Strengths and Vulnerabilities of Cloud Computing in Mauritius

Pravin Selukoto Paupiah
Amity Institute of Higher Education
Cybercity, Ebene, Mauritius
selukoto@gmail.com
pspaupiah@mauritius.amity.edu

ABSTRACT

This research paper is based on the Strengths and vulnerabilities of cloud computing in Mauritius and abroad. In this research paper, a holistic view was taken on some security concern in cloud computing spanning across the possible issues and vulnerabilities connected to different infrastructures and software platforms. It will give an insight of the aspect of securities of cloud computing on data protection, confidentiality, vendor lock-in and data portability and evaluate the security systems implemented within cloud service models like Software as a Service, Platform as a Service, Infrastructure as a Service and Network as a Service. This paper will help you to identify the areas where organisations should focus before choosing an appropriate Cloud Service Provider (CSP) prior to moving to clouds.

KEYWORDS

Cloud Computing, Security, Data Protection.

1 INTRODUCTION

Cloud computing is an emerging paradigm in delivering computing resources as a service (Software as a Service, Platform as a Service, Infrastructure as a Service or Network as a Service) to both consumers and corporate over the internet from large scale data centres or "clouds". Businesses are keen to capitalise on the services offered by cloud computing because of the operating costs rather than investing in hardware and software. Cloud computing is gaining immense popularity in the IT industry. It relies mostly on the internet broadband for users to access to its service on an "On-Demand Service Pay for Usage". With the rapid expansion in this new era of technology, the security threats inherent in the cloud are often ignored.

1.1 Characteristics of Cloud Computing

According to the National Institute of Standard and Technology, (NIST) some of the essential features of cloud computing are as follows [1]:

a. On demand self-service: It is possible for cloud computing clients to control the amount of server time and storage capacity that is required on a real-time basis on their own.

b. Broad network access: Users usually gain access to resources through the network (that is the internet), using standard mechanisms and protocols.

c. Resource Pooling: Different customers access the same facilities in a standard way. Sharing of resources maximises efficiently and reduces idle time of expensive equipment to a minimum.

d. Rapid elasticity: It is possible to respond promptly to changes in demand from different clients.

e. Measured service. Computer resource utilisation is regularly metered, promoting resource optimisation usage, and pay per use capabilities.

1.2 Categories of Service Model in Cloud Computing

Cloud Computing deployment models can differ depending on customer needs.
These cloud service models can either be delivered via a ‘public’ cloud, accessed via the internet, or a ‘private’ cloud which is more secured, using existing data centres and network capabilities. A hybrid combination of the two service models is also possible. The three deployment models are explained in more details below [2].

A public cloud is one where the cloud service providers (CSPs) have complete control over services provided. They set their own policies and charging models. A private cloud is used by a single organisation. However, it can be located outside the organisation and controlled by a third party.

A hybrid cloud is an amalgamation of multiple public and private cloud where data and applications can easily be shared among themselves by making use of appropriate technologies.

There are different ways in which cloud services can be deployed. This will depend on the requirements of the customers. The most popular models are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Network as a Service (IaaS).

Saas is a service whereby users do no longer needs to install a software on their desktop before using it. They can simply use it online. PaaS is another more advanced service whereby developers can create new applications on an online platform. Currently, there are many limitations in this type of deployment model. IaaS allows users to operate and run a full-fledged computing network. The client has the ability to choose its preformed operation system, the applications they want to run, the amount of storage they require and the type of network connectivity. NaaS allows companies to rent network services such as custom routing, virtual private networks, intrusion detection and bandwidth on demand on a pay-per-use or subscription basis.

2 DEFINING SECURITY IN CLOUD COMPUTING

In cloud computing, when we wish to empower cloud-driven development and enhancement through security, we must have an acceptable confining on what is implied by security. “Security has been famously tricky as characterise in the general” [3]. Data security and privacy protection are the principle cause for user’s concern about the cloud technology. Data security has always been the main problem in IT.

