# UNIT – IV

## CLOUD SECURITY

Cloud security is essential for the users who are concerned about the safety of the data they store in the cloud. They believe their data is safer on their own local servers where they feel they have more control over the data. But data stored in the cloud may be more secure because cloud service providers have superior security measures, and their employees are security experts. Cloud security is a key concern for cloud storage providers. They not only must satisfy their customers; they also must follow certain regulatory requirements for storing sensitive data such as credit card numbers and health information.

Cloud security is the protection of data stored online from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Major threats to cloud security include data breaches, data loss, account hijacking, and service traffic hijacking, insecure Application Program Interfaces (APIs), poor choice of cloud storage providers, and shared technology that can compromise cloud security. Distributed Denial of Service (DDoS) attacks are another threat to cloud security. These attacks shut down a service by overwhelming it with data so that users cannot access their accounts, such as bank accounts or email accounts.

When choosing a cloud provider, it is important to choose a company that tries to protect against malicious insiders through background checks and security clearances. Most people think outside hackers are the biggest threat to cloud security, but employees present just as large of a risk. These employees are not necessarily malicious insiders; they are often employees who unknowingly make mistakes such as using a personal smartphone to access sensitive company data without the security of the company's own network.

Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cyber security threats. Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cyber security threats.

## INFRASTRUCTURE SECURITY

The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS. The infrastructure security can be viewed, assessed and implemented according its building levels - the network, host and application levels.

**Infrastructure Security – The Network Level:** When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. If public cloud services are chosen, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account. There are four significant risk factors in this use case:

- Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider;
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources are used at the public cloud provider;
- Ensuring the availability of the Internet-facing resources in a public cloud that are being used by an organization, or have been assigned to an organization by public cloud providers;
- Replacing the established model of network zones and tiers with domains.

**Infrastructure Security – The Host Level:** When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services. IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (virtualization software security, customer guest OS or virtual server security).

**Infrastructure Security – The Application Level**: Application or software security should be a critical element of a security pro-gram. Most enterprises with information security programs have yet to institute an application security program to address this realm. Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reevaluate current practices and standards. The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by many users. The level is responsible for managing;

- Application-level security threats
- End user security
- SaaS application security
- PaaS application security
- Customer-deployed application security
- IaaS application security
- Public cloud security limitations

It can be summarized that the issues of infrastructure security and cloud computing lie in the area of definition and provision of security specified aspects each party delivers.

| Security problem | Attacks | Attack type | Preventive Method |
|---|---|---|---|
| Network Level | DNS attack | Sender and a receiver get rerouted through some evil connection. | Domain name system security Extensions (DNSSEC) reduces the effects of DNS threats. |
| | Eavesdropping | Attacker monitor network traffic in transit then interprets all unprotected data. | Methods of preventing intruders are Internet protocol security (IP sec) Implement security policies and procedures install anti-virus software. |
| | DoS Attack | Prevent the authorized user to accessing services on network. | DoS attacks can be prevented with a firewall but they have configured properly, Enforce strong password policies. |
| | Distributed Denial of Service attack | Against a single network from multiple computers or systems. | Limit the number of ICMP and SYN packets on router interfaces. Filter private IP addresses using router access control lists. |
| | Sniffer Attack | Data is not encrypted & flowing in network, and chance to read the vital information. | Detect based on ARP and RTT. Implement IPSec to encrypt network traffic. Using one time password or ticketing authentication. |
| | Issues of reused IP addresses | IP address is reassigned and reused by other customer. The address still exists in the DNS cache, it violating the privacy of the original user. | Old ARP addresses are cleared from cache. |
| | BGP Prefix Hijacking | network attack in which wrong announcement on IP address associated with autonomous system(AS) | Filtering and MD5/TTL protection(preventing the source of most attacks) |
| Host Level | hypervisor | Single hardware unit is difficult to monitor multiple operating systems. Code get control of the system and block other guest OS. | Malicious Hook safe that can provide generic protection against kernel mode root kits. |
| | Securing virtual server | Self-provisioning new virtual servers on an IaaS platform creates a risk that insecure virtual server. | Operational security procedures need to be followed. |
| | Cookie Poisoning | Unauthorized person can change or modify the content of cookies | Cookie should be avoided, or regular Cookie Cleanup is necessary. |
| | Back door and debug options | Debug options are left enabled unnoticed, it provide an easy entry to a hacker in to the web-site and let him make changes at the web-site level | Scan the system periodically for SUID/SGID files Permissions and ownership of important files and directories periodically |

