A STUDY ON SECURITY RESPONSIBILITIES AND ADOPTION IN CLOUD

Dasprakash.G[1], Megha.J[2], K.Srinivas[3]

[1, 2]*M.Tech (Student), Computer Network and Engineering, Acharya Institute of Technology, Bangalore*
[3]*Assistant Professor, Department of Information Science and Engineering, Acharya Institute of Technology, Bangalore*
dasprakash.mtcn.12@acharya.ac.in, megha.mtcn.12@acharya.ac.in, srinivask@acharya.ac.in

Abstract

Cloud computing is one of the popular enterprise models where computing resources are made available on-demand to the user as needed. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue. cloud computing is a construct that allows you to access applications that actually reside at a location other than your computer or other Internet-connected device, most often, this will be a distant data center. In a simple, topological sense, a cloud computing solution is made up of several elements: clients, the datacenter, and distributed servers. Each element has a purpose and plays a specific role in delivering a functional cloud based application, the increased degree of connectivity and the increasing amount of data has led many providers and in particular data centers to employ larger infrastructures with dynamic load and access balancing. So this paper shall look at ways in which security responsibilities and Cloud Adoption

Keywords: *Cloud Computing, Service models, Cloud Security, Secure Cloud Adoption,*

---***---

1. INTRODUCTION

Cloud computing is a term that involves delivering a services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [1]. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples [2].

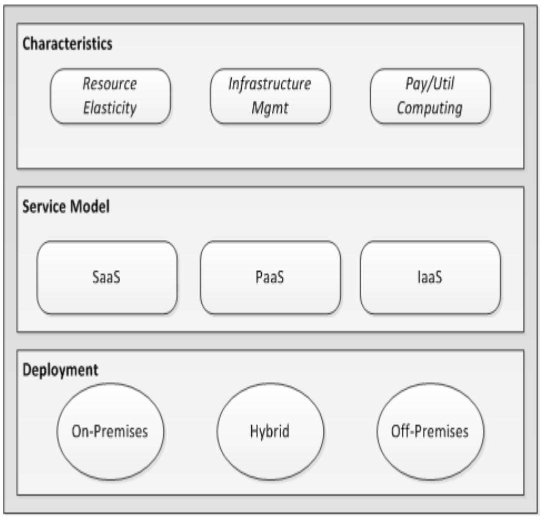


Fig 1: Cloud Computing Visual

2. SERVICE MODELS

The three most common service models for cloud computing is as follows:

2.1 Infrastructure as a Service (IaaS)

The capability provided to the customer is to provision processing, storage, networks, and other fundamentalcomputing resources where the customer is able to deploy and run arbitrary software, which can includeoperating systems and applications. The customer does not manage or control the underlying cloudinfrastructure but has control over operating systems, storage, and deployed applications [4].

2.2 Platform as a Service (PaaS)

The capability provided to the customer is to deploy onto the cloud infrastructure customer-created oracquired applications created using programming languages, libraries, services, and tools supported bythe provider. The customer does not manage or control the underlying cloud infrastructure includingnetwork, servers,operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

2.3 Software as a Service (SaaS)

The capability provided to the customer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as aweb browser (e.g., web-based email), or a program interface. The customer does not manage or control theunderlying cloud infrastructure including network, servers, operating systems, storage, or even individualapplication capabilities, with the possible exception of limited user specific application configuration settings.

3. DEPLOYMENT MODELS

How customers deploy the services from these providers also varies and generally falls into one of thefollowing three models [5].

3.1 Public

This type of cloud infrastructure is open to public or to a large industry group. The organization offering this type of cloud service generally owns, manages and operates on its own premises.

