Abstract

Cloud Computing provides a appropriate on-demand network access to a shared pool of configurable computing resources which could be rapidly deployed with much more great efficiency and with minimal overhead to management. This paper deals with the secure outsourcing of nonlinear programming. It provides a practical mechanism design which fulfills input/output privacy, cheating resilience, and efficiency. In the proposed approach practical efficiency is achieved by explicit decomposition of NLP into NLP solvers running on the cloud and private NLP parameters owned by the customer. When compared to the general circuit representation the resulting flexibility allows exploring appropriate security/efficiency trade-off via higher-level abstraction of NLP computations. It is possible to construct a set of effective privacy-preserving transformation techniques for any problem, by framing a private data possessed by the client for NLP problem as a combination of matrices and vectors, which allow customers to transform original NLP problem into some arbitrary value while defending sensitive input or output information. To confirm the computational result, the fundamental duality theorem of NLP computation should be explored and then derive the essential and adequate constraints that a accurate result must satisfy. Such a result verification mechanism is very competent and suffers close-to-zero extra cost on both cloud server and customers.

References
Index Terms

Computer Science Security

Keywords

Non-linear Programming Cloud Computing Privacy Preservation Information Security Outsourcing