# SecureMLlib: Privacy-Preserving Distributed Machine Learning

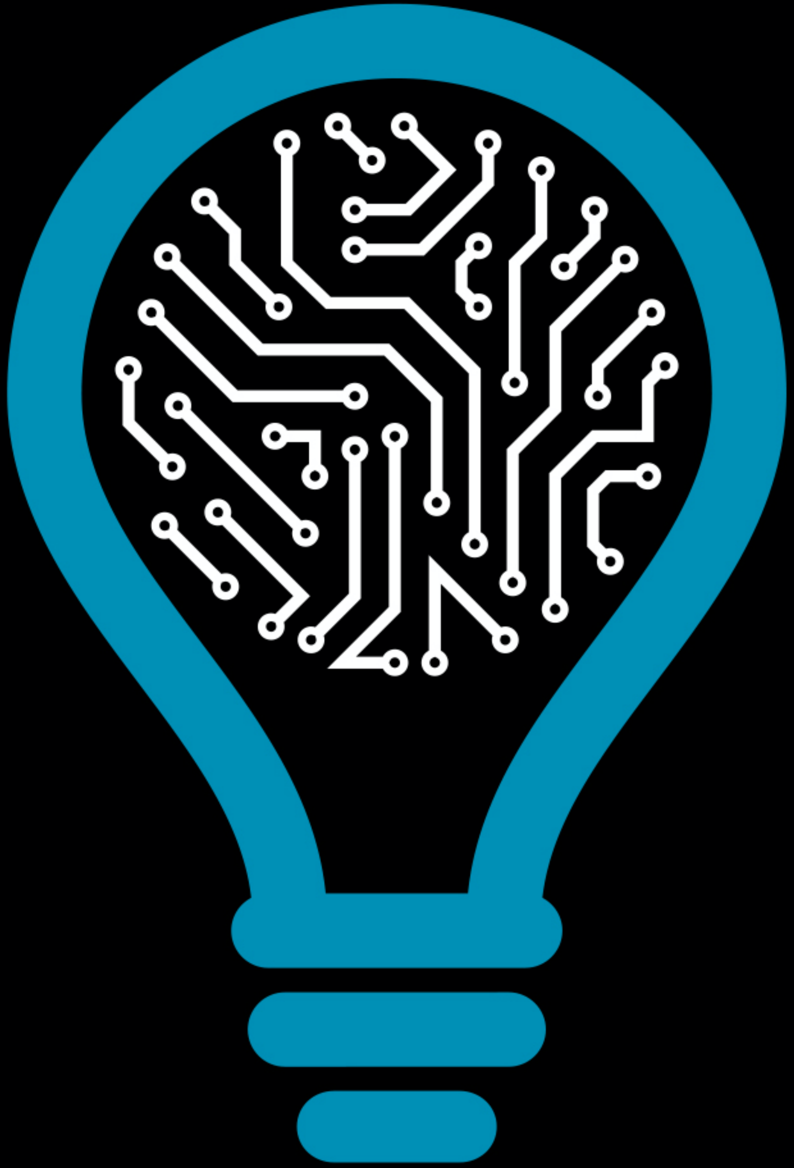
**Cláudia Brito**

Aveiro, Portugal

6 de fevereiro

INESCTEC INSTITUTE FOR SYSTEMS AND COMPUTER ENGINEERING, TECHNOLOGY AND SCIENCE

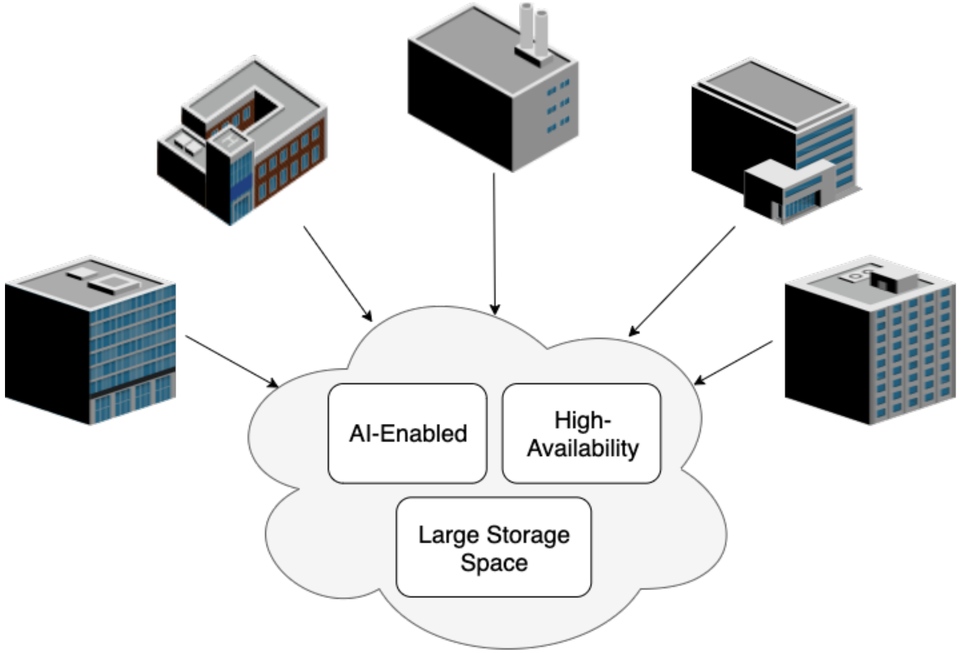
High-Assurance Software Laboratory

