Chapter 19
Architectural Design of Trusted Platform for IaaS Cloud Computing

Ubaidullah Alias Kashif
Shah Abdul Latif University Khairpur - Shikarpur Campus, Pakistan

Zulfiqar Ali Memon
National University of Computer and Emerging Sciences (FAST-NUCES), Pakistan

Shafaq Siddiqui
Sukkur IBA University, Pakistan

Abdul Rasheed Balouch
Sukkur IBA University, Pakistan

Rakhi Batra
Sukkur IBA University, Pakistan

ABSTRACT

This article describes how the enormous potential benefits provided by the cloud services, made enterprises to show huge interest in adopting cloud computing. As the service provider has control over the entire data of an organization stored onto the cloud, a malicious activity, whether internal or external can tamper with the data and computation. This causes enterprises to lack trust in adopting services due to privacy, security and trust issues. Despite of having such issues, the consumer has no root level access right to secure and check the integrity of procured resources. To establish a trust between the consumer and the provider, it is desirable to let the consumer to check the procured platform hosted at provider side for safety and security. This article proposes an architectural design of a trusted platform for the IaaS cloud computing by the means of which the consumer can check the integrity of a guest platform. TCG's TPM is deployed and used on the consumer side as the core component of the proposed architecture and it is distributed between the service provider and the consumer.

DOI: 10.4018/978-1-5225-8176-5.ch019

INTRODUCTION

Businesses are looking forward to Cloud computing model for outsourcing IT services as a utility through internet. Though, it evolves from distributed computing such as, cluster and grid computing yet the internet centric requirement for the cloud computing distinguishes it from cluster and grid computing.

As the name implies, the word cloud denotes the internet that hides the underlying abstraction for the users of cloud computing and yields a problem free thought for adopting the IT services from cloud service provider (CSP). Broadly speaking in cloud computing there may be the involvement of three entities: Cloud Infrastructure, Cloud Service Provider and Cloud consumer (Aboudi, 2017), (Bani-Mohammad, 2017), (Gupta, 2017), (Wang, 2017). The cloud computing demands some new paradigms to share the responsibilities of the provider.

In the literature, authors find some trust models for enhancing trust in the cloud infrastructure i.e. (Panneerselvam, 2017), (Nurmi, 2009), (Paladi, 2013), (Ristenpart, 2009), (Strasser, 2004), but these all models are based on the infrastructure of cloud service provider. Though in these model's, tamper proof trusted hardware such as Trusted Platform Module (TPM) chip is exploited; yet these can't be considered as trusted because, TPM is under physically control of the provider. So, if the provider is untrusted, how the devices through which trust is said to be established can be trusted. An alternative approach is required to fill this gap. It has been considered that trust of a consumer can be established by allowing the consumer to handle and implement security counter measures (Paladi, 2013), (Ruchika, 2016), (Bosse, 2017).

This article presents the architectural design of a trusted platform. In the proposed platform, consumer can exploit its infrastructure in performing security counter measures to check integrity and confidentiality of the Virtual Machine (VM). The core component of the proposed research work is Trusted Computing Group's (TCG's) tamper proof hardware chip known as Trusted Platform Module (TPM), by incorporating the provisions of TCG. The authors in (Bertholon, 2011) states that above-mentioned chip i.e. TPM, will be the essential hardware component for every computer in near future. Their prediction is becoming true and today almost every computer comes with TPM. Microsoft has also declared it as an essential component for every computer (Gupta, 2017), (Bosse, 2015). Keeping these facts, it can be argued that availability of the TPM is not an issue and authors are utilizing the very important component of computers to entrust the consumer in cloud computing.

The proposed solution provides an architecture to share the security responsibilities among the provider and consumer. As in traditional cloud architecture the sole responsible for security management and service hosting is provider; whose trustworthiness is difficult to validate. The aim of the proposed solution is to give some control to consumer side. The aim of this manuscript is not to provide complete isolation between provider and host VM, but rather divide the responsibilities among provider as well as consumer (Hoogendoorn, 2013).

Supporting from the literature, "trust" seems to be big problem in cloud computing. There are different techniques proposed in the literature (Khoshkholghi, 2017), (Nurmi, 2009), (Paladi, 2013), (Ristenpart, 2009), (Strasser, 2004), (Bosse, T., 2012) at different levels, i.e., SPI (Software, Platform, Infrastructure) of cloud computing to enhance the trust of consumer. IaaS is the fundamental layer that supports other layers of cloud computing i.e. SaaS and PaaS. This article is focused on IaaS model, where consumers rent Virtual Machines (VMs) on the infrastructure of Cloud Service Provider (CSP). All models presented in literature are absolutely reliant on the collaboration of provider. According to the models proposed in the literature, consumer requires to trust in provider's infrastructure. Trusted Computing Groups (TCG)