신뢰/기밀 컴퓨팅 개요

CySecLab
(Cyber Systems Security Research Lab)

강병훈
Brent ByungHoon Kang, Ph.D.,

May 27, 2021

Intro. to Confidential Computing in the Age of AI

CySecLab
(Cyber Systems Security Research Lab)

강병훈
Brent ByungHoon Kang, Ph.D.,

May 27, 2021

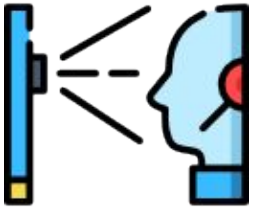
KAIST

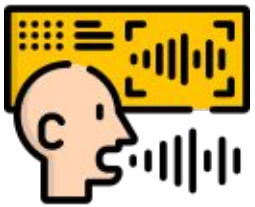
CySecLab

인공지능 기반 응용 서비스의 기초 요소들

인식

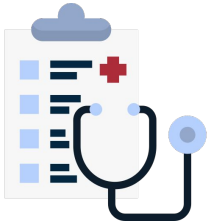
이미지, 얼굴, 언어, 음성

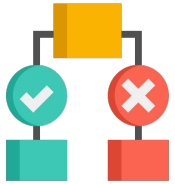




판단/연관/유추

의료 진단, 악성코드공격 판별, 상품 제안





예측

범죄방어, 금융시장, 의료 예측

KAIST

CySecLab

개인정보 데이터에 기반한 인공지능 서비스

Healthcare data

Medical images
(e.g., X-rays, CT)

Medical history

Medication privacy

Highly personal private data

SSN

GPS

Criminal records

Collective learning

Privacy-preserving data analysis

AI/ML (machine learning)