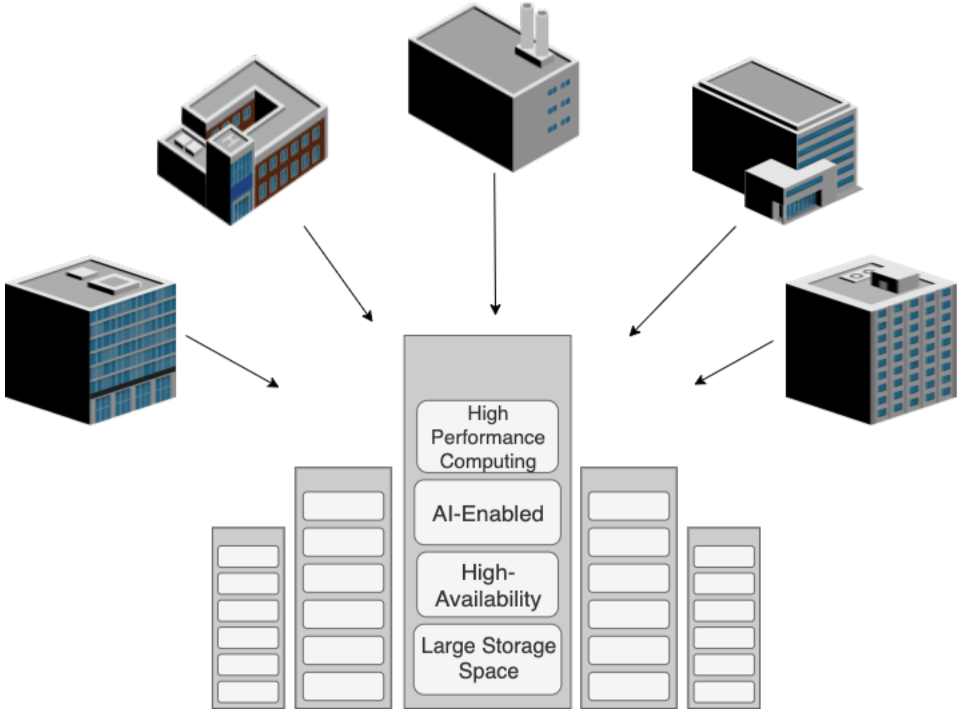


Improving Practice Through Theory

# Big Data & AI

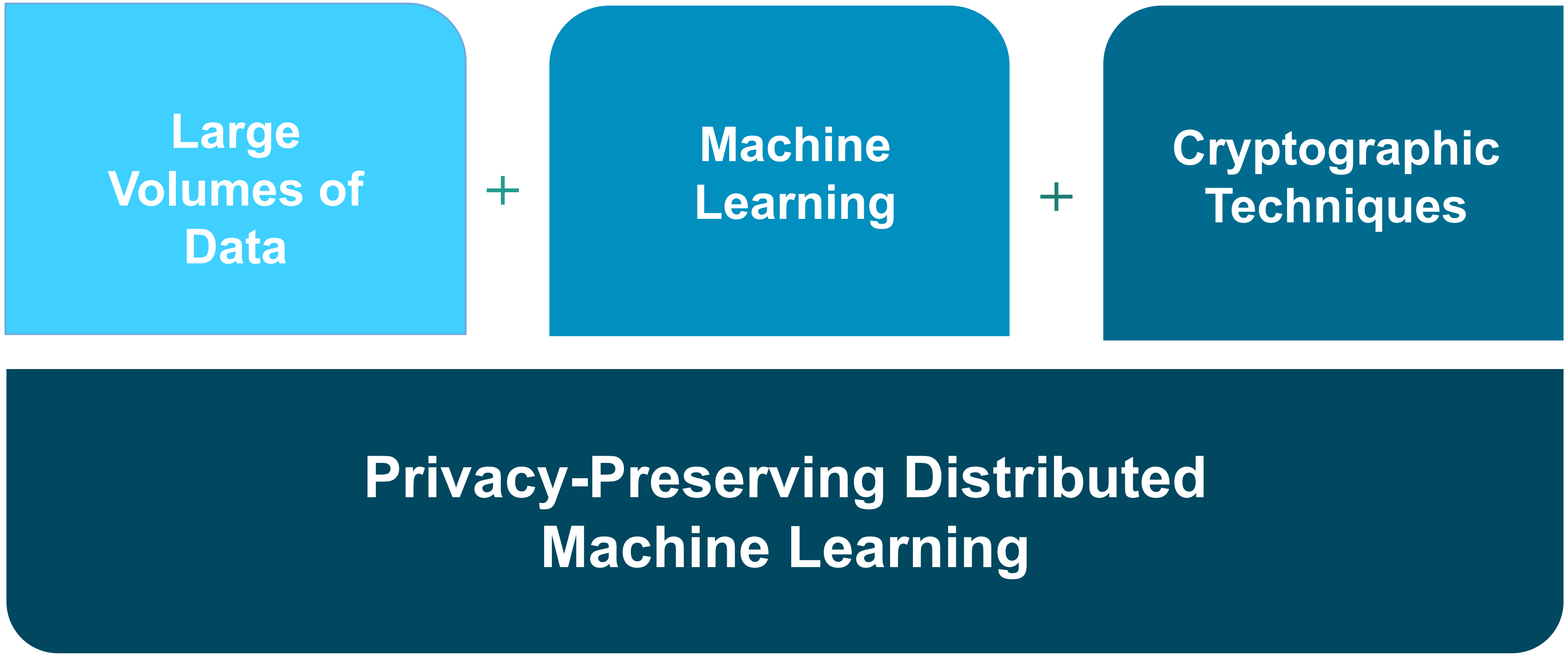
- The **exponential growth** of digital information is raising **novel** and **tougher** challenges for **large-scale data analytics**;
    - Outsourcing of computation to AI-based infrastructures;





