UNIT 4 Securing the Cloud Cloud Computing Security

***“Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.”***

**Definition - What does *Cloud Computing Security* mean?**

* Cloud computing security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment.
* Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered (public, private or hybrid delivery model).
* Cloud security encompasses a broad range of security constraints from an end- user and cloud provider's perspective, where the end-user will primarily will be concerned with the provider's security policy, how and where their data is stored and who has access to that data. For a cloud provider, on the other hand, cloud computer security issues can range from the physical security of the infrastructure and the access control mechanism of cloud assets, to the execution and maintenance of security policy. Cloud security is important because it is probably the biggest reason why organizations fear the cloud.
* The Cloud Security Alliance (CSA), a non-profit organization of industry specialists, has developed a pool of guidelines and frameworks for implementing and enforcing security within a cloud operating environment.

# Cloud Information Security Fundamentals

Cloud Information security depends on software of cloud. Developing secure software is based on applying the secure software design principles that forms the fundamental basis for assurance.

Software Assurance is defined as the basis of for gaining justifiable confidence that software will constantly exhibit all properties required to ensure that the software and operation will continue to operate dependably despite of intentional or un-intentional faults.

In concerned with the Cloud Security, we can say that cloud software must be able to resist and contain the damage and recover to a normal state of operation as soon as possible after any attack, if unable to resist or tolerate.

Cloud must exhibit these three properties to be considered as secure:-

1. **Dependability:** software that executes predictably and operates correctly under any condition.
2. **Trust-worthiness:** contains minimum or no vulnerabilities/weaknesses and must also be resistant to malicious actions.
3. **Resilience (Survivability):** Resistant or tolerate to attack and able to recover quickly with minimum efforts.

Cloud information security fundamental include the following three security objects objectives: confidentiality, integrity and availability and four Security Services: authentication, authorization, auditing and accountability.

#### Cloud Security objectives

Confidentiality, integrity and availability are three important objectives of cloud security.

1. **Confidentiality**: confidential refers to the prevention of intentional and unintentional unauthorised disclosure of information. Confidentiality in cloud system is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption and inference.
2. **Integrity**: the concept of cloud information integrity requires that the following principle is met:
   * Modification or not made to data by any authorised personal or processes.
   * Unauthorized modification is not made to data by authorized personal or processes.
   * Data is internally and externally consistent
3. **Availability**: Availability insurance the reliable and timely access to computing resources by appropriate personal. Availability guarantees that the system is functioning properly when needed. In addition this concept guarantees that the security of cloud system is in working order.

A denial service attack is example or thread against Availability. Unavailability of service due to any reason is not acceptable beyond the acceptable downtime of maintenance.

These three objectives are collectively called CIA trade of information system security and are important pillars of cloud software assurance.

# Cloud Security Services

**Authentication** is one such technique which plays a major role in Cloud Computing security. The various possible security attacks on the Cloud Service Providers (CSP) are prevented by applying different authentication mechanisms, which verifies a user's identity when a user wishes to request services from cloud servers.

**Authorization** refers to the process of adding or denying individual user access to a computer network and its resources. Users may be given different authorization levels that limit their access to the network and associated resources. Authorization determination may be based on geographical location restrictions, date or time-of-day restrictions, frequency of logins or multiple logins by single individuals or entities. Other associated types of authorization service include route assignments, IP address filtering, bandwidth traffic management and encryption.

**Accounting** refers to the record-keeping and tracking of user activities on a computer network. For a given time period this may include, but is not limited to, real-time accounting of time spent accessing the network, the network services employed or accessed, capacity and trend analysis, network cost allocations, billing data, login data for user authentication and authorization, and the data or data amount accessed or transferred.

Examples of AAA protocols include:

* Diameter, a successor to Remote Authentication Dial-In User Service (RADIUS)
* Terminal Access Controller Access-Control System (TACACS)
* Terminal Access Controller Access-Control System Plus (TACACS+) a proprietary Cisco Systems protocol that provides access for network servers, routers and other network computing devices.

Types of AAA servers include:

* Access Network AAA (AN-AAA) which communicates with radio network controllers
* Broker AAA (B-AAA), which manages traffic between roaming partner networks
* Home AAA (H-AAA)

**Auditing:** Cloud Audit is a specification for the presentation of information about how a cloud computing service provider addresses control frameworks.

The goal of Cloud Audit is to provide cloud service providers with a way to make their performance and security data readily available for potential customers. The specification provides a standard way to present and share detailed, automated statistics about performance and security.

Standardized information makes comparisons among providers easier, reducing the resources required to assemble documentation and analyse the data. Cloud Audit is intended to benefit cloud computing providers as well. For example, the cost of responding to a potential customer's compliance controls may be minuscule for a large vendor. However, a small vendor may find it burdensome to provide that information to multiple prospective customers. With Cloud Audit, vendors can provide information once and only update when there are changes.

Cloud Audit’s development codename was A6 (Automated Audit, Assertion, Assessment, and Assurance API). According to the Internet Engineering Task Force (IETF) draft document, Cloud Audit provides “a common interface, naming convention, set of

processes and technologies utilizing the HTTP protocol to enable cloud service providers to automate the collection and assertion of operational, security, audit, assessment, and assurance information."

# Cloud Security Design Principles

For the private cloud, the key security principle that drives an effective design is that your design should seek to build a system of controls, rather than a collection of controls. This unified system of controls is more than just the individual security technologies and methodologies – each part integrates with each other to provide the overall defences.

This unified security approach would include the following design principles:

* Apply generic security best practices
* Understand that isolation is key
* Consider security as a “wrapper”
* Assume attackers are authenticated and authorized
* Assume all data locations are accessible
* Use established strong cryptographic technologies
* Automate security operations
* Reduce attack surface
* Limit routing
* Audit extensively
* Implement effective governance, risk management and compliance

## Apply Generic Security Best Practices

Private clouds use existing technologies such as virtualization and extend the infrastructure designs current in many organizations. As such, you should maintain existing security practices as part of the security design for your private cloud.

For example, you should continue to:

* Implement the principles of least privilege and defense in depth.
* Use firewalls and use separate NICs for management functions.
* Carry out penetration testing and to audit your security processes.

However, private cloud architectures introduce new potential vulnerabilities and you must modify and add to your existing design to mitigate these new threats.

## Isolation is Key

Typically, private cloud implementations use virtualization technologies to make infrastructure, platform, and software resources available to clients within the enterprise. Tenants may be other business units within the enterprise, or other sections of the IT department using private cloud resources to deliver services to client business units. Even though private cloud tenants are part of the same organization, you must ensure isolation of their resources. For example, confidential human resources data

must not be generally accessible even though the human resources systems could be running on the same physical server as the company intranet.

It is not just an issue of simple confidentiality. In the IaaS, PaaS, and SaaS service delivery models, you may not know which tenant services are co-hosted on the same physical devices at any particular time. In consequence, a problem in one tenant service could affect the performance, network connectivity, or network availability of other tenant services on the same physical hardware. Your design must ensure isolation between tenants in both the physical and virtual environments that make up the private cloud.

