Unit: 3

Security Issues in Cloud Computing :

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

1. **Data Loss**
   Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

2. **Interference of Hackers and Insecure API'**
   As we know, if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.

3. **User Account Hijacking**

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities**.**

4. **Changing Service Provider**

   Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

5. **Lack of Skill**

   While working, shifting to another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employees. So it requires a skilled person to work with Cloud Computing.

6. **Denial of Service (DoS) attack**

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

7. **Shared Resources:** Cloud computing relies on a shared infrastructure. If one customer's data or applications are compromised, it may potentially affect other customers sharing the same resources, leading to a breach of confidentiality or integrity.

8. **Compliance and Legal Issues:** Different industries and regions have specific regulatory requirements for data handling and storage. Ensuring compliance with these regulations can be challenging when data is stored in a cloud environment that may span multiple jurisdictions.
9. **Data Encryption:** While data in transit is often encrypted, data at rest can be susceptible to breaches. It's crucial to ensure that data stored in the cloud is properly encrypted to prevent unauthorized access.
10. **Insider Threats:** Employees or service providers with access to cloud systems may misuse their privileges, intentionally or unintentionally causing data breaches. Proper access controls and monitoring are essential to mitigate these threats.
11. **Data Location and Sovereignty:** Knowing where your data physically resides is important for compliance and security. Some cloud providers store data in multiple locations globally, and this may raise concerns about data sovereignty and who has access to it.
12. **Loss of Control:** When using a cloud service, you are entrusting a third party with your data and applications. This loss of direct control can lead to concerns about data ownership, access, and availability.
13. **Incident Response and Forensics:** Investigating security incidents in a cloud environment can be complex. Understanding what happened and who is responsible can be challenging due to the distributed and shared nature of cloud services.
14. **Data Backup and Recovery:** Relying on cloud providers for data backup and recovery can be risky. It's essential to have a robust backup and recovery strategy in place to ensure data availability in case of outages or data loss.
15. **Vendor Security Practices:** The security practices of cloud service providers can vary. It's essential to thoroughly assess the security measures and certifications of a chosen provider to ensure they meet your organization's requirements.
16. **IoT Devices and Edge Computing:** The proliferation of IoT devices and edge computing can increase the attack surface. These devices often have limited security controls and can be targeted to gain access to cloud resources.
17. **Social Engineering and Phishing:** Attackers may use social engineering tactics to trick users or cloud service providers into revealing sensitive information or granting unauthorized access.
18. **Inadequate Security Monitoring:** Without proper monitoring and alerting systems in place, it's challenging to detect and respond to security incidents in a timely manner.

Cloud Security Mechanisms

A threat is a potential cause of an incident that can cause harm to a system or an organization while a vulnerability can be defined as a weakness in the system which is exploited by a threat. A threat agent exploits one or more vulnerabilities to carry out a threat. They are discussed in detail below:

Denial of Service:
Denial of Service (DoS) is an attack that is meant to shut down a network or a machine, thereby, making it inaccessible to the users who are intended to use it. DoS attacks flood the target server with traffic, or by sending information that triggers a crash on the server's end. Victims of DoS generally include web servers of high-profile organizations such as banking, media companies, trade, or government organizations. DoS attacks may not result in the theft or loss of any information but they can cost the victim a great wastage of time and money to get things fixed.

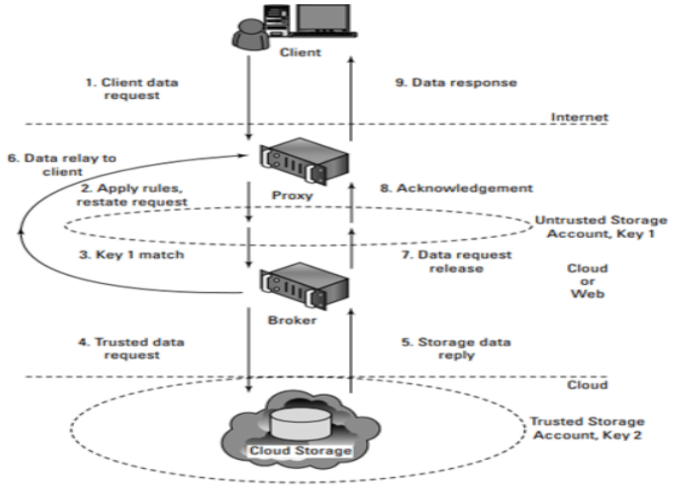
Distributed Denial of Service:
Distributed Denial of Service (DDoS) is a malicious attempt to disrupt the normal traffic of a target network, server, or service by flooding the target or its surrounding infrastructure with Internet traffic. The attacker takes control of several victim systems known as zombies, also known as a botnet by spreading various types of malware. Now, the attacker can shut down a network service by commanding the botnet to send fake traffic that fabricates data.