# Big Data & AI

- **Legislations**, such as GDPR or HIPAA, are **blocking** how **data** could be leveraged by new **AI algorithms**;
- **Private data should be kept private**;

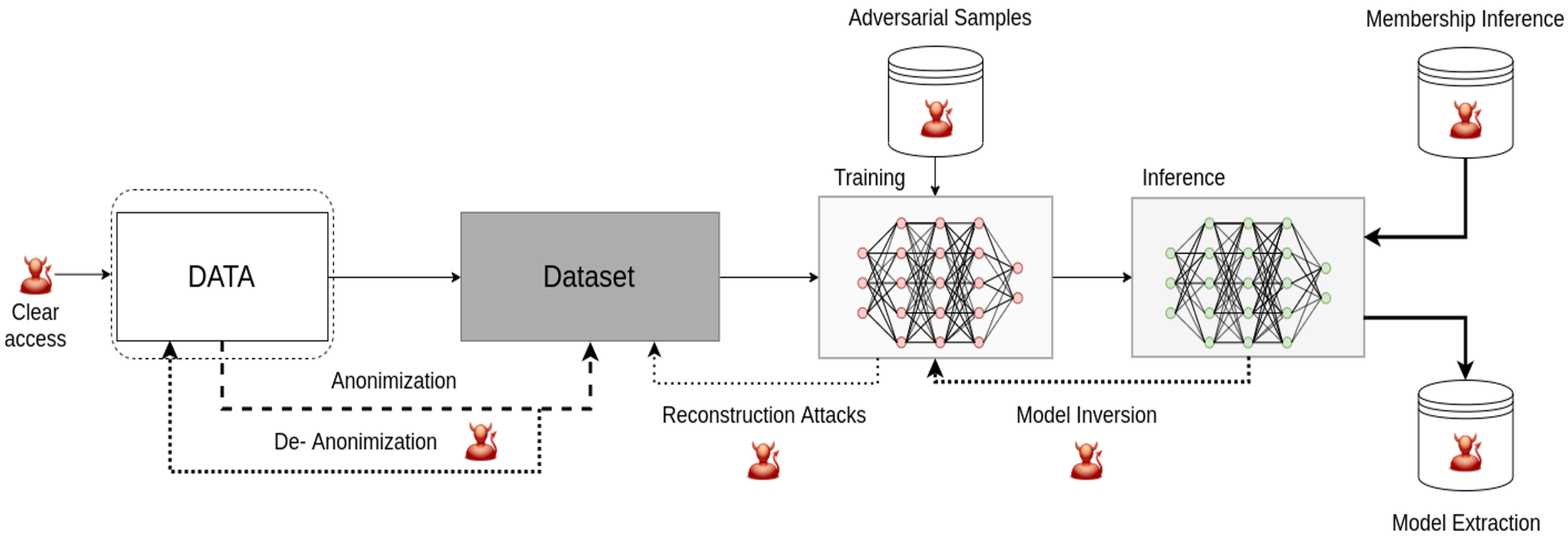


Large Volumes of Data + Machine Learning + Cryptographic Techniques

Privacy-Preserving Distributed Machine Learning

# Machine Learning Pipeline

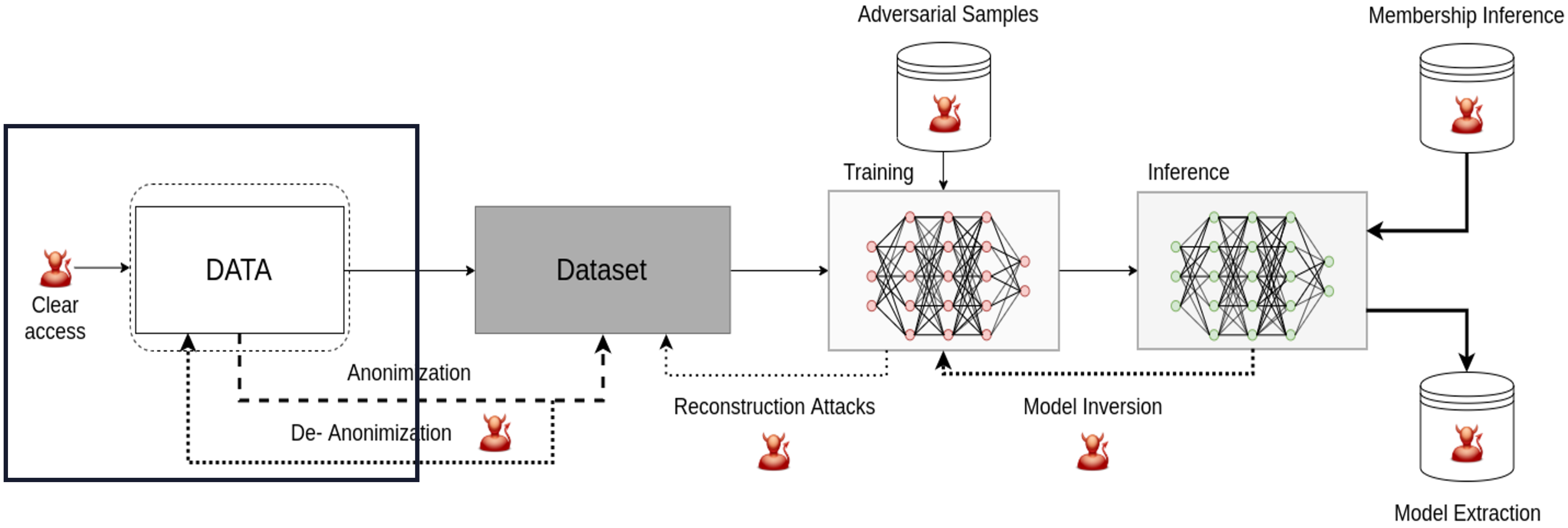
Several threats and attacks end jeopardising the normal functioning of the machine learning pipeline.