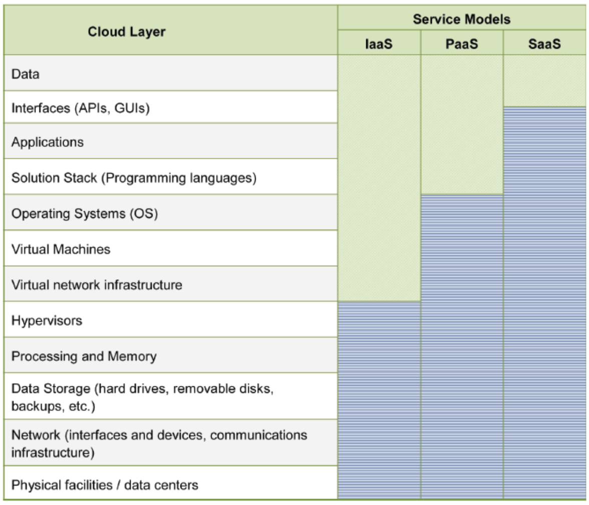
3.2 Virtual Private or On-Site Virtualized

The cloud infrastructure is operated solely for a single organization. It may be managed by the organization orby a third party and may be located on-premise or off-premise.

3.3 Hybrid IT

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remainunique entities but are bound together by standardized or proprietary technology that enables data and application portability

The following diagram from the PCI Security Standards Council provides a good example of how control is assigned between the customer and service provider in these different models:



Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data	🟩	🟩	🟩
Interfaces (APIs, GUIs)	🟩	🟩	🟩 ▨
Applications	🟩	🟩	▨
Solution Stack (Programming languages)	🟩	🟩	▨
Operating Systems (OS)	🟩	▨	▨
Virtual Machines	🟩	▨	▨
Virtual network infrastructure	🟩	▨	▨
Hypervisors	▨	▨	▨
Processing and Memory	▨	▨	▨
Data Storage (hard drives, removable disks, backups, etc.)	▨	▨	▨
Network (interfaces and devices, communications infrastructure)	▨	▨	▨
Physical facilities / data centers	▨	▨	▨

🟩	Client
▨	CSP

Fig 2: Customer and Service Provider Control

4. SECURITY RESPONSIBILITIES BY CLOUD SERVICE MODEL

To address the security needs of workloads running in the cloud, first organizations need to understand who is responsible for protecting those workloads. The roles and responsibilities transfer among the different cloud computing service models.

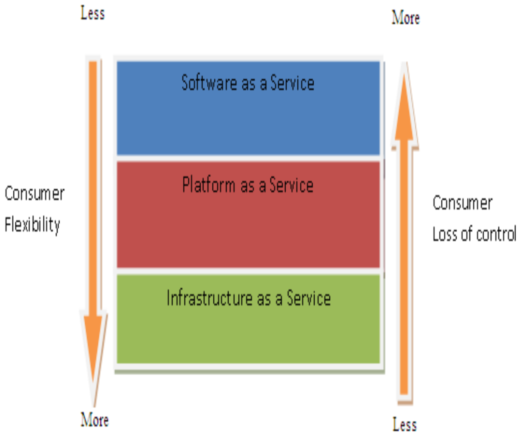


Fig 3: Security Responsibilities view basedon SPI Model

The cloud provider in an IaaS model is typically responsible for the security of the underlying infrastructure whereas in the SaaS model the cloud provider is responsible for securing the infrastructure and the application.

The providers' responsibility to provide security controls implementation increases as we move higher in the stack of a SPI model (i.e. SaaS, PaaS, IaaS) while cloud customer responsibility increases as we move lower in the stack of a SPI model.

5. SHARED SECURITY RESPONSIBILITY WITH CLOUD SERVICE PROVIDERS

While the specifics of the threats that face cloud computing implementations are not new, the way that they are mitigated and who is responsible, is different. For example, "inside threats" in a traditional IT model still apply to the cloud-computing model. But in a cloud service offering, the primary controls, e.g. administrative and physical controls, which can help mitigate this type of threat, are now provided by the cloud service provider. When an organization chooses to secure their data they implement one or more of the three types of controls.

5.1 Administrative Controls

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. When workloads are run in a traditional enterprise IT infrastructure, it is considered a trusted environment because it is either physically located within the organization's on-premise facilities and/or directly managed by the organization. Completecontrol over the networking infrastructure is exercised and includes physical access to the facility, background checks to hire new employees and implementing change management processes.

