Privacy-preserving Logistic Regression

Shiho Moriai, Le Trieu Phong
Security Fundamentals Laboratory
Cybersecurity Research Institute, NICT
JST CREST grant#:JPMJCR168A

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

Japan Science and Technology Agency

Outline

» Background

> Big Data Integration and Security & Privacy

> Our research project by JST CREST funding

> by Shiho Moriai

» Privacy-preserving Logistic Regression

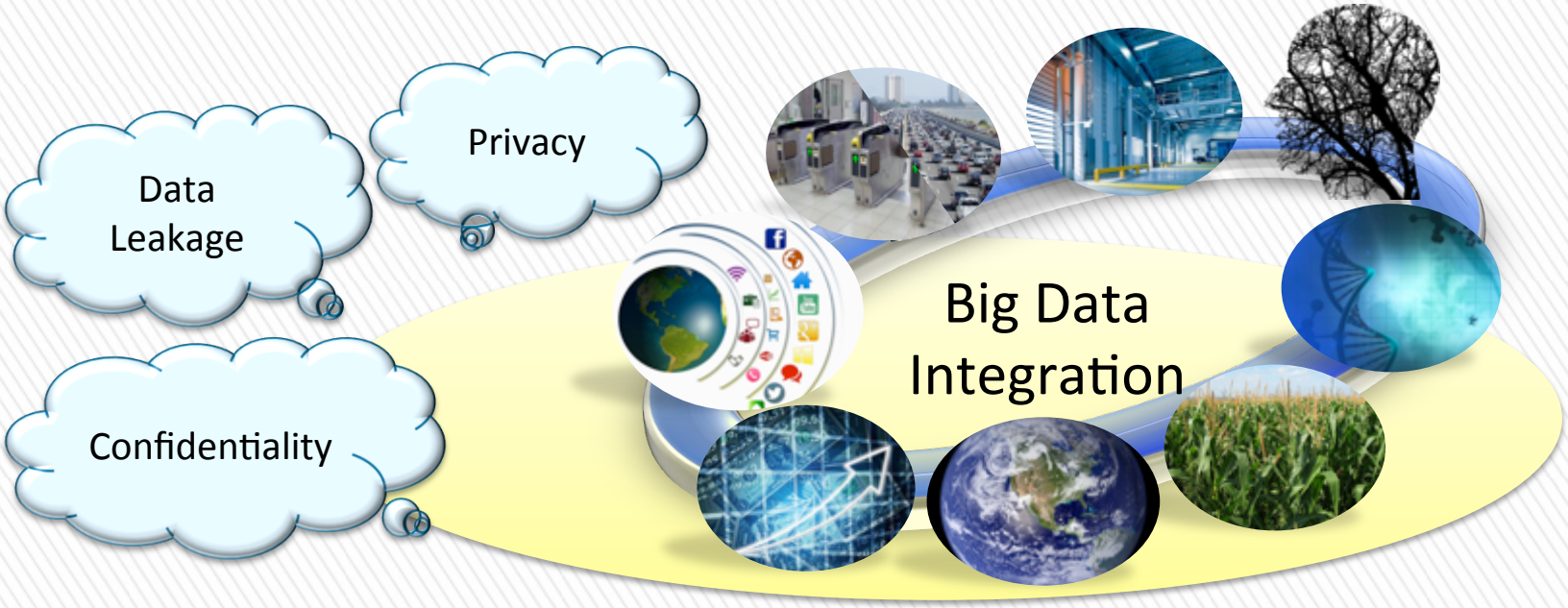
> Technical Details

> by Le Trieu Phong

Big Data Integration : Key to the new growth strategy

Security and Privacy: Key Issues for Datability

To Promote Big Data Integration across Sectors



Security and Privacy Enhancing Technologies

Data Analytics

While Encrypted/ Preserving Privacy

Create Value across Sectors
Innovation, Productivity, Growth

Japan Science and Technology Agency

CREST 戦略的創造研究推進事業 Core Research for Evolutionary Science and Technology

NICT

JST CREST Research Projects

» CREST is a funding program for team-oriented research with the aim of achieving the strategic goals set forth by the government.

