Migration to Cloud

Broad Approaches to Migrating into the Cloud

- Cloud computing is a "techno-business disruptive model"
- "Cloudonomics" deals with the economic rationale for leveraging the cloud and is central to the success of cloud-based enterprise usage.
- Decision-makers, IT managers, and software architects are faced with several dilemmas when planning for new Enterprise IT initiatives like
  - At what IT costs—both short term and long term—would one want to migrate into the cloud?
  - While all capital expenses are eliminated and only operational expenses incurred by leveraging the cloud, does this satisfy all strategic parameters for enterprise IT?
  - Does the total cost of ownership (TCO) become significantly less as compared to that incurred when running one's own private data center?

Why Migrate?

- An enterprise application can be migrated into the cloud because of:
  - Economic and business Reasons
  - Technological Reasons

Many of these efforts led Adoption of or integration with cloud computing services which is a use case of migration.

Why Migrate?

Migration can happen at one of the five levels :

a. Application : application is clean and independent, so it runs as it is

b. Code : some degree of code needs to be modified and adapted

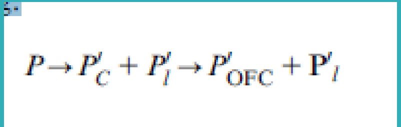
c. Design : the design(and therefore the code) needs to be first migrated into the cloud computing service environment

d. Architecture : core architecture being migrated for a cloud computing service setting, this resulting in a new architecture being developed, along with the accompanying design and code implementation.

e. Usage: while the application is migrated as is, it is the usage of the application that needs to be migrated and therefore adapted and modified.

Why Migrate?

With due simplification, the migration of an enterprise application is best captured by the following:



$$P \rightarrow P'_C + P'_l \rightarrow P'_{\mathrm{OFC}} + \mathrm{P}'_l$$

P: application before migration running in captive data center,

P’c : application part after migration either into a (hybrid) cloud

P’l : part of application being run in the captive local data center,

P’OFC : application part *optimized for cloud*.

If an enterprise application cannot be migrated fully, it could result in some parts being run on the captive local data center while the rest are being migrated into the cloud—essentially a case of a hybrid cloud usage. However, when the entire application is migrated onto the cloud, then P’l is null.

Cloudonomics

a. Migrating into the cloud is driven by economic reasons of cost cutting in both the IT capital expenses (Capex) as well as operational expenses (Opex).

b. There are both the short-term benefits of opportunistic migration to offset seasonal and highly variable IT loads as well as the long-term benefits to leverage the cloud.

c. It is the expression of when a migration can be economically feasible or tenable.

d. If the average costs of using an enterprise application on a cloud is su bstantially lower than the costs of using it in one's captive data center and if the cost of migration does not add to the burden on ROI, then t he case for migration into the cloud is strong.

Cloudonomics

a. Other factors that play a major role in the cloudonomics of migration are:

   a. The licensing issues (for perhaps parts of the enterprise application)

   b. The SLA compliances

   c. The pricing of the cloud service offerings

b. Most cloud service vendors, at a broad level, have tariffs for the kind of elastic compute, the elastic storage, or the elastic bandwidth.

c. The cloudonomics of migration should be soundly meaningful accommodating the pricing variability.

Deciding on the Cloud Migration

a. Post migration, the ROI on the migration should be positive for a broad range of pricing variability

b. Arriving at a decision for undertaking migration demands are that

- a. Either the compelling factors be clearly understood or
- b. The pragmatic approach of consulting a group of experts be constituted.
- c. Like software estimation, one applies wide Band delphi techniques to make decisions

Wide band delphi technique

a. A questionnaire with several classes of key questions that impact the IT due to the migration of the enterprise application is posed to a select audience chosen for their technology and business expertise.

b. Assume that there are M such classes. Each class of questions is assigned a certain relative weightage Bi in the context of the entire questionnaire.

c. Assume that in the M classes of questions, there was a class with a maximum of N questions.

