An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards

Abstract

The rapid growth and advancement in the field of Internet of Things (IoT), many IT based applications and also services are being provided to the consumers so that it would be easy for them to use the provision. As Cloud Computing will be playing an important part in the mere future it will be a great response if it is used in the application scenario. In this paper I would be discussing about the use of a smart card to use the cloud based services in a distributed IoT based environment, for which the identity based access management is used to ensure the secure access of the authentic persons.

1. Introduction

As the emerging field of IoT is playing a major role in almost all aspects in our everyday lives , the next generation of it with its applications and services should be emerged as a support with the development of its environment. Similarly cloud computing is also growing vitally and has an evolving support towards the application and services. Likewise, prospects of Cloud Computing are evolving to support these applications and on-demand services along with scalable storage, distributed computations, broad network access, rapid flexibility and data sharing capabilities [1]. Integration of IoT and Cloud will not only be effective on the performance and its security aspects but will also empower the development in the future.

Smart card is a portable hardware it stores some secret information of the user. They are utilized in many applications like online payment, banking, healthcare, and many more. It allows a gradual update and also it is capable in supporting much functionality along with the mobile or a remote support with the authentication. These can be used in integration with other technologies, such as Single Sign-On (SSO) mechanism, access control policies etc. to leverage multiple Cloud based services, and to establish connectivity among users and machines in distributed computing environment in a secure manner [2, 3].

However, to access Cloud based services and data, users have to pass through the network and communication environment which is vulnerable to a number of malicious attacks including eavesdropping, Man-In-The-Middle (MITM) attack, replay attacks, forgery, Denial of Service (DoS), and so on [Fig. 1] [4, 5]. Users are also susceptible to attack by themselves to another accounts that are gradually available or are accessible by them. In addition, end devices used to access these services are resource constrained and thus not capable enough to implement the security mechanisms by themselves. To mitigate these attacks and to ensure privacy of the user's identity, a light weight authentication framework is needed to be developed with efficient computations to enable access to multiple services with same credentials. In this paper, we propose a smart card authentication framework utilizing identity based access control mechanism for gaining access to multiple distributed Cloud services in a resource constrained IoT environment. Concept of SSO is utilized to enable access to multiple Cloud services without the need of maintaining separate credentials for each.

The rest of the paper is organized as follows. In Section 2,the related work to analyze the problems and corresponding solutions by some of the existing models proposed in the past is discussed. In Section 3, the proposed scheme along with the entities involved and working are discussed. After that, in Section 4, the informal security and functional analysis along with implementation results and comparative analysis of the proposed scheme are presented. Finally, Section 5 concludes the paper.



Fig. 1. Cloud based networking environment.