International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.92.04

A Study of Cloud Computing with its Risks Factors and Security Issues

Smt. Kirti Dinkar More
Department of Computer Science
M. V. P's K. T. H. M. College, Nashik
India

Abstract— nowadays, computing technologies are growing rapidly. Cloud computing is the technology used widely today due to its benefits. The most prominent benefit of cloud is cost saving. Cloud has main three roles- developer, provider and customer. Virtualization is an important component of cloud computing. Now it is getting more attention from businesses. Virtualization means separation of underlying hardware resources from provided resources. By using virtualization, two or more operating systems might run in the single machine with each having its own resources. Multitenancy is the concept in cloud which gives shared access of common resources to group of people. This paper reviews the cloud computing with its architecture, cloud service delivery models and cloud deployment models. There are some risks factors and security concerns in cloud computing, as given in last section of this paper.

Keywords—Cloud computing, Vitualization,cloud security, cloud risks, cloud architecture, multitenancy

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm that provides ever-present access to shared pools of configurable system resources and different services that can be swiftly provisioned with minimal effort and cost, over the Internet. Sharing of resources is the important concept in cloud computing. It provides on demand service delivery to customers reducing the expenditure on large capital outlays.

During the 1960s, the initial concepts of time-sharing became popularized via RJE (Remote Job Entry). Since 2000, cloud computing has come into existence. In August 2006, Amazon introduced its Elastic Compute Cloud. In April 2008, Google released Google App Engine in beta. Thereafter till today the cloud is world-famous. The name cloud computing was stimulated by the cloud symbol which is frequently used to represent the Internet in pictorial representation. Virtualization is the key to cloud computing, since it is the technology allowing the creation of an intelligent abstraction layer which hides the complexity of underlying hardware or software and used to provide the essential cloud characteristics of location independence, resource pooling and rapid elasticity. Multitenancy is vital the term in cloud computing refers to resource access with single instance serves multiple tenants. A tenant is a group of users who share a common access with specific privileges to the software instance. Security failure when using cloud services leads to high expense on security and may result in harm to business and its data, where the benefits of cloud computing losses. When using cloud computing customer must understand benefits and risks associated with cloud computing, also the customer must have clear understanding of expectations from service provider. Cloud services are provided at different levels like Saas, Paas, Iaas through different cloud deployment models such as private, public, hybrid, community cloud. Nowadays due to wide use of internet, data size is increasing and people are using cloud data centers for storing large data, instead of spending on storage devices needed for it. Trust is the major factor in cloud computing, as customer has to trust on service provider for storing data and using services from cloud.

II. CLOUD ARCHITECTURAL MODEL

Cloud architecture depicts the various functional modules in cloud computing environment. Figure 1 illustrates the three operational roles as:

1. *Cloud service provider*- Creates services and responsible for making services available to consumer and also maintenance of services.
2. *Cloud service consumer*- It is an organization or business or individual who request and contract with providers for services. Consumer pay for service usage and also responsible for service selection and its administration such as managing identities.
3. *Cloud service developer*- Design and implements the components of service. Service template is used by developer to describe the service. Developer interacts with cloud service provider to deploy the service components.

Consumer work with SLA (Service Level Agreement), which defines the policy that a cloud service provider allows per consumer and specifies how resources provided for consumer. In service provider part lowest layer of stack is hardware and on the top of it virtualization layer, OS or Kernel sits. The virtual image management manages virtual images used in the cloud which are used in virtual applications.

