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 4, April 2016

Cloud Computing Security Issues and Challenges

Rameshwar Basedia[1], Makhan kumbhkar[2]

Assistant Professor, Dept. of Comp Science & Elex, Christian Eminent College, DAVV, Indore, MP , India [1]

Assistant Professor, Dept. of Comp Science & Elex, Christian Eminent College, DAVV, Indore, MP , India

ABSTRACT: Cloud Computing fashion is speedily increasing that has an technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such as Amazon IBM, Google's Application, Microsoft Azure etc., provide the users in developing applications in cloud environment and to access them from everywhere. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud based environment and solutions to overcome.

KEYWORDS: Cloud Computing, Scalability, Infrastructure, IT.

I. INTRODUCTION

Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over a network.

Advocates claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

II. RELATED WORKS

A. Data Security

Security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys.

Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervious to attacks based on capturing this data. However, companies have implemented systems with unpublished APIs, claiming that it improves security; unfortunately, this can be reversed engineered; also, using DHCP and FTP to perform tasks such as firmware upgrades has long been rendered as insecure. Nevertheless, products from Wyse are marketed with their thin client as one of the safest, by using those exact features.

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 4, April 2016

B . Cloud Computing Security Issues

[Gartner] identified seven issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows:

privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water

regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't

data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located

data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.

recovery - every provider should have a disaster recovery protocol to protect user data

. investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation

long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm

C. Security Benefits

There are definitely plenty of concerns regarding the inability to trust cloud computing due to its security issues. However, cloud computing comes with several benefits that address data security. The following sections looks into addressing concepts such as centralized data, incident response or logging.

Centralized Data refers to the approach of placing all eggs in one basket. It might be dangerous to think that if the cloud goes down, so does the service they provide, but at the same time, it is easier to monitor. Storing data in the cloud voids many issues related to losing laptops or flash drives, which has been the most common way of loosing data for large enterprises or government organizations. The laptop would only store a small cache to interface with the thin client, but the authentication is done through the network, in the cloud. In addition to this, when a laptop is known to be stolen, administrators can block its attempted access based on its identifier or MAC address. Moreover, it is easier and cheaper to store data encrypted in the cloud that to perform disk encryption on every piece of hardware or backup tape.

Incident Response refers to the ability to procure a resource such as a database server or supercomputing power or use a testing environment whenever needed. This bypasses the supplemental red tape associated with traditional requesting of resources within the corporate world. Also, if a server is down for re-imaging or disk clean-up, the client may easily create similar instances of their environment on other machines, improving the acquisition time. From a security standpoint, cloud providers already provide algorithms for generating hashes or checksums whenever a file is stored in the cloud, which bypasses the local/client need for encrypting. This does not imply that clients should not encrypt the data before sending it, but merely that the service is already in place for them.

III. CLOUD SECURITY CONTROLS

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management.[3] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[3]

A. Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

B. Preventive controls

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 4, April 2016

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

C . Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[3] System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

D. Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

IV. DIMENSIONS OF CLOUD SECURITY

It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. Cloud security concerns can be grouped in various ways; Gartner named seven[9] while the Cloud Security Alliance identified fourteen areas of concern.[4][5] Cloud Application Security Brokers (CASB) are used to add additional security to cloud services.[6]

V. SECURITY AND PRIVACY

A.Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

B. Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive

C. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

VI. CONCLUSION

Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and
challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper
key security considerations and challenges which are currently faced in the Cloud computing are
highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure,
virtual and economically viable IT solution in the future.

REFERENCES

1. Hassan, Qusay (2011). "Demystifying Cloud Computing" (PDF). The Journal of Defense Software Engineering(CrossTalk) 2011 (Jan/Feb): 16–21. Retrieved 11 December 2014.
2. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
3. Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.
4. "Cloud Security Front and Center". Forrester Research. 2009-11-18. Retrieved 2010-01-25.

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 4, April 2016

5. "Cloud Access Security Brokers (CASBs) - Gartner IT Glossary". Retrieved 2015-10-01.
6. "Identity Management in the Cloud". Information Week. 2013-10-25. Retrieved 2013-06-05.
7. Ibikunle Ayoleke ,"Cloud Computing Security Issues and Challenges".
8. Makhan Kumbhkar et al , ―Performance Improvement of Software as a Service and Platform as a Service in Cloud Computing Solution‖, International Journal of Scientific Research in Computer Science and Engineering, ISSN: 2320 Vol- 1 Issue –VI .
9. Makhan Kumbhkar et al ,‖ Analysis of Cloud Computing Security Issues in Soft ware as a Service ― , International Journal of Scientific Research in Computer Science and Engineering, ISSN: 2320-7639 , Volume-2, Issue-3.
10. Makhan Kumbhkar, ―Security in Cloud Environment‖ , International Journal of Scientific Research in Computer Science and Engineering, SSN: 2320-7639, Volume-2, Issue-3.
11. Yashwant Singh Chouhan et al,‖ Analysis of Cloud Computing in Higher Education‖, Volume 5, Issue 6, June 2015 ISSN: 2277 128X.
12. http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/.