Cloud Computing Security & Challenges

Paper Presentation Report

Shashwat Kathuria - B17CS050

10th February 2020
CSL7090 - Fractal 1
Dr. Sumit Kalra

RESEARCH PAPER INFORMATION

Kuyoro, S. O. and Ibikunle, F. and Awodele, O. (2011) Cloud Computing Security Issues and Challenges. International Journal of Computer Networks

387 number of citations as of 10.02.2020

Link to paper : [Cloud Computing Security Issues and Challenges]

INTRODUCTION

The paper referenced above mentions some of the key issues faced or worried by organizations to deploy their services to the cloud and which hamper the ability of the cloud computing platform to grow even faster when it can be so useful and crucial for the growth of organizations.

CORE IDEA / NOVELTY

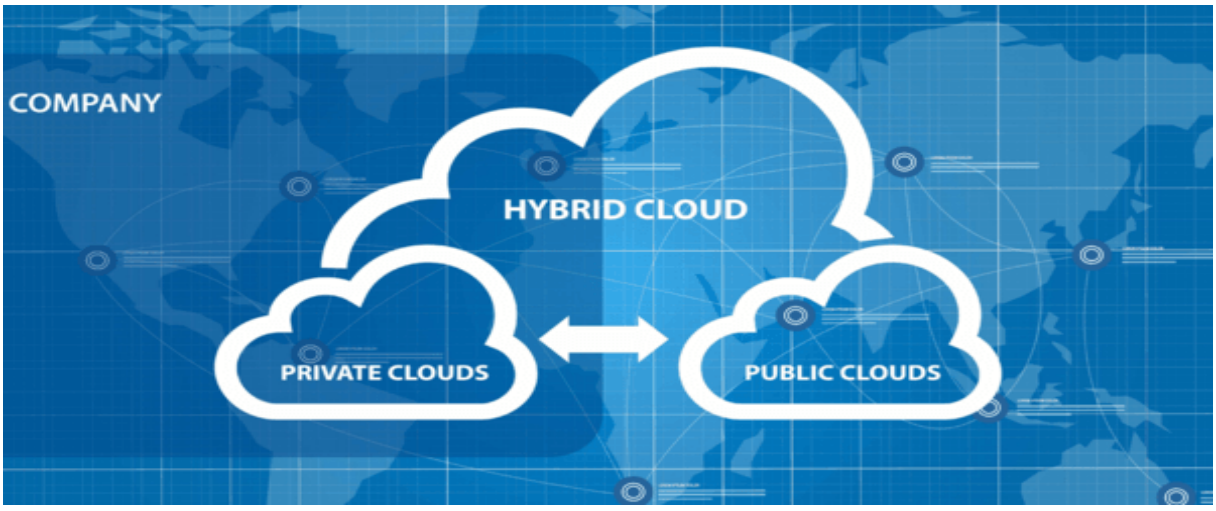
Some of the reasons why organizations hesitate to choose cloud computing (in order of decreasing priority in general) comprise of :

ISSUE	ISSUE RATING %
Security	74.6 %
Performance	63.1 %
Availability	63.1 %
Complexity of integrating with in-house IT	61.1 %
Less customizing availability	55.8 %
More cost on-demand	50.4 %
Switching back and forth for future	50.0 %
Regulatory requirements	49.2 %
Less number of providers	44.3 %

The following security issues are addressed :

- ➔ Privileged User Access
  - ◆ Data ownership issues
  - ◆ Information transmission risks from client through Internet
- ➔ Data Location
  - ◆ Information about country name in which data is stored
  - ◆ Also the law of that country
- ➔ Regulations
  - ◆ Clients accountable for the security of their solution
  - ◆ Reason being that they can choose between providers
- ➔ Segregating Data
  - ◆ Multiple clients having their data encrypted on the same hard disk
  - ◆ Separation mechanism required
- ➔ Recovery
  - ◆ In cases of corruption of data
  - ◆ Also for natural calamities and disaster
- ➔ Checking and Investigation of provider
  - ◆ Useful for client in cases of doubt or suspicious activity
- ➔ Long-Term Contract
  - ◆ Ability to revoke contract according to provider situation

The main focus remains on the security aspect of cloud computing services in the following domains :



