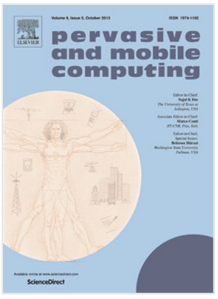
Accepted Manuscript



A secure cloud-assisted urban data sharing framework for ubiquitous-cities

Jian Shen, Dengzhi Liu, Jun Shen, Qi Liu, Xingming Sun

PII: S1574-1192(17)30161-X
DOI: http://dx.doi.org/10.1016/j.pmcj.2017.03.013
Reference: PMCJ 821

To appear in: *Pervasive and Mobile Computing*

Please cite this article as: J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud-assisted urban data sharing framework for ubiquitous-cities, *Pervasive and Mobile Computing* (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.013

A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities

Jian Shen[a,b,c,*], Dengzhi Liu[c], Jun Shen[c], Qi Liu[a,c], Xingming Sun[a,c]

[a] *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China*
[b] *Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, China*
[c] *School of Computer & Software, Nanjing University of Information Science & Technology, China*

Abstract

With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation.

*Corresponding author
Email addresses: s_shenjian@126.com (Jian Shen), liudzdh@126.com (Dengzhi Liu), sj310310@qq.com (Jun Shen), qrankl@163.com (Qi Liu), sunnudt@163.com (Xingming Sun)