If your private cloud is partially or wholly hosted by a third party, then you must be assured that the cloud infrastructure used by the third party also guarantees isolation, both between your services and between your services and any other organization's services that the third party also hosts.

## Consider Security as a Wrapper

You should consider security as a “wrapper” around all elements of your private cloud architecture. The private cloud reference model in figure 1 shows how security concerns are relevant to all elements in all layers and stacks within the architecture:

* Infrastructure
* Platform
* Software
* Service delivery
* Management

A private cloud typically hosts services in virtualized environments, with multiple services co-located on the same physical device. The security wrapper functions must be applied to both the physical and virtual environments because in a private cloud architecture you cannot assume that by protecting the physical environment you automatically protect the virtual environment, and vice versa.

If an attacker gains access to the physical infrastructure, they can disrupt not only the infrastructure, but also potentially gain access to the virtualized resources hosted in the cloud. If attackers manage to compromise a virtualized environment, they can potentially use the compromised environment as a platform to attack other virtualized environments within the cloud or to attack the infrastructure.

Although your design should consider security as a wrapper around all elements in the architecture, your design should take into account the possibility that responsibility for security may be split between the CSP and the tenants. For more information about this scenario, see the third paper in this series "Solution for Private Cloud Security: Service Operation."

Considering security as a wrapper should be part of your defense in depth strategy for securing your private cloud. For a more information about the private cloud reference model shown in Figure 1, see the first paper in this series "Solution for Private Cloud Security: Service Blueprint."

## Assume Attackers are Authenticated and Authorized

In the private cloud, you may delegate some of the responsibility for managing the security of the environment to the tenant. A tenant may provision resources through a self-service portal in order to run its tenant application or service in the private cloud. The cloud service provider may have little or no control over how the tenant configures and uses its virtual resources and this includes control over how the tenant grants access to its services to its end users. Because of this, you must assume that attackers can be authenticated users with authorized access to a virtual machine running in your data centre. The attacker could be an untrustworthy employee, someone using stolen credentials, or an attacker using elevated credentials.

You should consider this route of attack from within a virtual machine in your data centre in addition to more traditional attacks that may be mounted from outside your organization in an attempt to exploit weaknesses in your external defences. Attackers will now attempt to find weaknesses that they can exploit in the virtual environment.

For example, an attacker might try to gain access to the hypervisor from within the hosted virtual machine, a type of exploit known as hyper jacking.

## Assume All Data Locations are Accessible

This point closely relates to the previous point about authenticated and authorized attackers. In private cloud architectures, many data locations are exposed as services. For example, virtual machines may mount virtual hard disks from a storage resource, or they may use virtual queues, virtual tables, or virtual binary large object (BLOB) storage. A tenant may provision these resources through an automated self-service portal as part of the infrastructure or platform services provisioning process. If an attacker can gain access to a tenant's virtual environment, you must assume that they may also gain access to the tenant's data locations.

Because of this, you should consider when and how to encrypt data and how to store and manage the encryption keys that enable access to the data stored in the cloud.

## Do Not Trust Client Information

You cannot make any assumptions about the security of any of the client applications that access the tenant services hosted in the private cloud. This proviso is especially important when the tenant wants to enable broad network access to the tenant service from multiple device types and from multiple locations. Poorly designed client applications could accidently reveal credentials or keys, and may perform limited validation on the data that they send to the services hosted in the cloud. Therefore,

cloud management services and tenant services must perform their own validation of data sent from all client applications.

In contrast, you have more control over the client applications and tools that you use to manage the cloud infrastructure. For example, you may limit access to cloud management functions to client applications running on the corporate intranet, or use certificates to identify client applications. However, some cloud management operations may require calls to published APIs, which themselves may not require full validation of the data sent to the cloud and could be invoked from a custom application created by a developer.

## Use Established Strong Cryptographic Techniques

Encryption of data at rest, in transit, and during processing can help to ensure that the data is only visible to those who should be able to see it. Therefore using encryption can help to preserve the isolation of tenants' resources and help to mitigate the threat that attackers may be authenticated users with access to the locations where the application or service stores its data.

You should ensure that your infrastructure uses established, strong encryption techniques wherever it uses encryption. Tenants should also be encouraged or mandated to use established, strong encryption techniques in their own cloud-hosted applications and services.

Implementing cryptographic algorithms securely is complex and difficult. Using strong, established cryptographic algorithms and cryptographic systems rather than "rolling your own" helps to validate your approach to encryption, and makes your cryptographic processes auditable. Remember that attackers will only bother attacking the algorithm itself if they recognize it as weak – typically, they go after the keys.

## Automate Security Operations

The size of private clouds, self-service provisioning, and virtualization all combine to make it essential to automate operational activities such as collecting and correlating monitoring data, responding to security related incidents, and allocating resources to tenants to prevent denial of service situations.

A typical private cloud hosts a large number of tenant services and supports a large number of end users. To ensure effective and timely responses to security issues, you must automate those responses as far as possible.

Automated security responses rely on monitoring, so your design must include monitoring services that enable you to automatically identify and act on possible security issues. The automated response procedures must send notifications to the staff that are responsible for security and create a full audit trail of their actions. You should evaluate and review these procedures regularly.

Note that when configuring security monitoring, you must also not let yourself be swamped by security responses and turn off monitoring altogether. Better to build up a feel for what is important by enabling rules more slowly. When you have a baseline and an understanding for your environment, you can then add the automation.

If you are building your virtualization host and guest environments from standard templates or images, you should ensure that those templates and images include configuration of the monitoring on which your automated responses will rely.

Your private cloud design should include a comprehensive automation platform that will enable operational activities such as those outlined above. You should also ensure that the security monitoring and response automation can cope with cloud-based environments and with virtual machines that can be rapidly provisioned and deprovisioned.

## Reduce Attack Surface

As with all computer systems, reducing the attack surface is a key element to preventing attacks from succeeding. If the attacker only has a very small area to attempt to access, then he or she has far fewer options to find a successful exploit.

Within a private cloud environment where you are likely to be using virtualization, you must ensure that you reduce attack surface wherever possible on both host and guest computers. You should only enable the ports, services, and features that are essential to your operations. Your risk assessment should identify all unnecessary components and you should then remove or disable these components.

## Limit Routing

Anytime data transitions though the private cloud, it adds another possible place that an attacker might be able to access or tamper with that data. Your private cloud design should limit the number of nodes that data must pass through to reach its destination as a part of the overall design goal to reduce the attack surface.

For example, if a tenant is deploying a three-tier application to the private cloud, they should be able to configure the application so that the individual tiers can communicate directly with each other without the data passing through a shared broker component unless there is a specific requirement for this to happen.

Additionally, more complex routing requires more complex monitoring, and the more difficult it becomes to understand the flow of data within the already complex cloud environment.

## Audit Extensively

The cloud is a relatively new and fast changing environment that means that new usage patterns and new threats will emerge. Your security processes should be audited regularly in order to validate that the current security design includes mitigations for known threats. If not already applicable, you should consider gaining consider certifications such as ISO/IEC 27001and SAS 70 Type II.

