

# MUSKETEEER

BDVA workshop on HPC, data protection and data preserving techniques

IBM Research Europe - Ireland – Gal Weiss

Remote, March 15, 2022



"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824988".

1

## Who we are?



Imperial College  
London



uc3m | Universidad  
Carlos III  
de Madrid



KU LEUVEN | CITIP  
CENTRE FOR IT & IP LAW

INTERNATIONAL DATA  
SPACES ASSOCIATION



FCA  
ITEM



Biotronics 3D™  
Analyze - Collaborate - Discover



2

## Why, what and how?



### Project scope:

conduct research in the area of “Machine learning to augment shared knowledge in **federated privacy-preserving** scenarios”.

### Taken from the Abstract:

By the end of the project, MUSKETEEER aims to create a **validated, federated, privacy-preserving machine learning platform** tested on industrial data that is inter-operable, scalable and efficient enough to be deployed in real use cases. MUSKETEEER aims to alleviate data sharing barriers by **providing secure, scalable and privacy-preserving analytics** over decentralized datasets using machine learning.

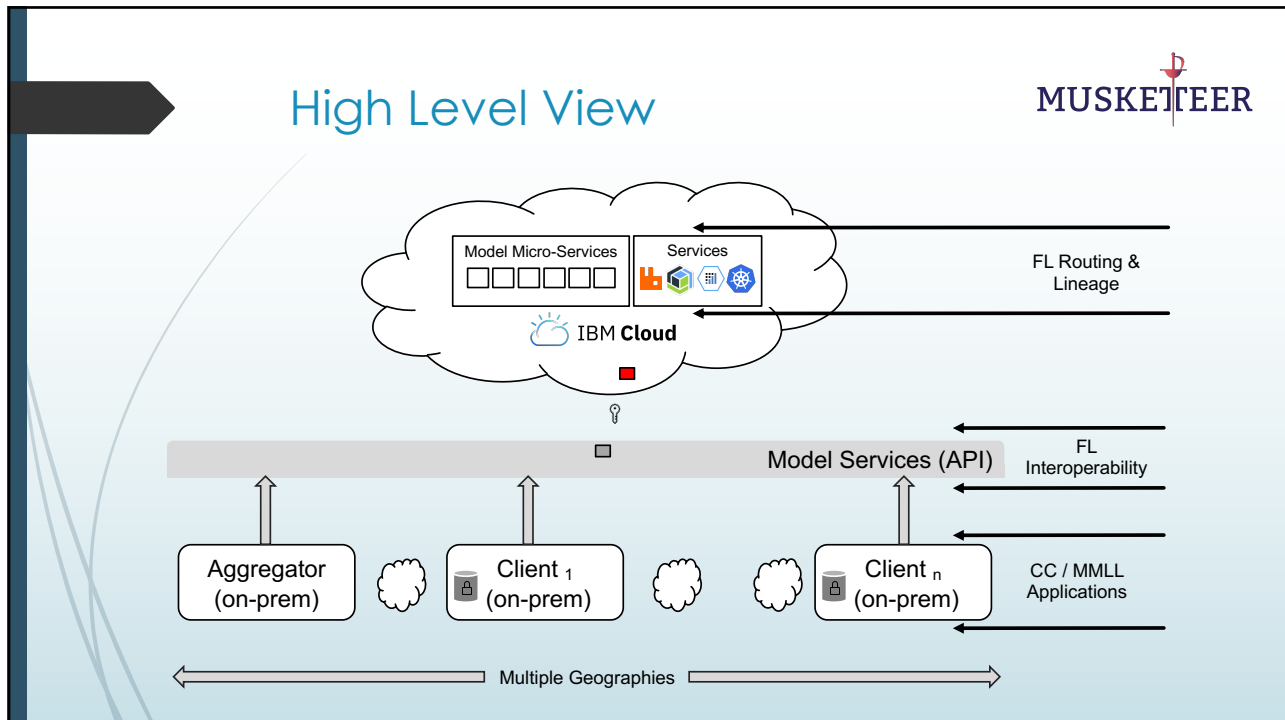
3

## Development methodology



- Emphasis on early integration of development efforts and ongoing regular integration.
- Github for ML algorithm collaboration, 18 repositories.
- Build on open standards and products and contribute to the open-source community.
- Dedicated cloud instances per use case.