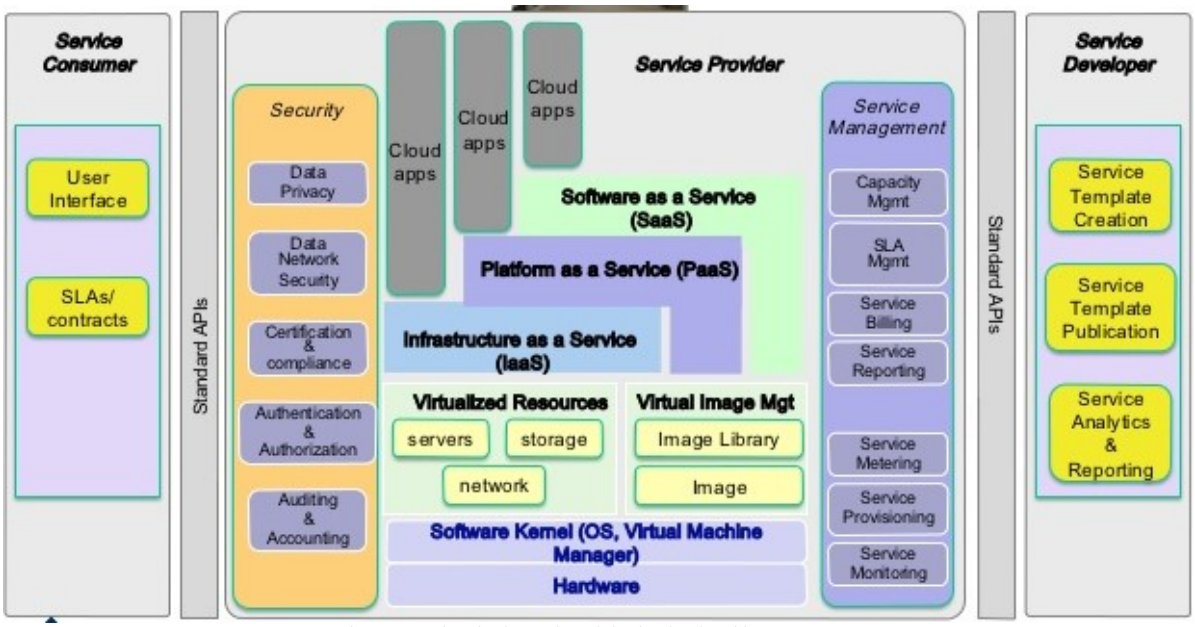

Fig. 1: Functional roles and modules in cloud architecture

A. Virtual Machine

In cloud computing virtualization Virtual Machine plays vital role. A virtual machine (VM) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination. The end user has the same experience on a virtual machine as they would have on dedicated hardware.

B. Cloud Service Delivery Models

The IaaS (Infrastructure as a Service) model –It is at lowest layer and provides infrastructure components to clients. Components may include virtual machines, storage, networks, firewalls, load balancers, and so on. With IaaS, clients have direct access to the lowest-level software in the stack – that is, to the operating system on virtual machines, or to the management dashboard of a firewall or load balancer. Currently the most prominent example of IaaS is Amazon Web Service, whose Elastic Compute Cloud (EC2) and simple Storage services (S3) are the products for computing and storage services.

The PaaS (Platform as a Service) model- It is between IaaS and Saas. PaaS refers to an environment where developers build and run an application platform in cloud and delivers a pre-built application platform to the consumer. Consumer needn't have to manage underlying infrastructure for their applications. PaaS automatically scales and provisions required infrastructure components depending on application requirements. PaaS consists of infrastructure software which includes a database, middleware and development tools for delivering web applications and services from internet. PaaS allows consumers to develop new applications using APIs deployed and configured remotely. Google AppEngine is a popular PaaS provider.

The SaaS (Software as a Service) model- It is an on demand application delivery model built upon the underlying IaaS and PaaS layers. It provides ready online software solutions. SaaS applications are owned, managed and delivered by one or more software service providers. SaaS application examples include SalesForce.com that offers CRM applications for sales, marketing and customer service .

C. Cloud deployment Models

Based on the differences in the deployment model, cloud services can be delivered in four principal ways: public cloud, private cloud, hybrid cloud and community cloud.