» The objective is to create revolutionary technical seeds for science and technology innovation.

"Development and Integration of Artificial Intelligence Technologies for Innovation Acceleration" (2016～)

Research Supervisor: Minoru Etoh (Senior Vice President, General Manager of Innovation Management Department, NTT DOCOMO, INC.)

Call for applications (2016. 6)

Japan Science and Technology Agency

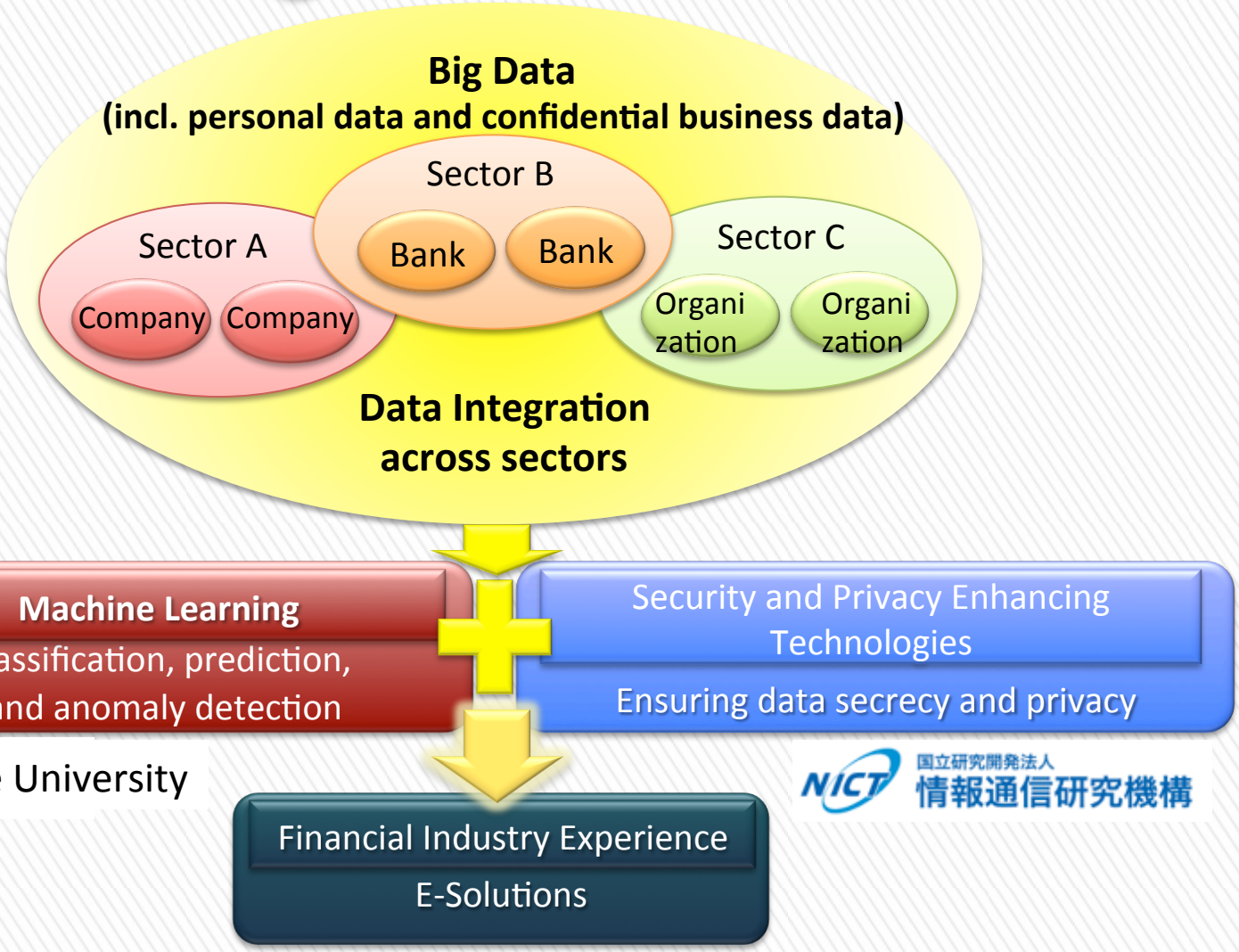
CREST 戦略的創造研究推進事業 Core Research for Evolutionary Science and Technology