We should tackle the challenge step by step.

# Machine Learning Pipeline

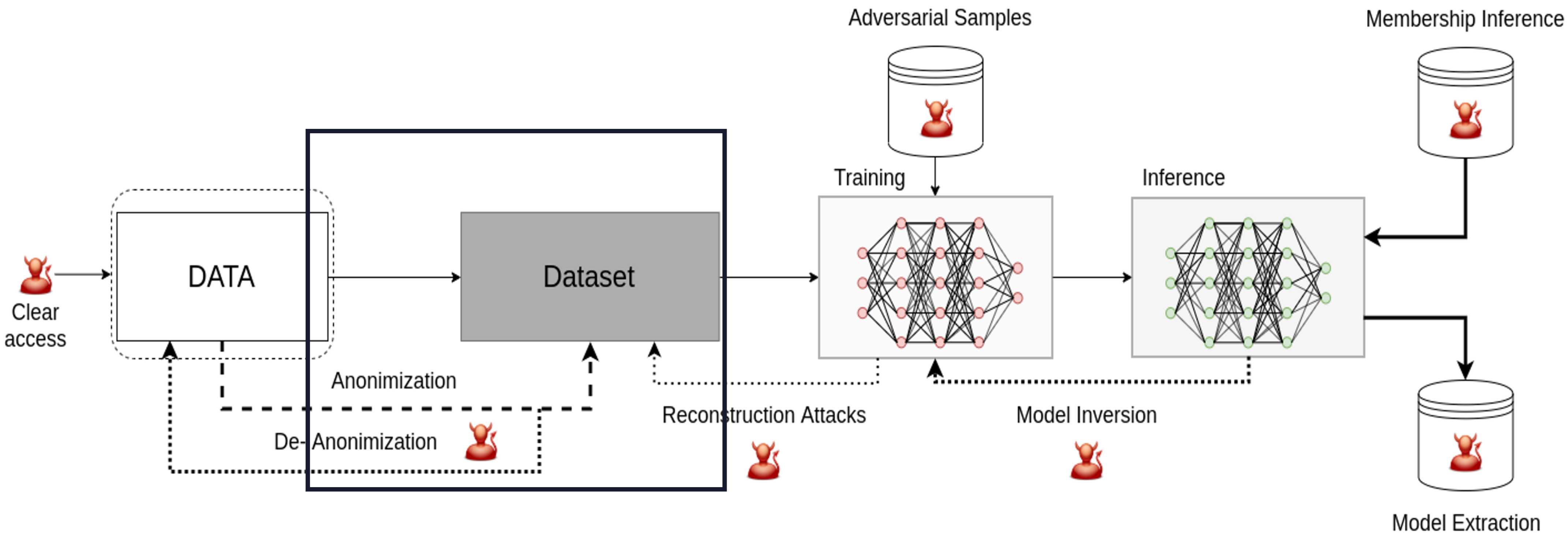
Several threats and attacks end jeopardising the normal functioning of the machine learning pipeline.



We should tackle the challenge step by step.

# Machine Learning Pipeline

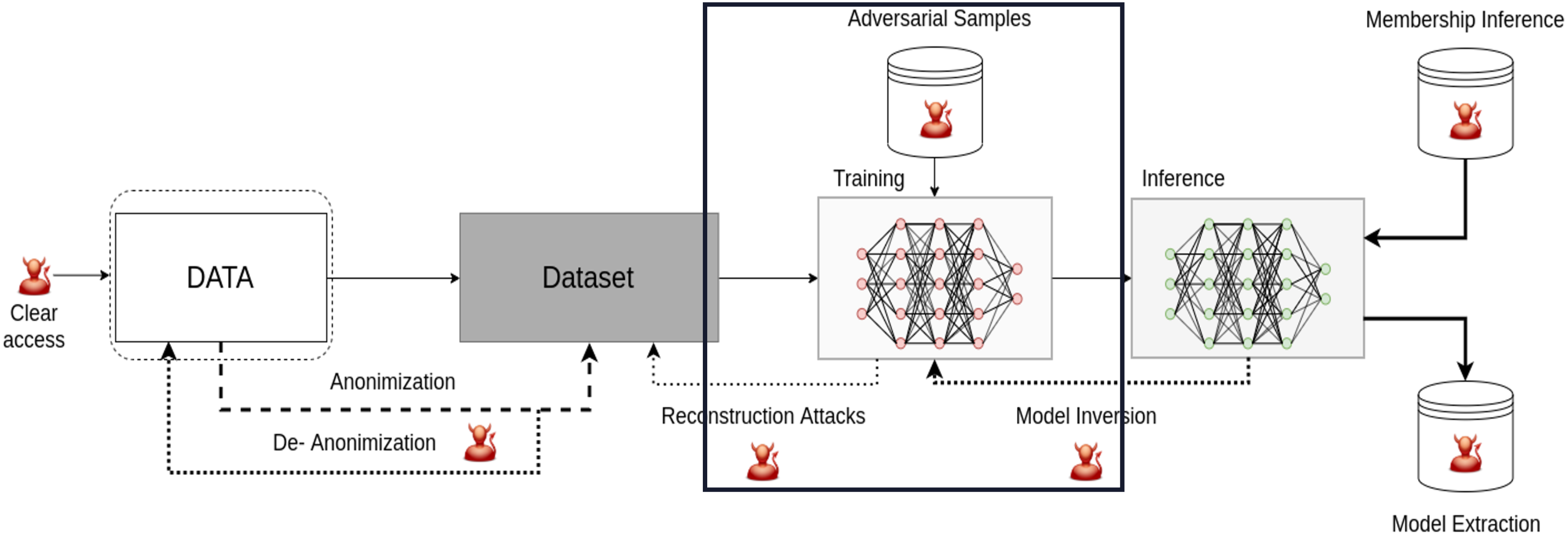
Several threats and attacks end jeopardising the normal functioning of the machine learning pipeline.