Wide band delphi technique

Weightage-based decision making as M * N weightage matrix will be as follows:

$$C_l \le \sum_{i=1}^{M} B_i \left(\sum_{j=1}^{N} A_{ij} X_{ij} \right) \le C_h$$

Cl is the lower weightage threshold

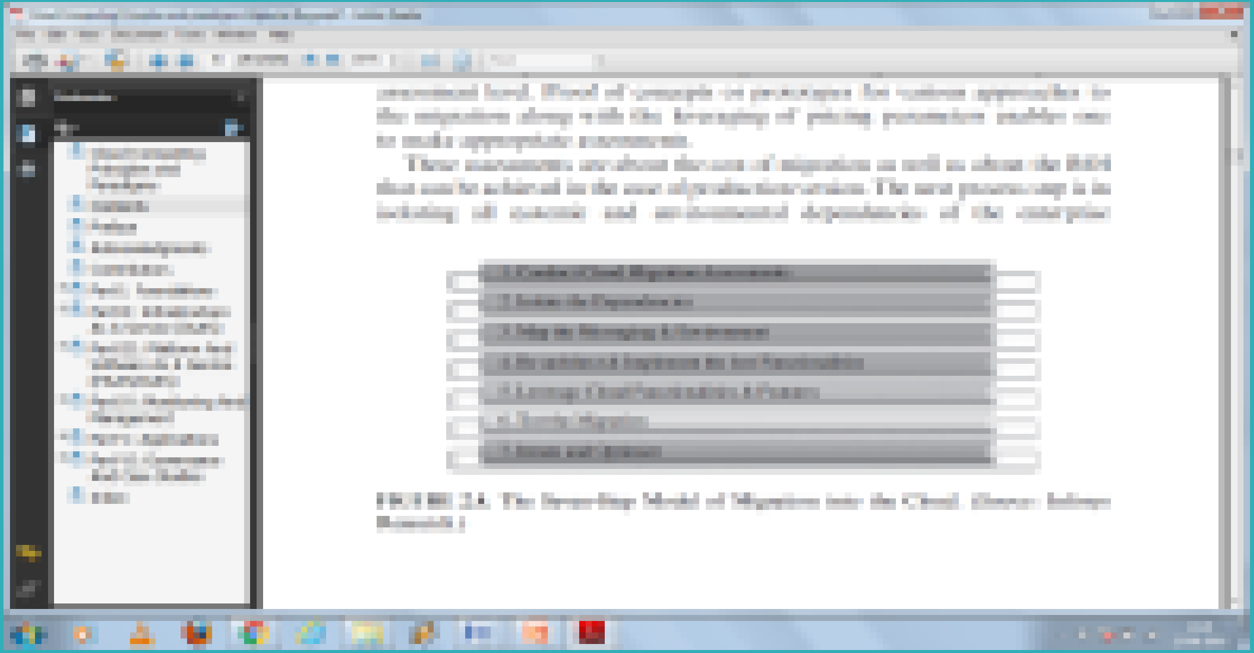
C_h is the higher weightage threshold

Aij is the specific constant assigned for a question

X_{ij} is the fraction between 0 and 1 that represents the degree to which that answer to the question is relevant and applicable

The lower and higher thresholds are defined to rule out trivial cases of migration. A simplified variant of this method can be presented as a balanced score card oriented decision making

The seven-step model of migration into a cloud



assessment level. Proof of concepts or prototypes for various approaches to the migration along with the leveraging of pricing parameters enables one to make appropriate assessments.

These assessments are about the cost of migration as well as about the ROI that can be achieved in the case of production version. The next process step is in isolating all systemic and environmental dependencies of the enterprise

1. Conduct Cloud Migration Assessments
2. Isolate the Dependencies
3. Map the Messaging & Environment
4. Re-architect & Implement the lost Functionalities
5. Leverage Cloud Functionalities & Features
6. Test the Migration
7. Iterate and Optimize

FIGURE 2.4. The Seven-Step Model of Migration into the Cloud. (Source: Infosys Research.)