ISO/IEC 27001 is an international standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). This International Standard can assess conformance by interested internal and external parties. For more

Statement on Auditing Standards No. 70 (SAS 70) is an international auditing standard that enables businesses that provide services to other organizations to provide an independent, trustworthy account of their internal control practices. An independent

auditor performs the SAS 70 audit and generates the resulting SAS 70 report, which the service provider supplies to its customers and clients for use when they themselves undergo auditing. For more

## Implement Effective Governance, Risk Management and Compliance

In a private cloud, because ownership of and responsibility for services hosted in the cloud is split between various parties, the SLAs between the parties must make clear where those responsibilities lie and what the different parties should expect from each other.

The set of SLAs that you must consider will depend, in part, on the particular cloud model adopted by your organization:

* If you chose to adopt a hybrid cloud model, or chose to host your private cloud with a third-party organization, then the enterprise CSP will have SLAs with the third-party cloud service provider and with the client business units within the organization. In these scenarios, the IT department is acting as a broker to deliver and manage cloud services provided by an external entity, to internal clients.
* If you are hosting the private cloud on premises, you must then negotiate SLAs between the IT department and the client business units.

If you are using a third party to provide some or all of the private cloud services in the enterprise, then you must ensure that the SLAs with the third party provider enable you to meet your SLAs with your internal clients. This requires a detailed understanding of what the third party SLAs offer in terms of security.

For example:

* How do they guarantee isolation between tenants?
* What do they guarantee in terms availability and disaster recovery?
* How do they ensure the integrity of your applications and data?
* What steps do they take to ensure the physical security of your data such as vetting employees who have access to the physical environment and hardware disposal procedures?

Regardless of whether you choose to host the private cloud externally with a third party, on premises, or adopt a hybrid approach, you will still need SLAs between the your IT department and the tenants within the organization. The on-demand, self- service attribute of the private cloud, means that there may be some delegation of responsibility for managing the security of the virtualized environment to the tenant.

In addition to the guarantees made to the tenant by the cloud service provider, SLAs may also need to specify requirements related to security that the tenant must fulfill. For example, an SLA might specify the encryption technologies that the tenant service should use to protect data, or that the tenant should use the enterprise directory for identity management through federation services provided by the CSP.

How much delegation of responsibility occurs will vary between organizations and between tenants. For some organizations, the primary motive behind adopting a private cloud model will be to make more efficient use resources by pooling them: the IT department will still deploy and manage applications and services on behalf of the client business units. In this scenario, the on-demand, self-service characteristic is not significant to the relationship between the cloud service provider and the client business unit, and SLAs will cover traditional areas such as availability, disaster recovery, and performance.

However in some scenarios, tenants will make use of the on-demand, self-service functionality of the private cloud to obtain and manage infrastructure or platform resources to run their own applications and services. In this case, the split in responsibility for security features such as identity and access management or data protection may be more complex and the SLAs must include clear definitions that are understood and agreed upon by all the concerned parties.

Scenarios that are more complex are also possible. For example, in addition to managing the private cloud infrastructure, the IT department may also commission, procure, or develop applications for other business units within the organization. In this scenario, one part of the IT department may use the on-demand, self-service capability of the private cloud to acquire infrastructure or platform services on behalf of the client business unit and also handle some or all of the ongoing management of the service on behalf of the client business unit. This arrangement creates a scenario where there are two SLAs: one between the cloud service provider and service provider sections of the IT department, and one between the service provider part of the IT department and the client business unit.

In a private cloud, all parties must have an explicit understanding of their obligations and responsibilities and agree to them. Depending on the model adopted by your organization, the list of parties involved might include:

* third-party cloud services providers
* an internal cloud-services provider
* application and software providers who are a part of the IT department and who consume private cloud services
* client business units within the organization whose applications and services are hosted in the private cloud

When you are negotiating and drafting SLAs you must ensure that:

* You cover all aspects of security for all hosted services and applications and there are no gaps in responsibility.
* Your SLAs with third party providers enable you to meet the SLAs with your tenants.

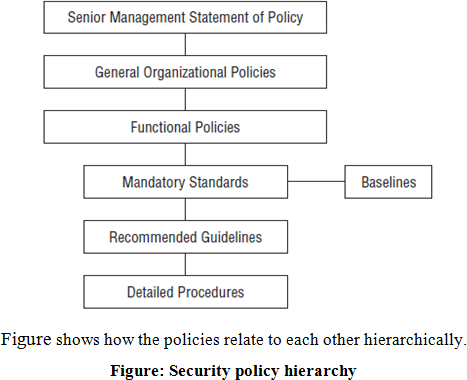
# CLOUD SECURITY POLICY IMPLEMENTATION

Security policies are the foundation of a sound security implementation. Often organizations will implement technical security solutions without first creating this

foundation of policies, standards, guidelines, and procedures, unintentionally creating unfocused and ineffective security controls.

A ***policy*** is one of those terms that can mean several things. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global information security policy.

A good, well-written policy is more than an exercise created on white paper — it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a governmental or regulatory function. A policy can also provide protection from liability due to an employee’s actions, or it can control access to trade secrets.



#### Policy Types

In the corporate world, when we refer to specific polices, rather than a group policy, we generally mean those policies that are distinct from the standards, procedures, and guidelines. Policies are considered the first and highest level of documentation, from which the lower-level elements of standards, procedures, and guidelines flow.

This is not to say, however, that higher-level policies are more important than the lower elements. These higher-level policies, which reflect the more general policies and statements, should be created first in the process, for strategic reasons, and then the more tactical elements can follow.

Management should ensure the high visibility of a formal security policy. This is because nearly all employees at all levels will in some way be affected, major organizational resources will be addressed, and many new terms, procedures, and activities will be introduced.

Including security as a regular topic at staff meetings at all levels of the organization can be helpful. In addition, providing visibility through such avenues as management presentations, panel discussions, guest speakers, question/ answer forums, and newsletters can be beneficial.

#### Senior Management Statement of Policy

The first policy of any policy creation process is the senior management statement of policy. This is a general, high-level policy that acknowledges the importance of the computing resources to the business model; states support for information security throughout the enterprise; and commits to authorizing and managing the definition of the lower-level standards, procedures, and guidelines.

#### Regulatory Policies

Regulatory policies are security policies that an organization must implement due to compliance, regulation, or other legal requirements. These companies might be financial institutions, public utilities, or some other type of organization that operates in the public interest. Such policies are usually very detailed and specific to the industry in which the organization operates.

#### Advisory Policies

Advisory policies are security policies that are not mandated but strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory. Most policies fall under this broad category.

#### Informative Policies

Informative policies are policies that exist simply to inform the reader. There are not implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.

# CLOUD COMPUTING SECURITY CHALLENGES

Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy.

