Poster: Hall E #930

Low-Complexity Deep Convolutional Neural Networks on Fully Homomorphic Encryption Using Multiplexed Parallel Convolutions

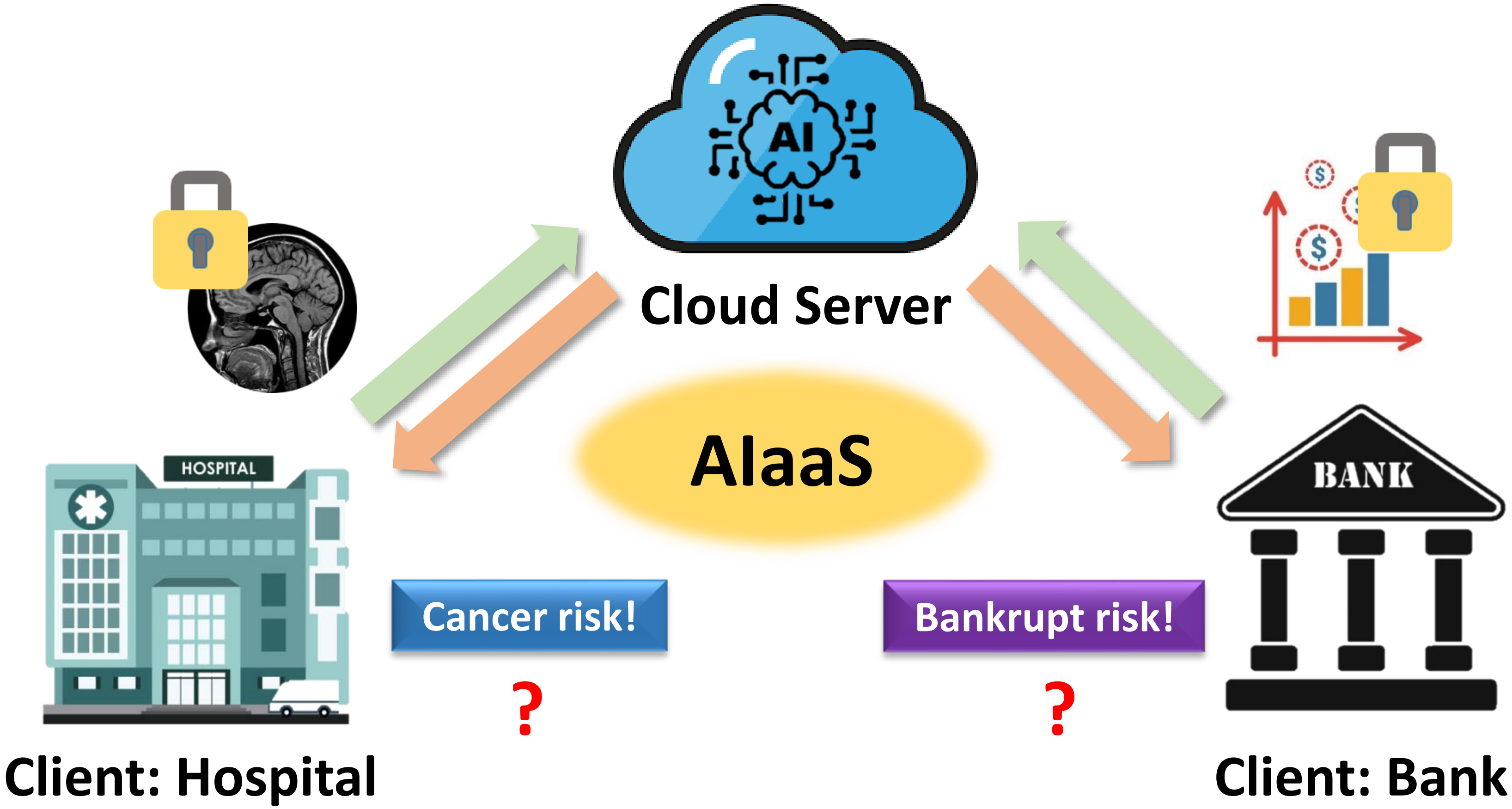
Eunsang Lee, **Joon-Woo Lee***, Junghyun Lee, Young-Sik Kim,
Yongjune Kim, Jong-Seon No, Woosuk Choi

Daegu Gyeongbuk
Institute of Science & Technology

SAMSUNG

ICML
International Conference
On Machine Learning

Motivation: Artificial Intelligence as a Service (AIaaS)



Cloud Server

AIaaS

Cancer risk!

?

Bankrupt risk!

?