The seven-step model of migration into a cloud

a. Conduct cloud migration assessment
   i. Understand the migration issues at the application level or the code, the design, the architecture, or usage levels
   ii. Assessing the tools being used, the test cases as well as configurations, functionalities, and NFRs of the enterprise application.
   iii. Cost of migration: ROI (Return on investment), TCO(Total cost of ownership), …

b. Isolate the dependencies
   i. Isolate all systematic and environmental dependencies of the enterprise application components within the captive data center

c. Map the messaging and environment
   i. Message map: displaying detailed, hierarchically organized responses to anticipated questions or concerns
   ii. Generate the mapping constructs between what shall remain in the local captive data center and what goes onto the cloud

The seven-step model of migration into a cloud

d. Re-architect and implement the lost functionalities

    i. Perhaps some functionality may be lost due to migration

    ii. Some part of the enterprise application may need to be re-architect, redesigned, and re-implemented on the cloud

e. Leverage cloud function and features

    i. Leverage the intrinsic features of the cloud computing service to augment the enterprise application

f. Test the migration

    i. Test the new form of the enterprise application (both on the captive data center and on the cloud as well)

g. Iterate and optimize

    i. Iterate and optimize the process

The seven-step model of migration into a cloud

The seven-step model of migration into a cloud

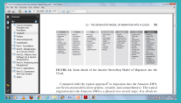


FIGURE 2.6. Some details of the iterative Seven-Step Model of Migration into the Cloud.

Compared with the typical approach to migration into the Amazon AWS, our Seven-step model is more generic, versatile, and comprehensive. The typical migration into the Amazon AWS is a phased over several steps. It is about six

Efficient Steps for Migrating to the Cloud

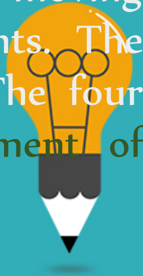
Based on the approach framed by the popular research firm, The Burton Group, the following five steps define the framework for a strong cloud adoption strategy.

- **Pre-Work**

To start with, organisations must build an internal cloud team, which together will set the scope of the cloud project. Expectations, standards to be achieved and cloud objectives must be well defined during the initial stages of the cloud journey.

- **Business and Application Analysis**

The cloud cannot be considered as plainly a technical enhancement since it has a strong impact on the various business functions. During this stage, business applications moving into the cloud are evaluated based on the costs and architectural requirements. The operational changes to be made within an organisation are also determined. The four significant components of this stage are business impact evaluation, assessment of organisational impact, cost analysis and application analysis.



Efficient Steps for Migrating to the Cloud

- **Selecting the Cloud Service Provider**

Solutions from different cloud service providers are reviewed and the most suitable one is chosen. The migration plan is initiated and the roadmap to cloud is thus made clear.

- **Building the Risk Mitigation Plan**

No cloud adoption framework can be complete without the risks and challenges being included. A risk mitigation plan is drawn and the exit strategy is devised.

- **Planning for the Steady State**

Once applications are moved to cloud, there needs to be a plan in place for the cloud governance and vendor management. Regular reviews of the strategy must be conducted and the cloud team must ensure that both internal processes and personnel issues are addressed during the move.

Risks in Cloud Computing

Risk can be defined as the probability that a malicious (hack attack or security breach) or non-malicious event (hardware or software malfunction) might occur that could potentially degrade the user experience (or) expose confidential information (or) threaten to corrupt the software or hardware components.

Types of Risks

a. Data Security:

Protecting sensitive and confidential data is termed as Data security.

Lack of security of data in the cloud implies to potential unauthorised access and privacy deficiency. Common areas of the cloud that show possibilities of compromised data are:

- Multiple tenants sharing the same infrastructure
- Industry-specific regulatory and compliance concerns
- Issues pertaining to mobility of data
- Storage recycling techniques adopted by the cloud service provider (CSP)
- Auditing and reporting of confidential business data

Data Storage Location

Data storage location is the physical place where the servers and storage devices are present.

With cloud, data has moved into the physical infrastructure of a third party and is maintained by an entity outside the control of the enterprise.

This shift in data storage location has caused considerable concern over data governance.

Cloud Service Outage

Cloud service outage is the time when cloud services are suspended due to reasons like technical glitches, failure of the cloud service provider or a security threat. Microsoft, Google, Amazon, Yahoo and almost every trusted brand have faced outages.

- It has a significant effect on the client business.
- Enterprises lose their credibility;
- Start-ups are dissuaded from greater cloud adoption and organisations of all types and sizes miss revenue opportunities- such is the impact of a business outage.