Simply, if we want to understand, then

* + CSPs believe that Security is End-users’ Issue
  + Lack of Awareness about Cloud Security
  + Inconsistent Network Connection Issues
  + Lack of Proper Cloud Security Standards

Broadly, Cloud computing security challenges fall into three categories:

* + **Data Protection:** Securing your data both at rest and in transit
  + **User Authentication:** Limiting access to data and monitoring who accesses the data
  + **Disaster and Data Breach:** Contingency Planning

#### DATA PROTECTION

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.

#### USER AUTHENTICATION

Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

#### CONTINGENCY PLANNING

With the cloud serving as a single centralized repository for a company's mission- critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns. Much of the liability for the disruption of data in a cloud ultimately rests with the company whose mission-critical operations depend on that data, although liability can and should be negotiated in a contract with the services provider prior to commitment. A

comprehensive security assessment from a neutral third-party is strongly recommended as well.

Companies need to know how their data is being secured and what measures the service provider will be taking to ensure the integrity and availability of that data should the unexpected occur. Additionally, companies should also have contingency plans in place in the event their cloud provider fails or goes bankrupt. Can the data be easily retrieved and migrated to a new service provider or to a non-cloud strategy if this happens? And what happens to the data and the ability to access that data if the provider gets acquired by another company?

#### VIRTUALIZATION SECURITY MANAGEMENT

Virtualization has made a huge impact in a very short time in the IT and networking worlds and has already provided huge cost savings and returns on investments for data centres, enterprises and the Cloud. What seems to be less substantial and lagging is the understanding of virtualization and virtualized environments from a security point of view. Some people think that virtualization is more secure than traditional environments because they’ve heard of isolation between virtual machines (VMs) and because they haven’t heard of any successful attacks on hypervisors. Others think that the new virtualized environment needs security just like traditional physical environments and therefore apply the same long standing approaches to securities that are already in place. The bottom line is that the new environment is more complex, and virtualization approaches added to current networks creates a new network that needs a new approach to security. This should include traditional security as well as additional security for virtualization.

#### Security benefits due to virtualization

The following are some of the benefits to security once virtualization is introduced into the environment:

* Centralized storage used in virtualized environments prevents a loss of important data if a device is lost, stolen or compromised.
* When VMs and applications are properly isolated, only one application on one OS is affected by an attack.
* When configured properly, a virtual environment provides flexibility in that it allows

the sharing of systems without necessarily having to share critical information across the systems.

* If a VM is infected, it can be rolled back to a prior “secure” state that existed before

the attack.

* Hardware reductions that occur due to virtualization improve physical security since there are fewer devices and ultimately fewer data centres.
* Desktop virtualization can be deployed to better control the user environment. An administrator can create and control a “golden image” that can be sent down to

users’ computers. This technology provides better control of the OS to ensure that it meets organizational requirements as well as security policies.

* Server virtualization can lead to better incident handling since servers can revert

back to a previous state in order to examine what occurred before and during an attack.

* The system and network administration’s access control as well as separation of

duties can be improved as certain individuals may be assigned to only control VMs within the network while others only deal with VMs in the DMZ. You can also have certain administrators deal with Windows servers only for example, while others deal with Linux servers.

* Hypervisor software is small and not really complex and this provides for a smaller

attack surface on the hypervisor itself. The smaller the attack surface and things running, the less potential vulnerabilities.

* Virtual Switches (vswitches) don’t perform the dynamic trunking necessary to

conduct Inter-switch link tagging attacks. They also drop double encapsulated packets so double encapsulation attacks aren’t effective. Vswitches also don’t allow packets to leave their assigned broadcast domain so they nullify the multicast brute force attacks that rely on overloading switches to let packets broadcast to other VLAN domains.

* Notice that I’ve qualified a number of the above benefits with statements like “if

configured or set up properly.” Virtualization is very complex so it must be secures properly to gain the above benefits.

**Common Virtualization Attacks**

The following are some of the common, known attacks with virtualization:

* + **Denial of Service (DoS):** A successful DoS attack here can lead to a shutdown of the hypervisor. This can lead to the ability to add a backdoor to allow access to the VMs underneath the hypervisor.
  + **VM Jumping**: If a security hole in the hypervisor occurs and is found, a user

logged into one VM can hop over to another VM and gain access to it to look at information or acquire it.

* + **Host Traffic Interception**: Vulnerabilities in the hypervisor can allow for

tracking of system calls, paging files, and monitoring of memory and disk activity.

#### Recommendations and Best Practices for Secure Virtualization

**Administrator Access and Separation of Duties**

* + Provide server adman’s with on/off rights for their servers only and no others.
  + You may want to give admins the right to deploy new VMs but not modify existing VMs. Other admins can then be able to modify existing VMs but not create new ones.
  + Separate authentication should be in place for each guest OS unless there’s a good reason for two or more guest OS to share credentials.

#### Desktop Virtualization and Security

The following are five effective measures for making sure that unauthorized and unsecured virtualization doesn’t exist in the environment:

#### Update Acceptable Use Policy

Spell out the exact conditions under which virtualization software can be installed and define what approvals are required. State what software can be run and how it should be protected. Spell out the repercussions that employees can expect if they don’t follow the rules.

#### Limit the Use of VMs to the Users That Need Them

Most users won’t need VMs on their desktops. Forbid the installation of freely downloadable software on corporate desktops and laptops. Limit permissions to a small group of developers and testers for virtual tools and VMs, and help them understand that they still have to conform to corporate security policies.

#### Keep Virtualization and Security Software Up to Date

Ensure all of the VMs contain the same firewalls, anti-virus and IDS/IPS as the physical desktops and laptops.

#### Choose Security Policies That Support Virtualization

Make sure that there aren’t any known security policy conflicts with existing virtualization platforms.

#### Create and Maintain a Library of Secure VM Builds

Maintain a repository of VM builds containing all of the configuration settings, security software and patches that users can download, use and re-use.

#### Network Security

* + Disconnect any unused NICs so that there isn’t an easy way to get onto the network.
  + Make sure that the host platform that connects the hypervisor and guests to the physical network is secure by setting file permissions, putting things in place to control users and groups, and setting up logging and time synchronization.
  + Encrypt all traffic between clients and hosts, between management systems and the hypervisor, and between the hypervisor and hosts using SSL.
  + Secure IP communications between two hosts by using authentication and encryption on each IP packet.
  + Do not use default self-signed certificates as they’re vulnerable to man-in-the- middle attacks.
  + Place virtual switches into promiscuous mode for monitoring purposes and enable MAC address filtering to prevent MAC spoofing attacks.

#### Disaster Recovery

* + Maintain your production firewall, security posture and IPS/IDS at your disaster recovery (DR) site. If your firewall is disabled at the DR site, until a disaster

occurs or if the rules on the firewall are different from the main site, audit the firewall regularly.

* + Implement proper change control so that your backup site and main site are kept as identical as possible.
  + Any logging and monitoring at the DR site should be treated as if it is at your primary site.
  + Audit and PEN test your DR site separate from your main site with the same frequency and importance.
  + Any replications to your backup site should be encrypted.
  + Place a copy of your business recovery plan at your offsite location.
  + Rotate your backup media and keep it in offsite storage.

