A Study of Prevalent Vulnerable Characteristics in Cloud Computing

Amirthavalli Madhwaraj[1], Suguna[2] and Priyadharshini[3]
[1,2,3] Computer Science& Engineering, Agni College of Technology,
Chennai, TamilNadu/600103, India.

Abstract

Cloud computing is a new paradigm shift in virtualization technology. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. In this paper, the vulnerable aspects of cloud and a a survey of the different security risks that exacerbates security and privacy challenges have been explored.Beside,a primitive security solution has been suggested.

Keywords— Cloud Computing,multitenancy, *rapid elasticity,hybrid model.*

1.Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.

Cloud computing entrusts remote services with a user's data, software and computation. In the business model using software as a service, users are provided access to application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run.

SaaS is sometimes referred to as “on-demand software” and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee. Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world.

In June 2011, a study conducted by VersionOne found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept,[1]highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average an 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs.

Cloud computing is at an early stage, with a motley crew of providers large and small delivering a slew of cloud-based services, from full-blown applications to storage services to spam filtering. Yes, utility-style infrastructure providers are part of the mix, but so are SaaS (software as a service) providers such as Salesforce.com. Today, for the most part, IT must plug into cloud-based services individually, but cloud computing aggregators and integrators are already emerging.

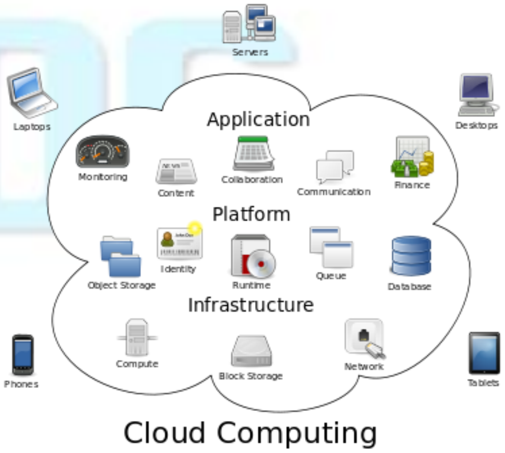

Fig 1.Cloud Computing Architecture

2.Vulnerability

According to the Open Group's risk taxonomy, Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force.

Based on the abstract view of cloud computing , we can now move toward a definition of what constitutes a cloud-specific vulnerability. A vulnerability is cloud specific if it

- is intrinsic to or prevalent in a core cloud computing technology,
- has its root cause in one of NIST's essential cloud characteristics,
- is caused when cloud innovations make tried-and-tested security controls difficult or impossible to implement, or
- is prevalent in established state-of-the-art cloud offerings.

2.1 Essential Characteristics

In its description of essential cloud characteristics,2 the US National Institute of Standards and Technology (NIST) captures well what it means to provide IT services from the conveyor belt using economies of scale:

• *On-demand self-service.* Users can order and manage services without human interaction with the service provider, using, for example, a Web portal and management interface. Provisioning and de-prov isioning of services and associated resources occur automatically at the provider.

• *Ubiquitous network access.* Cloud services are accessed via the network (usually the Internet), using standard mechanisms and protocols.

• *Resource pooling.* Computing resources used to provide the cloud service are realized using a homo geneous infrastructure that's shared between all service users.

• *Rapid elasticity.* Resources can be scaled up and down rapidly and elastically.

• *Measured service.* Resource/service usage is constantly metered, supporting optimization of resource usage, usage reporting to the customer, and pay-as-you-go business models.

2.2 Vulnerabilities in the cloud

According to Bernd Grobauer,Tobias walloschek,and Elmar stocker Siemens multi-tenant access vulnerable are prevalent in cloud services model namely Iaas,Paas,Saas.

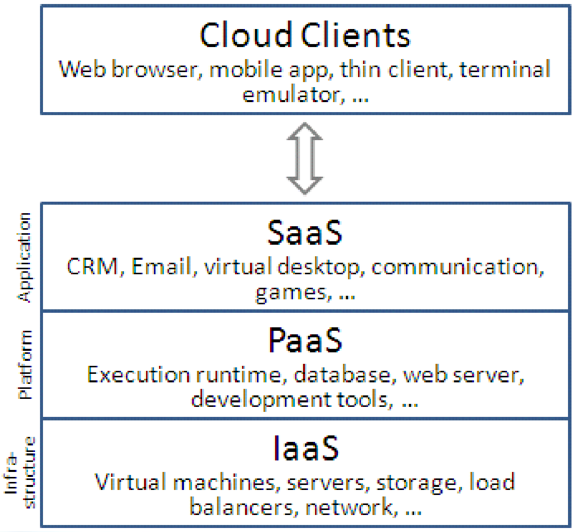
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig 2.Service Model

Software as a Service (SaaS)**:** In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its scalability. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand.

Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be multitenant, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud based application software with a similar naming convention: desktop as a service, business process as a service, test environment as a service, communication as a service.

The pricing model for SaaS applications is typically a monthly or yearly flat fee per user, so price is scalable and adjustable if users are added or removed at any point. Examples of SaaS include: Google Apps, Microsoft Office 365, Onlive, GT Nexus, Marketo, and TradeCard.

Platform as a Service (PaaS): In the PaaS model, cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand such that cloud user does not have to allocate resources manually.

Examples of PaaS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard, Mendix, OpenShift, Google App Engine, Windows Azure Cloud Services and OrangeScape.

