ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

Cloud Computing Security Issues And Methods to Overcome

Manas M N[1], Nagalakshmi C K[2], Shobha G[3]

MTech, Computer Science & Engineering, RVCE, Bangalore, India[1,2]

Professor & HOD, Computer Science & Engineering, RVCE, Bangalore, India[3]

Abstract: Cloud computing is a technology which satisfies customers dynamic resource demands and makes the job easier to work on all platforms for the user. Cloud computing is the delivery of computing services over the Internet. Security is the main criteria when working on cloud, as the third party involvement will be there. Secure architecture should be used to provide services through the cloud. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking.Methods show how to overcome the security issues of the cloud.

Keywords: Cloud Computing, Virtualization, Multi Tenant, Scalable.

I. INTRODUCTION

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Cloud computing can significantly reduce the cost and complexity of owning and operating computers and networks. If an organization uses a cloud provider, it need not spend money on information technology infrastructure, or buy hardware or software licenses. Cloud services can often be customized and flexible to use, and providers can offer advanced services that an individual company might not have the money or expertise to develop.

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software license, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop.

Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development.

Another potential benefit is that personal information may be better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start and the use of better security mechanisms. Cloud computing will enable more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers. Cloud computing may also allow for better audit trails. In addition, information in the cloud is not as easily lost (when compared to the paper documents or hard drives, for example).

The characteristics of cloud computing tells storage is not done on a single system, User terminal is only responsible for user interaction and access to service, Service can be provided directly to user terminal or access through network, Provides reliable secure data, up-to-date, no virus attacks, Users need not worry on configuration and it is easily manageable, Multitenancy, pay as you use, scalable. We can improvise cloud computing by virtualization, Reduce device dependency, Platform independent, Integrate resources [5].

II. TYPES OF CLOUD SERVICE

Cloud computing consists of three different types of service provision as shown in Fig.1. In each case services are hosted remotely and accessed over internet through customer web browser, rather than being installed locally on customer's computer. Firstly SAAS (software as a service) refers to the provision of software applications in the cloud. Secondly PAAS (platform as a service) refers to the provision of services that enable the customers to deploy in the cloud, applications created using programming languages and tools provided by the supplier. Thirdly IAAS (infrastructure as a service) refers to the services providing computer processing power, storage space and network capacity, which enable the customers to run arbitrary software in the cloud. These three elements are together called cloud computing ‘stack’.

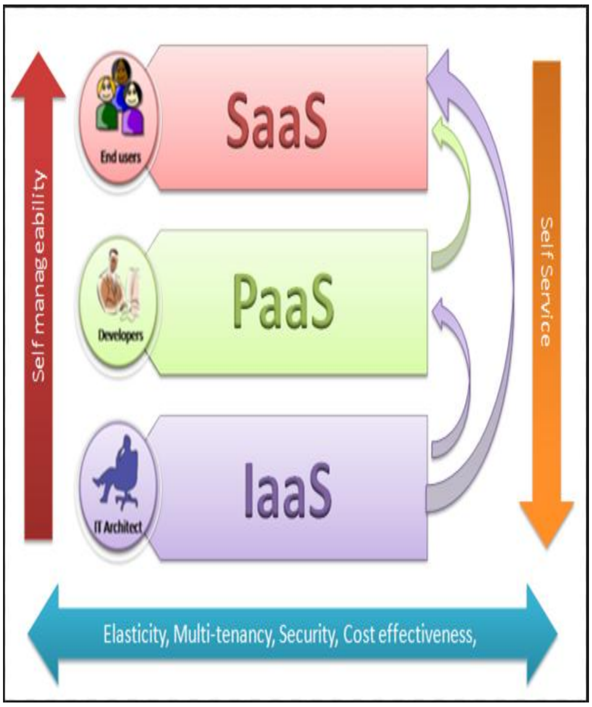

Figure 1: SaaS, PaaS, IaaS

III. CLOUD FORMATIONS

The cloud environment is subdivided into public, private, hybrid and community clouds as shown in Fig.2.

Public clouds are those in which services are available to the public at large over the internet. Public clouds provide an elastic, cost- effective means to deploy solutions and take care of deploying, managing, and securing the infrastructure. Companies can use it on demand, and with pay-as-you-option, it is much like utility consumption.