| | | | |
|---|---|---|---|
| **Application Level** | Hidden field manipulation | Certain fields are hidden in the web-site and it's used by the developers. Hacker can easily modify on the web page. | Avoid putting parameters into a query string. |
| | DoS Attack | Services used by the authorized user unable to be used by them. | Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks .Preventive tools are Firewalls, Switches, and Routers. |
| | Distributed Denial of Service attack | DDoS attack results in making the service unavailable to the authorized user similar to the way it is done in a DoS attack but different in the way it is launched. | Preventive tools are firewalls, Switches, Routers, Application front-end hardware, IPS based Prevention, etc. |
| | Google Hacking | Google search engine Best option for the hacker to access the sensitive information. | Prevent sharing of any sensitive information.<br>Software solution such as Web Vulnerability Scanner. |
| | SQL injection | Malicious code is inserted into a standard SQL code and gain unauthorized access to a database. | Avoiding the usage of dynamically generated SQL in the code. |
| | Cross site Scripting attacks | Inject the malicious scripts into web contents. | Various techniques to detect the security flaws like: Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology. |

## DATA SECURITY AND STORAGE

In today's world of (network-, host-, and application-level) infrastructure security, data security becomes more important when using cloud computing at all service levels: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Data storage security is a subset of the larger IT security field, and it is specifically focused on securing storage devices and systems.

Storage security and data security are closely related to data protection. Data security primarily involves keeping private information out of the hands of anyone not authorized to see it. Data protection is more about making sure data remains available after less nefarious incidents, like system or component failures or even natural disasters.

According to the Storage Networking Industry Association (SNIA), storage security represents the convergence of the storage, networking, and security disciplines, technologies, and methodologies for the purpose of protecting and securing digital assets. For storage administrators and managers, ensuring proper data storage security is a

careful balancing act. They must consider three primary concerns covered by the acronym "CIA": Confidentiality, Integrity and Availability.

- **Confidentiality:** Keeping data confidential by ensuring that it cannot be accessed either over a network or locally by unauthorized people is a key storage security principle for preventing data breaches.
- **Integrity:** Data integrity in the context of data storage security means ensuring that the data cannot be tampered with or changed.
- **Availability:** In the context of data storage security, availability means minimizing the risk that storage resources are destroyed or made inaccessible either deliberately – say during a DDoS attack – or accidentally, due to a natural disaster, power failure, or mechanical breakdown.

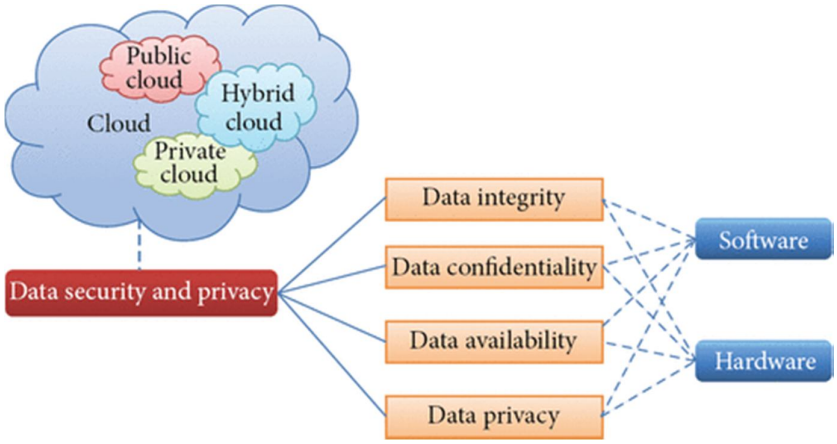



Figure: Organization of data security and privacy in cloud computing.