Securing data in the cloud is the single largest security concern that most organizations have with cloud computing. In any WAN traffic, one must assume that any data can be modified or intercepted. That's why traffic to and from a cloud service provider is encrypted. Some key mechanisms for protecting data are Access control, Auditing, Authentication, Authorization Every service model should have mechanisms operating in all these four areas that are based on the security requirements, whether operating through its own local infrastructure or any cloud service provider.

Brokered cloud storage access:
The problem with the data stored in the cloud is that the server can be located anywhere in the cloud service provider's system which can be in another data center, another country, or in many cases even in another continent. In client/server or with other types of system architectures, one can count on a firewall to serve as the network's security perimeter but cloud computing has no physical system that can be used to serve this purpose.

When a client makes a request for data, the request goes to the endpoint or external service interface of the proxy, which has only a partial trust.

- The proxy forwards the request to the broker using its internal interface.
- The broker then requests data from the cloud storage system.
- The storage system returns the results to the broker.
- The broker returns the results to the proxy.
- The proxy completes the response by sending the data requested to the client.



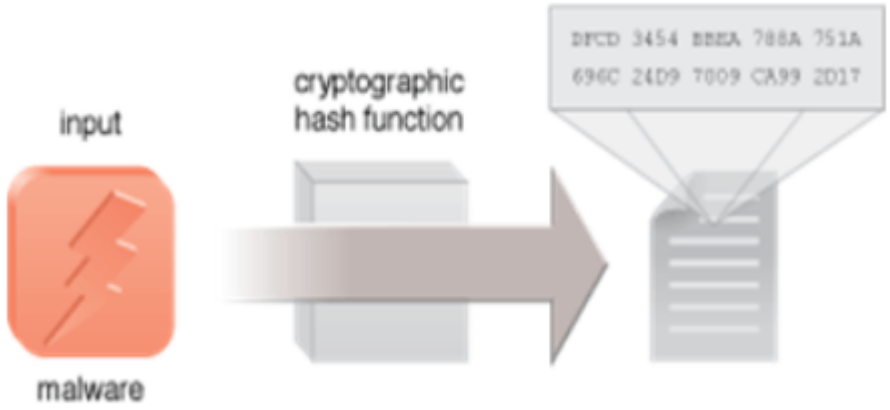
1. **Encryption:**
   The data, by default, is coded in a readable form known as plaintext. When transmitted over a network, the risk is unauthorized and potentially dangerous access.

Encryption technology relies on a standard algorithm called cipher to convert original text data into encrypted data, called ciphertext. Access to ciphertext does not disclose the exact details of writing, with the exception of other metadata types, such as message length and creation date. When encryption is used for listening data, data is paired with a string of characters called an encryption key. The encryption key is used to encrypt ciphertext back to its original writing format.

Asymmetric Encryption A malicious service provider cannot retrieve data from encrypted messages. Refund attempt may also reveal to the cloud service customer

2. **Hashing:**
Hashing is the conversion of a string of characters into a limited number of short lengths or a key that reflects the original string. Hashing is used to identify and retrieve items from the database because it is faster to find an object using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. There are many well-known hash functions used in cryptography. These include message-digest hash works MD2, MD4, and MD5, which is used to incorporate digital signatures into a short form called message-digest, and the Secure Hash Algorithm (SHA), a standard algorithm, which makes it large (60- bit) digestion message and similar to MD4. An effective hash function for storing and retrieving, however, may not work for cryptographic detection purposes or errors.

Malware hashes are used by anti-virus programs to identify viruses. They contain the numerical values of the code that differs from this virus. Anti-virus software compares malware hashes and software-hardware hashes within a computer program to detect malware.
The diagram shows the creation of a malware hash by creating a cryptographic hash of malware code to create a path that can be used by anti-virus software to identify the virus. The authors of Malware have learned to customize viruses on each infected machine, creating unique hashes for each copy submitted challenging the anti-virus programs.



3. **Digital Signatures:**
The digital signature mechanism is a means of providing data integrity, data authenticity through authentication, and non-repudiation. A message is assigned a digital signature prior to transmission, and if the message experiences any subsequent, unauthorized modifications then it is rendered as invalid. A digital signature provides evidence that the message received is the same as the original message sent by the rightful sender.

