Towards end-to-end trustworthy machine learning with homomorphic encryption

FORUM MobiliT.AI

Protecting data privacy and ensuring integrity computation

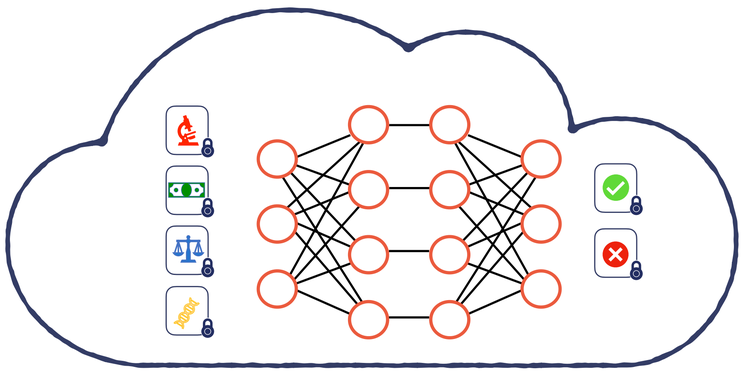
Privacy risks during training/inference

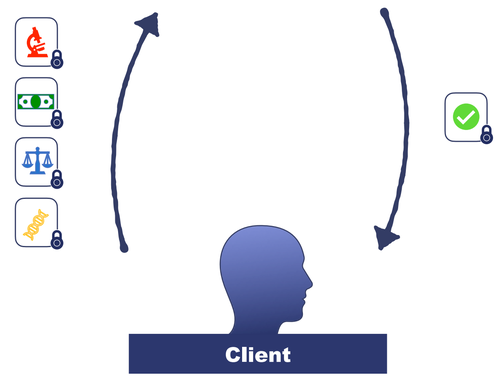
Machine Learning (ML) models implies some risks associated with the potential exposure or misuse of personal information.

Data exposure: uploading sensitive data (🔬 🧬 ⚖️ 💵) to the cloud for training or inference poses risk of unauthorized access or exposure. Without proper safeguards, the cloud provider or malicious actors could gain access to the data, leading to privacy breaches.

Model privacy: Parties may be concerned about protecting the intellectual property of their ML models. The cloud provider might have access to the model during training or inference, potentially exposing it to unauthorized use or replication.

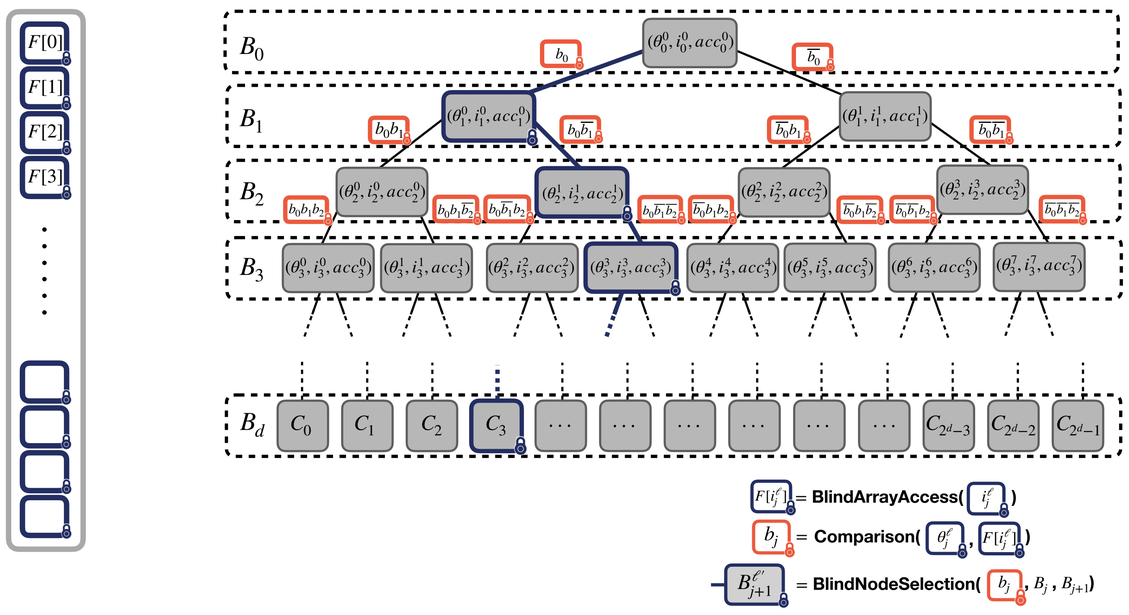
Homomorphic encryption provides a potential solution to mitigate some of these risks. By applying homomorphic encryption techniques, sensitive data can be encrypted before it is utilized in ML processes (🔒).





