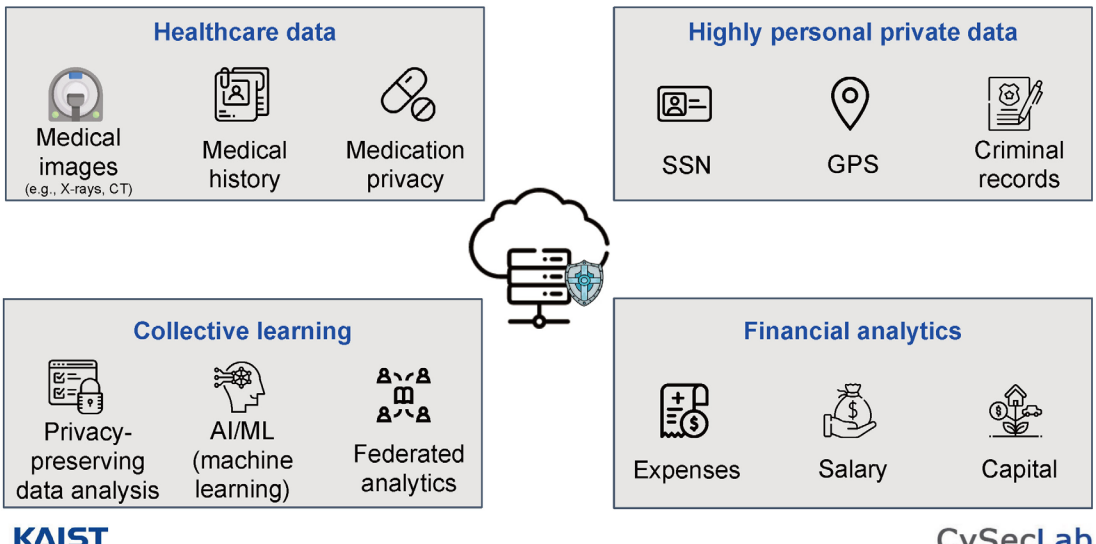


Figure adapted from: Trusted Execution Environments on Mobile Devices. ACM CCS 2013 tutorial.

KAIST CySecLab

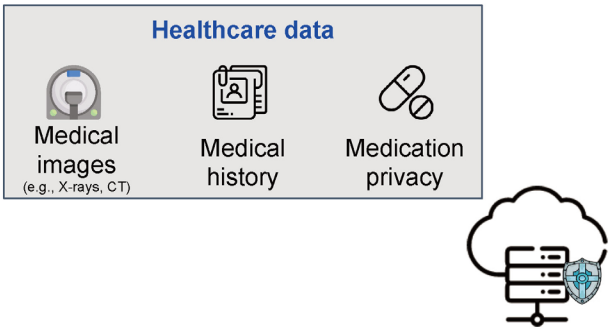
Confidential Computing: AI Analytics on Private Data



KAIST CySecLab

25

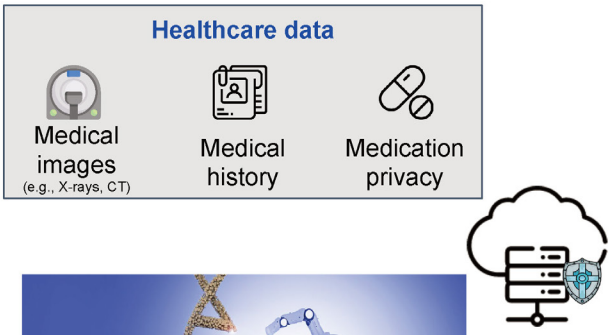
Confidential Computing: AI Analytics on Private Data