NICT

“Privacy-preserving Data Analytics to Promote Cross-industry Data Sharing” (2016-)

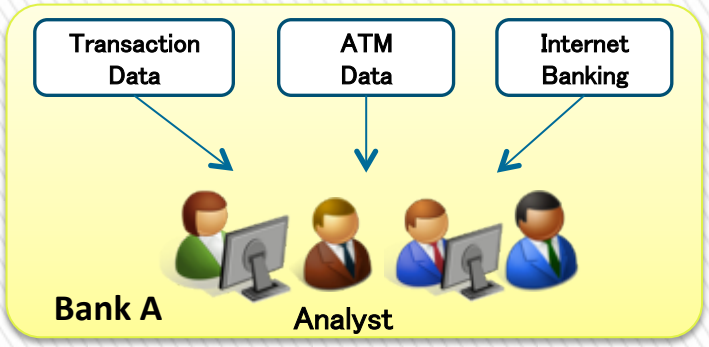
- Research Director：Shiho Moriai (NICT)
- Joint work with Seiichi Ozawa (Kobe Univ.) and Eltes Co., Ltd.
  - Integration of AI (Machine Learning) and Cryptography
  - Apply our research results to real problems in financial industry such as detecting illegal money transfers

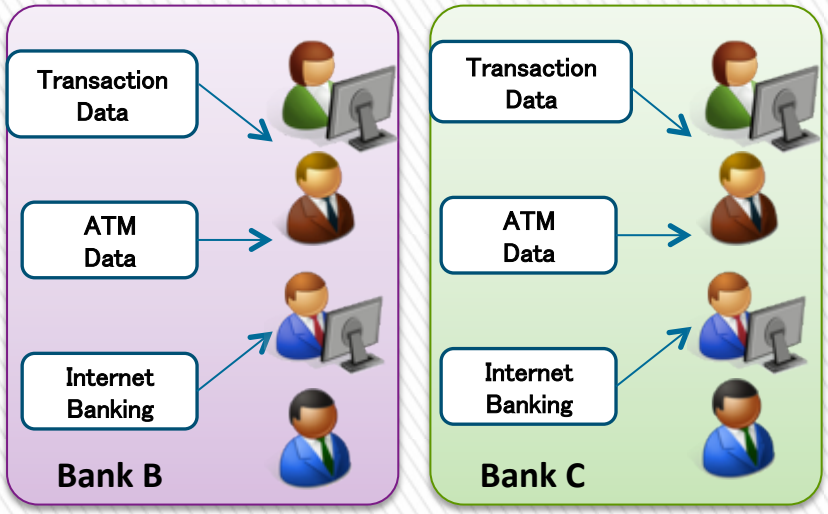
Research Organization



Current Status and Our Aims

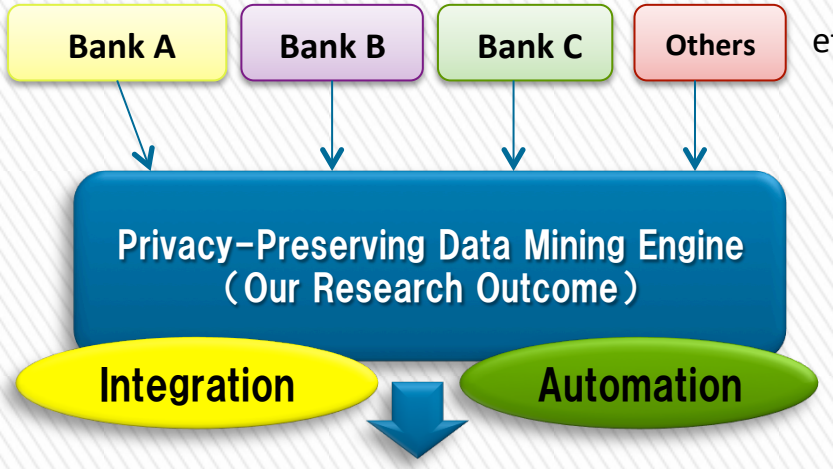
Current Status





Data is handled internally and separately

Our Aims



1) Anomaly Detection of Transaction
2) Decision of Interest Rate

- **Cost Reduction**
- **Human Mistake Avoidance**
- **Accuracy Improvement**
  - **Possible to detect more anomaly transaction !**

Privacy Preserving Data Analytics (1)

» SPHERE: Security-updatable Public-key Homomorphic Encryption with Rich Encodings (2015)

> **Homomorphic Encryption**

+ Computations over both binary strings and real numbers