When migrating to the cloud, applications and data are now in an environment that is not controlled directly by the organization. In its place is a separately managed and maintained infrastructure hosted externally with the cloud provider. Now, instead of controlling the IT environment directly through the implementation of various controls that are defined by the organization, this is now achieved through the relationship with the cloud service provider and their associated service level agreements (SLA s).

5.2 Physical Controls

Physical controls monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. Administrative and technical controls ultimately depend on proper physical security controls. An administrative policy allowing only authorized employee access to the data center serves no purpose if there is no physical access control stopping an unauthorized employee access to the facility. In a traditional IT model the organization is responsible for implementing these physical controls to secure the computing facility, while separating the network and workplace environments and putting up environmental safeguards.

When moving to cloud services, physical controls implementation is the responsibility of the cloud provider. It is important to understanding the specific physical controls and maps them to ensure that these meet the organization's requirements.

5.3 Logical Controls

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, intrusion prevention systems, access control lists, and data encryption are logical controls.

Control over the implementation of the logical controls varies depending upon the cloud service model. In the IaaS cloud service model, you have complete control of the logical control implementations that are associated with the systems.

When choosing logical controls to protect instances, consider answering questions such as:
- Is the selected control scale based on the demand?
- Is it "cloud aware" and is it integrated with provider API's to provide an instant view when the instances scale up and down?
- Can it be extended from existing IT infrastructure to the cloud infrastructure to help enforceconsistent security policy and provide a single policy management interface?
- Does it have the capability to automatically detect new resources and install neededaccesscontrols?
- Can security policies be enforced as soon as the instance is brought online to reduce the window of exposure?

6. CLOUD SECURITY AND IAAS –A SHARED RESPONSIBILITY

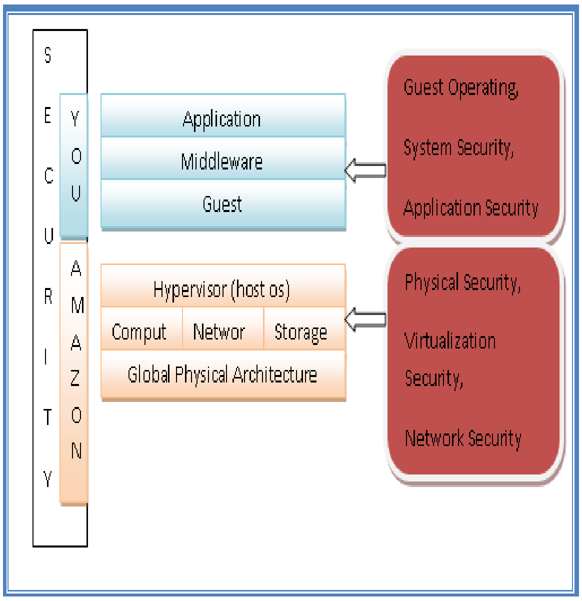


Fig 4: Shared Responsibilities Model

So for organizations leveraging cloud providers, security becomes a shared responsibility [6]. The model below lays out in more detail the various areas that organizations leveraging an IaaS are responsible for along with the associated security controls and security practices.

AWS provides security up to the hypervisor, meaning they will address security controls such as physical security, environmental security, and virtualization security The cloud customer is responsible for security controls that relate to the IT system (i.e. instance), including the guest operating system, middleware technologies and applications.

7. STEPS FOR SECURE CLOUD ADOPTION

7.1 Step 1 - Put Away Your AWS “root” Account and Use IAM to Enable Access

An AWS account is the first entity that is created when initiating a relationship with AWS. This account isconsidered a “root” accounts and provides access to all AWS resources including billing information. It isrecommended to not use this account and instead leverage the AWS IAM service to create users, groups androles to interact with AWS

To manage AWS accounts easily and with added security, it is recommended that customers create usersand groups and then assign permissions specific to their functional requirements. Assigning permissionsto allow users access to AWS is no different than the approach used in the traditional IT model i.e. assigning permissions at the group level. It is more convenient to manage permissions at the group level then individualusers. Groups can be created according to job functions (e.g. administrators, managers, testers etc.), andrelevant permissions for each group can be established and then IAM users can be assigned to those groups. When creating security policies (set of permissions) to control access to AWS resources, use the “leastprivilege” model. Following this model will require some research by the customer to correctly determine theright set of permissions that allow users to perform their job duties. Users can also leverage AWS IAM groupsto enforce the “separation of duties” security practice. Amazonprovides default built-in policy templates, whichinclude predefined permissions. These templates can be used for common use cases such as AdministrativeAccess and Read-only Access.