Client's Features

Server's Decision Tree



Example of PROBONITE decision tree evaluation where the client sends its encrypted attribute vector to the server.

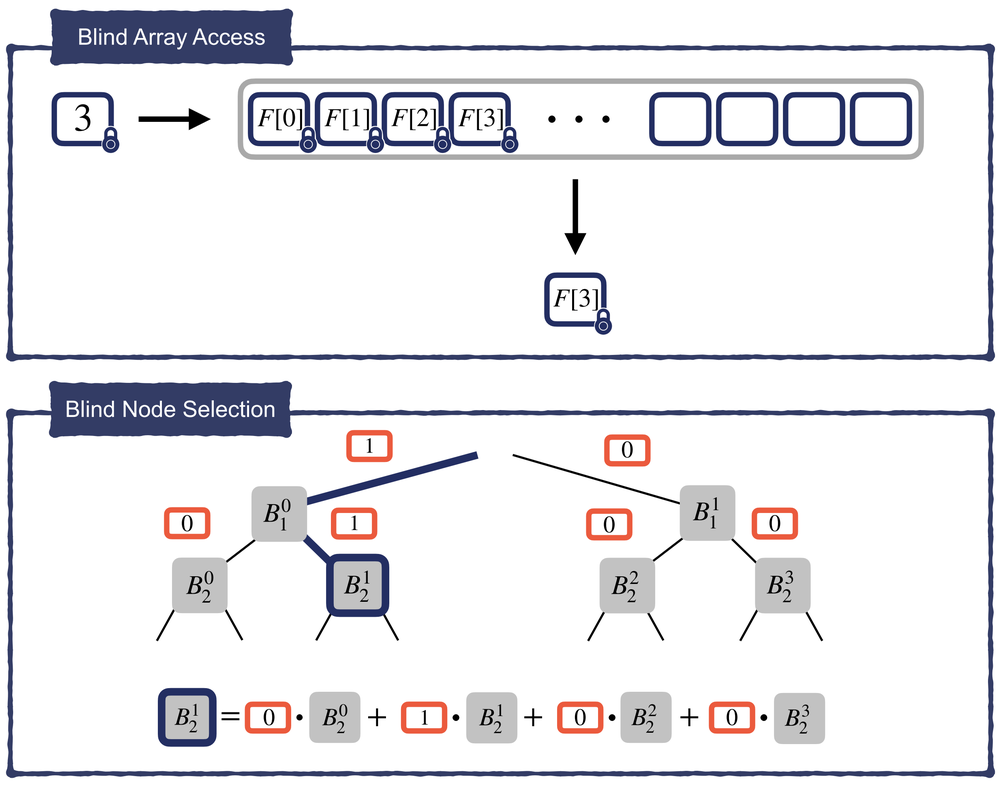
PROBONITE : PRivate One-Branch-Only Non Interactive decision Tree Evaluation

A decision tree is a machine learning method that involves evaluating multiple operations, including **comparing** features $(F[i])$ and thresholds (θ) in each node, to make sequential decisions.

To enable this evaluation by the cloud, one can encrypt the features with homomorphic encryption and send it as is. This inherently implies that **the cloud has to consider all the nodes**, otherwise he would trivially learn which nodes were not used and so learn information on the client's attributes.

Our main contribution consists in **reducing the number of comparisons to its bare minimum** and managing the integration of all nodes in our evaluation with encrypted bits (b) that we accumulate (acc).

Our protocol is based on two primitives that we also introduce in this paper an that may be of independent interest: **Blind Node Selection** and **Blind Array Access**



Train and verify

Leveraging these new primitives to develop others which can be used to make the whole machine learning life cycle private

Full paper : https://ia.cr/2022/936

Sofiane Azogagh : azogagh.sofiane@courrier.uqam.ca
Marc-Olivier Killijian : killijian.marc-olivier.2@uqam.ca
Sébastien Gambs : gambs.sebastien@uqam.ca