4



5



## Poisoning Attacks

**MUSKETTEER**

- Compromise data collection or the parameters of the model.
- The attacker subverts the learning process for the machine learning system.
- Degrades or manipulate the performance of the system.

**Possible attack scenarios in federated learning settings:**

- Applications that rely on untrusted datasets.
- Data from some of the participants is crowdsourced.
- Applications where data curation is not always possible.
- Scenarios where some of the participants want to compromise the trained model.

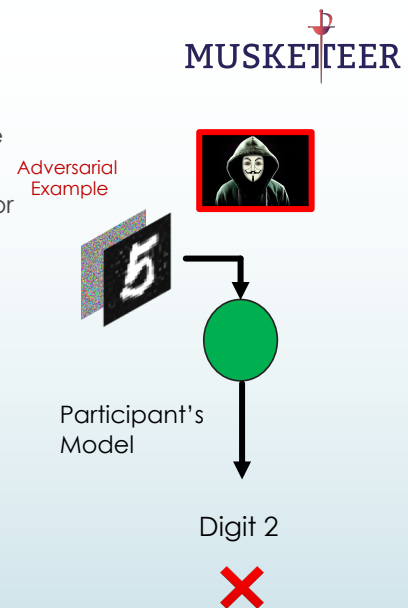



6

## Evasion attacks

- Evasion attacks threaten the deployment scenarios of machine learning systems
- Adversaries can supply corrupted inputs to alter model behavior at test time
- Deep Learning models have been found to be vulnerable to such **adversarial examples**
- Popular examples are found in high-dimensional settings like images where the resulting adversarial examples are **imperceptibly** different from their original counterparts
- Models learnt from Federated Learning systems fail to correctly predict for adversarial examples

We implemented effective mechanisms to **detect malicious or faulty users** and characterise their behaviour.



7

8

## Privacy Operation Modes (POMs)

- **POM1 (ARAMIS)**: equivalent to standard Federated Learning (FL)
- **POM2 (ATHOS)**: FL with encrypted aggregation (shared key)
- **POM3 (PORTHOS)**: FL with encrypted aggregation (different keys)
- **POM4 (ROCHEFORT)**: Data is encrypted (HE) and outsourced, all computations at the aggregator (+cryptonode)
- **POM5 (deWINTER)**: Model is encrypted (HE), aggregator and workers cooperate to update the model
- **POM6 (RICHELIEU)**: No encryption is used, model update relies on secure protocols/computations

MUSKETTEER

8

## Simple guide to select the POM

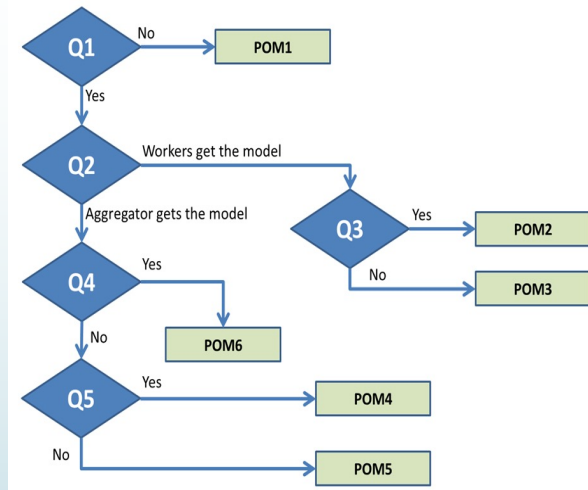


### • Operative aspects:

- **Q1:** Do I need to protect the model?
- **Q2:** Who gets the trained model?
- **Q3:** Do workers trust each other?
- **Q4:** Avoid encryption?
- **Q5:** Can I run a non-colluding cryptoprocessor?

### • Other requirements:

- Computational, Transmission, Storage
- Worker participation



9



MUSKETEEER developed 5 open-source tools using machine learning capabilities, for different Privacy Operation Modes (POMs), applying Federated Learning techniques, while ensuring security and privacy in various flavours for different POMs. These MUSKETEEER tools can be used for future research and collaboration but also for business purposes and improvement.

Gal Weiss |  
Technology Business Development  
Executive at IBM Research Europe - Ireland



Gal Weiss, [galw@ibm.com](mailto:galw@ibm.com); [HTTPS://MUSKETEEER.EU](https://MUSKETEEER.EU)

10