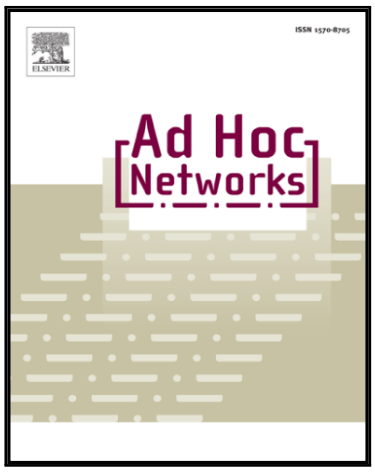

Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services

Alexandre Viejo, David Sánchez

PII: S1570-8705(18)30549-3
DOI: https://doi.org/10.1016/j.adhoc.2018.08.002
Reference: ADHOC 1732

To appear in: *Ad Hoc Networks*

Received date: 14 March 2018
Revised date: 31 July 2018
Accepted date: 2 August 2018

Please cite this article as: Alexandre Viejo, David Sánchez, Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services, *Ad Hoc Networks* (2018), doi: https://doi.org/10.1016/j.adhoc.2018.08.002

Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services

Alexandre Viejo, David Sánchez

Universitat Rovira i Virgili, Department of Computer Science and Mathematics, UNESCO Chair in Data Privacy, CYBERCAT-Center for Cybersecurity Research of Catalonia, Av. Països Catalans 26, 43007 Tarragona, Spain
E-mail: {alexandre.viejo,david.sanchez}@urv.cat

Abstract

Fog-enabled IoT applications are the next step in the deployment of cloud computing backed services through the Internet. The use of fog nodes at the edge of the network reduces traffic to cloud servers, decreases latency of services and improves ubiquity. Security is, however, a fundamental challenge of fog computing because both fog and IoT nodes may be deployed in disperse non-secure locations. Solutions to this challenge rely on expensive cryptography, such as attribute-based encryption of homomorphic encryption, which significantly degrades the response time of the service delivery due to the limited resources of IoT nodes. In this paper, we tackle this issue by relying on the novel concept of *fog orchestration*. Through orchestration, the network is self-tailored to the service to be delivered, and we use this possibility to enable a secure and efficient service delivery. Specifically, we propose several secure and privacy-by-design protocols for the orchestration and delivery fog-enabled IoT services. We also assume the most challenging scenario in which nodes exchange data in open and potential unsecured networks and they can be subjected to a wide range of active attacks. The feasibility of our proposal and the improvements it brings over related works are discussed through a set of theoretical and empirical evaluations of its performance.

Keywords: Security, Privacy, Fog Computing, Orchestration, Internet of Things.