Privacy Preserving High-Order Bi-Lanczos in Cloud-Fog Computing for Industrial Applications

Jun Feng, Laurence T. Yang, *Fellow, IEEE*, Ronghao Zhang, Weizhong Qiang, and Jinjun Chen, *Senior Member, IEEE*

***Abstract*—Industrial cyber-physical-social systems (CPSSs), a prominent data-driven paradigm, tightly couple and coordinat social space into cyber-physical systems (CPSs) within industrial environments. With the proliferation of cloud-fog computing, cloud-fog computing becomes the most prominent computing paradigm used to implement industrial data analysis. However, the open environment of cloud-fog computing and the limited control of industrial CPSSs users make industrial data analysis without compromising users' privacy one great research challenge in practical cloud-fog-based industrial applications. High-order Bi-Lanczos (HOBI-Lanczos) approach has shown remarkable success in heterogeneous data analysis in industrial applications. In this paper, a novel privacy preserving HOBI-Lanczos approach using tensor train in cloud-fog computing is proposed for industrial data applications. Specifically, a privacy preserving industrial data analysis model using cloud-fog computing and tensor train is firstly proposed. The proposed model enables fogs and clouds to securely carry out industrial data analysis for large-scale tensors given in a tensor train format. In addition, by using this model, a privacy preserving HOBI-Lanczos approach is provided. Last but not least, by using a brain-controlled robot system case study, the proposed approach is theoretically and empirically analyzed. Our proposed approach is proven to be secure. A series of experiments corroborate the superiority of the proposed approach in cloud-fog computing for industrial applications.**

***Index Terms*—Fog Computing, privacy protection, high-order Bi-Lanczos, tensor analysis, industrial application, cloud-fog computing.**

I. Introduction

RECENTLY, we have been witnessing the flourish development of cyber-physical-social systems (CPSSs) in some practical industrial fields (e.g. manufacturing process control, and transportation systems) and hence industrial CPSSs appear [1, 2]. Industrial CPSSs include social space as a key part of modern industrial systems, promise a great number of innovative manufacturing intelligence and novel user experiences, and enable unprecedented performance and sustainable industrial production. Industrial CPSSs are the main enabling technology for Industrial Internet, Industry 4.0, and China Manufacturing 2025 [3]. In industrial processes, terabytes of data (i.e., big data) describing factory operations are produced from different sources worldwide per day. These data can be analysed to extract knowledge for helping industrial CPSSs to provide useful services, such as appropriate industrial decision-making, and equipment failure predictions.

In recent years, cloud-fog computing has shown great promising opportunities in industrial CPSSs [4]. Cloud is a centralized IT infrastructure providing huge resources, economical and flexible services for industrial CPSSs in an on-demand manner. Fog has bridged the gap between cloud data centers and industrial CPSSs devices. It can decrease bandwidth, and can reduce the burden of industrial clouds. Both the fog computing and cloud computing are interdependent with each other, and cloud-fog computing combines their advantages. Due to the requirements of industrial CPSSs data storage and analysis and the excellent features of cloud-fog computing, industrial CPSSs data storage and analysis are most commonly outsourced to cloud-fog computing [3]. Cloud-fog computing can solve many industrial problems properly. However, directly performing industrial CPSSs data storage and analysis in cloud-fog computing will arise some serious security concerns, for example violation of sensitive customer information and production-related data [5, 6]. To guarantee the privacy protection of industrial CPSSs, the sensitive and raw data in industrial CPSSs are encrypted locally before being sent to cloud-fog computing. After the industrial CPSSs data are encrypted, it becomes one of the emerging and grand challenging problems to efficiently mine them in a privacy-preserving way in cloud-fog-assisted industrial CPSSs [7, 8].

In the industrial CPSSs era, there is a rapidly growing requirement for industrial CPSSs data analysis. The high-order Bi-Lanczos (HOBI-Lanczos) approach is useful and has been applied to industrial CPSSs data analysis, such as feature extraction, clustering and recommendation of heterogeneous data [3]. The HOBI-Lanczos approach can significantly improve the efficiency of industrial CPSSs data analysis.

The ultimate goal of using cloud-fog computing is to carry out industrial CPSSs data analysis and hence a pri-

This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0801804, Grant 2019YFB170062, and Grant 2018YFB1800103; in part by the National Natural Science Foundation of China under Grant 61932010; and in part by the Fundamental Research Funds for the Central Universities in China under Grant 2018KFYXKJC046. (Corresponding author: Laurence T. Yang)

J. Feng is with the School of Cyber Science and Engineering, and Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: junfeng989@gmail.com).

L. T. Yang is with the School of Computer Science and Technology, and Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, Wuhan 430074, China, and the Department of Computer Science, St. Francis Xavier University, Antigonish, NS, Canada (e-mail: E-mail: ltyang@ieee.org).

R. Zhang is with the Luoyang Institute of Electro-Optical Equipment, AVIC, Luoyang 471000, China (e-mail: zrhfight@163.com).

W. Qiang is with the School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: wzqiang@hust.edu.cn).

J. Chen is with the Swinburne Data Science Research Institute, Swinburne University of Technology, Australia (e-mail: jinjun.chen@gmail.com).

vacy preserving HOBI-Lanczos approach over encrypted data is an essential requirement in cloud-fog computing based industrial CPSSs. To design reasonable HOBI-Lanczos approach over encrypted data for cloud-fog computing based industrial CPSSs, there are, however, several challenges and considerations which are presented as follows. Firstly, to preserve industrial CPSSs user's data security, HOBI-Lanczos is required to be executed without the fog or cloud obtaining or inferring the user's raw data in privacy preserving cloud-fog-assisted industrial CPSSs. Secondly, because industrial CPSSs users may have limited resources in terms of computation and communication, and after outsourcing data to cloud-fog computing we cannot guarantee the users remain online. As a consequence, we should design an approach which can keep users from participating in some tasks during the procedure of HOBI-Lanczos in cloud-fog computing.

For addressing the above problems, the paper proposes a privacy preserving HOBI-Lanczos approach based on tensor train (TT) over semantically secure encrypted TT cores in cloud-fog computing for industrial CPSSs. In the paper, we make the following specific contributions.

- A privacy preserving industrial CPSSs data analysis model is designed for cloud-fog computing. The model combines the properties of tensor train networks and homomorphic encryption. The model allows user to employ the storage and analysis power of cloud-fog computing, without divulging any sensitive data in industrial environments. In the model, after the encrypted tensor-train cores have been sent to the cloud-fog computing, industrial CPSSs user does not need to participate in any calculations in industrial CPSSs data analysis, which can significantly reduce the computation burden on the industrial CPSSs user. This paper is, as we know, the first to propose concrete privacy preserving industrial CPSSs data analysis model that enables privacy preserving and efficient storage and computation in cloud-fog computing.
- A privacy preserving HOBI-Lanczos approach based on TT is presented by using the privacy preserving industrial CPSSs data analysis model. The proposed approach can be deployed in cloud-fog computing to protect industrial CPSSs user's privacy. To implement the approach, we design some privacy preserving tensor-train-based protocols, which can be widely used for other privacy preserving industrial CPSSs data analysis.
- The formal security analysis is provided to demonstrate that the privacy preserving HOBI-Lanczos approach based on TT guarantees user's privacy in the well-known semi-honest model. In addition, the approach was implemented and evaluated with a brain-controlled robot system case study. A series of experiments corroborate that the proposed approach in cloud-fog computing can achieve privacy preserving, low user costs, flexible services, and accuracy assurance.

The paper is organized as follows. Section II provides preliminaries used in the paper. Section III proposes the privacy preserving industrial CPSSs data analysis model using cloud-fog computing. The privacy preserving HOBI-Lanczos approach based on TT in cloud-fog computing is elaborated in Section IV. The validations for the proposed approach are reported in Section V. Sections VI and VII summarize the previous works and our conclusions.

