CONSORTIUM

The **MUSKETEER Consortium** consists of **11 partners** from all over Europe and combines experts from the technical, research and industrial sectors:

info@musketeer.eu

@H2020Musketeer

H2020_MUSKETEER

MUSKETEER

MACHINE LEARNING TO AUGMENT SHARED KNOWLEDGE IN FEDERATED PRIVACY-PRESERVING SCENARIOS

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

www.MUSKETEER.eu

The massive increase in data collected and stored worldwide calls for new ways to preserve privacy while still allowing data sharing that respects the sovereignty of multiple data owners.

Today, the lack of usable trusted and secure environments for data sharing inhibits data economy while legality, privacy, trustworthiness, data value and confidentiality hamper the free flow of data.

MUSKETEER aims to create a validated, federated, privacy-preserving machine learning Industrial Data Platform (IDP) that is inter-operable, scalable and efficient enough to be deployed in real use cases.

MUSKETEER aims to alleviate data sharing barriers by providing secure, scalable and privacy-preserving analytics over decentralized datasets using machine learning based on IDSA concepts (architecture model and components). An initial set of privacy preserving machine learning algorithms to solve regression, classification and clustering problems will be provided, although the platform will be flexible enough to accept new algorithmic implementations.

Data can continue to be stored in different locations with different privacy constraints, but shared securely.

The **MUSKETEER** cross-domain platform will validate progress in the industrial scenarios of smart manufacturing and health.

MUSKETEER

The **MUSKETEER mission** is to develop an Industrial Data Platform with scalable algorithms for federated and privacy-preserving machine learning techniques, detection and mitigation of adversarial attacks, and a rewarding model capable of fairly monetizing datasets according to the real data value.

Objectives

1. Machine Learning over a high variety of different privacy-preserving scenarios.
2. Robustness against external and internal threats.
3. Enhancement of the Data Economy.
4. Standardized and extensible architecture.
5. Industrial demonstration of the technology advances in operational environments.

For more information visit
www.MUSKETEER.eu

Use Cases

MUSKETEER will validate its results in two specific use cases, however the final platform will be extensible to additional ones.

SMART MANUFACTURING

The project aims to collect and analyse automotive plant welding data, with the support of artificial intelligence technologies, to search for correlations among the variables that characterize the welding process so that the final welding point will be of the expected quality.

HEALTH

The project aims to demonstrate the application of the federated artificial intelligence approach, enabling access to vast amounts of distributed medical imaging data to train and improve the learning algorithms, providing powerful tools to improve clinical practice.

Privacy Preserving Approach

Every machine learning algorithm will use privacy techniques such as federated machine learning, differential privacy, homomorphic encryption or secure multiparty computation. Other variables could be incorporated in the future thanks to the modular design of the platform.

MUSKETEER will support several Privacy Operation Modes (POMs) with different features:

· Privacy level.
· Computational local overload.
· Central Storage requirements.
· Communication requirements.
· Data Utility Accountability.