Security of data is perhaps the most pressing issue in cloud computing systems. To increase availability and robustness, data is often stored in different places, on different devices and on different networks which escalates the issue of data security. Providing security in the cloud is more challenging than providing security in a desktop environment.

To increase the adoption of cloud computing by individuals and organisations, the security concerns of users should be amended first to make the cloud environment highly reliable. A trustworthy environment is the elementary necessity needed to gain the faith of users to embrace this technology [4].

The traditional objectives of computer security have been confidentiality, integrity and availability [5]. The National Institute of Standards and Technology (NIST) also includes accountability, assurance and resilience.

Confidentiality refers to the protection of private information. Data privacy is of equivalent importance as information leaves the boundaries of the organisation. Not only must critical and sensitive information be protected but also delicate transactional data belonging to the organisation should not be leaked. Confidentiality should also be supported by specialised encryption tools and legal assurances.

Integrity is the ability of a system to protect its data by preventing unauthorized modification to them during transmission, in storage or under unexpected breakdowns. Integrity can be achieved by making use of strong access control mechanism and through the use of checksum and parity bits. Integrity also implies that data must be kept up-to-date. This is how trust in the system can be built.

The resources must be available (availability) as decided in the terms of agreement. Cloud innovations through latest technologies can expand accessibility through the Internet. The services must usually be available 24 hours a day and 7 days a week. Timely availability of resources is critical to the well-being of organization.

Accountability is the set of actions that must be followed as part of the overall good governance practices in many organizations. Policies must be set in place to avoid or catch unlawful advents. In order to achieve accountability, it is important to log all transactions and to review them periodically. Other more complete authentication mechanisms can also be used to trace illegal or suspicious practices.

Assurance is a requirement for the cloud service provider to supply what had been asked for. And it is essential the services or infrastructure works as planned. This is not just a matter of programming or providing the right equipment but it is of high necessity that the requirements of the client are understood properly before implementing them in the cloud.

Resilience permits a system to adapt to any security threats and keep it a redundant as possible. With the latest cloud innovations, reinforcement of information as backup of data and systems, and identification of potential threats to act and neutralise the danger have become easier. Before moving their critical services to the cloud, it is important for organization to know about the resilience of the cloud infrastructure.

3 THE VULNERABILITIES IN CLOUD COMPUTING

In cloud computing, vulnerability is regarded as a noticeable factor of risk. The ISO/IEC 27005 [6] has set some guidelines for information security risk management. It has defined risk as, “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation”. The likelihood of the event is assessed as well as the consequences.

There are several vulnerabilities that should be taken into consideration when an organisation is planning to move towards cloud computing services [7]:

a. Session Hijacking occurs when an intruder is able to obtain the session id of a legitimate user. The intruder is then able to get access to all parts of the system that is accessible to that legitimate user. This treat can be tackle by using a Secure Socket Layer (SSL) connection. The SSL protocol encrypts the connection between a client and a server, thus making it more difficult for the attack to take place.

b. In a Virtual Machine Escape (VME), an attacker runs malicious code on virtual machines and tries to gain access to the host operating system and all other virtual machine running on that host

c. Insecure Cryptography occurs when a malicious user is successful in accessing confidential data, for example, usernames and passwords just because of a lack in security while storing the data. However, this can be prevented using strong encryption algorithms.

d. A Denial of service (DoS) attack is an attack in the cloud system where where a mal-intentioned user bombard, the server with many requests in a short period of time so that the server can no longer answer regular queries coming for legitimate users. If the attack continues for a long time, the server will no longer be able to deliver services as planned. Hence resources will be unavailable for legitimate users.

4 FROM HYPE TO FUTURE

According to a survey conducted by KPMG in 2010 on Cloud Computing [9], 76% of respondents considered security issues as the biggest risk in cloud computing.

In addition to that, the “legal issues” represent 51%, followed by “privacy issues” with 50% and the “compliance issues” with 50%.

These areas are considered to be the most concerned in an enterprise. The least concerned is immature technology with only 10%.

