A hybrid approach to **privacy**-preserving **federated learning**

S Truex, N Baracaldo, A Anwar, T Steinke… - Proceedings of the 12th …, 2019 - dl.acm.org

… We propose a novel **federated learning** system which provides formal **privacy** guarantees, … with existing **privacy**-preserving approaches. Data never leaves the participants and **privacy** is …

☆ Save ❞ Cite Cited by 683 Related articles All 11 versions »

A survey on security and **privacy** of **federated learning**

V Mothukuri, RM Parizi, S Pouriyeh, Y Huang… - Future Generation …, 2021 - Elsevier

… are mature enough to be expected to solve all **privacy** issues by default, at least not for the time … the existing **privacy** issues and the current relevant achievement in **federated learning** …

☆ Save ❞ Cite Cited by 623 Related articles All 3 versions Web of Science: 294

A survey on **federated learning** systems: Vision, hype and reality for data **privacy** and protection

Q Li, Z Wen, Z Wu, S Hu, N Wang, Y Li… - IEEE Transactions on …, 2021 - ieeexplore.ieee.org

… **federation** and motivation of **federation**. The categorization can help the design of **federated learning** … By systematically summarizing the existing **federated learning** systems, we present …

☆ Save ❞ Cite Cited by 558 Related articles All 8 versions Web of Science: 70

Federated learning with differential **privacy**: Algorithms and performance analysis

K Wei, J Li, M Ding, C Ma, HH Yang… - IEEE Transactions …, 2020 - ieeexplore.ieee.org

Federated learning (FL), as a type of distributed machine **learning**, is capable of significantly … a novel framework based on the concept of differential **privacy** (DP), in which artificial noise …

☆ Save ❞ Cite Cited by 948 Related articles All 9 versions Web of Science: 388

Related searches

federated learning privacy **preserving**

centralized and federated learning privacy **analysis**

federated learning **systems**

survey on federated learning

federated learning **user level**

federated learning **internet of things**

federated learning **in mobile edge networks**

federated learning **at scale**

Efficient and **privacy**-enhanced **federated learning** for industrial artificial intelligence

M Hao, H Li, X Luo, G Xu, H Yang… - IEEE Transactions on …, 2019 - ieeexplore.ieee.org

… In order to solve above challenges, we propose **privacy**enhanced **federated learning** (PEFL) to achieve efficient and PEFL for IAI. Our contributions are summarized as follows: 1) PEFL …

☆ Save ❞ Cite Cited by 361 Related articles All 3 versions Web of Science: 223

Federated learning: Challenges, methods, and future directions

T Li, AK Sahu, A Talwalkar… - IEEE signal processing …, 2020 - ieeexplore.ieee.org

… aim to enhance the **privacy** of **federated learning** using tools such as secure multiparty computation (SMC) or differential **privacy**, these approaches often provide **privacy** at the cost of …

☆ Save ❞ Cite Cited by 3200 Related articles All 6 versions Web of Science: 1262

A comprehensive survey of **privacy**-preserving **federated learning**: A taxonomy, review, and future directions

X Yin, Y Zhu, J Hu - ACM Computing Surveys (CSUR), 2021 - dl.acm.org

… rapid development of **federated learning** (FL). However, new **privacy** concerns have also emerged during the aggregation of the distributed intermediate results. The emerging **privacy**-…

☆ Save ❞ Cite Cited by 205 Related articles All 2 versions Web of Science: 83 »

Hybridalpha: An efficient approach for **privacy**-preserving **federated learning**

R Xu, N Baracaldo, Y Zhou, A Anwar… - Proceedings of the 12th …, 2019 - dl.acm.org

… proposed based on differential **privacy** and secure multiparty … for **privacy**-preserving **federated learning** employing an SMC … exchanged using a **federated learning** process to train a CNN …

☆ Save ❞ Cite Cited by 252 Related articles All 6 versions »

A survey on **federated learning**

C Zhang, Y Xie, H Bai, B Yu, W Li, Y Gao - Knowledge-Based Systems, 2021 - Elsevier

… (1) **Privacy** protection: Since **federated learning** is proposed to solve the problem of … In order to guarantee the **privacy** of the data, **federated learning** only permits all the remote devices …

☆ Save ” Cite Cited by 423 Related articles Web of Science: 194

Beyond inferring class representatives: User-level **privacy** leakage from **federated learning**

Z Wang, M Song, Z Zhang, Y Song… - IEEE INFOCOM 2019 …, 2019 - ieeexplore.ieee.org

… the **privacy** risk of **federated learn**ing, which is considered as a **privacy**-preserving **learning** … Against federated **learning**, we proposed a generic and practical reconstruction attack named …

☆ Save ” Cite Cited by 611 Related articles All 5 versions