Client: Hospital

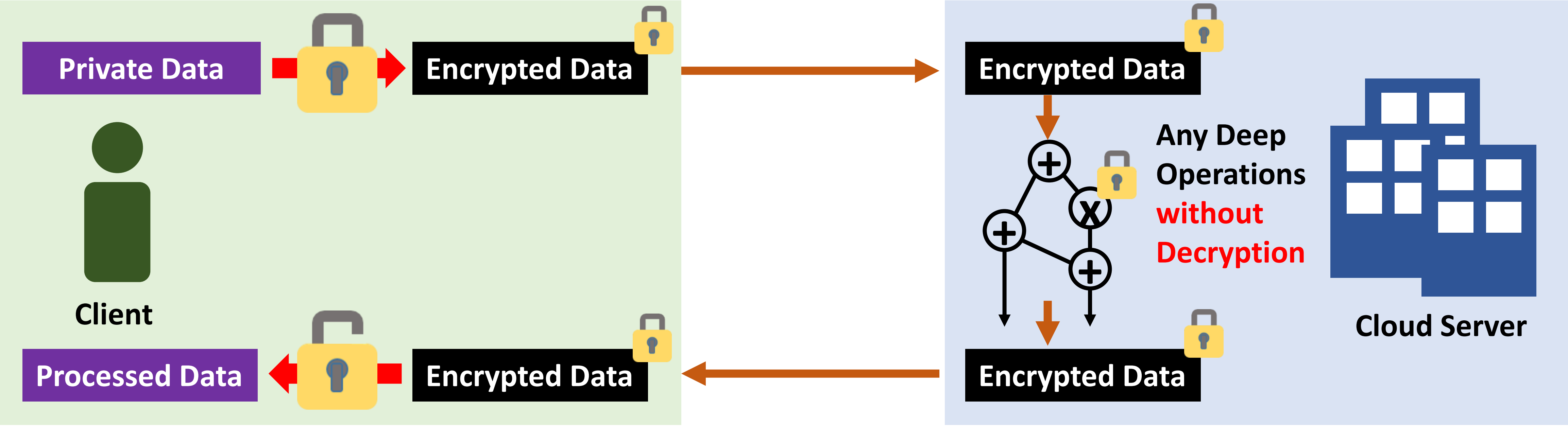
Client: Bank

Security problem in AIaaS is important!

Main Concept: Fully Homomorphic Encryption (FHE)

✓ Cryptographic system supporting unlimited addition and multiplication on encrypted data

Privacy-Preserving AIaaS on FHE



Private Data

Encrypted Data

Client

Processed Data

Encrypted Data

Encrypted Data

Any Deep Operations without Decryption

Encrypted Data

Cloud Server

✓ **We focus on convolutional neural networks (CNNs) on FHE!**

Previous Works about CNN on FHE

HE-friendly Network

(2016 ~)

- Modified CNNs to suit basic FHE operations
- Only shallow networks (3 ~ 11 layers)
- ReLU, ELU, GeLU → Low-degree polynomial (e.g., x^2)
- No effective models for advanced datasets (e.g., ImageNet)

Pretrained Network

(2022 ~)

(Lee et al., 2022)

- No modification of CNNs (ResNet model)
- ReLU activation function
- Well-known to be effective for advanced datasets
- **Only ResNet-20 yet**
- **High latency & Considerable computing resources**
  - **3 hours per image with 64 threads**

Main Question

Is it really possible to realize **deep neural networks** on **FHE** by using the **pretrained standard models** such as **ResNet-110**?

NOT YET IMPLEMENTED!

Two Main Techniques for Deep CNN on FHE

First Technique

- **Problem:** Too much runtime and too many computation resources (3h w/ 64 thread)
  → Multiplexed Parallel Convolution
- **Improved to 40 min w/ single thread (x134 reduced!)**

Second Technique

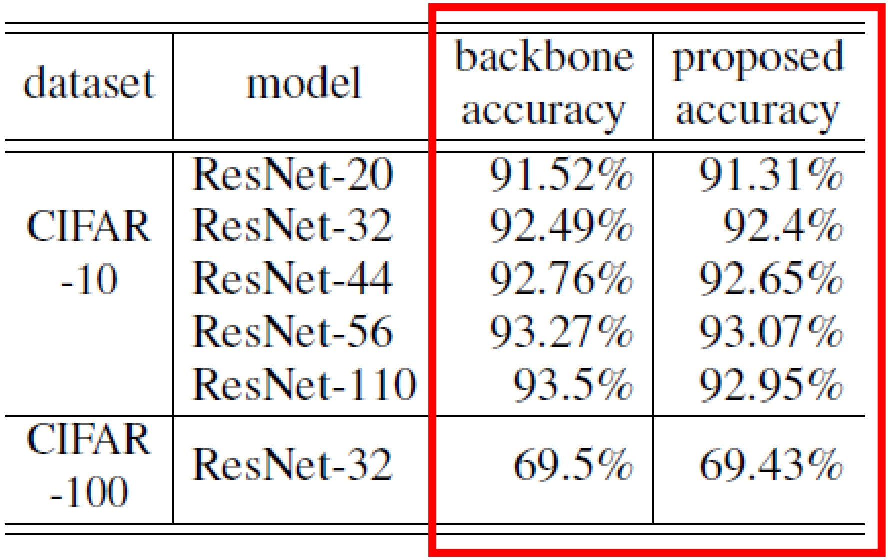
- **Problem:** Catastrophic divergence in ReLU function of deep CNN with probability 25%
  → Imaginary-Removing Bootstrapping
- **The divergence problem is completely removed even in deep CNN!**

ICML
International Conference
On Machine Learning

Result: Almost the Same Accuracy as the Backbone Network

Original AI model

Privacy-preserving AI model



dataset	model	backbone accuracy	proposed accuracy
CIFAR -10	ResNet-20	91.52%	91.31%
	ResNet-32	92.49%	92.4%
	ResNet-44	92.76%	92.65%
	ResNet-56	93.27%	93.07%
	ResNet-110	93.5%	92.95%
CIFAR -100	ResNet-32	69.5%	69.43%

Classification accuracy of ResNet models

First implemented!

Deep CNNs on FHE with same classification accuracy! (~110 layers!)

Is it really possible to realize **deep neural networks** on **FHE** by using the **pretrained standard models** such as **ResNet-110**?

→ **YES!**

Thank You!

More info: Hall E #930