Accepted Manuscript

Design of secure key management and user authentication scheme for fog computing services

Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V. Vasilakos

PII: S0167-739X(18)30395-9
DOI: https://doi.org/10.1016/j.future.2018.09.017
Reference: FUTURE 4452

To appear in: *Future Generation Computer Systems*

Received date : 23 February 2018
Revised date : 2 September 2018
Accepted date : 5 September 2018

Please cite this article as: M. Wazid, et al., Design of secure key management and user authentication scheme for fog computing services, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.09.017

Design of Secure Key Management and User Authentication Scheme for Fog Computing Services

Mohammad Wazid [a], Ashok Kumar Das [b], Neeraj Kumar [c], Athanasios V. Vasilakos [d]

[a] Cyber Security and Networks Lab, Innopolis University, Innopolis 420500, Russian Federation
E-mail: wazidkec2005@gmail.com
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[c] Department of Computer Science and Engineering, Thapar University, Patiala 147004, India
E-mail: neeraj.kumar@thapar.edu
[d] Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea 971 87, Sweden
E-mail: th.vasilakos@gmail.com

Abstract

Fog computing (fog networking) is known as a decentralized computing infrastructure in which data, applications, compute as well as data storage are scattered in the most logical and efficient place among the data source (i.e., smart devices) and the cloud. It gives better services than cloud computing because it has better performance with reasonably low cost. Since the cloud computing has security and privacy issues, and fog computing is an extension of cloud computing, it is therefore obvious that fog computing will inherit those security and privacy issues from cloud computing. In this paper, we design a new secure key management and user authentication scheme for fog computing environment, called SAKA-FC. SAKA-FC is efficient as it only uses the lightweight operations, such as one-way cryptographic hash function and bitwise exclusive-OR (XOR), for the smart devices as they are resource-constrained in nature. SAKA-FC is shown to be secure with the help of the formal security analysis using the broadly accepted Real-Or-Random (ROR) model, the formal security verification using the widely-used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool and also the informal security analysis. In addition, SAKA-FC is implemented for practical demonstration using the widely-used NS2 simulator.

Keywords: Fog computing, key management, authentication, services, security, AVISPA, NS2 simulation.

1. Introduction

Fog computing is an extension of cloud computing and services to the edge of the network. Fog computing offers data, storage, compute, and application services to the end-users as the cloud computing also does [1, 2, 3, 4, 5, 6, 7, 8]. Fog computing fills the hole among remote data centers and IoT devices as it allows for relevant IoT applications. In addition, it also provides several benefits including enhanced security, decreased bandwidth, and reduced latency. Therefore, fog computing looks promising technology for many IoT services [9]. Some of the advantages of using fog computing include better real time interaction, geo-distribution, location awareness support for mobility and very low delay jitter. A scenario of fog computing based IoT environment is illustrated in Fig. 1. There are various types of users who wish to access the data of the smart devices using the fog servers. Due to the benefits provided by fog computing, the users can directly access the data of smart devices efficiently without any long delay. Since fog computing is an extension of cloud computing, it also receives several security and privacy challenges of cloud computing, which in tern causes a serious security concern in the fog computing environment. For example, spoofing, man-in-the middle, impersonation, physical capturing of smart devices, offline/online user's password guessing and privileged insider attacks can be mounted by an adversary as the communicating entities communicate over insecure (public) channels. Consider the real-time data access by an external party (user) directly from the smart devices in the fog computing environment. The designed protocol needs to be secure in the sense that no illegal users should gain access to the smart devices in fog computing environment, and only authorized users need to be given access. To allow this facility, a legal user can access the data at any time from a smart device. This problem is typically termed as user authentication problem. On the other hand, using the pre-loaded (pre-distributed) credentials stored in the nodes (i.e., smart devices, fog servers and cloud servers), these entities can establish pairwise keys between them for secure communication among each other. Such a problem is known as the key management problem. This paper deals with designing a secure key management and user authentication scheme for the fog computing-based IoT environment, called SAKA-FC. SAKA-FC is composed of two parts: 1) key management and 2) user authentication. In the first part, key management procedure between smart devices and fog servers, and fog servers and cloud servers is presented. In the second part, the user authentication between a user and smart devices is proposed in which after their mutual authentication a session key is established for secure communication in future.

1.1. Research Contributions

The contributions of this paper are manyfold: