International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-5, February 2014

An Overview on Cloud Computing Services And Related Threats

Bipasha Mallick
Assistant Professor,
Haldia Institute Of Technology
bipasm@gmail.com

Dipankar Pramanik
CSE,AIET
prdipu@gmail.com

Abstract. Cloud computing promises to increase the velocity with which applications are deployed, increase innovation,
and lower costs, all while increasing business agility. Cloud computing is enabling the agility required by organizations to be leaders in today's ever growing global economy. It is accelerating the time to market for new products and services while reducing the costs to design, build, deploy, and support these products and services. This white paper discusses various services of cloud computing and related threats.

Keywords: Cloud Computing, Security treats, Cloud service user, Cloud service provider.

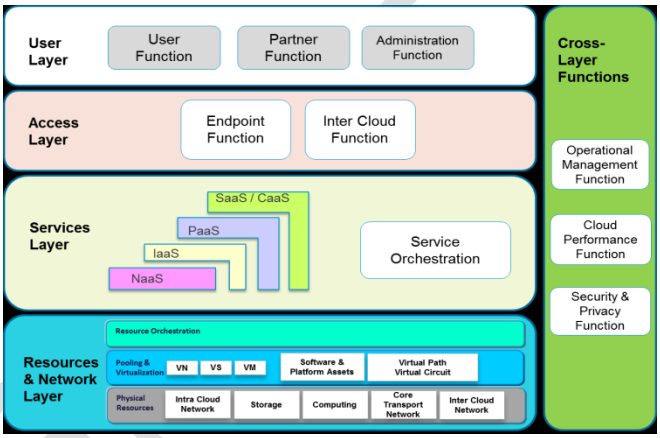
1. Introduction

Cloud computing [1][2] is a model for enabling service user's ubiquitous, convenient and 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. Cloud computing enables cloud services.

The security architecture and functions highly depend on the reference architecture, and this paper shows the reference architecture and the main security issues concerning this architecture.

2.Technical Components and services of Cloud Computing.

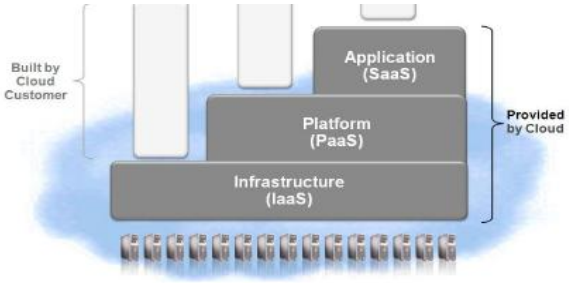
As shown in the Figure 1, key functions of a cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each



layer includes a set of functions:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services [2] Layer includes the main categories of cloud services, namely NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.

Other functions like Management, Security & Privacy, etc. are considered as cross- layer functions that covers all the layers. The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who wants to use the reference architecture may select and implement only a subset of these layers.



2.1.Infrastructure as a Service (IaaS)

One of the primary goals for companies is to reduce the amount of time and money required to procure, provision, and install new hardware systems. Companies want a faster time to market solution in order to better capitalize on market opportunities for new products and services.

Infrastructure as a Service (Iaas)[2] is one enabler that will aid in achieving this goal. With IaaS, standards and processes are established at the corporate levels which dictate a standardized infrastructure in support of a set of given business functions. From a server perspective, this includes standardized hardware, operating system, and HW/OS configurations among others. Predefined storage arrays can also be defined as part of the infrastructure, as well as standard VLAN configurations to support network isolation. Further, the management of these resources should be standardized so as to provide a single logical interface for affective change and collecting information for the infrastructure as a whole.

Once the standards are in place, governance boards are established or enhanced to support the use of the standards. With the standards and processes in place, the organization is ready to offer infrastructure to support business initiatives in a rapid, cost effective manner. In the public cloud space, Amazon E2C is a prime example of this. Companies can rapidly provision infrastructure components (CPU, OS, and Network) through E2C, and storage through S3.

Rapid deployment and cost efficiencies of these infrastructure components are supported primarily through shared infrastructure and virtualization technologies. Instead of dedicated hardware for each application, virtualization enables hardware resources to be shared and pooled across multiple applications, resulting in higher efficiency and utilization and lower costs.

Virtualization and Clustering are the two key technologies that make up Grid Computing. These technologies are complementary. Cloud Computing is NOT just server virtualization. Clustering is also an important enabler to cloud computing.

Virtualization: makes a single computer look like many computers.

- The size and power are variable/configurable.
- Virtual machines can be migrated without downtime
- Database or Middleware Clustering is also a type of virtualization. It makes many computers (or even virtual machines) look like a single resource.
- Huge databases and middleware tiers can be built using powerful, low-cost, high volume components (like blades or rack servers)
- Redundancy of clusters enables high-performance and scalability through parallel operations
- Redundancy also enables inherent high availability, as clusters can survive one or more node failures

2.2.Platform as a Service (PaaS)

The business needs IT to rapidly develop, deploy, and maintain new applications to remain competitive. Platform-as-a-Service [2] builds upon the principles of IaaS by providing an environment where applications can be built and deployed in a secure, rapid, high quality manner, all on standardized infrastructure stack. By establishing a common platform to build applications, IT is enabling the agility required by the business.