We should tackle the challenge step by step.

# Machine Learning Pipeline

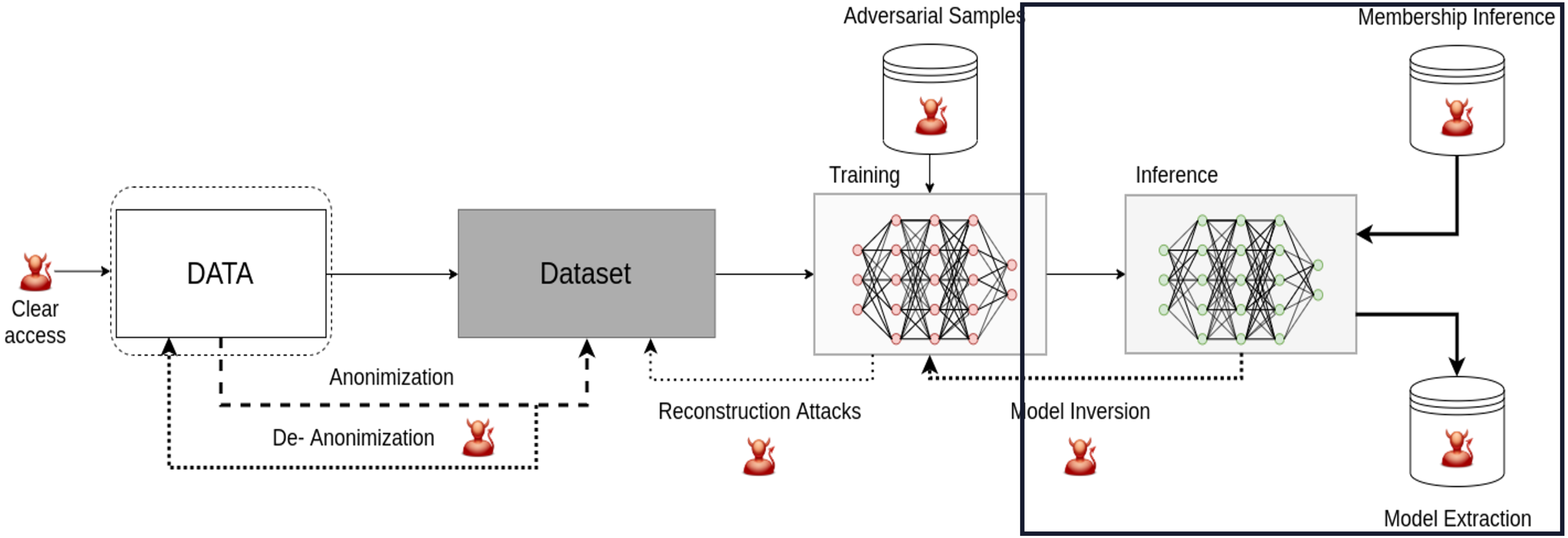
Several threats and attacks end jeopardising the normal functioning of the machine learning pipeline.



We should tackle the challenge step by step.