Private cloud is essentially a private network used by one customer for whom data security and privacy is usually a primary concern. The downside of this type of cloud is that the customer will have to bear the significant cost of setting up and then maintaining the network alone.

Hybrid cloud environments are often used where a customer has requirements for a mixed set of dedicated server and clod hosting, for example if some of the data being stored is of a very sensitive nature. In such circumstances the organization may choose to store some data on its dedicated server and less sensitive data in the cloud. Another reason for using hybrid clouds is when the organization needs more processing power than is available in-house and obtains extra requirement in the cloud. This is referred to as ‘cloud bursting’. Additionally hybrid clouds environments are used in situations where customer is moving from an entirely private to entirely public cloud setup.

Community clouds usually exist where a limited number of customers with similar IT requirements share an infrastructure provided by a single supplier. The cost of the services are spread between the customers so this model is better, from an economic point of view, than a single tenant arrangement. Although the cost savings are likely to be greater in a public cloud environment, community cloud users generally benefit from greater security and privacy, which may be important for policy reasons.

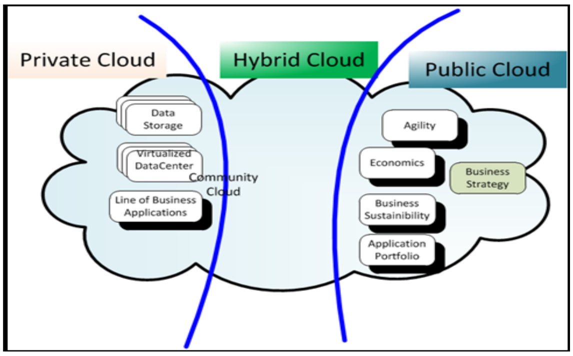

Figure 2. Types of cloud

IV. CLOUD CHARACTERISTICS

Cloud carries the basic infrastructure characteristics that are helpful to deploy cloud service in a fast and cost-effective way. The following characteristics set apart cloud from other computing techniques.

A.On Demand Service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

B.Ubiquitous Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

C. Location-Independent Resource Pooling (Multi-Tenant)

The provider’s computing resources are pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the demand.

D.Rapid Elasticity

Capabilities can be rapidly and elastically provisioned, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quality at any time.

V. SECURITY ISSUES AND ITS SOLUTIONS

The cloud is the delivery of on-demand computing resources—everything from applications to data centres—over the Internet on a pay-for-use basis. Merit of cloud include Reduced capital costs, Improve accessibility, improve flexibility. Despite of its merits the most serious of all is being that is the security of information in the cloud. There are many security implications of which the serious issues are concentrated in this paper. This paper investigates the possibility of the data/information being secure in the cloud computing environment. The cloud security issues are summarized as follows[1][3][4]:

A. Multi tenancy

Implies sharing of computational resources, storage, services, database, physical and logical access with other tenants residing on same physical or logical platform at provider's premises. This sharing of resources violates the confidentiality of tenants IT assets which leads to the need of secure multi tenancy. To deliver secure multi-tenancy there should be a level of isolation among tenant data as well as location transparency where tenants may not have knowledge of where their data is located and or their process is resident.

To have secure multitenancy platform, isolation among tenants data and location transparency where tenants have no knowledge or control over specific location of resources to avoid planned attacks.Always keep data at multiple location so that even if at one place attack occurs back up is in other place.

- Isolation on PAAS should be done on running services and API.
- Isolation on SAAS isolate among transaction carried out on same instance by different tenants.
- Isolation on IAAS is on VM storage,memory network and cache memory.

B. Elasticity

Implies that consumers are able to scale up or down resources assigned to resources based on current demand. The solution for this can is that data location should be within the tenant's country boundaries. In addition, the placement engines include mitigation strategy where services are migrated from logical or physical host to another or from one cloud provider to another in order to meet demands and efficient utilization of the resources.

C. Availability of information

Implies that when an organization ports its process, services and applications to cloud they take a calculated risk in terms of non-availability of critical data or information or processes when needed the most. The way to mitigate the unavailability of resources is to have backup plan to cover an outage event also for local resources for crucial information. The provider should provision a monitoring and notification system that enable the consumers know of the possible down time.