Both hashing and asymmetrical encryption are involved in the creation of a digital signature, which exists as a message digest that was encrypted by a private key and appended to the original message. To decrypt the digital signature's encrypted hash, the recipient verifies the signature validity by using the corresponding public key, which produces the message digest. To produce the message digest hashing mechanism is applied to the original message. Identical results from the two different processes is an indication that the message maintained its integrity.

4. **Single Sign-On:**
   The single sign-on (SSO) mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context while the cloud service consumer accesses cloud-based IT resources. Otherwise, with every subsequent request, the service consumer would need to re-authenticate itself.
   The advantage to the SSO machine is how it enables independent IT resources to generate and distribute operational authorization and validation signals. The information originally provided by the cloud client remains active during the user's session, while its security information is shared with other IT resources. SSO Security Vendor assists when a cloud buyer needs access to cloud-based cloud services.

5. **Public Key Infrastructure:**
   A common approach for managing the issuance of asymmetric keys is based on the PKI (public key infrastructure) mechanism, which exists as a system of protocols, practices, rules, and data formats that enable large-scale systems to securely use public-key cryptography. This system is used to associate public keys with their corresponding key owners (known as public-key identification) while enabling the verification of key validity. PKIs have digitally signed data structures that rely on the use of digital certificates, that bind public keys to certificate owner identities, as well as to related information, such as validity periods. A third-party certificate authority (CA) digitally signs the Digital certificates.

   The components of a PKI include a CA that issues the certificates, a registration authority (RA) to approve the issuance of the certificates, a public directory containing the issued certificates, and the certificate revocation list (CRL).

6. **Identity and Access Management:**
   Cloud Identity and Access Management typically include the following features:

   Single Access Control Interface: Cloud IAM solutions provide a clean and consistent access control interface for all cloud platform services. All cloud services can use the same interface.

   Enhanced Security: You can define increased security for critical applications. Resource-level Access Control. You can define roles and grant permissions to users for allowing them to access resources at different granularity levels.

Identity and access management (IAM)

It is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.

IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model.

On a fundamental level, IAM encompasses the following components:

- how individuals are identified in a system (understand the difference between identity management and authentication);
- how roles are identified in a system and how they are assigned to individuals;
- adding, removing and updating individuals and their roles in a system;
- assigning levels of access to individuals or groups of individuals; and
- protecting the sensitive data within the system and securing the system itself.

Why is IAM important?

Businesses leaders and IT departments are under increased regulatory and organizational pressure to protect access to corporate resources. As a result, they can no longer rely on manual and error-prone processes to assign and track user privileges. IAM automates these tasks and enables granular access control and auditing of all corporate assets on premises and in the cloud.

IAM, which has an ever-increasing list of features -- including biometrics, behavior analytics and AI -- is well suited to the rigors of the new security landscape. For example, IAM's tight control of resource access in highly distributed and dynamic environments aligns with the industry's transition from firewalls to zero-trust models and with the security requirements of IoT. For more information on the future of IoT security, check out this video.

What is Single Sign-On?

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.
How Does SSO Work?

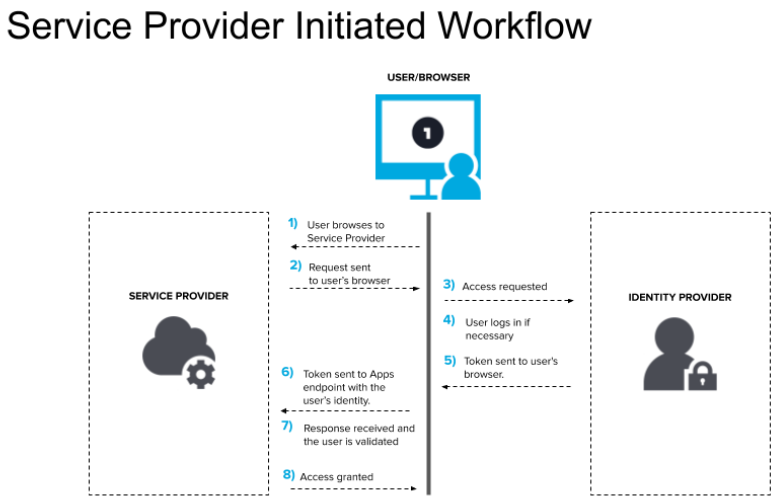
SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider, like OneLogin. This trust relationship is often based upon a certificate that is exchanged between the identity provider and the service provider. This certificate can be used to sign identity information that is being sent from the identity provider to the service provider so that the service provider knows it is coming from a trusted source. In SSO, this identity data takes the form of tokens which contain identifying bits of information about the user like a user's email address or a username.

The login flow usually looks like this:

1. A user browses to the application or website they want access to, aka, the Service Provider.
2. The Service Provider sends a token that contains some information about the user, like their email address, to the SSO system, aka, the Identity Provider, as part of a request to authenticate the user.
3. The Identity Provider first checks to see whether the user has already been authenticated, in which case it will grant the user access to the Service Provider application and skip to step 5.
4. If the user hasn't logged in, they will be prompted to do so by providing the credentials required by the Identity Provider. This could simply be a username and password or it might include some other form of authentication like a One-Time Password (OTP).
5. Once the Identity Provider validates the credentials provided, it will send a token back to the Service Provider confirming a successful authentication.
6. This token is passed through the user's browser to the Service Provider.

7. The token that is received by the Service Provider is validated according to the trust relationship that was set up between the Service Provider and the Identity Provider during the initial configuration.
8. The user is granted access to the Service Provider.

When the user tries to access a different website, the new website would have to have a similar trust relationship configured with the SSO solution and the authentication flow would follow the same steps.



Hardened Virtual Server Images.

A hardened virtual server image is a template for virtual service instance creation that has been subjected to a hardening process (Figure 1). This generally results in a virtual server template that is significantly more secure than the original standard image.

Virtual Image vs. Hardened Virtual Image

Every day, more and more organizations are moving to the cloud. Shifting from on-premise systems enables greater flexibility and scalability in ever-changing computing workloads. And that can translate to significant fixed cost savings. As with any change, however, cloud computing presents its own challenges — including how to ensure your VM images are secure.

A virtual machine image is a snapshot of a virtual machine used to create a running instance in a virtual environment, and it provides the same functionality as a physical computer. Virtual images reside in the cloud and enable you to cost-effectively perform routine computing operations without investing in local hardware and software.

When operating in the public cloud, the security of your systems and data is ultimately your responsibility. CIS Hardened Images are designed to harden your operating systems in the cloud.

Hardening limits potential weaknesses that make systems vulnerable to cyber attacks. More secure than a standard image, hardened virtual machine images help protect against denial of service, unauthorized data access, and other cyber threats.

Enhanced Security and Achieving Compliance

CIS Hardened Images are configured according to CIS Benchmark recommendations, which are developed through consensus by a global community of cybersecurity experts.

These recommendations are recognized as a secure configuration standard by the DoD Cloud Computing Security Recommendation Guide (SRG), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and the National Institute of Standards and Technology (NIST). This recognition also applies to CIS Hardened Images, as their configuration is based on the CIS Benchmarks.

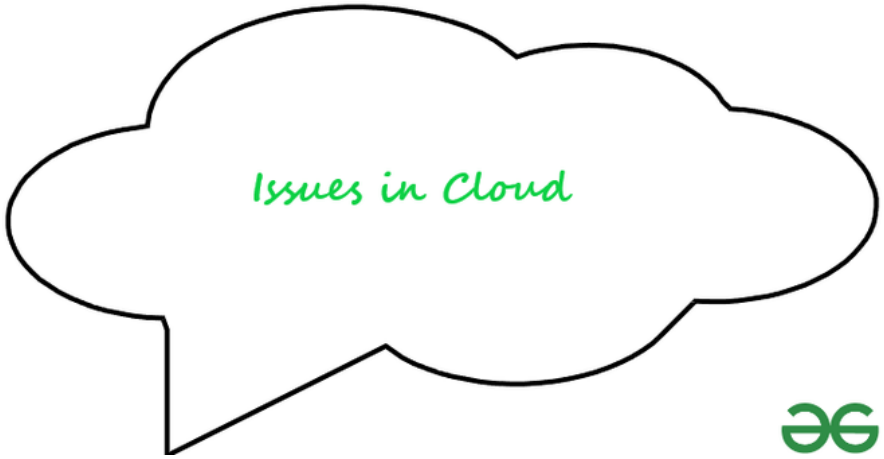
For organizations and industries that want to achieve compliance with Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) standards, CIS offers several CIS Benchmarks mapped to STIG standards. CIS STIG Benchmarks note any DISA STIG recommendations not included in the CIS STIG Benchmarks. From these guidelines, CIS also offers CIS STIG Hardened Images.

