Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

An Analysis of Threats and Security Issues in the World of Cloud Computing

Pandya Dhavalchandra

Computer Engineering, Atmiya Institute of Science and Technology, Rajkot, Gujarat, India

Abstract – *The world has changed its way of communication from centralized to distributed and now towards Cloud computing. Cloud computing allows users to access devices distributed in the network and reduces the management efforts. Cloud computing relies on sharing of on-demand resources like network, application, services, storage and servers. So this way, the resources are used without investing money either in infrastructure or in purchasing expensive licensed new software. The rapid transition from mainframe computers through grid computing to the cloud computing has increased our concern on security. Security of the data is major issue in Cloud Computing because the cloud providers can access data of users at any time. This paper provides a perspective about the Threats and Security issues occurring in the Cloud Computing.*

Keywords: *Cloud Computing, Threats, Security, Risks, Trust, Distributed Computing*

I. INTRODUCTION

Cloud Computing is in high demand nowadays. It popularity is increasing day by day. Cloud Computing provides dynamic scalable resources as a service to provide economic benefits. The cloud computing can be defined in three different layers.

The bottom layer is the Infrastructure – as – a – Service (IaaS) which provides basic components like CPU, memory and storage. Amazon's EC2 (Elastic Compute Cloud) is an example of IaaS. On the top of IaaS is the Platform – as – a Service (PaaS) which provides platform specific service. Google App Engine is an example of PaaS. The top – most layer is the Software – as – a – Service (SaaS) which provides applications that can be directly accessed by the users. Access to IaaS is provided by Web Services and access to SaaS is provided by Web Browser.

Cloud computing includes service – oriented architecture (SOA) and virtual applications of hardware and software [1]. Cloud security issues focus mainly on data confidentiality, data safety and data privacy and discuss mostly organizational means to overcome these issues [2].

International Data Corporation (IDC) conducted a survey of 263 IT executives and their line-of business colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing [3].

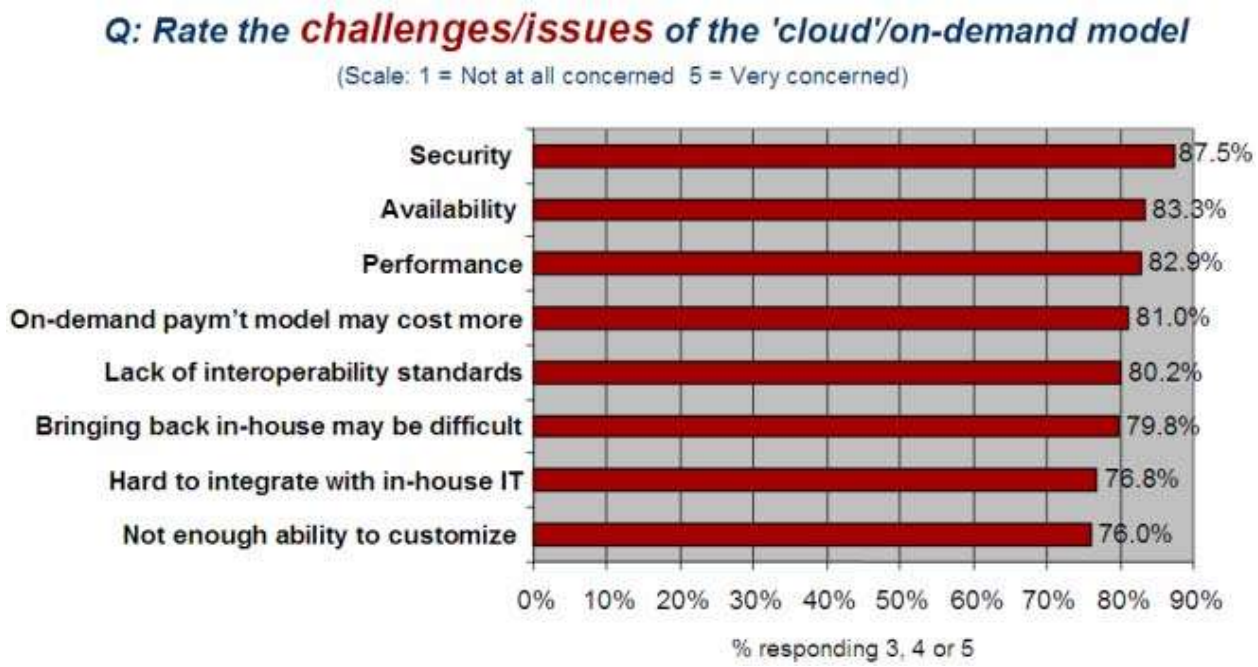

Figure 1. Results of IDC ranking security challenges (3Q2009, n=263)

A. Cloud Computing Issues

Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. The various cloud computing issues are:

a) **Security:** Security issue is one of the major issue of cloud computing because data will be stored in the computers that are distributed over network.

b) **Privacy:** Data is scattered on various computers and due to this the user may leak hidden information while accessing computing services.

c) **Reliability:** The Cloud server experiences downtimes and uptimes, but the users have a higher dependency on Cloud Service Providers (CSPs).

d) **Legal Issues:** Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" [5].

e) **Open Standard:** There are a number of open standards under development, including the OGF's Open Cloud Computing Interface for exposing APIs.

f) **Compliance:** Managing Compliance and Security for Cloud Computing, provides insight on how a top-down view of all IT resources within a cloud-based location can deliver a stronger management and enforcement of compliance policies.

g) **Freedom:** Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

h) **Long – term Viability:** The data into the cloud must never become invalid even when cloud provider shuts down.

i) **Solution:** Data must be encrypted before storing the data to ensure security.

