

주제강연

개인정보 보호를 위한 신뢰계산기술

이병영 교수
(서울대학교)



개인정보 보호를 위한 신뢰계산기술

서울대학교 전기정보공학부

이병영

byoungyoung@snu.ac.kr

Speaker: 이병영

- Research areas: Hacking, Systems Security, Software Security
 - Microsoft Research, Research Intern (2012 Summer)
 - Google Chrome, Software Engineering Intern (2014 Summer)
 - Purdue University, Assistant Professor (2016-2018)
- Found 100++ vulnerabilities from Windows kernel, Linux kernel, Chrome, Firefox, etc.
- Internet Defense Prize by Facebook and USENIX (2015)
- Three times DEFCON CTF Finalist (2007, 2009, and 2011)
- DARPA Cyber Grand Challenge (CGC) Finalist (2016)
- Google ASPIRE Awards (2019)

My Research Areas: Protecting Commodity Systems

Apps



DangNull [NDSS 15]
Expector [WWW 15]
TrackMeOrNot [WWW 16]
MEDS [NDSS 18]
CRFuzz [FSE 20]



CaVer [USENIX Sec 15]
HexType [CCS 17]

NGINX

ASLR-Guard [CCS 15]

Attack
Mitigation

OS



Juxta [SOSP 15]
KUP [ATC 16]
Razzer [S&P 19]
uXOM [Security 19]
HFL [NDSS 20]



Morula [S&P 14]
Kenali [NDSS 16]
ExpRace [BlackHat20]



CAB-Fuzz [ATC 17]

Intel® SGX

SGX-ASLR [NDSS 17]
Obliviate [NDSS 18]
Obfuscuro [NDSS 19]
Trustore [CCS 20]

Vulnerability
and
Exploitation

HW



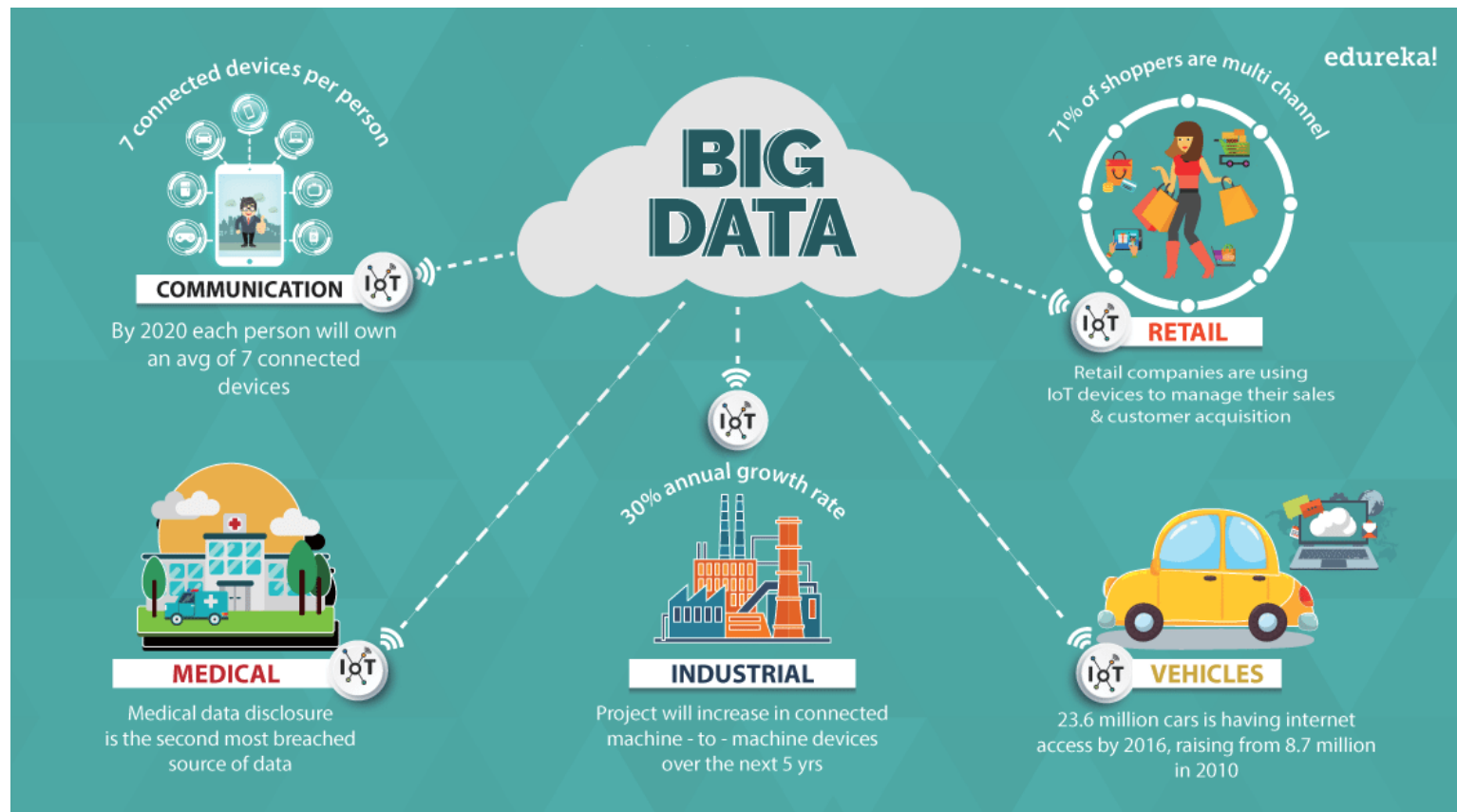
HDFI [S&P 16]



Minion [NDSS 18]