II. Preliminaries

In this section, we briefly introduce some preliminaries (See also Table I).

TABLE I
Summary of Notations.

Notation	Definition
$\|\|X\|\|$	norm of tensor X
$G_1^X, G_2^X, \cdots, G_M^X$	core tensors of tensor $X \in R^{K_1 \times \cdots \times K_M}$
$X_{k_1 k_2 \cdots}$	$(k_1 k_2 \cdots)$ element of tensor X
$\times_i$	i-mode product
$*_N$	multilinear mode product
$E_{pk}(m)$ $(D_{sk}(c))$	encryption (decryption) of message m (ciphertext c) with public key pk (secret key sk)
$[\![m]\!]$	ciphertext of message m
$[\![X]\!]_{k_1 k_2 \cdots}$	$(k_1 k_2 \cdots)$ element of encrypted tensor $[\![X]\!]$

A. Tensor Basics

Tensors have been frequently used in data analyses [3] involving industry 4.0, smart factory, digital manufacturing, brain data analysis, urban computing and transportation systems [9, 10].

Multilinear Mode Product: The multilinear mode product of a tensor $T \in R^{I_1 \times I_2 \times \cdots \times I_M \times J_1 \times J_2 \times \cdots \times J_N}$ and a tensor $S \in R^{J_1 \times J_2 \times \cdots \times J_N \times K_1 \times K_2 \times \cdots \times K_O}$ is defined as $T *_N S$. $T *_N S$ has a size of $I_1 \times I_2 \times \cdots \times I_M \times K_1 \times K_2 \times \cdots \times K_O$, and the $(i_1 i_2 \cdots i_m k_1 k_2 \cdots k_o)$-th element of $T *_N S$ is computed by:

$$(T *_N S)_{i_1 i_2 \cdots i_m k_1 k_2 \cdots k_o} = \sum_{j_1 j_2 \cdots j_n} (t_{i_1 i_2 \cdots i_m j_1 j_2 \cdots j_n} s_{j_1 j_2 \cdots j_n k_1 k_2 \cdots k_o}). \quad (1)$$

Tensor Train (TT) Factorization: The tensor train factorization can decompose a tensor $T \in R^{I_1 \times \cdots \times I_M}$ as contracted products of TT cores $G_1^T, G_2^T, \cdots, G_M^T$. We can write

$$T = G_1^T \times^1 G_2^T \times^1 \cdots \times^1 G_M^T, \quad (2)$$

where $G_m^T \in R^{R_{m-1} \times I_m \times R_m}$, R_m $(m = 1, \cdots, M)$ is TT rank, and $R_0 = R_M = 1$.

B. Bi-Lanczos Approach

The Bi-Lanczos approach [3] is able to be used to reduce a matrix A with an orthogonal matrices $P = [p_1, p_2, \ldots]$ and $Q = [q_1, q_2, \ldots]$ into a bidiagonal matrix B where

$$B = \begin{bmatrix} \alpha_1 & & & \\ \beta_2 & \alpha_2 & & \\ & \beta_3 & \alpha_3 & \\ & & \ddots & \ddots \end{bmatrix}. \quad (3)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998086, IEEE Transactions on Industrial Informatics

The matrix B is gotten by iteratively calling the following iteration procedures

$$\begin{aligned} &q_i = A^T p_i - \beta_i q_{i-1}, \alpha_i = \|q_i\|, \\ &q_i = q_i/\alpha_i, p_{i+1} = Aq_i - \alpha_i p_i, \\ &\beta_{i+1} = \|p_{i+1}\|, p_{i+1} = p_{i+1}/\beta_{i+1}. \end{aligned} \tag{4}$$

In each iteration, the entries α_j and β_j of the matrix B can be obtained.

C. Homomorphic Cryptosystem

BV Homomorphic encryption is based on ring-LWE assumption [11]. Its construction is introduced as follows.

Let n be a power of 2, and q be odd prime number. $R_q \triangleq Z_q[x]/\langle x^n + 1\rangle$ is used to parametrize the cryptosystem. $R_p \triangleq Z_p[x]/< x^n + 1 >$ is used to define the message space, where p is a prime. Let $X = D_{Z^n,\sigma}$ denote a discrete Gaussian error distribution and its standard deviation is σ.

Key generation: Define the secret key $sk = s$, where s is a ring element sampled from X. Define the public key $pk = (b_0, b_1)$, where $b_0 = -(b_1 s + pe)$, b_1 is a uniformly random ring element sampled from R_q, and e is an error sampled from X.

Encryption: Given a message m , its ciphertext is calculated via

$$En(m, pk) = (ct_0, ct_1) \triangleq (b_0 u + pw + m, b_1 u + pv). \tag{5}$$

Decryption: Let $c = (ct_0, ct_1, \cdots, ct_\delta)$ is a ciphertext, we can calculate and output the message as

$$En(c, sk) = \left[\sum_{j=0}^{\delta} ct_j s^j\right]_q \mod p. \tag{6}$$

There are other homomorphic encryption schemes like Paillier cryptosystem, FHEW cryptosystem etc. Paillier cryptosystem only directly supports additive homomorphic, can not directly support multiplication homomorphic. FHEW scheme only supports boolean circuits and is computationally expensive. The BV homomorphic encryption scheme directly supports a limited number of both addition and multiplication operations between the encrypted data, and is easy to understand and implement. Following some recent works [12, 13] using BV homomorphic encryption scheme, we therefore also choose to use the BV homomorphic encryption scheme in this paper.

III. Problem Statement

The problem statement about privacy preserving industrial CPSSs data analysis model using cloud-fog computing and a framework of the proposed model for industrial applications are introduced in this section.

A. Problem Definition

The industrial CPSSs user plans to carry out industrial data storage and analysis, but he/she would not like to do these by himself/herself. The industrial CPSSs user will outsource the industrial data storage and analysis to cloud-fog computing.

To guard the industrial CPSSs privacy and reduce storage consumption in cloud-fog computing, the TT cores $G_1^X, G_2^X, \cdots, G_M^X$ of tensor $X \in R^{I_1 \times \cdots \times I_M}$ are encrypted, and these ciphertexts $[[G_1^X]], [[G_2^X]], \cdots, [[G_M^X]]$ are transmitted to one or more clouds. When the industrial CPSSs user implements a function, he/she requests the cloud-fog computing to carry out the function on his/her encrypted tensor-train cores $[[G_1^X]], [[G_2^X]], \cdots, [[G_M^X]]$. The industrial CPSSs user will receive the desired results from cloud-fog computing. The procedure of carrying out the function F without exposing the industrial CPSSs user's privacy over encrypted data $[[G_1^X]], [[G_2^X]], \cdots, [[G_M^X]]$ on cloud-fog computing is termed as privacy preserving function computation (PPFC) for industrial CPSSs. We assume the output is r_1. Only the industrial CPSSs user gets r_1 and nothing is revealed to the clouds or the fogs. Suppose r_2 is the output of the function F without any privacy protection on industrial CPSSs user's data X. In order to not decrease usability, we need to ensure that the following equation is satisfied: $r_1 \cong r_2$.

B. Privacy Preserving Industrial Data Analysis Model

To solve this problem properly, a privacy preserving industrial CPSSs data analysis model in cloud-fog computing is designed. The internal entities in the model are a user, m fog nodes $(F_1, F_2, \cdots, F_m)$, and two clouds (C_1 and C_2) as shown in Fig. 1. Let the two clouds together form a federated cloud. The framework using cloud-fog computing for industrial CPSSs is explained as follows.