Shared Access

One of the defining features of public cloud computing is multi-tenancy. The multi-tenant environment of a public cloud allows the sharing of resources such as CPU, memory, storage space and servers between multiple unrelated clients. Such shared access to computing resources may pave the way for accidental sharing of data and higher chances of access to private data from the smallest discrepancies in the system.

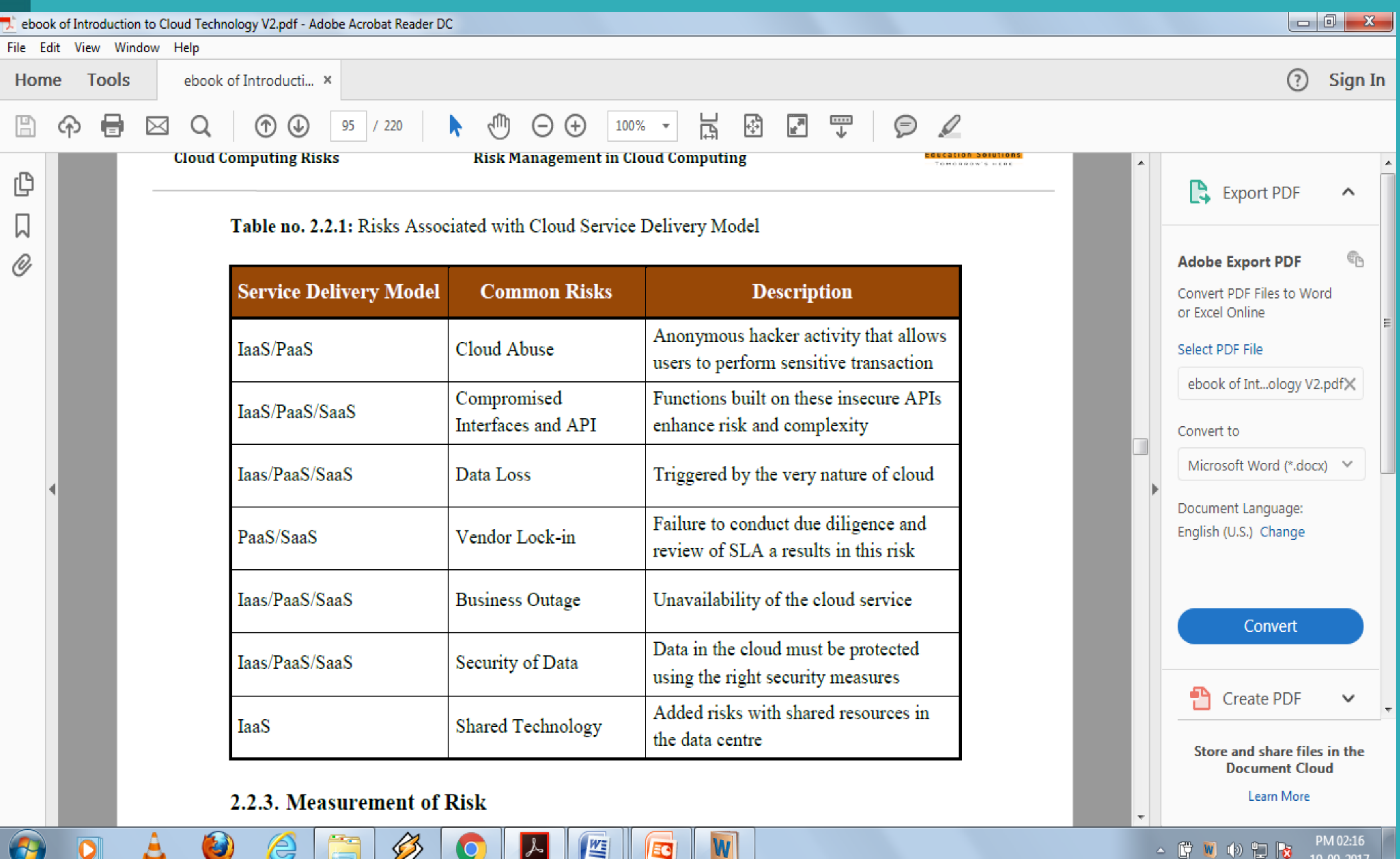
Service Level Agreements (SLA)

In order to set the expectations right for both the cloud vendor and the customer, a service level agreement is essential. A comprehensive agreement between the two parties must eliminate the risks related to service uptime, performance, security, disaster recovery, access to data as well as the location of data. Service level agreement also plays a key role in accommodating changes and in dispute mediation.