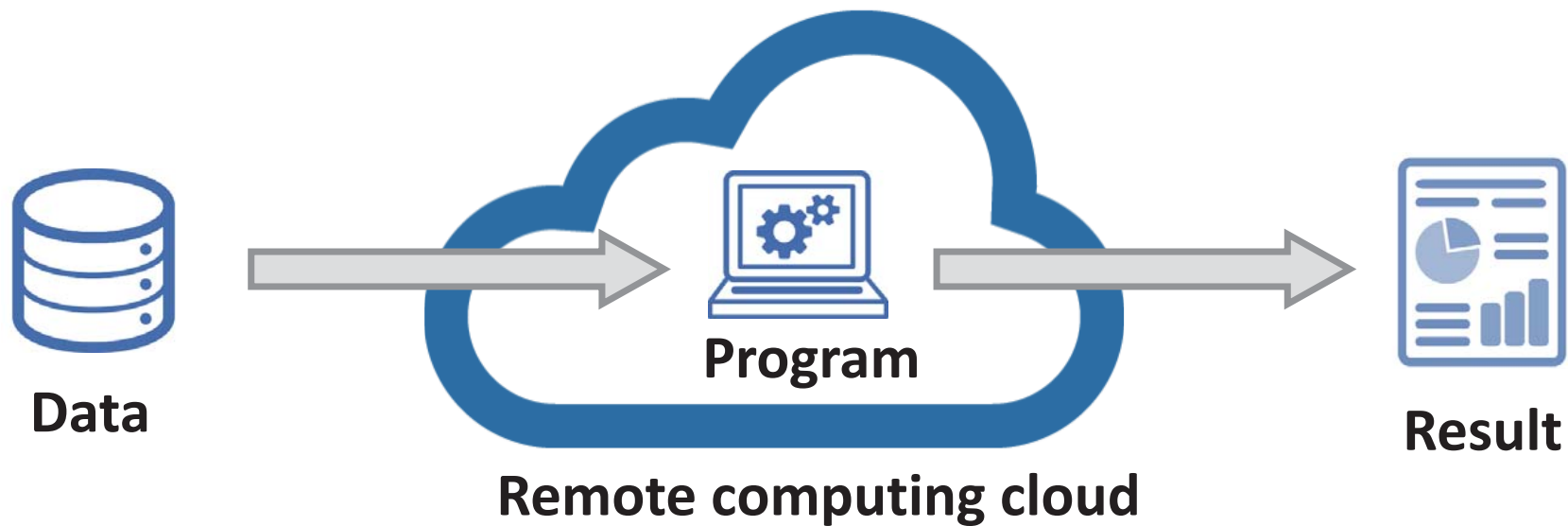
Secure
Trusted
Computing

The Age of Big Data

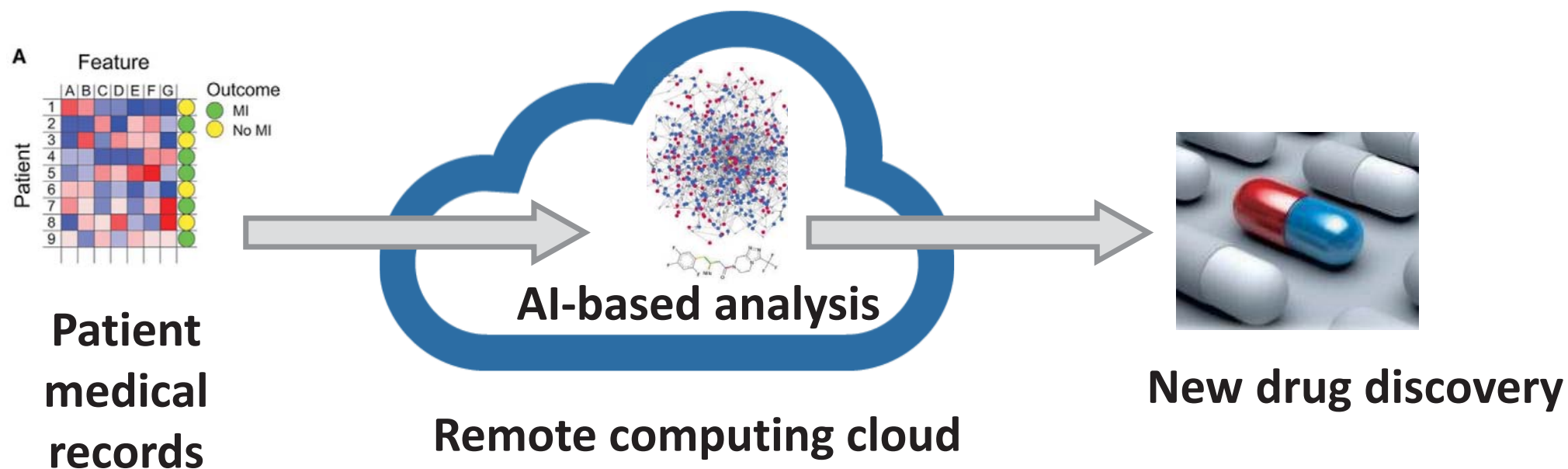


<https://www.edureka.co/blog/big-data-applications-revolutionizing-various-domains/>

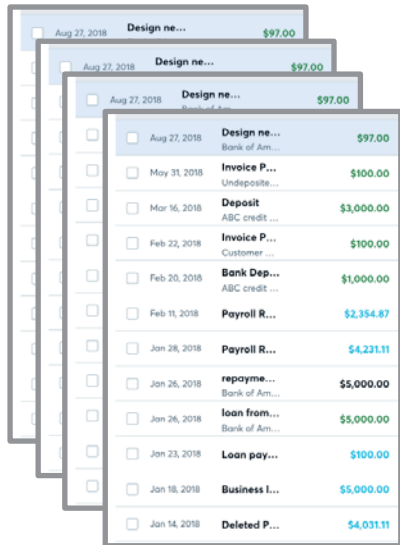
Frameworks for Big Data, AI, ML, and DL



Frameworks for Big Data, AI, ML, and DL



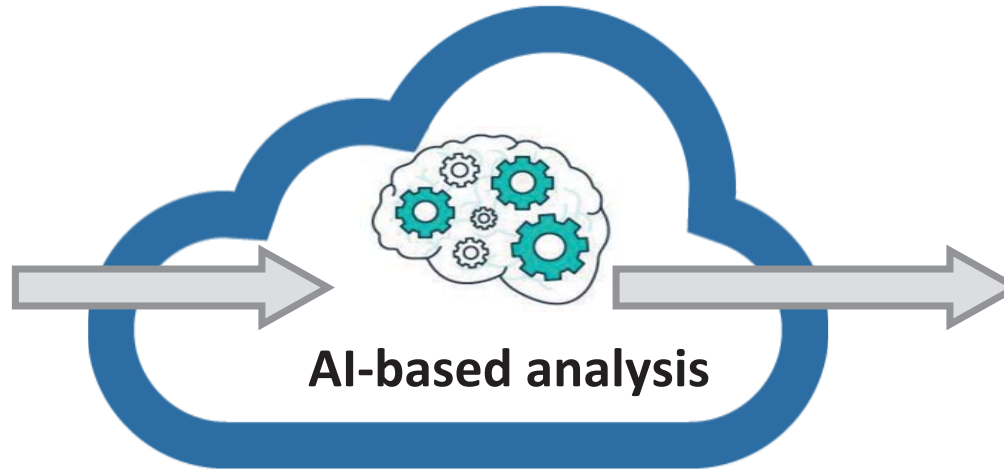
Frameworks for Big Data, AI, ML, and DL



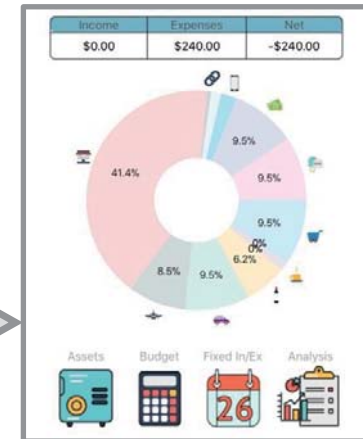
A stack of three overlapping screenshots of a bank transaction record. The top record shows a list of transactions with columns for date, description, and amount. The transactions include 'Design ne...', 'Invoice P...', 'Deposit', 'Bank Dep...', 'Payroll R...', 'repayme...', 'loan from...', 'Loan pay...', 'Business I...', and 'Deleted P...'.