#### Auditing and Logging

* + Use centralized logging to determine whether guests have gone offline. These guests can get out of sync in regards to patches and updates. Log any VM power events (such as On, Off, Suspended or resumed), changes in hardware configurations or any login events related to those with elevated privileges. VMs that are copied, moved or deleted should also be logged.
  + Audit files should be read only and should only be read by those in an auditing role to ensure forensic integrity. Unauthorized and authorized login attempts to the audit files and other virtual resources should be logged.
  + Conduct regular audits of the environment including the virtual network, storage, the hypervisor, the VMs and the management systems.
  + Send log files securely to a remote log server.

#### Virtual Machine Security

* + Don’t create more VMs than is necessary. Keep track of all of your running VMs to track potential entry points for attacks. Limit use of VMs to critical staff only.
  + Turn off any unused VMs.
  + Unused hardware ports like USB on VMs should be disabled.
  + Use IPSec or other forms of encryption between the host and VM.
  + Security policy can be used to make sure that a new VM is not allowed to join a VM group or cluster unless it has a specific configuration and has related updates installed.
  + If users are allowed to create VMs, consider allowing them to create VMs from an authorized template.
  + A security gateway (firewall and IDS/IPS) can be employed to inspect traffic between VMs.

#### Management System

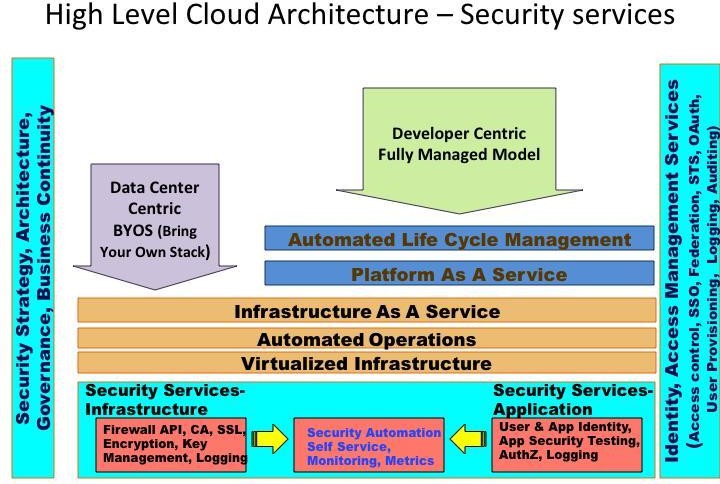
* + Do not allow a management server to be accessible from all workstations.
  + Secure your communications between management systems and the hosts to prevent data loss, eavesdropping and any chance for man-in-the-middle attacks.

Enable one or more of the available SSH, IPSec and SSL protocols for this purpose.

* + Separate management servers from database servers.
  + Backups, Configuration and Change Management, Remote Access are some other recommendations.

# Cloud Security Architecture – Plan

As a first step, architects need to understand what security capabilities are offered by cloud platforms (PaaS, IaaS). The figure below illustrates the architecture for building security into cloud services.



Security offerings and capabilities continue to evolve and vary between cloud providers. Hence you will often discover that security mechanisms such as key management and data encryption will not be available. For example: the need for a AES 128 bit encryption service for encrypting security artifacts and keys escrowed to a key management service. For such critical services, one will continue to rely on internal security services. A “Hybrid cloud” deployment architecture pattern may be the only viable option for such applications that dependent on internal services. Another common use case is Single Sign-On (SSO). SSO implemented within an enterprise may

not be extensible to the cloud application unless it is a federation architecture using SAML 1.1 or 2.0 supported by the cloud service provider.

The following are cloud security best practices to mitigate risks to cloud services:

* **Architect for security-as-a-service** – Application deployments in the cloud involve orchestration of multiple services including automation of DNS, load balancer, network QoS, etc. Security automation falls in the same category which includes automation of firewall policies between cloud security zones, provisioning of certificates (for SSL), virtual machine system configuration, privileged accounts and log configuration. Application deployment processes that depend on security processes such as firewall policy creation, certificate provisioning, key distribution and application pen testing should be migrated to a self-service model. This approach will eliminate human touch points and will enable a security as a service scenario. Ultimately this will mitigate threats due to human errors, improve operational efficiency and embed security controls into the cloud applications.
* **Implement sound identity, access management architecture and practice** – Scalable cloud bursting and elastic architecture will rely less on network based access controls and warrant strong user access management architecture. Cloud access control architecture should address all aspects of user and access management lifecycles for both end users and privileged users – user provisioning &deprovisioning, authentication, federation, authorization and auditing. A sound architecture will enable reusability of identity and access services for all use cases in public, private and hybrid cloud models. It is good practice to employ secure token services along with proper user and entitlement provisioning with audit trails. Federation architecture is the first step to extending enterprise SSO to cloud services. Refer to cloud security alliance, Domain 12 for detailed guidance here.
* **Leverage APIs to automate safeguards** – Any new security services should be deployed with an API (REST/SOAP) to enable automation. APIs can help automate firewall policies, configuration hardening, and access control at the time of application deployment. This can be implemented using open source tools such as puppet in conjunction with the API supplied by cloud service provider.
* **Always encrypt or mask sensitive data** – Today’s private cloud applications are candidates for tomorrow’s public cloud deployment. Hence architect applications to encrypt all sensitive data irrespective of the future operational model.
* **Do not rely on an IP address for authentication services** – IP addresses in clouds are ephemeral in nature so you cannot solely rely on them for enforcing network access control. Employ certificates (self-signed or from a trusted CA) to enable SSL between services deployed on cloud.
* **Log, Log, Log** – Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics. In the event of a security incident, logs and audit trails are the only reliable data leveraged by forensic engineers to investigate and understand how an application was exploited. Clouds are elastic and logs are ephemeral hence it is critical to periodically migrate log files to a different cloud or to the enterprise data center.
* **Continuously monitor cloud services** – Monitoring is an important function given that prevention controls may not meet all the enterprise standards. Security monitoring should leverage logs produced by cloud services, APIs and hosted cloud applications to perform security event correlation. Cloud audit (cloudaudit.org) from CSA can be leveraged towards this mission.

# Cloud Computing: Legal Challenges



* + Liability
  + Security
  + Risk allocation
  + Date Retention Issues
  + 3rd party contractual limitations
  + Regulatory compliances
  + Control over physical location of the data
  + Security breach
  + Trade secret protection
  + Hacking of cloud provider
  + Financial liability of cloud vendor
  + Legal/practical liability for force majeure events
  + IPR issues
  + Jurisdiction and court of law

# Data Security in Cloud Computing

Data protection is a crucial security issue for most organizations. Before moving into the cloud, cloud users need to clearly identify data objects to be protected and classify data

based on their implication on security, and then define the security policy for data protection as well as the policy enforcement mechanisms.