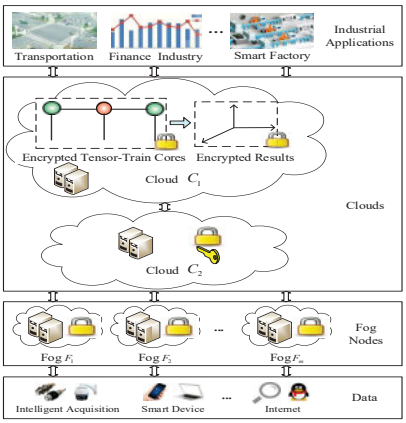


Fig. 1. Privacy preserving industrial CPSSs data analysis in cloud-fog computing.

1) In industrial CPSSs, data are continuously collected by industrial terminal nodes, such as sensors, actuators, high-definition cameras, and controllers from cyber world, physical world and social world. The data are represented by tensors T. The tensor train cores $G_1^X, G_2^X, \cdots, G_M^X$ of tensors T are encrypted. The encrypted tensor train cores $[[G_1^X]], [[G_2^X]], \cdots, [[G_M^X]]$ are transmitted to the clouds C_1, C_2, the fogs F_1, F_2,...,F_n.
2) The clouds C_1, C_2, the fogs F_1, F_2,...,F_n with the encrypted tensor train cores $[[G_1^X]], [[G_2^X]], \cdots, [[G_M^X]]$

collectively carry out industrial CPSSs data analysis using tensor-train operations in privacy preserving way. At the end of industrial CPSSs data analysis, the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n get the encrypted results and send them to the user. The privacy preserving tensor-train operations are obtained via tensor-train operations and homomorphic properties.

3) The results of industrial CPSSs data analysis are obtained from from the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n and can be used in transportation systems, industrial control, finance industry, smart factory and so on. For instance, high-speed train systems use the results to monitor the status of human operators in real time.

There are already some researches working on collusion-free angle, but they only focused on some problems, such as content-based publish subscribe, crowdsensing, data collection. These researches significantly differ from our work and the literatures [14, 15]. Our work is to solve the privacy-preserving HOBI-Lanczos problem, and especially our task is complex. Our security model assumes the existence of non-colluding semi-honest fogs and clouds. We emphasize that the security model is not new and has already been extensively used in a lot of recent related literatures [14, 15]. The reasons that the collusion attack between fogs and clouds is not considered in this paper are as follows. The majority of the cloud service providers (CSPs) are some well-established companies (e.g. General Electric Company Cloud and Amazon Cloud) in the industry. The clouds and the fogs are offered by different entities. The collusion attack between fogs and clouds is highly unlikely because the collusion will tarnish their reputations and will impact their revenues. In fact, it is also not hard to find non-colluding clouds and fogs in the market. Hence, it is a reasonable assumption that clouds and fogs will not collude in our proposed method. The security goal in our paper is to ensure that user's data are kept private against clouds and fogs.

IV. Proposed Approach

The privacy preserving HOBI-Lanczos approach based on TT is proposed in this section. Firstly, we give a HOBI-Lanczos approach. Then, to protect industrial CPSSs user's privacy in cloud-fog computing, we develop a privacy preserving HOBI-Lanczos approach using the privacy preserving tensor train model.

A. High-Order Bi-Lanczos (HOBI-Lanczos) Approach

A HOBI-Lanczos approach by extending Bi-Lanczos approach to tensor space is proposed in this subsection. Bi-Lanczos approach only can process matrix data whereas HOBI-Lanczos can be used to process tensor data.

Given a tensor $M \in R^{I_1 \times I_2 \times \cdots \times I_H \times I_{H+1} \times \cdots \times I_S}$, the HOBI-Lanczos algorithm is able to calculate the tensor M to tensors $W = (W_1\ W_2\ \cdots W_k)$, $Q = (Q_1\ Q_2\ \cdots Q_k)$, and one bidiagonal matrix $B \in R^{k \times k}$ so that

$$M = W *_1 B *_1 Q^T, \tag{7}$$

where W_i and Q_i $(1 \le i \le k)$ are orthonormal tensors. Algorithm 1 shows the outline of the HOBI-Lanczos approach.

Algorithm 1 High-Order Bi-Lanczos Approach

Input: Tensor $M \in R^{I_1 \times I_2 \times \cdots \times I_H \times I_{H+1} \times \cdots \times I_S}$.

Output: Orthogonal tensors $W \in R^{I_1 \times I_2 \times \cdots \times I_H \times k}$ and $Q \in R^{k \times I_{H+1} \times I_{H+2} \cdots \times I_S}$, and bidiagonal matrix $B \in R^{k \times k}$.

1: Input $W_1 \in R^{I_1 \times I_2 \times \cdots I_H}$, $Q_0 \in R^{I_{H+1} \times I_{H+2} \cdots \times I_S}$ such that $\|W_1\|_2 = 1$, $Q_0 = 0$
2: **for** $i = 1, 2, \cdots, p$ **do**
3: Compute $Q_i = M^T *_H W_i - \beta_i Q_{i-1}$
4: Obtain $\alpha_i = \|Q_i\|$
5: Compute $Q_i = Q_i / \alpha_i$
6: Compute $W_{i+1} = M *_{S-H} Q_i - \alpha_i W_i$
7: Obtain $\beta_{i+1} = \|W_{i+1}\|$
8: Compute $W_{i+1} = W_{i+1} / \beta_{i+1}$
9: **end for**

B. Privacy Preserving HOBI-Lanczos Approach Using TT in Cloud-Fog Computing

The privacy preserving HOBI-Lanczos approach can be leveraged to protect industrial CPSSs user's privacy. In this subsection, however, we try to present an alternative approach. We propose a set of privacy preserving tensor train protocols and apply them to construct a new privacy preserving HOBI-Lanczos approach in cloud-fog computing.

The privacy preserving division (SD) protocol over encrypted data $[\![m_1]\!]$ and $[\![m_2]\!]$ is as follows: $SD([\![m_1]\!], [\![m_2]\!]) \rightarrow [\![m_1/m_2]\!]$.

Privacy Preserving Tensor Addition Protocol and Privacy Preserving Inner Product Protocol over Encrypted TT: If the fog F_i or the cloud C_1 holds the encrypted TT cores $\left[\!\left[G_1^A\right]\!\right], \left[\!\left[G_2^A\right]\!\right], \cdots, \left[\!\left[G_H^A\right]\!\right]$ of tensor $A \in R^{I_1 \times \cdots \times I_H}$ and the encrypted TT cores $\left[\!\left[G_1^B\right]\!\right], \left[\!\left[G_2^B\right]\!\right], \cdots, \left[\!\left[G_H^B\right]\!\right]$ of tensor $B \in R^{I_1 \times \cdots \times I_H}$, and the cloud C_2 holds private key, then (1) the cloud C_1 can get the encrypted TT cores $\left[\!\left[G_1^C\right]\!\right], \left[\!\left[G_2^C\right]\!\right], \cdots, \left[\!\left[G_H^C\right]\!\right]$ of tensor $C = A + B$ with the help of the cloud C_2, where

$$\left[\!\left[G_i^C\right]\!\right] = \left[\!\left[G_i^A\right]\!\right] \oplus \left[\!\left[G_i^B\right]\!\right], \tag{8}$$

for $i = 1, \cdots, H$. Furthermore, The fog F_i or the cloud C_1 can get

$$[\![C]\!] = \left(\left[\!\left[G_1^A\right]\!\right] \oplus \left[\!\left[G_1^B\right]\!\right]\right) \tilde{\times}^1 \cdots \tilde{\times}^1 \left(\left[\!\left[G_H^A\right]\!\right] \oplus \left[\!\left[G_H^B\right]\!\right]\right). \tag{9}$$

(2) the cloud C_1 can get the encrypted inner product

$$\begin{aligned}[\![\langle A, B\rangle]\!] = (\widetilde{\odot}_{i_1=1}^{I_1}(&\left[\!\left[G_{i_1}^A\,[i_1]\right]\!\right] \widetilde{\otimes} \left[\!\left[G_{i_1}^B\,[i_1]\right]\!\right]))\widetilde{\times} \cdots \\ \widetilde{\times}(\widetilde{\odot}_{i_H=1}^{I_H}(&\left[\!\left[G_{i_H}^A\,[i_H]\right]\!\right] \widetilde{\otimes} \left[\!\left[G_{i_H}^B\,[i_H]\right]\!\right]))\end{aligned} \tag{10}$$

with the help of the cloud C_2. No information about the tensors A, B and C, and the inner product $\langle A, B\rangle$ will be divulged to the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n.