Federated analytics

Financial analytics

Expenses

Salary

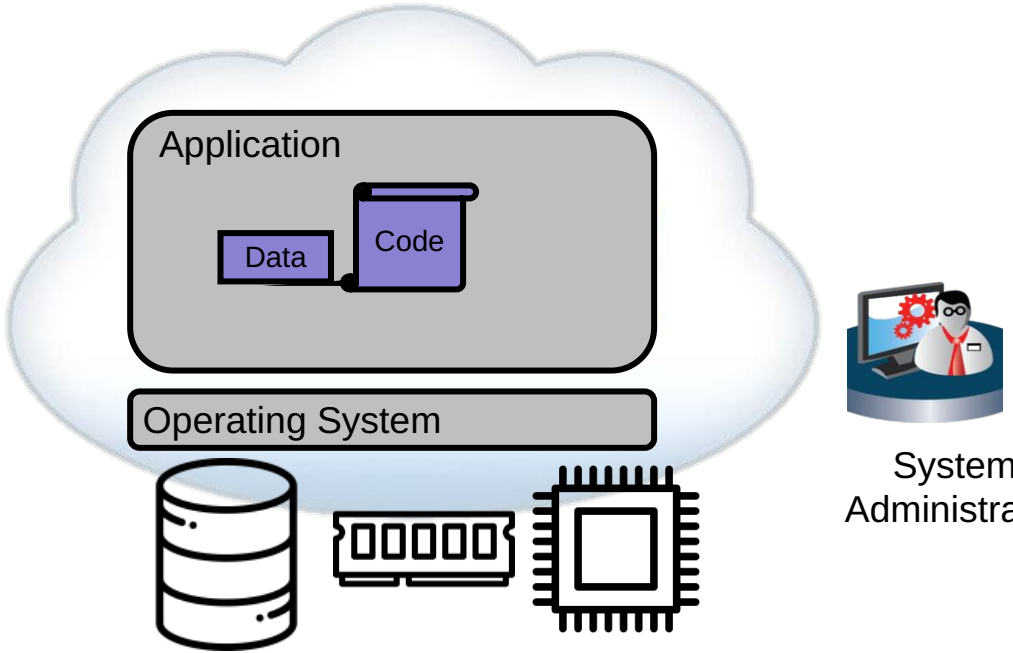
Capital

KAIST

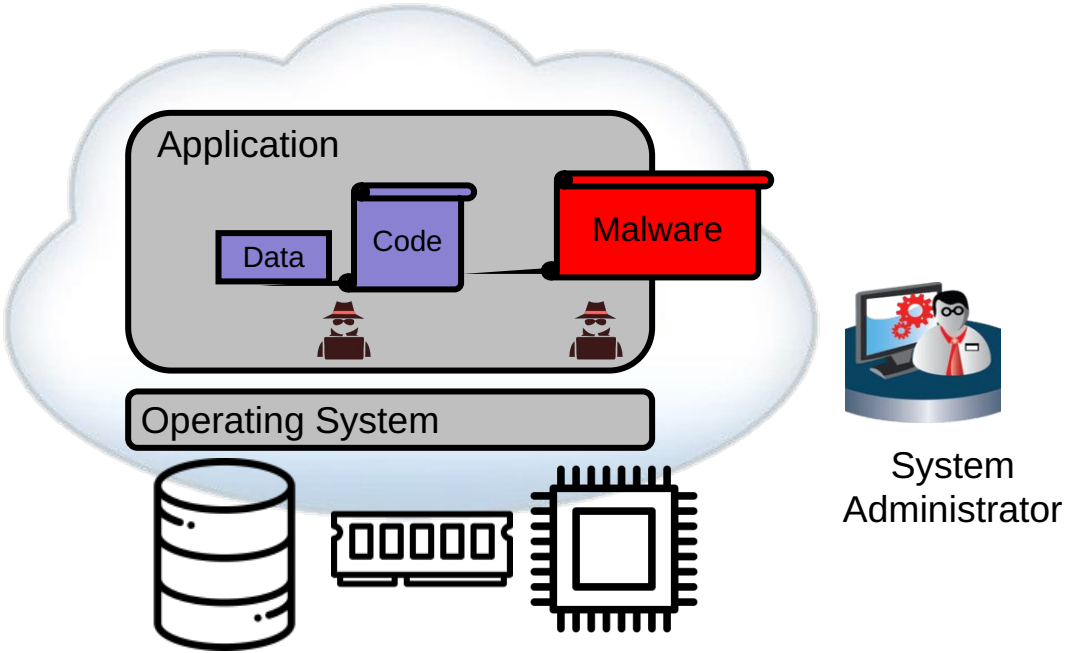
CySecLab

인공지능 기반 어플리케이션 및 서비스 시스템

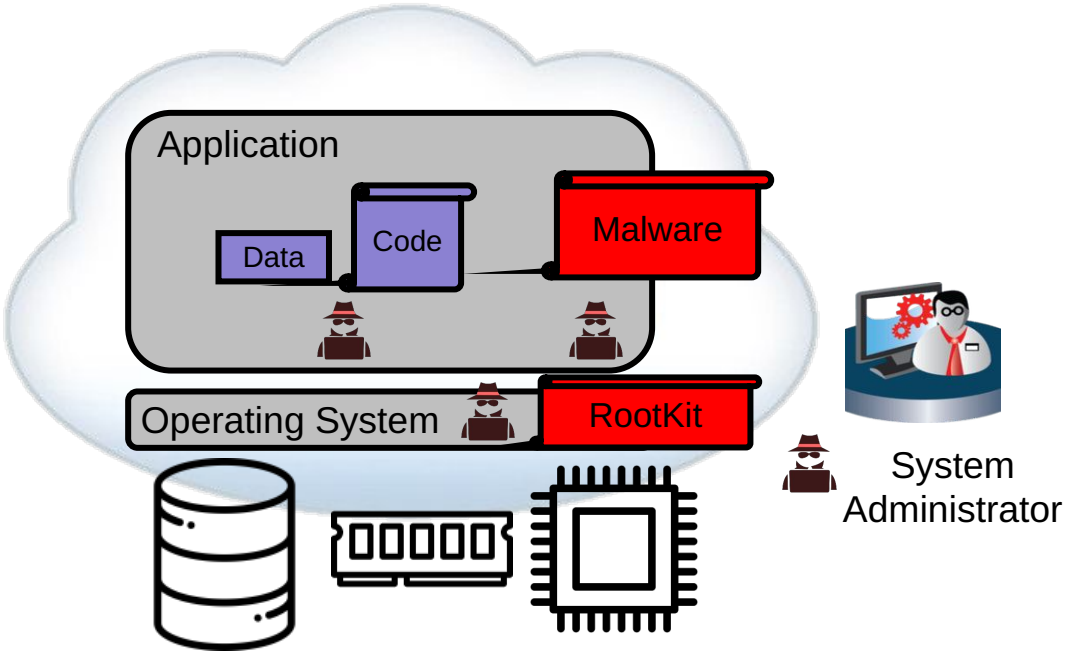
Applications and Platform Systems



Vulnerable Applications and Malwares

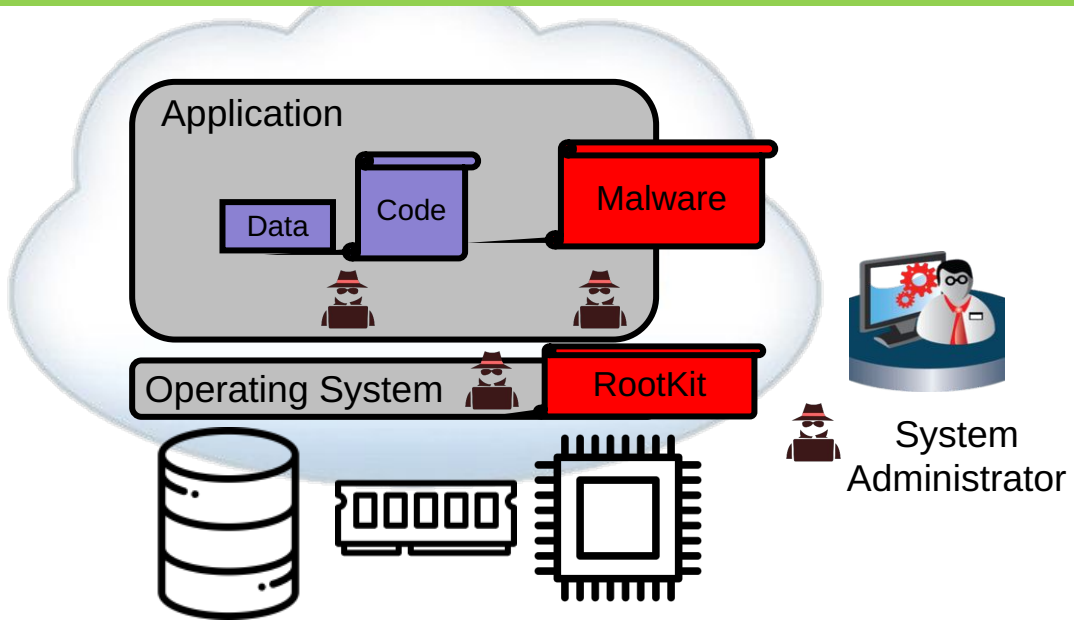


Vulnerable Applications, Systems and Malwares

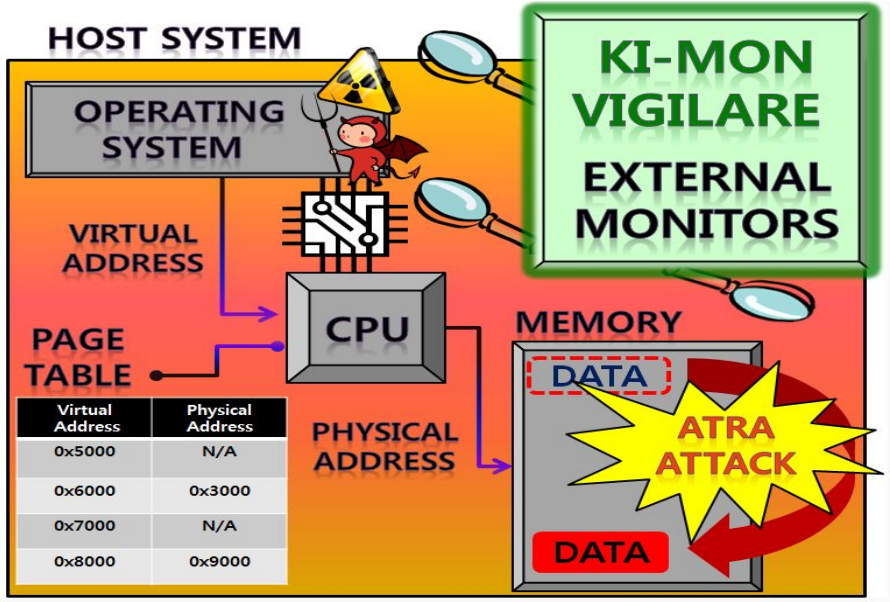


Vulnerable Applications, Systems and Malwares

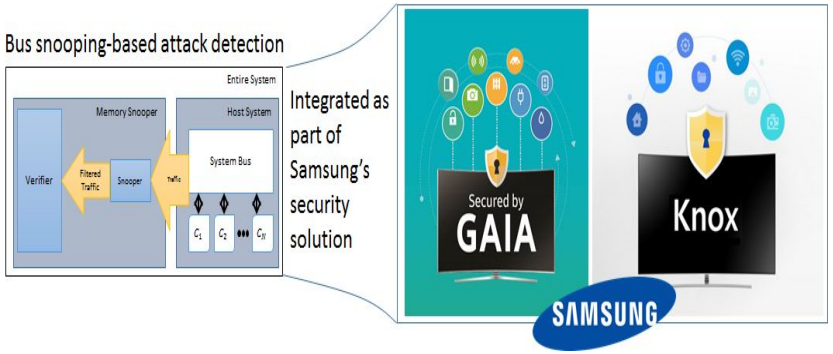
<<궁극의 질문 1.>>
악성코드 없는 세상이 가능할까 ?



Platform System Integrity Monitor



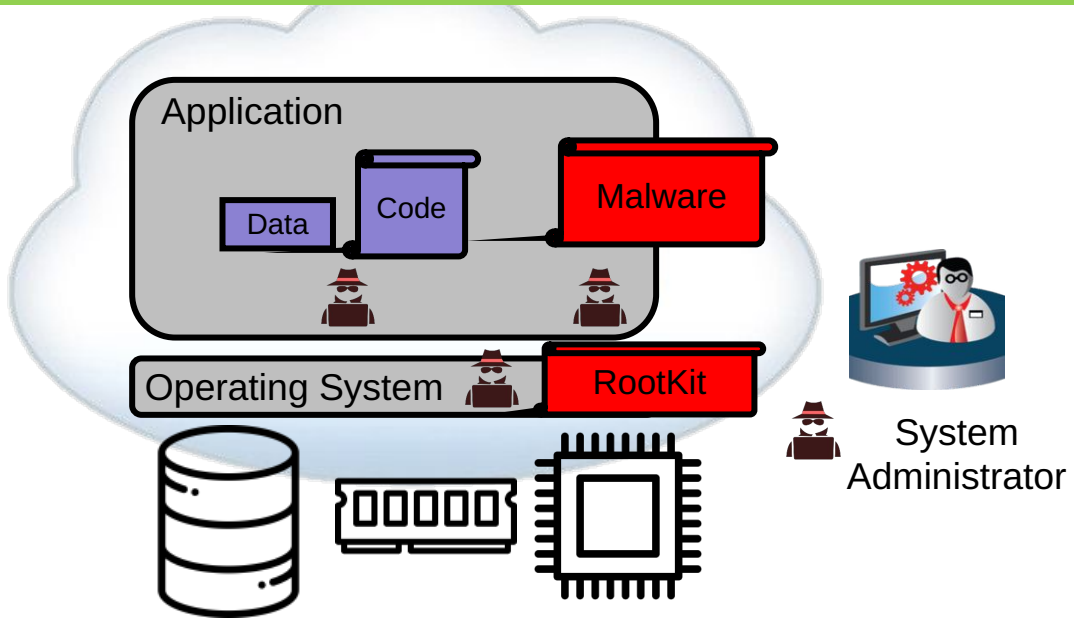
- 연구 결과 적용 사례
  - 삼성 스마트 TV 보안 시스템(GAIA)에 연구 결과 적용 및 탑재
  - 삼성 사업부 소프트웨어 보안 솔루션에 Anti-Emulation 탐지 방어기능(2018년), 힙 취약점 공격 방어기술(2017년)



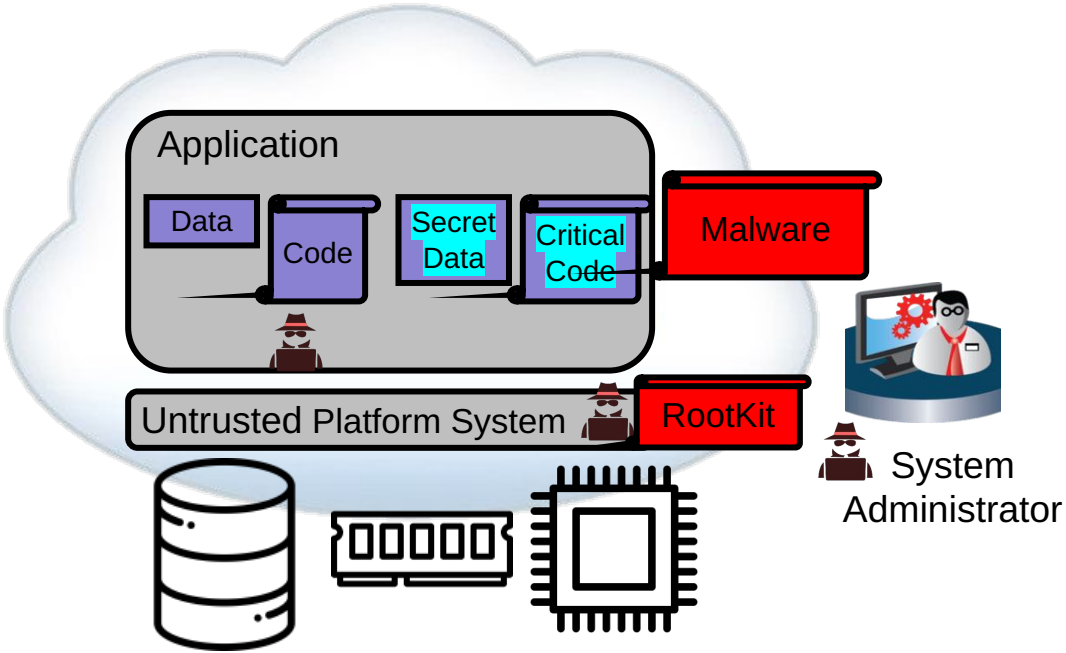
http://breakthroughs.kaist.ac.kr/?post_no=163