> **Security-updatability**

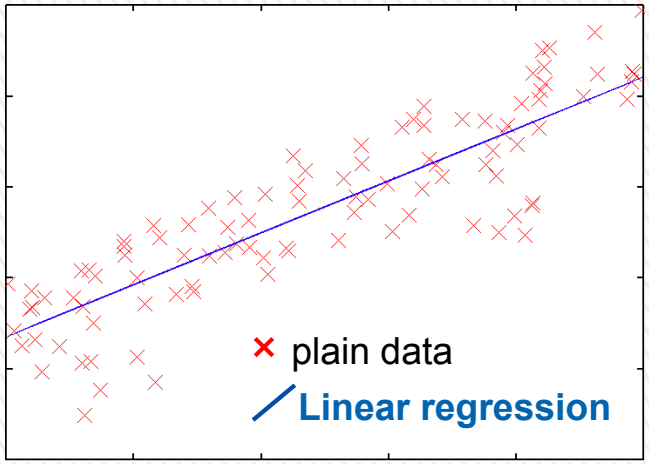
+ Change security level (key length) on encrypted data for long-term security

+ Security under the LWE assumption

Privacy Preserving Data Analytics (2)

> **Linear regression** using SPHERE can be computed efficiently* while data are encrypted.

* Compared to the best previous, our system reduces the server running time from about 8.75 hours to 10 minutes.

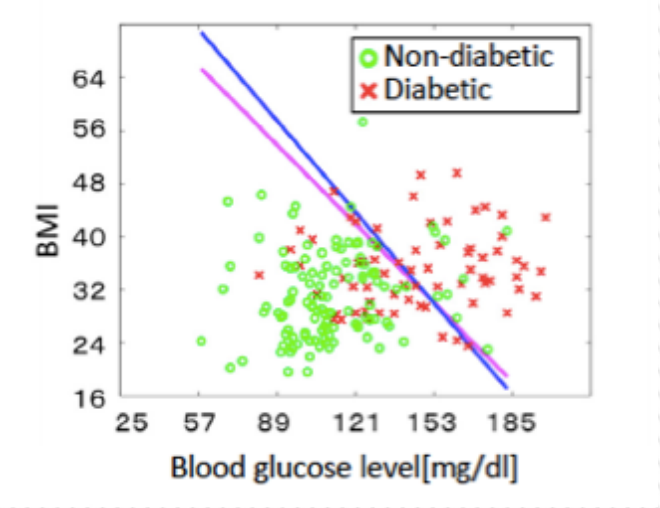


Privacy Preserving Data Analytics (3)

» **Logistic regression**

> powerful machine learning tool to classify data

» Proposed a secure system for protecting both the training and predicting data in logistic regression via homomorphic encryption.



Privacy Preserving Deep Learning

» Many learning participants perform neural network-based deep learning over a combined dataset of all, without revealing the participants' local data.

» Improve the previous work by Shokri and Shmatikov (ACM CCS 2015)

> local data may be leaked to the server