7.2 Step 2 - Enforce Strong Password Policy

The need for a strong password policy seems obvious but it is extremely important to prevent passwords frombeing guessed or cracked. The role that passwords play in securing customer systems is often underestimatedand overlooked. Passwords provide the first line of defense against unauthorized system access. Amazonallows the customer to define and enforce password policies such as a passwords minimum length and whetherit requires a non-alphabetic character. It is recommended that customers define and enforce strong passwordpolicy, which requires users to update their credentials at a regular interval of time e.g. 90 days.

7.3 Step 3 - Enable Multi-Factor Authentication for Privilege Users

When enforcing a strong password policy for authentication and using AWS IAM service to define authorizationlevels, consider enabling multi-factor authentication (MFA) for privilege and administrative users. AWS MFA isan additional layer of security that offers enhanced control over AWS account settings and the management oftoday, many organizations requires additional security controls when an administrative user has even greateraccess to the system. It is recommended that AWS resources be protected by configuring AWS MFA for allprivilege users. A privilege user could be a user who has access to instances with permissions that can disruptbusiness operations. For example, a privilege user is a user with access to AWS resources and permissions to terminate production instances.

By enabling MFA, extra security is added by requiring all such users to enter a unique authentication codefrom their authentication device when accessing AWS websites or services. This will prevent anyone withunauthorized knowledge of email addresses and passwords from impersonating system controls.Amazon provides two choices to enable MFA; either use of hardware base token devices from third-partyvendors or software base tokens running an AWS MFA compatible application virtual token service on asmart phone, tablet, or computer.

7.4 Step 4 - Build a Secure Base Amazon Machine Image (AMI)

When using a pre-configured operating system template aka Amazon Machine Image (AMI) or a customizedconfiguration AMI to create a virtual machine within the Amazon Elastic Compute Cloud (EC 2), the customeris responsible for performing the appropriate due diligence before using the instance to host applications. Thecustomer has full root access or administrative control over this virtual system. AWS does not have any accessrights to customer instances and cannot log into the guest OS hence cannot vouch for the integrity or securityof that instance. It is recommended that customers go through an exercise of operating system hardening toensure only required applications and services are enabled. It will help reduce the attack surface if running software services are streamlined, and instances are configureddown to the bare minimum, for example, disabling password-only access to hosts, utilizing some form of multifactor authentication to allow access to critical instances and disabling remote “root” account logins.

7.5 Step 5 - Protect the Guest Operating System

Amazon has a very robust process for implementing and managing the administrative and physical controltypes as well as securing the virtualization or hypervisor layer (Host OS), but it is the customer's responsibilityto continuously maintain and equip their AWS instances with defensive security controls and regularly assesstheir effectiveness. Amazon EC 2 provides tools such as AWS Security Groups for securing cloud-based servers. It is recommendedthat customers take advantage of these basic tools to implement basic security and then implement additionalsecurity by leveraging technology solutions such as; anti-virus, host-based firewalls, host-based intrusionprevention, file integrity monitoring, log inspection, encryption and key management solutions.

Protecting the guest operating system also means applying regular security updates and OS patches. Forexample, updating security patches for an instance hosting "always-up" web applications may be extremelydifficult and costly. To ease patch management difficulties it is recommended that customers use vulnerabilityshielding, aka "virtual patching" solutions. This will ensure that application availability goals are met without compromising security.

7.6 Step 6 - Create Restrictive Firewall Policy and Use HOST -BASED Firewalls

Amazon provides tools such as AWS (EC 2) firewall for securing cloud-based servers. Every Amazon EC 2 instance is protected by either one or more security groups which contain sets of firewall rules that specifywhich type of network traffic should be delivered to that particular instance. By default, the firewall operates ina deny-all mode and customers must explicitly open the ports needed to allow inbound traffic.

