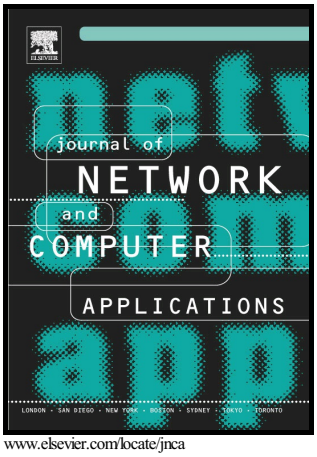
Privacy-Preserving Data Sharing Scheme over Cloud for Social Applications

Chen Lyu, Shi-Feng Sun, Yuanyuan Zhang, Amit Pande, Haining Lu, Dawu Gu



www.elsevier.com/locate/jnca

PII: S1084-8045(16)30160-6
DOI: http://dx.doi.org/10.1016/j.jnca.2016.08.006
Reference: YJNCA1688

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

Received date: 25 January 2015
Revised date: 1 July 2016
Accepted date: 9 August 2016

Cite this article as: Chen Lyu, Shi-Feng Sun, Yuanyuan Zhang, Amit Pande, Haining Lu and Dawu Gu, Privacy-Preserving Data Sharing Scheme over Clou for Social Applications, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2016.08.006

Privacy-Preserving Data Sharing Scheme over Cloud for Social Applications

Chen Lyu[a*], Shi-Feng Sun[b], Yuanyuan Zhang[b], Amit Pande[c], Haining Lu[b], Dawu Gu[b]

[a] *School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai, China, 200433.*

[b] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, 200240.*

[c] *Department of Computer Science, University of California, Davis, CA, USA, 95616.*

Abstract

Social applications are becoming one of the most popular applications for users to share data and communicate online. These applications deal with a lot of personal data, e.g., users' locations, interests and documents stored on the remote cloud storage servers. Therefore, we need to pay a deeper attention to data confidentiality and privacy. To address the problem of data confidentiality, existing solutions usually count the security requirement of data owner for data sharing in social applications. However, on the side of the data consumer or member, we want to securely and efficiently get our own interested data. Both the data owner and the member are two roles of users in data sharing applications, and there are little existing research efforts to investigate the implementation of achieving both of their requirements at the same time. In this paper, we propose DASS, a privacy-preserving DAta Sharing Scheme to comprehensively satisfy users' security requirements for social applications. Our solution consists of a fine-grained access control scheme, a dynamic social attribute management model, and a multi-user searchable encryption scheme. We have described our scheme and provided performance evaluation. Validations are done to demonstrate that our scheme is secure, fine-grained and efficient.

*Corresponding author, Email: lyu.chen@mail.shufe.edu.cn, Telephone: +86 21 65908168.