Issues in Cloud Computing

- Cloud Computing is a new name for an old concept. The delivery of computing services from a remote location. Cloud Computing is Internet-based computing, where shared resources, software, and information are provided to computers and other devices on demand.
  These are major issues in Cloud Computing:

  1. Privacy: The user data can be accessed by the host company with or without permission. The service provider may access the data that is on the cloud at any point in time. They could accidentally or deliberately alter or even delete information.

2. Compliance: There are many regulations in places related to data and hosting. To comply with regulations (Federal Information Security Management Act, Health Insurance Portability and Accountability Act, etc.) the user may have to adopt deployment modes that are expensive.
3. Security: Cloud-based services involve third-party for storage and security. Can one assume that a cloud-based company will protect and secure one's data if one is using their services at a very low or for free? They may share users' information with others. Security presents a real threat to the cloud.
4. Sustainability: This issue refers to minimizing the effect of cloud computing on the environment. Citing the server's effects on the environmental effects of cloud computing, in areas where climate favors natural cooling and renewable electricity is readily available, the countries with favorable conditions, such as Finland, Sweden, and Switzerland are trying to attract cloud computing data centers. But other than nature's favors, would these countries have enough technical infrastructure to sustain the high-end clouds?
5. Abuse: While providing cloud services, it should be ascertained that the client is not purchasing the services of cloud computing for a nefarious purpose. In 2009, a banking Trojan illegally used the popular Amazon service as a command and control channel that issued software updates and malicious instructions to PCs that were infected by the malware So the hosting companies and the servers should have proper measures to address these issues.



6, Higher Cost: If you want to use cloud services uninterruptedly then you need to have a powerful network with higher bandwidth than ordinary internet networks, and also if your organization is broad and large so ordinary cloud service subscription won't suit your organization. Otherwise, you might face hassle in utilizing an ordinary cloud service while working on complex projects and applications. This is a major problem before small organizations, that restricts them from diving into cloud technology for their business.
7. Recovery of lost data in contingency: Before subscribing any cloud service provider goes through all norms and documentations and check whether their services match your requirements and sufficient well-maintained resource infrastructure with proper upkeeping. Once you subscribed to the service you almost hand over your data into the hands of a third party. If you are able to choose proper cloud service then in the future you don't need to worry about the recovery of lost data in any contingency.
8. Upkeeping(management) of Cloud: Maintaining a cloud is a herculin task because a cloud architecture contains a large resources infrastructure and other challenges and risks as well, user satisfaction, etc. As users usually pay for how much they have consumed the resources. So, sometimes it becomes hard to decide how much should be charged in case the user wants scalability and extend the services.
9. Lack of resources/skilled expertise: One of the major issues that companies and enterprises are going through today is the lack of resources and skilled employees. Every second organization

is seeming interested or has already been moved to cloud services. That's why the workload in the cloud is increasing so the cloud service hosting companies need continuous rapid advancement. Due to these factors, organizations are having a tough time keeping up to date with the tools. As new tools and technologies are emerging every day so more skilled/trained employees need to grow. These challenges can only be minimized through additional training of IT and development staff.

10. Pay-per-use service charges: Cloud computing services are on-demand services a user can extend or compress the volume of the resource as per needs. so you paid for how much you have consumed the resources. It is difficult to define a certain pre-defined cost for a particular quantity of services. Such types of ups and downs and price variations make the implementation of cloud computing very difficult and intricate. It is not easy for a firm's owner to study consistent demand and fluctuations with the seasons and various events. So it is hard to build a budget for a service that could consume several months of the budget in a few days of heavy use.

Service level agreements in Cloud computing

- A **Service Level Agreement (SLA)** is the bond for performance negotiated between the cloud services provider and the client. Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer. Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services. Service level agreements are also defined at **different levels** which are mentioned below:
  - Customer-based SLA
  - Service-based SLA
  - Multilevel SLA

  Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law. It is fine to have an attorney review the documents before making a major agreement to the cloud service provider. Service Level Agreements usually specify **some parameters** which are mentioned below:
  1. Availability of the Service (uptime)
  2. Latency or the response time
  3. Service components reliability
  4. Each party accountability
  5. Warranties