D. Secure information management

States that the cloud management layer is the microkernel that can be extended to incorporate and coordinate components such as service monitoring, billing, services registry and security management of the cloud. This layer is very critical since any breach of this layer will result in a malicious user ending up in having control alike an administrator, over the whole cloud platform. The solution for this is to include security requirements and policies specifications derived from tenant organizations which are reviewed and applied in tenant's specific logical and physical environment, security configurations and feedback from environment to security management and cloud consumer base.

E. Information integrity and privacy

Means exposing resources over the internet to valid users and malicious attackers. A tenants resources can be accessed through web browsers, remote connections etc. some of major information security privacy and authentication issues are absence of authentication, authorization and accounting controls and no management of encryption and decryption keys. To overcome this problem there should be proper authentication, authorization should be implemented so that any attempt to access the information goes through multilevel check to ensure only authorized tenants have access to the information.

F. Cloud secure federation

Is an issue when cloud consumer leverages applications and information that depend on services from different clouds, it needs to maintain its security requirements enforced on both clouds and in between. This problem can be overcome by identity federation, leveraging identity attributes federation, single sign on, authentication and authorization can help resolve federation security issues.

G. Multiple Stake holders

Different stake holders in cloud computing are

1. Cloud provider, is the one who delivers infrastructure to cloudcustomers.
2. Service provider is the onewho uses cloud infrastructure to deliver applications to end users.
3. Customer is the one who uses the service hosted on cloud environment.

Each of the above have their own security issues. Each customer will have different trust relation with providers,sometimes user himself can be attacker. Provider and customer need to agree on conditions, however so standard conditions are present.

H.Third Party Control

Owner has no control on their data processing as this is a third party issue.Cloud providers are not aware of architecture of Cloud so effective security is not provided. Sometimes user can be locked with one vendor.This happens because of agreement or difficult in migrating data to new vendor.

I. Integrity of information

Is achieved when there is a mutual trust between the provider and consumer and they complement each other and support the security such that whole system works seamlessly. To achieve this proper authentication, Authorization and accounting controls should be implemented by the cloud service provider and consumer. The credentials to access the information on cloud should be individual, secure (RSA tokens or one time password) and should not be shared among the entities of the consumer organization.

J.Repudiation of information

The consumer and the provider find themselves in a deep-hole when it comes to prove the transaction they did was indeed them, or may decline that it was them. To prevent this issue at cloud level, cloud provider has to ensure that non-repudiation enabled protocol or handshake is deployed whereby, the engaging parties cannot dismiss their participation in argued transaction.

K. Service disruptions

It can land any business/organization into a difficult situation, the information required is not available when it is most desired and also unpleasant behavior can be caused by DOS, DDOS attack. This issue can be addressed by employing defence –in-depth technique in order to have security controls implemented at various layers throughout the cloud access path as well as within the consumer and provider network, sharing of account credentials between consumers should be strictly denied.

L. Loss of Control

Loss of controls can be a disaster for an organization. This is one of the CIO’s major concerns before they take a decision to move their data/information to the cloud. To minimize this effect the organizations should understand clod provider’s security policies, storage policies and SLAs. This will enable in mutual understanding between the provider and consumer about the way the consumer’s data will be handled in cloud.

M. Security Management

The successful security management in cloud depends on two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform and how must an organization’s security in the cloud. Both of these factors must be continually reevaluated based on the sensitivity of the data and the service-level changes over time.

VI. SECURITY THREATS PRESENT IN THE CLOUD

There are various security concerns that presents customer from taking the benefits of the cloud. Following are fewthreats present in the cloud and their mitigation[2].

A. VM Attacks

Cloud computing is based on VM technology. For implementation of cloud, hypervisor such as VMware, Sphere etc are used. Developers need to take care of attacks. When coding and also by using IDS and IPS we can solve these and use the suitable firewall.

B. Use of Cloud Computing

- This is used mainly due to weak registration system
- By implementing stricter registration process
- By credit card fraud monitoring.

C. Loss of Governance

SLA may not have commitment on part of cloud provider or cloud provider. But there is no proper SLA i.e. standard SLA’s are not present.