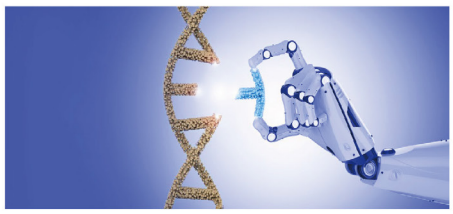


KAIST

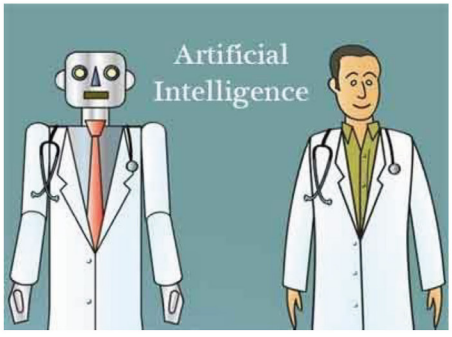
CySecLab
26

Privacy Issue in AI with Medical Data Processing





Gene editing backed by AI

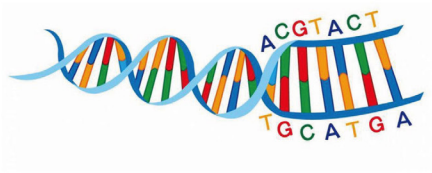


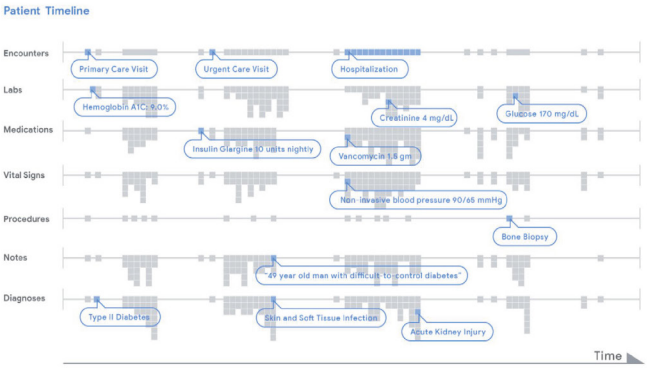
AI Doctor

KAIST

CySecLab
27

AI needs lots of Private Data for Machine Learning



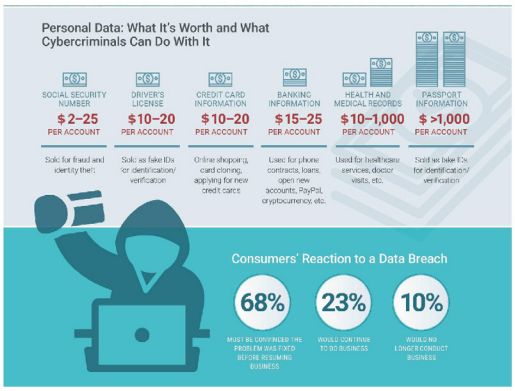


Medical Information & DNA Genome

KAIST

CySecLab

Privacy Protection of Medical Data is Critical



655,000 Healthcare Records Being Sold on Dark Web

(출처: https://threatpost.com/655000-healthcare-records-being-sold-on-dark-web/118933/)