A. Public Cloud- A public cloud refers to a cloud service delivery model in which a service provider makes massively scalable IT resources, such as CPU and storage capacities, or software applications,

available to the general public over the Internet. Public cloud services are typically offered on a usage-based model. Public cloud is the first deployment model of cloud services to enter the IT industry's vocabulary. The concept of public clouds has clearly demonstrated the long-term potential of the cloud computing model.

B. *Private Cloud*- Private cloud, in contrast, represents a deployment model where enterprises (typically large corporations with multi-location presence) offer cloud services over the corporate network (can be a virtual private network) to its own internal users behind a firewall-protected environment. Recent advances in virtualization and data center consolidation have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their customers within these corporations. Private clouds allow large corporations to benefit from the "resource pooling" concept associated with cloud computing and their very own size, yet in the mean time addressing the concerns on data security, corporate governance, government regulation, performance, and reliability issues associated with public clouds today.

C. *Hybrid Cloud*- While public and private clouds represent the two ends of the cloud computing spectrum in terms of ownership and efficiency of shared resources – and each is finding acceptance in accordance to the services offered and customer segments targeted – a third deployment model of cloud computing, the hybrid cloud model that blends the characteristics of public and private clouds, is emerging. A hybrid cloud is a deployment model for cloud services where an organization provides cloud services and manages some supporting resources in-house and has others provided externally. For example, an organization might store customer data within its own data center and have a public cloud service, such as Amazon's EC2, to provide the computing power in an on-demand manner when data processing is needed. Another example is the concept of "public cloud as an overflow for private clouds" where an IT manager does not need to provision its enterprise private cloud for the worst-case workload scenario (doing so will certainly defeat the economics of a private cloud), but to leverage a public cloud for overflow capacities to move less-mission-critical workloads on and off premise dynamically and transparently to accommodate business growth or seasonal peak load demands.

D. *Community Cloud*- In this model, the cloud provider provides cloud infrastructure to many organizations that forms community that shares mission, security requirements, compliance consideration, or policy. This infrastructure is to be used exclusively for their uses and needs. The owner, manager, and operator of this cloud could be one of organizations, a third party, or the organization and third party together. This Community cloud could be on premises or off premises.

III. VIRTUALIZATION

Cloud computing is aggregation of different technologies and virtualization is one of them. Virtualization is the method of creating a software-based i.e. virtual representation of resource rather than a physical one. Virtualization can apply to different resources like applications, servers, storage, and networks and is the single most effective way to reduce IT expenses while boosting efficiency and agility for all size businesses. Server Virtualization is a way of making a physical computer function as if it were two or more computers where each non-physical or virtualized computer is provided with the same basic architecture as that of a physical computer. With virtualization, you can make one physical resource look like multiple virtual resources. Server virtualization is most commonly implemented with hypervisor technology. *Hypervisors* are software or firmware components that can virtualizes system resources

There are two types of hypervisors:

- Type 1 hypervisor/bare metal hypervisor
- Type 2 hypervisor/hosted virtualization

Type 1 hypervisors run directly on the system hardware.

Type 2 hypervisors run on a host operating system that provides virtualization services, such as I/O device support and memory management.

Virtualization supports isolation and gives the way for multitenancy.

Benefits of virtualization

Virtualization can increase IT agility, flexibility, and scalability with cost savings. Task get deployed faster, increasing performance, availability. Additional benefits include:

- Reduce capital and operating costs.
- Minimize or eliminate downtime.
- Increase IT productivity, efficiency, agility and responsiveness.
- Provision applications and resources faster.
- Enable business continuity and disaster recovery.
- Simplify data center management.
- Build a true Software-Defined Data Center

IV. MULTITENANCY

In cloud environment network, storage, virtual servers and applications need to be efficiently shared between clients. High degrees of multitenancy over large number of platforms are needs for cloud computing to achieve the envisioned flexibility of reliable services, cost benefits and efficiencies due to economy of scale. Multitenancy is the capability to service multiple clients from a shared common hosting environment by sharing same physical instance and version of cloud application. To achieve multitenancy multiplexing of virtual machines execution is done from different users on same physical server. The multitenant style of interaction allows one tenant to customize application's interface and business logic without offering the functionality or availability of application for all other tenants. Multitenancy offers several advantages to both cloud clients and providers. From client perspective it allows them to operate in virtual isolation from one another while from provider perspective it offers tremendous economy of scale. In fact from service provider point of view multitenancy is a technical solution that can optimize resource utilization and reduce capital cost.