The relevant international standard for storage security is ISO/IEC 27040 (*provides specific, detailed implementation guidance relevant to storage security for the general security controls for protection of data*), which calls for the application of physical, technical and administrative controls to protect storage systems and infrastructure as well as the data stored within them. It notes that these controls may be: preventive; detective; corrective; deterrent; recovery; or compensatory in nature.

## Data Storage Security: Physical Controls

Physical controls are designed to protect storage resources and the data they contain from physical, as opposed to logical, access by unauthorized or malicious persons. These physical controls come in many forms but may include:

- Guards or other security personnel monitoring data centers and storage resources to prevent unauthorized access.
- CCTV monitoring with video retention.
- Access controls such as biometric readers or smart card readers to prevent unauthorized access.
- Internal environment monitoring using systems such as temperature sensors and smoke detectors.
- Alternative power sources such as a backup generator.

**Data storage security: Technical controls**

Technical controls include many of the security procedures that are familiar to IT security professionals such as network perimeter security measures, intrusion detection and prevention systems, firewalls, and anti-malware filtering.

In relation to data storage security in particular, the following controls are recommended:

**User authentication and access controls:**

- Ensure that users have the minimum privileges
- Ensure that user access rights are retired automatically (when employees leave or are transferred to a new role.)

**Traffic profiling:** One of the most useful controls that can be applied to data storage security is the profiling of normal data access and movement patterns so that anomalous or suspicious behavior can be detected and flagged for closer investigation.

**Monitoring and reporting:** Implement effective monitoring and reporting capabilities, including systems logs, which help to detect and understand security breaches and prevent similar ones in the future.

**Protection of management interfaces:** Many organizations set controls to protect data storage resources and data from unauthorized access while forgetting to secure the management systems themselves. They should consider strong encryption for data both at rest in storage systems and in motion on the network as well as Endpoint protection for all PCs.

**Storage Security: Administrative controls**

Administrative controls come under the three P's: Policy, Planning, and Procedures, all of which play an important role in data storage security. In particular, security policies for data should include where different types of data can be stored, who can access it, how it should be encrypted, and when it should be deleted.

SNIA recommends considering:

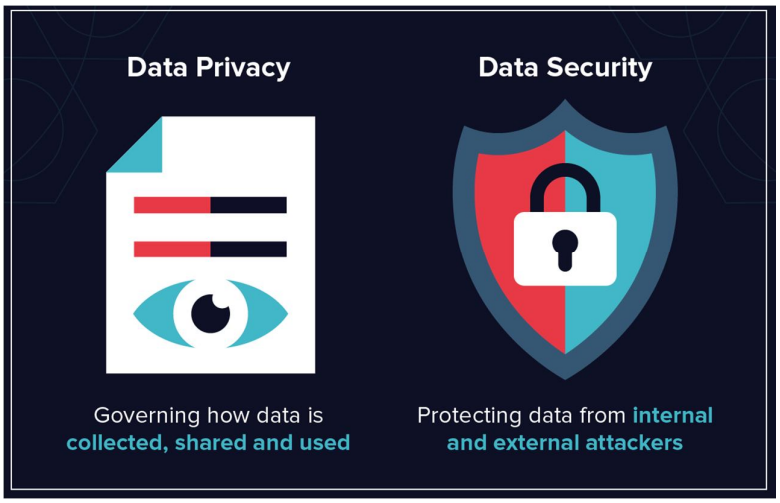
- Incorporating storage considerations into policies after identifying the most sensitive and business-critical data categories
- Integrating storage-specific policies with other policies
- Addressing data retention and protection
- Addressing data destruction and media sanitization
- Ensuring that all elements of storage infrastructure comply with policies

## DATA PRIVACY AND SECURITY ISSUES

Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

Data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used. Data Security and data privacy are often used interchangeably, but there are distinct differences:

- Data Security protects data from compromise by external attackers and malicious insiders.
- Data Privacy governs how data is collected, shared and used.