Privacy Preserving Einstein Product Protocol on Encrypted TT: If the fog F_i or the cloud C_1 holds the encrypted TT cores $\left[\!\left[G_1^A\right]\!\right], \left[\!\left[G_2^A\right]\!\right], \cdots, \left[\!\left[G_H^A\right]\!\right]$ of tensor $A \in R^{I_1 \times \cdots \times I_H}$ and the encrypted TT cores $\left[\!\left[G_1^B\right]\!\right], \left[\!\left[G_2^B\right]\!\right], \cdots, \left[\!\left[G_L^B\right]\!\right]$ of tensor $B \in R^{I_1 \times \cdots \times I_L}$, and the cloud C_2 holds private key, then the fog F_i or the cloud C_1 can get the encrypted TT cores

$\left[\left[G_1^E\right]\right], \left[\left[G_2^E\right]\right], \cdots, \left[\left[G_{H+L-2k}^E\right]\right]$ of tensor $E = A *_k B$ with the help of the cloud C_2, where

$$\begin{aligned}
&\left[\left[G_m^E\right]\right] = \left[\left[G_m^A\right]\right], \text{ for } m = 1, \cdots, H-k-1;\\
&\left[\left[G_{H-k}^E\right]\right] = \left[\left[G_{H-k}^A\right]\right] \widetilde{\times}^1 \left(\left[\left[G_{H-k+1}^A\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_H^A\right]\right]\right)\\
&\widetilde{*}_k \left(\left[\left[G_1^B\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_k^B\right]\right]\right);\\
&\left[\left[G_{H-k+m}^E\right]\right] = \left[\left[G_{k+m}^B\right]\right], \text{ for } m = 1, \cdots, L-k.
\end{aligned} \tag{11}$$

The fog F_i or the cloud C_1 can get the encrypted tensor

$$\begin{aligned}
&[\![E]\!] = \left[\left[G_1^A\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 (\left[\left[G_{H-k}^A\right]\right] \widetilde{\times}^1 (\left[\left[G_{H-k+1}^A\right]\right]\\
&\widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_H^A\right]\right]) \widetilde{*}_k (\left[\left[G_1^B\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_H^B\right]\right]))\\
&\widetilde{\times}^1 \left[\left[G_{k+1}^B\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_L^B\right]\right]
\end{aligned} \tag{12}$$

with the help of the cloud C_2. No information about the tensors A, B and E will be divulged to the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n.

The user selects a random tensor $G_s^{M'}$ and encrypts the tensor G_s^M by computing the tensor $G_s^{M''} = G_s^M - G_s^{M'}$ for $1 \le s \le S$. The user sends the ciphertext tensors $G_s^{M'}, G_s^{M''}$ of the tensor G_s^M $(1 \le s \le S)$ to the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n, respectively. For convenience, we denote $[\![A]\!]$ as the ciphertext tensors A', A'' of tensor A.

Then, we propose a privacy-preserving HOBI-Lanczos approach based on TT ($PHBLT$) in cloud-fog computing, summarized in Algorithm 2. Its basic idea is to combine privacy preserving tensor train and HOBI-Lanczos approach to achieve privacy preserving in the computations of HOBI-Lanczos. One user outsources the encrypted TT cores $\left[\left[G_1^M\right]\right], \left[\left[G_2^M\right]\right], \cdots, \left[\left[G_S^M\right]\right]$ of tensor $M \in R^{I_1 \times I_2 \times \cdots \times I_H \times I_{H+1} \times \cdots \times I_S}$ to cloud-fog computing for storage and analysis. The cloud C_1 with the encrypted TT cores $\left[\left[G_1^M\right]\right]$, $\left[\left[G_2^M\right]\right]$, $\cdots$,$\left[\left[G_{2H}^M\right]\right]$, the fogs F_1, F_2,...,F_n, and the cloud C_2 with private key sk will calculate the encrypted orthogonal tensors $[\![W]\!]$ and $[\![Q]\!]$ and the encrypted matrix $[\![B]\!]$ without divulging M, W, Q, B, or intermediate values to the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n. Only the cloud C_1 will have access to ciphertexts $[\![V]\!]$ and $[\![L]\!]$. The $PHBLT$ approach is written as follows:

$$PHBLT(\left[\left[G_1^M\right]\right], \left[\left[G_2^M\right]\right], \cdots, \left[\left[G_S^M\right]\right]) \rightarrow ([\![W]\!], [\![B]\!], [\![Q]\!]). \tag{13}$$

The protocol is shown in details.

Firstly, the cloud C_1 inputs $W_1 \in R^{I_1 \times I_2 \times \cdots I_H}$ such that $\|W_1\|_2 = 1$, and $\beta_1 = 0$ in step 2. Using the tensor train factorization, the cloud C_1 gets $W_1 = G_1^{W_1} \times^1 \cdots \times^1 G_H^{W_1}$ in step 3.

Then, for $j = 1, 2, \cdots, p$:

1) In steps 7 and 8, applying the privacy preserving Einstein product protocol over encrypted TT, the cloud C_1, the fogs F_1, F_2,...,F_n, and the cloud C_2 jointly and securely calculate the encrypted TT cores $\left[\left[G_h^{Q_j}\right]\right]$ $(h = 1, \cdots, H)$ of the tensor $Q_j = M^T *_H W_j - \beta_j Q_{j-1}$. After the cloud C_1 obtains the encrypted TT cores $\left[\left[G_h^{Q_j}\right]\right]$ $(h = 1, \cdots, H)$, the clouds C_1, C_2, and the fogs F_1, F_2,...,F_n carry out the privacy preserving TT-rounding procedure to reduce the ranks of the encrypted TT cores $\left[\left[G_h^{Q_j}\right]\right]$ $(h = 1, \cdots, H)$.

Algorithm 2 Privacy Preserving HOBI-Lanczos Approach Using TT in Cloud-Fog Computing

Input: Cloud C_1: Encrypted TT cores $\left[\left[G_1^M\right]\right], \left[\left[G_2^M\right]\right], \cdots, \left[\left[G_S^M\right]\right]$. Cloud C_2: Private key sk.
Output: Cloud C_1 outputs encrypted orthogonal tensors $[\![W]\!]$ and $[\![Q]\!]$, and encrypted bidiagonal matrix $[\![B]\!]$.

