CLOUD COMPUTING ISSUES

SATYANARAYANA PANUGANTI

LINUX ADMINISTRATOR AND CERTIFIED SOLUTIONS ARCHITECT AWS

ROADMAP

- Security
- Costing Model
- Service Level Agreement (SLA)
- Cloud Interoperability Issue
- What to migrate?
- Legal and compliance

SECURITY

It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack

COSTING MODEL

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds.

SERVICE LEVEL AGREEMENT

- Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA meta specifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework

CLOUD INTEROPERABILITY ISSUE

Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data center for highly interactive modeling applications in a pharmaceutical company).

LEGAL AND COMPLIANCE

AWS COMPLIANCE:

https://aws.amazon.com/compliance/

AZURE COMPLIANCE:

https://aws.amazon.com/compliance/

WHAT TO MIGRATE

Solely depend on the consumer and organizations.

Thank you