Security Concerns In Cloud Computing

Neha Khandelwal
M.Tech Student, KITE, Jaipur

Chetan Kumar
Asst. Prof, KITE, Jaipur

Abstract - Cloud computing is the emerging technology that is used worldwide for storage as well as distributed data processing. In the cloud technology client's data is stored and on the Cloud service providers' domain. Data and Services are appeared on the client devices (PCs, notebooks, Smartphone, etc.) temporarily as they needed by client. The concept of this new technology i.e. cloud computing is adopted by many clients, but is receiving criticism from many people, who observe in this cloud technology the loss of client control on computing processes. In such distributed computing scenario many issues arises between the client and the cloud service provider. This dissertation thesis mainly aims to a survey that highlights the fundamental security issues that existing in present cloud computing environments.

Keywords: - Cloud Computing, Distributed data processing, System Controls Mechanism.

I. INTRODUCTION

This part of the paper mainly highlights the basic security concern in the cloud computing. In the cloud computing infrastructure, the whole data of client reside on a set of network resources, which enables the data which is, resides in data centers to be accessed by client through the virtual machines. These data centers can lie in anywhere in the world and the user will not be able to reach and control the data, So that there are a lot of multifarious security concerns and privacy challenges that should be well understood and must be take care of. In addition, anyone can never refuse the risk of server's breakdown that is happening quite frequently in the present times. At present there are many concern and issues that always needs to be treated with respect for overcome to security and privacy issues in a cloud computing environment. This paper contains extensive-survey of various research papers to analyze and elaborate the number of unresolved issues which is threatening the client in order to adoption of cloud computing.

1.1 Challenges in Cloud Computing

According to a survey which is conduct by "The National Institute of Standards and Technology" (NIST) [1] the main challenges which anticipated the adoption of cloud computing environment is security and it rated with a 74.6% , as shown in given figure below, security is higher than all other issues :

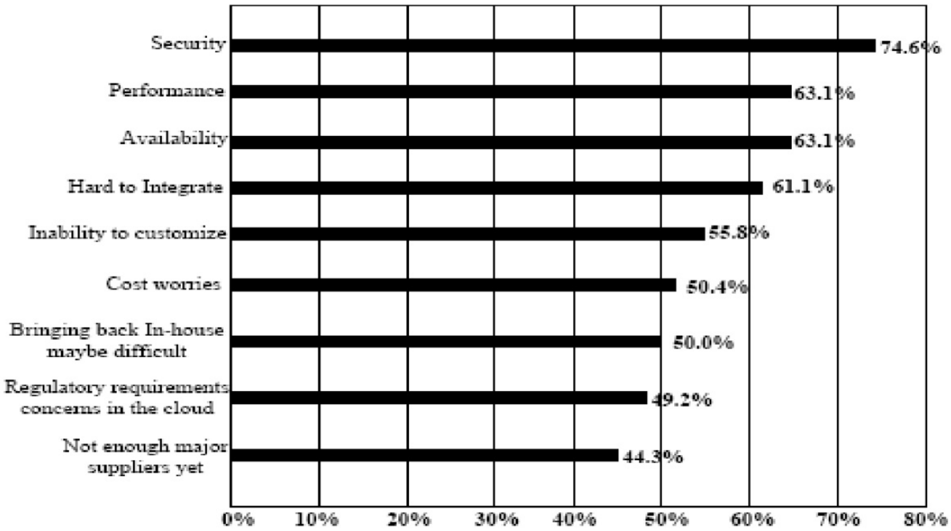

Fig.1: Challenges that expected from adoption to cloud computing (NIST)

The above figure clearly describes that almost all organizations are worried about the implementation of security mechanism in cloud computing infrastructure.

Gartner [2], another one of leading information technology advisory and research company that conducted a survey-investigation regarding the cloud information security issues and concerns that must be well thought-out when ever dealing with Cloud computing paradigm. The following list has some major security issues:

1.1.1 Privileged access

This security issue always considers about specialization or privilege for accessing the client's data and "Who will decide about the hiring as well as management of administrator?"

1.1.2 Regulatory compliance

In this issue organization should consider that "Is the Cloud Service Provider (CSP) eager to go through by an external audits or security certifications?"

1.1.3 Data location

In this issue client should consider about the control or any decision on location of data because the data centers are operated by the cloud service provider.

1.1.4 Data segregation

This means, "Is encryption techniques available for data at all stages, and were those encryption techniques had designed as well as tested by any experienced professionals?"

1.1.5 Investigative Support

It issues means "Does the service provider have the effective ability for investigation of any illegal or inappropriate activity?"

1.1.6 Data availability

In this issue the client of CSP should be aware about "Can the cloud provider move all their users data into a different environment should the present environment turns into unavailable and compromised?"

II. BARRIERS TO CLOUD COMPUTING

Cloud computing is a hot technology in present time, many research is going on this technology to improve it .In spite of this research, there are some aspects in the wake of the fact that most of organizations and client of cloud are yet not so confident to moving into this new technical paradigm that is known as cloud. There are certain loopholes are there in its fundamental architecture that has made this cloud computing technology vulnerable to many security as well as privacy issues. This section describes some of the issues that are the limitation of the transformational concept:

2.1 Security and Privacy

The fundamental aspect which defines the success of a new emerging computing technology always resides on the fact that how much secure it is [3,4]. It is always considered by the client of cloud that whether the client's data which resides over the cloud is secure up to that level so as it can avoid each security threat. In the cloud computing servers may reside at anywhere in this world and if there are any sort of internet breakdown happens there it can refuse client to access the data which reside in the cloud.

Basically this is also an important part of cloud infrastructure architecture, that client's data will be distributed on these individual servers in spite of where the base or main repository of data is eventually stored. In many cases their security infrastructure has been attacked and the overall system had been shut down for hours.