Data privacy is complying with local and central laws within and also outside your industry to ensure the data you're collecting and the processes behind obtaining and what you do with that data are law abiding. Data security focuses on the technology and tools required to deter cybercriminals from getting their hands on your information such as social security numbers, credit cards, accounts, etc. Both are incredibly important.

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

- Whether or how data is shared with third parties.
- How data is legally collected or stored.
- Regulatory restrictions such as GDPR, HIPAA, GLBA, or CCPA.

There are two drivers for why data privacy is one of the most significant issues in our industry.

- Data is one of the most important assets a company has. With the rise of the data economy, companies find enormous value in collecting, sharing and using data. Companies such as Google, Facebook, and Amazon have all built empires over the data economy. Transparency in how businesses request consent, abide by their privacy policies, and manage the data that they've collected is vital to building trust and accountability with customers and partners who expect privacy.
- Second, privacy is the right of an individual to be free from uninvited surveillance. To safely exist in one's space and freely express one's opinions behind closed doors is critical to living in a democratic society.

"Privacy forms the basis of our freedom. You have to have moments of reserve, reflection, intimacy, and solitude," says Dr. Ann Cavoukian, former Information & Privacy Commissioner of Ontario, Canada.

There are six specific areas of the cloud computing environment where equipment and software require substantial security attention (Trusted Computing Group's White Paper, 2010). These six areas are:

(1) Security of data at rest,
(2) Security of data in transit,
(3) Authentication of users/applications/ processes,
(4) Robust separation between data belonging to different customers,
(5) Cloud legal and regulatory issues, and
(6) Incident response.

(1) For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group's White Paper, 2010). These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact.
(2) Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit.
(3) Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. The trusted computing group's (TCG's) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user's access privilege is revoked or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time.
(4) One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid unintentional or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the trusted platform module (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security.
(5) Legal and regulatory issues are extremely important in cloud computing that have security implications. To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider's policies and practices to ensure their adequacy. The issues to be considered in this regard include data security and export, compliance, auditing, data retention and destruction, and legal discovery. In the areas of data retention and deletion, trusted storage and trusted platform module access techniques can play a key role in limiting access to sensitive and critical data.

(6) As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response o at least automated notification is the best solution for this purpose. The IF-MAP (Metadata Access protocol) of the trusted computing group (TCG) specification enables the integration of different security systems and provides real-time notifications of incidents and of user misbehavior.

The security issues in cloud computing can be categorized into the following three broad classes:

- Traditional security concerns
- Availability issues
- Third party data control-related issues

Traditional Security Issues: These security issues involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Concerns in this category include; VM-level attacks, SQL-injection or cross-site scripting vulnerability, Phishers.

Availability: These concerns center on critical applications and data being available. Well-publicized incidents of cloud outages include Gmail's one-day outage in mid-October 2008, Amazon S3's over seven-hour downtime on July 20, 2008, and FlexiScale's 18-17 hour outage on October 31, 2008. Maintaining the uptime, preventing denial of service attacks and ensuring robustness of computational integrity are some of the major issues in this category of threats.

Third Party Data Control: The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation-independent, but in reality, regulatory compliance requires transparency into the cloud. Various security and data privacy issues are prompting some companies to build clouds to avoid these issues and yet retain some of the benefits of cloud computing. However, the following concerns need to be addressed properly; Due diligence, Auditability, Contractual obligations, Cloud provider surveillance.

In addition, security threats that are relevant in cloud computing and are being detected and researched by academia, security organization and both cloud service providers and the cloud customers.

