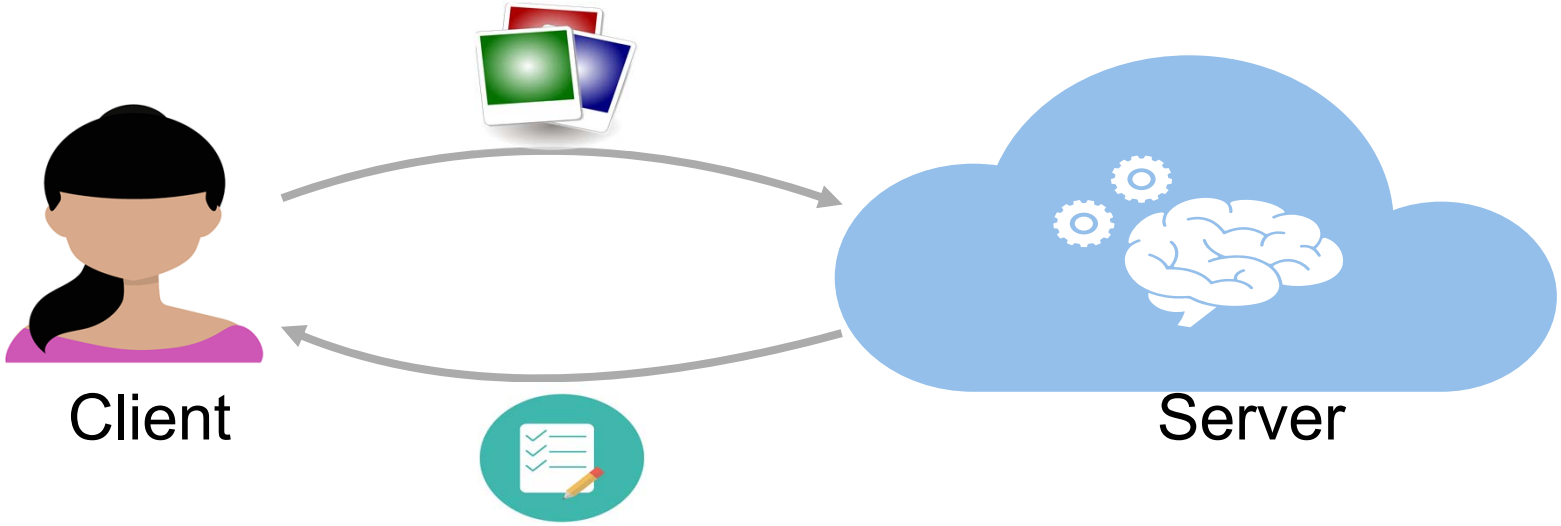
3iA Côte d'Azur
Institut interdisciplinaire d'intelligence artificielle

Melek Önen
AI & Security

EURECOM
https://www.eurecom.fr

Machine Learning as a Service (MLaaS)