# Machine Learning Pipeline

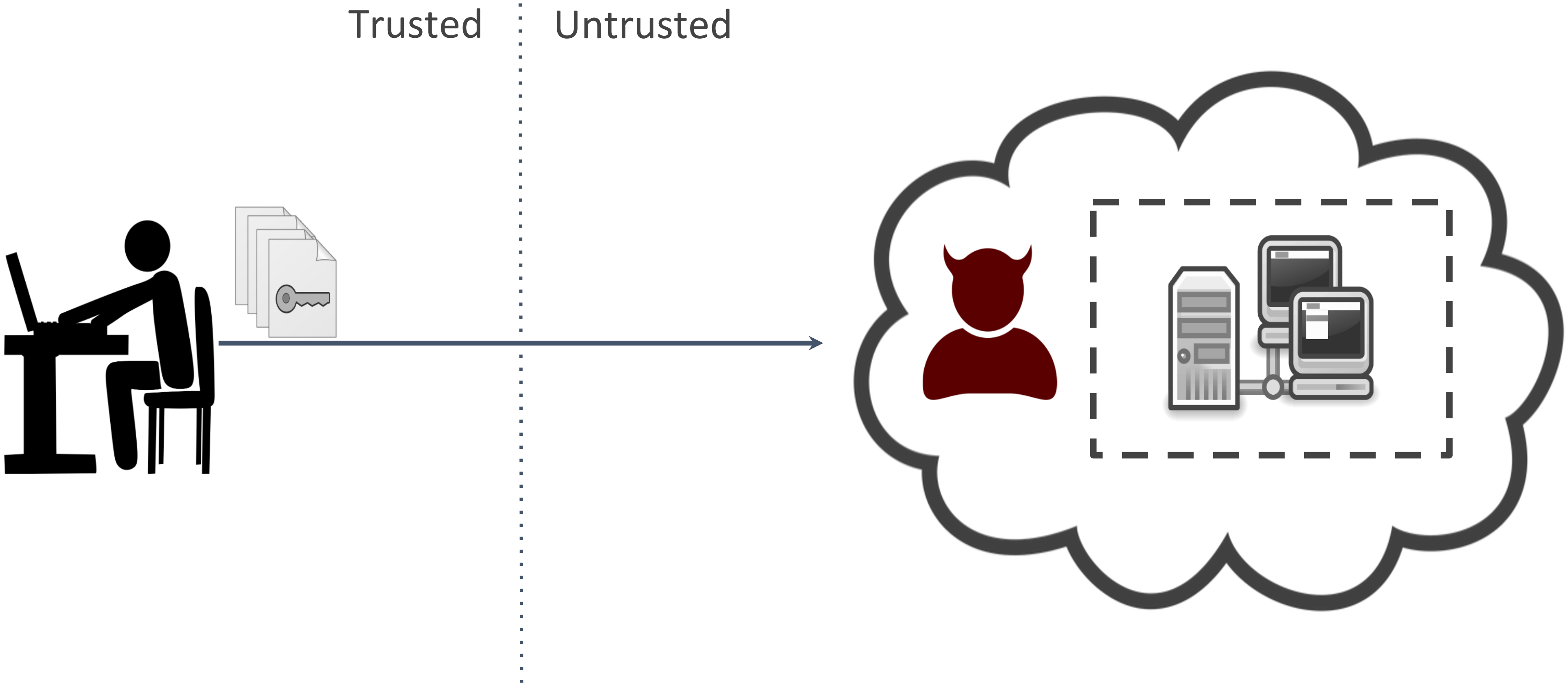
Several threats and attacks end jeopardising the normal functioning of the machine learning pipeline.



We should tackle the challenge step by step.

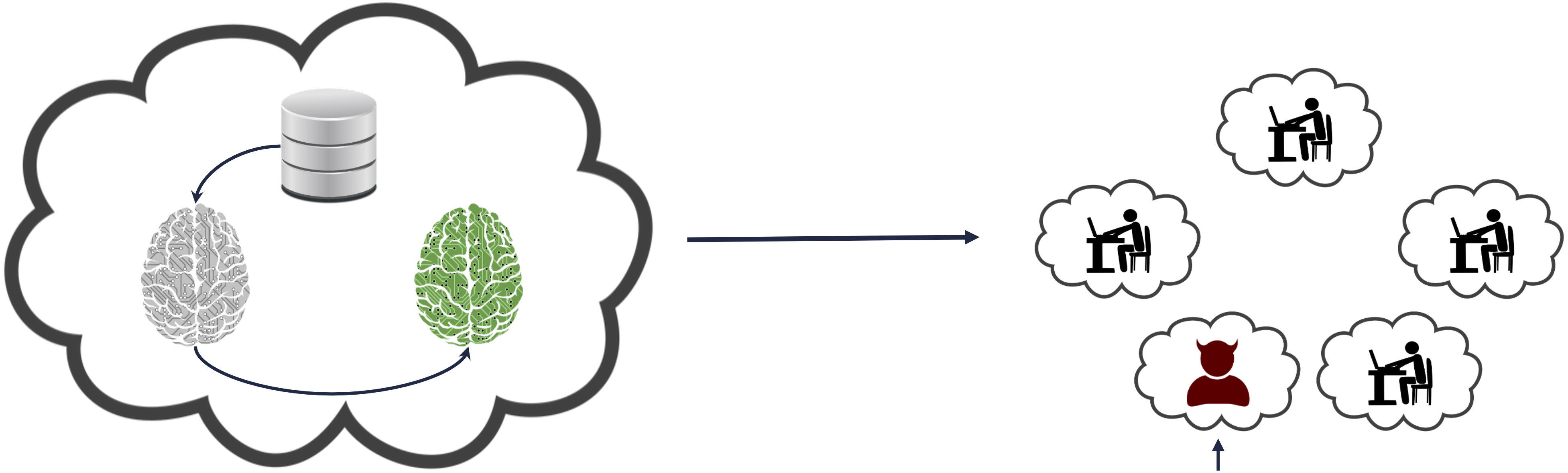
# Challenges

How can we prevent data leakage in distributed machine learning frameworks?



# Challenges

How can we guarantee that our models do not remember the training data and how can we prevent data leakage?