Vulnerable Applications, Systems and Malwares

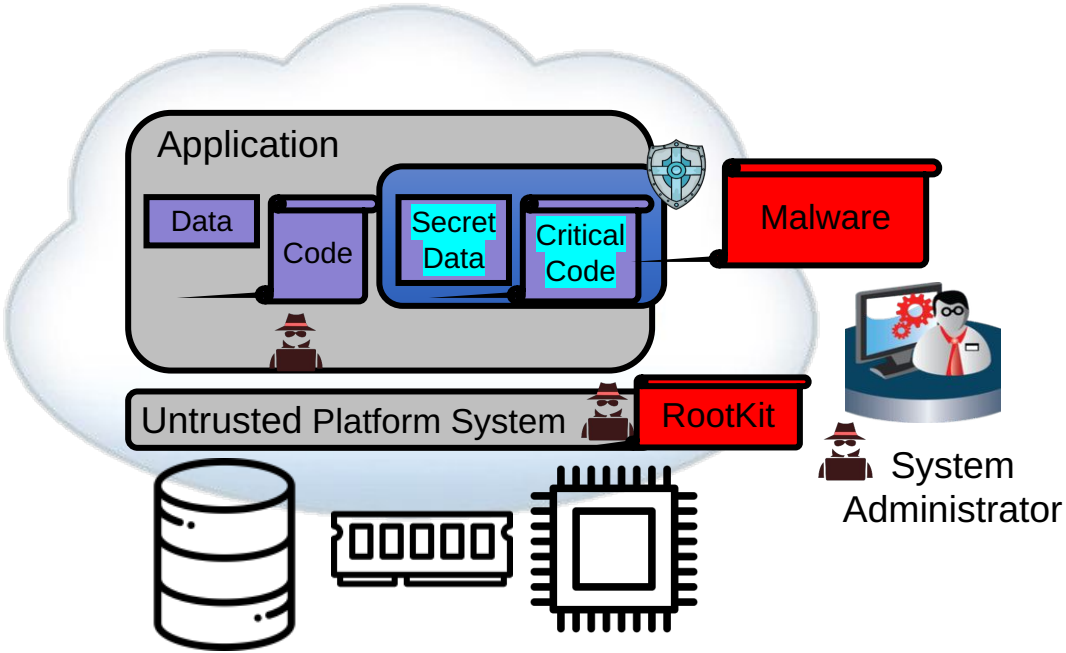
<<궁극의 질문 2.>>
악성코드가 있어도 상관없이 안전한 컴퓨팅 세상이 가능할까 ?



