Cryptology ePrint Archive: Report 2011/614

On Security of RASP Data Perturbation for Secure Half-Space Queries in the Cloud

Keke Chen

Abstract: Secure data intensive computing in the cloud is challenging, involving a complicated tradeoff among security, performance, extra costs, and cloud economics. Although fully homomorphic encryption is considered as the ultimate solution, it is still too expensive to be practical at the current stage. In contrast, methods that preserve special types of data utility, even with weaker security, might be acceptable in practice. The recently proposed RASP perturbation method falls into this category. It can provide practical solutions for specific problems such as secure range queries, statistical analysis, and machine learning. The RASP perturbation embeds the multidimensional data into a secret higher dimensional space, enhanced with random noise addition to protect the confidentiality of data. It also provides a query perturbation method to transform half-space queries to a quadratic form and, meanwhile, preserving the results of half-space queries. The utility preserving property and wide application domains are appealing. However, since the security of this method is not thoroughly analyzed, the risk of using this method is unknown. The purpose of this paper is to investigate the security of the RASP perturbation method based on a specific threat model. The threat model defines three levels of adversarial power and the concerned attacks. We show that although the RASP perturbed data and queries are secure on the lowest level of adversarial power, they do not satisfy the strong indistinguishability definition on higher levels of adversarial power. As we have noticed, the indistinguishability definition might not be too strong to be useful in the context of data intensive cloud computation. In addition, the noise component in the perturbation renders it impossible to exactly recover the plain data; thus, all attacks are essentially estimation attacks. We propose a weaker security definition based on information theoretic measures to describe the effectiveness of estimation attacks, and then study the security under this weaker definition. This security analysis helps clearly identify the security weaknesses of the RASP perturbation and quantify the expected security under different levels of adversarial power.

Category / Keywords: half-space query, data perturbation, cloud computing

Publication Info: no

Date: received 14 Nov 2011, last revised 27 May 2012

Contact author: keke chen at wright edu

Available formats: Postscript (PS) | Compressed Postscript (PS.GZ) | PDF | BibTeX Citation

Version: 20120527:192621 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]