Often enough the firewall policy contains an overly permissive set of rules which create security holes. It is recommended that customers lockdown their firewall policy and only allow communication that is absolutely required. Creating a restrictive traffic management and security design on a per-instance basis is their job. For example, customers should not open remote access (RD P or SSH) to all of their production instances insteadthey should use "Bastion Hosts" to get remote access to production instances and lock down administrative access to only the "Bastion Host" from the external network.The AWS EC 2 security groups give customers basic firewall with semi-state full protection capabilities to control only incoming communications (except when using AWSVPC services). It does not prevent a server from initiating outbound communications and it does not have any logging optionsavailable for any rules that are configuredwhich could be important in some casese.g. troubleshooting and monitoring. It's recommended that customers take advantage of these security groups to restrict ingress (incoming) communications and then implement additional security by leveraging technology such as host-based firewalls to strengthen network-based security in Amazon EC 2. Customers should choose a host-based Bi-directional state full firewall with logging and alerting capabilities. This will help them create a "defense in depth" security posture.

7.7 Step 7 - Secure Your Applications and Use HOST -BASED Intrusion Prevention System

Creating a restrictive firewall policy and augmenting AWS EC 2 firewall with a host-based firewall is not enough. The traditional firewalls are designed to reduce the attack surface but they still have to allow traffic on open ports. For example, if the customer is running a web based application and their firewall policy allows traffic onport 80/443 of the application then the firewall will allow all such traffic. It lacks the intelligence to determine ifthe allowed traffic is legitimate traffic. Securing an application involves many important elements ranging fromsecure coding practices to penetration testing; it could simply mean following a practice which allows access toencrypted sensitive information only "on-demand" and not caching it into memory.

Today, customer demand requires that businesses run short development cycles with increased functionalityand rich feature sets. This can result in the release of applications that aren't properly secured which in turn could potentially harm a customer's business reputation. If an organization has developed a web applicationthat is accessible externally over the Internet, one that interacts with in-house or third party technologies, theninevitably it is susceptible to security holes. The most common web application vulnerabilities that an application could potentially be facing are SQLinjection and Cross Site Scripting (XSS) attacks. To protect an application from these attacks customers shouldconsider using web application protection technologies such as host base intrusion preventions system (HI PS).

7.8 Step 8 - File Integrity Monitoring & Logging

The next step is to ensure the continuous integrity of critical system files, application configuration files, andapplication logs. File integrity monitoring is emerging as a critical aspect of information security. It providesan early indication of a compromised system and it is required by various compliance standards such as PCI. It is recommended that customers implement file integrity monitoring and log analysis solutions to detect anyunauthorized modifications to their system components – files, registry, services, processes and critical systemfiles. Logging is another important component of information security. If logs are not taken, security incidents cannot be captured and if log and security events are not monitored, incidents cannot be detected. It isimportant to enable logging for all components that provide visibility into computing environments including; operating system, firewall, antivirus software, intrusion prevention, and application logs.
There are many solutions available to customers from host-based solutions to a MSS P. If a customer hasalready

established a monitoring solution and is collecting logs to a central server, then instances running inthe cloud are just another resource that must be monitored. Firewall configurations changes may be requiredto allow logs from the cloud environment to reach the central log-collection server on-premises in addition tosecuring the data transmission path.

7.9 Step 9 - Encrypt Sensitive Data

It is important that customers do their due-diligence and evaluate the nature, sensitivity and classification ofmoving data and accept the potential consequences of putting the sensitive data in the public cloud. Sensitivedata could be user identity and credentials as well as any personally identifiable information (PII) such as socialsecurity number. When data is moved to public cloud it may become subject to the regulations of an unknown jurisdiction so it's important that customers instruct their cloud provider to store their data in a specific region. For example, if a European company is storing the data in a US region, it becomes subject to the USA Patriot Act, which allows the US government to access data stored within US borders. Amazon does allow its customers to specify theirgeographical region preferences when using AWS services. Customers must ensure they inform Amazon oftheir preferred region for data storage, appropriate for their business.

