Accepted Manuscript

Leakage resilient ID-based proxy re-encryption scheme for access control in fog computing

Zhiwei Wang

PII: S0167-739X(17)31007-5
DOI: https://doi.org/10.1016/j.future.2017.12.001
Reference: FUTURE 3839

To appear in: *Future Generation Computer Systems*

Received date : 13 May 2017
Revised date : 12 October 2017
Accepted date : 3 December 2017

Please cite this article as: Z. Wang, Leakage resilient ID-based proxy re-encryption scheme for access control in fog computing, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.12.001

Leakage Resilient ID-based Proxy Re-encryption Scheme for Access Control in Fog Computing

Zhiwei Wang
1.School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2.Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing 210023, China
3.Shanghai Key Laboratory of information security integrated management technology, Shanghai 200240, China
Email: zhwwang@njupt.edu.cn

***Abstract*—In fog computing, fog-devices are usually physically close to end-devices, and have a high speed connection with cloud servers. They provide good access control service for end-devices to cloud, if an ID-based proxy re-encryption scheme is deployed on them. Each file stored on a cloud sever is encrypted using a symmetric key, and these keys are encrypted by a public master key which is stored in a fog-device. If an end-device want to access a file in cloud, then the fog-device re-encrypts these encapsulated symmetric keys from the master key to the key of the end-device. However, due to the geographic dispersion of fog-devices, they are apt to be attacked by side channel attacks. In this work, we propose a leakage resilient ID-based proxy re-encryption scheme in auxiliary input model. It can resist the continuous leakage of secret keys caused by side channel attacks. We implement our scheme over two platforms, and the results show that our scheme is feasible in practice.**

***Keywords*-fog-devices; ID-based proxy re-encryption; access control; auxiliary input; leakage resilient**

I. Introduction

Fog (From cOre to edGe) computing, a term coined by Cisco in 2012[1], is a distributed computing paradigm, that empowers the network devices at edge levels with various degrees of computational and storage capability. Fog computing serves the demands of the realtime, latency-sensitive applications in the context of IoT systems[2], [3]. In IoT system, the physical world and cyber world are more tightly coupled than before, which makes the physical world easy to be attacked, since a malicious instruction from the cyber world may bring serious damage for the physical world. Thus, we hope that IoT security issues can be handled effectively by fog computing.

As Fig.1, the IoT system is a typical three-layer architecture[4], including a fog layer. We depict these layers as follows. 1)*Things layer*, which is used to collect data and control the physical world[5]. Most end-devices in the things layer are resource-constrained, which is low as 64 bytes of RAM and 2KB of storage[6]. 2) *Fog layer*, which is introduced to help end-devices. Fog-devices, such as smartphones, routers, and home servers, also help connect end-devices to the clouds. There are some advantages in deploying security services at the edge layer. Firstly, fog-devices have much more resources than the end-devices. And then, end-devices can can leverage these resources to offload computation-intensive tasks. Secondly, fog-devices are physically close to end-devices, which can set up the relatively stable relationship. Finally, fog-devices can be used to access control from end-devices to clouds. 3) *Cloud layer*, which is resource-rich, and can be used to store, process, and analyze the collected data. The fog layer usually has high-speed connection with the cloud layer, and it is easy for the fog-devices to get extra support from clouds as needed. Fog computing refers to the enabling technologies allowing computation to be performed at the edge of the network. Here we define fog as any computing and network resources along the path between end-devices and cloud centers. For example, a smart phone is at the fog between body end-devices and cloud, a gateway in a smart home is at the fog between home end-devices and cloud. In fog computing, data security protection are the most important services that should be provided[7]. Keeping the computing at fog (the edge of the network) may be a decent method to protect data security, but two challenges remain open.

First is the missing of efficient tools to protect data security at the fog. Some of the end-devices and fog-devices are highly resource constrained so the current methods for security protection might not be able to be deployed on the fog because they are resource hungry. Second is the awareness of security to the fog. We take WiFi networks security as an example. 89% of public WiFi hotspots are unsecured. If fog-devices are located in such unsecured network, then cryptographic primitives running on the fog-devices can leak additional information, such as the computation time, power-consumption, radiation/noise/heat emission etc. Moreover, the highly dynamic environment at the fog also makes the network become vulnerable or unprotected.

It is difficult for enforcing cryptographic access control over remotely stored data in cloud[12], [13]. If the encrypted data is given a classification level, and keys are shared with users according to access control policy, then re-encryption is used to enforce changes to the policy. In particular, re-encryption can signify a change in user access rights. Proxy re-encryption enables a third party (proxy) to re-encrypt a ciphertext using an update token generated by the user, in