INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

Introduction to Cloud Computing and Its Security Issues

Monali A. Pimpalkar
Shri.Shivaji Science College,Congress Nagar,Nagpur,Department of Computer Science,India
mpunekar11@gmail.com

Abstract :Cloud computing is a technique of providing computing services via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it reduced the managing cost and also saves the time for organizations. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of any cloud provider. So limited control over the data may arise various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. This paper provides brief details about what cloud computing is and the main security issues that are currently present within the cloud computing industry.

Keywords : Availability, Cloud Computing, Deployment ,Integrity , Security, Segregation ,Vulnerability.

INTRODUCTION :

The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Example of cloud services include online file storage , social networking sites , webmail , online business applications.

Cloud computing provides various benefits such as ,the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. And also it provides the flexibility and highly automated processes wherein the customer need not worry about very ordinary concerns like software up-gradation [1]. Cloud is not only used by the Multinational companies but it's also being used by small and medium enterprises [2]. Cloud Computing is an emerging trend to deploy and maintain software and is being adopted by the industry such as Google, IBM, Microsoft, and Amazon. Several prototype applications and platforms, such as the IBM ―Blue Cloud infrastructure, the Google App Engine, the Amazon Cloud, and the Elastic Computing Platform [3].

SERVICE MODELS OF CLOUD COMPUTING :

1.Software as-a-Service:-

In SaaS model a software provider license a software application to be used and purchase on demand [4]. This service run on cloud and multiple end users are uses it. Basically It runs on web browser e.g. Gmail- a popular SaaS product. Applications can be accessed through network from various client(web browser,mobile phones etc) by application use. It does not require client installation just a browser or other client device and network connectivity.

2.Platform as-a-service:-

A PaaS platform developer to write application those run on cloud[5]. It is cloud based application development and used by deployers and developers. It has highly scalable multi tier architecture e.g. Azure and salesforces.com. PaaS offer an environment where developer can create and deploy applications and do not need necessarily to know how much memory and how many processor their application will be using .

3.Infrastructure as-a-service:-

It offer a service to get a virtual server in few minute and pay only for the resource they use [6]. It allow accessibility of infrastructure using Internet technology consist of server, storage and other peripherals devices. It can be coupled with managed services for operating system and application support. In IaaS model consumer can directly use infrastructure components (storage,firewall,network etc)

There are some deployment models in cloud computing are :

1. Public cloud :The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
2. Hybrid cloud:The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized technology that enables data and application portability(e.g. cloud bursting for load balancing between clouds).
3. Private cloud: This cloud infrastructure operated solely for a single organization[7], It may be managed by the organization or a third party .
4. Community cloud:The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations) [8].

SECURITY ISSUES IN CLOUD COMPUTING :

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Various Security issues in cloud computing environment are discuss below :

1.Access to Servers & Applications:

In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which is not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data.

In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be followed by the cloud to avoid intrusion of data by unauthorized users[9] .

2.Data Transmission:

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. In Cloud environment most of the data is not encrypted in the processing time. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider.

3.Virtual Machine Security:

Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and moved between physical servers. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and write access to any portion of the host's file system including the system folder and other security-sensitive files.

4. Network Security:

Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems because of incomplete path between them.

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

Reused IP address issue have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user [10].

4.Data Security:

For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

5. Data Privacy:

The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [12].

6. Data Integrity:

Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

7. Data Location:

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications [12].

8. Data Availability:

Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers.

9. Data Segregation:

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

10.Data Storage Security:

Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important.

COCLUSIONS:

In this paper, we first discussed what is cloud computing is, various models and services of cloud computing.Then we discuss the major security issues in cloud computing enviornment. Data security is major issue for Cloud Computing. One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed by removing the drawbacks of old techniques.

References :

[1] Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S. Parekh, ―Automated Control in Cloud Computing: Opportunities and Challenges‖, Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1- 60558-585-7.

[2] Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[3] W.K. Chan, Lijun Mei, and Zhenyu Zhang, "Modeling and testing of cloud applications", to appear in Proceedings of2009 IEEE Asia-Pacific Services Computing Conference (APSCC 2009), (Singapore, December 7-11, 2009), IEEE Computer Society Press, Los Alamitos, CA, USA, 2009.

[4] I-Hsun Chuang, "An Effective Privacy Protection Scheme for Cloud Computing," ISBN 978-89-5519-155-4Feb. 13~16, 2011 ICACT2011

[5] Junchao Li," Study on Service-Oriented Cloud Conferencing," 978-1-4244-5540-9/10/$26.00 ©2010 IEEE

[6]. Jianfeng Yang, Zhibin Chen "Cloud Computing Research and Security Issues" Vol 978-1-4244-5392-4/10/$26.00 ©2010 IEEE

[7] Ohlman, B., Eriksson, A., Rembarz, R. (2009) WhatNetworking of Information Can Do for Cloud Computing.The 18th IEEE International Workshops on EnablingTechnologies: Infrastructures for Collaborative Enterprises,Groningen, The Netherlands, June 29 - July 1, 2009

[8] Cong Wang, Qian WangKui Ren, Ning Cao, and Wenjing Lou ―Toward Secure and Dependable Storage Services in Cloud Computing‖ IEEE transactions on services computing, vol. 5, no. 2, april-june 2012

[9] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628,Chengdu, China, December, 2009. ISBN: 978-0-7695-3929 -4.

[10] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing OpenArchitecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.

[11] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secur Cloud Computing", Wiley Publishing, Inc.,2010

[12] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.