Security Issues in Cloud Computing

Ayushi Saxena, Aarushi Jain

***Abstract*— In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. It offers an on demand and scalable access to a shared pool of resources hosted in a data centre at providers' site. It reduces the overheads of up-front investments and financial risks for the end-user. The qualitative services and lower cost of services are the key requirements of this technology. Regardless of the fact that cloud computing offers great advantages to the end users, there are several challenging issues that are mandatory to be addressed. This paper discusses security issues, requirements and challenges that cloud service providers face during cloud engineering.**

***Keywords*— Cloud computing, SOA and SLA.**

Introduction

The variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing. However, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's existing capabilities. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still Reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing. In one aspect, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a survey more specific to the different security issues and the asocial challenges that has emanated in the cloud computing system. The following section highlights a brief review on cloud characteristics, service models and deployment models and the remaining sections are organized as follows. Section 3.0 discusses security issues and challenges in cloud computing. And Section 5.0 presents the conclusion.

Cloud Computing-

Is a style of computing over internet where shared servers provide resources software and data to computers/other devices on demand

Cloud Services-

IaaS (Infrastructure as a service) – Is the delivery of computer architecture over internet. It involves the use of remote computers(O.S , database , middle ware , applications) and storage. SaaS (Software as a service) –

Is the delivery of Applications (e.g., CRM or ERP) as a service to end users over internet through browsers.

PaaS (Platform as a service) – Is the delivery of application development and deployment platform (e.g., Pega) as a service to developers over internet through browsers, who use the platform to build , deploy and manage SaaS applications.

Cloud Types-
Private cloud is also called internal or corporate cloud, which provides hosted devices to a limited number of people behind firewall.
Public cloud is also called external cloud, where resources are dynamically provisioned on a self-services over internet.

Cloud Monitor-
Is a kind of dashboard that provides monitoring for cloud resources and provides visibility into resource utilization, operational performance including CPU utilizations, disk read/writes and network traffic.

Cloud Storage-
Is a model of networked data storage where data is stored in multiple virtual servers rather than being hosted on dedicated server. Hosting companies operate large data centers, who virtualizes the resources according to customer requirements and expose them as virtual servers, which customers can manage.

Security-
Security on physical, virtual and cloud environments. Roles/User management for authentication and authorization. Firewall settings to control network access between group of instances Virtual private cloud by specifying IP range for the access. Backups and Monitoring. Logs and Reporting.

Availability and Performance-
Multiple locations – Cloud instances will be hosted Available in multiple locations to ensure high availability Load Balancer–Automatically distributes incoming traffic to multiple cloud instances for fault tolerance and load balancing for higher performance.

Benefits-
Cost is greatly reduced as infrastructure is provided by third party. Device and Location independence. Scalability via dynamic provisioning of resources on a fine-grained, self-service basis. Reliability is improved if multiple redundant sites used. Maintenance is easier since they don't have to be installed on each user's computer.

Providers-
Amazon http://aws.amazon.com/ec2// Oracle http://www.oracle.com/us/technologies/cloud/
Google http://code.google.com/appengine// Microsofthttp://www.microsoft.com/windowsazure //

II. OVERVIEW OF CLOUD COMPUTING

To properly understand cloud, it is important to know what it is, some essential characteristics that a system must possess to qualify as a cloud along with various services that can be offered using it through various deployment models. Cloud computing is in its infant form and numerous definitions have been proposed by many scientists. One of them is ―A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models‖ [8].

A. Characteristics

The cloud computing must have some characteristics in order to meet expected user requirements and to provide qualitative services. According to NIST [8], these five essential characteristics can be classified as:

a) On-demand self-service- A consumer can access different services such are computing capabilities, storage services, software services etc. as needed automatically without service provider's intervention.

b) Broad network access- To avail cloud computing services, internet works as a backbone of cloud computing. All services are available over the network and are also accessible through

standard protocols using web enabled devices such are computers, laptops, mobile phones etc.

c) Resource pooling- The resources that can be assigned to users can be processing, software, storage, virtual machine and network bandwidth. The resources are pooled to serve the users at a single physical location and/or at different physical location according to the optimality conditions (e.g. security, performance, consumer demand). The cloud gives an impression of resource location independence at lower level (e.g. server, core) but not at the higher level (e.g. data enter, city, country).

d) Rapid elasticity- The beauty of cloud computing is its elasticity. The resources appear to users as indefinite and are also accessible in any quantity at any time. The resources can be provisioned without service provider intervention and can be quickly scale in and scale out according to the user needs in a secure way to deliver high quality services.

e) Measured service- A metering capability is deployed in cloud system in order to charge users. The users can achieve the different quality of services at different charges in order to optimized resources at different level of abstraction suitable to the services.