KAIST

CySecLab

Confidential Computing: AI Analytics on Private Data

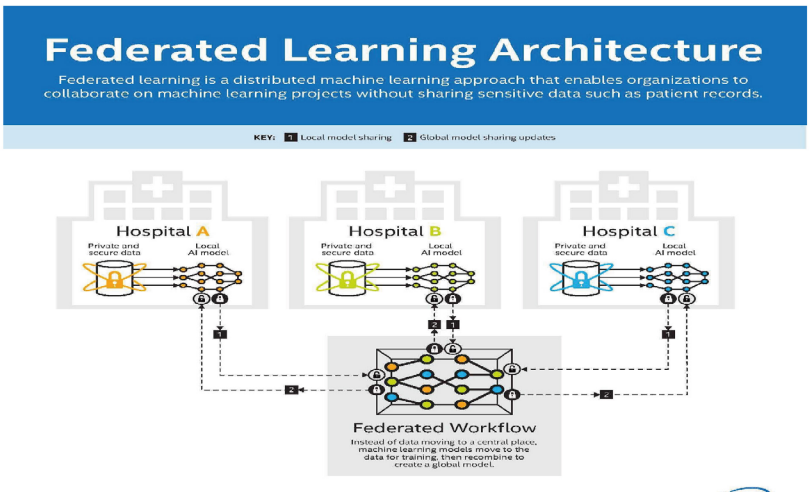
Collective learning

Privacy-preserving data analysis	AI/ML (machine learning)	Federated analytics

KAIST

CySecLab

Federated Learning: Sharing Private Medical Data

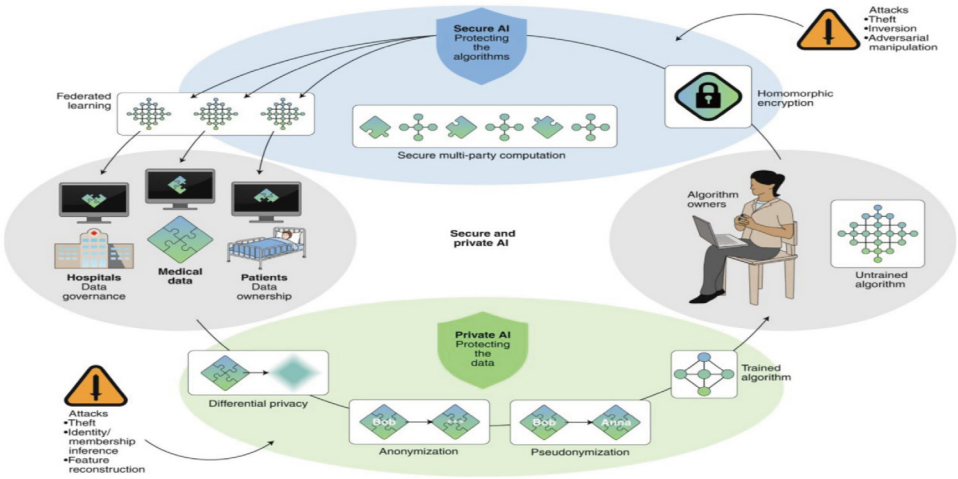


KAIST

https://mms.businesswire.com/media/20200511005132/en/790513/5/Intel-federated-learning-explainer.jpg

CySecLab

Secure and Private AI in Federated Machine Learning



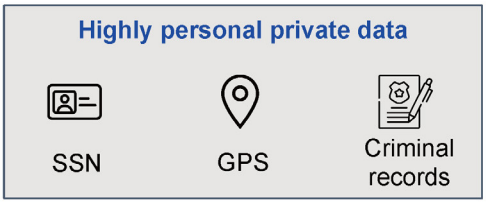
Schematic overview of the relationships and interactions between data, algorithms, actors and techniques in the field of secure and private AI.

KAIST

출처: https://www.nature.com/articles/s42256-020-0186-1

CySecLab

Confidential Computing: AI Analytics on Private Data



KAIST

CySecLab

Self-Isolation Tracing App for Covid-19

KAIST

CySecLab

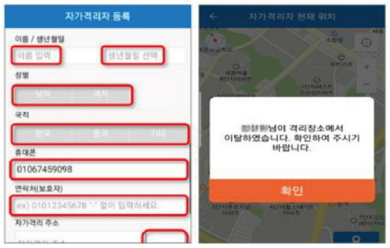
Self-Isolation Tracing App for Covid-19

행정안전부

4

자가격리자 정보·격리위치 등록

자가격리자 개인정보(자가격리 위치 등) 등록합니다.
위치 이탈 시 자가격리자 앱과 전담공무원 앱에 **알림**이 갑니다.