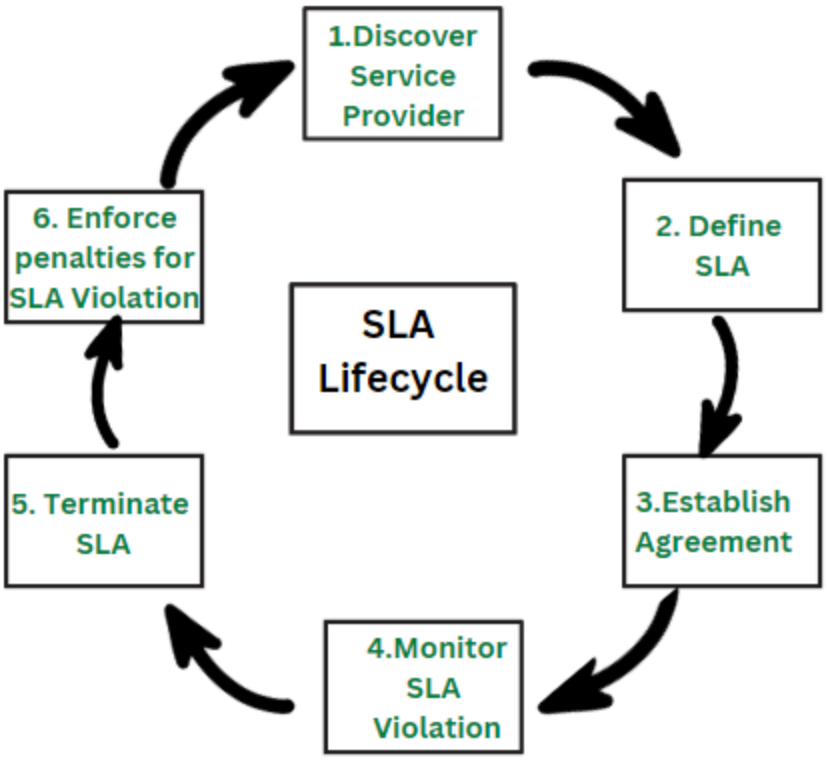
  In any case, if a cloud service provider fails to meet the stated targets of minimums then the provider has to pay the penalty to the cloud service consumer as per the agreement. So, Service Level Agreements are like insurance policies in which the corporation has to pay as per the agreements if any casualty occurs. Microsoft publishes the Service Level Agreements linked with the Windows Azure Platform components, which is demonstrative of industry practice for cloud service vendors. Each individual component has its own Service Level Agreements. Below are two **major Service Level Agreements (SLA)** described:
  1. **Windows Azure SLA –** Window Azure has different SLA's for compute and storage. For compute, there is a guarantee that when a client deploys two or more role instances in separate fault and upgrade domains, client's internet facing roles will have external connectivity minimum 99.95% of the time. Moreover, all of the role instances of the client are monitored

and there is guarantee of detection 99.9% of the time when a role instance's process is not runs and initiates properly.

2. **SQL Azure SLA –** SQL Azure clients will have connectivity between the database and internet gateway of SQL Azure. SQL Azure will handle a "Monthly Availability" of 99.9% within a month. Monthly Availability Proportion for a particular tenant database is the ratio of the time the database was available to customers to the total time in a month. Time is measured in some intervals of minutes in a 30-day monthly cycle. Availability is always remunerated for a complete month. A portion of time is marked as unavailable if the customer's attempts to connect to a database are denied by the SQL Azure gateway.

Service Level Agreements are based on the usage model. Frequently, cloud providers charge their pay-as-per-use resources at a premium and deploy standards Service Level Agreements only for that purpose. Clients can also subscribe at different levels that guarantees access to a particular amount of purchased resources. The Service Level Agreements (SLAs) attached to a subscription many times offer various terms and conditions. If client requires access to a particular level of resources, then the client need to subscribe to a service. A usage model may not deliver that level of access under peak load condition.

SLA Lifecycle



Steps in SLA Lifecycle

1. **Discover service provider:** This step involves identifying a service provider that can meet the needs of the organization and has the capability to provide the required service. This can be done through research, requesting proposals, or reaching out to vendors.
2. **Define SLA:** In this step, the service level requirements are defined and agreed upon between the service provider and the organization. This includes defining the service level objectives, metrics, and targets that will be used to measure the performance of the service provider.
3. **Establish Agreement:** After the service level requirements have been defined, an agreement is established between the organization and the service provider outlining the terms and conditions of the service. This agreement should include the SLA, any penalties for non-compliance, and the process for monitoring and reporting on the service level objectives.
4. **Monitor SLA violation:** This step involves regularly monitoring the service level objectives to ensure that the service provider is meeting their commitments. If any violations are identified, they should be reported and addressed in a timely manner.
5. **Terminate SLA:** If the service provider is unable to meet the service level objectives, or if the organization is not satisfied with the service provided, the SLA can be terminated. This can be done through mutual agreement or through the enforcement of penalties for non-compliance.
6. **Enforce penalties for SLA Violation:** If the service provider is found to be in violation of the SLA, penalties can be imposed as outlined in the agreement. These penalties can include financial penalties, reduced service level objectives, or termination of the agreement.

