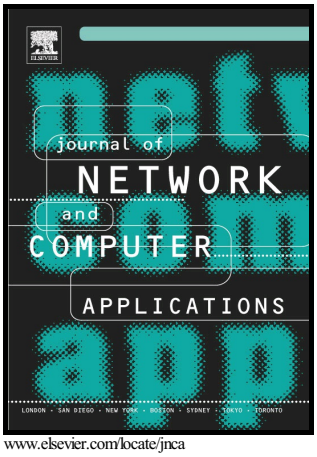
# Efficient Searchable Symmetric Encryption for Storing Multiple Source Dynamic Social Data on Cloud

Chang Liu, Liehuang Zhu, Jinjun Chen




www.elsevier.com/locate/jnca

PII: S1084-8045(16)30217-X
DOI: http://dx.doi.org/10.1016/j.jnca.2016.09.010
Reference: YJNCA1722

To appear in: *Journal of Network and Computer Applications*

Received date: 1 June 2016
Revised date: 9 August 2016
Accepted date: 26 September 2016

Cite this article as: Chang Liu, Liehuang Zhu and Jinjun Chen, Efficien Searchable Symmetric Encryption for Storing Multiple Source Dynamic Socia Data on Cloud, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2016.09.010

# Efficient Searchable Symmetric Encryption for Storing Multiple Source Dynamic Social Data on Cloud *

Chang Liu[a,b], Liehuang Zhu[a], Jinjun Chen[b]

[a]*Beijing Engineering Research Center of Massive Language Information Processing and Cloud Computing Application, School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China*
[b]*Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

**Abstract**

Cloud computing has greatly facilitated large-scale data outsourcing due to its cost efficiency, scalability and many other advantages. Subsequent privacy risks force data owners to encrypt sensitive data, hence making the outsourced data no longer searchable. Dynamic Searchable Symmetric Encryption (DSSE) is an advanced cryptographic primitive addressing the above issue, which maintains efficient keyword search over dynamic encrypted data without disclosing much information to the storage provider. Existing DSSE schemes implicitly assume that original user data is centralized, so that a searchable index can be built at once. Nevertheless, especially in pervasive social networking applications, user-side data centralization is not reasonable. E.g., social chatting records are often separately distributed over multiple devices such as mobile phones, laptops, tablet computers, etc. In this paper, we propose the notion of Multi-Data-Source DSSE (MDS-DSSE), which allows each data source to build a local index individually and enables the storage provider to merge all local indexes into a global index afterwards. We propose a novel MDS-DSSE scheme, in which an adversary only learns the number of data sources, the number of entire data files, the access pattern and the search pattern, but not any other distribution information such as how data files or search results are distributed over data sources. We offer rigorous security proof of our scheme, and report experimental results to demonstrate the efficiency of our scheme.



*Email addresses:* changliu.bit@gmail.com (Chang Liu), liehuangz@bit.edu.cn (Liehuang Zhu), jinjun.chen@gmail.com (Jinjun Chen)

* A preliminary version [21] of this paper was presented at the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'15).