For most applications, data objects would include not only bulky data at rest in cloud servers (e.g., user database and/or file system), but also data in transit between the cloud and the user(s) which could be transmitted over the Internet or via mobile media (In many circumstances, it would be more cost-effective and convenient to move large volumes of data to the cloud by mobile media like archive tapes than transmitting over the Internet.). Data objects may also include user identity information created by the user management model, service

audit data produced by the auditing model, service profile information used to describe the service instance(s), temporary runtime data generated by the instance(s), and many other application data. Different types of data would be of different value and hence have different security implication to cloud users.

For example, user database at rest in cloud servers may be of the core value for cloud users and thus require strong protection to guarantee data confidentiality, integrity and availability. User identity information can contain Personally Identifiable Information (PII) and has impact on user privacy. Therefore, just authorized users should be allowed to access user identity information. Service audit data provide the evidences related to compliances and the fulfilment of Service Level Agreement (SLA), and should not be maliciously manipulated.

Service profile information could help attackers locate and identify the service instances and should be well protected. Temporary runtime data may contain critical data related to user business and should be segregated during runtime and securely destroyed after runtime.

Security Services: The basic security services for information security include assurance of data Confidentiality, Integrity, and Availability (CIA). In Cloud Computing, the issue of data security becomes more complicated because of the intrinsic cloud characteristics. Before potential cloud users are able to safely move their applications/data to the cloud, a suit of security services would be in place which we can identify as follows (not necessarily all needed in a specific Application):

1. **Data confidentiality assurance**: This service protects data from being disclosed to illegitimate parties. In Cloud Computing, data confidentiality is a basic security service to be in place. Although different applications may have different requirements in terms of what kind of data need confidentiality protection, this security service could be applicable to all the data objects discussed above.
2. **Data integrity protection**: This service protects data from malicious modification. When having outsourced their data to remote cloud servers, cloud users must have a way to check whether or not their data at rest or in transit are intact. Such a security service would be of the core value to cloud users. When auditing cloud services, it is also critical to guarantee that all the audit data are authentic since these data would be of

legal concerns. This security service is also applicable to other data objects discussed above.

1. **Guarantee of data availability**: This service assures that data stored in the cloud are available on each user retrieval request. This service is particularly important for data at rest in cloud servers and related to the fulfilment of Service Level Agreement. For long-term data storage services, data availability assurance is of more importance because of the increasing possibility of data damage or loss over the time.
2. **Secure data access**: This security service is to limit the disclosure of data content to authorized users. In practical applications, disclosing application data to unauthorized users may threat the cloud user’s business goal. In mission critical applications, inappropriate disclosure of sensitive data can have juristic concerns. For better protection on sensitive data, cloud users may need fine-grained data access control in the sense that different users may have access to different set of data. This security service is applicable to most of the data objects addressed above.
3. **Regulations and compliances:** In practical application scenarios, storage and access of sensitive data may have to comply specific compliance. For example, disclosure of health records may be limited by the Health Insurance Portability and Accountability Act (HIPAA) [12]. In addition to this, the geographic location of data would frequently be of concern due to export-law violation issues. Cloud users should thoroughly review these regulation and compliance issues before moving their data into the cloud.
4. **Service audition:** This service provides a way for cloud users to monitor how their data are accessed and is critical for compliance enforcement. In the case of local storage, it is not hard to audit the system. In Cloud Computing, however, it requires the service provider to support trustworthy transparency of data access.

# Business continuity and disaster recovery (BCDR)

Business continuity and disaster recovery (BCDR) are closely related practices that describe an organization's preparation for unforeseen risks to continued operations.

The trend of combining business continuity and disaster recovery into a single term has resulted from a growing recognition that business and technology executives need to collaborate closely instead of developing plans in isolation.

### What's the difference between business continuity and disaster recovery?

[**Business continuity**](https://searchdisasterrecovery.techtarget.com/definition/business-continuity) **i**s more proactive and generally refers to the processes and procedures an organization must implement to ensure that mission-critical functions

can continue during and after a disaster. BC involves more comprehensive planning geared toward long-term challenges to an organization's success.

[**Disaster recovery**](https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery) is more reactive and comprises specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident, and response times can range from seconds to days.

BC typically focuses on the organization as a whole, whereas DR zeroes in on the technology infrastructure. Disaster recovery is a piece of business continuity planning and concentrates on accessing data easily following a disaster. BC includes this element, but also takes into account [risk management](https://searchcompliance.techtarget.com/definition/risk-management) and other planning an organization needs to stay afloat during an event.

There are similarities between business continuity and disaster recovery. They both consider various unplanned events, from cyber attacks to human error to a natural disaster. They also have the goal of getting the business running as close to normal as possible, especially concerning mission-critical applications. In many cases, the same team will be involved with both BC and DR within an organization.

### Importance of BCDR

As cyber threats increase and the tolerance for downtime decreases, business continuity and disaster recovery gain importance. These practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve operations while decreasing the chance of emergencies.

BCDR professionals can help an organization and its employees achieve resiliency. Developing a strategy is a complex process that requires research and analysis, including conducting a business impact analysis ([BIA](https://searchstorage.techtarget.com/definition/business-impact-analysis)) and a [risk analysis,](https://searchmidmarketsecurity.techtarget.com/definition/risk-analysis) and developing BCDR plans, tests, exercises and training.

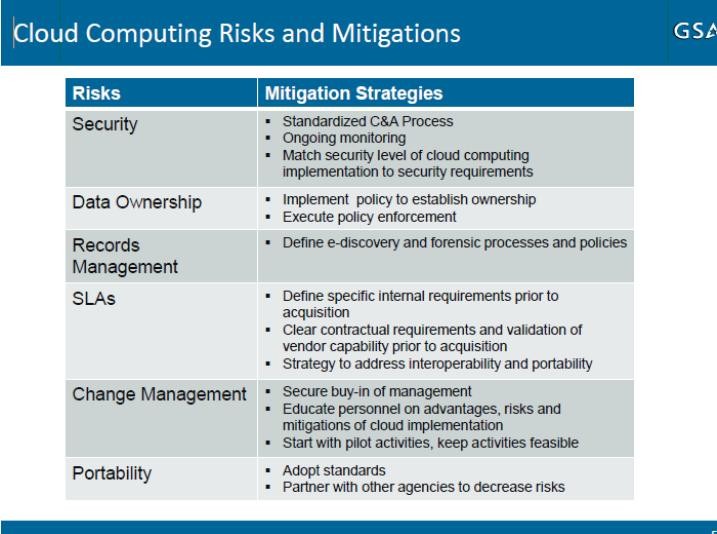


Plans also provide information such as employee contact lists, emergency contact lists, vendor lists, instructions for performing tests, equipment lists, and technical diagrams of systems and networks.

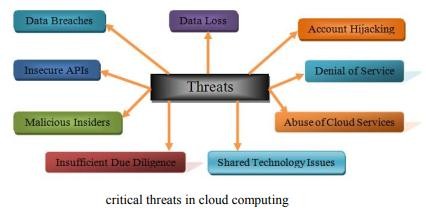
BCDR expert Paul Kirvan notes several other reasons for the importance of business continuity and disaster recovery planning:

* Results of the BIA identify opportunities for process improvement and ways the organization can use technology better;
* Information in the plan serves as an alternate source of documentation;
* The plan provides a single source of key contact information; and
* The plan serves as a reference document for use in product planning and design, service design and delivery, and other activities.

