Analyzing **federated learning** through an **adversarial** lens

AN Bhagoji, S Chakraborty, P Mittal… - … on Machine **Learning**, 2019 - proceedings.mlr.press

… **Federated learning** distributes model training among a … In this work, we explore how the **federated learning** setting gives … Model poisoning is carried out by an **adversary** controlling a …

☆ Save 99 Cite Cited by 829 Related articles All 14 versions »

Poisoning attack in **federated learning** using generative **adversarial** nets

J Zhang, J Chen, D Wu, B Chen… - 2019 18th IEEE …, 2019 - ieeexplore.ieee.org

… However, we notice that the **federated learning** architecture … act as a benign participant in **federated learning** to upload the … in **federated learning** system based on generative **adversarial** …

☆ Save 99 Cite Cited by 150 Related articles All 5 versions

Federated learning in **adversarial** settings

R Kerkouche, G Ács, C Castelluccia - arXiv preprint arXiv:2010.07808, 2020 - arxiv.org

… **Federated Learning** enables entities to collaboratively **learn** a shared prediction model … This paper presents a new **federated learning** scheme that provides different trade-offs between …

☆ Save 99 Cite Cited by 11 Related articles All 5 versions »

Threats to **federated learning**: A survey

L Lyu, H Yu, Q Yang - arXiv preprint arXiv:2003.02133, 2020 - arxiv.org

… Under the malicious setting, an active, or malicious **adversary** tries to **learn** the private states … This strong **adversary** model allows the **adversary** to conduct particularly devastating attacks…

☆ Save 99 Cite Cited by 317 Related articles All 3 versions »

Adversarial training in communication constrained **federated learning**

D Shah, P Dube, S Chakraborty, A Verma - arXiv preprint arXiv …, 2021 - arxiv.org

… **Federated learning** enables model training … **adversarial** examples – designed to elicit misclassification. We study the feasibility of using **adversarial** training (AT) in the **federated learning** …

☆ Save 99 Cite Cited by 30 Related articles All 2 versions »

Federated robustness propagation: Sharing **adversarial** robustness in **federated learning**

J Hong, H Wang, Z Wang, J Zhou - 2021 - openreview.net

… a sound solution for centralized **learning**, extending its usage … we study a novel **learning** setting that propagates **adversarial** … cannot effectively propagate **adversarial** robustness among …

☆ Save 99 Cite Cited by 26 Related articles All 3 versions »

A robust analysis of **adversarial** attacks on **federated learning** environments

AK Nair, ED Raj, J Sahoo - Computer Standards & Interfaces, 2023 - Elsevier

… types, and working in a **Federated Learning** environment in detail. This study will give a precise idea of security issues faced in **Federated** Machine **Learning** and possible solutions. …

☆ Save 99 Cite Cited by 5 Related articles All 2 versions

Fairvfl: A fair vertical **federated learning** framework with contrastive **adversarial learning**

T Qi, F Wu, C Wu, L Lyu, T Xu, H Liao… - Advances in …, 2022 - proceedings.neurips.cc

… to be applied in vertical **federated learning**. Different from these methods, we propose a fair vertical **federated learning** framework, which applies **adversarial learning** to improve the …

☆ Save 99 Cite Cited by 11 Related articles All 4 versions »

Delving into the **adversarial** robustness of **federated learning**

J Zhang, B Li, C Chen, L Lyu, S Wu, S Ding… - arXiv preprint arXiv …, 2023 - arxiv.org

… **adversarial** attacks. We first find that directly adopting **adversarial** training in **federated learning** … We then propose a novel and effective **adversarial** training method called DBFAT, which …

☆ Save 99 Cite Cited by 7 Related articles All 2 versions »

PDGAN: A novel poisoning defense method in **federated learning** using generative **adversarial** network

Y Zhao, J Chen, J Zhang, D Wu, J Teng… - … and Architectures for …, 2020 - Springer

… In **federated learning**, we notice that the poisoning attack can be easily … of **federated learning** and generative **adversarial** nets. The overview of the poisoning attack in **federated learning** …

☆ Save 99 Cite Cited by 55 Related articles All 3 versions »

Related searches

federated learning adversarial **robustness**

federated learning adversarial **lens**

federated learning adversarial **training**

vertical federated learning

federated learning **systems**

federated learning **poisoning attacks**

federated learning adversarial **approach**

federated learning **generative** adversarial **nets**

federated learning **generative** adversarial **network**

federated learning adversarial **settings**

privacy of federated learning

accelerated federated learning

continual federated learning

robust federated learning **industrial iot systems**

heterogeneous federated learning

practical vertical federated learning

unsupervised representation