International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

Cloud Computing Security & Its Challenges

Anisha Tandon[1], Mamta Madan[2]
[1]Research Scholar, JIMS, Vasant Kunj, Delhi
[2]Professor, Vivekananda School of Information Technology, Vivekananda Institute of Professional Studies, Delhi
[1]84.anisha@gmail.com, [2]mam_madan@yahoo.com

Abstract: Cloud computing is the latest technology that changes the way people are interacting with the web. Cloud computing is the style of computing where applications and services are provided over the Internet. Such services are offered all over the world from data centers which are collectively known as the "cloud". The paper advocates a proactive and holistic cloud-cyber security prevention typology to prevent e-crime, with guidance of what features to look for when choosing an appropriate cloud service provider (CSP).

Keywords: Cloud computing, CSP, CSA

NOMENCLATURE

1. AV- Antivirus
2. GHDB -Google Hack Database
3. RIA -Rich Internet Application
4. SOAP: Simple Object Access protocol
5. REST-Representational state transfer

I. INTRODUCTION

Cloud Computing is a recent technology that offers internet services to the user. Examples of cloud computing services are Gmail, Yahoo Mail or Hotmail etc. For this you need an internet connection and can start sending emails.

Cloud computing[1] is the style of computing where applications and services are provided over the Internet. Such services are offered all over the world from data centers which are collectively known as the "cloud". Cloud computing includes online applications, i.e. offered through Microsoft Online Services.

Figure 1. The Cloud

Most organizations are aware of what cloud computing has to offer. It is an IT software and hardware resource that is capable of offering a service on an "as-needed basis" and paid for as it is used. Organizations will quickly see the advantages of these systems which range from expense savings and lower capital expenditure as well as to rapid use of a service which has great elasticity.

II. CLOUD COMPUTING ATTACKS

Listed below are some of the security breach that were encountered by the organizations who have been victim of cyber attack via cloud deployment [2]:

- inaccurate billing of application usage;
- insider theft;
- session hijacking;
- application programming interfaces (API) session corruption;
- loss of encryption keys;
- man in the middle attack; and
- Back up lost.

Further breaking down the comments resulted in the following threats identified by the survey group:

- unsecured access to admin interface;
- poor encrypted communication channel for data in transit;
- Lack of information on encrypted standards/format for data stored at CSP;
- Lack of standard for auditing in cloud;
- Insider threat, appropriate vetting of CSP employees;
- Lack of forensic standards for remote data retrieval;
- Lack of cloud standards concerning data sanitization;

III. SURVEY

The survey highlighted that no single definition of cloud computing stood out as being the obvious choice, which

shows the pattern of the industry where various definition of the term exists. There needs to be agreement among the top cloud bodies such as the Cloud Security Alliance (CSA), European Network and Information Security Agency (ENISA) and National Institute of Standards and Technology (NIST) so that the basic cloud principles can be established and some global unification of the powers can be recognized. The potential damage that can be created by malicious or disgruntled employees is a major concern for cloud customers. This is mainly as a result of a lack of transparency by Cloud Service Provider (CSP) and the merging of IT services and cloud customers into a single manageable entity.

CSPs [3] offer very little insight into their human resource practices and particularly the minimum standards that an employee in such a position of power must hold in order to gain employment. This is very important as employees of CSPs may have a level of access to a customer's confidential data that procedure in relation to security breaches.

CSPs have a major role to play in relation to data protection policies. Many of respondents felt that CSPs should align themselves with international standards of data protection so that their clients will have peace of mind that they are adhering to well established standards. The survey results confirm that security is by far the biggest concern of respondents when moving to the cloud, followed by governance issues and a lack of control over service availability. Companies who have been victim of the cloud attack identified data loss leakage as the biggest threat. It was felt that security would become one of the primary differentiators among CSPs. From a security perspective the survey highlighted a major concern about respondent ignorance on decryption keys controlled by majority of the cloud providers. The results from the survey proved to be very informative as it provided a solid foundation of cloud related practices and current key issues. The opinions of IT professionals were invaluable as it demonstrated how diverse the opinions were on the topic of cloud computing.

The Cloud Security Alliance (CSA) has advanced 14 IT operation areas as "critical areas of focus" for organizations deploying cloud computing resources. We asked respondents in both the cloud user study and cloud provider studies to select the IT operation from the 14 areas they believe are critical areas of focus for the security of their operations. The five top-rated critical IT operations according to both cloud users and cloud providers are shown in Bar Chart. As can be seen, cloud providers and cloud users have different priorities for their security practices.

