Secured Multi-tenant Network Collocation in Horizontal IaaS Federation

by

Anant Vitthalrao Nimkar

Research Scholar, Department of Computer Science and Engineering, IIT Kharagpur, India

PhD Thesis Abstract

Cloud computing delivers virtual resources as a utility over the Internet using Infrastructure as a Service (IaaS) delivery model. If the cloud provider cannot fulfill customers' requirements, it may borrow virtual infrastructures through collaboration with additional cloud providers. In Horizontal IaaS Federation (HISF), Service Providers (SePs) federates with Infrastructure Providers (InPs) and supply virtual networks out of data centers to their customers. Virtual networks consist of sets of virtual nodes connected by virtual links. The collocation of tenants' virtual networks across data centers is termed as Multi-tenant Network Collocation (MNC). In HISF, management of federated virtual resources and management services must be cooperatively handled by subsets of federating participants, viz. SePs, InPs and customers. The virtual resources are also jointly owned by subsets of federating participants. To provision secured multi-tenant network collocation in HISF, this thesis focuses on three research issues, namely, (i) Authorization of federated virtual resources, (ii) Authentication of subjects in federated environment and (iii) Secure placement of federated resources after authorization and authentication. It attempts to address the issues like, service provider lock-in, unavailability of a particular service provider and unavailability of heterogeneous environment etc.

In HISF, the management of federated virtual resources and federation services must be cooperatively handled by subsets of federating participants, viz. SePs, InPs and customers. The virtual resources are also jointly owned by subsets of federating participants. The proposed Federation Access Control Model (FACM) addresses the authorization using a companion Name and Label Space Model (NLSM) using a new concept of subjects as subsets of federating participants. The authorization of subject over object using FACM and NLSM is carried out in two steps. First, NLSM finds the security labels of subject and object. Second, FACM finds the discretionary access rights of subject over object. Subjects can be authorized to access objects by collective decisions of MAC and DAC policies through i) comparison of security labels using Cartesian operators and ii) federated discretionary access rights respectively. Caucus Authentication Protocol (CAP) addresses the issue of authentication of subjects composed of one or more federating participants using a variant of Multi-Party Computation. CAP first authenticates all federating participants in the subject and finally the subject itself. The secure placement of virtual resources is addressed by proposing two protocols, viz. Node-and-Path Label Distribution Protocol (NPLDP) and Secure Virtual Topology Embedding Protocol (SVTEP). NPLDP and SVTEP facilitate secure placement and balanced embedding of virtual networks using MAC-and-DAC based Access Control Enforcement Engine (ACEE) and MAC-based Enforcement Engine (MACEE) of FACM. SVTEP finds optimal physical router and physical path, and then calls NPLDP for secure placement of the virtual routers and links. NPLDP is a signaling protocol to instruct physical routers for secure placements of virtual resources. ACEE provides security provisions by enforcing MAC and DAC policies. MACEE uses MAC policies to multiplex and de-multiplex traffics between physical and virtual routers. This work addresses the security issues related to authorization, authentication and secure placement of virtual resources in multi-tenant network collocation in horizontal IaaS federation.