In public-cloud computing environment, there are multiple security issues. A public cloud works as a host of virtual machines, supporting middleware, virtual machine monitors [5] etc. The security in cloud always depends on the overall activities of these objects and on the basic interactions between each of them. Because the public cloud enables a shared multi-tenant environment, so that as the number of client is increased, the security risks will get more and more diverse. It is always essential to recognize the attack surfaces which is used to security attacks as well as find out the mechanisms that ensuring the successful server-side and client-side protection [6].

2.2 Latency, Performance and Reliability

Latency [7] is also a serious issue in cloud computing infrastructure with respect to flow of data around different clouds infrastructure. Encryption and decryption for data is other factor that adds to the latency when data moves around untrustworthy and public networks, packet loss and congestion. When the flow of network traffic is high congestion directly adds to the latency and there may be many requests that should to be executed at that time. Next one is windowing, which is a message passing technology in which the receiver client sends a message to sender client that receiver has received the sent packet that is sent earlier and hence it adds to the overall network latency.

In addition, the overall performance of the system is one of the factors that should be considered. Sometimes the CSP execute short of capability by allowing the access to too many VMs and reaching higher throughput on their internet links because of high demand arising from the customer section. This harms the system performance and it adds to the latency of the infrastructure.

2.3 Portability and Interoperability

Sometimes organizations or clients may wants to change the cloud service providers and there may be cases when organization can’t shift their application and data if they find some another cloud computing platform that they like much better than the platform they are using currently. In addition, some time organizations uses different cloud service platforms for different types of applications based on the requirements as well as the services provided by the CSPs. In many cases, for completing a particular task, different cloud service platforms may be used for a particular data and application or different cloud service platforms wants to interact with any other cloud service platform. Hence the internal organizational infrastructure is always needed to preserve a balance to hold the interoperability between different cloud service platforms [8].

Controlling the outsourced services is a big challenge in hybrid public cloud as well as in the private cloud environment, there is always a risk that these services may go out of control. All data must be encrypted for appropriate security, and management of keys becomes a very difficult task in such infrastructure. The client has in fact no ideas of where his information is store. The fundamental issue of the inter-security managing becomes an important task in such type cases. A security management model for cloud computing is discussed in which is serve as a standard architectural model for designing a cloud security management tool. This model basically uses four types of interoperating layers that are used to managing the proper cloud security [9].

Hence we can see that though the cloud computing paradigm exists all over the place because of multi-fold aspects and features provided by it, but still here are many issues that should be needed to be solved in order to get better performance.

2.4 Data-Breach through Fiber Optic Networks

It has been observes that the security threat for the data in transit mode has been increased in the last few years. The security of data when it leaving from a data centre to another data centre is a foremost concern because it has been breached rather a number of times in the present times.

This data transmission is basically done over the networks of fiber-optic cables and these are considered as a safe mode of data-transfer till now, until recently when an illegal device that used for eavesdropping in Telco Verizon’s optical network which is placed at a company of mutual fund was exposed by US Security forces [10]. There are certain devices that are used to tap the flow of data without any disturbing it. Hence it becomes an important factor that guarantees security of data over the networks.

2.5 Data Storage over IP Networks

At present time the data storage at online is becoming very popular and it is observed that the majority of organizational storage will be online in the near future, because it allows organizations to preserve huge amount of data without setting up required infrastructure. Even though there are certain advantages of data storage at online, there are some serious security threats also present there that could be source of data unavailability or data leakage at crucial time. There are many issues that are observed frequently in the dynamic data situation that keep flowing in the cloud infrastructure with compare to static data.

Depending upon the various levels of storage and operation provided, this type of networked devices can be categorized into NAS (network-attached-storage) and SAN (Storage-area-network) and because such type of storage networks basically resides on servers, there are various types of risk and threats attached to them.

III. CONCLUSION & FUTURE WORK

High availability, high fault tolerance and high efficiency accesses to Internet based cloud data centers where failures are normal rather than exceptional are significant issues are often considered more valuable than high performance. This paper presents a security module in cloud computing and introduces agent to the data protection.

There are still some studies to be done in the future, for instance, further reducing the user waiting time, speeding up data access, and further increasing data availability. It is also planned to improve agents ability to satisfy the special demands of cloud computing. More verification should be done.

REFERENCES

[1] Brodkin, J. (2008, July 02). “Gartner: Seven cloud computing security risks”, see InfoWorld: http://www.infoworld.com/d/security-central/gartner-seven-cloud- computing-security-risks-853.

[2] Information technology - Open Systems Interconnection - Upper layers security model, International standard ISO/IEC 107 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18835

[3] S. Pearson, “Taking account of privacy when designing cloud computing services,” CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE ISBN: 978-1-4244-3713-9. May 2009.

[4] Julisch, K., & Hall, M., “Security and control in the cloud,” Information Security Journal: A Global Perspective, vol. 19, no. 6, pp.

299-309, 2010.

[5] L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616.DOI: 10.1109/ICWS.2009.144. July 2009.

[6] Wayne Jansen, Timothy Grance, “NIST Guidelines on Security and Privacy in Public Cloud Computing,” Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft- SP-800-144_cloud-computing.pdf.

[7] S. Pearson, “Taking account of privacy when designing cloud computing services,” CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE ISBN: 978-1-4244-3713-9. May 2009.

[8] Julisch, K., & Hall, M., “Security and control in the cloud,” Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.

[9] L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616.DOI: 10.1109/ICWS.2009.144. July 2009.

[10] Wayne Jansen, Timothy Grance, “NIST Guidelines on Security and Privacy in Public Cloud Computing,” Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft- SP-800-144_cloud-computing.pdf.