Secure Optimization Computation Outsourcing In Cloud Computing: A Case Study of Linear Programming

OBJECTIVE:

The aim of this project is investigates secure outsourcing of widely applicable linear programming (LP) computations.

ABSTRACT:

Cloud Computing has great potential of providing robust computational power to the society at reduced cost. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation. Treating the cloud as an intrinsically insecure computing platform from the viewpoint of the cloud customers, we must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by enabling the validation of the computation result. Such a mechanism of general secure computation outsourcing was recently shown to be

feasible in theory, but to design mechanisms that are practically efficient remains a very challenging problem.

This paper investigates secure outsourcing of widely applicable linear programming (LP) computations. In order to achieve practical efficiency, our mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate secu rity/efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation.

<u>INTRODUCTION:</u>

Cloud Computing provides convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead. One fundamental advantage of the cloud paradigm is computation outsourcing, where the computational power of cloud customers is no longer limited by their resource-constraint devices. By outsourcing the workloads into the cloud, customers could enjoy the literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays in the purchase of both hardware and the operational overhead therein.

We summarize our contributions as follows:

- For the first time, we formalize the problem of se-curely outsourcing LP computations, and provide such a secure and practical mechanism design which fulfills input/output privacy, cheating resilience, and efficiency .

- Our mechanism brings cloud customer great computa-tion savings from secure LP outsourcing as it only incurs for some $2 < \rho \leq 3$ local computation overhea on the customer, while solving a normal LP problem usually requires more than time .

- The computations done by the cloud server shares the same time complexity of currently practical algorithms for solving the linear programming problems, which ensures that the use of cloud is economically viable.

- The experiment evaluation further demonstrates the im-mediate practicality: our mechanism can always help customers achieve more than 30× savings when the sizes of the original LP problems are not too small, while introducing no substantial overhead on the cloud.