International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Cloud Computing Security

Vinutha Gogineni
Associate Professor, Cse Dept, St. Martins Engineering College

Abstract: *Resource sharing in a pure plug and play model that dramatically simplifies infrastructure planning is the promise of „cloud computing‟. The two key advantages of this model are ease-of-use and cost-effectiveness, benefits in this model offers are many aspects such as:*

•Realities and risks of the model

•Components in the model

•Characteristics and Usage of the model

Keywords

Cloud Computing, Security, Cryptography

I. Introduction

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.
Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.
The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'.
Forrester defines cloud computing as:
"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption."

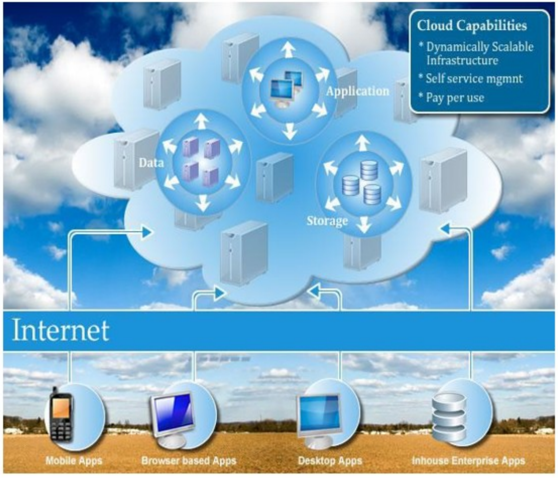


Figure 1: Conceptual view of cloud computing

II. Cloud Computing Models

Cloud Providers offer services that can be grouped into three categories.

1. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zhou, etc.

2. Platform as a Service (Pass): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc. are some of the popular PaaS examples.

3.Infrastructure as a Service (Iaas):IaaS provides basic storage and computing capabilities asstandardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, Go Grid, 3 Tera, etc.

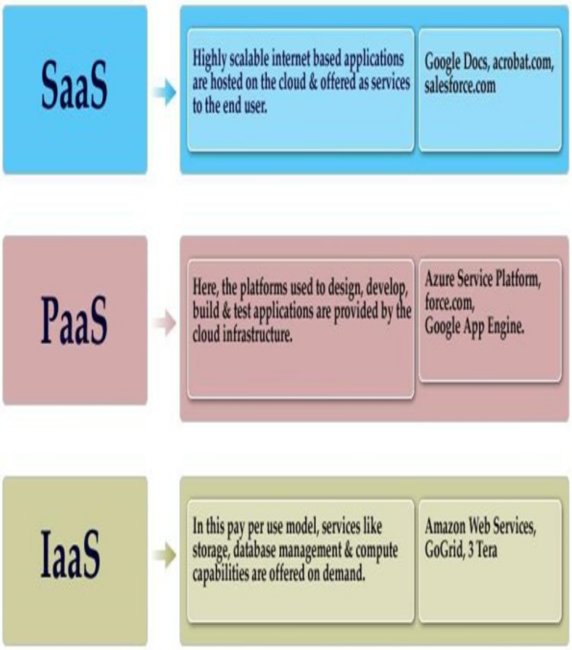

SaaS
Highly scalable internet based applications are hosted on the cloud & offered as services to the end user.
Google Docs, acrobat.com, salesforce.com
PaaS
Here, the platforms used to design, develop, build & test applications are provided by the cloud infrastructure.
Azure Service Platform, force.com, Google App Engine.
IaaS
In this pay per use model, services like storage, database management & compute capabilities are offered on demand.
Amazon Web Services, GoGrid, 3 Tera

Figure 2: Cloud models

Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud:

- On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

- Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources.

Hybrid Cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment can provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

III.Cloud Computing Benefits

1. Reduced Cost

There are many reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

2. Increased Storage

With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

3. Flexibility

This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

IV.Cloud Computing Challenges

Despite its growing influence, concerns regarding cloud computing remain. Some common challenges are:

1. Data Protection

Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

- Appropriate clustering and Fail over
- Data Replication

- System monitoring (Transactions monitoring, logs monitoring and others)
- Maintenance (Runtime Governance)
- Disaster recovery
- Capacity and performance management

3. Management Capabilities

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling‟ for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features providedtoday.