Regulations Across Geographies

When critical information moves past the boundaries of the data centre of an organisation, it carries the risk of noncompliance to industrial and geographical regulatory measures.

For instance, a healthcare organisation located in Germany stores data based on the European Data Protection Directive regulations (EU DPD). When that same company partners with a US-based cloud service provider for backup solutions, the Health Insurance Portability and Accountability Act regulations (HIPAA) comes into picture. Failure to abide by these location- or industry-specific regulations may result in substantial penalties and prove to be a heavy blow to small- and medium-sized organisations


ebook of Introduction to Cloud Technology V2.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools ebook of Introducti...
Sign In
95 / 220
100%
Export PDF
Create PDF
Convert
Select PDF File
Learn More
PM 02:16

Cloud Computing Risks Risk Management in Cloud Computing

Table no. 2.2.1: Risks Associated with Cloud Service Delivery Model

Service Delivery Model	Common Risks	Description
IaaS/PaaS	Cloud Abuse	Anonymous hacker activity that allows users to perform sensitive transaction
IaaS/PaaS/SaaS	Compromised Interfaces and API	Functions built on these insecure APIs enhance risk and complexity
Iaas/PaaS/SaaS	Data Loss	Triggered by the very nature of cloud
PaaS/SaaS	Vendor Lock-in	Failure to conduct due diligence and review of SLA a results in this risk
Iaas/PaaS/SaaS	Business Outage	Unavailability of the cloud service
Iaas/PaaS/SaaS	Security of Data	Data in the cloud must be protected using the right security measures
IaaS	Shared Technology	Added risks with shared resources in the data centre

2.2.3. Measurement of Risk

Adobe Export PDF

Convert PDF Files to Word or Excel Online

ebook of Int...ology V2.pdf

Convert to: Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Store and share files in the Document Cloud

Measurement of Risk

a. Measures related to data security such as data encryption standards, key management and hierarchal access.

b. Client side efforts - as nothing can prevent data espionage when the customers are not vigilant enough to avert disasters.

c. Geographical location and physical protection of data centres.

d. Service level agreements to ensure proper service by the cloud service providers.

e. Access Controls to ensure efficient, effective and secure sharing of resources between clients utilising the same infrastructure.

f. Financial Controls within and outside the organisation to ensure that both internal teams and cloud service providers operate well within budgets allocated

Risk Assessment

The risk assessment strategy used by an organisation must contain the following elements:

a. **Effective Control Mechanism:** All the current controls over data are to be analysed. If it doesn't provide adequate protections for the data or service, then necessary data control mechanisms are to be implemented.

b. **Necessary Periodical Audits:** The cloud service provider and the services rendered are to be analysed and audited on a monthly, quarterly or annual basis. Any kind of discrepancies in service should be noted, informed and necessary corrective measures are to be implemented.

c. **Technical Security Architecture:** A thorough analysis of the present technical architecture of the cloud service provider should be done. Firewalls, Virtual Private Network provisions, patching, intrusion prevention mechanism and network segregation are few things to be analysed well. These are potential high risk areas especially when confidential customer data is at stake.

d. **Data Integrity:** The cloud service provider would be rendering the services to multiple clients at a time. How well the data is stored, what kind of hardware is being used, if the confidential data is being stored in a shared storage etc. - are to be analysed and understood beforehand. It is much better to have discussions with the cloud service provider before even moving all the data to the cloud.

e. **Data Encryption:** The data encryption standards that the cloud service providers utilise is to be audited beforehand. Strict investigation has to be carried out in this aspect, as its one of the high risk areas. Sony suffered a major outage in its PlayStation Network in 2011 due to their poor data encryption standards and hackers exploiting it.

f. **Disaster Recovery Plan:** What happens when there is an earthquake? Or flooding (or) some other natural calamity that hits the data center in which all the confidential data is being stored? Before getting into contracts, the disaster recovery and contingency plan provided by the cloud service provider should be reviewed thoroughly. Internally, the organisation should have a clear business continuity plan to ensure that the business doesn't get affected if in case there is a disaster.