When choosing an encryption solution to protect sensitive data "at-rest" whether a open source solution orbuilt-in OS solution, (e.g. Microsoft Encrypting File System (EFS), encrypts or a commercial solution), customersmust evaluate each solution and see what fits best with their security practice. Is encrypting individual filesenough to meet security requirements or is encryption of the entire volume required? Another importantfactor when selecting a solution is the key management and custodianship of these keys. Does the securitypractice require that the encryption keys not leave the premises? If the answer is yes, then OS built-in solutionscannot be used since they all require that encryption keys be stored on the system.

7.10 Step 10 - Conduct Vulnerability Assessment

The main objective of the vulnerability assessment (VA) is to find as much vulnerability as possible thatan attacker can use to cause damage to an organization. This vulnerability assessment can be run againstcustomer networks, systems or the web applications. There are many tools, services or a combination of bothavailable that can be used to conduct vulnerability assessments. It is recommended that a trained securityassessor, either internal or from an external company, perform this assessment even if customers are using atool to perform this exercise. A trained security assessor may find more security flaws and help customer'sfine-tunetheir existing security controls or add more controls.

7.11 Step 11 - Perform Penetration Testing

Once customers have created their desired security posture around their running instances, it is recommendedthat they evaluate the security of their systems by conducting penetration testing to safely exploit systemvulnerabilities, including OS service and application weaknesses. By conducting the vulnerability assessment, customers have identified the vulnerabilities but not the potentialconsequences if the vulnerabilities are exploited. For example, the vulnerability scan may show SQL injection vulnerability, but when they attempt to exploit it in the penetration testing, it could reveal personallyidentifiable information (PII) or data that is with-in the risk tolerance of the organization.

Penetration testing is very useful approach to validating the effectiveness of the defensive mechanisms. This exercise will help customers determine if their security controls implementation can withstand realworld attacks. Amazon understands the critical importance of penetration testing in any secure application deployment; hence it has established a policy for its customers to request permission to conduct penetrationtests. The PCI Data Security Standard, FISMA, NIST, and other legislative and industry regulations also mandate

7.12 Step 12 - Stay Involved and Maintain Security

In a traditional IT computing model, security is not a one-time exercise. The same rule applies in thecloud-computing model. Customers need to stay involved and maintain their security practice. Customerresponsibility doesn't end after selecting AWS as a vendor of choice, creating their security framework andmoving workloads to the cloud. Most likely customers will continue to migrate new workloads to the cloudor acquire new services to meet business needs. As customer requirements change, they must evaluate thechanges from a security perspective and deploy updated or new controls to provide protection. Customersneed to ensure the ongoing management aspect of security continues which may involve documenting implemented controls and monitoring changes.

CONCLUSIONS

Cloud provides attractive options to improve business and it is flexibility. But taking advantage of thesebenefits means continuing to be responsible for numerous aspects of security. While these concerns shouldnot discourage adopting cloud computing, it is necessary to understand responsibilities in this shared securitymodel and adapt security practices to this new environment.

REFERENCES

[1]. Danish Jamil, Cloud Computing Security, Department Of Computer Engineering, Sir Syed University Of Engineering &Technology,Main University Road, Karachi, Sindh-75300,Pakistan

[2]. Ren K Et Al. 2009. Ensuring Data Storage Security In Cloud Computing. [Online]Available From:Www.Ece.Iit.Edu/~Ubisec/Iwqos09.Pdf

[3]. "Service Level Agreement Definition And Contents", Http://Www.Service-Level-Agreement.Net, Accessed On March 10, 2009.

[4]. Wesamdawoud, Ibrahim Takouna and Christophmeinel, "Infrastructure As A Service Security: Challenges And Solutions," In 2010 The 7th International Conference On Informatics And Systems, 2010

[5]. Cloud Computing - A Practical Approach by Velte, Tata Mcgraw-Hill Edition (Isbn-13:978-0-07-068351-8)

[6]. "Secure Group Addresses Cloud Computing Risks", Http://Www.Secpoint.Com/Security-Group-Addresses-Cloud-Computing-Risks.Html, April 25, 2009.