4. Regulatory and Compliance Restrictions

In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. To meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle.

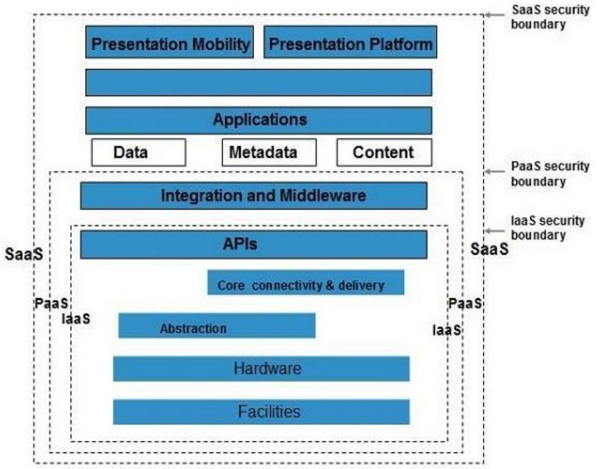
Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and breakage se vices should be employed.

Before deploying a resource to cloud, one should need to analyze several attributes about the resource such as:

1. Select which resources he is going to move to cloud and analyze its sensitivity to risk.
2. Consider cloud service models such as IaaS, PaaS, and SaaS. These models require consumer to be responsible for security at different levels of service.
3. Consider which cloud type such as public, private, community and hybrid.
4. Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud.
5. Mainly the risk in cloud deployment depends upon the service models and cloud types.

V.Security Boundaries

A service model defines the boundary between the responsibilities of service provider and consumer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the CSA stack model:



Key points to CSA model:

1. IaaS is the most basic level of service with PaaS and SaaS next two above levels of service.
2. Moving upwards each of the service inherits capabilities and security concerns of the model beneath.
3. IaaS provides the infrastructure, PaaS provides platform development environment and SaaS provides operating environment.
4. IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
5. This model describes the security boundaries at which cloud service provider's responsibility ends and the consumer's responsibilities begin.
6. Any security mechanism below the security boundary must be built into the system and above should be maintained by the consumer.
7. Although each service model has security mechanism, but security needs also depends upon where these services are located, in private, public, hybrid or community cloud.

Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in cloud. Here are key mechanisms for protecting data mechanisms listed below:

- Access Control
- Auditing
- Authentication
- Authorization

All the service models should incorporate security mechanism operating in all above-mentioned areas.

Isolated Access to Data

Since data stored in cloud can be accessed from anywhere, therefore to protect the data, we must have a mechanism to isolate data from direct client access.

Brokered Cloud Storage Access is one of the approaches for isolating storage in cloud. In this approach, two services are created:

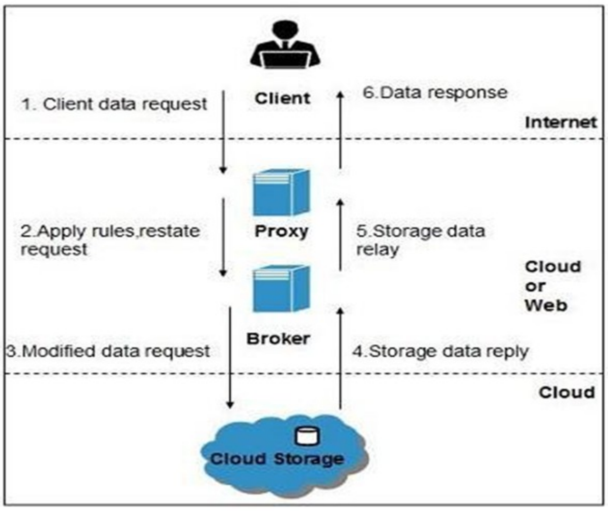
- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

VI. Workflow of the system

When the client issue request to access data:

- The client data request goes to proxy's external service interface.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally, the proxy sends the data to the client.

All the above steps are shown in the following diagram:



Encryption:

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent from data loss.

VII.Conclusion & Future Scope

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. This gallery, written for Computer Weekly, by Bob Tarzey of Quocirca aims to provide further insight.

VIII.References

[1]. Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 2011, "Parity Cloud Service: A Privacy-Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[2]. Vijaykumar Javaraiah, Brocade Advanced Networks and Telecommunication systems (ANTS), 2011,"Backupforcloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.