- Side channel attacks (Data leakage)
- Social networking attacks
- Mobile device attacks
- Mash-up authorization
- Increased authentication demands

## JURISDICTIONAL ISSUES RAISED BY DATA LOCATION

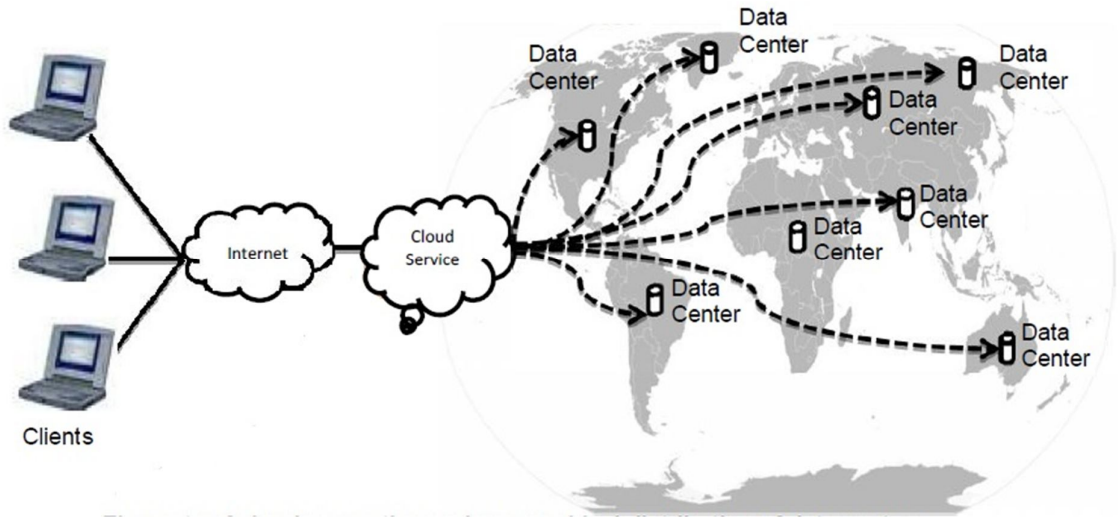
Jurisdictional issues are mostly related to location of data and the specific laws that apply in that location. In cloud services location of data is usually uncertain. The owner of data is not aware of the country where the data is stored. The owner of the data should be aware of the country's court system which will govern the conflict arose between the parties.

Cloud computing service is made up of several elements and can be divided into three aspects: clients, a datacenter, and distributed servers across data centers. Each element has a specific role in delivering cloud service. These elements are:

**The Client**: clients are connected to local area networks; includes desktop, laptops, tablets, mobile phones.

**Data centers**: a data center is a collection of servers where users' applications are stored. It could be a large room full of servers. On the other hand, there may be virtual servers, running half a dozen of virtual servers through one physical server.

**Distributed servers**: Cloud computing does not always use servers in the same physical location, and, often, servers are geographically dispersed. As shown in Figure, data centers are located in different parts of the world, with user data and applications stored across the globe. The client is remotely connected to a data center through the Internet, his data travelling across different political borders. The multiplicity of jurisdictions used in cloud computing raises legal issues concerning data protection as a consequence of the distributed nature of cloud computing.




The Latin words comprising the term "jurisdiction" literally mean "the power to speak the law". The basic concept and/or the definition of "jurisdiction" vary from country to country, depending on the tradition of the given legal system and the approach of local courts. Basically, jurisdiction is determined by three elements:

- The power to prescribe (establish law)
- The power to adjudicate (courts)
- The power to enforce (application of compliance)

These jurisdictional powers can be exercised in a particular nation on the basis of the defendant's nationality. When it comes to analyzing jurisdictional aspects of cloud computing, the basic features of cloud computing - virtualization, the presence of the

Internet, the borderless nature of cloud services, the presence of international and multinational elements, the dynamic distribution of data, and the lack of physical access to the server - create a very difficult jurisdictional situation and complicate data protection issues.

For example, a cloud user from India can potentially be using a US-based cloud service, employing an application developed in Japan and storing data at a data center physically located in Switzerland. If an incident occurs, how would one traces or tracks the data, and who would act as the adjudicating authority? From this perspective, it becomes clear that jurisdictional aspects of cloud computing raise potential data protection issues.