g. **Standard Procedures:** Its good to evaluate the standard procedures followed by the cloud service provider internally in their operations. A typical example would be the offsite tape backup procedure for all the data stored in their data centre. Another example would be a background pre-employment screening procedure to see if any of the employees working at the data center (or) those to be involved in managing the data centre has any malicious intent.

h. **Business Operations of the Cloud Service Provider:** The current operational and financial conditions of the cloud service provider should be diligently verified along with the history of operations. For publicly traded companies, its easy to find this information. For private companies, either an internal team can do the due-diligence (or) a third-party can do the background check.

Cloud Risk Mitigation Strategies

The most effective cloud risk mitigation strategies are listed below:

a. **Due-Diligence on Various Cloud Solutions** Cloud computing leads to a higher dependence on cloud-based vendors and thus demands clients of an evaluation of their capabilities beforehand. Optimised security measures, industry recognised compliance standards and the ability to support the unique requirements of an expanding organisation must be analysed to mitigate the risk potential in a cloud project.

b. **Adapting Encryption Standards** Encryption of data is the act of converting sensitive data into undecipherable text by using the relevant algorithms. The encrypted data is called cipher text, and the level of encryption depends on the sensitivity of the data. Encryption solutions are of **two types:**

i. **Provider-side cloud encryption:** The cloud service provider encrypts the data received from clients and adds an extra layer of protection from potential threats. Many leading cloud vendors in the market, such as Amazon, Microsoft and EMC, offer these solutions to their clients.

ii. **Client –side cloud encryption:** Companies dealing with multiple cloud vendors make use of cloud encryption gateways to turn their plain text data into cipher text. Encryption makes the text unreadable without a special key.

c. **Secure Third Party Validation** Cloud security is better said than done. Not every cloud service provider is successful in keeping up with the security demands of the customer. This makes third party validation a must for cloud solutions. Independent technology auditors assess the solutions to ensure that they are capable of delivering the desired results.

User Access Controls: Cloud environments work better with Role-Based Access Control (RBAC). In this method, users of the system are assigned a specific role and can perform a precise set of functions based on this role. By restricting access to cloud resources, unauthorised access, accidental manipulation of data and sharing of credentials can be prevented.

Service Level Agreements and SSO Solution : A robust service level agreement holds the key to the performance levels of every element of the service provided by the cloud vendor. It affirms the ownership of data and lays the foundation for the security measures to be adopted during implementation.

The Single Sign-On (SSO) is one way of mitigating risk when it comes to protecting user data. The SSO technique eliminates the need for multiple re-authentications while using the system (or) set of applications and thus prevents authentication requests to be made to the server back and forth every time the user wants to use a particular application.

Hybrid Approach

This model of cloud computing allows organisations to host their most sensitive data internally while allowing the other secondary functions to reside on the public infrastructure. It offers the highest level of flexibility with no additional capital expense. With more business critical applications moving to the cloud, hybrid offers the best of both worlds.

Sony PlayStation Network Outage 2011: Case Study

Case Scenario

Sony Corporation first introduced the PlayStation Console in December 1994 in Japan. Since then the product has undergone a series of upgrades and enhancement. The latest version of the PlayStation called PS3 was a complete entertainment package and included internet browsing capabilities, chat functions, media downloads and gaming options. Registered users of the system were more than 75 million, and a huge chunk had also recorded sensitive information like credit card details for the purpose of online purchases.

The Outage

On April 19, 2011, Sony’s PlayStation Network experienced one of the worst cases of data security breach in the history of IT. The servers were hacked by an unauthorised group leading to the theft of usernames, passwords, credit card details and other personal information of millions of PSN users. The system was shut down for almost 7 days following the attack. The cause of the incident was mainly due to the poor security mechanisms of Sony and its failure to encrypt critical data.

Impact

This unfortunate event for Sony brought down its reputation, credibility and stock value. Sony rebuilt its security system, faced a lawsuit that was settled after almost 4 years and paid huge compensation to its customers who were exposed to the incident. The service was made to shut down for almost 3 weeks, and the cost of the outage was over 170 million dollars.

Thank You