



truffles@uvigo.es



https://truffles.webs.uvigo.es/

atlanTTic Universida_{de}Vigo Escola de Enxeñaría de Telecomunicación

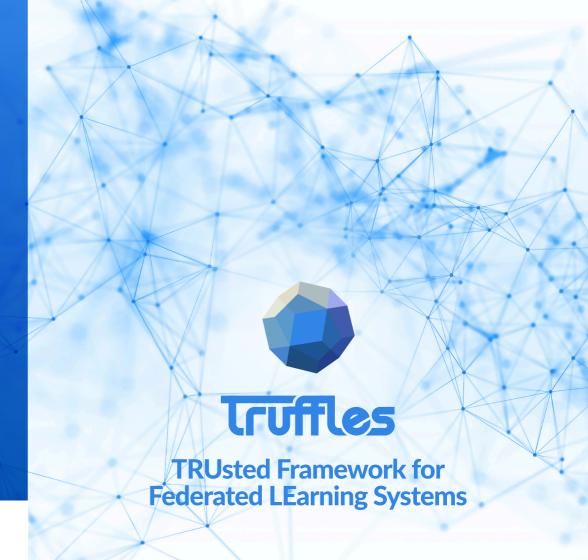
<u>Universidade</u>Vigo











ABOUT THE PROJECT

The TRUsted Framework for Federated LEarning Systems (TRUFFLES) project was granted in the strategic cybersecurity projects call by the INCIBE (Spain). It pursues research advances in the Trusted (Decentralized) Federated Learning, (D)FL, area, that jointly addresses the challenges of privacy, security and robustness for distributed learning systems by combining information theory techniques, post-quantum encryption, crypto-coded computation and adversarial machine learning. Additionally, and since the INCIBE projects also have an important social aspect, TRUFFLES proposes some dissemination and social awareness activities.

RESEARCH OBJECTIVES

- O1 Analysis of threat models in FL
- O2 Design of attacks with active adversaries in FL
- O3 Evaluation of the level of privacy in FL
- O4 Design of secure aggregation techniques in (D)FL to prevent attacks against the aggregator(s) or the learning network computation nodes
- O5 Design of authentication and accountability algorithms in (D)FL
- O6 Improving the efficiency and robustness of (D)FL algorithms to deal with adverse situations
- O7 Create a toolbox to experiment countermeasures in the private, secure and robust operation of (D)FL systems

DISSEMINATION ACTIVITIES

- A1 Creation of short videos about critical aspects on the balance between utility and privacy within the scope of the project.
- Workshop on security and privacy in HF for technology centers and companies: identification of synergies and transfer of knowledge.
- A3 Workshop on security and privacy in HF for technology centers and companies: sharing results and advances.
- 44 Seminar about (D)FL and cybersecurity (researchers & students oriented).
- A5 Challenge/hacking in the privacy field (students oriented).
- 46 Working sessions within international projects and organizations.
- A7 Organization of a special session at an international research congress.





READ MORE ABOUT PROJECT ACTIVITIES