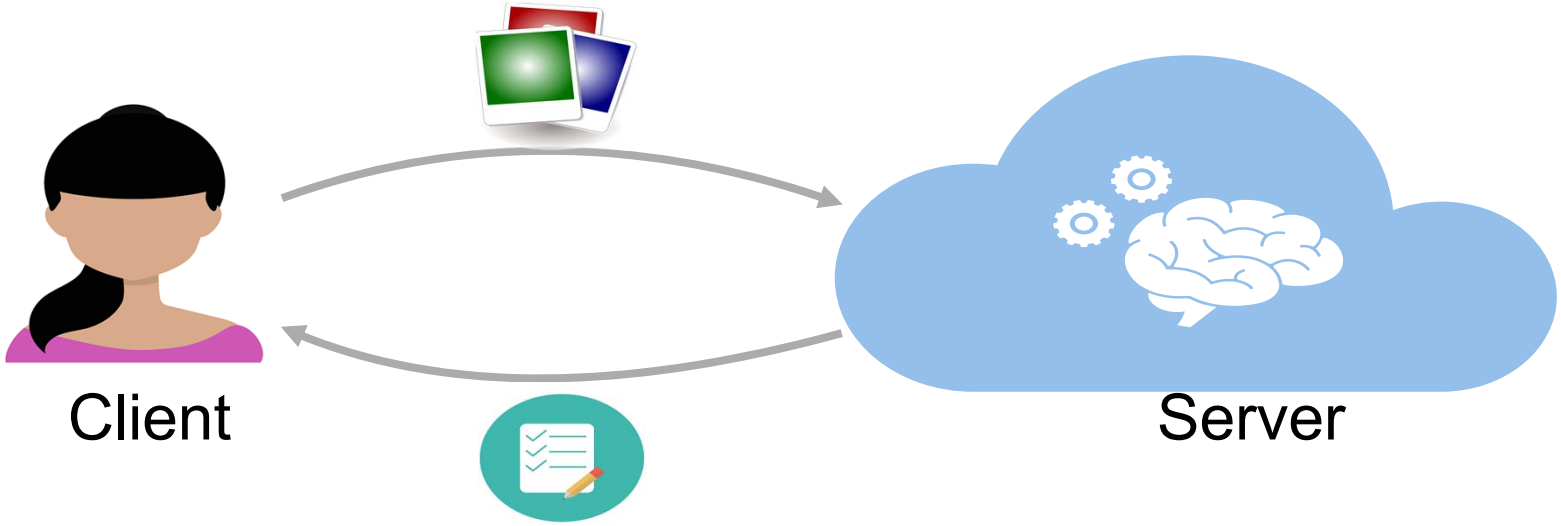
Performance

No need for ML knowledge

Cost reduction

EURECOM
Sophia Antipolis

Sensitive and Confidential Data



- Sensitive personal data
- Corporate data (IP)
- Intellectual property
- Legal restrictions

General Data Protection Regulation

EURECOM
Sophia Antipolis

Data Protection Tools

- Traditional PETs  **not adapted**

EURECOM
Sophia Antipolis

Data Protection Tools

- Traditional PETs  **not adapted**

- Advanced PETs
  - Homomorphic Encryption
  - Secure Multiparty Computation
  - Differential Privacy
  - Functional Encryption

EURECOM
Sophia Antipolis

Advanced Cryptographic tools

- Homomorphic encryption

$$\boldsymbol{Encrypt(m_1)\ op1\ Encrypt(m_2) = Encrypt(m_1 op2\ m_2)}$$

  - Partially HE: one operation only
  - Somewhat HE: arbitrary number of +, limited number of x
  - Fully HE: any function

- Two party computation

leak no other information than what Ideal model leaks

  - Yao's Garbled Circuits
  - Boolean sharing
  - Arithmetic sharing

EURECOM
Sophia Antipolis

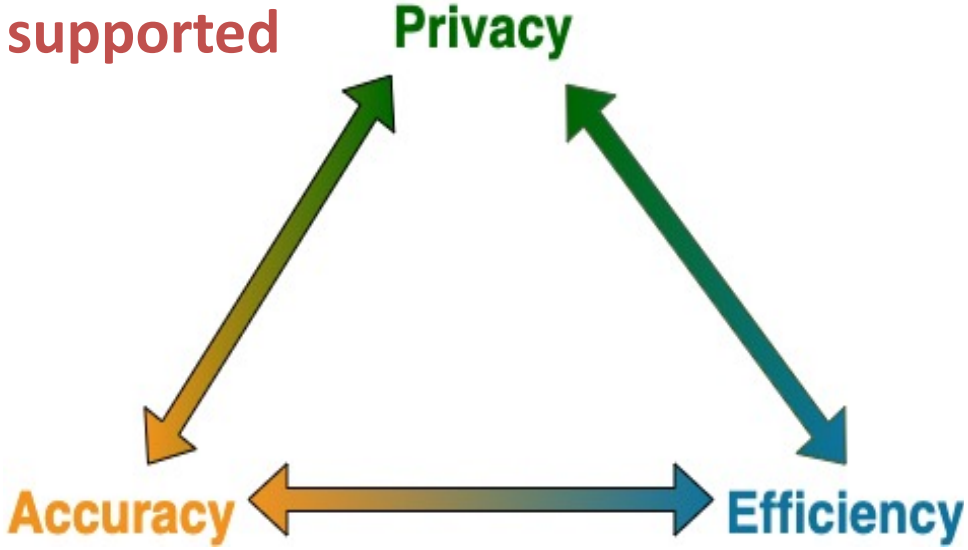
Data Protection Tools

- Traditional PETs → **not adapted**

- Advanced PETs
  - Homomorphic Encryption
  - Secure Multiparty Computation
  - Differential Privacy
  - Functional Encryption

