Computers and Electrical Engineering 000 (2017) 1–11

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An efficient and secure ridge regression outsourcing scheme in wearable devices☆

Xinshu Ma[a], Youwen Zhu[a,b,*], Xingxin Li[a]

[a] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
[b] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China

ARTICLE INFO

Article history:
Received 14 December 2016
Revised 18 July 2017
Accepted 21 July 2017
Available online xxx

Keywords:
Cloud computing
Ridge regression
Secure outsourcing
Wearable medical devices
Privacy

ABSTRACT

Ridge regression is an important approach in many applications, such as healthcare system of smart wearable equipments. Due to the limited resources of wearable devices, outsourcing is a promising computation paradigm. Nevertheless, it also suffers from some privacy challenges, as outsourced computation probably involves some sensitive data. In this paper, we propose a ridge regression outsourcing scheme, which can securely utilize the cloud to analyse large-scale wearable device dataset and dramatically reduce the computation cost of the resource-limited clients. Technically, we use random vectors and dense matrices to perturb input dataset and regression output, such that both input privacy and output privacy can be efficiently protected. Then, we present a highly-efficient verification algorithm to robustly check the correctness of cloud's answer against a dishonest/lazy cloud server. Finally, we evaluate our scheme through theoretical analysis and extensive experiments. The results show we can achieve input/output privacy, correctness, robust checkability and practical efficiency.

1. Introduction

Ridge regression (RR) is an important approach for modeling the relationship between a dependent variable and one or more independent variables. Compared to linear regression, RR is more suitable for the case with ill-conditioned independent variables and the case with many predictors. Nowadays, regression analysis has been widely applied in many scenarios, such as air quality prediction, recommendation system and wearable devices.

As well known, wearable device is a kind of portable device with constrained resources, worn directly on the body or integrated into the user's clothing or accessory. With the rapid development of cloud computing, outsourcing computation is inevitably becoming a popular and practical computing paradigm, which enables clients with low computation power to off-load their heavy computation workloads from themselves to the cloud server and to enjoy the unlimited computing resources in a pay-per-use manner [1–3]. For example, heart rate monitor collects heart rates of users and then sends these data to the cloud server. After that, the cloud server runs diagnostic functions to identify the signs of illness and answers computation result to the monitor. Therefore, cloud computing can be utilized to enhance the utility of wearable devices. However, outsourcing computation also suffers from some security and privacy challenges [4–6]. Firstly, the most significant

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Debiao He.

* Corresponding author at: College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China.
E-mail addresses: zhuyw@nuaa.edu.cn, zhuyouwen@gmail.com (Y. Zhu).

http://dx.doi.org/10.1016/j.compeleceng.2017.07.019
0045-7906/

one is the *privacy* issue. Data collected by wearable devices usually contains private information. Meanwhile, the regression output is also sensitive generally. That is, neither the input nor the output of RR should be learned by the cloud server. Secondly, another challenge is the *checkability* of this computing paradigm. The client should have the ability to verify the results returned from the cloud server. It is considered that semi-trusted cloud server might give an invalid result. For one thing, casual software bugs and hardware faults would lead to a wrong computation. For another, despite having more computation resources than the client, cloud server still has restricted resources and the financial incentive to laze. Besides, due to some intentional reasons, cloud server might acquire some useful information of the client's data via returning a false answer. Therefore, algorithms for secure outsourcing should have an efficient way to detect whether the server misbehaves or not. Finally, the third challenge is *efficiency*. Although the original computation problem needs to be securely transformed, the transformation must be more efficient than carrying out the computation task locally. Hence, an outsourcing computing algorithm should meet four requirements: correctness, input/output security, checkability and efficiency.

