Accepted Manuscript

Title: Efficient *k*-NN query over encrypted data in cloud with limited key-disclosure and offline data owner

Author: Lu Zhou, Youwen Zhu, Aniello Castiglione

PII: S0167-4048(16)30166-3
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.11.013
Reference: COSE 1067

To appear in: *Computers & Security*

Please cite this article as: Lu Zhou, Youwen Zhu, Aniello Castiglione, Efficient *k*-NN query over encrypted data in cloud with limited key-disclosure and offline data owner, *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.11.013.

Efficient k-NN Query over Encrypted Data in Cloud with Limited Key-disclosure and Offline Data Owner

Lu Zhou[c], Youwen Zhu[a,b,*], Aniello Castiglione[d]

[a]*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China.*

[b]*Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing 210021, China*

[c]*Shandong University, Jinan 250100, China*

[d]*Dept. of Computer Science, University of Salerno, I-84084 Fisciano, Italy*

☆Partial content of this paper was presented at the 20th Pacific Asia Conference on Knowledge Discovery and Data Mining [50] and the 11th EAI International Conference on Collaborative Computing [51].

*Corresponding author

Email address: zhuyw@nuaa.edu.cn (Youwen Zhu)

Abstract

Several schemes for k-nearest neighbors (k-NN) query over encrypted data in cloud have been proposed recently. Nevertheless, existing schemes either suppose each query user is fully-trusted, or need data owner to be online for each query. A fully-trusted query user is assumed to obtain the decryption key of data owner's outsourced dataset, thus, cloud server could entirely break the outsourced dataset upon gaining the decryption key from some untrustworthy query user. Because of the online requirement, data owner still need to burden too many computational tasks during the k-NN queries, which thus is impractical. In this paper, we propose a new scheme to perform k-NN query over encrypted data in cloud while protecting the privacy of both data owner and query users from cloud. Our new method just reveals limited information about data owner's key to query users, and has no need of an online data owner. For gaining the properties, we present a new scalar product protocol, then the new protocol and some other transformation approaches are merged into our secure k-NN query system. Additionally, we confirm our security and efficiency through theoretical analysis and extensive simulation experiments.