Multi-Layer Token Based Authentication Through Honey Password in Fog Computing

Praveen Kumar Rayani, CSE Department, VEMU Institute of Technology, Tirupati, India
Bharath Bhushan, CSSE Department, Sree Vidyanikethan Engineering College (SVEC), Tirupati, India
Vaishali Ravindra Thakare, CSE Department, Koneru Lakshmaiah Education Foundation (KLEF), Guntur, India

ABSTRACT

This article describes how fog computing empowers network resource utilization by providing services to low bandwidth users in cloud environment. Here, authentication mechanisms are used by fog nodes while providing services to end users. In cloud computing there are several types of authentication mechanisms, in which token based authentication takes less time for validating password. The proposed technique uses token based authentication mechanism with honey password. The aim of this article is to focus on multi-layer token based authentication for identifying the authorized user at fog node. In authentication phase end user instantaneously frame his user account password with honey password that makes illusion to shoulder surfers password has changed. The proposed mechanism avoids and detects shoulder surfing attacks, password guessing attacks, and application denial of service attacks.

KEYWORDS

Authentication, Cloud Computing, Fog Computing, IoT

1. INTRODUCTION

Past few years’ usage of IoT devices has increasing tremendously in almost all application areas. Cloud computing fail to meet requirements such as mobility support, geo-graphical distribution, location-awareness and low latency (Bonomi et al., 2012; Zhu et al., 2013; “Fog Computing,” 2016). It makes challenge to cloud computing platform through large data computations. If N number of devices directly communicate with cloud server leads to overload of the cloud server. It can solve by decentralizing the cloud architectures through edge computing at end users. The

DOI: 10.4018/IJFC.2018010104
processing of received data is done at edge nodes, which helps in efficient utilization of bandwidth and significant reduction of load on the cloud servers. Edge computing enables computing operations directly at edge of the network, but security is the major concern in fog computing. List of security issues has shown in Figure 1.

In business applications, every bit of information also plays major role. It requires five-point methods to maintain business information in safe state. That is confidentiality, integrity, authentication, authorization, and non-repudiation (Maher Abdelshkour, 2015). If any point lost in five points method leads to unsafe state of information. If the information is moving from Machine to Machine, or Human to Machine requires authentication to validate human or device with valid credentials.

In user authentication, the selection and distribution of key is given as highest priority in information security field. Keys are divided into three types i.e.:

Figure 1. Fog computing security issues
Privacy Enhanced Cloud-Based Recommendation Service for Implicit Discovery of Relevant Support Groups in Healthcare Social Networks
www.igi-global.com/chapter/privacy-enhanced-cloud-based-recommendation-service-for-implicit-discovery-of-relevant-support-groups-in-healthcare-social-networks/205986?camid=4v1a

Predictive Modeling for Imbalanced Big Data in SAS Enterprise Miner and R
www.igi-global.com/article/predictive-modeling-for-imbalanced-big-data-in-sas-enterprise-miner-and-r/210567?camid=4v1a