Date	Description	Amount
Aug 27, 2018	Design ne...	\$97.00
Aug 27, 2018	Design ne...	\$97.00
Aug 27, 2018	Design ne...	\$97.00
Aug 27, 2018	Design ne...	\$97.00
Aug 27, 2018	Design ne...	\$97.00
May 31, 2018	Invoice P...	\$100.00
Mar 16, 2018	Deposit	\$3,000.00
Feb 22, 2018	Bank Dep...	\$100.00
Feb 20, 2018	Bank Dep...	\$1,000.00
Feb 11, 2018	Payroll R...	\$2,354.87
Jan 28, 2018	Payroll R...	\$4,221.11
Jan 26, 2018	repayme...	\$5,000.00
Jan 26, 2018	loan from...	\$5,000.00
Jan 23, 2018	Loan pay...	\$100.00
Jan 18, 2018	Business I...	\$5,000.00
Jan 14, 2018	Deleted P...	\$4,031.11

**Bank transaction
record**

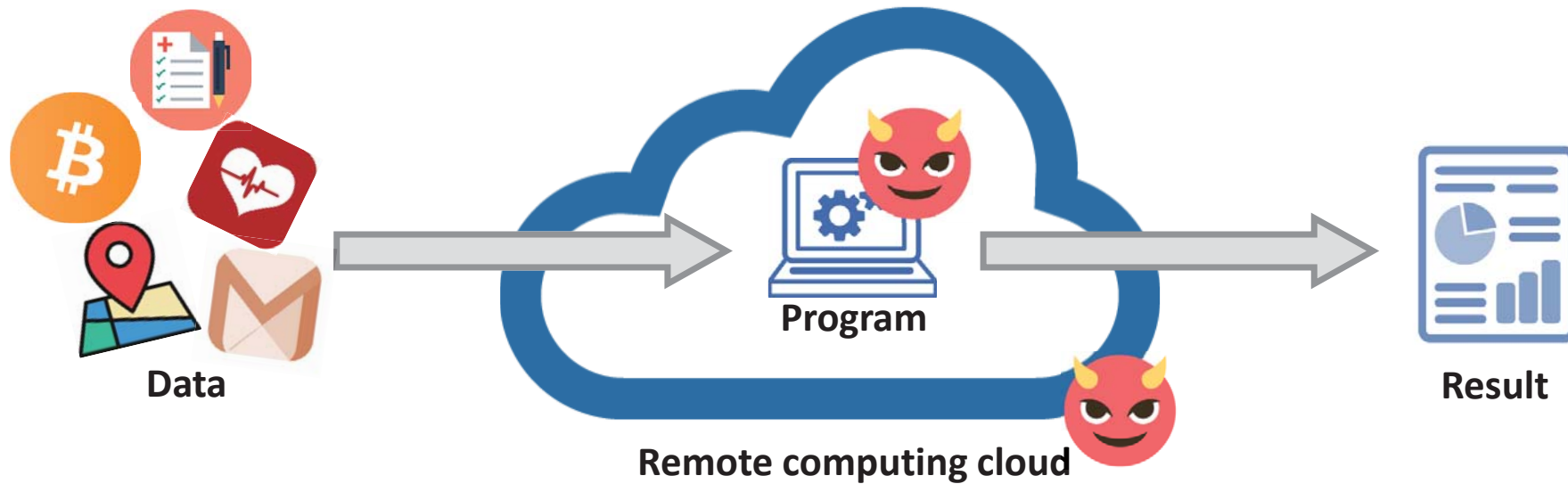


Remote computing cloud



**Account book summary
with recommendation**

Security and Privacy Threats



Data anarchy: Users have no control over their data

Challenges: Too strong attack models

- A program (or program owners) can be malicious
 - A program may promise it would not abuse the data, but there's no technical enforcement

고객님
환영합니다!

스타벅스커피 코리아는 회원님의 개인정보를 안전하게 보호하고 취급합니다.

☐ 약관 전체동의

☒ 이용약관 동의(필수) >

☒ 개인정보 수집 및 이용동의(필수) >

☐ E-mail 및 SMS 광고성 정보 수신동의(선택)
다양한 프로모션 소식 및 신규 매장 정보를 보내 드립니다.

다음

개인정보 제3자 제공 동의
(주)스타벅스커피 코리아는 회원님의 개인정보를 안전하게 취급하는데 최선을 다합니다.

제공받는 자: [redacted] 서비스

제공받는 목적: [redacted]

보유기간: 서비스 탈퇴시 지체없이 파기

제공되는 개인정보 항목
선택 정보는 동의를 거부하시는 경우에도 서비스 이용이 가능합니다.

[필수] 프로필 정보(닉네임/프로필 사진)

서비스 접근 권한
앱의 기능을 사용하기 위해서는 아래의 접근권한을 가질 수 있습니다.

[필수] 카카오톡리 글 목록, 카카오톡리 글 작성

동의안함 동의

특별검역 신고

* 여권번호 (Passport No.)
여권번호를 입력 해 주세요.

* 최근 14일 이내 방문하거나 실거주한 구역을 선택하세요.
(Please select the Region you have visited or actually lived in the last 14 days.)
방문 혹은 거주 한 적 없음

* 휴대전화 번호 (Phone Number)
본인 전화번호 인증

한국에서 연락 가능한 지인 전화번호
하이픈(-)을 제외하고 숫자로만 입력 해 주세요.

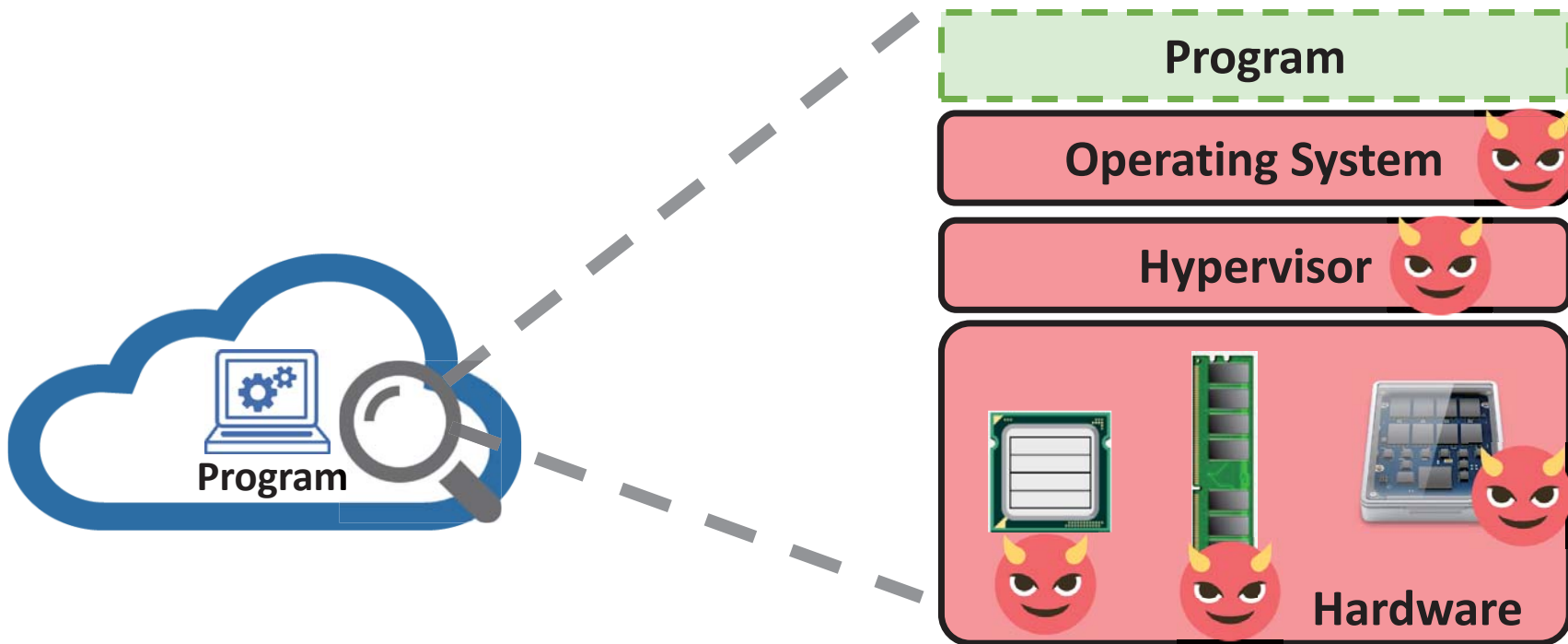
한국 내 학교명 (Name of School in Korea)
학교명을 입력해주세요.

* [감염법] 제15조, 제17조 및 [감염병예방법] 제49조, 제76조의 2에 따른 감염병 예방 및 감염 전파의 차단을 위해 [개인정보보호법] 제23조의 건강정보 및 [위치정보의 보호 및 이용 등에 관한 법률] 제15조의 위치정보가 포함된 개인정보의 제공 및 활용에 동의합니다.
자세히 보기

완료

Challenges: Too strong attack models

- Cloud infrastructures can be malicious
 - Clouds include entire computing infrastructure to run a program
 - If any of those is malicious, user's data can be leaked



Challenges: Too strong attack models

- Clouds can be malicious
 - Physical attacks make this problem even more challenging
 - System admins can easily pull out the disk to read the data



Challenges: Too strong attack models

- Clouds can be malicious
 - Cold-boot attack: Even DRAM's data can be stolen

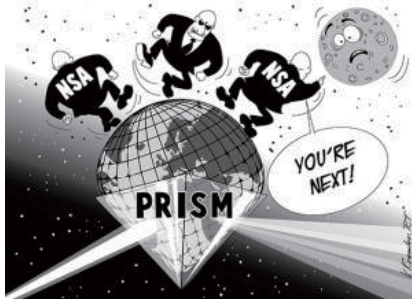


-50°C: less than 0.2% decay after 1 minute

“Lest We Remember: Cold Boot Attacks on Encryption Keys [USENIX Security 08]”

Fundamental Issue: Data Utility vs. Data Privacy

- **Data utility**
 - Data is the key to truly enable AI/ML/DL services
- **Data privacy**
 - Data contains critical privacy information of users
- How to satisfy both **data utility** and **data privacy**?



**코로나19(COVID-19) 관련
개인정보 불법유포
이렇게 대응하고 있습니다!**

	개인정보 불법 유포 집중 모니터링
	탐지된 개인정보는 정보통신망법에 따라 사업자와 협력하여 삭제 조치 <small>정보통신망법 제 23조(정보주체의 권리) 제 2항(정보주체의 권리 행사에 따라)</small>
	개인정보 법령 위반사항이 발견되면 수사기관에 수사요청

코로나19(COVID-19) 관련 공개된 정보를 제외한
특정한 개인을 알아볼 수 있는 **개인정보를 유포**하는 행위는
사생활 침해로 **민·형사상 처벌**을 받을 수 있으므로
각별한 주의가 필요합니다!

방송통신위원회 경찰청

Potential Solutions for Data Security

- Data anonymization (데이터 비식별화)
- Differential Privacy (차등보호)
- Homomorphic Encryption (동형암호)
- **Hardware-Assisted Trusted Computing (신뢰계산)**
 - **The most efficient: near to native execution speed**
 - **The most practical: running a generic program**

Data Anonymization (데이터 비식별화)

- Remove personally identifiable information from data
 - While maintaining the data utilization
- k-anonymity
 - Blend each data item with k-1 items having identical column information

microdata

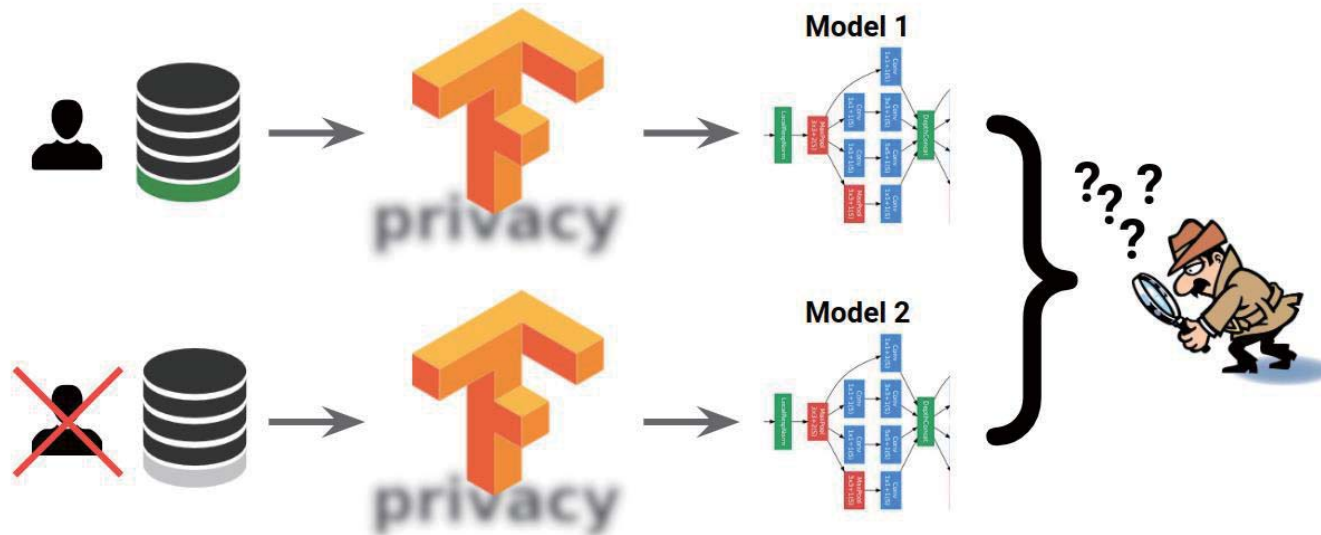
id	Zipcode	Sex	National.	Disease
1	13053	28	Russian	Heart Disease
2	13068	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease
7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

