Chapter 83
Trust Management in Cloud Computing

Vijay L. Hallappanavar
KLE College of Engineering and Technology, India

Mahantesh N. Birje
Visvesvaraya Technological University, India

ABSTRACT

Cloud computing is a model for enabling everywhere, suitable, on-demand network access. There are a number of challenges to provide cloud computing services and to accomplish this, it is necessary to establish trust across the cloud, between the user and the service provider. It is becoming increasingly complex for cloud users to make distinction among service providers offering similar kinds of services. There must be some mechanisms in the hands of users to determine trustworthiness of service providers so that they can select service providers with confidence and with some degree of assurance that service provider will not behave unpredictably or maliciously. An effective trust management system helps cloud service providers and consumers reap the benefits brought about by cloud computing technologies. Hence the objective of this chapter is to describe existing mechanisms that are used to determine a trust worthiness of a cloud service, various models that are used for calculating a trust value and method to establish trust management system.

INTRODUCTION

Cloud computing is a model for enabling ever-present, suitable, on-demand network access to a shared pool of configurable computing resources, e.g., networks, servers, storage, applications and services that can be rapidly provisioned and made available easily with minimal management effort or service provider interaction described by Siani (2012). Cloud environments provide several benefits such as reduced expenses and simplicity to service providers and service requesters. The cloud computing provides hardware and systems software resources on remote datacenters, as well as Internet gives access to the services based upon these resources. These resources dynamically scale up to match the load, using a pay-per resources business model. The significant features of cloud computing are elasticity,

multitenancy, maximal resource utilization and pay-per-use. Figure 1 shows an abstracted view of the cloud computing environment with the interacting parties.

Virtualization or job scheduling techniques unifies the shared pool of resources. A host computer runs an application known as a hypervisor which creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications, Siani Pearson (2012). At hardware level processors, hard drives and network devices, are located in datacenters, independent from geographical location, which are accountable for storage and processing needs. Above this, the combination of software layers, the virtualization layer and the management layer, allow for the effective management of servers. Virtualization is an important element of cloud implementations and is used to provide the essential cloud characteristics of location independence, resource pooling and rapid elasticity. Differing from traditional network topologies, such as client–server, cloud computing can offer robustness and alleviate traffic congestion issues. The management layer can monitor traffic and respond to peaks or drops with the creation of new servers or the destruction of unnecessary ones. The management layer has the additional ability to be able to implement security monitoring and rules throughout the cloud. Figure 2 shows the basic diagram of this layout.

Cloud can worsen the damage on traditional frameworks for privacy that globalization has already started. For example, location of the data is critical from a legal point of view. But in the cloud, information might be in multiple places, might be managed by different entities and it may be difficult to know the geographic location and which specific servers or storage devices are being used. It is currently difficult to discover and meet compliance requirements, as existing global legislation is complex and includes export restrictions, data retention restrictions, sector- specific restrictions and legislation at state and/or national levels. Legal advice is required, transborder data flow restrictions need to be taken into account, and care must be taken to delete data and virtual storage devices when appropriate.

High security is one of the major obstacles for the adoption of computing as a utility as the sensitive applications and data are moved into the cloud data centers. This unique attributes, however, poses many novel tangible and intangible security challenges such as accessibility vulnerabilities, virtualization
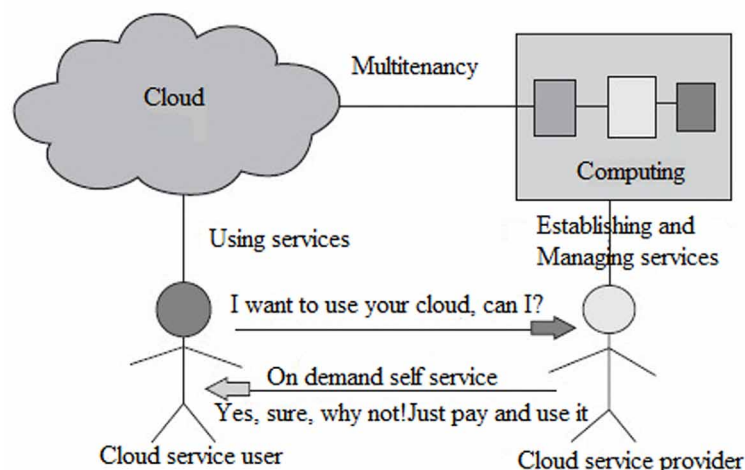
Figure 1.

Related Content

Cloud Computing Networks: Utilizing the Content Delivery Network
Yale Li, Yushi Shenand Yudong Liu (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 648-659).*
www.irma-international.org/chapter/cloud-computing-networks/119876

Realm Towards Service Optimization in Fog Computing
Ashish Tiwariand Rajeev Mohan Sharma (2019). *International Journal of Fog Computing (pp. 13-43).*
www.irma-international.org/article/realm-towards-service-optimization-in-fog-computing/228128

Accessing Big Data in the Cloud Using Mobile Devices
Haoliang Wang, Wei Liuand Tolga Soyata (2014). *Handbook of Research on Cloud Infrastructures for Big Data Analytics (pp. 444-470).*
www.irma-international.org/chapter/accessing-big-data-in-the-cloud-using-mobile-devices/103225

Fog Computing Quality of Experience: Review and Open Challenges
William Tichaona Vambe (2023). *International Journal of Fog Computing (pp. 1-16).*
www.irma-international.org/article/fog-computing-quality-of-experience/317110

IoT-Fog-Blockchain Framework: Opportunities and Challenges
Tanweer Alam (2020). *International Journal of Fog Computing (pp. 1-20).*
www.irma-international.org/article/iot-fog-blockchain-framework/266473