DYDAS

Secure Training

1. **Homomorphic encryption:** ML models can be run on encrypted data by using a cryptographic method that allows mathematical operations to be carried out on ciphertext instead of plain data itself.

2. **Secure Enclaves:** it is important to protect data that is currently "in use". Enclaves are used to execute ML workloads in a memory region that is protected from unauthorized access.

3. **Federated Learning:** originally proposed by Google, the main idea is to build ML models based on datasets that are distributed across multiple devices. This solution makes possible to train a model collectively without sharing private data between devices.

PROJECT NUMBER: 2018-IT-IA-0101
DURATION: 01/12/2019 – 31/01/2023

Co-financed by the Connecting Europe Facility of the European Union

DYDAS

Privacy-Preserving

Deep Learning models require large amount of data to be trained. Any use case requiring the processing of data like: images, videos, full names, addresses, sensitive information and so on. This represents a potential risk for privacy breaches.

For this reason, there are different methods for protecting data during training and others during the inference time.

Go on to learn more about them

TRY THE DYDAS PLATFORM

www.dydas.eu

DYDAS

Privacy-Preserving Deep Learning

Giovanni Nardini
R&D Artificial Intelligence Lead at Key2

DYDAS EU
www.dydas.eu

DYNAMIC DATA ANALYTICS SERVICES

Co-financed by the Connecting Europe Facility of the European Union

DYDAS

Secure Inference with Visual data

1. **Edge Computing:** AI models are deployed on edge devices, enabling real-time and on-device image processing, without sending and storing sensitive visual data.

2. **Image Obfuscation:** traditionally private sensitive visual data are anonymized by applying techniques such as pixelation, blacking and blurring. However, the traditional obfuscation is an approach that can be defeated by sophisticated neural networks that can successfully reconstruct up to the 70% of original data.

3. **Removal of Moving Objects:** an alternative to blurring is represented by the automatically removal and inpainting of sensitive regions like faces and licence plates that are typically moving objects.

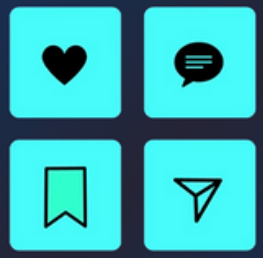
TRY THE DYDAS PLATFORM

Co-financed by the Connecting Europe Facility of the European Union

Did you like the idea?

Test DYDAS Platform

Let us know:



DYDAS

www.dydas.eu

Co-financed by the Connecting Europe Facility of the European Union

DYDAS

DYNAMIC DATA ANALYTICS SERVICES

PROJECT NUMBER: 2018-IT-IA-0101
DURATION: 01/12/2019 – 31/01/2023

Co-financed by the Connecting Europe Facility of the European Union