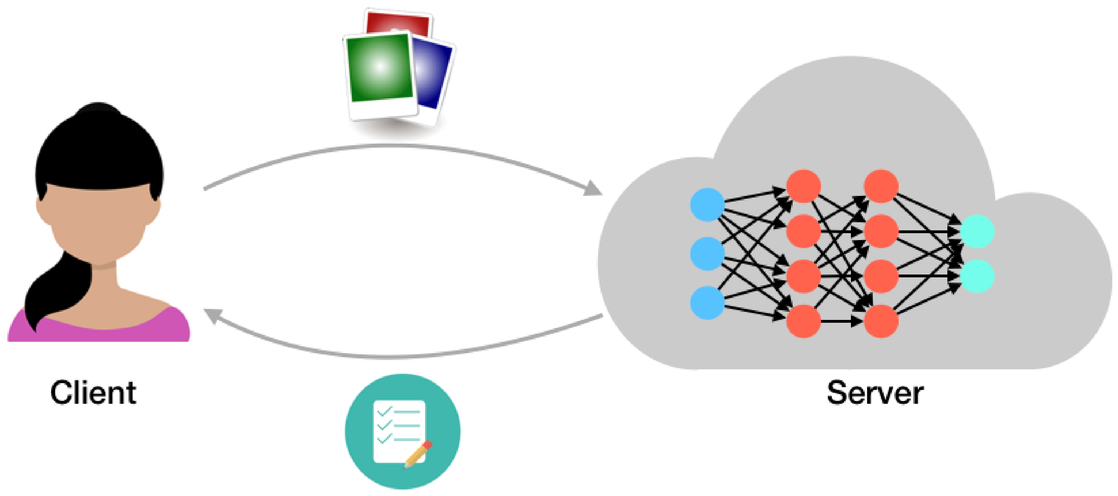
Private Neural Network Predictions

Gamze Tillem[1], Beyza Bozdemir[2], Melek Önen[2]

[1]Cyber Security Group, Delft University of Technology, The Netherlands
[2]Digital Security Group, EURECOM, France

Machine Learning as a Service



Challenges

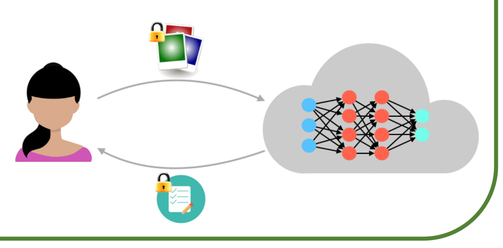
- Efficiency
- Accuracy
- Privacy
  - Sensitive personal data
  - Intellectual property
  - Legal restrictions

General Data Protection Regulation

Privacy-Preserving Machine Learning as a Service – Existing solutions

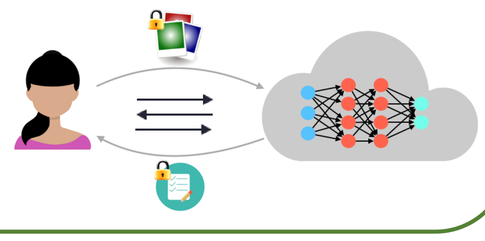
via Homomorphic Encryption

- Allows computations on ciphertexts without decryption
- Lower prediction accuracy
- High computation cost

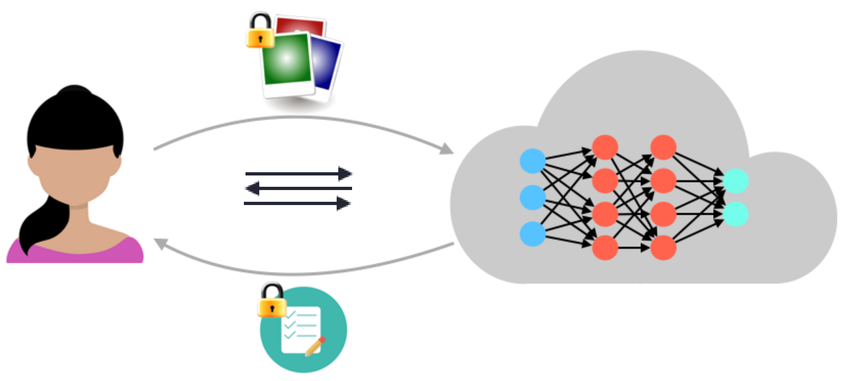


via Secure Two-party Computation

- Allows to jointly compute a function without revealing individual inputs.
- Higher prediction accuracy
- Lower computation cost
- Higher bandwidth usage



Our Proposal: A Hybrid Protocol for Private Neural Network Predictions

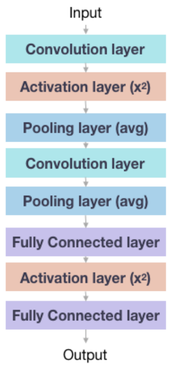


- Uses both homomorphic encryption and secure two-party computation
  - HE for linear operations
  - 2PC for non-linear operations
- Switches between HE and 2PC
- Less computation time compared to HE
- Less bandwidth usage compared to 2PC
- Similar level of accuracy with 2PC

Results

- Paillier cryptosystem for homomorphic encryption
- ABY library for 2PC operations

- Computation cost 30-fold better than HE
- Communication cost 27-fold better than 2PC



Technique	Computation Cost (s)	Communication Cost (MB)
HE[1]	297	372.2
2PC[2]	1.2	47.6
Hybrid	10	1.73

References:
[1] Gilad-Bachrach, Ran, et al. "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy." *International Conference on Machine Learning*. 2016.
[2] Liu, Jian, et al. "Oblivious neural network predictions via minionn transformations." *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017.

Gamze Tillem

Cyber Security Group
Delft University of Technology
G.Tillem@tudelft.nl

EURECOM Sophia Antipolis

TU Delft

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767. This poster reflects the view of the consortium only. The Research Executive Agency is not responsible for any use that may be made of the information it contains.