

Federated learning is a machine learning approach where a central AI model is trained collaboratively across many devices or servers without directly sharing user raw data. Each device (like a phone, IoT device, vehicle) trains the AI model locally using its own data. Only the AI model updates (like weights or gradients) are sent to the central server, which aggregates them to improve the global model.

Adoption of a federated learning framework is highly advantageous as it does not require to centralise sensitive information, drastically reducing data breach risks and helping organizations effortlessly comply with strict regulations like GDPR. This decentralized approach also unlocks collaboration on high-value AI tasks across competitive or highly regulated sectors without requiring exposure of sensitive and proprietary data.

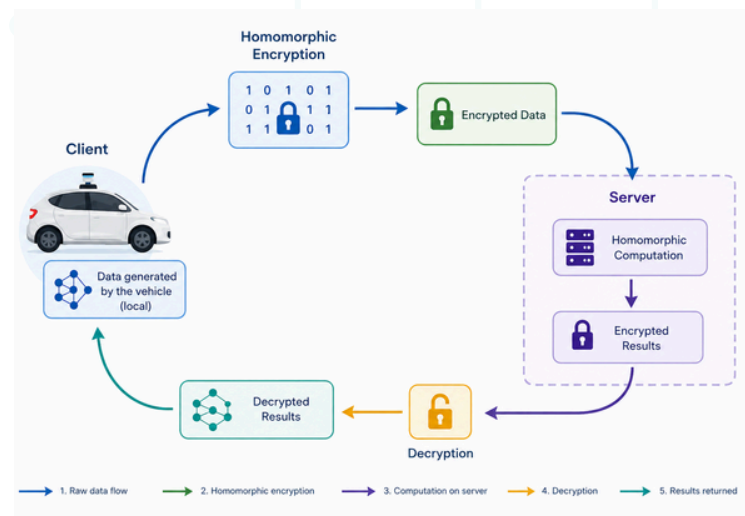
### Connected and Autonomous Vehicles

Connected and Autonomous Vehicles (CAVs) combine two technologies: autonomous driving and communication between vehicles, infrastructure, and other road users.

These CAVs use many systems (cameras, lidars, GPS, and mobile networks), to understand their surroundings and support driving decisions. They also exchange information with nearby vehicles and road infrastructure allowing them to better detect events and improve their awareness beyond what their own sensors can see.

A key feature of CAVs is this cooperative perception. However, these systems also face important risks. Because they depend on sensor data and shared information, they can be affected by cyberattacks or technical failures.

For this reason, use of 5G, IOT and Federated Learning Algorithms is essential to make CAVs robust and resilient to anomalies, whether they are caused intentionally or by faulty equipment.



**IOT (Internet of Things)** is a network of interconnected physical devices embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet. IoT enhances automation, efficiency, and decision-making by providing real-time data insights, enabling smarter environments in healthcare, manufacturing, transportation, or food industries.

**5G** is the fifth generation of mobile network technology, offering high-speed data transfer, ultra-low latency, massive IoT connectivity and supporting millions of devices, network slicing for customized services, and enhanced security and energy efficiency.

**Artificial Intelligence (AI)** is a branch of computer science that enables machines to mimic human intelligence, including learning, reasoning, and problem-solving. In the context of data security, AI can enhance threat detection, speed-up response times, and ensure data protection.

### Contacts:

CITC : [mkonan@citc-eurarfid.com](mailto:mkonan@citc-eurarfid.com)  
UPHF: [yassin.elhillali@uphf.fr](mailto:yassin.elhillali@uphf.fr)