4-anonymous data

id	Zipcode	Sex	National.	Disease
1	130**	<30	*	Heart Disease
2	130**	<30	*	Heart Disease
3	130**	<30	*	Viral Infection
4	130**	<30	*	Viral Infection
5	1485*	≥40	*	Cancer
6	1485*	≥40	*	Heart Disease
7	1485*	≥40	*	Viral Infection
8	1485*	≥40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

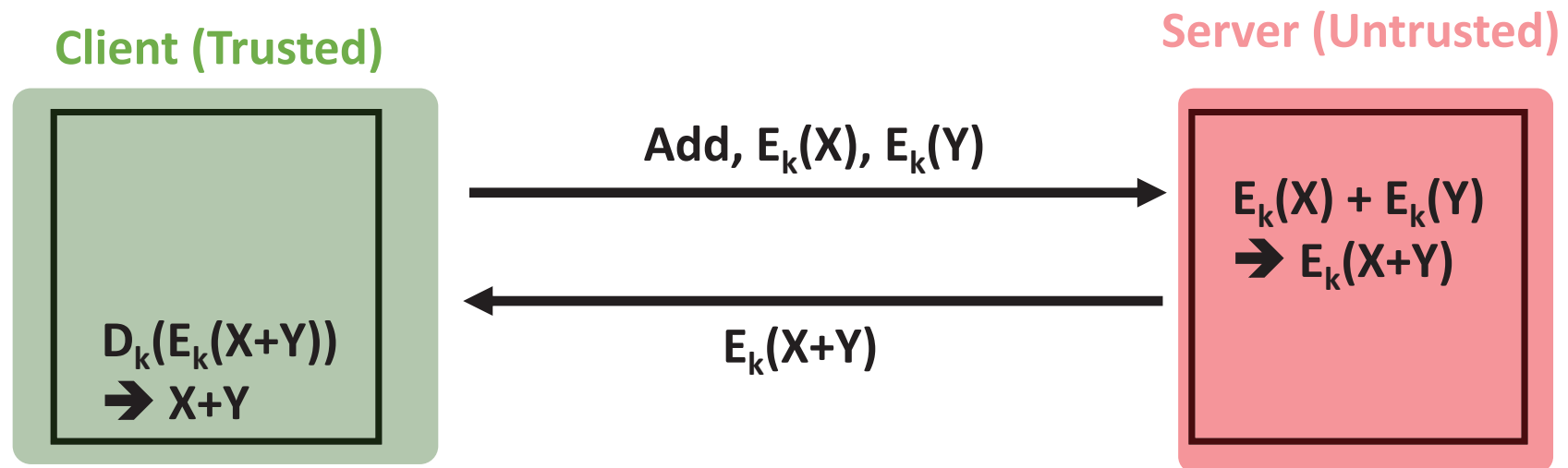
Differential Privacy (차등보호)

- Privacy protection algorithm for a statistical database
- Differential private
 - An observer seeing the output cannot tell if a particular individual's information was used in generating the output



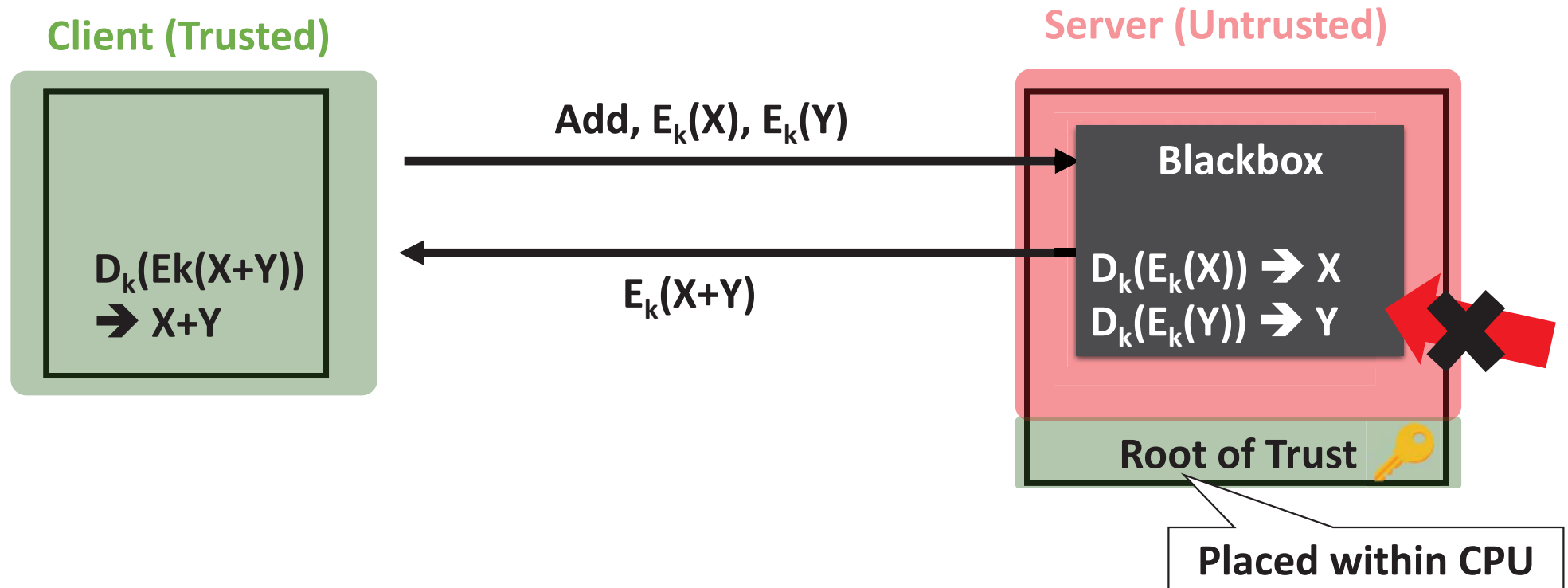
Homomorphic Encryption (동형암호)

- Computation over encrypted data
 - Example: Client wants to offload the computation, $X+Y$