V. CLOUD SECURITY AND RISKS

The impact of cloud computing on security is intense. Service provider when deploy any service to cloud environment, it's a need to provide secure isolation, with providence of benefits of shared resources. The security and availability of general cloud services is dependent upon security of basic API's. from authentication and access control to encryption and activity monitoring, these interface must be designed to protect against both accidental and malicious attempts to avoid policy. Furthermore organizations and third parties often build upon these interfaces to offer value added services to their customers. This introduces complexity of a new layered API which also increases risk as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

Inside cloud it is difficult to locate physical location of stored data, where risk arrives.

Security measures might be hidden behind layer of abstraction and this lack of visibility can create number of security and compliance issues.

According to Cloud Standards Customer Council (CSCC), there are number of security risks associated with cloud computing as follows:

- Cloud service agreements may not offer a commitment to resolve issues occurring in public cloud deployment in which customers give up control to the cloud provider over a number of issues that may affect security, thus leaving gaps in security defenses.
- Responsibility of security may be split between the provider and the customer and if there is a failure to allocate responsibility clearly, some important parts will might be uncovered from security.
- Users in public cloud include employees, contractors, partners and customers. Strong authentication and authorization becomes a critical concern.
- Multi-tenancy and shared resources are defining characteristics of public cloud computing. Data in cloud must be held securely in order to protect it when multiple customers use shared resources. This risk involve is c the failure of mechanisms separating the usage of storage, memory, routing and even reputation between tenants.
- The cloud customer's investment in achieving certification (e.g., to demonstrate compliance with industry standards or regulatory requirements) may be lost if the cloud provider cannot provide evidence of their own compliance with the relevant requirements, or does not permit audits by the cloud customer. The customer must check that the cloud provider has appropriate certifications in place.
- Notification rules must be added in cloud service agreement, so that, detection, reporting and subsequent management of security breaches by cloud provider can be informed to customer within time.
- Customer uses a set of software interfaces or APIs to manage and interact with cloud services. The security and availability of cloud services is dependent on the security of APIs
- Traditionally, applications have been protected by security solutions based on a clear separation of physical and virtual resources, and on trusted zones. With the delegation of infrastructure security responsibility to the cloud provider, organizations need to rethink perimeter security at the network level, applying more controls at the user, application and data level. The same level of user access control and protection must be applied to workloads deployed in cloud services as to those running in traditional data centers. This requires creating and managing workload-centric policies as well as implementing centralized management across distributed workload instances.
- Here, the major concerns are exposure or release of sensitive data as well as the loss or unavailability of data. It may be difficult for the cloud service customer (in the role of data controller) to effectively check the data handling practices of the cloud provider. This problem is exacerbated in cases of

multiple transfers of data, (e.g., between federated cloud services or where a cloud provider uses subcontractors).