1: Cloud C_1:
2: Input $[\![W_1]\!] \in R^{I_1 \times I_2 \times \cdots I_H}$ such that $\|W_1\|_2 = 1$
3: Compute $W_1 = G_1^{W_1} \times^1 \cdots \times^1 G_H^{W_1}$
4: Cloud C_1, Fogs F_1, F_2,...,F_n and Cloud C_2:
5: **for** $j = 1, 2, \cdots, k$ **do**
6: /*Compute the encrypted TT cores $\left[\left[G_h^{Q_j}\right]\right]$ $(h = 1, \cdots, H)$*/
7: $\left[\left[G_h^{Q_j}\right]\right] = \left[\left[G_h^{M^T}\right]\right] \oplus \left[\left[G_h^{Q_{j-1}}\right]\right]$ $(h = 1, \cdots, S-H-1)$
8: $\left[\left[G_{S-H}^{Q_j}\right]\right] = (\left[\left[G_{S-H}^{M^T}\right]\right] \widetilde{\times}^1 ((\left[\left[G_{S-H+1}^{M^T}\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_S^{M^T}\right]\right]) \widetilde{*}_H (\left[\left[G_1^{W_j}\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_H^{W_j}\right]\right])))$ $\oplus (\left[\left[G_{S-H}^{Q_{j-1}}\right]\right] \widetilde{\cdot} [\![\beta_j]\!]^{N-1})$
9: /*Obtain the encrypted value $\left[\left[\|Q_j\|^2\right]\right]$*/
10: $\left[\left[\|Q_j\|^2\right]\right] = (\widetilde{\odot}_{i_1=1}^{I_1} (\left[\left[G_{i_1}^{Q_j^T}[i_1]\right]\right] \widetilde{\otimes} \left[\left[G_{i_1}^{Q_j}[i_1]\right]\right]))$ $\widetilde{\times} \cdots \widetilde{\times} (\widetilde{\odot}_{i_H=1}^{I_{S-H}} (\left[\left[G_{i_{S-H}}^{Q_j^T}[i_{S-H}]\right]\right] \widetilde{\otimes} \left[\left[G_{i_{S-H}}^{Q_j}[i_{S-H}]\right]\right]))$
11: /*Compute the encrypted TT cores $\left[\left[G_{S-H}^{Q_j}\right]\right]$*/
12: $\left[\left[G_{S-H}^{Q_j}\right]\right] = \left[\left[G_{S-H}^{Q_j}\right]\right] \widetilde{\div} [\![\alpha_j]\!]$
13: /*Compute the encrypted TT cores $\left[\left[G_h^{W_{j+1}}\right]\right]$, $(h = 1, \cdots, H)$*/
14: $\left[\left[G_h^{W_{j+1}}\right]\right] = \left[\left[G_h^{M^T}\right]\right] \oplus \left[\left[G_h^{Q_j}\right]\right]$ $(h = 1, \cdots, H-1)$
15: $\left[\left[G_H^{W_{j+1}}\right]\right] = (\left[\left[G_H^{M^T}\right]\right] \widetilde{\times}^1 ((\left[\left[G_{H+1}^{M^T}\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_S^{M^T}\right]\right]) \widetilde{*}_{S-H} (\left[\left[G_1^{Q_j}\right]\right] \widetilde{\times}^1 \cdots \widetilde{\times}^1 \left[\left[G_{S-H}^{Q_j}\right]\right]))) \oplus (\left[\left[G_H^{W_j}\right]\right] \widetilde{\cdot} [\![\alpha_j]\!]^{N-1})$
16: /*Obtain the encrypted value $\left[\left[\|W_{j+1}\|^2\right]\right]$*/
17: $\left[\left[\|W_{j+1}\|^2\right]\right] = (\widetilde{\odot}_{i_1=1}^{I_1} (\left[\left[G_{i_1}^{W_{j+1}^T}[i_1]\right]\right] \widetilde{\otimes} \left[\left[G_{i_1}^{W_{j+1}}[i_1]\right]\right]))$ $\widetilde{\times} \cdots \widetilde{\times} (\widetilde{\odot}_{i_H=1}^{I_H} (\left[\left[G_{i_H}^{W_{j+1}^T}[i_H]\right]\right] \widetilde{\otimes} \left[\left[G_{i_H}^{W_{j+1}}[i_H]\right]\right]))$
18: /*Compute the encrypted TT cores $\left[\left[G_H^{W_{j+1}}\right]\right]$*/
19: $\left[\left[G_H^{W_{j+1}}\right]\right] = \left[\left[G_H^{W_{j+1}}\right]\right] \widetilde{\div} [\![\beta_{j+1}]\!]$
20: **end for**

2) Using the privacy preserving inner product protocol on encrypted TT, the cloud C_1, the fogs F_1, F_2,...,F_n, and the cloud C_2 compute the encrypted value $\left[\left[\|Q_j\|^2\right]\right]$ in a privacy preserving way on the encrypted TT cores $\left[\left[G_1^{Q_j^T}\right]\right], \left[\left[G_2^{Q_j^T}\right]\right], \cdots, \left[\left[G_{S-H}^{Q_j^T}\right]\right]$ and $\left[\left[G_1^{Q_j}\right]\right], \left[\left[G_2^{Q_j}\right]\right], \cdots, \left[\left[G_{S-H}^{Q_j}\right]\right]$ in step 10.
3) With the help of the cloud C_2, the cloud C_1 obtains the encrypted TT cores $\left[\left[G_{S-H}^{Q_j}\right]\right] = \left[\left[G_{S-H}^{Q_j}\right]\right] \widetilde{\div} [\![\alpha_j]\!]$ in

step 12.

4) The procedures in steps 13-19 are similar to those in steps 6-9. The encrypted data $\left[\left[G_h^{W_{j+1}}\right]\right]$ $(h = 1, \cdots, H)$, $\left[\left[\left\|W_{j+1}\right\|^2\right]\right]$, and $\left[\left[G_H^{W_{j+1}}\right]\right]$ can be computed.

The clouds C_1, C_2, and the fogs F_1, F_2,...,F_n send the ciphertexts W', W'', Q', Q'', and B', B'' to the user.

After obtaining the data W', W'', Q', Q'', B', and B'', the user decrypts them to obtain W, Q, and B by calculating W=$W' + W''$, Q =$Q' + Q''$, and B=$B' + B''$.

V. Evaluations and Application

Brain-controlled robot systems are emerging and important industrial systems, where the brain-controlled robot can provide an extra hand for human. In this section, using the case study of a brain-controlled robot system, we show how the proposed PHBLT approach can be applied in practice. We assume that in brain-controlled robot system the user's electroencephalogram data are uploaded to cloud-fog computing for storage and analysis. For protecting the data owner's privacy, the electroencephalogram data are encrypted. The cloud-fog computing performs the proposed PHBLT approach and can not see the user's real data. The processing results can be used for feature extraction, clustering and recommendation.

A. Performance analysis

1) Security: The fogs F_1, F_2,...,F_n, and the cloud C_1 only obtains the encrypted values $[\![M]\!]$ and $\left[\left[G_1^M\right]\right], \left[\left[G_2^M\right]\right], \cdots, \left[\left[G_S^M\right]\right]$ of the user's electroencephalogram data, the encrypted values of the intermediate results, and the encrypted variables $[\![W]\!]$, $[\![Q]\!]$, and $[\![B]\!]$. The encrypted values are gotten via the homomorphic cryptosystem. So, our PHBLT approach preserves the data owner's privacy from F_1, F_2,...,F_n, and C_1. The cloud C_2 only knows blinded values or random values. Hence, the data owner's privacy is protected from C_2 in the proposed PHBLT approach.

The formal definition from the literature [14, 15] is used to describe security against semi-honest adversaries, which is used in many researches.

Definition 1: Assume a_k and b_k represent the input and the output of protocol P for party C_k, $EI(P, C_k)$ denotes the execution image of P for party C_k, $\equiv$ denotes computational indistinguishability. Then the protocol P is secure against semi-honest adversaries if $EI(P, C_k) \equiv SI(P, C_k)$, where $SI(P, C_k)$ represents the simulated image of P for party C_k and is able to be simulated from a_k and b_k.

Proposition 1: The PHBLT approach proposed in this paper is secure under the semi-honest model.