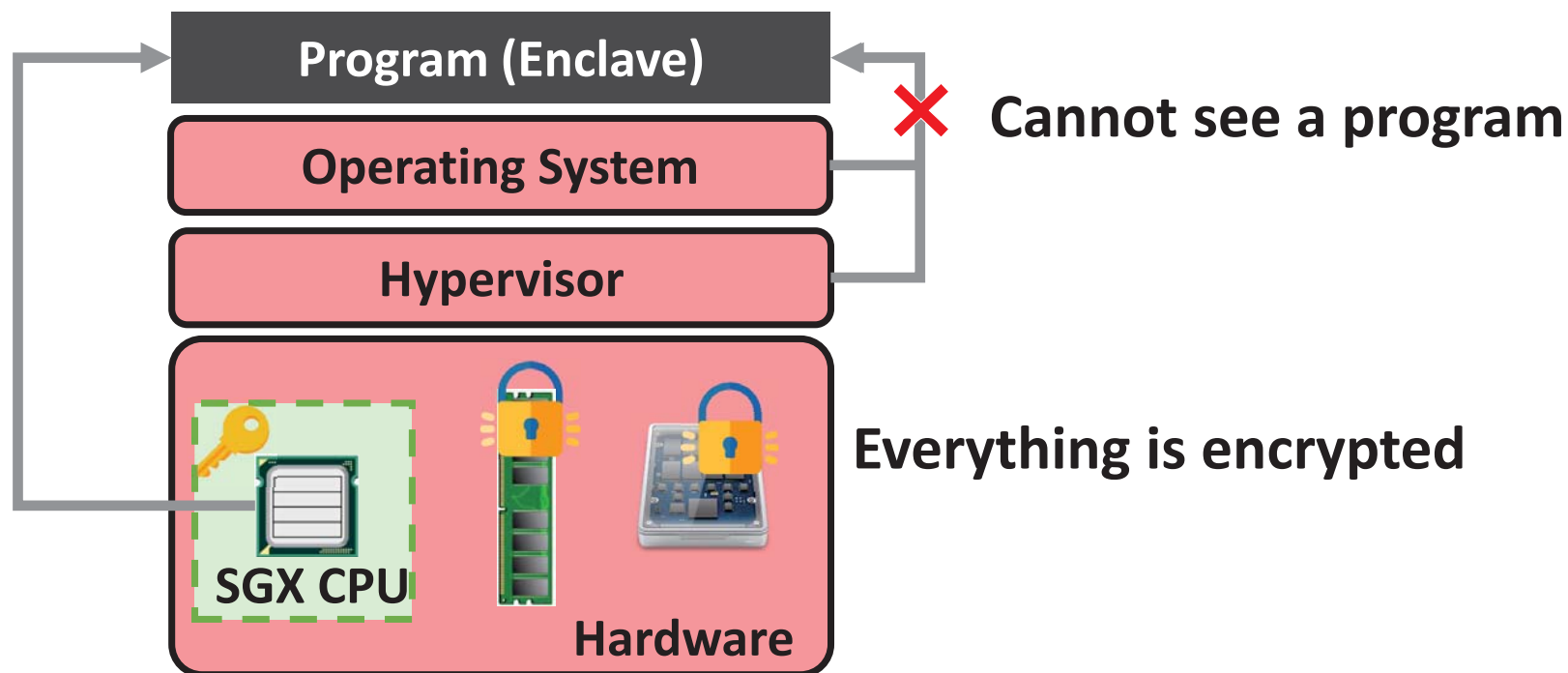
Hardware-Assisted Trusted Computing (신뢰계산)

- Trusted computation by placing a small root of trust in hardware



Intel SGX: Data Security Feature for the Future

Hardware-protected execution region



Most Intel CPUs today are shipped with SGX support.

Intel SGX: already market available

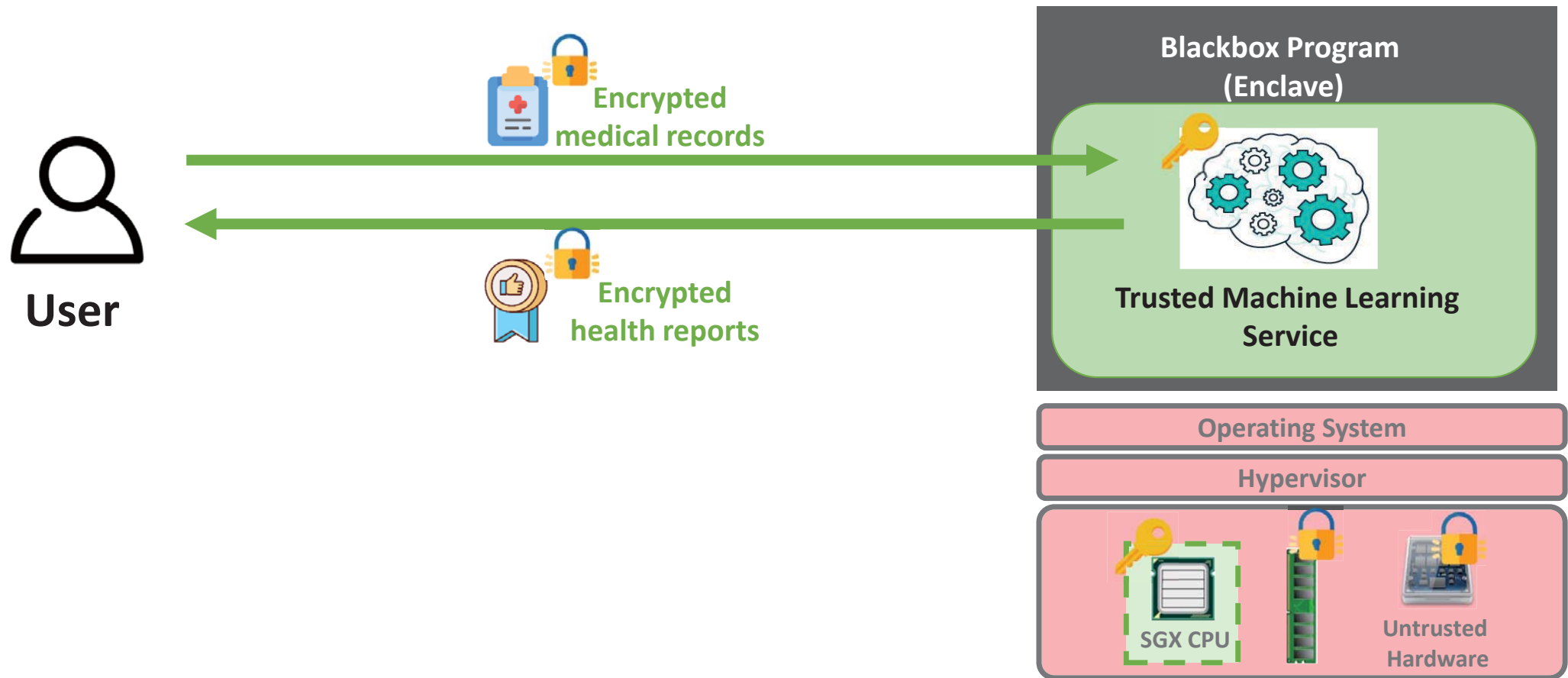
- Most of consumer-grade Intel CPUs are shipped with SGX support
- Strong demands on SGX features from cloud providers
 - Growing security needs for trusted computing
 - Observing EU GDPR and any (expected) national regulation
 - Azure Confidential Computing is already available (since 2020 May)
 - SGX-based secure cloud services



