Evaluation and Establishment of Trust in Cloud Federation

By
Ayesha Kanwal
2011-NUST-MS-CCS-10

Supervisor
Dr. Muhammad Awais Shibli
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(February , 2014)

Abstract

Cloud computing provides scalable, elastic and on-demand services to various individual consumers, organizations and IT industry. It offers optimum resource utilization, broad network access, availability and measured services to all the consumers. The next evolutionary step of this technology is the Cloud federation, which brings remarkable advancement in Cloud services by extending the existing infrastructure for sharing of resources. It allows Cloud Service Providers (CSPs) to share their computing resources to fulfil the consumer's requests when the demand exceeds the limitations at certain time. One Cloud provider (home CSP) may rent in the resources of other provider (foreign CSP) who is available with its vacant capacity of infrastructure.

Besides various advantages, the Cloud federation has many challenges which mainly include optimum resource discovery, interoperable services, resource migration, establishment of trust between the participating Cloud providers and dynamic resource provisioning. Trust is one of the challenging issues that limit the adoption of Cloud federation by service providers. During the federation, the complete virtual machine images or partial data objects are migrated from home to foreign CSP domain which brings security and privacy concerns for Cloud consumers. In order to assure the security of data at foreign CSP platform, there is need to evaluate and establish trust between both participating Cloud providers.

Considerable work has been proposed over the last few years on trust evaluation and establishment in Cloud computing; however trust issues still emerge in Cloud federation with more advance risks. Existing trust evaluation techniques, methodologies and mechanisms are known as trust models in literature. These trust models are used to evaluate the trustworthiness of CSP based on certain factors and establish trust between Cloud consumers and CSPs. However, these modes are not adequate to evaluate trust between two CSPs participating in federation. There is need for more effective trust models that are based on multiple factors for trust evaluation and dynamically establish the trust in Cloud federation.

In this thesis we have carried out research in two major folds, where

one direction includes the comprehensive analysis of existing trust models in Cloud computing. After the detailed literature survey, we have proposed a benchmark for assessment of trust models in Cloud domain comprising of most essential trust evaluation parameters. Furthermore, we have proposed foremost taxonomies for functional and non-functional features provided by the existing trust models. First, we have explored and identified the obligatory functional features of trust models and presented them in form of comprehensive taxonomy. Our second taxonomy comprises of non-functional features which mainly covers the security, control, deployment and performance perspectives of trust models along with their mechanism of realization. We have analyzed existing trust models using our taxonomies to find the differences among them, in terms of providing these essential functional and non-functional features.

In second fold of research, we have proposed and implemented a trust evaluation system for establishment of trust between home and foreign CSPs participating in Cloud federation. The proposed system is based on two significant factors for trust evaluation namely the feedback provided by Cloud consumers and Service Level Agreements (SLAs) of participating service providers. After the evaluation of trust for CSPs, the Security Assertion Markup Language (SAML) is used to exchange the trust credentials between both the service providers. We have extended the SAML protocol by introducing a new profile "Trust Credential Exchange" which includes the new trust assertion and request response protocol. We have evaluated our work using two important verification tools which are Netlogo and Scyther. The verification of trust evaluation system is performed in Netlogo platform whereas the exchange of trust credentials using SAML protocol is verified through Scyther tool.