(SD2019-340) Collaborative High-Dimensional Computing

Tech ID: 32280 / UC Case 2019-340-0

BACKGROUND

Internet of Things (IoT) applications often analyze collected data using machine learning algorithms. As the amount of the data keeps increasing, many applications send the data to powerful systems, e.g., data centers, to run the learning algorithms . On the one hand, sending the original data is not desirable due to privacy and security concerns.

On the other hand, many machine learning models may require unencrypted (plaintext) data, e.g., original images , to train models and perform inference . When offloading theses computation tasks, sensitive information may be exposed to the untrustworthy cloud system which is susceptible to internal and external attacks . In many IoT systems , the learning procedure should be performed with the data that is held by a large number of user devices at the edge of Internet . These users may be unwilling to share the original data with the cloud and other users if security concerns cannot be addressed.

TECHNOLOGY DESCRIPTION

Reseachers from UC San Diego have addressed the current limitations by developing a new framework, referred to as SecureHD, which can provide a secure learning solution based on the application of high-dimensional (HD) computing. This invention can provide systems, circuits and computer program products providing a framework for secured collaborative training using hyper-dimensional vector based data encoding/decoding and related methods.

In one example, the original data can be encoded as secure, high-dimensional vectors , which can be used to train a model . Thus, applications can send their data to the cloud in a secured form , while the cloud can perform the offloaded tasks without additional decryption steps . In particular, SecureHD can be used to implement classification methods suitable to handle a large amount of data that the cloud typically processes. In addition , SecureHD can recover the encoded data in a lossless manner. As described herein, the SecureHD framework can perform the encoding and decoding tasks 145.6 times and 6.8 times faster, respectively, than an encryption / decryption library running on in a conventional system. In addition, embodiments according the present invention can provide accuracy of about 95% on average for diverse practical classification tasks including cloud scale datasets.

APPLICATIONS

ADVANTAGES

This technology (SecureHD framework):

- Performs the encoding and decoding tasks with high efficiency, e.g., 145.6× and 6.8× faster than the state-of-the-art encryption/decryption library.
- Achieves accuracy of 95% on average for diverse practical learning tasks.
- Provides lossless data recovery with 4× reduction in the data size compared to the existing encryption solution.

STATE OF DEVELOPMENT

CONTACT

Skip Cynar
scynar@ucsd.edu
tel: 858-822-2672.

OTHER INFORMATION

KEYWORDS

Internet of Things, Hyper-dimensional, high-dimensional (HD) computing, cloud computing, Machine learning, pattern classification, learning (artificial intelligence), data privacy, cryptography, Brain-inspired computing, Distributed learning, Secure learning, groupware

CATEGORIZED AS

- **Communications**
  - Internet
- **Computer**
  - Hardware
  - Security
  - Software

RELATED CASES

2019-340-0

UC San Diego's Office of Innovation & Commercialization is seeking companies interested in commercializing this technology into useful products and services.

INTELLECTUAL PROPERTY INFO

US 16/915,643 - Publication No.US-2020-0410404

SYSTEMS, CIRCUITS AND COMPUTER PROGRAM PRODUCTS PROVIDING A FRAMEWORK FOR SECURED COLLABORATIVE TRAINING USING HYPER-DIMENSIONAL VECTOR BASED DATA ENCODING/DECODING AND RELATED METHODS

RELATED MATERIALS

- M. Imani et al., "A Framework for Collaborative Learning in Secure High-Dimensional Space," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Milan, Italy, 2019, pp. 435-446, doi: 10.1109/CLOUD.2019.00076. - 07/08/2019

PATENT STATUS

Patent Pending

University of California, San Diego
Office of Innovation and Commercialization
9500 Gilman Drive, MC 0910, ,
La Jolla,CA 92093-0910

Tel: 858.534.5815
innovation@ucsd.edu
https://innovation.ucsd.edu
Fax: 858.534.7345