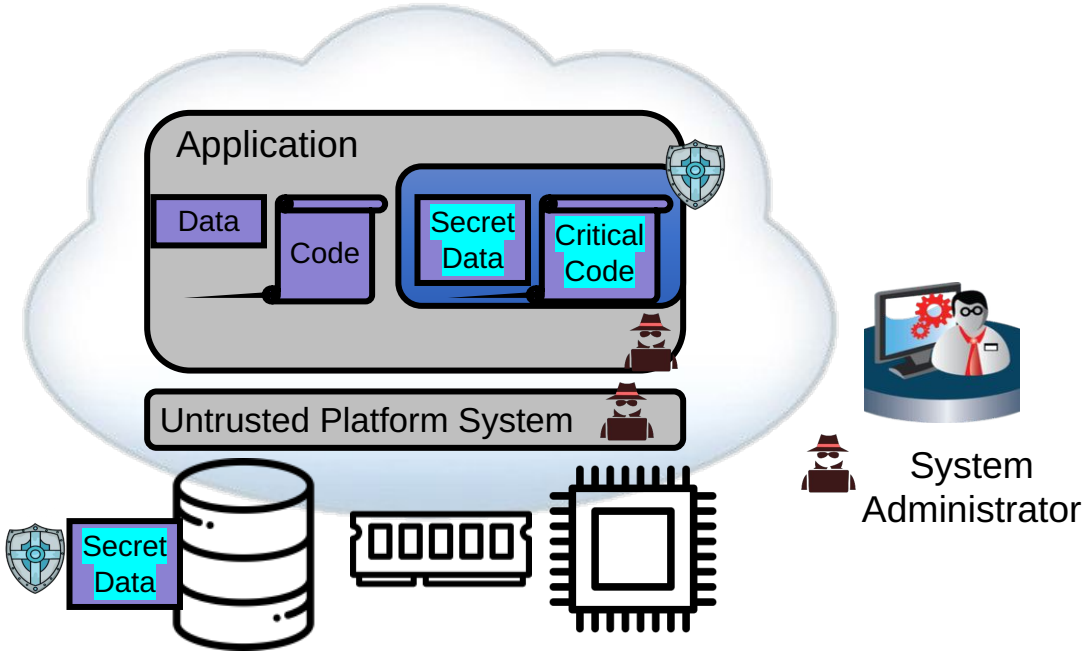
Secure Isolation of Application



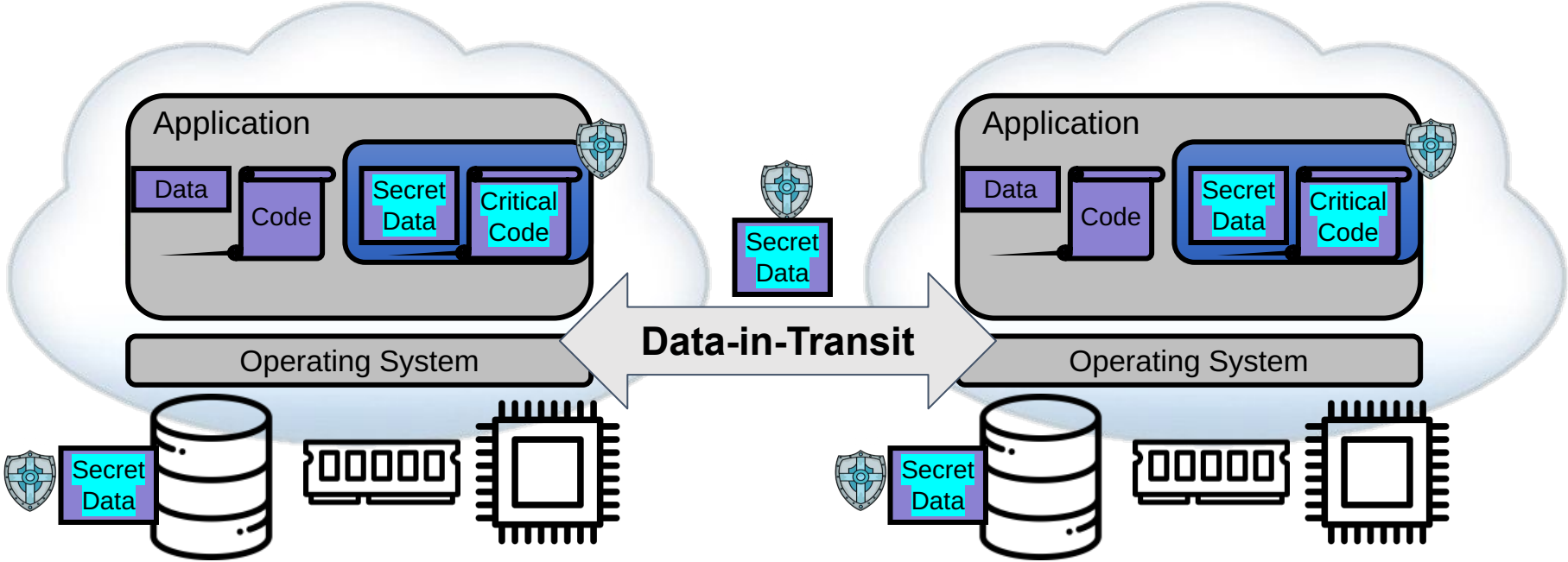
Secure Isolation of Application



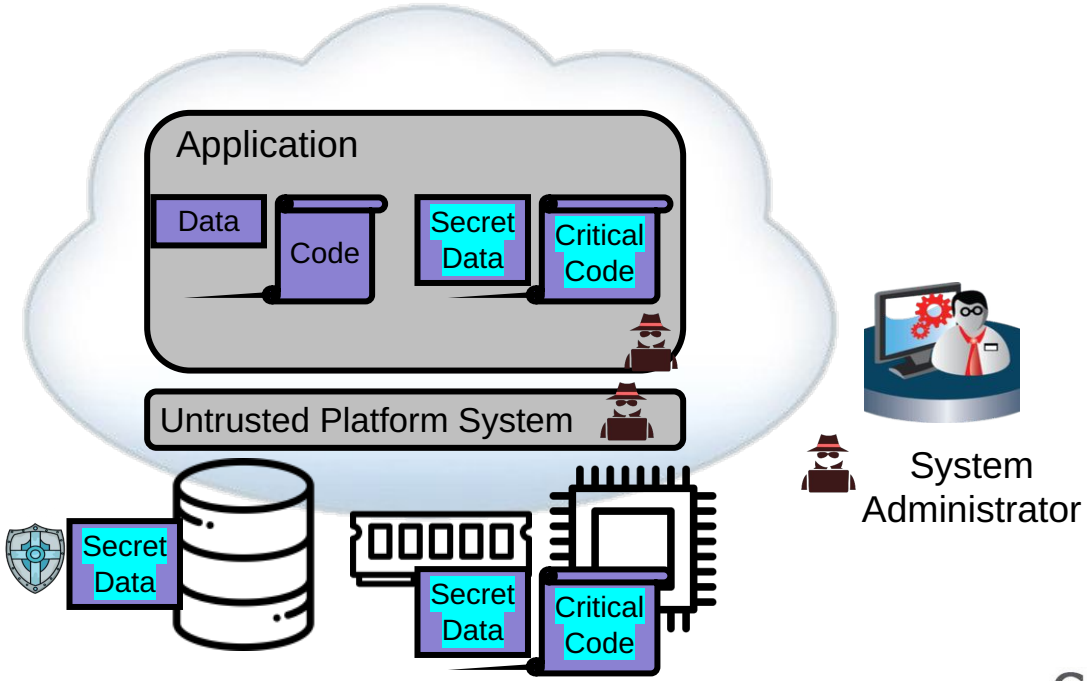
Data-at-Rest Protection



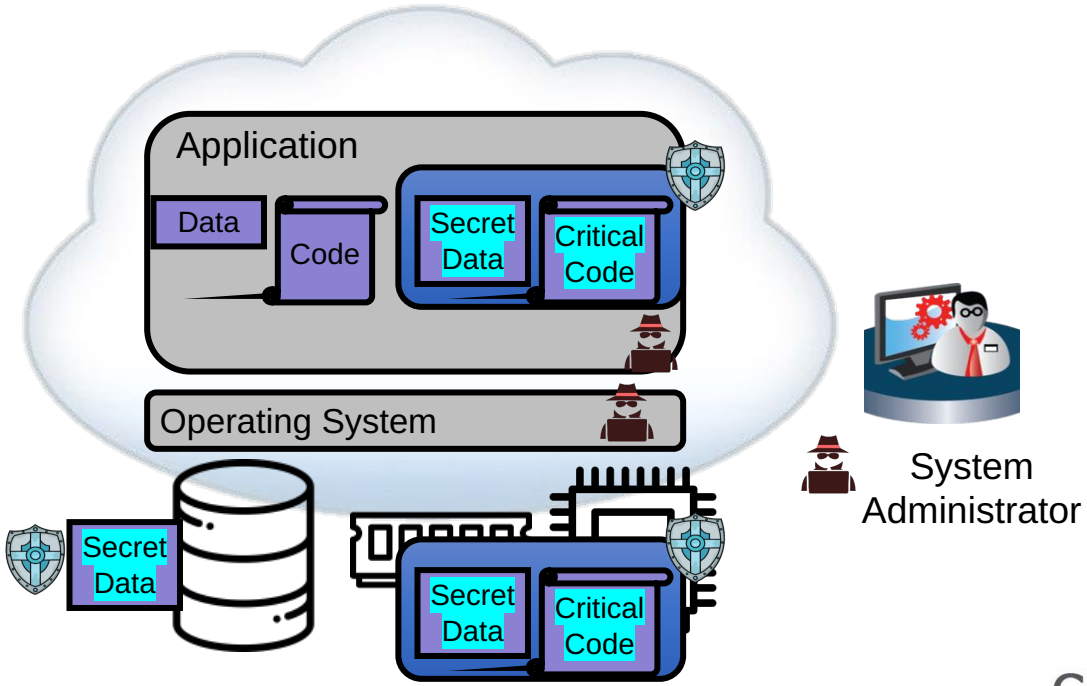
Data-in-Transit Protection



Data-in-Use Protection



Data-in-Use Protection: Confidential Computing



Trusted Confidential Computing (신뢰 기밀 컴퓨팅)

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

TEE 하드웨어 아키텍처

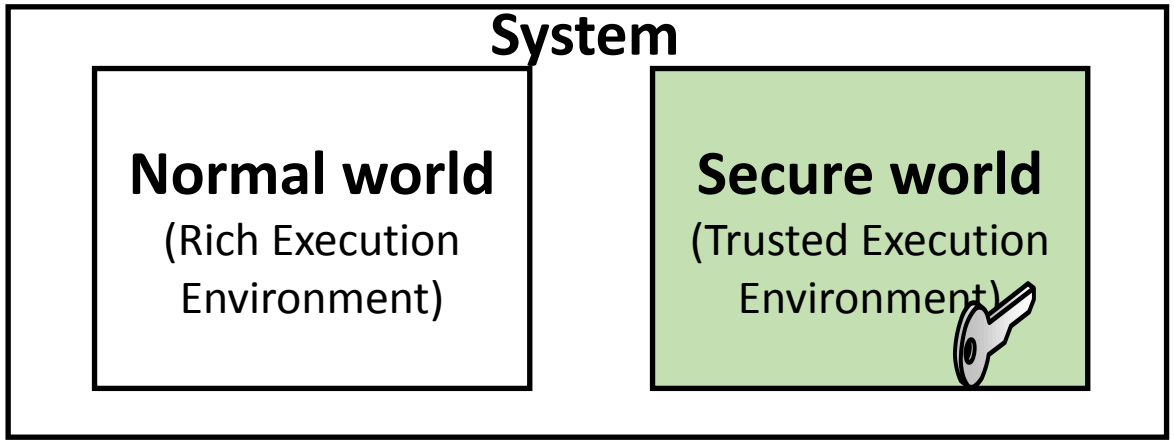
❖ **Internal hardware security module**

- 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

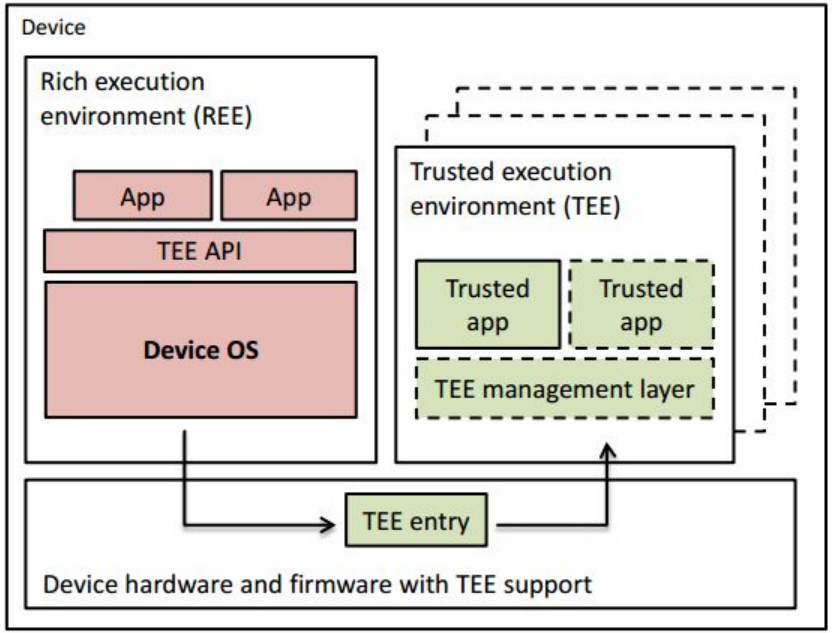
TEE 하드웨어 아키텍처

❖ **Processor secure environment**

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



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

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

TEE Hardware Realizations

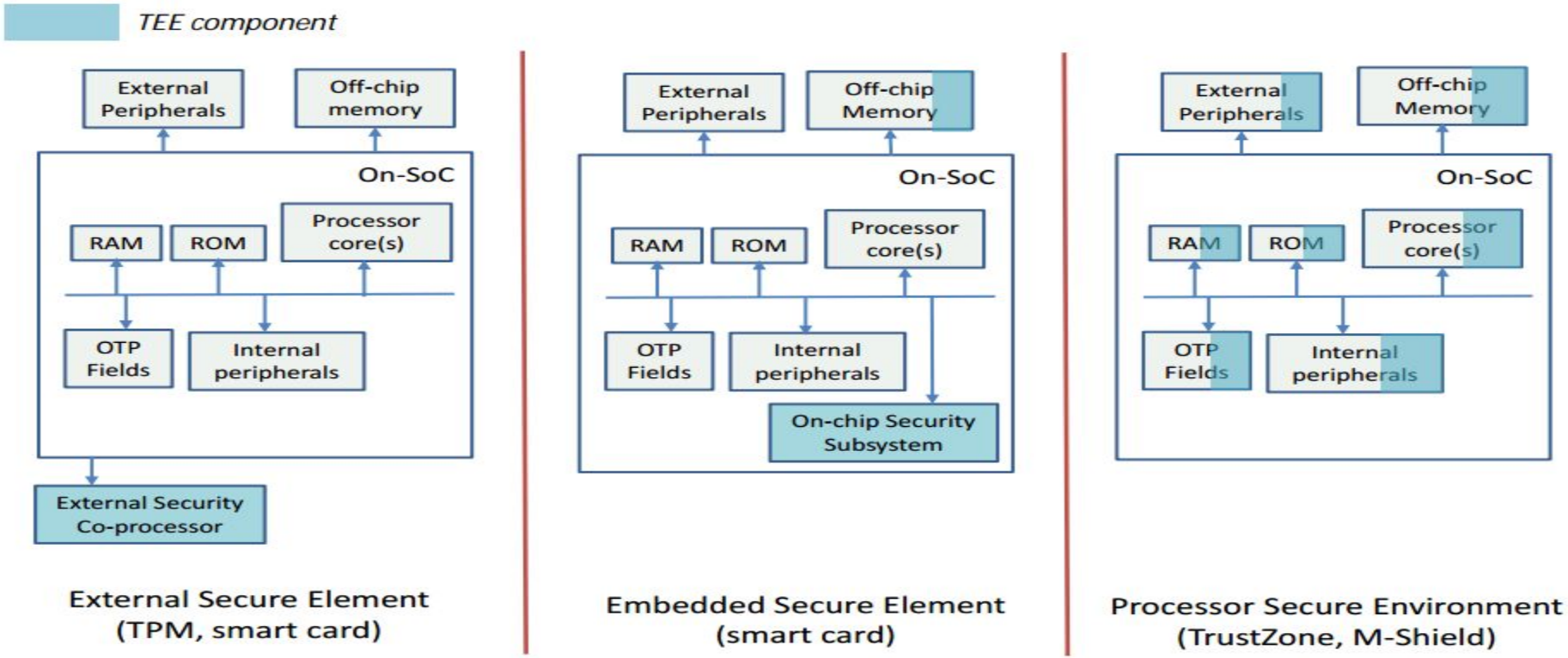


Figure adapted from: Trusted Execution Environments on Mobile Devices. ACM CCS 2013 tutorial.

