ARTIFICIAL INTELLIGENCE AND BIG DATA

Welcome to information sharing 2.0

The economy is going through a process of unprecedented digital transformation. A key aspect in this process is the mass exploitation of data-driven customer-centric business strategies and models.

Security control within organisations make it difficult for data scientists to perform aggregated analyses of multiple data silos, particularly if they are dispersed.

To date it has been necessary to choose between privacy and utility. At GMV we are posing the following question: “Would the problem be solved if instead of sharing data we shared information?”

From that question arose the idea to develop ***uTile PET** (Privacy-Enhancing Technologies)*, a solution which allows calculations to be made in a safe, private manner using distributed data, without exposing them or moving them out of the organisations.

This solution, developed by GMV, uses confidential data in order to improve machine learning algorithms and analytical models, while at all times meeting organisational requirements, guaranteeing data privacy, in accordance with current legislation.

marketing.TIC@gmv.com

gmv.com

gmv®
INNOVATING SOLUTIONS

INFORMATION SHARING 2.0

We live in a world undergoing a major digital transformation, and the process has accelerated as a result of changes in the way we work and the need to increasingly share more and better information.

Big data is a reality and its inclusion within business processed in increasing over time.

There are two new technologies that are helping with this transformation:

- *Machine learning* and advanced analytics
- Privacy-enhancing technologies (PETs)

Thanks to PETs, advanced analytics and *machine learning* can take full advantage of their potential, if we can also include confidential data in a secure manner.

PETs are the technological response to the new challenges regarding privacy and data protection which the current evolution in the digital handling of data must address, and they are preferred both due to their falling cost and a constantly increasing processing capability.

> “Before the end of 2023, **over 80%** of the world will be facing at least one **data protection regulation** focussed on **privacy**

(“Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation” Gartner)

We are creating more data than ever, and these data often contains private, sensitive information

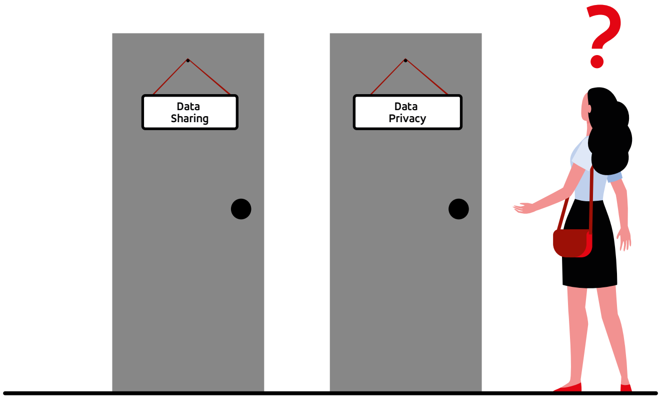
Governments and organisations are applying measures to protect data privacy in order to keep this information private, decentralised and secure

It presents fresh challenges with respect to data analysis and AI

uTile PET

uTile PET is a solution developed by GMV which allows use to be made of confidential, private data in order to improve automated learning algorithms and analytical models, while at all times meeting organisational requirements and guaranteeing data privacy, in accordance with current legislation.

With ***uTile*** we do not need to choose between data privacy and the possibility to use them, as it uses advanced cryptographic methods which keep the data encrypted while performing all the necessary computations. In that way, ***uTile*** enables the possibility that an organisation’s sensitive data never needs to be exposed or transferred via departments, organisations or other countries.



It allows the performance of calculations in a safe, private manner using distributed data, without exposing them or moving them

It uses sensitive data to improve *machine learning* algorithms and analytical models

It meets organisational requirements and guarantees data privacy, in addition to meeting current legislation

TECHNOLOGIES FORMING PART OF *UTILE PET*

uTile PET is a suite of solutions which employs the following technologies:

MPC (Secure Multiparty Computation)

- Secure multiparty computation makes use of additive secret sharing, which allows the segmentation of secret data into parts in such a way that none of the participating parties has the capability to reconstruct the original secret data, but all of them can benefit from the result of sharing.

FL (Federated Learning)

- Federated learning is an algorithmic solution which allows the training of ML models by sending copies of a model and carrying out the training where the data is stored, thus eliminating the need to share the data on a central server.

PSI (Private Set Intersection)

- It is used in cases of vertical partitioning. PSI is a cryptographic technique which allows the intersection to be found among various datasets without having to expose the data, and it thus protects data privacy.

Differential Privacy

- This technique permits data to remain anonymous by deliberately injecting noise into the data set, so that all manner of statistical analyses of huge utility can be performed, without the possibility of any personal information being revealed.

A NEW PARADIGM FOR SHARING INFORMATION

The new paradigm introduced by ***uTile*** means that, finally, it is not necessary to choose between privacy or confidentiality and have collective joint analyses which benefit all parties

It ensures that sensitive data is never exposed or transferred via departments, organisations or geographies

The owners of the data do not have to entrust third parties with their data

The data remain protected behind internal controls, whether *on-premise or cloud*, and any sensitive information remains private during computations

An additional advantage of this new paradigm is that it opens the doors to **cooperation between organisations from different fields**, for example, public-private or inter-sector collaboration exploiting synergies.

uTile, using distributed architecture, swaps the impossibility of exchanging confidential data for **secure information sharing**, which we have called **Information Sharing 2.0**

In conclusion, all organisations could benefit from ***uTile***, achieving a **balance between privacy and data use**, as it securely shares (and even monetises) knowledge based on their data, thanks to encrypted computation, in compliance with the privacy of distributed data sources, while facilitating the secure exchange of information.

A global technology group

Multinational technology group

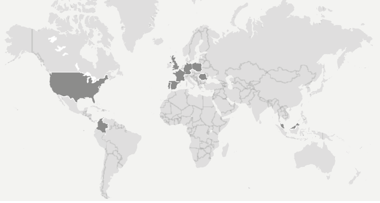
Headquarters in Spain (Madrid)

Over **2.200** employees

Aeronautics, Automotive, Banking & finances, Cybersecurity, Defense & Security, Health, Intelligent Systems of Transport, Public administrations, Space, Telecommunications and ICT for company

Private capital

International presence



Founded in **1984**

Roots tied to the Space and Defence industry

Engineering, development and integration of systems, software, hardware, specialized products and services

International technology leadership

#1 Worldwide Satellite Control Center provider to commercial telecom operators (+300 Satellite missions worldwide)

First ever worldwide intraoperative radiotherapy planning system

Responsible of safety critical systems of European GNSS systems (EGNOS and Galileo)

Leader of Intelligent Transportation Systems for the **public transport sector** (+100 cities in Europe, Asia and America)

GMV's ***checker ATM security*** is the worldwide leader as multivendor cyber security protection for ATMs

An outstanding team

Team Work + Passion for Challenges + Imagination + Innovation + Technology + Customer Focus + Hard Work

GMV in the world

Spain
Madrid – headquarters
Valladolid
Seville
Barcelona
Valencia
Zaragoza

Colombia
France
Germany
Malaysia
North America
Portugal
Poland
Romania
United Kingdom

🟥 BRANCHES AND OFFICES
▨ PROJECTS

gmv.com