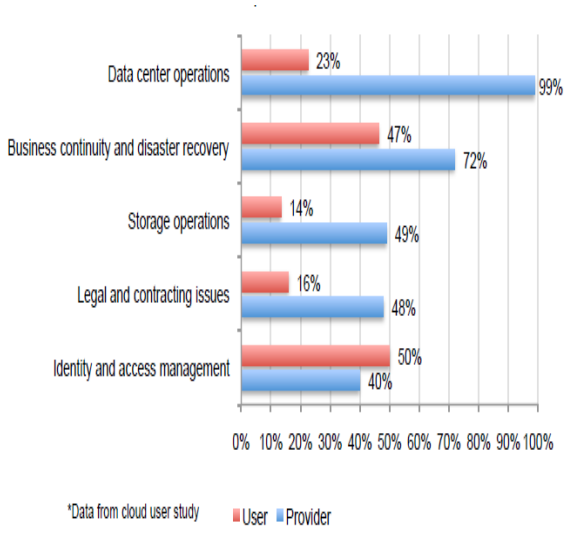

Figure 2. Bar Chart: Critical areas of security for cloud providers, US & Europe results combined [3]

Specifically, nearly all cloud compared to only 23 percent of cloud users. In the cloud users study, we learned that users of cloud computing are not any more diligent in protecting cloud resources. Only 36 percent of US and 57 percent of European cloud computing users strongly agree or agree that their organization is vigilant in conducting audits or assessments of cloud computing providers before deployment.

IV. PROBLEM STATEMENT

- What is the assurance given to the cloud subscriber b the vendor or CSP in terms of privacy and security?
- How can the CSP ensure they provide a secure infrastructure with high data integrity and least downtime[4]?
- Can we leverage on existing open source tools to ensure security in the cloud?

V. CURRENT OPTIONS

There are many industry-standard tools which work very well for vulnerability analysis, both in legacy three-tier and cloud architecture. The only limitation on these tools is that they depend on a hack database such as GHDB to provide the information about the vulns, which becomes available only if someone has published them.

Antivirus and Firewall: It is really easy for any malicious software to stop an AV and shutdown the firewall with

just a three-line script on the intended victim. Hence the obvious might not be the savior[5].

VI. Some Common Mistakes

- Too many open ports exist in the CSP's infrastructure
- The platform patches that are applied may have regression effects.
- The application patches applied might have cascading effects
- The existing patches to the RIA on cloud might be cached on client machines, so might not be the latest ones.
- Exposing too many web services which can lead to XML encryption/ decryption related attacks
- 400% increase in ARM related malware -which only shows how easy it is to hack a wireless device

VII. Developing a Holistic Cyber Cloud Strategy

Keeping the above survey in mind a holistic strategy to assess the following areas should be implemented to select an appropriate CSP [6] that is:

Communication route: The communication route between client administrator and cloud host usually occur on an open channel mostly with clear data text transmitted over the internet; there is a need to set up secure channel by organizations to prevent man in the middle attack. It is therefore essential for organizations to assess whether CSP offer encrypted admin access to cloud operating systems and applications. The data encryption level (standard) should be assessed before selecting a particular cloud.

Effective security controls: CSP must outline how data would be stored and retained; the existing security controls should be highlighted to ensure data integrity and confidentiality. How CSP is storing and segregating its various customers' data is important – during the event of a security breach how a cloud provider handles customers enquiries are some of the important areas to be

looked into. However, over extension of data transparency can create issue as it may aid malefactor and insider theft. It is recommended that reporting channel needs to be agreed and tested before the service commence.

Audit: The audit facilities needs to be thoroughly assessed as in case of a security breach organization needs to ensure that data available by authorities or IT

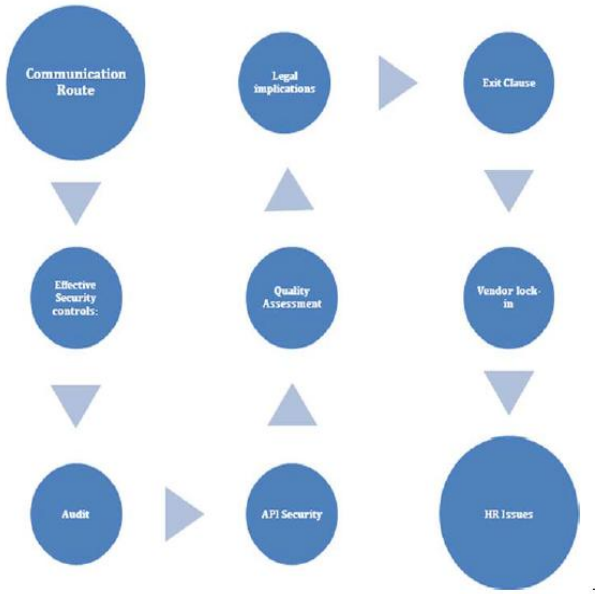

Figure 7 Holistic Cyber Cloud Strategy [6]

Auditors is easily accessible through the cloud; the issue of data storage in various locations by a CSP should be examined in details as organization do not want to end into situation where providers declines clients auditing requests in case of a breach.