An organization should strive for continual improvement, driven by the BCDR process.



***Security Threads in Cloud Computing***



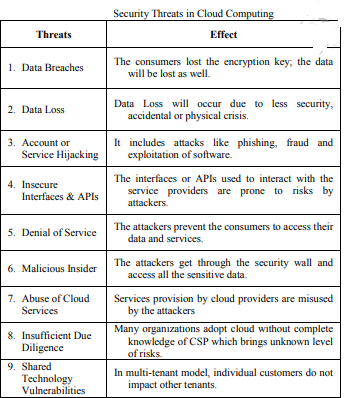
Many computer technology fields are adopting the cloud, and the trend is expected to continue due to its various [advantages.](https://searchdatabackup.techtarget.com/tip/The-pros-and-cons-of-cloud-backup-technologies) Most enterprises are already using some kind of cloud-based service, so it's important to understand that despite the advantages, there are also [cloud security threats](https://searchcloudsecurity.techtarget.com/video/Qualys-CEO-discusses-cloud-computing-threats-cloud-without-borders) that need to be addressed when moving there. The basic principle an enterprise needs to remember is that it cannot rely on the [cloud service](https://searchcloudprovider.techtarget.com/definition/cloud-provider) [provider](https://searchcloudprovider.techtarget.com/definition/cloud-provider) (CSP) to take care of every problem. Instead, companies have to communicate with the CSP and solve the issues together.

In this tip, we'll review the most important threats enterprises should be aware of before migrating to the cloud.

**Cloud computing threats**

When moving to the cloud, enterprises need to address the threats of cloud computing to enhance the security of the entire environment. Some of the most important [security](https://searchcompliance.techtarget.com/feature/Threats-to-cloud-data-security-remain-a-business-concern) [threats in cloud computing](https://searchcompliance.techtarget.com/feature/Threats-to-cloud-data-security-remain-a-business-concern) include:

* **Ease of use:** Cloud services can be easily used by businesses -- but they can also be easily used by attackers for malicious purposes like [spamming,](https://searchsecurity.techtarget.com/definition/spam) [malware](https://searchsecurity.techtarget.com/definition/malware) distribution, [command-and-control servers,](https://whatis.techtarget.com/definition/command-and-control-server-CC-server) [distributed denial-of-service (DDoS) attacks,](https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack) password/hash cracking, etc.
* **Vulnerable data transmission:** Data transferred from clients to the cloud needs to be properly encrypted by using [SSL](https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL)/[TLS,](https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS) which prevents attackers from intercepting unencrypted data off the wire. The data can be intercepted by [man-in- the-middle attacks,](http://searchsecurity.techtarget.in/definition/man-in-the-middle-MitM-attack) which can be hard to decrypt.
* **Insecure** [**APIs**](https://searchmicroservices.techtarget.com/definition/application-program-interface-API)**:** Various web cloud services are exposed by APIs, which are accessible from anywhere on the Internet. Malicious attackers with the authentication/authorization token will be able to access the API in the customer's name and therefore be able to manipulate the customer's data. It's imperative for the CSPs to provide secure APIs to minimize the attack surface.
* **Malicious insiders:** CSP employees could have complete access to enterprise data and resources, so CSPs need to have security measures in place to track employee actions like viewing customer data. Since CSPs don't always follow the best security guidelines or security policies employees can gather confidential customer information without being detected.
* **Shared technology issues:** CSPs use scalable infrastructure to support multiple tenants that share an underlying infrastructure with multiple layers. Each layer can be attacked by using different techniques such as exploiting [a vulnerability in a hypervisor,](https://searchcloudsecurity.techtarget.com/news/2240232384/Provider-reboots-call-cloud-computing-hypervisor-security-into-question) breaking out of [the virtual machine](https://searchservervirtualization.techtarget.com/definition/virtual-machine) (VM) sandbox (Red/Blue Pill), unauthorized access to shared data through [side-channel attacks,](https://searchsecurity.techtarget.com/answer/ASLR-side-channel-attack-How-is-JavaScript-used-to-bypass-protection) etc.
* **Data loss:** Data stored in the cloud could be lost due to a number of reasons. A hard drive could fail, a CSP employee could accidentally delete the data, or an attacker could modify or steal the data. The best way to protect against data loss is by having [data backup in place](https://searchcloudsecurity.techtarget.com/tip/Crafting-a-secure-data-backup-strategy-on-a-private-cloud) that can restore data.
* **Data breach:** A VM could have access to the data of another VM on the same physical host, which could lead to a data breach. By having multiple VMs, each belonging to separate enterprises, on the same physical server, one company could have access to the data of another company. These attacks are known as side- channel attacks, in which data is stolen from shared components like processor's cache, for instance.
* **Account/service hijacking:** If cloud access is only password protected, an attacker that knows the password will have equally easy access. Therefore, it's better to use [two-factor authentication](https://searchsecurity.techtarget.com/definition/two-factor-authentication) when available. This requires an attacker to also have access to the user's phone -- in the case that SMS messages are enabled for additional security -- to be able to access the cloud service.
* **Unknown risk profile:** When moving to the cloud, companies must have an accurate risk profile of their systems and infrastructure, even if they are off-premise. Software security updates need to be applied regularly, log monitoring needs to be enabled, IDS/IPS systems should constantly scan for malicious traffic, and [SIEM](https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM) needs to be used to gather all the data in one place. Additionally, multiple unknown attack techniques that haven't been discovered yet could be lurking on the Internet.
* [**Denial of service**](https://searchsecurity.techtarget.com/definition/denial-of-service) **(DoS):** An attacker can disrupt cloud services by issuing a DoS attack against the cloud service to render it inaccessible. There are several ways an attacker can disrupt the service in a virtualized cloud environment by using shared resources like CPU, RAM, disk space or network bandwidth.
* **Lack of understanding:** Enterprises should invest time and resources into education before moving to the cloud, because there's nothing worse than a company not knowing what it is getting itself into. The enterprises and the CSPs should agree on the services each will be taking care of. For example, if the CSP doesn't provide a backup strategy, the enterprise should. Users should understand the [cloud security threats](https://searchcloudcomputing.techtarget.com/feature/Cloud-security-breaches-still-the-stuff-of-IT-nightmares) in order to properly defend against them, which is why proper education of users is an important aspect of enhancing the security when moving to the cloud.