B. Cloud Service Models

The cloud services are delivered in three forms such are Infrastructure as a Service (IaaS), Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS). The services are delivered over the network by using Web browser, Web Based mail etc.

The service models are as follows:

Software-as-a-Service (SaaS): In this multitenant service model, the consumers use application running on a cloud infrastructure. The cloud infrastructure including (servers, OS, Network or application etc.) is managed and controlled by the service provider with the user not having any control over the infrastructure [8, 9]. Some of the popular examples are SalesForce.com, NetSuite, IBM, Microsoft and Oracle etc. Platform-as-a-Service (PaaS): With this model, the provider delivers to user a platform including all the systems and environments comprising software development life cycle viz. testing, deploying, required tools and applications. The user does not have any control over network, servers, operating system and storage but it can manage and control the deployed application and hosting environments configurations [8, 9]. Some popular PaaS providers are GAE, Microsoft's Azure etc.

Infrastructure-as-a-Service (IaaS): In this service model, the provider delivers to user the infrastructure over the internet. With this model, the user is able to deploy and run various software's including system or application softwares. The user has the ability to provision computing power, storage, networks. The consumers have control over operating systems, deployed applications, storage and partial control over network. The consumer has no control over underlying infrastructure [8, 10]. Some important IaaS providers are GoGrid, Flexiscale, Joyent, Rackspace etc.

C. Cloud Deployment models

Cloud systems can be deployed in four forms such are private, public, community and hybrid cloud as per the access allowed to the users and are classified as follows:

Private cloud-

This deployment model organization and is exclusively used by their employees at organizational level and is managed and controlled by the organization or third party. The cloud infrastructure in this model is installed on premise or off premise. In this deployment model, management and maintenance are easier, security is very high and organization has more control over the infrastructure and accessibility [8, 10].

Public cloud-

This deployment model is implemented for general users. It is managed and controlled by an organization selling cloud services. The users can be charged for the time duration they use the services. Public clouds are more vulnerable to security threats than other cloud models because all

the application and data remains publicly available to all users making it more prone to malicious attacks. The services on public cloud are provided by proper authentication [8, 10].

Community cloud-

This cloud model is implemented jointly by many organizations with shared concerns viz. security requirements, mission, and policy considerations. This cloud is managed by one or more involved organizations and can be managed by third party. The infrastructure may exist on premise to one of the involved organization or it may exist off premise to all organizations [8, 10].

Hybrid cloud-

This deployment model is an amalgamation of two or more clouds (private, community, public or hybrid). The participating clouds are bound together by some standard protocols. It enables the involved organization to serve its needs in their own private cloud and if some critical needs (cloud bursting for load balancing) occur they can avail public cloud services [8, 10].

III. RESEARCH ISSUES

The existing computing paradigms viz. distributed computing, SOA, networking etc. are building blocks of cloud computing. There are numerous issues associated with theses computing paradigms and some new challenges emerged from cloud computing are required to be addressed properly in order to realize the cloud to its full extent. Current cloud adoption is associated with numerous challenges and 3 depicting the specific business risk of adopting cloud services and biggest barriers. Therefore, these issues must be addressed in order to provide high quality services to the users while complying with the service provider's needs. The issues can be organized into several different categories varying from security, protection, identity management, resource management, power and energy management, data isolation, availability of resources, heterogeneity of resources. Although, there are several issues that demand attention but the following could be treated as of prime concern [11-14].

A. Performance-

The cloud must provide improved performance when a user moves to cloud computing infrastructure. Performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources like disk space, limited bandwidth, lower CPU speed, memory, network connections etc. Many times users prefer to use services from more than one cloud where some applications are located on private clouds while some other data or applications being on public and community cloud. The data intensive applications are more challenging to provide proper resources. Poor performance can results in end of service delivery, loss of customers, reduce bottom line revenues etc. [2, 11, 13].