Proof 1: We assume that $EI(PHBLT, C_1)$ and $SI(PHBLT, C_1)$ represent the execution and simulated images of C_1 of our PHBLT approach. $EI(PHBLT, C_1) = \{G_s^{M''}, m_1^k | 1 \le s \le S, 1 \le k \le K\}$ can be obtained, where $G_s^{M''} = G_s^M - G_s^{M'}$, and m_1^k represents the data that C_1 receives in our PHBLT approach. We assume that $E(Y)$ represents any element for any tensor Y. $SI(PHBLT, C_1) = \{R_s, r_1^k | 1 \le s \le S, 1 \le k \le K\}$, and R_s is one picked random tensor, and $E(R_s) \in Z_N$. As $G_s^{M'}$ is one random tensor and $E(G_s^{M'}) \in Z_N$, $G_s^{M''} \equiv R_s$ for $1 \le s \le S$ is obtained. The corresponding simulator can be called to simulate m_1^k. $m_1^k \equiv r_1^k$ for $1 \le k \le K$ is obtained. Hence $EI(PHBLT, C_1) \equiv SI(PHBLT, C_1)$. We assume that $EI(PHBLT, C_2)$ and $SI(PHBLT, C_2)$ denote the execution and simulated images of C_2, and $EI(PHBLT, F_j)$ and $SI(PHBLT, F_j)$ denote the execution and simulated images of F_j. $EI(PHBLT, C_2) \equiv SI(PHBLT, C_2)$ and $EI(PHBLT, F_j) \equiv SI(PHBLT, F_j)$ $(1 \le j \le n)$ can be obtained in a similar way.

The fogs F_1, F_2,...,F_n, and the clouds C_1, C_2 cannot see the user's data. Consequently, based on the above results, the proposed PHBLT approach is secure in the semi-honest model in brain-controlled robot system.

2) Computational Cost and Communication Cost: Let $rt(X)$ denote the maximum rank of the TT cores of arbitrary tensor X. The tensor $M \in R^{I_1 \times I_2 \times \cdots \times I_H \times I_{H+1} \times \cdots \times I_S}$ is an S-th order tensor of size $I_1 \times I_2 \times \cdots \times I_H \times I_{H+1} \times \cdots \times I_S$. Assume k represents the number of iteration, $rt(W_i)$ <= $rt(M)$, $rt(Q_i)$ <= $rt(M)$. Then, the computational cost of the proposed privacy preserving HOBI-Lanczos approach is $O(k \cdot (I_1 \cdot I_2 \cdots \cdot I_H \cdot (rt(M))^2 + I_{H+1} \cdot I_{H+2} \cdots \cdot I_S \cdot (rt(M))^2))$ secure multiplications. Let se denote the size of the ciphertext in this paper. The communication cost of the secure multiplication protocol is small constant rounds. Therefore, the communication complexity of the proposed privacy preserving HOBI-Lanczos approach is bounded by $O(k \cdot (I_1 \cdot I_2 \cdots \cdot I_H \cdot (rt(M))^2 + I_{H+1} \cdot I_{H+2} \cdot \cdots \cdot I_S \cdot (rt(M))^2) \cdot se)$ bits.

B. Performance Evaluations

The subsection shows experiment results to corroborate the performance of the proposed PHBLT approach. Our experiments are implemented in JAVA on computers with 16GB RAM running Windows systems. The homomorphic cryptosystem is used to encrypt the user's data. The original basic PHBLT approach and the PHBLT approach based on TT are also implemented. The data are multiplied by an appropriate number to scale up the values.

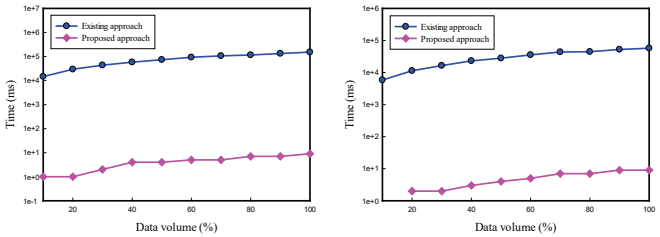
We used the electroencephalogram data from real-world BCI dataset (EEGDataset.rar, http://bcmi.sjtu.edu.cn/resource.html), which is widely used in brain-controlled robot research. The BCI dataset contains left/right motor imagery movements of five subjects. The dataset forms a channel-frequency bin-time frame-number tensor of size $62 \times 23 \times 50 \times 60$.

1) Computation Overhead of Users: After the user's encrypted data are outsourced to the cloud C_1, the user does not partake in the computation in the proposed PPTD approach. So, the computation cost for the user rests with the number of data records, the encryption time, and the decryption time.

We empirically compared the user's costs of the proposed PHBLT approach and those of the existing approach using the properties of homomorphic cryptosystem over the BCI dataset for the varying number of data. Fig. 2(a) and Fig. 2(b) depicts the comparison results in terms of the encryption time and the decryption time on the user side.

There is a linear growth of the user's time with the number of data the user encrypts or decrypts. As depicted by Fig. 2(a),

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998086, IEEE Transactions on Industrial Informatics



(a) Encryption time on user side (b) Decryption time on user side

Fig. 2. Time consumption of user sides for the PHBLT approach and the existing approach on the BCI dataset.

the encryption time on the user side of the PHBLT approach increases from 1ms to 4ms, while that of the existing approach increases from 29436ms to 73508ms as the proportion of the number of data records grows from 20% to 50%. But, the PHBLT approach posts lesser time compared to the existing approach. For instance, the user's time of the PHBLT approach and the existing approach is 5ms and 35551ms respectively, when the proportion of the number of data records is 60%, as shown in Fig. 2(b).

Therefore, the computation overheads of the user sides of our PHBLT approach are very low. The proposed PHBLT approach is particularly suitable for resource restricted industrial CPSSs devices (controller, smart cards, smart sensors, for example).

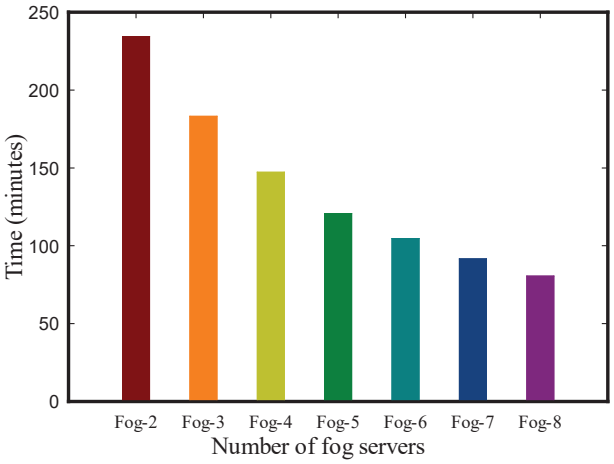


Fig. 3. Time cost of the PHBLT approach on the BCI dataset.

2) Storage Cost: The storage costs of the proposed PHBLT approach and the existing approach [3] were empirically compared. Table II shows the comparison of storage costs. From Table II, the storage of the proposed PHBLT approach needs much less space than that of the existing approach. For example, the number of the elements in the original tensor is 4278000 while that of the elements in the TT cores is 89740 when the TT-ranks are 20, 35, and 40. This is because the number of the elements in the TT cores is less than that of the elements in the original tensor. Therefore, significant storage space saving can be achieved by the proposed PHBLT approach in cloud-fog computing.

3) Execution Time in Cloud-Fog Computing: The execution time in cloud-fog computing of the PHBLT approach was empirically evaluated. The computations in the PHBLT approach are based on TT decomposition. We implemented the distributed PHBLT approach in cloud-fog computing. We tested the time for the varying number of fogs.

TABLE II
COMPARISON OF STORAGE COST.