PRIVATE CLOUD

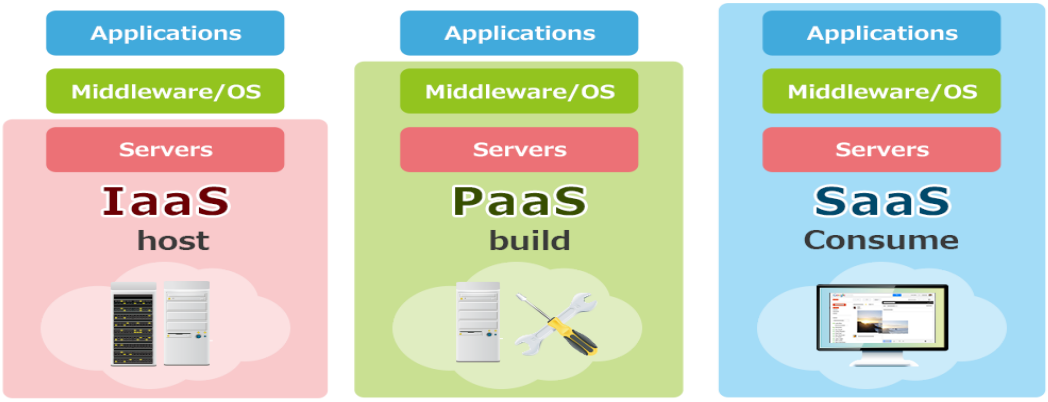
Refers to cloud computing on private networks. Usually much more secure than public cloud because of the known structure inside the organization along with the stakeholders.

PUBLIC CLOUD

Refers to cloud computing in the common mainstream sense. Because it places an additional task of ensuring all applications and data accessed on the public cloud are not subject to malicious attacks, it is usually less secure than other cloud models.

HYBRID CLOUD

It is a private cloud linked to one or more centrally managed external services, it provisions as a single unit and also is a secure network. Usually more secure provision of control of data and applications and allows multiple clients to access information over the Internet.



INFRASTRUCTURE AS A SERVICE - IaaS

It is a single tenant cloud layer where the cloud computing vendor's resources are only shared with contracted clients at a fee. They provide only basic security like perimeter firewall, load balancing, etc. Applications that are moved to the cloud in general require higher levels of security provided at the host.

PLATFORM AS A SERVICE - PaaS

PaaS refers to a set of software and development tools provided and hosted on the cloud provider's machines. The virtual machines used here must be protected against malicious attacks such as cloud malware. Well enforced authentication checks and integrity of the applications across networking channels is very much required here.

SOFTWARE AS A SERVICE - SaaS

SaaS refers to the end product softwares used by users, typically on the internet. Web browser security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL), etc for data protection are crucial here.

CLOUD COMPUTING CHALLENGES

SECURITY

Security has played the most significant role in hindering the growth and widespread use of cloud computing. Using someone else's hard disk to store an organization's data is still hesitant to many. Many security issues like data loss, phishing, botnet pose serious detrimental effects on the organization's data and software, along with the introduction of new models like multi-tenancy.

COSTING MODEL

Although using the cloud can significantly decrease the infrastructure costs, it raises the cost of data communication, referring to the cost of transferring of organization's data to and from the public. The problem is even more if the client or organization uses a hybrid model of cloud where the data is distributed both in private and public clouds.

CHARGING MODEL

The cost analysis is very complicated for elastic resource pools rather than data centers, and they often calculate their cost according to static computing time also. Charging models of SaaS providers can be changed by introducing multi-tenancy and amortization based on the host machine cost rather than the single virtual machine cost. Therefore, for SaaS sustainability, these strategic moves are required along with reduced overheads for multi-tenancy.

SERVICE LEVEL AGREEMENT

The cloud providers need to ensure quality, availability, reliability and performance of their hosted infrastructure along with regular feedback and improval to stay in sync with their clients who often find the agreements rather granular and complicated.

MIGRATION

Organizations often migrate the marginal tasks and functions to the cloud and handle their core competencies themselves in-house, so, cloud providers should provide them with the security, performance, trust and easiness to make them eager to move their core competencies to the clouds too.

CLOUD INTEROPERABILITY ISSUE

This happens due to vendor lock-in, i.e., being forced to the amount of options available to the specific vendor and also, due to very different ways of providing services depending on the cloud provider. It is sometimes also difficult for the organization to integrate the cloud services to the organization's legacy systems. Standardization remains the key to address this interoperability issue, though it is not such a major issue.

CONCLUSION

It is important to be cautious of the security concerns of this very new revolutionizing technology. There are many security risks for the cloud computing platform as seen above. Cloud computing has the potential to become a leader in providing a secure, virtual and economically feasible IT solution.

REFERENCES

Kuyoro, S. O. and Ibikunle, F. and Awodele, O. (2011) Cloud Computing Security Issues and Challenges. International Journal of Computer Networks

---

THANK YOU