Advantages of SLA

1. **Improved communication:** A better framework for communication between the service provider and the client is established through SLAs, which explicitly outline the degree of service that a customer may anticipate. This can make sure that everyone is talking about the same things when it comes to service expectations.
2. **Increased accountability:** SLAs give customers a way to hold service providers accountable if their services fall short of the agreed-upon standard. They also hold service providers responsible for delivering a specific level of service.
3. **Better alignment with business goals:** SLAs make sure that the service being given is in line with the goals of the client by laying down the performance goals and service level requirements that the service provider must satisfy.
4. **Reduced downtime:** SLAs can help to limit the effects of service disruptions by creating explicit protocols for issue management and resolution.
5. **Better cost management:** By specifying the level of service that the customer can anticipate and providing a way to track and evaluate performance, SLAs can help to limit costs. Making sure the consumer is getting the best value for their money can be made easier by doing this.

Disadvantages of SLA

1. **Complexity:** SLAs can be complex to create and maintain, and may require significant resources to implement and enforce.
2. **Rigidity:** SLAs can be rigid and may not be flexible enough to accommodate changing business needs or service requirements.

3. **Limited service options:** SLAs can limit the service options available to the customer, as the service provider may only be able to offer the specific services outlined in the agreement.
4. **Misaligned incentives:** SLAs may misalign incentives between the service provider and the customer, as the provider may focus on meeting the agreed-upon service levels rather than on providing the best service possible.
5. **Limited liability:** SLAs are not legal binding contracts and often limited the liability of the service provider in case of service failure.

Difference between Cloud Computing and Distributed Computing

- **1. Cloud Computing :**
  Cloud computing refers to providing on demand IT resources/services like server, storage, database, networking, analytics, software etc. over internet. It is a computing technique that delivers hosted services over the internet to its users/customers. Cloud computing provides services such as hardware, software, networking resources through internet. Some characteristics of cloud computing are providing shared pool of configurable computing resources, on-demand service, pay per use, provisioned by the Service Providers etc.
  It is classified into 4 different types such as
  - Public Cloud
  - Private Cloud
  - Community Cloud
  - Hybrid Cloud
  2. Distributed Computing :
  Distributed computing refers to solve a problem over distributed autonomous computers and they communicate between them over a network. It is a computing technique which allows to multiple computers to communicate and work to solve a single problem. Distributed computing helps to achieve computational tasks more faster than using a single computer as it takes a lot of time. Some characteristics of distributed computing are distributing a single task among computers to progress the work at same time, Remote Procedure calls and Remote Method Invocation for distributed computations.
  It is classified into 3 different types such as
  - Distributed Computing Systems
  - Distributed Information Systems
  - Distributed Pervasive Systems

Difference between Cloud Computing and Distributed Computing :

S.No.	CLOUD COMPUTING	DISTRIBUTED COMPUTING
01.	**Cloud computing refers to providing on demand IT resources/services like server, storage, database, networking, analytics, software etc. over internet.**	**Distributed computing refers to solve a problem over distributed autonomous computers and they communicate between them over a network.**
02.	**In simple cloud computing can be said as a computing technique that delivers hosted services over the internet to its users/customers.**	**In simple distributed computing can be said as a computing technique which allows to multiple computers to**

		communicate and work to solve a single problem.
03.	**It is classified into 4 different types such as Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud.**	**It is classified into 3 different types such as Distributed Computing Systems, Distributed Information Systems and Distributed Pervasive Systems.**
04.	**There are many benefits of cloud computing like cost effective, elasticity and reliable, economies of Scale, access to the global market etc.**	**There are many benefits of distributed computing like flexibility, reliability, improved performance etc.**
05.	**Cloud computing provides services such as hardware, software, networking resources through internet.**	**Distributed computing helps to achieve computational tasks more faster than using a single computer as it takes a lot of time.**
06.	**The goal of cloud computing is to provide on demand computing services over internet on pay per use model.**	**The goal of distributed computing is to distribute a single task among multiple computers and to solve it quickly by maintaining coordination between them.**
07.	**Some characteristics of cloud computing are providing shared pool of configurable computing resources, on-demand service, pay per use, provisioned by the Service Providers etc.**	**Some characteristics of distributed computing are distributing a single task among computers to progress the work at same time, Remote Procedure calls and Remote Method Invocation for distributed computations.**
08.	**Some disadvantage of cloud computing includes less control especially in the case of public clouds, restrictions on available services may be faced and cloud security.**	**Some disadvantage of distributed computing includes chances of failure of nodes, slow network may create problem in communication**