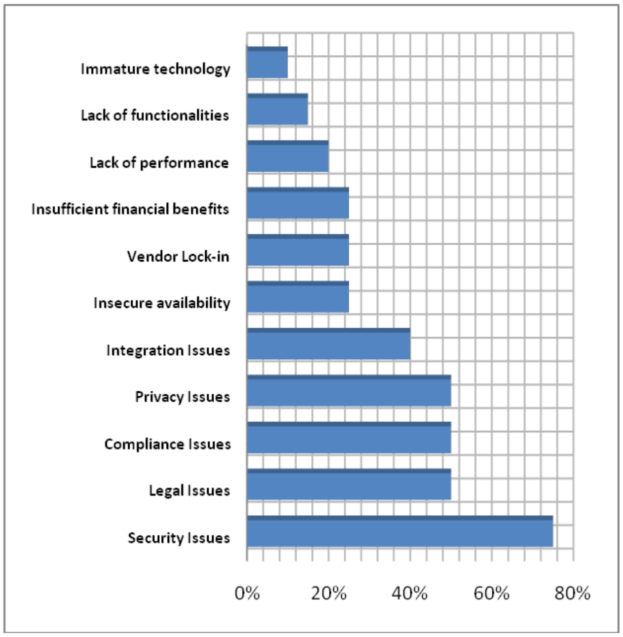

Figure 3. KPMG Survey
Source: KPMG the Netherlands, 2010 [8]

According to the same KPMG report, it was noted that only 63% of participants were focused on security issue. It was also understood that the primarily concern was the absence of transparency of Cloud Service Providers.

5 PROBLEM STATEMENT

The adoption of Cloud Computing is on the rise and becoming more and more popular as many enterprises are using cloud platforms to host their applications or data. However, a major hurdle for adoption of cloud services is the perceived lack of security.

Some of the problems in Cloud Security which have classified as the core cloud vulnerabilities are as follows:

a. Data protection and confidentiality: Data protection and confidentiality of information in cloud computing is the biggest security concern. By outsourcing a remote cloud based infrastructure and without knowing the companies infrastructure and the capacity to operate as a Cloud Service Provider, an organisation would basically gives away some or part of its private information and data, things that could be very critical and secret. Therefore it is the responsibility of the cloud vendors to ensure that critical data is well protected under their custody and also to oversee and secure them. This is where the Service Level agreement come into play (SLA), the SLA [9] is a trust bond between cloud service provider and consumer. It defines a maximum time for which the network resources or application may not be available for use by consumer. This value usually varies between 98%-99.99% for providers. This in turn sets expectations beforehand for the consumer so the consumer can have remediation methods in place to mitigate any non-availability issues.

b. Data breaches: A data breach [10] is coordinated by an unauthorised hacker geared towards electronic data stored on cloud. The four most causes of data breaches are malware, theft, insider attempt and attack by an unauthorised user. It is every (chief information officer) CIO's or Management worst nightmare that their organisation's sensitive and critical and sensitive office data are leaked to their competitors. To avoid data breaches we should prevent unauthorized parties to gain access to our sensitive data.

6 CLOUD COMPUTING IN MAURITIUS

As cloud computing is the new boom nowadays, Mauritius is not left behind. Below are the examples of three companies operating in Mauritius which uses the cloud technology. One of the cloud computing service provider company in Mauritius is Orange [11], Orange provide the cloud services that a consumer may need that is infrastructure as a service (Iaas), platform as a service(Paas), and software as a service(Saas). In addition to that that they provide with an end to end managed network connectivity with the right cloud support and the right secured environment. Emtel is the next one [12], Emtel e-Cloud, connects customers and cloud service providers in a simple, flexible, scalable and cost-effective way. Bhumisq Technologies, who is another Cloud Computing service provider and a big data enabler for economic sectors such as heathcare, education and agriculture [13]. In addition, Bhumisq technologies uses a pay as you go business model hence demonstrating the capabilities of the cloud technology.