## Jurisdiction aspects of data protection and cloud computing

### The borderless nature of the cloud and applicable jurisdiction:

The concept of cloud computing is globalized, and there are no borders within the cloud. When data travels around the globe across the Internet, it becomes very difficult to locate it. Even if data can be located, it is very difficult to find out the following:

- Who does the data belong to?
- Who processed the data?
- Who is responsible for the loss of data in the cloud in the event of an incident?

It is not clear which laws apply to data protection. The nature of cloud computing requires proper legal arrangements for data protection for global application.

### Applicable law:

Conflicting laws present one of the biggest obstacles to cloud computing services. Cloud computing is distributive in nature: data is collected, used, stored, processed and duplicated (for disaster management) in multiple places, often at the same time. Cloud computing is part of an Internet ecosystem, and it is clear that the same rules will govern cloud computing as any other service that operates over the Internet. These rules are a combination of national laws, foreign laws and international laws and conventions. However, each law has its own limitations (territorial limit) when it comes to the application of the law and its jurisdiction. It has the same implications for cloud computing data.

### National law (state-centric):

As discussed above, jurisdiction is subject to territorial limits (nation-state systems). Cloud computing operates in a territory-free environment, whereas national law is constrained by national borders. Legal aspects of data protection currently depend on the country in which cloud services are offered. In the instance that the cloud provider and user come from different countries, which national law applies? What happens if a data center is located in another country and that country does not have sufficient laws in place to protect the data? Additionally, if relevant laws exist but do not recognize cloud users' rights, how can data be protected? Therefore, national laws cannot regulate cloud computing services directly to protect user data.

### Foreign law:

Cloud computing is still in its infancy in many countries across the world. Not all countries are prepared for or have kept pace with the development of rules and regulations

concerning cloud computing and data protection. The "physical location" of cloud computing data raises the question of legal governance over these data. In cloud services, data is distributed dynamically to its geographical data centers. It is very important to know the data's physical location and the provisions of the prevailing law in that particular country. Data that may be secure in one country may not be secure in another. A foreign government may recognize or refuse users' rights. For this reason, it is essential to include a "choice of law" clause in the terms and conditions of a cloud computing contract.

**International laws:**

International law is a law between two countries. It considers only countries and not private citizens. It cannot be directly applied to individuals. There are two types of international law: public international law and private international law. Public international law governs the relationship between provinces and international entities. Private international law is a set of rules which deal with questions relating to international and multinational transactions. Private international law addresses the following questions:

(1) In which jurisdiction will a court hear the case?

(2) In which jurisdictions does the law apply?

(3) Under what conditions can a national court exercise its jurisdiction to decide multistate disputes?

From a private international law perspective, cloud computing parties in a dispute are often from different countries. This requires a multinational legal system. In the absence of a multinational legal system, private international law can play a role in settling international jurisdiction disputes.

Location and jurisdiction are important for several reasons:

- Organizations are finding it increasingly important to ensure that their data remains within a cloud in their jurisdiction as it is therefore covered by their legal system. This can help maintain control of data.
- Storing important documentation in the cloud is becoming more common, so it makes it easier to copy and transfer documents between jurisdictions. This can be problematic if the data ends up in unscrupulous territory in the wrong jurisdiction.
- Foreign governments can more readily access your data if it is within their own jurisdiction and outside of yours. This is because being permitted access to data within a local jurisdiction is a lot more straightforward than having to obtain access to data under another nation's jurisdiction.
- Data protection laws differ between countries. The laws and regulations of another country can differ greatly from laws in in your own country, in respect to both access of data and who can access it.
- Some countries or jurisdictions may be lacking in the same level of IT or data security that your own affords you. This can result in disproportionate security expectations and assurances across jurisdictions.