Infrastructure as a Service (IaaS): In the most basic cloud-service model, providers of IaaS offer computers - physical or (more often) virtual machines - and other resources. (Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.) IaaS clouds often offer additional resources such as images in a virtual-machine image-library, raw (block) and file-based storage, firewalls, load balancers, IP addresses,virtual local area network (VLANs), and software bundles.IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers.For wide area connectivity, customers can use either the Internet or carrier cloud (dedicated virtual private networks).To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis[1]: cost reflects the amount of resources allocated and consumed. Examples of IaaS providers include Amazon CloudFormation,Amazon EC2, Windows Azure Virtual Machines, DynDNS, Google Compute Engine, HP Cloud, iland, Joyent, Oracle Infrastructure as a Service, Rackspace Cloud, ReadySpace Cloud Services, SAVVIS, Terremark, NaviSite, and Linode.

Rent processing, storage, network capacity, and other computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity. Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

Peak-load capacity increases (users need not engineer highest possible load-levels) *efficiency* improvements for systems that are often only 10–20% utilised.

3.Authentication and Identity Management

Authenticate can use an identity management (IDM) mechanism and services based on credentials and characteristics using different identity tokens and identity negotiation protocols leads to interoperability drawbacks and it is a major issue concerning IDM in cloud. Early password-based authentication has inherited limitation and also have some significant risks.

According to Bernd grobauer,Tobias walloschek,and Elmar stocker Siemens All cloud services (and each cloud service's management interface) require mechanisms for identity management, authentication, *authorization, and auditing (IAAA).*

To a certain extent, parts of these mechanisms might be factored out as a stand-alone IAAA service to be used by other services. Two IAAA elements that must be part of each service implementation are execution of adequate authorization checks (which, of course, use authentication and/or authorization information received from an IAA service) and cloud infrastructure auditing.

Most vulnerabilities associated with the IAAA component must be regarded as cloud-specific because they're prevalent in state-of-the-art cloud offerings. Earlier, we gave the example of weak user authentication mechanisms; other examples include

Denial of service by account lockout. One often-used security control—especially for authentication with username and password—is to lock out accounts that have received several unsuccessful authentication attempts in quick succession. Attackers can use such attempts to launch DoS attacks against a user.

Weak credential-reset mechanisms. When cloud computing providers manage user credentials themselves rather than using federated authentication, they must provide a mechanism for resetting credentials in the case of forgotten or lost credentials. In the past, password-recovery mechanisms have proven particularly weak.

3.1 Insufficient or faulty authorization checks

State-of-the- art Web application and service cloud offerings are often vulnerable to insufficient or faulty authorization checks that can make unauthorized information or actions available to users. Missing authorization checks, for example, are the root cause of URL-guessing attacks. In such attacks, users modify URLs to display information of other user accounts.

3.2 Coarse authorization control.

Cloud services' management interfaces are particularly prone to offering authorization control models that are too coarse. Thus, standard security measures, such as duty separation, can't be implemented because it's impossible to provide users with only those privileges they strictly require to carry out their work.

3.3 Insufficient logging and monitoring possibilities.

Currently, no standards or mechanisms exist to give cloud customers logging and monitoring facilities within cloud resources. This gives rise to an acute problem: log files record all tenant events and can't easily be pruned for a single tenant. Also, the provider's security monitoring is often hampered by insufficient monitoring capabilities. Until we develop and implement usable logging and monitoring standards and facilities, it's difficult—if not impossible—to implement security controls that require logging and monitoring.

4.Perception of Security issues

According to Hanqian Wu,Yi Ding, Chuck Winer Li Yao,

4.1Remote management Vulnerabilities.

Commercial hypervisors normally have management consoles as new facilities for administration to manage Vms.Xen,for instances,uses XenCenter to manage their VMs.These consoles also open new vulnerabilities,such as Cross-site scripting,SQL injection,etc.

4.2 Denial of services(DOS) Vulnerabilities.

In virtualization environment,resources such as CPU,memory,disk and network are shared by VMs and the host.so it is possible that a DOS will be imposed to VMs which correspondingly take all the possible resources from the host.As a result,the system will deny any request from the guest because of no resources available.

4.3 Security issues in SaaS

According to S. Subashini n, V.Kavitha in Saas model ,the Saas provider's data center stores the enterprise data along with the data of other enterprises. so multiple copies are maintained at different location and the data reside within the enterprise boundary,subject o policies.since there is great deal od uncomfort with lack of control.

5.Security solution

The security issues is most significant concern in cloud computing.A survey on various security solution relies on cryptography and network security technique for each service model.

The proposed solution based on the literature survey is to combine different policies in hybrid model and use standard cryptography algorithm to prevent security attack in the cloud.

6. Conclusion

The security issues is the major concern in public cloud.the vulnerable factors which hinders the growth of cloud computing have been discussed.The future enhancement can ne made by implementing the cryptography techniques to secure each service model and also the security issue which has been elaborated for the same.

References

[1] Amazon. AmazonElasticComputeCloud(EC2),2010 /http://www.amazon.com/ ec2/S. Attanasio CR.Virtualmachinesanddatasecurity.
[2]Securityissuesinservicedeliverymodelsofcloudcomputing S. Subashini n, V.Kavitha, Journal of Network and Computer Applications 34 (2011) 1–11.
[3] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http:// w.cloudsecurityalliance.org/csaguide.pdf.
[4]. D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," ENISA, 2009; www.enisa.europa.eu/act/rm/ files/deliverables/cloud-computing-risk-assessment/
[5]Rajkumar Buyya Market-Oriented Cloud Computing:Vision,Hype,and Reality for Delivering IT Services as Computing Utilities 2008