Confidential Computing: AI Analytics on Private Data

Healthcare data

Medical images
(e.g., X-rays, CT)

Medical history

Medication privacy

Highly personal private data

SSN

GPS

Criminal records

Collective learning

Privacy-preserving data analysis

AI/ML (machine learning)

Federated analytics

Financial analytics

Expenses

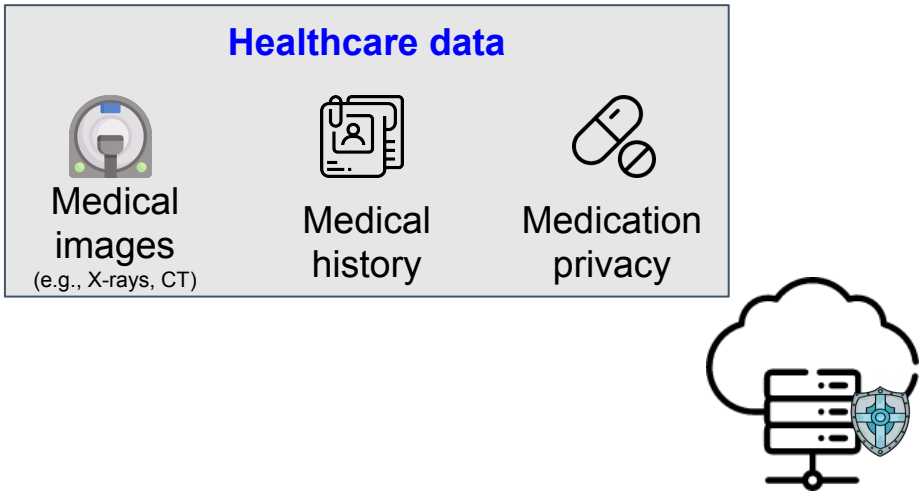
Salary

Capital

KAIST

CySecLab

Confidential Computing: AI Analytics on Private Data



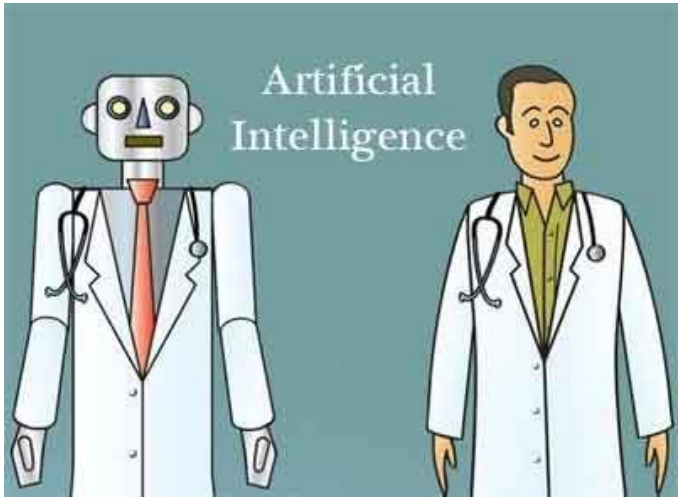
Privacy Issue in AI with Medical Data Processing

Healthcare data

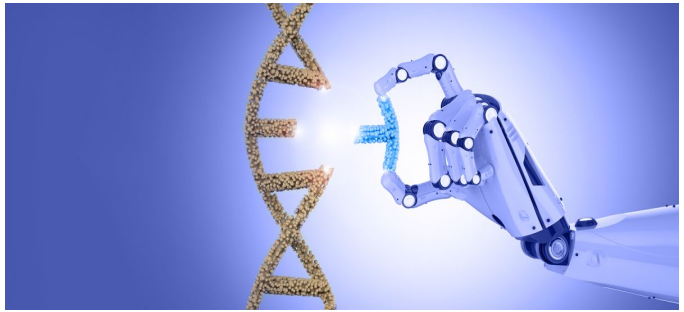
Medical images
(e.g., X-rays, CT)

Medical history

Medication privacy

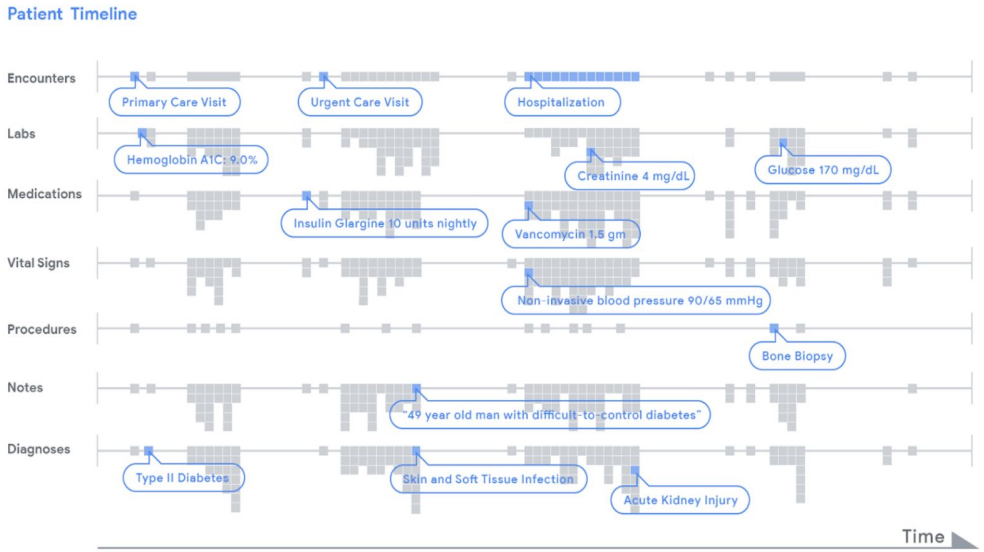


AI Doctor



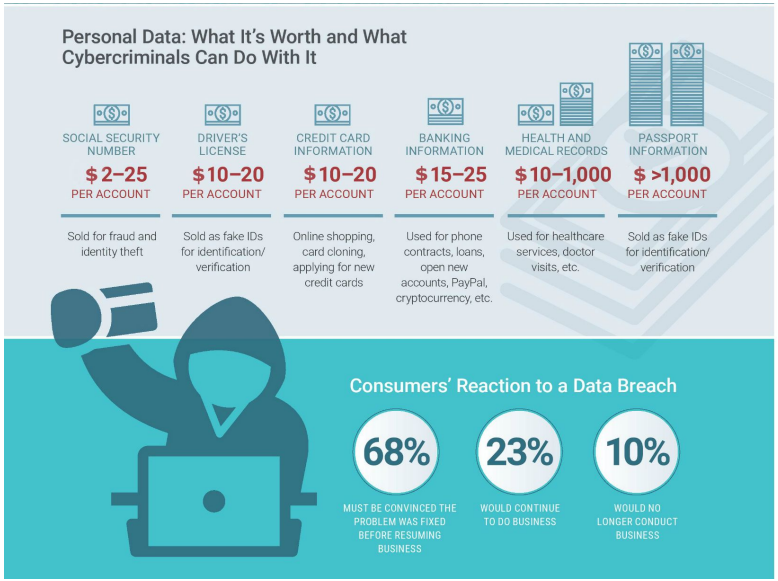
Gene editing backed by AI

AI needs lots of Private Data for Machine Learning



Medical Information & DNA Genome

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/)