- Damage caused by the malicious actions of people working within an organization can be substantial, given the access and authorizations they enjoy. This is compounded in the cloud computing environment since such activity might occur within either or both the customer organization and the provider organization.
- Business failure of the provider could render data and applications essential to the customer's business unavailable over an extended period.
- Service unavailability could be caused by hardware, software or communication network failures.
- Dependency on proprietary services of a particular cloud service provider could lead to the customer being tied to that provider. The lack of portability of applications and data across providers poses a risk of data and service unavailability in case of a change in providers; therefore it is an important if sometimes overlooked aspect of security. Lack of interoperability of interfaces associated with cloud services similarly ties the customer to a particular provider and can make it difficult to switch to another provider.
- The termination of a contract with a provider may not result in deletion of the customer's data. Backup copies of data usually exist, and may be mixed on the same media with other customers' data, making it impossible to selectively erase. The very advantage of multi-tenancy (the sharing of hardware resources) thus represents a higher risk to the customer than dedicated hardware.
- Some enterprise users are creating a "shadow IT" by procuring cloud services to build IT solutions without explicit organizational approval. Key challenges for the security team are to know about all uses of cloud services within the organization (what resources are being used, for what purpose, to what extent, and by whom), understand what laws, regulations and policies may apply to such uses, and regularly assess the security aspects of such uses.
- Security concern at IaaS level is securing virtual images. These virtual images must be taken from trusted third parties or it must be own image. Images must be hardened and standard images should be used for instantiating virtual machines in public cloud.
- Inter host communication in cloud environment must be secured. Securing communication depends on mode of message exchange. For synchronous communication, such as point-to-point network channel level security is important. For asynchronous communication, message based security is needed to protect the sensitive information while data is in transit.
- In cloud as numbers of different users are going to share common resources, identity, access and key management are the vital factors for providing security against unauthorized access to services and data. Cloud environment must support federated identity management facilities.
- Customer should expect to see a report of cloud provider's operations by independent auditors. The level of access to essential audit information is a key consideration of contracts and SLA terms with any cloud provider. Cloud provider should offer timely access to audit events, logs and report information relevant to customer specific data or applications.
- For IaaS, more responsibility of security is likely to be with customer. Ex. Encryption.
- For SaaS, , more responsibility of security is likely to be with provider, as there is not direct control of customer on stored data and application code.
- For PaaS, Security can be shared between in customer and provider with transparency and trust.

VI. CONCLUSION

Cloud computing is widely used technology today as it is giving more benefits as compared to traditional computing approach. However as each technology as pros and cons, in cloud risk and security are the major concerns ,since these services are provided over the network from remote locations and data is exchanged through these services and stored on network, whose location might be unaware to customer. For the customers who have little skilled security personnel cloud computing is a boon. Also, if providers commitment is trustworthy, cloud computing is best to use.

REFERENCES

[1] Jon Brodkin , Network World, " Gartner: Seven cloud-computing security risks," July 02, 2008

[2] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore,"Cloud Computing Security" ,IJRITCC,volume 1 issue 1, ISSN 2321 – 8169.

[3] Cloud Standards Customer Council, " Security for Cloud Computing Ten Steps to Ensure Success Version 2.0 " , March, 2015

[4] V.Rakesh Goud, Dr. J. Srinivasa Rao," Data Integrity Constraints in Cloud Computing",ijdcst, Volume-1, Issue-V, Issn-2320-7884 (Online), Issn-2321-0257 (Print).

[5] *Sean Carlin,Kevin Curran,"* Cloud Computing Security", International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011.

[6] Sultan Aldossary, William Allen," Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", *IJACSA,* Vol. 7, No. 4, 2016.

[7] Dimitrios Zissis , Dimitrios Lekkas," Addressing cloud computing security issues", Future Generation Computer Systems 28 (2012) 583–592, www.elsevier.com.

[8] Michael P. Papazoglou ,"Web Services & SOA Principles and Technology", Second Edition.

[9] Marios D. Dikaiakos and George Pallis ,Dimitrios Katsaros,Pankaj Mehra,Athena Vakali," Cloud Computing ,*Distributed Internet Computing for IT and Scientific Research",* Published by the IEEE Computer Society.

[10] Borko Furht ,Armando Escalante Editors, "Handbook of Cloud Computing", Springer.

[11] Eugene Gorelik,Cloud computing Models, Working Paper CISL# 2013-01, January 2013

[12] https://en.wikipedia.org/