Author : Adda Akram BENDOUKHA

Title: « Vers un apprentissage fédéré robuste face aux attaques Byzantines»

Short Abstract:

L'IA de confiance exige équité, confidentialité et robustesse. Ces défis sont amplifiés dans les systèmes d'apprentissage fédéré du fait de leur nature distribuée. Nous nous appuyons sur le progrès des attaques d'inférence afin d'éliminer les activités Byzantines, sans compromis de confidentialité grâce au chiffrement homomorphe.

Télécom SudParis • Site d'Évry : 9 rue Charles Fourier - 91011 Évry-Courcouronnes Cedex - France • Site de Palaiseau : 19 place Marguerite Perey - 91120 Palaiseau France • Tél. +33 (0)1 60 76 40 40 • Siret : 180 092 025 00055 • NDA 11910803791 • APE : 8542Z
www.telecom-sudparis.eu