CLOUD SECURITY BENEFITS

[1] MR.K.Gowtham,

[1] II M.COM CA,
[1] PG and Research Department of Commerce CA,
[1] Hindusthan College of Arts and Science

Abstract: Cloud computing refers to high scalable computing applications, storages and platforms as a service to companies, individuals and governments. Therefore, SMB (Small and Medium Business) organizations are adapting cloud computing services gradually to save cost and to increase efficiency in their business environment. While cloud service benefits and robustness are comprehensible, but now more concern about security in cloud computing “How much secure is cloud computing environment”. Noted that security is one of the main barrier for continuing growth of cloud computing. For some major security risks and issues enterprises and individuals are unwilling to deploy their data and applications in cloud environment. In this paper, the main objective is to identified major security risks and issues those are need to think about during deployment and development of services in cloud and the way how to mitigate those security risks and issues. However, it is significant to know that, cloud computing is not insecure primarily; it just needs to be managed and accessed securely.

Index Terms- Cloud computing, security**.**

I. Introduction

Information Technology industries are driving technology to a new arena from time to time. The Internet is one of the most popular technology now-a-days by the elegance of information technology. Now it is on the edge of revolution, where resources are globally interconnected. Hence, resources can be easily shared and managed from anywhere and anytime. Cloud computing is the main element of this standard, that provides a large storage area where resources are available from everywhere to everyone as a service rather than as a product. Cloud computing comes focus only when think about what information technology always needs: a way to increase the capabilities of a system on fly without investing any new infrastructure, training a new personnel and licensing of any new software the services provide over the Internet in real time, in which extends basic information technology capabilities into robust area. The small medium business companies are realizing that simply by tapping into cloud environment they can gain fast access to best business applications facilities and dramatically boost their resource infrastructure at very minimum cost. The main focus of this study is to describe various security issues due to cloud service delivery models and provides some recommendation to mitigate cloud computing risks as for development guidelines and standards for secure cloud computing environment.

II SECURITY ISSUES IN CLOUD SERVICES

Cloud computing service models are software as a service, platform as a service and infrastructure as a service, which provides software as a service, platform as a services and infrastructure as a service to end users or customers. These three service models are built on top of each other, as shown in as a result their capabilities are inherited as well as security issues and risks. So, service providers are not be able to take care only part of it, rather than as a whole to provide secure environment. In this part of this paper clearly indicate major security issues based on these service models and what needs to be addressed by implementing appropriate countermeasures.

2. 1 .SECURITY ISSUES IN SOFTWARE AS A SERVICE:

In term of software as a service, a consumer needs to depend on the service providers for data security and service providers have to be responsible for providing proper security mechanism to protect data and applications. In this model data is being stored in cloud along with others companies or individuals data. The cloud service providers may replicate data in various places for data availability and efficiency. As a result, there are some security issues arise such as: how is being data stored and where, what types of security is being provided for data manipulation and storage. There are some key security basics need to be considered during SaaS deployment and development. There are:

2.1.1 DATA SECURITY:

When enterprise sensitive data are stored in cloud, vendors should provide physical and logical security, secure access policies and some additional security checks due to security vulnerabilities in applications and concern about malicious employees, who can Exploit weakness in data security model. Data control over cloud services make difficult to protect and enforce identity theft and cybercrime security. Sharing resources across multiple domains and failures of data backup also arise some data leakage.

2.1.2 NETWORK SECURITY:

In cloud environment data are being transferred over the Internet, thus data flow security is an important issue to avoid leakage of information. To sniff network packets an intruder can make use of data packet to analyze weakness in network security configuration. Attackers can gain access applications and data through hacking such as: some kind of remote access mechanism and injection (SQL and some bad command) vulnerabilities. DOS (Denial of Service), DDOS (Distributed DOS), man in the middle attacks, social networking attacks and some unauthorized attacks creates grate security issues in cloud.