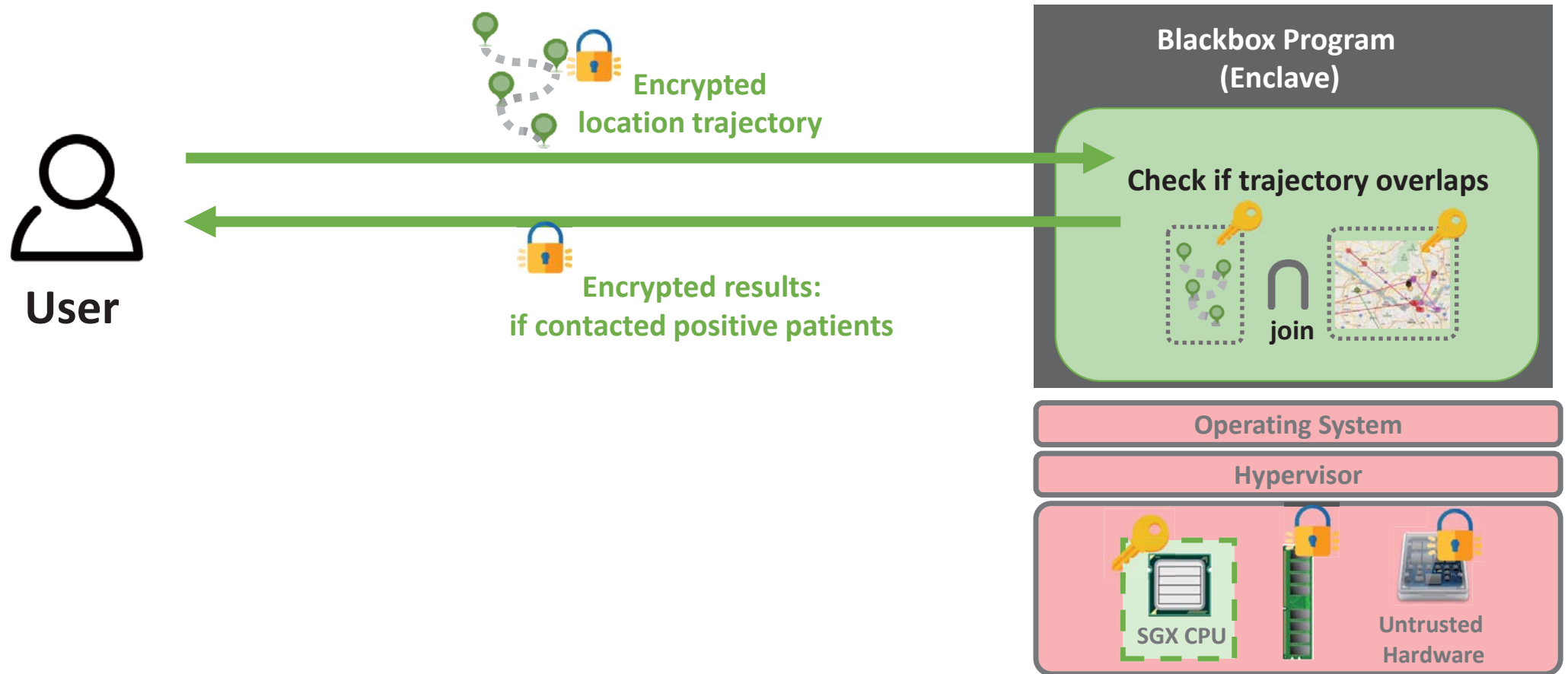
Truly Secure Applications with Intel SGX

- Trusted Machine Learning
 - 예제: 안전한 AI 기반 건강관리 서비스
- Trusted Private Join
 - 예제: 개인정보를 보호하는 코로나바이러스 환자 동선 확인
- Trusted Network Middleware/Server
 - 예제: 안전한 화상회의 아키텍처 (Zoom, Google Meet)

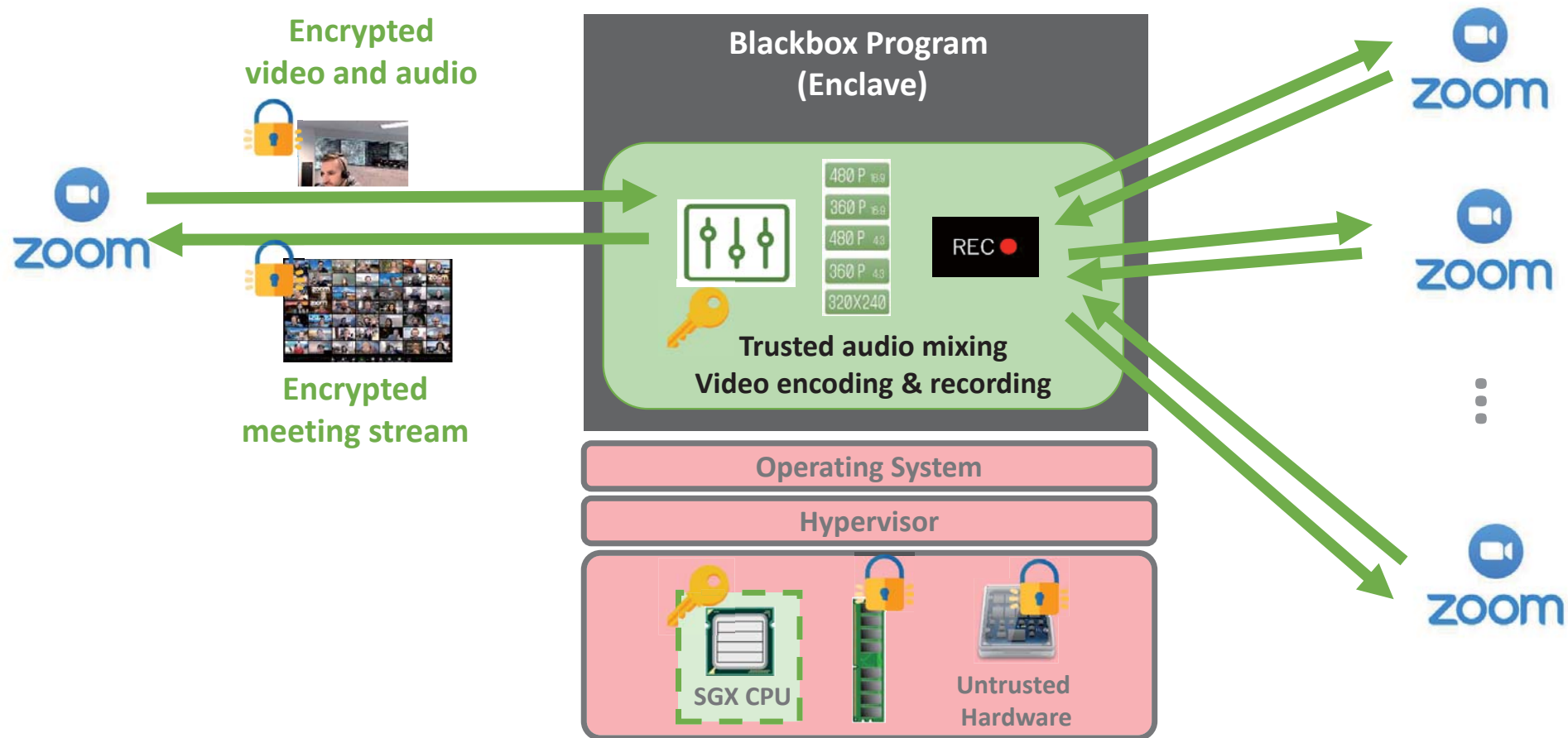
Trusted Machine Learning: Health Prediction



