Accepted Manuscript

Anonymous and secure aggregation scheme in fog-based public cloud computing

Huaqun Wang, Zhiwei Wang, Josep Domingo-Ferrer

PII: S0167-739X(17)30255-8
DOI: http://dx.doi.org/10.1016/j.future.2017.02.032
Reference: FUTURE 3350

To appear in: *Future Generation Computer Systems*

Received date: 16 April 2016
Revised date: 28 January 2017
Accepted date: 15 February 2017

Please cite this article as: H. Wang, Z. Wang, J. Domingo-Ferrer, Anonymous and secure aggregation scheme in fog-based public cloud computing, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.02.032

Anonymous and Secure Aggregation Scheme in Fog-Based Public Cloud Computing

Huaqun Wang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China. E-mail: wanghuaqun@aliyun.com

Zhiwei Wang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China. E-mail: zhwwang@njupt.edu.cn

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Department of Computer Engineering and Mathematics, UNESCO Chair in Data Privacy, Av. Països Catalans 26, E-43007 Tarragona, Catalonia. E-mail: josep.domingo@urv.cat

Abstract

By using fog computing, cloud computing can be extended to the edge of the network. Generally, in the public cloud, fog computing comprises three components: terminal device, fog node and public cloud server (PCS). In this paper, we propose the concept of anonymous and secure aggregation scheme (ASAS) in fog-based public cloud computing. In the ASAS model, a fog node aggregates the data from terminal nodes and forwards the aggregated data to the public cloud server. By using the ASAS scheme, the fog node can help terminal devices upload their data to PCS. By using the data aggregation technique, our ASAS scheme can save bandwidth between the fog node and PCS. At the same time, our ASAS scheme not only protects the identities of terminal devices by using pseudonyms but it also guarantees data secrecy