B. Security Issues

The security issues do not suffer a lot when using cloud model, because security issues can be outsourced by the experts. The various security issues are:

a) **Access:** Access risk may be increased in cloud computing while accessing confidential information. Access risk can be firstly due to the government surveillance and secondly due to the unauthorized access.

b) **Control over Data Lifecycle:** This issue deals with the control of lifecycle to the customer. More specific risk is the use of cloud service model.

c) **Availability and Backup:** When data is on remote location, backup is critical as it would be done without customer's informed approval.

d) **Lack of Standardization:** There is no standardized communication between and within cloud providers and no standardized data export format which makes it difficult to leave a cloud provider. Establishment of security framework is also difficult if there is a lack of standards.

e) **Multi – Tenancy:** Customers are the actual users of multi – tenant applications. Data security is the responsibility of the CSPs (Cloud Service Provider) as they develop the Cloud Service Model.

f) **Audit:** Transactions involving data residing in the cloud needs to be properly made and recorded, to ensure integrity of data and the data owner needs to trust the background that no untraceable action has occurred.

g) **XML Signature:** Attacks on Protocols using XML Signature for authentication or integrity can be easily attacked. The XML Signature Element Wrapping is applied to Web Services for providing protection.

C. Security identification of threats

Identifying the unique threats and challenges needs to be addressed by implementing measures. The infrastructure proposes unique security challenges such as:

a) **Confidentiality and Privacy:** Data Confidentiality allows authorized systems to access the protected data. As there are number of systems connected in the cloud increases, the threat of data compromise increases which in turn increases the access point making data accessible to number of systems.

Multi – tenancy refers to resource sharing at network level, host level, and application level. Although the resources are shared, the data recollected may lead to disclosure of private data and user may claim huge amount of storage space and then forage the data.

Privacy is desired for every organization and they need to follow country's legal framework to ensure privacy and confidentiality protection.

b) **Integrity:** Integrity ensures that the data must be modified by the authorized system. Data integrity protects data from unauthorized fabrication. Authentication is also provided to determine the level of access to the user. Software integrity is also provided to protect software from unauthorized modifications.

c) **Availability:** Availability ensures that the system is available whenever usage demand is high for the authorized users. Upon demand of users, hardware, software and data must be available to the authorized user.

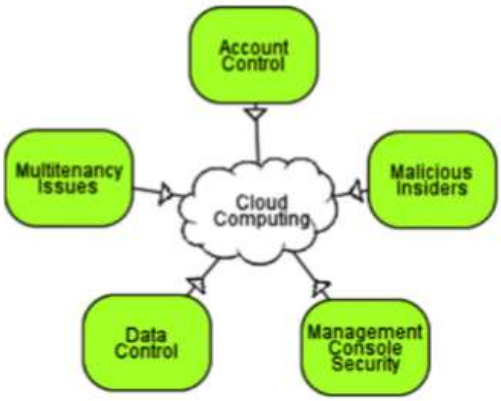

Figure 2. Categorization of Threats [6]

II. LITERATURE REVIEW

The cloud name comes from the cloud symbol used to represent the internet. Cloud computing shares its resources among a cloud of service consumers, partners, and vendors. In 1999, Salesforce.com introduced one of the first practical cloud computing implementations and established the concept of delivering enterprise services through a Web site. In 2002, Amazon Web Services launched a suite of cloud – based services, including storage, computation, and even human intelligence through the Amazon Mechanical Turk [1].

The US government projects between 2010 and 2015, on cloud computing was almost approximately a 40-percent compound annual growth rate and passed $7 billion by 2015. Centaur partners also predict that SaaS Revenue will grow from US$13.5 in 2011 to $32.8B in 2016 [7]. Today, the latest example of cloud computing is Web 2.0; Browser-based enterprise service applications are offered by Google, Yahoo, Microsoft and others.

III. CONCLUSION

Cloud computing has the ability to address vulnerabilities recognized in traditional ones. In this paper different cloud computing issues, security issues and the issues in the threats have been broadly classified. By solving such issues the application developed on cloud computing model will be completed and without any vulnerabilities. While developing any application, these issues must be taken into consideration to develop fully fledged error free application.

REFERENCES

[1] John Harauz, Lori M. Kaufman, Bruce Potter "Data Security in the World of Cloud Computing", Co – published by the IEEE Computer and Reliability Societies, 1540-7993/09/$26.00 © 2009 IEEE,JULY/AUGUST 2009.

[2] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing,", Gartner Report, 2009. [Online]. Available: http://www.gartner.com/DisplayDocument? id=685308

[3] Krešimir Popović, Željko Hocenski "Cloud computing security issues and challenges ", MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[4] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit "Cloud Security Issues", 2009 IEEE International Conference on Services Computing.

[5] C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, [2005] "Live migration of virtual machines" In Proc. Of NSDI'05, pages 273-286, Berkeley CA, USA, 2005. USENIX Association

[6] Dimitrios Zissis, Dimitrios Lekkas " Addressing Cloud Computing Security Issues", Future Generation Computer Systems 28 (2012) 583 – 592, Elsevier publication.

[7] "Round of Cloud Computing Forecasts And Market Estimates, 2014" Forbes retrieved on 22-11-2015.