Confidential Computing: AI Analytics on Private Data

Collective learning

Privacy-preserving data analysis

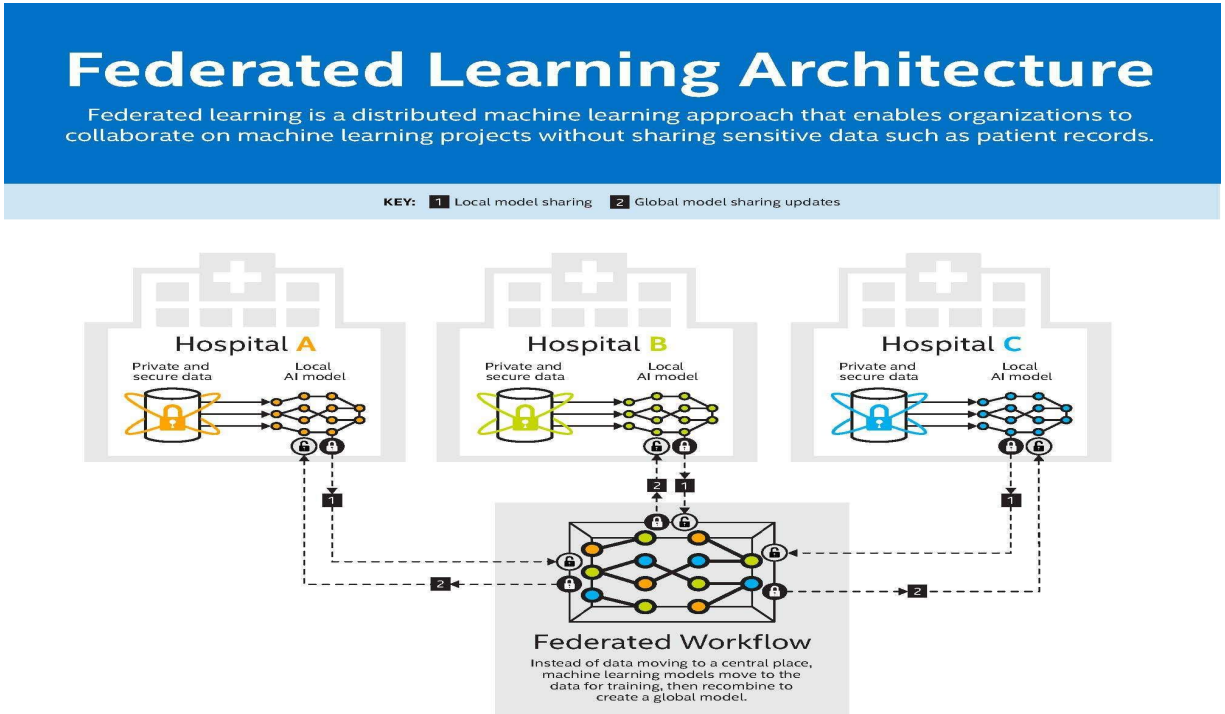
AI/ML (machine learning)

Federated analytics

KAIST

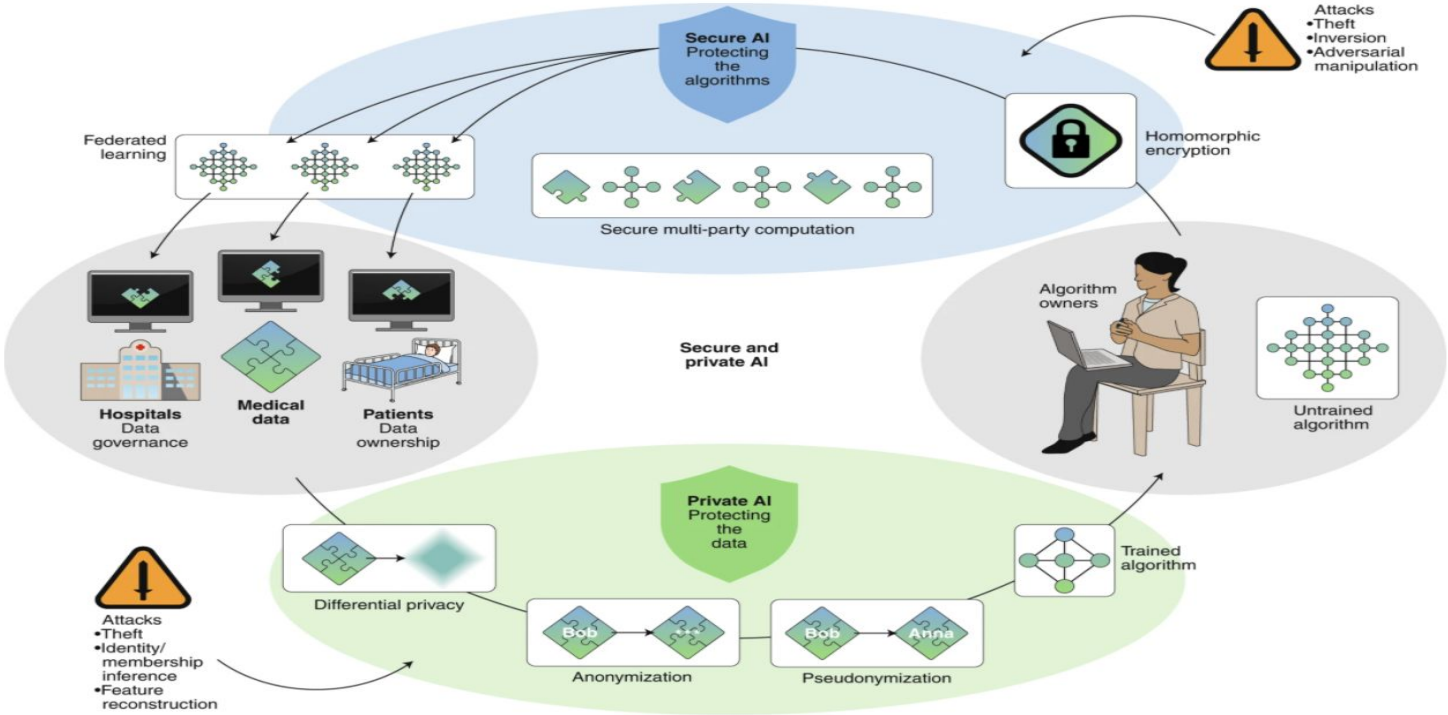
CySecLab

Federated Learning: Sharing Private Medical Data



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

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.