B. Security-

The critical challenge is how it addresses security and privacy issues which occur due to movement of data and application on networks, loss of control on data, heterogeneous nature of resources and various security policies. Data stored, processing and movement of data outside the controls of an organization poses an inherent risk and making it vulnerable to various attacks. The security threats can be of two types such are internal and external. The external risk is posed by various persons and organizations e.g. enemies or hackers that do not have direct access to the cloud. The internal security risk is a well-known issue which can be posed by organizational affiliates, contractors, current or former employees and other parties that have received access to an organization's servers, networks and data to facilitate operations. Cloud computing poses privacy concerns because the service providers may access the data that is on the cloud that could accidentally or deliberately be changed or even removed posing serious business trust and legal consequences [8, 11-14].

C. Reliability and Availability-

Any technology's strength is measured by its degree of reliability and availability. Reliability denotes how often resources are available without disruption (loss of data, code reset during execution) and how often they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time. One way to achieve reliability is redundant resource utilization. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration to the time it takes for these resources to be provisioned. Regardless of employing architectures having attributes for high reliability and availability, the services in cloud computing can experience denial of service attacks, performance slowdowns, equipment outages and natural disasters. Data shows that some of the current cloud computing providers have some frequent outages last year. e.g Amazon EC2 outage. In order to remove FUDD (fear, uncertainty, doubt, and disinformation), probably the reliability, availability and security are the important and prime concern to an organization. Therefore, the level of reliability and availability of cloud resources must be considered as a serious issue into the organization's planning to set up the cloud infrastructure in order to provide effective services to consumers [19].

D. Virtualization-

Virtualization is the creation of a virtual version of a storage device, an operating system, a server or network resources. The virtualization divides the resource into multiple execution environments and hides the physical characteristics of computing resources to simplify the way in which other systems, applications or end users interact with those resources. Virtualization is used in two forms are Type 1 hypervisors / Bare-Metal Virtualization and Type2 hypervisors / OS virtualization. Virtualization is one of the key technology in order to make it possible to realize the cloud computing. Virtualization realization typically enables consumers to migrate their computation and data to a remote location with some varying impact on performance. There are numerous benefits of virtualization which could not otherwise be achieved. However, virtualization provides many benefits to users, while on the other hand it poses many challenges to cloud computing. It has many critical issues to be address viz. VM sprawl challenges, workload characterization of VMs, security issues in hypervisor based cloud communication, Live migration security, unnecessary migration to a private cloud etc. Virtualization makes infrastructure management more complex, and massive automation is required in order to support the key aspects such as automation, on-demand and elasticity requirements.

E. Scalability and Elasticity-

Scalability and elasticity are the most amazing and unique features of the cloud computing. These features provide users to use cloud resources being provisioned as per their need in unlimited amount as required. Scalability can be defined as the ability of the system to perform well even when the resources have been scaled up. Elasticity, on the other hand, is the ability to scale resources both up and down as and when required. Elasticity goes one step further, though, and does also allow the dynamic integration and extraction of physical resources to the infrastructure. The elastic cloud computing means that allocation of resources can get bigger or smaller depending on the requirement. Elasticity enables scalability— which means the system can easily scale up or down the level of services to which the user has subscribed. Scalability can be provided in two ways- horizontally and vertically whereby horizontal scalability (Scale Out) refers to addition of more nodes to the system such as adding a new computer to an existing service provider system while vertical scalability (scale up) refers to addition of resources to a single node in the system, typically involving the addition of memory or processors to a single computer [19].

F. Bandwidth Cost -

High speed communication channels work as a backbone of cloud computing. With cloud

computing, business gets the ability to save money on hardware and/or software but still requires spending more on the bandwidth. It is almost impossible to fully exploit the services of cloud computing without high speed communication channels. Migration to cloud almost removes the up-front cost, while it increases the cost of data communication on network i.e. the cost involved in transfer of data to and from the private and other clouds [17]. This problem is prominent if consumer application is data intensive and the consumer's data is distributed amongst a number of clouds (private/public/community). Cloud computing provides lesser cost for CPU intensive jobs than data intensive jobs with gray's argument ―Put the computation near the data‖ still applicable for data intensive jobs still finding relevance [18]. In other words, data intensive applications can perform better being employed on private cloud rather than public/hybrid cloud.

