From Gradient Leakage To Adversarial Attacks In Federated Learning

Publisher: IEEE

Cite This PDF

Jia Qi Lim ; Chee Seng Chan **All Authors**

387
Full
Text Views

Alerts

Manage Content Alerts

Add to Citation Alerts

More Like This

Prediction and Visualisation of Viral Genome Antigen Using Deep Learning & Artificial Intelligence
2021 5th International Conference on Computing Methodologies and Communication (ICCMC)
Published: 2021

Combined IASI-NG and MWS Observations for the Retrieval of Cloud Liquid and Ice Water Path: A Deep Learning Artificial Intelligence Approach
IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing
Published: 2022

Show More

Downl PDF

Abstract: Deep neural networks (DNN) are widely used in real-life applications despite the lack of understanding on this technology and its challenges. Data privacy is one of the b... **View more**

Metadata

Abstract:

Deep neural networks (DNN) are widely used in real-life applications despite the lack of understanding on this technology and its challenges. Data privacy is one of the bottlenecks that is yet to be overcome and more challenges in DNN arise when researchers start to pay more attention to DNN vulnerabilities. In this work, we aim to cast the doubts towards the reliability of the DNN with solid evidence particularly in Federated Learning environment by utilizing an existing privacy breaking algorithm which inverts gradients of models to reconstruct the input data. By performing the attack algorithm, we exemplify the data reconstructed from inverting gradients algorithm as a potential threat and further reveal the vulnerabilities of models in representation learning. Pytorch implementation are provided at https://github.com/Jiaqi0602/adversarial-attack-from-leakage/

Published in: 2021 IEEE International Conference on Image Processing (ICIP)

Footnotes

Date of Conference: 19-22 September 2021

Date Added to IEEE *Xplore*: 23 August 2021

▸ **ISBN Information:**

▸ **ISSN Information:**

INSPEC Accession Number: 21731444

DOI: 10.1109/ICIP42928.2021.9506589

Publisher: IEEE

Conference Location: Anchorage, AK, USA

☰ Contents

1. Introduction

Deep neural networks (DNN) based solutions have pervaded into our daily lives because of their impressive success across various machine learning problems [1]. However, this achievement is heavily depending on having sufficient number of image-label pairs to train the DNN models. Now, this process is further complicated with the recently announced data protection legislation such as the General Data Protection Regulation (EU GDPR) which aims to safeguard the privacy of data. [1]

Sign in to Continue Reading

[1] https://gdpr-info.eu/

Authors ⌄

Figures ⌄

References ⌄

Keywords ⌄

Metrics ⌄

Footnotes ⌄

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

Follow

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History
- » View Purchased Documents

Profile Information

- » Communications Preferences
- » Profession and Education
- » Technical Interests

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies