ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Study on Issues of Cloud Computing

Mamta Sharma[1], Romika Yadav[2], Vinti parmar[3]

Jamia Hamdard University, New Delhi, India[1]

Research Scholar, Indira Gandhi University, Meerpur, Rewari, India[2]

Research Scholar, Indira Gandhi University, Meerpur, Rewari, India[3]

ABSTRACT: Cloud Computing has the potential to transform large tracts of the IT industry and reshape the way computing hardware and software is purchased. Cloud offers a platform that encourages innovative and new technologies from developers as well as flexibility and cost advantages to cloud users. However, the nature of the shared environment and scalability of cloud computing pose a significant threat to data privacy. This paper outlines key opportunities, risks, and vendor consideration in regard to cloud computing.

KEYWORDS: cloud computing, federal risk, security survey, cloud technologies, as-a-service.

I. INTRODUCTION

Cloud Computing has grown at a blistering pace: the term was first used in the mainstream in 2007, and its 2013 market is predicted to be $ 150 billion. A multitude of services are now provided, with the “as-a-service” model expanding far beyond applications to such offerings as desktops and networking in the cloud. Service models vary widely and continue to branch out in new areas. Xaas refers to anything as a service as more companies are offering varied products and providing an alternative to almost every traditional IT function. High-level advantages and constraints of the cloud environment are listed below.

ADVANTAGES

- Flexibility: adds alternatives in cost structure and operations platforms for IT
- Scalability: storage and processing power appear unlimited from user’s perspective.
- Low Initial Cost: no large outlay for infrastructure or support.
- Service Model: pay for what is used-no excess capacity.
- Speed to market: allow for significant decrease in deployment time.

CONSTRAINTS

- Shared Environment: concerns around sensitive data on potentially desegregated systems
- Data Segregation/Custody: issues of ownership and physical location of data
- Vendor Lock-in: Complexity of support and increased cost over time
- Migration: many applications and operations are prohibitively difficult to implement

Advantages of transforming applications and systems to the cloud must be weighted carefully against what is being outsourced, namely control of an internally managed system and a level of comfort over its security. A high degree of responsibility and trust is given to the cloud provider to manage critical services. Due diligence must be performed to validate that trust.

II. WHAT IS THE CLOUD?

There seems to be a divide in familiarity with the use of cloud services and their terminology. Many activities that are not explicitly in the cloud are used extensively by the average internet user. Web-based email and online backup

DOI: 10.15680/IJIRCCE.2016. 0402045

existed long before anyone had heard of cloud computing, making cloud services more recognized in their use than their description. Confusion exists even among governing bodies and industry leaders.

The National Institute for Standards and Technology (NIST) issued guidelines on cloud computing in December 2011 and offered the following definition of the public cloud: "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources(e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction."

Put more simply: The cloud offers remote computing resources (hardware and software) delivered over a network as a service. The network, particularly with public cloud, is usually the internet. Hybrid clouds (any blend of private, community, or publics environments are also possible. As these technologies develop and market acceptance increases, the future shape of the landscape will continually become clearer.

III. UNIQUE RISKS

Large questions loom from companies considering moving critical IT services to the cloud. Four keys concerns needs to be addressed for cloud to convince companies that their solutions are effective and secure.

1. **TRANSPARENCY**
   Open communication and expectations are critical. The cloud customers should be comfortable with standards and controls of the cloud provider. The provider should provide assurance that all operational and regulatory concerns are known and well-controlled.

2. **STANDARDS**
   Progress is already being made in standardization. Both the Federal Financial Institution Examination Council and European Commission have recently provided guidance on vetting and implementing cloud services. The FFIEC focused on due diligence, vendor management, and legal considerations for financial institutions. They view cloud as an extension of traditional IT outsourcing with only a few caveats. The critical factor for the FFIEC is that a cloud provider will meet all the institution's existing requirements for outsourcing IT services.

3. **INTEGRATION**
   Although investments may be low, lack of familiarity with cloud services and the challenges of integrating with existing systems can result in additional operating cost. Employees of the Enterprise will need additional expertise to accommodate cloud technologies and integrate them with existing infrastructure.

4. **SHARED INFRASTRUCTURE**
   Nothing fundamentally prevents private cloud environments from being as secure as traditional in-house IT infrastructure. Many security concerns can be overcome with the use of the right technologies, such as VLANs and encrypted storage.

