Secure Cloud Computing and Cloud Forensics

Dr. Bhavani Thuraisingham
The University of Texas at Dallas (UTD)

April 15, 2011

Cloud Computing: NIST Definition

- Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five **key characteristics**, three **delivery models**, and four **deployment models**.
- **Key Characteristics:** *On-demand self-service, Location independent resource pooling. Rapid elasticity, Pay per use.*
- **Delivery Models:** *Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS).*
- **Deployment Models:** *Private cloud, Community cloud, Public cloud. Hybrid cloud.*
- Our goal is to demonstrate policy based assured information sharing on clouds

Security Challenges for Clouds

- Policy
  - Access Control and Accountability
- Data Security and Privacy Issues
  - Third party publication of data; Security challenges associated with data outsourcing;
  - Data at the different sites have to be protected, with the end results being made available; querying encrypted data
  - Secure Query Processing/Updates in Cloud
- Secure Storage
- Security Related to Virtualization
- Cloud Monitoring
- Protocol and Network Security for Clouds
- Identity Management
- Cloud Forensics