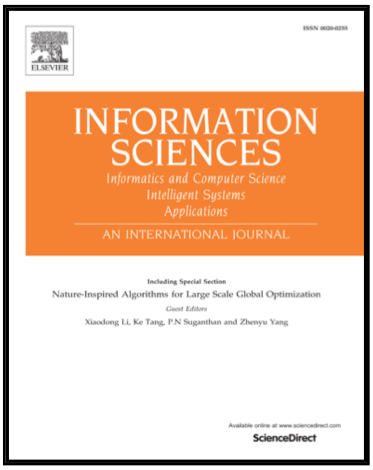

ISSN 0020-0255

ELSEVIER

INFORMATION SCIENCES

Informatics and Computer Science
Intelligent Systems
Applications

AN INTERNATIONAL JOURNAL

Including Special Section

Nature-Inspired Algorithms for Large Scale Global Optimization

Guest Editors

Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang

Available online at www.sciencedirect.com

ScienceDirect

Privacy Preserving Multi-Party Computation Delegation for Deep Learning in Cloud Computing

Xu Ma, Fangguo Zhang, Xiaofeng Chen, Jian Shen

PII: S0020-0255(18)30360-8
DOI: 10.1016/j.ins.2018.05.005
Reference: INS 13633

To appear in: *Information Sciences*

Received date: 11 December 2017
Revised date: 1 May 2018
Accepted date: 2 May 2018

Please cite this article as: Xu Ma, Fangguo Zhang, Xiaofeng Chen, Jian Shen, Privacy Preserving Multi-Party Computation Delegation for Deep Learning in Cloud Computing, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.05.005

Privacy Preserving Multi-Party Computation Delegation for Deep Learning in Cloud Computing

Xu Ma[a,b], Fangguo Zhang[c], Xiaofeng Chen[a,*], Jian Shen[d]

[a]*State Key Laboratory of Integrated Service Networks (ISN),*
Xidian University, Xi'an, China
[b]*School of Software,*
Qufu Normal University, Qufu, China
[c] *School of Data and Computer Science,*
Sun Yat-Sen University, Guangzhou, China.
[d]*School of Computer and Software,*
Nanjing University of Information Science and Technology, Nanjing, China

Abstract

The recent advances in deep learning have improved the state of the art in artificial intelligence, and one of the most important stimulants of this success is the large volume of data. Although collaborative learning can improve the learning accuracy by incorporating more datasets into the learning process, serious privacy issues have also emerged from the training data. In this paper, we propose a new framework for privacy-preserving multi-party deep learning in cloud computing, where the large volume of training data is distributed among many parties. Our system enables multiple parties to learn the same neural network model, which is generated based on the aggregate dataset, and the privacy of the local dataset and learning model is protected against the cloud server. Extensive analysis shows that our schemes satisfy the security requirements of verifiability and privacy. Our implementation and experiments demonstrate that our system has a manageable computational efficiency and can be applied to a wide range of privacy-sensitive areas in deep learning.

Keywords: Deep learning, Privacy-preserving, Multi-party computation delegation, Cloud computing

[*] Corresponding author. Tel.: +86-029 88204749. *E-mail:* xfchen@xidian.edu.cn