IV. VENDOR CONSIDERATIONS

Specific criteria should be considered when evaluating service offering from cloud vendors. The services should achieve internal goals of security and performance. Does the vendor have a track record of strong performance against SLAs and provide resources for performance monitoring. Do they have clear and available channels of communication for performance issues?

Ultimately, the vendor must prove their security governance processes are mature and well-aligned with the information security process of the business. If expectations are not explicitly clear, performance issues can damage the implementation and relationship. Just as critically, the vendor should be aware of the regulatory climate faced by the client. Many cloud providers are technology-oriented firms that may be unfamiliar with legal requirements and the consequences of failing to protect sensitive information.

V. VIABILITY OF THE CLOUD

Cloud Computing is here to stay. It provides a significant opportunity for small businesses to overcome technology hurdles that hinder rapid growth. Companies without mature IT infrastructure and little capital can benefit from the cloud computing low initial cost and ease of deployment. Large companies can benefit from the cloud's ability to rapidly magnify computing ability for large workloads. Retailers are able to outsource data processing when loads increase during holiday season. Companies with large software development operation benefit from using deployment and test environments that offers increased efficiency and agility. Cloud solutions are also finding improved acceptance in the business world. A 2012 study revealed 50% of C-level and purchasing managers had "complete confidence" in the cloud, up from only 13% in 2011.

Vendors are making a compelling case for the adoption of cloud services due to additional functionality at a potentially lower cost of ownership. Security concerns are easing as well. Although still the top inhibitor to cloud adoption , security was a concern to only 55% of survey respondents. Initial wariness surrounding security features and vendor reputation has given way to more openness due to increased familiarity and the realization of cost and performance benefits.

VI. CONCLUSION

When an organization evaluates a cloud service, it is important to confirm the appropriateness of the migration. All the data involved should be analysed to identify potential risk to the organization. Business analysis and consultation with the Enterprise Risk and Resilience group should be performed before implementing any cloud based services.
Every organization faces particular challenges with cloud providers due to the nature of business. Client contracts require the same high security standards and data accountability, regardless of location.

Expected requirements that may apply to any cloud vendor include:

- ✓ Right to audit clauses in cloud contracts
- ✓ PCI-DSS compliance at all times for applicable systems
- ✓ All personnel handling customer data should complete a background check and annual security awareness training
- ✓ Annual external penetration tests with available reports
- ✓ Daily or constant review of systems and application logs for security issues
- ✓ Vulnerability scans completed periodically, available for review, and issues remediated promptly
- ✓ Requirements for data and systems log retention for forensic purposes

Any of contractual obligations can extend to vendors. Everything in information security programs: change control, patch management, control environment (including ethical training, hiring practices, and audit processes) should exist at vendors at the same level of quality. The cloud present many unique advantages, but any agreement necessitates careful evaluation and due diligence. We are ultimately responsible for assuring the safety of client data and proprietary information.

REFERENCES

[1] Researchpedia, Cloud Computing Services- Market Size and Adoption [online]. Available from : http:///www.theresearchpedia.com
[2] Dmitry Bestuzhev,SecureList-Financial data Stealing Malware [online]. Available from: http:///www.securelist.com
[3] North Bridge Venture Partners, Cloud Computing Survey [online], Available from: http://www.northbri
[4] R. B. Guin et al, "A smart Architectural concept for making of a University Education System using Cloud Computing Paradigm", IEEE World Congress on Information and Communication Technologies, pp. 48-52, 2011.
[5] G. Fernández st al, "Analysis of the Cloud Computing Paradigm on Mobile Health Records Systems", 36th IEEE
Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 927-932, 2012.

[6] D. S. Phatak et al, "A New Paradigm to Approximat Oblivious Data Processing (ODP) for Data Confidentiality in Cloud Computing", IEEE World Congress on Services, pp. 391-398, 2011.

[7] Z. Yang et al, "A Cost-based Resource Scheduling Paradigm in Cloud Computing", IEEE 12th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 417-422, 2011.

[8] D. C. Barboza et al, "A Simple Architecture for Digital Games on Demand using low Performance Resources under a Cloud Computing Paradigm", IEEE Brazilian Symposium on Games and Digital Entertainment, pp. 33-39, 2010.

DOI: 10.15680/IJIRCCE.2016. 0402045