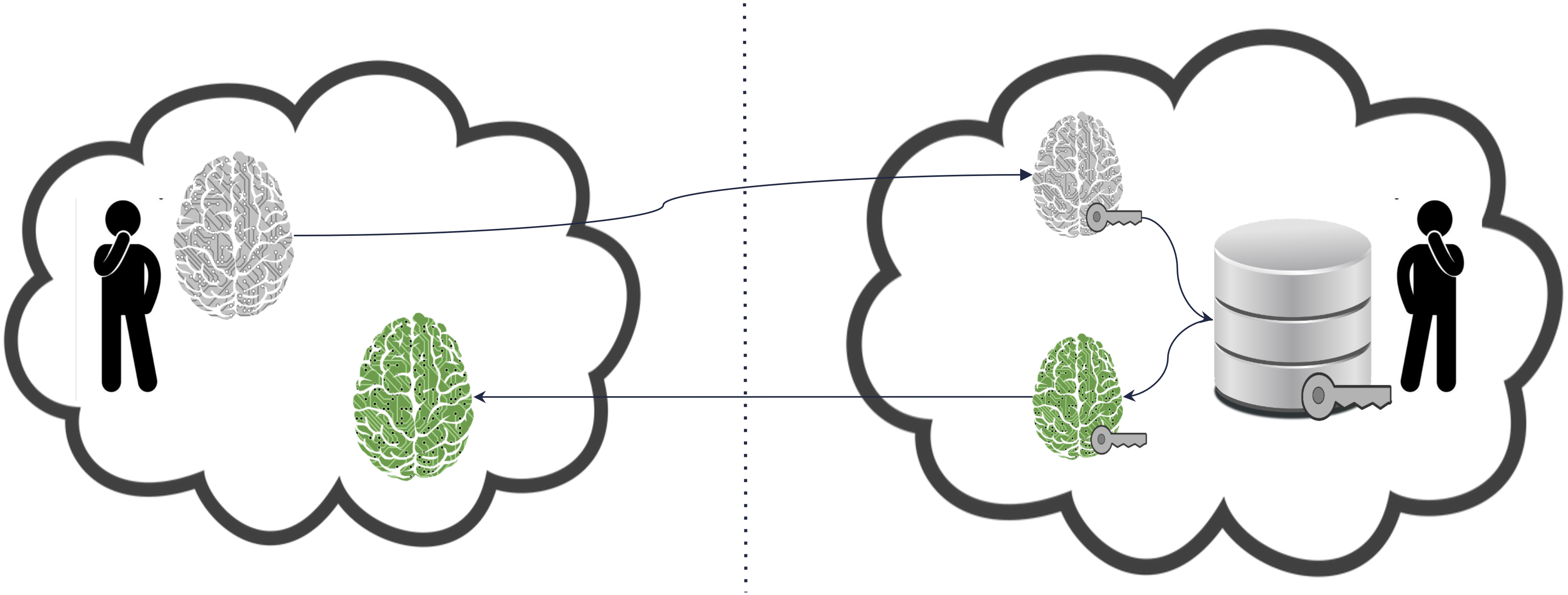
Untrained Model

Trained Model

- Membership Attacks
- Reconstruction Attacks
- Model Inversion
- Model Extraction

# Challenges

How can we protect the intellectual property of our models?



Untrained Model

Trained Model

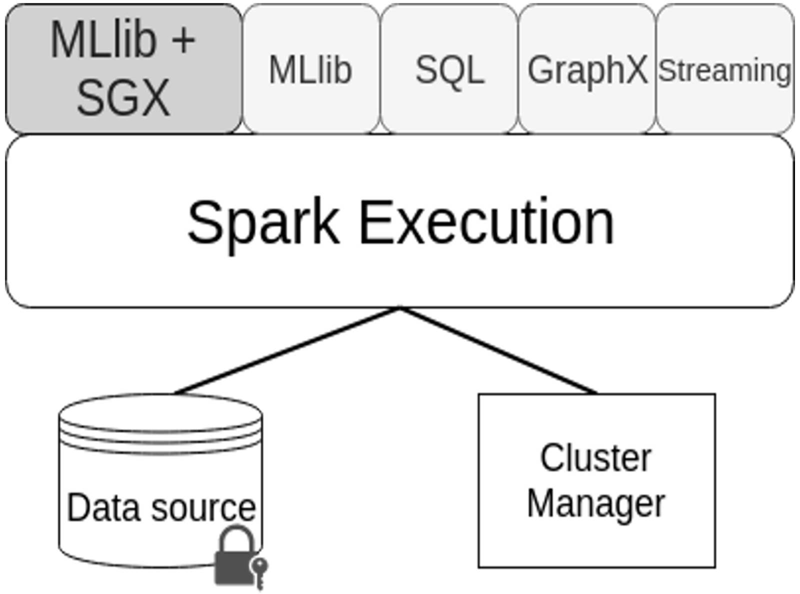
# The solution?

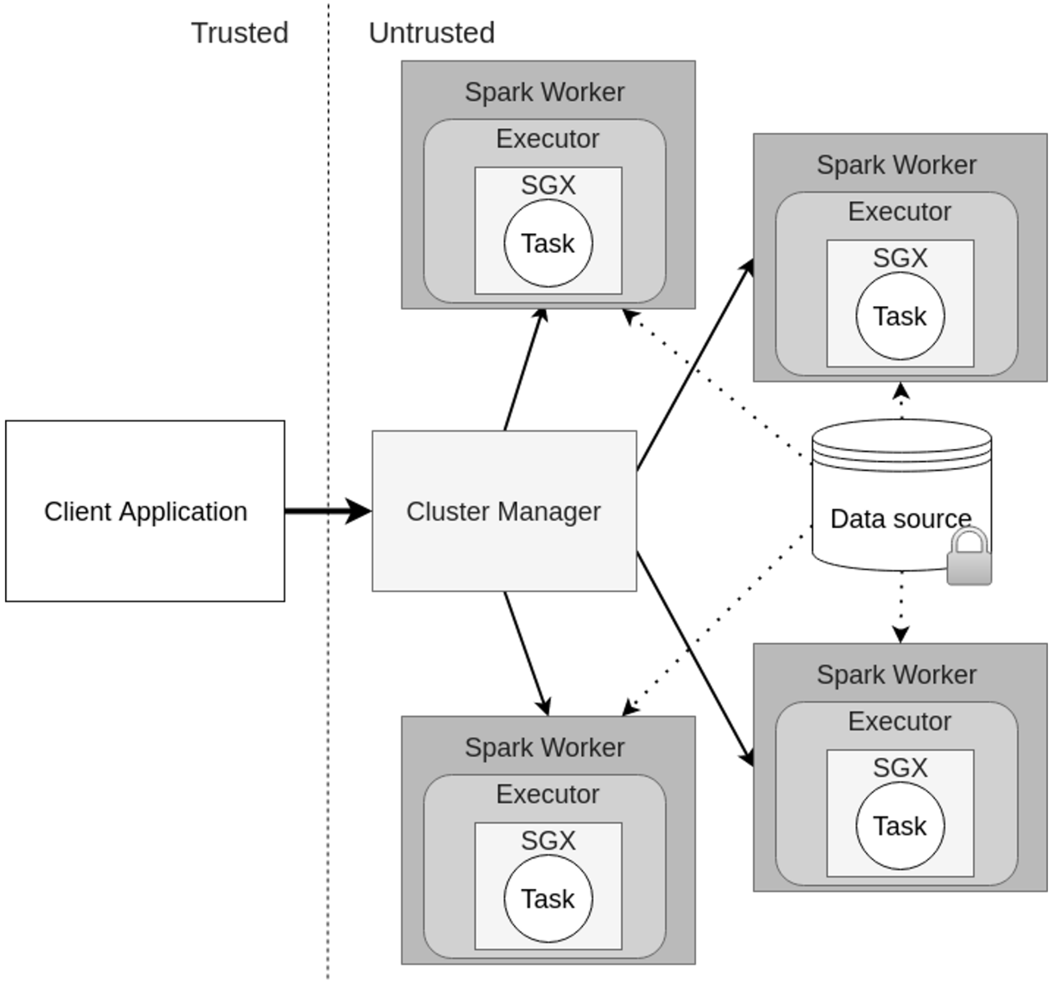
# SecureMLlib

- By relying on Apache Spark, we offer:
  - Scalability;
  - High-Availability;
  - Different APIs for different purposes.

# SecureMLlib

- Data encryption with different cryptographic primitives;
- Modification of MLlib algorithms to compute inside Intel's SGX.



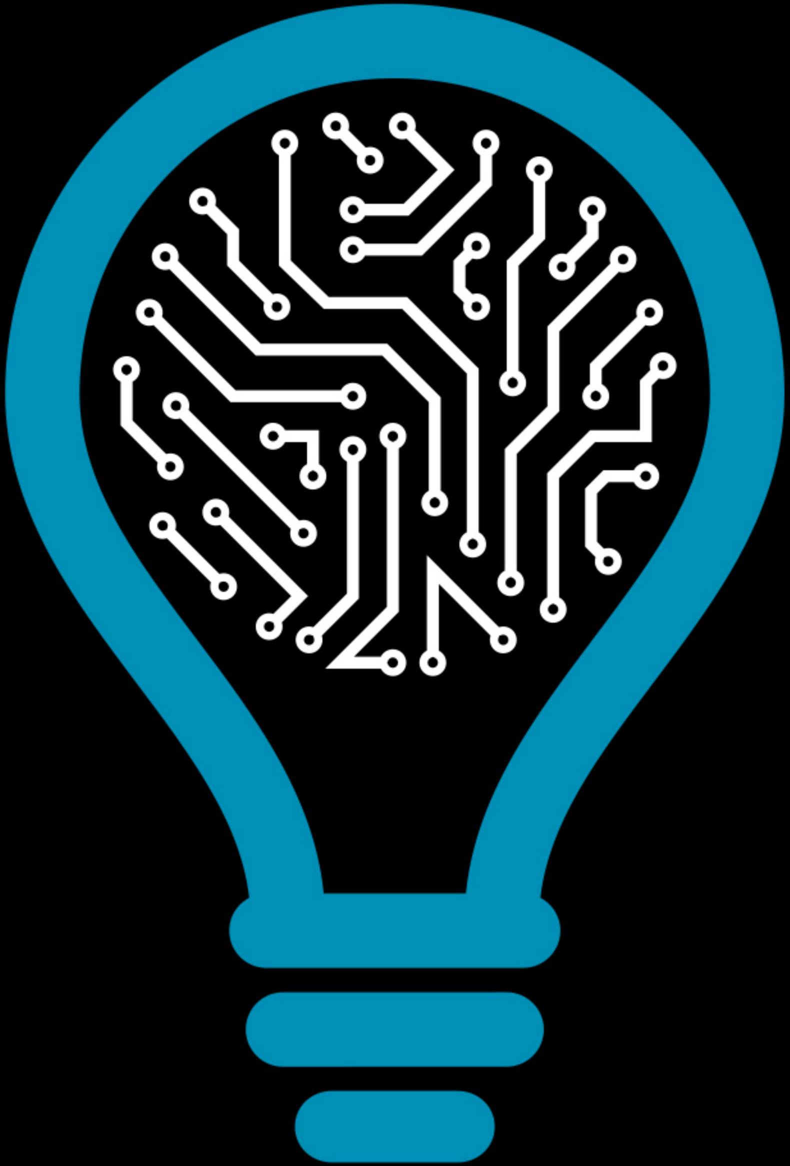


# SecureMLlib: Privacy-Preserving Distributed Machine Learning

**Cláudia Brito**

Aveiro, Portugal

6 de fevereiro



Improving Practice Through Theory

INESCTEC INSTITUTE FOR SYSTEMS AND COMPUTER ENGINEERING, TECHNOLOGY AND SCIENCE

High-Assurance Software Laboratory