Efficient Secure Outsourcing of Large-scale Convex Separable Programming for Big Data

Abstract—Big data has become a key basis of innovation and intelligence, potentially making our lives more convenient and bringing new opportunities to the modern society. Towards this goal, a critical underlying task is to solve a series of large-scale fundamental problems. Conducting such large-scale data analytics in a timely manner requires a large amount of computing resources, which may not be available for individuals and small companies in practice. By outsourcing their computations to the cloud, clients can solve such problems in a cost-effective way. However, confidential data stored at the cloud is vulnerable to cyber attacks, and thus needs to be protected. Previous works employ cryptographic techniques like homomorphic encryption, which significantly increase the computational complexity of solving a large-scale problem at the cloud and is impractical for big data applications. For the first time in the literature, we present an efficient secure outsourcing scheme for convex separable programming problems (CSPs). In particular, we first develop efficient matrix and vector transformation schemes only based on arithmetic operations that are computationally indistinguishable both in value and in structure under a chosen-plaintext attack (CPA). Then, we design a secure outsourcing scheme in which the client and the cloud collaboratively solve the transformed problems. The client can efficiently verify the correctness of returned results to prevent any malicious behavior of the cloud. Theoretical correctness and privacy analysis together show that the proposed scheme obtains optimal results and that the cloud cannot learn private information from the client’s concealed data. We conduct extensive simulations on Amazon Elastic Cloud Computing (EC2) platform.
and find that our proposed scheme provides significant time savings to the clients.

CONCLUSIONS

In this paper, we have investigated the problem of secure outsourcing of large-scale CSPs. To the best of our knowledge, this is the first work to solve CSPs in a secure manner in cloud computing. To protect the client’s private data, we have developed efficient vector and matrix transformation and permutation schemes that are solely based on linear algebra. We have shown that the values and positions of the transformed data are computationally indistinguishable from random vector and matrices under chosenplaintext attack (CPA), or CPA-secure. Therefore, the client can confidently share the transformed data with the cloud.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

• System : Pentium IV 2.4 GHz.
• Hard Disk : 40 GB.
• Floppy Drive : 1.44 Mb.
• Monitor : 15 VGA Colour.
• Mouse : Logitech.
• Ram : 512 Mb

SOFTWARE REQUIREMENTS:
• Operating system : Windows 7/UBUNTU.
• Coding Language : Java 1.7, Hadoop 0.8.1
• IDE : Eclipse
• Database : MYSQL

REFERENCES