KAIST

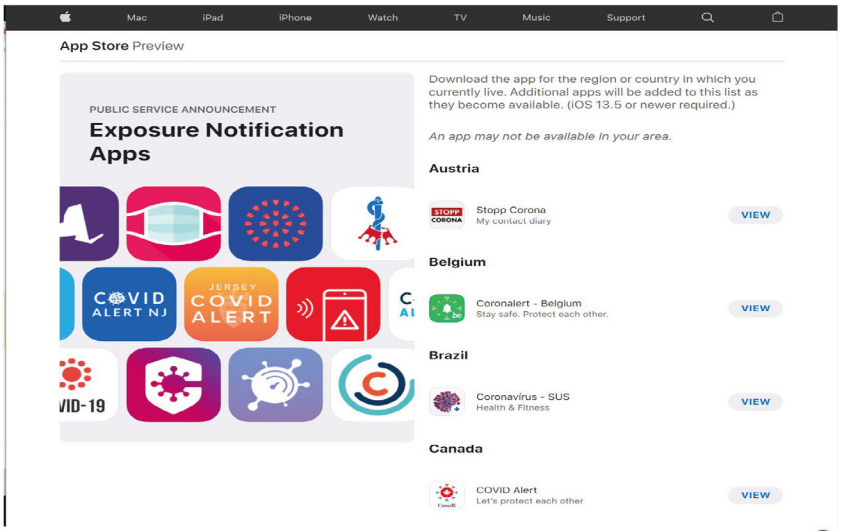
CySecLab

Contact Tracing Application for Android and IOS

KAIST

CySecLab

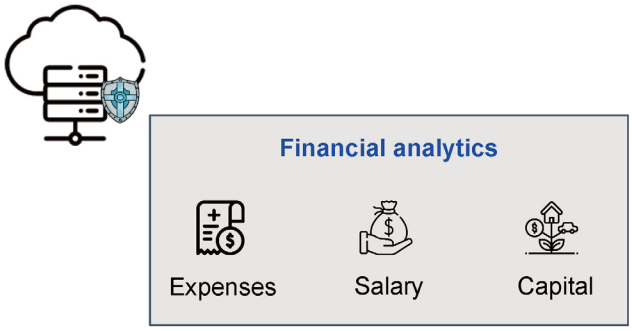
Contact Tracing Apps in the World



KAIST

CySecLab

Confidential Computing: AI Analytics on Private Data



KAIST

CySecLab
38

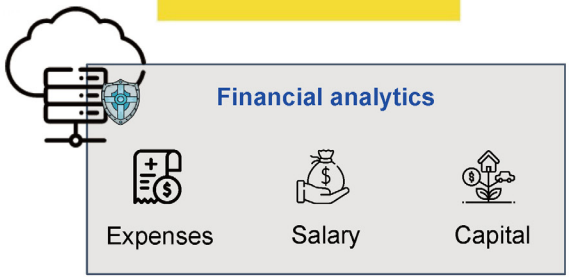
신뢰 컴퓨팅 (TEE) 적용 사례: AI 금융 보안

- 페이 열풍 시대

PAYCO SSGPAY. kakaopay

Pay SAMSUNG Pay

N Pay Pay

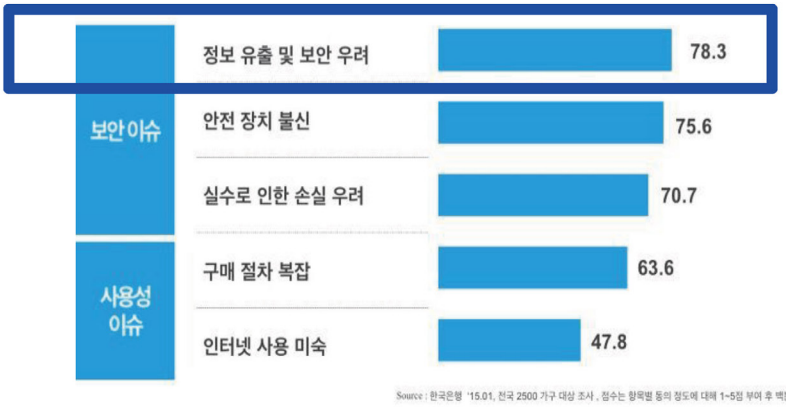


KAIST

CySecLab
39

AI 금융 보안

- 페이를 사용하지 않는 이유



Source : 한국은행 '15.01, 전국 2500 가구 대상 조사 , 점수는 항목별 동의 정도에 대해 1~5점 부여 후 백분율로 환산

KAIST

CySecLab
40

페이 보안

- 안전한 디바이스(TEE) 기반의 페이

온라인 서버 기반의 페이

PAYCO
SSGPAY.
kakaopay
N Pay

디바이스(TEE) 기반의 페이

SAMSUNG pay
KNOX, TrustZone

Pay
Secure Enclave

KAIST

CySecLab
41

신뢰 컴퓨팅 (TEE e.g., TrustZone)를 이용한 금융 보안

- 일반 실행 영역에서 동작하는 금융 앱
- 신뢰 컴퓨팅 실행환경에서 동작하는 금융 앱

KAIST

CySecLab
42

신뢰 컴퓨팅 (TEE) 적용 사례: 전자키 보호의 필요성

Digital (Crypto) Keys are an essential part of our digital lives

은행 및 금융 | 데이터 베이스 | DRM | 전자문서 서명 | 클라우드 | IoT | 블록체인 | 커넥티드 카(V2X)