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

Confidential Computing: AI Analytics on Private Data

Highly personal private data

SSN

GPS

Criminal records

Self-Isolation Tracing App for Covid-19

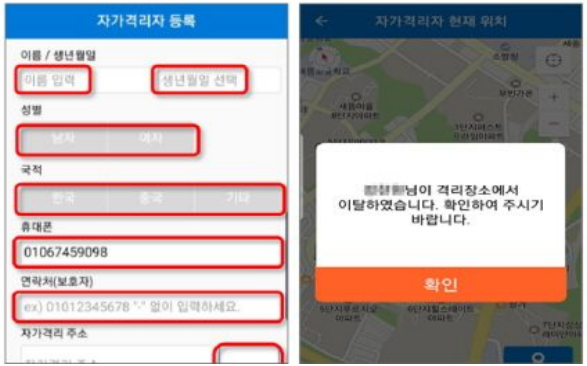
Self-Isolation Tracing App for Covid-19

행정안전부

4

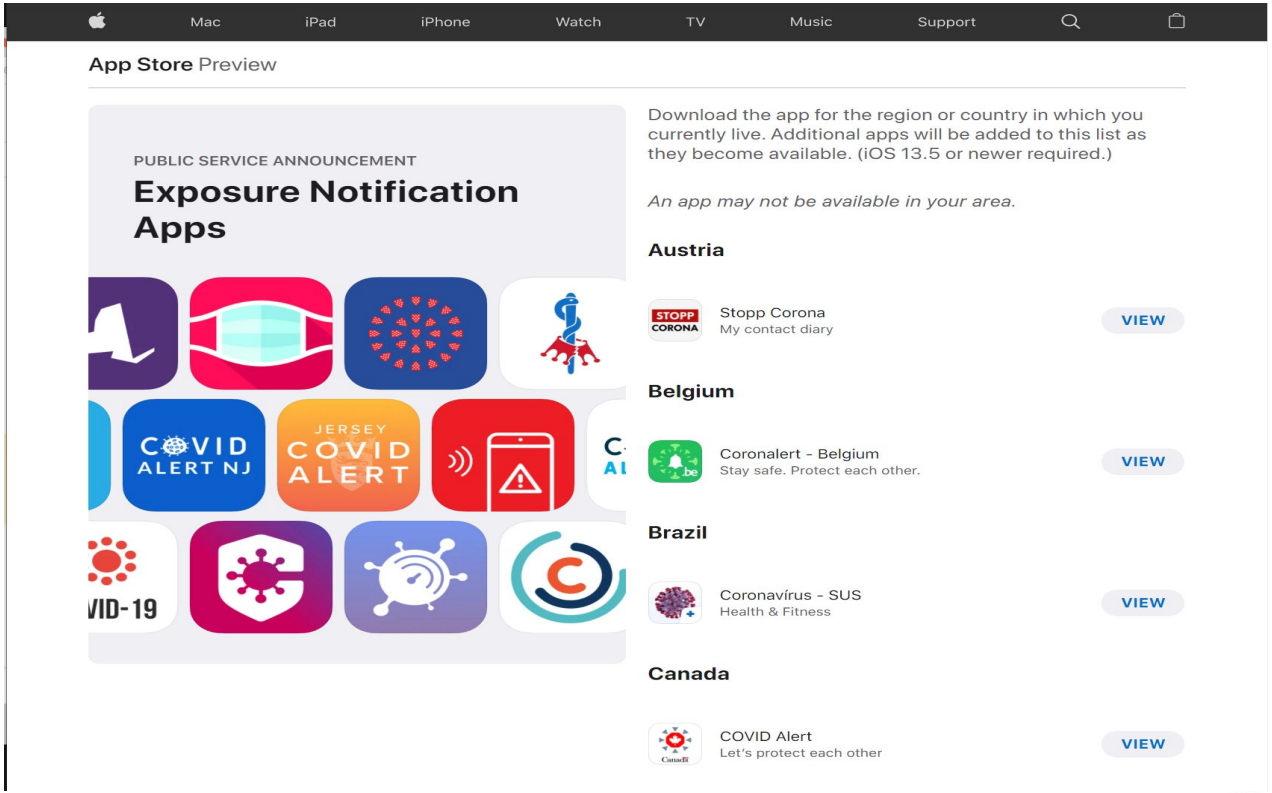
자가격리자 정보·격리위치 등록

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

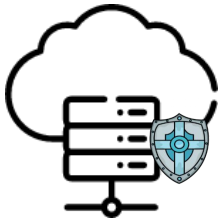


Contact Tracing Application for Android and IOS

Contact Tracing Apps in the World



Confidential Computing: AI Analytics on Private Data



Financial analytics

Expenses

Salary

Capital

KAIST

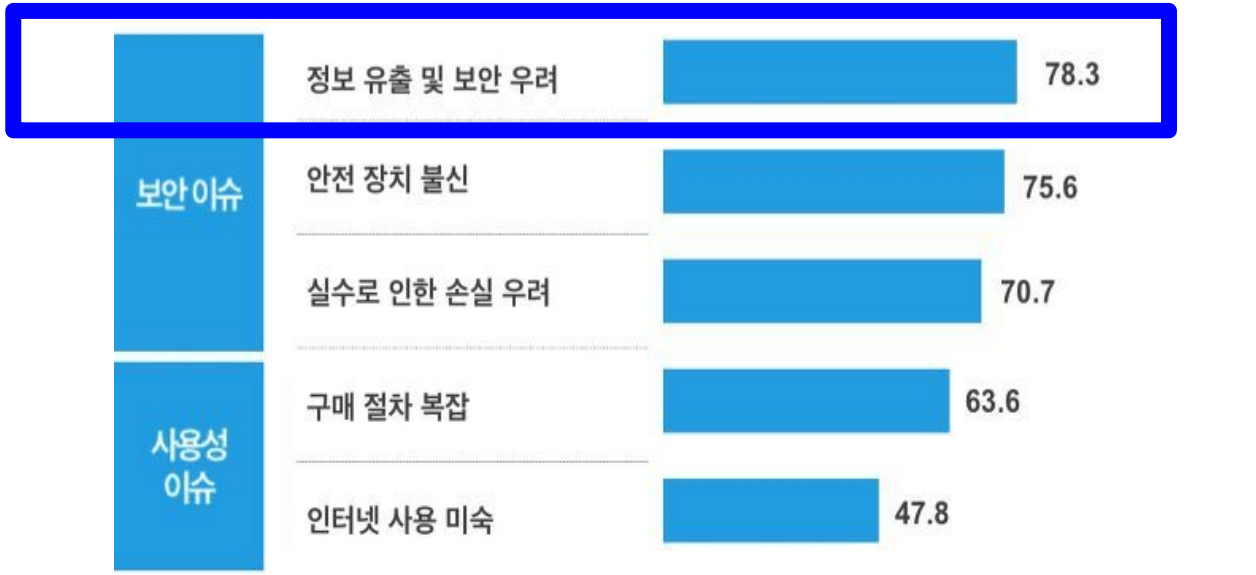
CySecLab

신뢰 컴퓨팅 (TEE) 적용 사례: AI 금융 보안

- 페이 열풍 시대

AI 금융 보안

- 페이를 사용하지 않는 이유

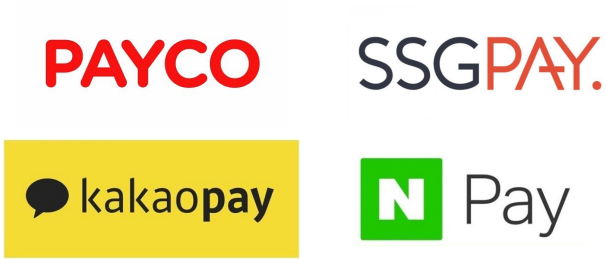


Source : 한국은행 '15.01, 전국 2500 가구 대상 조사 , 점수는 항목별 동의 정도에 대해 1~5점 부여 후 백분율로 환산

페이 보안

- 안전한 디바이스(TEE) 기반의 페이

온라인 서버 기반의 페이



디바이스(TEE) 기반의 페이

KNOX, TrustZone

Secure Enclave

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

- 일반 실행 영역에서 동작하는 금융 앱

- 신뢰 컴퓨팅 실행환경에서 동작하는 금융 앱

KAIST

CySecLab

신뢰 컴퓨팅 (TEE) 적용 사례: 전자키 보호의 필요성

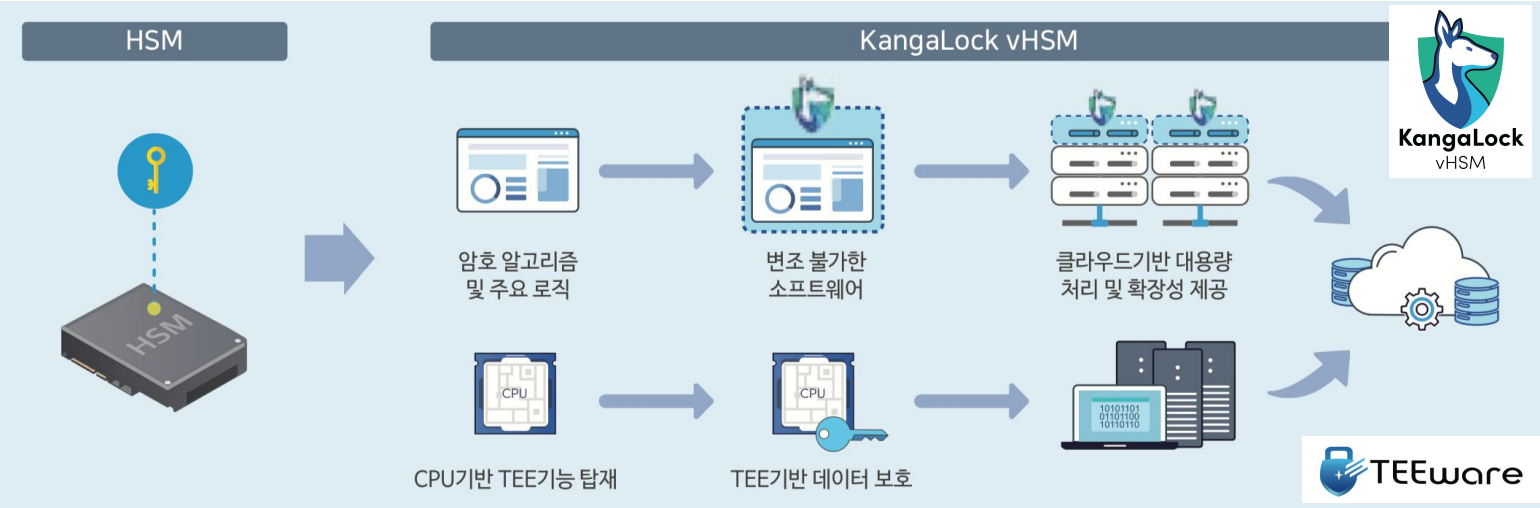
Digital (Crypto) Keys are an essential part of our digital lives

- 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

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

출처: https://confidentialcomputing.io/

Acknowledgements and Contacts: cysec.kaist.ac.kr

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

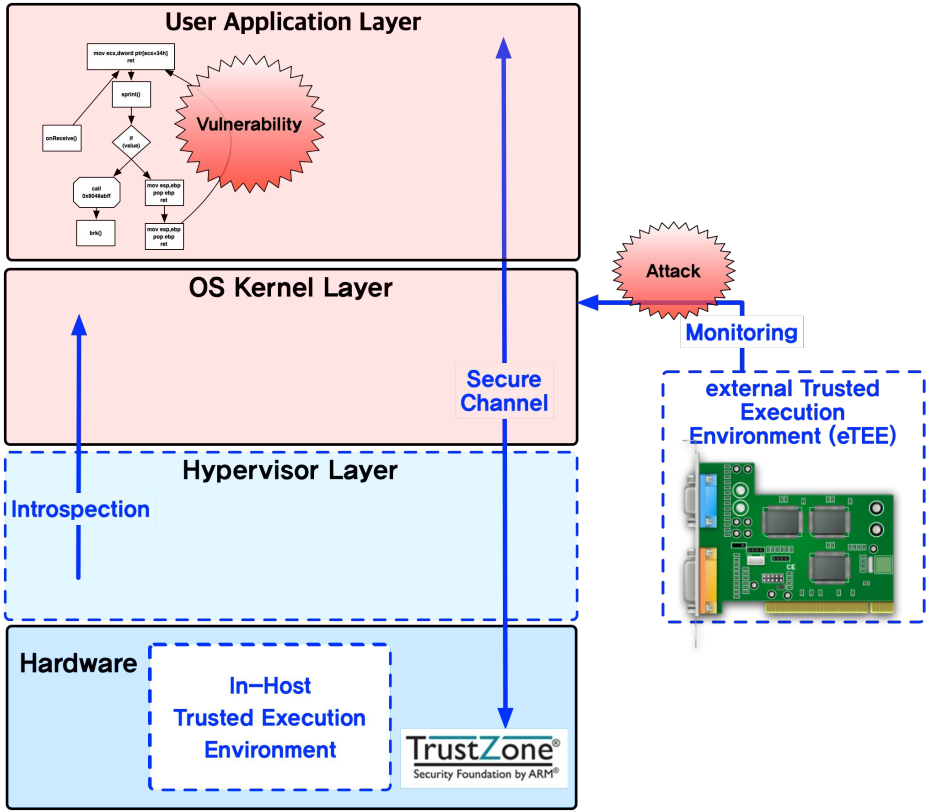
- [PrivateZone] J. Jang, C. Choi, J. Lee, N. Kwak, S. lee, Y. Choi, B. Kang*, "PrivateZone: Providing a Private Execution Environment using ARM TrustZone", IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)
- [SECRET] J. Jang, S. Kong, M. Kim, D. Kim and B. Kang. SeCReT: Secure Channel 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