***SERVICE LEVEL AGREEMENT (SLA)***

A **service level agreement (SLA)** is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. SLAs do not define how the service itself is provided or delivered. The SLA an Internet Service Provider (ISP) will provide its customers is a basic example of an SLA from an external service provider. The metrics that define levels of service for an ISP should aim to guarantee:

* + **A description of the service being provided**– maintenance of areas such as network connectivity, domain name servers, dynamic host configuration protocol servers
  + **Reliability** – when the service is available (percentage uptime) and the limits outages can be expected to stay within
  + **Responsiveness** – the punctuality of services to be performed in response to requests and scheduled service dates
  + **Procedure for reporting problems** – who can be contacted, how problems will be reported, procedure for escalation, and what other steps are taken to resolve the problem efficiently
  + **Monitoring and reporting service level** – who will monitor performance, what data will be collected and how often as well as how much access the customer is given to performance statistics
  + **Consequences for not meeting service obligations** – may include credit or reimbursement to customers, or enabling the customer to terminate the relationship.
  + **Escape clauses or constraints** – circumstances under which the level of service promised does not apply. An example could be an exemption from meeting uptime requirements in circumstance that floods, fires or other hazardous situations damage the ISP’s equipment.

Though the exact metrics for each SLA vary depending on the service provider, the areas covered are uniform: volume and quality of work (including precision and accuracy), speed, responsiveness, and efficiency. In covering these areas, the document aims to establish a mutual understanding of services, areas prioritized, responsibilities, guarantees, and warranties provided by the service provider.

The level of service definitions should be specific and measureable in each area. This allows the quality of service to be benchmarked and, if stipulated by the agreement, rewarded or penalized accordingly. An SLA will commonly use technical definitions that quantify the level of service such as mean time between failures (MTBF) or mean time to recovery, response, or resolution (MTTR), which specifies a “target” (average) or “minimum” value for service level performance.

SLAs are also very popular among internal departments in larger organizations. For example, the use of a SLA by an IT helpdesk with other departments (the customer) allows their performance to be defined and benchmarked. The use of SLAs is also common in outsourcing, cloud computing, and other areas where the responsibility of an organization is transferred out to another supplier.

***Why are SLAs important?***

Service providers need SLAs to help them manage customer expectations and define the circumstances under which they are not liable for outages or performance issues. Customers can also benefit from SLAs in that they describe the performance characteristics of the service, which can be compared with other vendors' SLAs, and also set forth the means for redressing service issues -- via service credits, for example.

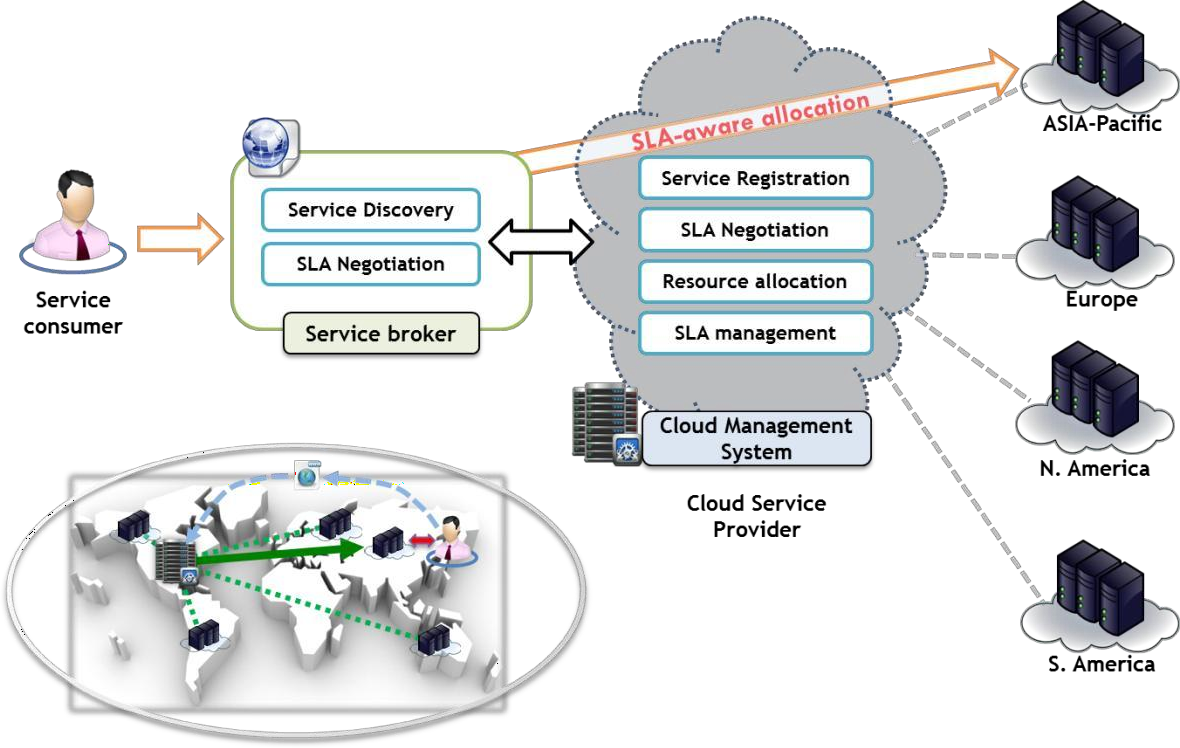
For a service provider, the SLA is typically one of two foundational agreements it has with customers. Many service providers establish a master services agreement to establish the general terms and conditions in which they will work with customers. The SLA is often incorporated by reference into the service provider's master services agreement. Between the two service contracts, the SLA adds greater specificity regarding the services provided and the metrics that will be used to measure their performance.

Cloud computing is a type of parallel or distributed system that consists of combinations of interconnected computing resources and virtualized computing resources, and it provisions virtualized resources to customers as services. In Cloud computing the resource demands and loads fluctuate by time. For example, in Cloud there will be a higher resource demand during late evening than a resource demand during work hours. Also, physical resources (computing clusters) of a Cloud provider is geometrically distributed, and the resource load of the provider can be distributed to physical resources that are geometrically distributed.

Since a Cloud computing system utilizes unified resources, it is necessary for a Cloud framework to have a load balancing scheme to increase system performance and stability. Whereas it is important to design such a Cloud framework, there is no Cloud framework considering temporal and locational Cloud load so far.

Therefore, this project proposes a Cloud computing framework to facilitate temporal and locational load-aware resource allocation, and we implement a testbed of the proposed Cloud framework to verify the usefulness of the proposed framework in a case study.

A cloud computing service providers can offer their resources as a service (e.g., Infrastructure, Platform, or Software). Before deliver the resource of a provider as a service to a consumer, the provider and the consumer should make an agreement in regard to its service level (Service Level Agreement, SLA): price, execution time or average response time. However, there may exist gap between the expected requirements (i.e. service level) of two different entities. To reduce the gap, they would negotiate in regard to requirement and regulation so that they can reach to mutually agreed level of requirements. In this research, we designed automated SLA negotiation scheme that is considering price, time slot, and response time particularly. In addition, to guarantee the SLA, we also designed SLA management scheme in this research.



SLA Negotiation and Management Framework based Cloud Computing Environment

In this cloud computing environment, there are number of service providers and consumers. Each of the service providers may have several data centres that are geographically distributed around the world. From the proposed framework, the service providers can manage these distributed data centres through a centric cloud management system. The management system has four different components for deploying new services and managing services.