7. RECOMMENDATIONS

Based on this research work, we would recommend our findings to clients and public in general who are willing to subscribe to cloud computing facility.

a) Confidentiality and Data Protection

It is highly recommended that when a company is subscribing to a cloud computing service, security of data should be the key element when a service level agreement is prepared. The contract requirements should consist of the CIA "confidentiality, integrity, availability" and without forgetting the audit of the services. There should be a Legal Clarifications approach when cloud privacy is concerned. There should be transparency and disclosure of privacy of what is offered between the cloud service providers and the clients.

b) Portability and Vendor Lock-in

It is very important that the clients know their risk exposure when cloud service providers have put the vendor lock-in situation or data portability. Data protection law and Abdication of liability in Cloud contract should well be set in the Service Level agreement (SLA). Companies and public in general who want to move to cloud must have a clear sense of cloud platform that they will be using and how these privacy protections are carried out across different domains or jurisdictions. The cloud vendor should ensure that there is a common operating procedure of applications and database used in case of termination of contract from both parties and the transition should be seamless and transparent for both parties.

8 CONCLUSION

In this paper, we have addressed some of the key challenges, benefits and vulnerabilities of cloud computing, especially on data protection and confidentiality of information and vendor lock-in and data portability. Cloud adoption still remain a challenge for many organisations as we have several significant threats which should not be discarded when moving to a cloud environment with critical and sensitive data. Many people do need feel comfortable when their data is on the cloud, located at the vendor's server. However, we do have some benefits like cost savings in terms of front-end cost, scalability, efficient use of IT resources, teleworking, increase of productivity and no licensing of software applications which encourages more and more business organisations to adopt IT solutions based on the cloud. In future, we intend to conduct a detailed survey of all Cloud Service Providers in Mauritius and the technologies that they are using.

REFERENCES

[1] Peter, M. and Grance, T., 2014. The NIST Definition of Cloud Computing. NIST Special Publication 800-145, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg.

[2] Leloglu, E., Ayav, T. and Aslan, B.G., 2013. A review of cloud deployment models for e-learning systems. In proceedings of Dependable Systems and Networks (DSN), 2013 43rd Annual IEEE/IFIP, 24-27 June 2013, pp. 1-2.

[3] Avizienis, A., Laprie J. C., Randell, B. and Landwehr C., 2004. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, pp. 11-33.

[4] Yunchuan S., Junsheng Z., Yongping X., and Guangyu Z., 2014. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, vol. 2014, pp. 1-9.

[5] Friedman, A. A. and West, D. M., 2010. Privacy and Security in Cloud Computing. Issues in Technology Innovation, No. 3, pp. 1-13.

[6] Bernd G., Tobias W., Elmar S., 2011. Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy, Vol.9, No. 2, pp. 50-57.

[7] Neela, K. L. and Kavitha, V., 2013. A Survey on Security Issues and Vulnerabilities on Cloud Computing. International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4, No. 7.

[8] Chung, M. and Hernans, J., 2010. From Hype to Future, KPMG's 2010 Cloud Computing Survey, Netherlands.

[9] Behl, A. and Behl, K., 2012. An analysis of cloud computing security issues, In proceedings of Information and Communication Technologies (WICT), World Congress on Information and Communication Technology, Trivandrum, pp. 109 - 114.

[10] Nandhakumar, C., Ranjithprabhu, K. and Raja, M., 2014. International Journal of Research in Computer Applications and Robotics, Vol. 2 No. 11, pp. 124-129.

[11] Orange Cloud Solutions, 2015. [ONLINE] Available at: http://www.orange.mu/pdf/cloud.pdf. [Accessed 15 May 2015].

[12] EMTEL Data Centre, 2015. [ONLINE] Available at:http://the-outsourcing.com/issue36/files/assets/downloads/page0017.pdf. [Accessed 18 May 2015].

[13] Technology | Bhumishq Group, 2015. Technology | Bhumishq Group. [ONLINE] Available at: http://www.bhumishq.com/business/. [Accessed 18 May 2015].

[14] Dialogic corporation, 2010, Introduction to Cloud Computing, [ONLINE] Available at: http://www.dialogic.com/~/media/products/docs/ Whitepapers/12023-cloud-computing-wp.pdf [Accessed 15 May 2015].