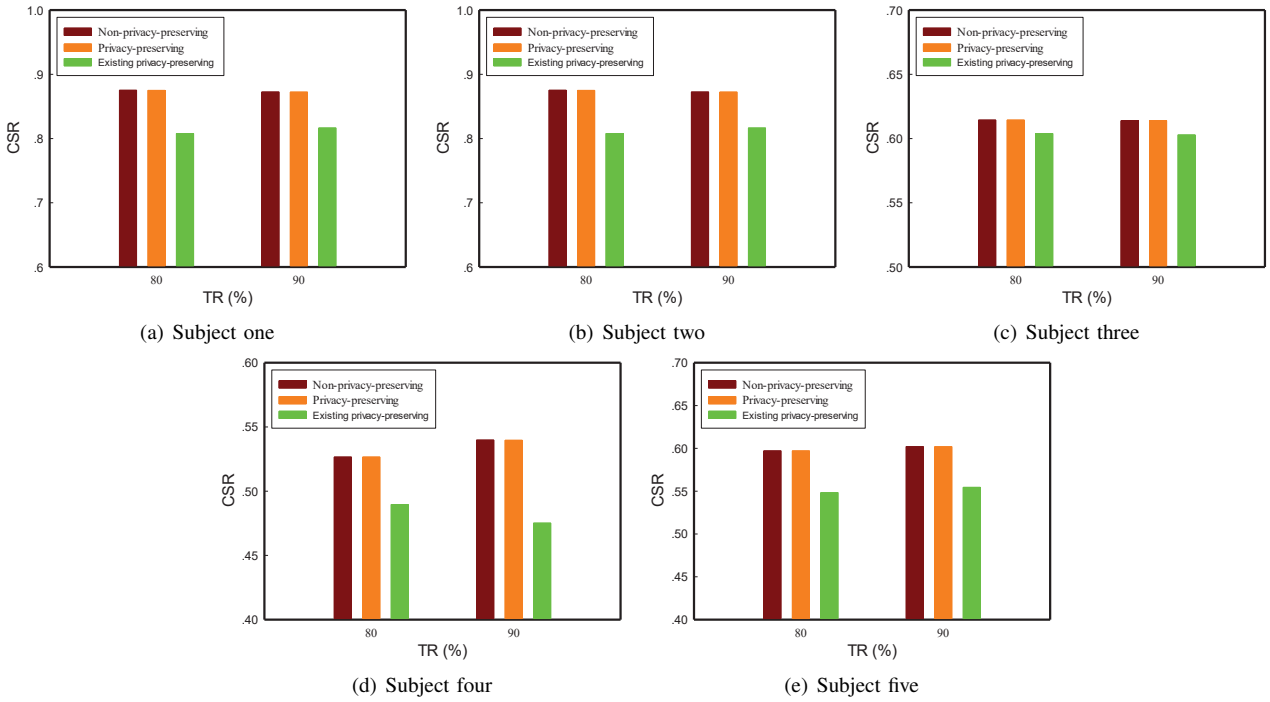
	Existing approach	Proposed approach
$R_1 = 40, R_2 = 50, R_3 = 60$	4278000	202080
$R_1 = 20, R_2 = 35, R_3 = 40$	4278000	89740

The execution time in cloud-fog computing of the PHBLT approach on the BCI dataset is shown in Fig. 3. Fog-i represents that the proposed PHBLT approach is run on i fogs. From Fig. 3, the execution time decreases from 183.11 minutes to 104.62 minutes when the number of fogs grows from 3 to 6. We find that that the distributed PHBLT approach is efficient. The performance of the proposed PHBLT approach can be improved in practical cloud-fog computing environments with high processing power.

4) Accuracy of the PHBLT approach: In order to evaluate the effectiveness of our proposed PHBLT approach, we implemented the electroencephalogram data classification based on our proposed PHBLT approach for the brain-controlled robot system. The proposed PHBLT approach was used for preprocessing on electroencephalogram data, and then the linear discriminant analysis (LDA) classifier algorithm with input data generated from the proposed PHBLT approach was employed for classification. The classification results were used to enable robot to understand the electroencephalogram. Some empirical experiments were conducted validate the effectiveness of our proposed PHBLT approach on the BCI dataset. Both the empirical experiments using the HOBI-Lanczos approach without privacy preserving and the empirical experiments using the existing privacy-preserving approach in the literature [3] were conducted. The classification success rate (CSR), one representative evaluation criterion criteria in classification, was employed to assess the accuracy of classification results for these approaches. Let nu_{cs} and nu respectively represent the number of the objects classified successfully and the total number of the objects. The CSR is defined as $CSR = nu_{cs}/nu$.

Fig. 4 provides the accuracy of the approach based on the proposed PHBLT approach, the HOBI-Lanczos approach without privacy preserving, and the existing privacy-preserving approach. Fig. 4(a), Fig. 4(b), Fig. 4(c), Fig. 4(d), and Fig. 4(e) show the accuracy for subject one, subject two, subject three, subject four, and subject five. From Fig. 4(a), we can get that the CSR of the proposed PHBLT approach is 87.24% while that of the approach without privacy preserving is 87.25% and that of the existing privacy-preserving approach is 81.65% on the BCI dataset when the truncate rate TR is 90% for subject one. We find the accuracy of the PHBLT approach is nearly equal to that of the approach without privacy preserving. We also find that the accuracy of our proposed PHBLT approach

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998086, IEEE Transactions on Industrial Informatics



(a) Subject one (b) Subject two (c) Subject three

(d) Subject four (e) Subject five

Fig. 4. Comparison of CSR of the proposed PHBLT approach, the approach without privacy preserving, and the existing privacy-preserving approach [3] on the BCI dataset.

is higher than that of the existing privacy-preserving approach in the literature [3].

The proposed PHBLT approach takes advantage of cloud-fog computing, ease user's burden, and guarantees the privacy protection of user's data, furthermore the approach can achieve accuracy assurance. Hence, the proposed PHBLT approach is superior when deployed in cloud-fog computing.

VI. Related Works

A lot of efforts have been made about privacy computing. Existing researches about privacy computing in fog or cloud-fog enhanced industrial CPSSs are provided in this section.

Privacy computing in fog environments is to use multiple fog nodes to aid users while ensuring the privacy protection of the data owner's data. Recent literature has proposed some methods. For example, the literature [16] showed the related security and trust issues in fog computing, and reviewed the existing solutions to such issues. Lu et al. [17] designed an efficient and secure data aggregation method in fog computing for IoT. Ni et al. [18] proposed a task allocation and secure data deduplication method based on fog computing. A differentially private publish-subscribe method in fog computing environment was proposed by Wang et al. [19]. A secure caching scheme solution based on fog computing was presented for disaster backup in mobile social networks in the literature [20]. However, our approach significantly differs from these above researches in terms of problem setting and target.

Recently, some elegant efforts for privacy computing in cloud-fog environments have been presented. Privacy preserving cloud-fog computing is to research how to guarantee the privacy protection of the user's data in cloud-fog computing environment and make use of cloud-fog computing. Yu et al. [21] presented a verifiable data deletion and flexible access control method for cloud-fog-based industrial applications. The literature [22] proposed a verifiable and secure outsourced access control method in cloud-fog environments. Similar to the literature [22], a cryptography-based verifiable and privacy-preserving access control method was proposed for data sharing in cloud-fog computing in the literature [23].

An efficient privacy preserving query approach using cloud-fog computing for IoT was presented in the literature [24]. Lyu et al. [25] proposed an efficient and privacy preserving aggregation scheme for cloud-fog computing enhanced smart grid. A efficient and secure data storage and searching system using cloud-fog computing for industrial IoT was designed by Fu et al. in the literature [26]. A differential privacy scheme based on cloud-fog computing was designed for governmental data publishing in the literature [27]. A privacy-preserving approach for outsourcing computation of high-order Bi-Lanczos in cloud-fog computing was proposed in the literature [3]. Inspired by previous researches, we propose the privacy preserving HOBI-Lanczos approach based on TT over encrypted data in cloud-fog computing. However, the approach in our paper significantly differs from these above researches. The proposed approach focuses on HOBI-Lanczos problem based on TT in cloud-fog computing for industrial CPSSs whereas these above researches focuses on other problems. In comparison with the existing approach [3], our proposed approach has low storage consumption and high accuracy.