Quality assessment: Selection of a particular CSP should not be based solely on cloud provider own threat assessment. It is recommended to assess CSP quality prior to selection; third part validation n of the controls and assessment of the data security would be increasingly vital. Whether communication channels are periodically tested is an important factor for selection[7].

API security: Confidence in cloud services is reliant on the security of the API that are responsible for safeguarding against the unintentional or premeditated attempts to thwart policy. An API is a specific set of rules that enables software to interact with the software environment that is native to the cloud. Third parties often create add-ons to these interfaces to offer additional functionality which increases organizational risk as they often have to resign certain credentials to them for the APIs to work correctly. This threat can alleviated by ensuring the strongest encryption standards, authentication methods and access controls are implemented.

Legal implications: Discussion should be carried out with CSP about legal obligation in terms of storing data offshore in other countries. While choosing a CSP the location of the data centers should be kept in mind as the

European Union privacy and data regulation prohibits transmission and storage of sensitive personal data outside the EU. Who is liable for the data breach and service outages during an incident involving a criminal activity at one of the data centers of CSP based in countries (for example, Asia Pacific) where data protection laws are not that stringent are some of the important issues to think about before selecting a CSP. While choosing a CSP the organizations should make an effort to enquire whether the provider has attained SAS 70 or ISO 27001 certifications.

Exit clause: One of the common mistakes the organizations makes are to ignore the "exit clause" when evaluating the SLAs. In the event of failure of the cloud,

steps need to be highlighted at how to regain ownership and control of the data. This is a complicated process in terms of retrieved data compatibility and processing of capability of the client[8].

Vendor lock-in: It is one of the major concerns identified – there are no standard APIs and each CSP is comfortable with its own customized interface; as a result data import, and data move becomes more difficult and the businesses are in a lock-in situation. In case of CSP closure (economic condition the main issue) business clients can face serious repercussions for data migration. Current efforts to develop a consortium of standard APIs such as SOAP or REST to manage cloud services are underway by various stakeholders (cloud forum, cloud alliance, etc.).

HR issues: Migration to the cloud will bring also bring new HR issues of appropriate corporate training; the processing of business applications remotely will bring new challenges enforcing corporate standards and procedures.

VIII. CONCLUSION

Cloud Computing paradigm provides a new approach as a solution for old problems. It also offers benefits to industries, enterprises, as well as universities. Many huge IT companies develop new cloud-based applications, and construct new cloud infrastructure. Most of the research in literature focused on benefits, opportunities, advantages, disadvantages, risks and configuration of Cloud computing for enterprises.

However, the public literature that discusses the research issues in cloud computing are still inadequate. We have discussed the new research challenges that are raised by cloud computing. The main conclusion gained from this research is that security concerns are well founded in a cloud environment due to increasing organized cyber crime activities. Any move to cloud will bring new challenges in terms of security of the data and third party applications. However, many organizations are in a better security position by being on the cloud than on their internal networks.

IX. REFERENCES

[1] S. Singh, "Different Cloud Com- 4. Putting Standards a Huge Challenge," The Economic Times, 4 June 2009;

[2] Klems, M, Lenk, A, Nimis, J, Sandholm T and Tai S, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape", IEEE Xplore, pp 23-31, viewed 21 (2009).

[3] Security of Cloud Computing Providers Study, CA Technologies

[4] Mladen A. Vouk, ―"Cloud Computing – Issues, Research and Implementations", Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008, Cavtat, Croatia

[5] Kiran Karnad, Saravanan Nagenthram, "Cloud Security" , The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)

[6] Azeem Aleem, Let me in the cloud: analysis of the benefit and risk assessment of cloud platform, Emerald Group Publishing Limited, Journal of Financial Crime, Vol. 20 Issue: 1, pp.6 - 24

[7] Sharon Q. Yang, Move into the Cloud, shall we, Library Hi Tech News, Vol. 29 Issue: 1, pp.4 - 7

[8] Jon Brodkin, ―Gartner: Seven cloud-computing security risks‖, InfoWord

[9]. Boss G, Malladi P, Quan D, Legregni L, Hall H. "Cloud Computing" IBM White Paper(2007)