In this paper, we are motivated to propose a secure and efficient approach for outsourcing RR problem to a public cloud that addresses all the challenges above. To protect the privacy of the client's sensitive input and output, we propose a novel encryption method by adding random vectors and multiplying our constructed dense invertible matrices against the untrusted cloud server. The cloud server will then perform RR on the encrypted dataset and send the encrypted result back to the client. Meanwhile, we present an efficient decryption approach corresponding to our encryption scheme, by which the client can recover the answer of her original RR problem rapidly. To verify the returned result from cloud server, we propose a new RR answer verification algorithm, in which the client can find any deviation effectively by checking a simple equation. Recently, the work [7] and [8] also consider secure ridge regression problem. However, the cloud server in their schemes can access the secret key (for decryption), which is much different from ours. In our scheme, only the client knows decryption key, and the cloud server cannot learn anything useful about it.

Generally, our contribution in this work can be summarized as follows.

- We present a new encryption algorithm to securely outsource RR to a public cloud. We can well preserve the sensitive information of the client with the new encryption method, such that curious cloud server cannot learn anything useful about the client's private dataset.
- We can dramatically reduce the computation cost of the client. Besides, our scheme only require two rounds communication between the client and cloud server, thus our communication overhead is practically small.
- We also propose an efficient verification algorithm and decryption algorithm, by which the client can rapidly check the correctness of cloud's answer, and efficiently decrypt a correct answer to recover the original RR output.
- Additionally, we provide detailed theoretical analysis and extensive simulation experiments to evaluate our scheme, which validate the correctness, input/output privacy, checkability and practical efficiency of our solution.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 formulates the ridge regression outsourcing problem and introduces the framework of our problem. The proposed new secure outsourcing algorithm of ridge regression is presented in Section 4. We present detailed theoretical analysis in Section 5. Then, Section 6 shows experimental results of the proposed algorithm. Finally, the paper is concluded in Section 7.

2. Related work

Much attention has been paid to the problem of securely outsourcing various kinds of expensive computations recently. In this section, we review several recent works related to such outsourcing problem.

The work [9] addresses the problem of secure outsourcing scientific computations and presented some disguise techniques to guarantee the security of outsourcing. Nevertheless, the verification of the returned answer is not discussed in [9]. Recently, Chen et al. [6] propose two protocols for outsourcing linear regression problems to the cloud with security and efficiency. To preserve the privacy, the original linear regression problem is transformed into a new one before being sent to cloud server. Then the client recover the real result from cloud server's answer. Besides, a new secure outsourcing algorithm for (variable-exponent, variable-base) exponentiation modulo a prime in the two untrusted program model is proposed by Chen et al. [10]. Zhu et al. [11] propose a new efficient solution dealing with outsourcing linear regression with robust answer verification. In [3], Chen et al. investigate a new secure outsourcing algorithm of large-scale linear equations efficiently. Additionally, considering the challenge of verifiability in outsourcing, the work [12] provides a new VDB framework based on the idea of commitment binding. In 2016, Chen et al. [13] present a general Inc-VDB framework by incorporating the primitive of vector commitment and the encrypt-then-incremental MAC mode of encryption, and a concrete Inc-VDB scheme based on the computational Diffie–Hellman (CDH) assumption. In the cryptography community, two highly non-trivial protocols [14,15] are put forward to solve the problem of outsourcing any reasonable computation, which can be completed within polynomial time by a Turing machine. Barbosa et al. [16] investigate homomorphic encryption to cope with secure computation outsourcing. In 2013, Nikolaenko et al. [7] propose a privacy-preserving ridge regression scheme on hundreds of millions of records. It combines both homomorphic encryption and Yao garbled circuits protocol where each is used in a different part of the algorithm to obtain the best performance. After that, a new efficient privacy-preserving ridge regression scheme is presented in [8] utilizing Paillier encryption with excellent performance. Although the homomorphic algorithm can theoretically solve the secure outsourcing problems, it is still far from practice due to the expensive computations on homomorphic encryptions.

Please cite this article as: X. Ma et al., An efficient and secure ridge regression outsourcing scheme in wearable devices, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.07.019