Cloud Data Management Policies: Security and Privacy Checklist

Karuna Pande Joshi

CSEE Department, University of Maryland, Baltimore County
(karuna.joshi@umbc.edu)

Organizations have complex enterprise data policies, as well as legal and statutory constraints, that require compliance. Such policies are today enforced on internal resources that are completely controlled by the organization. On moving to a cloud based solution, the organization has to often hand over this control to the service provider. Hence, acquiring cloud services requires significant human intervention and negotiation -- people have to check whether a provider's service attributes ensure compliance with their organization's constraints. It is critical to ensure security and privacy of data on the cloud. In fact security concerns are one of the key adoption barriers of cloud services, especially for public or hybrid cloud deployments. Multi-tenancy related security/isolation issues and cross domain cloud access/authorization are some of the important privacy issues that organizations are concerned about.

In this paper we define the critical security and privacy policies that an organization adopting cloud computing must formulate to ensure their enterprise data policies and constraints are addressed by the cloud provider. These policies are part of an essential check list that should be referred to by every organization migrating to the cloud.

Data Security: The critical policies to formulate for ensuring data security are listed below.

1. Cloud Data Location policy – e.g. US jurisdiction, Europe jurisdiction, Global etc.
2. Data Deletion policy - e.g. Data Archived, Secure wipe, etc.
3. Data Encryption policy - includes Encryption Key management
4. Identity Management policy
   a) Authentication Mechanism (e.g. ID/Password, SmartCard (CatCard), PIN, etc.)
   b) Authorization Methods (e.g. Limited Administrator Access, Group Level Access, Need-to-know access – Individual based)
5. Service Level Agreement (SLA) Monitoring plan - critical to ensure performance and ROI
6. Incident response - Cloud support SLAs should include
   a) Availability timeframe of services
   b) Contingency (Business Continuity) plans
   c) Timeframes for notification and recovery following an unplanned service disruption or a security incident
   d) Problem resolution and escalation procedures
   e) Scheduled maintenance times.
7. Cloud Forensics – track data access, specifically hacking attacks.
8. Cloud Data Audit – track cloud data usage, update, by user, by application etc.

Data Privacy: The critical policies to formulate for ensuring data privacy include:

1. Privacy policy on data access across services, across consumers.
   a. Personal Identity Information (PII) data policy
2. Virtual Machine Separation
3. Controlled Multi-tenancy – e.g. restrict tenancy of organizations not following compliance.
4. Disclosure Risk Assessment
   a. Existing Data – e.g. data breach by authenticated users etc.
   b. Inferred Data – e.g. released data can be combined with social media data to get PII.