D. Lock-IN

Customer cannot move from one service provider to another. So to overcome this API’s should be used, this should be standardized. So anybody can use it on cloud.

E. Data Loss or Leakage

It is a negative impact on business. By encrypting and protecting the integrity of data in transit. Analysis of data protection at both design and runtime should be done.

VII. SECURE CLOUD ARCHITECTURE

Security continues to be a concern for customers as they consider moving to the cloud [2]. However, some aspects of a secure infrastructure are common in many customer deployments. To satisfy on security requirements and address the security issues as analyzed above, we can summarize various security issues by a cloud security architecture as depicted in Fig.3.

A. Single Sign On

Usually users of cloud will have multiple logins but this will lead to authentication problems, so strong authentication at user level should be provided within the cloud.

B. Increase Availability

To increase the data availability dynamic server load balancing and ISP load balancing within the network infrastructure.

C. Defense in Depth Approach

There should be a proper intrusion detection and prevention components within the network. Proper virtual firewall should be implemented instead of first generation firewalls. Intrusion prevention systems (IPS) should be installed to protect networks from internal threats from insiders.

D.Single Management Console

Additional network protection devices are used to protect virtual network this single management console should be used.

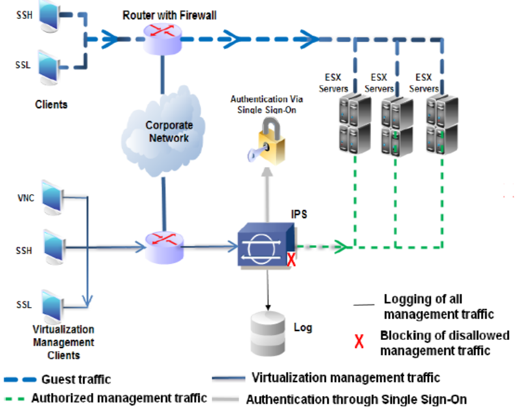
SSH
SSL
Clients
Router with Firewall
Corporate Network
Authentication Via Single Sign-On
ESX Servers
ESX Servers
ESX Servers
VNC
SSH
SSL
Virtualization Management Clients
IPS
X
Log
Logging of all management traffic
X Blocking of disallowed management traffic
Guest traffic
Authorized management traffic
Virtualization management traffic
Authentication through Single Sign-On

Figure 3. Secure Cloud Architecture

VIII. CONCLUSION

As a new technology is expected to significantly reduce thecost of existing technologies, cloud computing is the development trend of IT industry. For information security, there are both favorable factors and negative factors brought by cloud computing. The final effect depends on whether we can develop its strengths and avoid its disadvantages. Only in this way, the cloud can become a real cost savings, improving productivity efficiency and secure platform. The most serious of all these issues is security of information whether it is at rest or in transit. There are numerous security issues pertinent to cloud infrastructure of which most critical ones are discussed in this paper. Next cloud computing security considerations are discussed which must be included in every cloud for the data in it to be secure. Next secure cloud architecture is proposed to secure the data from external attacks.

REFERENCES

[1] AkhilBehl, KanikaBehl, “Security Paradigms for Cloud Computing**”,**Fourth International Conference on Computational Intelligence, Communication Systems and Networks, IEEE, 2012

[2] MeikoJensen ,JorgSehwenk et al., “On Technical Security,Issues in cloud Computing ”IEEE International conference on cloud Computing, 2009

[3] AkhilBehl, KanikaBehl, “An analysis of cloud computing security issues”, World Congress on Information and Communication Technologies, IEEE, 2012

[4] HuagloryTianfield, “Security Issues In Cloud Computing”, International Conference on Systems, Man, and Cybernetics, IEEE, OCT 14-17,2012

[5] Zhang Yandong, Zhang Yongsheng, “Cloud Computing and Cloud Security Challenges”, International symposium on information technology in medicine and education, 2012

[6] Luis Vaquero, Luis Rodero-Merino, Juan Caceres, et al, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, pp. 50-55, 2009

[7] Ni Zhang Di Liu Yun-Yong Zhang, “Research on cloud computing security”, International Conference on Information Technology and Applications”, IEEE, 2013