VII. Conclusions

Security and privacy are non-trial problems in cloud-fog-assisted industrial CPSSs. In the paper, a novel privacy preserving HOBI-Lanczos approach based on TT in cloud-fog

computing for industrial CPSSs was proposed. Besides, the proposed approach was applied to a brain-controlled robot system to verify the effectiveness of the proposed approach. Our results corroborated that the proposed approach based on cloud-fog computing is superior for industrial CPSSs.

As future research work, we would like to explore the approach to some other tensor-based applications in cloud-fog computing, particularly in the field of industrial CPSSs. The research about collusion-free approach is different from the research in our paper. We also plan to extend the proposed approach to one new approach which can resist collusion attacks to move the industrial CPSSs forward. We also plan to explore the energy cost [28] in the proposed approach to achieve sustainable secure industrial CPSSs.

REFERENCES

[1] J. Zeng, L. T. Yang, M. Lin, H. Ning, and J. Ma, "A survey: Cyber-physical-social systems and their system-level design methodology," *Future Generation Computer Systems*, vol. 105, pp. 1028–1042, 2020.

[2] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC based provable secure authentication protocol with privacy protection for industrial internet of things," *IEEE Trans. Industrial Informatics*, 2017, DOI: 10.1109/TII.2017.2773666.

[3] J. Feng, L. T. Yang, and R. Zhang, "Practical privacy-preserving high-order bi-lanczos in integrated edge-fog-cloud architecture for cyber-physical-social systems," *ACM Trans. Internet Technology*, vol. 19, no. 2, p. 26, 2019.

[4] C. Tang, X. Wei, C. Zhu, W. Chen, and J. J. Rodrigues, "Towards smart parking based on fog computing," *IEEE Access*, vol. 6, pp. 70 172–70 185, 2018.

[5] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT," *Future Generation Computer Systems*, vol. 90, pp. 175–184, 2019.

[6] Y. Fan, J. Li, D. Zhang, J. Pi, J. Song, and G. Zhao, "Supporting sustainable maintenance of substations under cyber-threats: An evaluation method of cybersecurity risk for power CPS," *Sustainability*, vol. 11, no. 4, p. 982, 2019.

[7] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[8] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the internet of things: A survey," *ACM Trans. Internet Technology*, vol. 19, no. 2, pp. 1–41, 2019.

[9] X. Zheng, W. Ding, Z. Lin, and C. Chen, "Topic tensor factorization for recommender system," *Information Sciences*, vol. 372, pp. 276–293, 2016.

[10] S.-Y. Chou, J.-S. R. Jang, and Y.-H. Yang, "Fast tensor factorization for large-scale context-aware recommendation from implicit feedback," *IEEE Trans. Big Data*, vol. 6, no. 1, pp. 201–208, 2020.

[11] P. Martins, L. Sousa, and A. Mariano, "A survey on fully homomorphic encryption: An engineering perspective," *ACM Computing Surveys*, vol. 50, no. 6, pp. 1–33, 2017.

[12] Q. Tang and J. Wang, "Privacy-preserving context-aware recommender systems: Analysis and new solutions," in *European Symposium on Research in Computer Security (ESORICS'15)*, 2015, pp. 101–119.

[13] C. Li, R. Lu, H. Li, L. Chen, and J. Chen, "PDA: A privacy-preserving dual-functional aggregation scheme for smart grid communications," *Security and Communication Networks*, vol. 8, no. 15, pp. 2494–2506, 2015.

[14] X. Meng, H. Zhu, and G. Kollios, "Top-k query processing on encrypted databases with strong security guarantees," in *Proc. IEEE 34th Int. Conf. Data Engineering (ICDE'18)*, 2018, pp. 353–364.

[15] C. Zhang, L. Zhu, C. Xu, X. Liu, and K. Sharif, "Reliable and privacy-preserving truth discovery for mobile crowdsensing systems," *IEEE Trans. Dependable and Secure Computing*, 2019, DOI: 10.1109/TDSC.2019.2919517.

[16] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, 2018.

[17] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[18] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. S. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," *IEEE Trans. Dependable and Secure Computing*, 2018, DOI: 10.1109/TDSC.2018.2791432.

[19] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: A privacy-preserving content-based publish-subscribe scheme with differential privacy in fog computing," *IEEE Access*, vol. 5, pp. 17 962–17 974, 2017.

[20] Z. Su, Q. Xu, J. Luo, H. Pu, Y. Peng, and R. Lu, "A secure content caching scheme for disaster backup in fog computing enabled mobile social networks," *IEEE Trans. Industrial Informatics*, vol. 14, no. 10, pp. 4579–4589, 2018.

[21] Y. Yu, L. Xue, Y. Li, X. Du, M. Guizani, and B. Yang, "Assured data deletion with fine-grained access control for fog-based industrial applications," *IEEE Trans. Industrial Informatics*, 2018, DOI: 10.1109/TII.2018.2841047.

[22] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," *Sensors*, vol. 17, no. 7, p. 1695, 2017.

[23] K. Xue, J. Hong, Y. Ma, D. S. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 7–13, 2018.

[24] N. I. Yekta and R. Lu, "XRQuery: Achieving communication-efficient privacy-preserving query for fog-enhanced IoT," in *Proc. 2018 IEEE Int'l Conf. Communications (ICC'18)*, 2018, pp. 1–6.

[25] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: Privacy preserving fog-

enabled aggregation in smart grid," *IEEE Trans. Industrial Informatics*, vol. 14, no. 8, pp. 3733–3744, 2018.

[26] J. Fu, Y. Liu, H. C. Chao, B. Bhargava, and Z. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Trans. Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018.

[27] C. Piao, Y. Shi, J. Yan, C. Zhang, and L. Liu, "Privacy-preserving governmental data publishing: A fog-computing-based differential privacy approach," *Future Generation Computer Systems*, vol. 90, pp. 158–174, 2019.

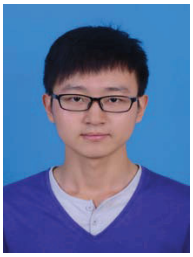
[28] X. Zhai, X. Guan, C. Zhu, L. Shu, and J. Yuan, "Optimization algorithms for multiaccess green communications in internet of things," *IEEE Internet of Things J.*, vol. 5, no. 3, pp. 1739–1748, 2018.

Jun Feng received the Ph.D. degree from Huazhong University of Science and Technology, China, in 2018.

He is currently a postdoctoral research fellow with the School of Cyber Science and Engineering, and Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, China. His current research interests include blockchain, deep learning, and big data security and privacy.

Laurence T. Yang received the B.E. degree in Computer Science and Technology and B.Sc degree in Applied Physics both from Tsinghua University, Beijing, China, and the Ph.D. degree in Computer Science from the University of Victoria, Victoria, BC, Canada.

He is currently a professor with the School of Computer Science and Technology, and Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology, Wuhan, China, and with the Department of Computer Science, St. Francis Xavier University, Antigonish, NS, Canada. His current research focuses on big data, security and privacy, parallel and distributed computing, embedded and ubiquitous/pervasive computing, and blockchain.



Ronghao Zhang received the M.Sc degree from Huazhong University of Science and Technology, China.

He is currently an engineer with the Luoyang Institute of Electro-Optical Equipment, AVIC, China. His current research focuses on fog computing, industrial IoT security, and privacy-preserving data mining.

Weizhong Qiang received the Ph.D. degree in computer engineering from Huazhong University of Science and Technology in 2005.

He is currently an associate professor at Huazhong University of Science and Technology, China. His current research interests are cyber security, virtualization and cloud security, and system security.

Jinjun Chen received the Ph.D. degree from the Swinburne University of Technology.

He is currently a professor from Faculty of Science, Engineering and Technology, the Deputy Director of Swinburne Data Science Research Institute and the Director of Data Science Platforms and Systems Program in Swinburne University of Technology, Australia. His current research interests include data and computation security, big data, cloud computing, scalable software systems, and data mining.