2.1.3 DATA CONFIDENTIALITY:

Privacy and confidentiality issues are taking placed when data shares between various users, devices and applications. Here multi tenancy and multitasking (resource sharing and sharing processing resources: CPU- Central Processing Unit) presents a number of confidentiality threats and risks. Data confidentiality in cloud environment related to user authentication. For overall system security software and data confidentiality is also important to prevent unauthorized use of data.

2.1.4 DATA INTEGRITY:

Data integrity ensures that data are being integral and modified by only authorize entity. Due to increasing number of entities and access points in cloud, authorization becomes crucial that only authorized entities are interact with data. If cloud system resources are not properly segregated among clients then some security issues arise for data integrity. Inadequate encryption and week key management scheme can also lead to security breach.

2.1.5 AVAILABILITY:

Cloud services access on demand by authorized parties even if some authorized entities misbehave or any security breaches. To test availability of the security as eservice vendors need to consider authentication process and session management weakness issues. Other issues are also need to consider as well such as: data and information service lock in, bandwidth and connectivity speed over the network in cloud services.

2.1.6 DATA LOCALITY:

In the SaaS model, the consumers are unaware that, where there data is being resided. Some cases it is an issue for some companies for data privacy laws in various countries. So, this service model must be capable of proving data security based on location issues.

2.1.7 ACCESS CONTROL:

Many SMB (Small and Medium Business) companies store their employees' data in cloud database. The companies have its own policies to access or use data based on their user limitation. So, when an employee left and onboard the security as service users must bear in mind to enable or disable users account else security breach might be occurred. The security as a service and service providers must offer some flexibility to adhere companies' policies in cloud to avoid intrusion of data by unauthorized users.

2.2 SECURITY ISSUES IN PLATFROM AS A SERVICE:

The main purpose of this model is to protect data. In this model, service provider gives possible command of control such as operating system platform, program development tools and storage area, to build application or program on top of service platform by using resources. Even though some controls are given to the clients, but still need to consider and control some security issues below the application levels such as: network and host intrusion. The service providers have to assure against possible use of outage and data remain inaccessible between different applications. Another aspect of security issue needs to consider that load balancing across on platforms. The vulnerabilities in the cloud computing environment are not only related to web related applications but also machine to machine service oriented architecture applications. It is noted that, service oriented architecture applications are progressively more deployed in cloud.

2.3. SECURITY ISSUES IN INFRASTRUCTURE AS A SERVICE:

Cloud computing combines virtualization technologies are creative way to provide better information technology services to consumers. Due to rising virtualization technology poses some security issues for control over the owner of data regardless of physical location. Various security issues are arising to deploy models in infrastructure as a service. Private cloud environment creates fewer security risks compared to public cloud. The cloud concept implemented just over the Internet, so whatever security issues and threats are facing in the Internet, for cloud services need to consider as well. Infrastructure is not only appropriate for hardware resources, where data is being reside or processed, but also the way data are being transmitted over the media from source to destination over the open network. There are some possibilities that data can be routed through intruder's network or infrastructure.

III CONCLUSION

Cloud computing model has the ability to scale up services and virtual resources on demand. To process users conventional cluster system, cloud services provides a lot of advantages. There is no big investment required to update infrastructure, labor and continuing cost. In fact cost is almost zero when resources are not in used .Throughout this paper clearly discussed about security risks and issues in various aspects, such as confidentiality, integrity, availability and authenticity and issues related to various service delivery models such as network security, data security and locality in software as a service models, network and host intrusion in platform as a service and infrastructure as a service not only considered where data is being stored and process but also concerned the media of data transfer is being used over the Internet. Thus cloud computing is not mature enough, therefore many academic researches and industries are moving toward to cloud computing environment. Cloud technology is still now in cloud for users.

REFERENCES

[1] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, 2011.

[2] M.Carroll, A.Van der Merwe, P.Kotze, Secure cloud computing: Benefits, risks and controls, Information Security South Africa (ISSA), pp. 1-9, September 2011.

[3] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010. [4] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2011.

[5] National Institute of Standards and Technology, NIST Cloud Computing Program, 2010 [Accessed on: 18 October 2011].