Dynamic Trust Evaluation Framework for Cloud Federation

By
Fowz Masood
NUST201260823MSEECS63012F

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 , 2015)

Dedicated

to

my Parents

and beloved sister!

Abstract

Cloud computing is an emerging technology, which is rapidly expanding. It offers a wide range of benefits like cost effectiveness, reduction in computational overhead, better accessibility and resource management to its customers. It is a demanding technology and more consumers and organizations are shifting their business to the cloud. Cloud federation is a newborn concept in cloud paradigm, in which different cloud service providers (CSPs) form federation; to enable resource pooling and better scalability.

Despite a number of benefits, cloud federation is facing a number challenges that need to resolved on immediate basis. One the prominent challenge is the lack of trust between the participating CSPs in cloud federation. Trusting a CSP whether it is providing the legitimate services is a major hurdle in the formation of federation. In this regard, numerous trust evaluation frameworks, models and schemes have been proposed to evaluate the trust of a CSP. A considerable work has been done to cater this issue however, the existing solutions don't provide the adequate level of trust evaluation required. The limitation of existing frameworks is they are static; the trust of a CSP is evaluated once and not monitored or updated later. However, the dynamic nature of cloud demands a continuous monitoring of the services offered by a CSP; this brings a major threat in case one of the CSP's performance gets malice. Recently, risk based access control model (RAC) has been introduced, unlike traditional access control models it is considered to be more dynamic and adaptable. RAC is a flexible access control model, which makes it one of the most appropriate safeguards for mitigating the security issues in cloud environment.

In this thesis, we have carried out research in two folds. In the first fold, we have highlighted the need of trust in cloud computing specifically in cloud federation. After that, we have performed an extensive literature survey on the existing trust models/frameworks. We have analyzed that existing trust models/frameworks don't provide the appropriate security level

required, which creates a need for an advanced trust model that can mitigate those security issues.

In the second fold, we have proposed a dynamic framework for the evaluation of CSP's trust in cloud federation. The proposed framework actively monitors the CSP's services and based on it updates the trust value. This trust value is further used for the calculation of risk score and finally the decision of allowing or disallowing access to a resource is executed. We have used RAC (risk based access control) model for countering the existing trust challenges in cloud federation. RAC is an emerging access control model and currently there is no well-defined interpretation of RAC model in a standard policy language. This creates a strong need for representing the RAC model into a standard policy language therefore; to address this issue we have presented a comprehensive eXtensible access control markup language (XACML 3.0) profile for it. The profile provides the core components of RAC model and also the mapping of RAC model to XACML tags. The profile will not only help people in understanding the components of RAC but it will also provide assistance to the development community in the implementation and deployment of RAC model.