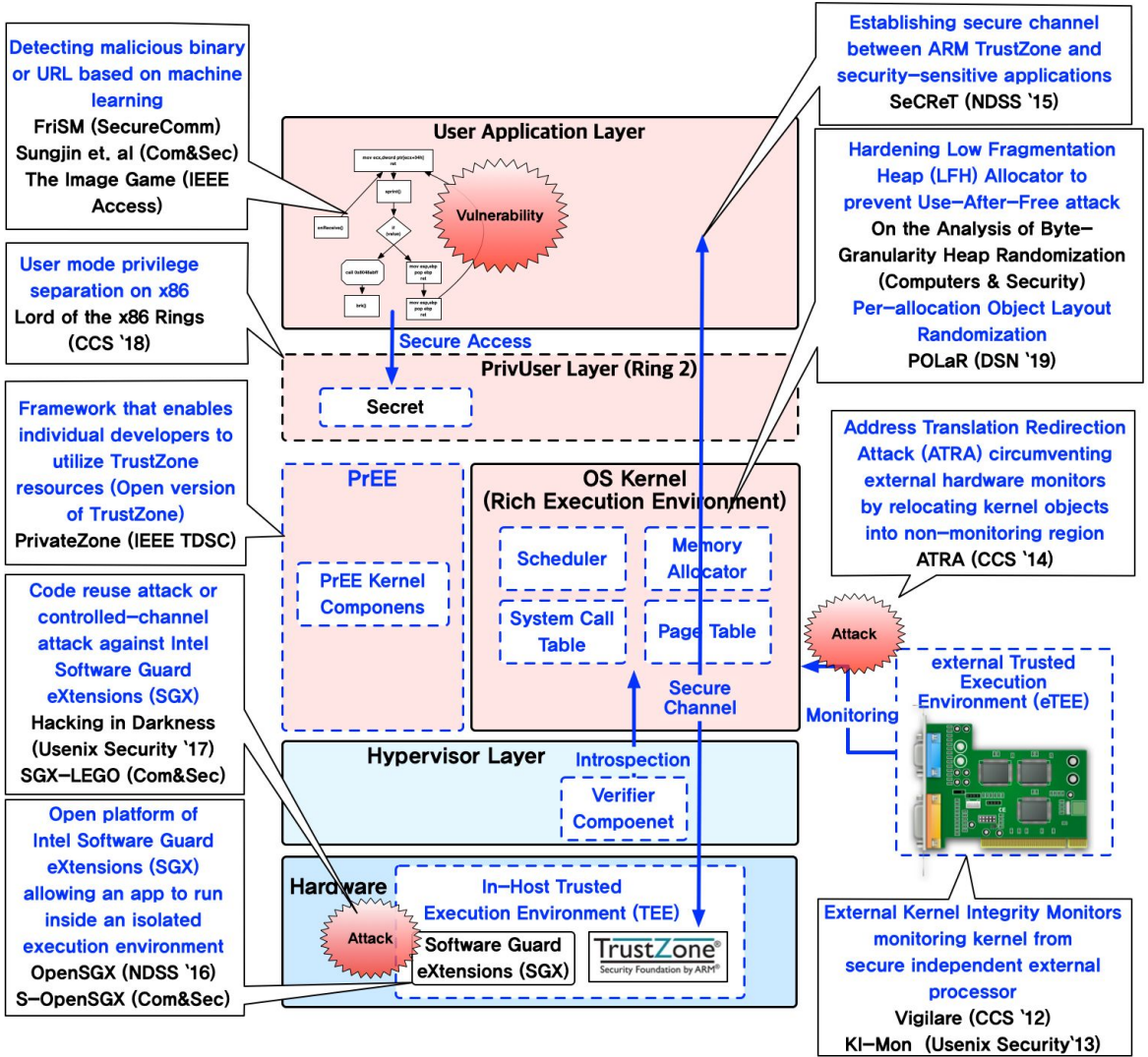
Icons made by Freepik, Smartline, Kiranshastry, Bercis, Smashicons, Eucalyp, prettycons from www.flaticon.com

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

KAIST CySecLab

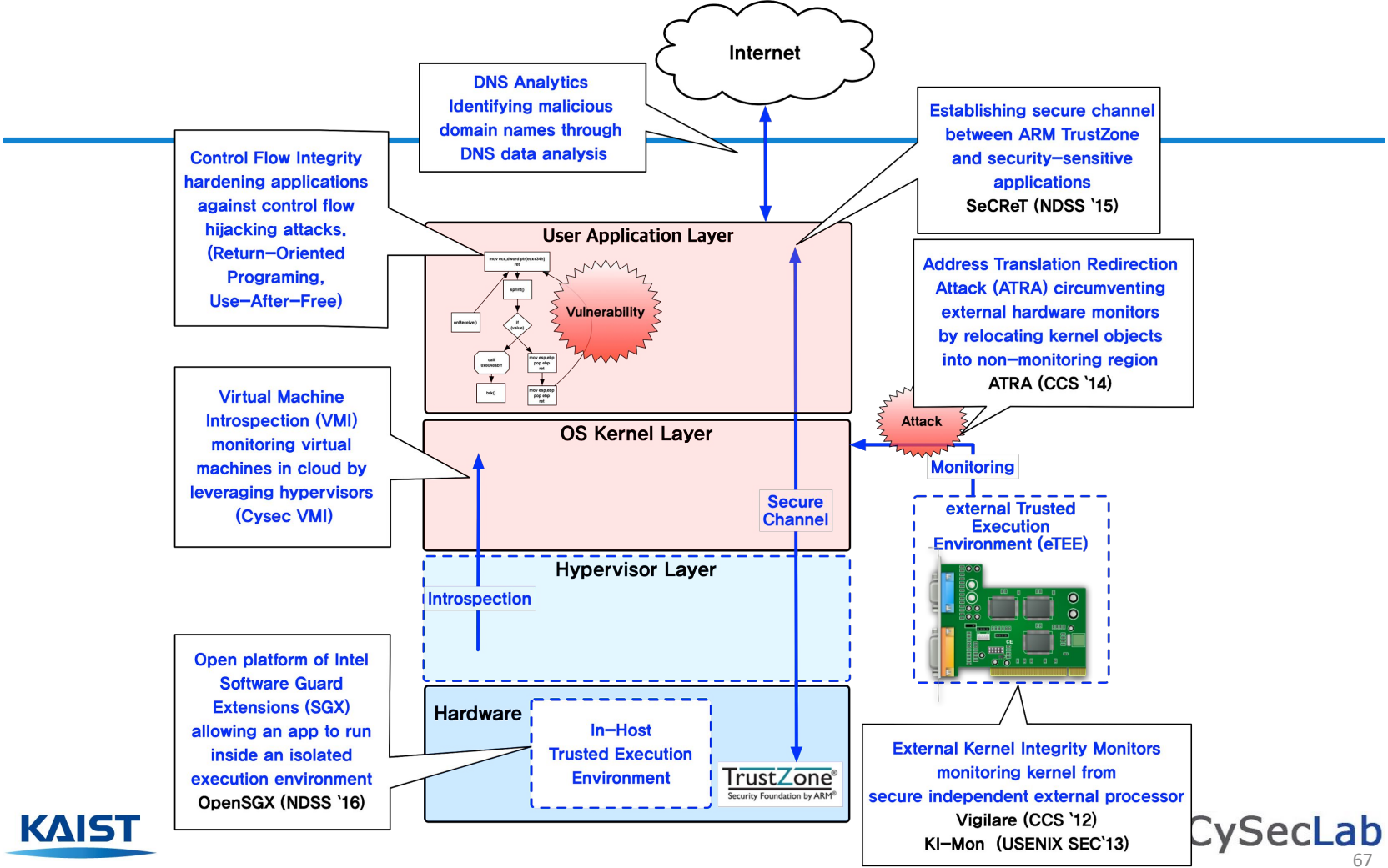
Q & A


User Application Layer
Vulnerability
OS Kernel Layer
Attack
Monitoring
Secure Channel
external Trusted Execution Environment (eTEE)
Hypervisor Layer
Introspection
Hardware
In-Host Trusted Execution Environment
TrustZone
Security Foundation by ARM



KAIST

CySecLab


Internet
DNS Analytics
Identifying malicious
domain names through
DNS data analysis
Establishing secure channel
between ARM TrustZone
and security-sensitive
applications
SeCReT (NDSS '15)
Control Flow Integrity
hardening applications
against control flow
hijacking attacks.
(Return-Oriented
Programing,
Use-After-Free)
User Application Layer
Vulnerability
Address Translation Redirection
Attack (ATRA) circumventing
external hardware monitors
by relocating kernel objects
into non-monitoring region
ATRA (CCS '14)
Attack
Monitoring
Virtual Machine
Introspection (VMI)
monitoring virtual
machines in cloud by
leveraging hypervisors
(Cysec VMI)
OS Kernel Layer
Secure
Channel
external Trusted
Execution
Environment (eTEE)
Hypervisor Layer
Introspection
Open platform of Intel
Software Guard
Extensions (SGX)
allowing an app to run
inside an isolated
execution environment
OpenSGX (NDSS '16)
Hardware
In-Host
Trusted Execution
Environment
TrustZone
Security Foundation by ARM
External Kernel Integrity Monitors
monitoring kernel from
secure independent external processor
Vigilare (CCS '12)
KI-Mon (USENIX SEC'13)