- 데이터량 및 디바이스의 빠른 증가로 대용량의 암호키 생성 및 처리가 매우 중요해짐
- 클라우드 환경이 확대됨에 따라 클라우드 환경에서 이용이 편리하여야 함
- 물리적인 접근에 대한 방어보다는 SW 중심의 강력한 보안 기술이 더욱 절실해짐
- 새로운 암호 알고리즘을 적용하여 서비스 차별화 및 경쟁력 확보가 필요함

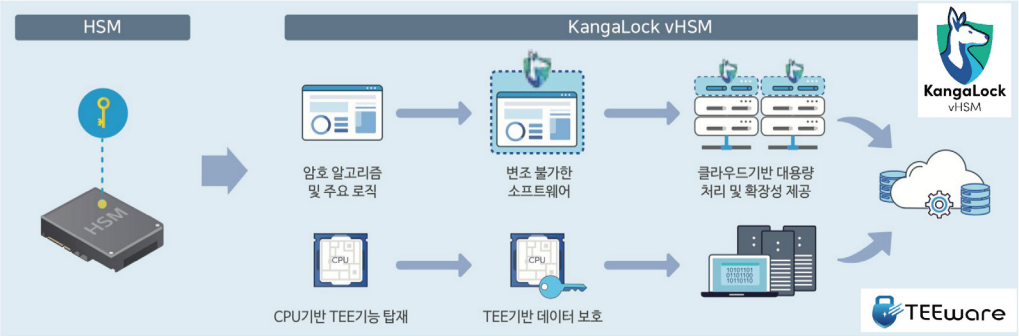
→ 고도화된 암호키 솔루션 요구증대

KAIST

CySecLab
43

신뢰 컴퓨팅 (TEE) 적용 사례: 전자키 보호 관리

Scalable and Secure Digital Key Management with TEE



출처: https://teeware.kr/

Confidential Computing Consortium and TEE Companies

intel Google Microsoft arm

ORACLE HUAWEI Red Hat

출처: https://confidentialcomputing.io/

TEEware

Acknowledgements and Contacts: cysec.kaist.ac.kr

https://cysec.kaist.ac.kr/#publications

- [PrivateZone] J. Jang, C. Choi, J. Lee, N. Kwak, S. lee, Y. Choi, B. Kang*, "PrivateZone: Providing a Private Execution Environment using ARM TrustZone", IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)
- [SECRET] J. Jang, S. Kong, M. Kim, D. Kim and B. Kang. SeCReT: Secure Channel between Rich Execution Environment and Trusted Execution Environment , NDSS 2015
- [HackingEnclave] J. Lee, J. Jang, Y. Jang, N. Kwak, Y. Choi, C. Choi, T. Kim, M. Peinado, B. Kang*, "Hacking in Darkness: Return-oriented Programming against Secure Enclaves", USENIX Security 2017
- [SystemOpenSGX] C. Choi, N. Kwak, J. Jang, D. Jang, K. Oh, K. Kwag, B. Kang* "S-OpenSGX: A System-level Platform for Exploring SGX Enclave-Based Computing", Computer & Security, 2017
- [ATRA] D. Jang, H. Lee, M. Kim, D. H. Kim, D. G. Kim and B. Kang. ATRA: Address Translation Redirection Attack against Hardware-based Kernel Integrity Monitors. ACM CCS 2014.
- [KIMON] H. Lee, H. Moon, D. Jang, K. Kim, J. Lee, Y. Paek and B. Kang. KI-Mon: A Hardware-assisted Event-triggered Monitoring Platform for Mutable Kernel Object. USENIX Security 2013.
- [VIGILARE] H. Moon, H. Lee, J. Lee, K. Kim, Y. Paek and B. Kang. Vigilare: Toward Snoop-based Kernel Integrity Monitor. ACM CCS 2012. & Detecting Kernel Rootkit Attacks with Bus Snooping, IEEE Transactions on Dependable and Secure Computing
- Kernel Integrity Monitors (Securing computing systems from the core: Kernel defense against insidious rootkit malware): http://breakthroughs.kaist.ac.kr/?post_no=163

Icons made by Freepik, Smartline, Kiranshastry, Bercis, Smashicons, Eucalyp, prettycons from www.flaticon.com

KAIST

More information: http://cysec.kaist.ac.kr **Contacts:** brentkang@kaist.ac.kr

CySecLab