Trusted Private Join: Covid-19 Proximity Check



Trusted Network Server: Trusted Online Meeting



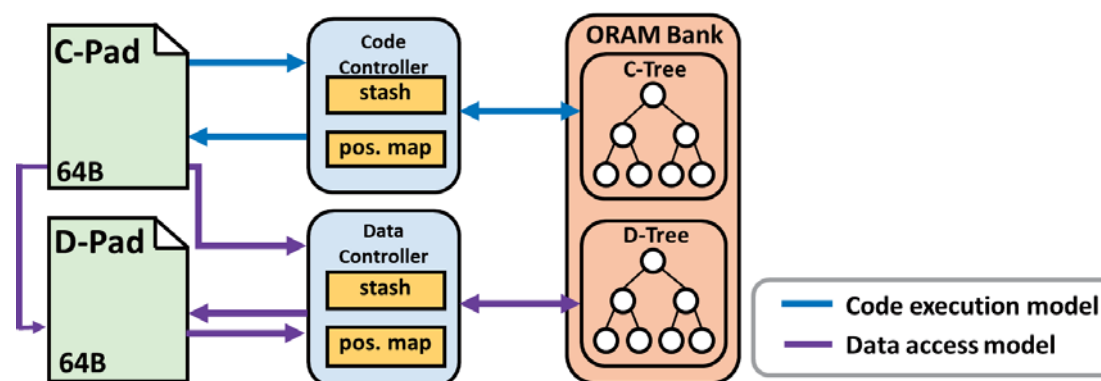
Side-Channel Resistant Intel SGX

- **Obliviate [NDSS 2018]**

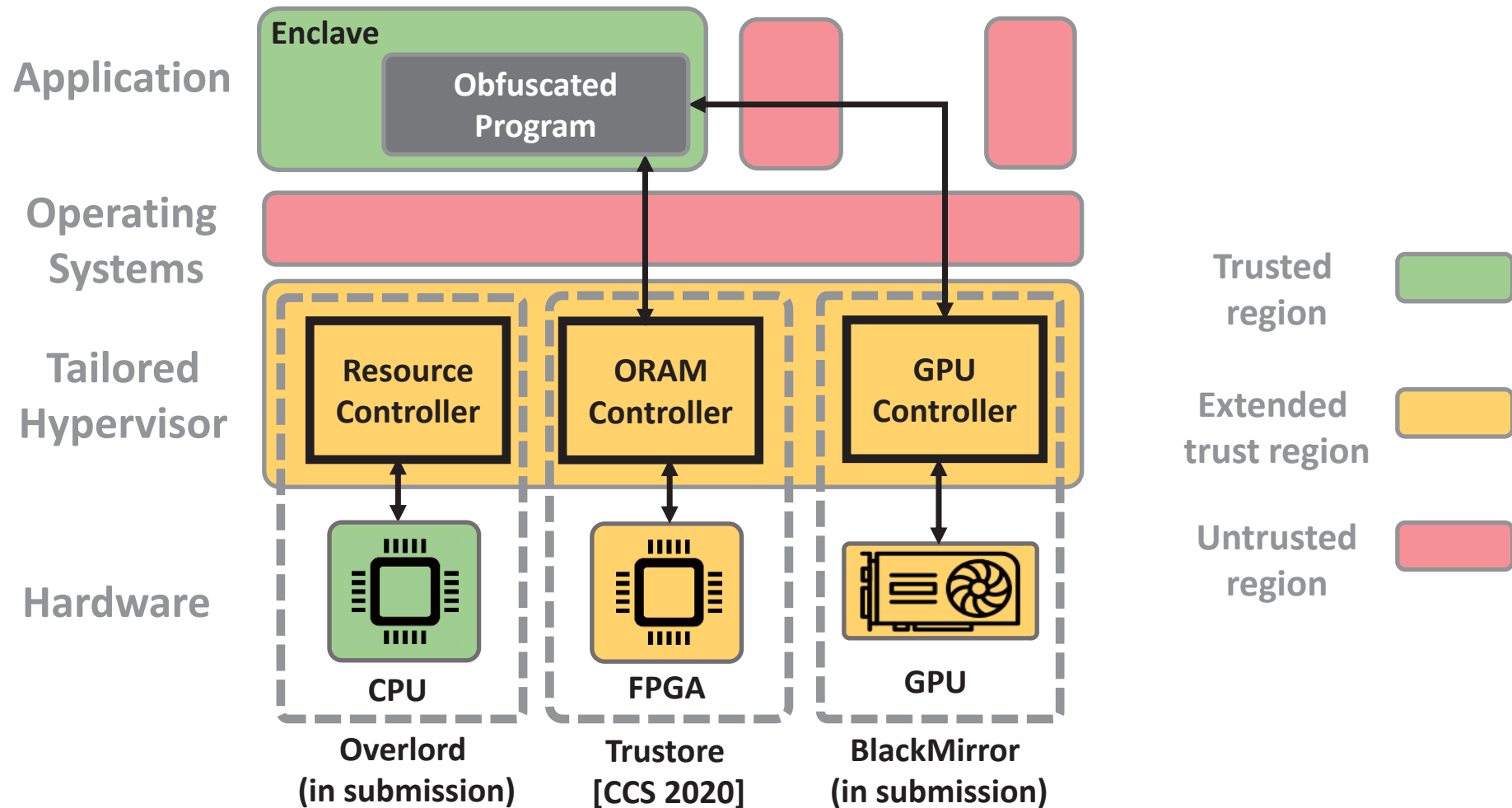
- ORAM-based file systems to prevent side-channel attacks
- All file accesses are performed with ORAM

- **Obfuscuro [NDSS 2019]**

- Program obfuscation on Intel SGX
- All programs always exhibit the same control/data flows (using ORAM)



Enabling Practical Services for Intel SGX



Conclusion

- Protecting the data is crucial in the age of big data
- Trusted computing opens up new opportunities towards truly secure services
 - With systematic and technical security assurance

감사합니다

서울대학교 전기정보공학부
이병영
byoungyoung@snu.ac.kr