Performance Optimization of Distributed System

- The term “distributed systems” refers to a group of several components situated on various machines that interact and coordinate actions to appear to the end-user as a single system. This article will go through the concept of how we can optimize the performance of Distributed Systems in detail.

  Performance Optimization of Distributed Systems:
  The following are the parameters that should be taken care of for optimizing performance in Distributed Systems:

- **Serving Multiple Requests Simultaneously:** While a server waits for a momentarily unavailable resource, the main issue is a delay. A server invokes a remote function that requires a lot of computation–or has a significant transmission latency. To avoid this, multithreading can accept and process other requests.
- **Reducing Per-Call Workload of Servers:** A server's performance can be quickly impacted by a large number of client requests. Each request necessitates a significant amount of processing on the server's part. So, keep requests brief and the amount of work a server has to do for each request to a minimum. Use servers that are not tied to any one state i.e. use stateless servers.
- **Reply Caching of Idempotent Remote Procedures:** If a server is unable to handle the client requests because of the difference in pace between them. The requests are arriving at a higher rate than the server can tackle. As a result, a backlog starts building up due to the unhandled client requests at the same pace. So, in this case, the server uses its reply cache for sending the response.
- **Timeout Values Should Be Carefully Chosen:** A timeout that is "too small" may expire too frequently, resulting in unnecessary retransmissions. If communication is genuinely lost, a "too large" timeout setting will cause an unnecessarily long delay.
- **Appropriate Design of RPC Protocol Specifications:** The protocol specifications should be well designed to bring down the amount of transferring data over the network and also the rate (frequency) with which it is sent.
- **Using LRPC (Lightweight Remote Procedure Call) for Cross-Domain Messaging:** LRPC (Lightweight Remote Procedure Call) facility is used in microkernel operating systems for providing cross-domain (calling and called processes are both on the same machine) communication. It employs following the approaches for enhancing the performance of old systems employing Remote Procedure Call:
- **Simple Control Transfer:** In this approach, a control transfer procedure is used that refers to the execution of the requested procedure by the client's thread in the server's domain. It employs hand-off scheduling in which direct context switching takes place from the client thread to the server thread. Before the first call is made to the server, the client binds to its interface, and afterward, it provides the server with the argument stack and its execution thread for trapping the kernel. Now, the kernel checks the caller and creates a call linkage, and sends off the client's thread directly to the server which in turn activates the server for execution. After completion of the called procedure, control and results return through the kernel from where it is called.

- **Simple Data Transfer:** In this approach, a shared argument stack is employed to avoid duplicate data copying. Shared simply refers to the usage by both the client and the server. So, in LRPC the same arguments are copied only once from the client's stack to the shared argument stack. It leads to cost-effectiveness as data transfer creates few copies of data when moving from one domain to another.
- **Simple Stub:** Because of the above mechanisms, the generation of the highly optimized stubs is possible using LRPC. The call stub is associated with the client's domain and the entry stub is associated with the server's domain is having an entry stub in every procedure. The LRPC interface for every procedure follows a three-layered communication protocol:
    - **From end to end:** communication is carried out as defined by calling conventions
    - **stub to stub:** requires the usage of stubs
    - **domain-to-domain:** requires kernel implementation
- The benefit of using LRPC stubs is that cost for interlayer gets reduced as it makes the boundaries blurry. The single requirement in a simple LRPC is that one formal procedure call to client stub and one return from server procedure and client stub should be made.
- **Design for Concurrency:** For achieving high performance in terms of high call throughput and low call latency, multiple processors are used with shared memory. Further, throughput can be increased by getting rid of unnecessary lock contention and reducing the utilization of shared-data structures, while latency is lowered by decreasing the overhead of context switching. The factor-by-3 performance is achieved using LRPC. The cost involved in cross-domain communication is also gets reduced.