Secure and Robust Data Services in Cloud and Fog

Chunming Rong

Cloud Computing makes resources such as data available anywhere at anytime, by enabling IT-related capabilities to be provided as services, accessible without requiring detailed knowledge of the underlying technology. Many mature technologies are used as components in Cloud Computing, but still there are many unresolved and open problems. Security in the cloud domain is considered as one of the top challenges. Cloud and IT service providers should be responsible for the data of their customers and users. However, accountability frameworks for distributed IT services is needed but still absent; hence it is difficult for users to understand, influence and determine how their service providers honor their obligations. It is important to support users in deciding and tracking how cloud service providers use their data. By combining methods of risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress. In any cloud service model, multiple stakeholders are involved. One service provider can be the consumer of another service. The complex stakeholder relationships require precise monitoring and accounting. Monitoring can be performed in multiple layers with different granularities. In the Infrastructure as a Service (IaaS) model, a customer has a set of virtual machine instances that are reachable by each other. Instances can be located in different geographical regions. A variety of technologies are capable of providing instances connectivity, including network virtualization. From the network monitoring perspective, distinguishing customers activities in a multi-tenant network is crucial. There are recent studies to improve architecture of the networking services for cloud platform using Software Defined Networking (SDN). Fog Computing extending the Cloud paradigm closer to the source using these newly available virtualization tools to redirect the data stream locally. Data may be processed locally within a trusted perimeter. Hence, data may be shared only after a controlled and processed in a fog before forwarding into a cloud. Raw data is often kept behind and there is less traffic burden for the core infrastructure to datacenters in the cloud.