Platform-as-a-Service generally refers to an application development and deployment platform delivered as a service to developers, allowing them to quickly build and deploy a SaaS application to end-users. These platforms are often built on a grid computing architecture and include either static of virtualized database and middleware layers. They are often specific to a language or API. For example Google AppEngine is Java and Python. EngineYard is Ruby on Rails. Salesforce.com‘s Force.com is a proprietary variation of Java.

.3.Software as a Service (SaaS)

Many companies today are adopting Software-as-a-Service [2] as a model for implementing business functionality. Among other things, SaaS promises to

lower capital expenditures, decrease IT support costs, and provide better cash flow by spreading out payments for the service over the life of the contract. Businesses also like the fact that SaaS solutions tend to have a higher user adoption rate, and have the ability to scale up and down with demand. To determine whether or not SaaS is a good fit, an organization needs to consider at least three factors (Forrester 2009).

- Key Benefits: SaaS enables fast deployment, better user adoption, reduced support needs
- Key Costs:
- Risk Analysis: Cost savings, adoption Subscriptions balance with reduced implementation, upgrades, training

The potential benefits of SaaS are well advertised. All of these benefits can and have been realized by many organizations implementing SaaS based applications. It is important however, to do a full analysis of any given SaaS solution in order to determine if it is a good fit for the specific business need of the organization. For example, an organization that currently has a CRM application with a high degree of customization and integration needs may not find a competitive SaaS based solution that can fulfill their functional requirements for the application.

When examining the cost factors of a SaaS solution, both hard and soft costs must be taken into account. Soft costs include such things as training staff on the new application, and the modification the existing business processes that may need to occur based on the functionality of the new SaaS solution. Hard costs include integration requirements for the new application into existing in-house hosted systems, and the support personnel required for the new application – although studies have shown that support costs for SaaS applications can be significantly less than in-house hosted applications.

3. Threats for Cloud Service Users

3.1 Responsibility Ambiguity

Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility [3] among cloud service users and Providers may evoke conceptual conflicts.

Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

3.2 Loss of Governance

For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.

It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level [3][4] in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

3.3 Service Provider Lock-in

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.

3.4 Unsecured Cloud Service User Access

As most of the resource deliveries are through remote connection, non -protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector).

Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base

for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

3.5 Lack of Information/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

3.6 Data loss and leakage

The loss of encryption key [5] or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data center reliability; and disaster recovery can be recognized as major behaviors in this threat category.

4.Threats for Cloud Service Providers

4.1 Responsibility Ambiguity

Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities [4][5] definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissension (Especially when dealing with third parties. The cloud service provider is so me how a cloud service user).

4.2 Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

4.3 Evolutional Risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes.
However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

4.4 Business Discontinuity

The “as a service” feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows [4] thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

4.5 Supplier Lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked-in could be a lack of freedom regarding how to replace a supplier.

4.6 License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a “clouded” license management scheme which allows to pay only for used licenses may cause software use conflicts.

4.7 Bylaw Conflict

Depending on the bylaw of hosting country, data may be protected by different applicable jurisdiction. For instance, the USA Patriot Act may authorize such seizures. EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of protection guarantees. An international cloud service provider may commit bylaws of its local data-centers which is a legal threat to be taken into account.

4.8 Bad Integration

Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non - functional impacts.

4.9 Unsecure Administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment.
However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

4.10 Shared Environment

Cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

4.11 Hypervisor Isolation Failure

The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms isolating attack" could be launched on a hypervisor to gain illegal access to other virtual machines' memory.

4.12 Service Unavailability

Availability is not specific to cloud environment. However, because of the service - oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers much more possibilities for an attacker. A typical Denial of Service attack on one service may clog the whole cloud system.

4.13 Data Unreliability

Data protection includes access to data for the confidentiality as well as its integrity.
Cloud service users have concerns about how providers handle with their data, and whether their data is disclosed or illegally altered. Even if the cloud service user trust is not in the central of cloud security, it is a major marketing differentiator for a cloud service provider to advance the migration of IT system to cloud environment.

4.14 Abuse Right of Cloud Service Provider

For a cloud service user, migrating a part of its own IT to a cloud infrastructure implies to partially give control to the provider. This becomes a serious threat to cloud service user's data, notably regarding role and privileges assignment to providers.
Coupled with lack of transparency regarding cloud provider practices may conduce mis-configuration or malicious insider attack. Such security breaches will lower the provider's reputation, resulting in lower cloud service user confidence.

5. Conclusion

In any cloud service (infrastructure, software or platform) the end service provider or enterprise will control the access to the services. If these services are being hosted on the cloud, then the cloud provider (which may be different from the service provider or enterprise) also needs to protect their network from unauthorized accesses. However, since the cloud provider and the service provider or enterprise is

legally different entities, they may in certain cases need to isolate their respective user information.
In this paper, we provide Cloud Security treats in terms of Cloud Service user and provider. Based on these Cloud Security treats, the following items are main topic for Cloud Security standardization:

References

[1]"Achieving The Cloud Computing Vision", An Oracle white paper in enterprise architecture, October 2010.

[2]"Introduction to cloud computing architecture", White paper by Sun Microsystems , 1st edition, June-2009.

[3]"Security threats and countermeasures in cloud computing", Vahid Ashkorab, Seyed Reza Taghizadeh,IJAIEM, volume 1, issue 2, October 2012.

[4] Architecture for Managing Clouds White Paper (DSP-IS0102),http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf.

[5] Special Publication 800-53, Recommended Security Controls for Federal Information Systems, (2006)December.