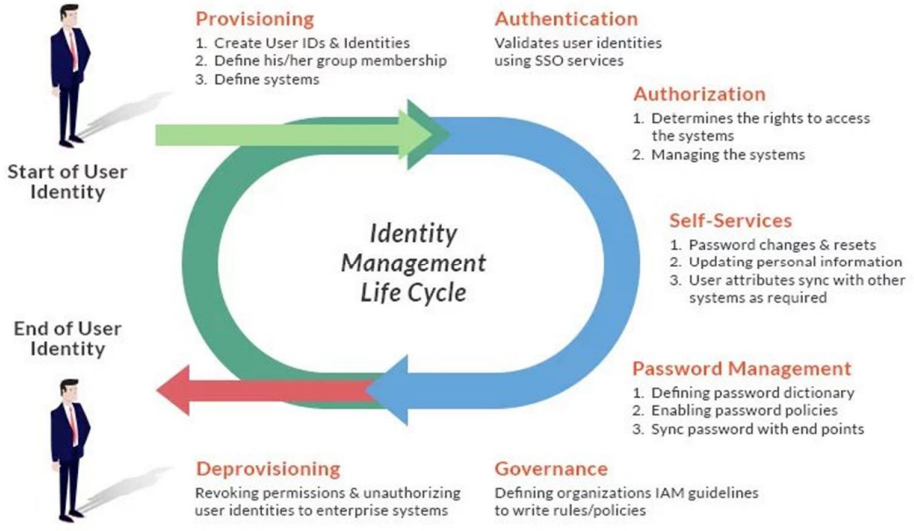
## IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity management has an important role in the area of cloud security issues. Privacy and interoperability are the major issues in the existing identity management approaches, especially in public cloud environments. Identity Management (IdM) is capable of performing functions like, administration, authentication, privileges, authorization, maintenance, policy enforcement, information exchange and roles of the enterprise boundaries. This represents the systematic management of any single identity and provides.

Identity and Access Management (IAM) ratifies that same identity are used and managed for all applications and simultaneously ensures security. It is used to authenticate users, devices or services and to grant or deny rights to access data and other system resources based on pre-established policies. Identity and Access Management (IAM) simplifies the management of large-scale distributed systems. Identity and Access Management (IAM) are used within an enterprise or outside of an enterprise in a business-to-business relationship or even between a private enterprise and a cloud provider.

Identity and Access Management (IAM) provides effective security for cloud systems. IAM systems perform different operations for providing security in the cloud environment that include authentication, authorization, and provisioning of storage and verification. IAM system guarantees security of identities and attributes of cloud users by ensuring that the right persons are allowed in the cloud systems. IAM systems also help to manage access rights by checking if the right person with the right privileges are accessing information that are stored in cloud system. Currently, many organizations use Identity and Access Management systems to provide more security for sensitive information that are stored in the cloud environment. The IAM implemented as the cloud service can benefit the user with all the advantages offered by Security-as-a-Service (SECaaS).

In Cloud Security Alliance (CSA) Security-as-a-Service (SECaaS) defined category of service, the core functionalities of Identity and Access Management are defined as account provisioning/de-provisioning, authentication, authorization, policy management, role based access and federated single sign on.



There are a number of operational areas related to identity and access management. These operational areas ensure that the authorized users are securely and effectively incorporated into the cloud. The operational areas include;

- Identity management and provisioning
- Authentication management
- Federated identity management
- Authorization management
- Compliance management

The Service **Provisioning** Markup Language (SPML) is an XML-based framework that is used for **identity management**. It exchanges resources, user, and service provisioning information between organizations. One of the shortcomings of SPML is that it uses multiple proprietary protocols from various vendors which lead to a bunch of different APIs (Application Peripheral Interfaces). As the APIs are not of the same vendor, it is difficult to make them interact with each other.

**Authentication management** ensures that credentials such as passwords and digital certificates are managed securely.

**Federated Identity Management** authenticates cloud services using the organization's selected identity provider. Federated identity management ensures privacy, integrity and non-repudiation. This also ensures the trust between a web-based application and the identity provider by exchanging Public Key Infrastructure (PKI) certified public keys.

After successful authentication, **authorization management** determines whether the authenticated entity is allowed to perform any function within a given application.