G . Resource Management-

Resources management can be consider at various levels viz. hardware, software, virtualization level with performance, security and other parameters being dependent on the management and provisioning of resources. It includes the management of memory, disk space, CPU's, cores, threads, VM images, I/O devices etc. Resource provisioning can be defined as allocation and management of resources to provide desired level of services. Job scheduling is a type of resource provisioning where jobs execution order is established in order to finish job execution to optimize some parameters viz. turnaround time, response time, waiting time, throughput and resource utilization. Since cloud computing is a combination of many existing technologies, existing job scheduling strategies are eligible to be applied on cloud system. The major issues of job scheduling on cloud systems are partitioning of jobs into parallel tasks, interconnection network between clouds or processors, assigning priority to jobs and selection of processors or cloud to allocate the job(s), job flexibility, level of pre-emption supported, workload characteristics, memory allocation, task execution monitoring, recourse allocation requirements, topology, nature of the job, effect of existing load, load balancing, parallelism, job migration policy, redundant Resource selection, synchronization, communication overheads, job pre processing requirements etc. The job scheduling is one of critical process that must be decided very carefully and wrong selection of scheduling strategy can lead to devastating effect on performance leading to wastage of resources while falling to meet Quality of Service (QoS) standards.

Whatever, various issues and challenges of cloud computing have been taken up in this section still there are many other compelling issues that needs to be considered. Some of these like capacity planning, management of additional and remaining resources, management of automation of resources, costing model, Service Level Agreement (SLA) etc. are also there demanding an early attention. These issues should not be considered as road blocks in the pursuit of cloud computing, it is rather important to give serious consideration to these issues and explore the possible ways out before adopting this technology.

CONCLUSION

Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

[1] E. Anderson et al., Forecast overview: Public cloud services, worldwide, 2011-2016, 4Q12 Update, Gartner Inc., February 2013.

[2] IBM, Google and IBM announced university initiative to address internetscale computing challenges, October-2007.

[3] S. Lohr, Google and I.B.M. join in Cloud computing research, October2007.

[4] IBM, ―IBM introduces ready-to-Use Cloud computing‖, November-2007

[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, Cloud computing and emerging ITplatforms: Vision, hype, and reality for delivering computing as the 5th utility‖, Future generation computer systems, vol. 25, no. 6, pp. 599–616, June 2009.

[6] J. Geelan, Twenty one experts define cloud computing, August 2008. Article available at http://virtualization.syscon. com/node/612375.

[7] L. Badger, T Grance, R. P. Comer and J. Voas, DRAFT cloud computing synopsis and recommendations, Recommendations of National Institute of Standards and Technology (NIST), May-2012.

[8] D. A. Menasce and P. Ngo, Understanding cloud computing: Experimentation and capacity planning,‖ in Proc. of computer measurement group conf., pp. 1-11, December 2009.

[9] IBM Global Services, Cloud computing: defined and demystified explore public, private and hybrid cloud approaches to help accelerate innovative business solutions, April2009.

[10] Y. Ghanam, J. Ferreira and F. Maurer, ―Emerging issues & challenges in Cloud-A hybrid approach‖, Journal of software engineering and applications, vol. 5, no. 11, pp. 923-937, November 2012.

[11] M. A. Vouk, ―Cloud computing – Issues, research and implementations‖, Journal of computing and information technology, Vol. 16, no. 4, pp. 235-246, June- 2008.

[12] T. Dillon, C. Wu and E. Chang, ―Cloud computing: Issues and challenges‖, 24th IEEE International Conference on Advanced Information Networking and Applications. pp. 27-33, 2010.

[13] European CIO Cloud Survey, Addressing security, risk and transition, May -2011.

[14] Energy Star, Report to congress on server and data centre energy efficiency, Public Law 109-431, U.S. Environmental Protection Agency, August - 2007.

[15] J. Hamilton, ―Cooperativeexpendablemicro-slice servers(CEMS): Low cost, low power servers for internet-scale services‖, Proc. 4th Biennial Conf. Innovative Data Systems Research (CIDR), Jan 2009.