- Additional overhead

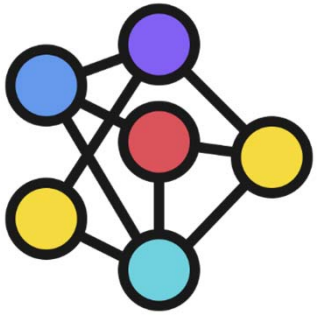
- Only some operations are supported



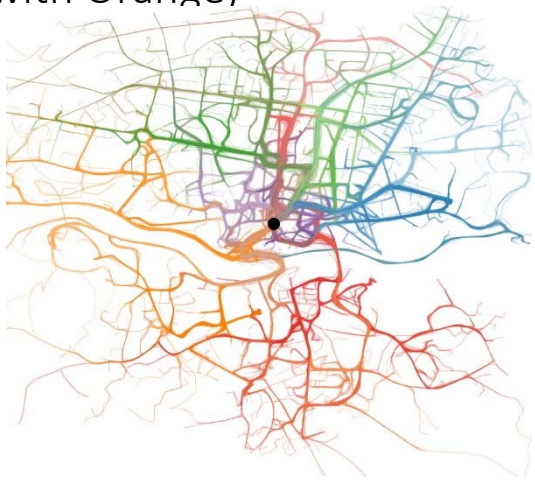
EURECOM
Sophia Antipolis

Privacy Preserving AI

- Neural Network classification (in collaboration with MediaClinics Italia)
  - With HE, with 2PC
  - Use Case: Arrhythmia detection



- Trajectory clustering (in collaboration with Orange)
  - With 2PC



EURECOM
Sophia Antipolis

PAPAYA
PlAtform for PrivAcY preserving data Analytics

Other topics

- Model Security (in collaboration with SAP)
  - ML watermarking
  - Study of different attacks

EURECOM
Sophia Antipolis

Other topics

- Model Security (in collaboration with SAP)
  - ML watermarking
  - Study of different attacks

- PETs as an attack tool (A. Ünsal)
  - Differential privacy vs. Adversarial learning

EURECOM
Sophia Antipolis

References

- Azraoui, Monir; Bahram, Muhammad; Bozdemir, Beyza; Canard, Sébastien; Ciceri, Eleonora; Ermis, Orhan; Masalha, Ramy; Mosconi, Marco; Önen, Melek; Paindavoine, Marie; Rozenberg, Boris; Vialla, Bastien; Vicini, Sauro, SoK: Cryptography for neural network, IFIP Summer School on Privacy and Identity Management, 18-23 August 2019, Brugg Windisch, Switzerland
- Mansouri, Mohamad; Bozdemir, Beyza; Önen, Melek; Ermis, Orhan, PAC: Privacy-preserving Arrhythmia Classification with neural networks, FPS 2019, 12th International Symposium on Foundations and Practice of Security, November 5-7, 2019, Toulouse, France / Also published in LNCS, Vol. 12056
- Tillem, Gamze; Bozdemir, Beyza; Önen, Melek, SwaNN: Switching among cryptographic tools for privacy-preserving neural network predictions, SECRYPT 2020, 17th International Conference on Security and Cryptography, 8-10 July 2020,
- Bozdemir, Beyza; Ermis, Orhan; Önen, Melek, ProteiNN: Privacy-preserving one-to-many Neural Network classifications, SECRYPT 2020, 17th International Joint Conference on Security and Cryptography, 8-10 July 2020, Lieusaint-Paris, France (Online conference)
- Lounici, Sofiane; Negri, Carlo Maria; Rosa, Marco; Trabelsi, Slim; Önen, Melek, Optimizing leak detection in open-source platforms with machine learning techniques, ICISSP 2021, 7th International Conference on Information Systems Security and Privacy, 11-13 February 2021

EURECOM
Sophia Antipolis

Thank you!

melek.onen@eurecom.fr

EURECOM
Sophia Antipolis