**Compliance management** ensures that an organization's resources are secure and accessed in accordance with the existing policies and regulations.

Presently, IAM systems are the efficient mechanisms to reduce risks associated with cloud environment. Many organizations provide IAM system to secure the information by controlling the access permission of each user. The popular IAM system providers are SailPoint, IBM, Oracle, RSA and Core security.

- SailPoint's identity management solution has capabilities in the areas of password management, compliance control, data access governance, access request, automated provisioning and Single Sign-On.
- IBM Identity and access management suite of products provide solutions in web access request, user provisioning, multi-factor authentication, enterprise single sign-on, privileged identity & access control and user activity compliance.
- Oracle Identity and Access Management provide four major solutions for cloud security. Its products leverage its first solution through the various capabilities in identity administration like, self-service account request, identity life cycle management, password management and enterprise role management.
- RSA SecurID Suite offers a comprehensive set of capabilities including authentication, access management, identity governance, risk analytics and lifecycle management.

- Core Security provides a comprehensive suite of identity management and access governance solutions in the areas of compliance, privileged services, password management and access & identity management.

## ACCESS CONTROL

Today, data is the most valuable asset of a company, safeguarding it is the next thing to do. Data can be secured and protected by ensuring that only the authenticated and authorized users access it. One of the solutions for providing security and privacy to the data is through the use of access control mechanisms.

Access Control in cloud computing gives companies the control to restrict unauthorized user access and, at the same time, give enough access for smooth functioning at work. Among all security requirements of cloud computing, access control is one of the fundamental requirements in order to avoid unauthorized access to systems and protect organizations assets. Access Control in cloud security is a system with which a company can regulate and monitor permissions, or access to their business data by formulating various policies suited chosen by the company. Access control in cloud security helps companies to gain macro-level visibility into their data and user behavior, which a cloud app may not be able to offer, given their on-demand services and mobility.

Access Control allows one application to trust the identity of another application. The traditional model for access control is application-centric access control, where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures. Because in this method we need a lot of memory for storing the user details such as username and password. So cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information.

Each user and each resource is assigned an identity, based on which they may either be granted or denied access to the data. These methods are called the identity-based access control methods. Examples of such methods are;

- Access Control List (ACL)
- User Based Access Control (UBAC) system
- Role-Based Access Control (RBAC) mechanism
- Attribute-Based Access Control (ABAC) mechanism

**Access Control List (ACL):** In this mechanism, the names of all the registered users along with their access privileges to a particular system object are maintained in a list. These system objects may be a file directory or an individual file. The access privileges are the ability to read, write and execute a file. The access control list is generally created by the system administrator or the object owner. So, any time a user requested the use of data or the resource from the cloud, the list was checked to verify whether the user was registered or not. If it was on the list, the user was granted the permission to access the data or the resource.

Disadvantage: It could be used only in a static environment with a limited number of users. The cloud computing environment being a large distributed system could not use the access control list method for access control, mainly because of the huge number of dynamic users.

**Mandatory Access Control (MAC):** It is a system-wide policy decree who is allowed to have access. This mechanism relies on the system to control the access and therefore, an individual user cannot alter the access.
Disadvantage: MAC is not flexible, resulting in user frustration as they cannot dynamically change the underlying access policies. Also, it is difficult and expensive to implement.

**Discretionary Access Control (DAC):** This method centers on the concept of users having control over the system resources. The access control of the objects (e.g., the files and resources) in the system is left to the discretion of the object's owner who determines the object access privileges and thus, can specify which users are granted access to the resources and which users are restricted from accessing the resources.
Disadvantage: Since the users are allowed to control object access permissions, this mechanism makes the system susceptible to Trojan Horse and also, system maintenance and security principles verification are extremely difficult for the DAC systems.

**Role Based Access Control (RBAC):** In this method, security policies are maintained through granting of access rights to roles rather than to individual users. Here, the system assigned roles to all the users and each role was assigned a set of access privileges. Thus, the roles determined the user's access to the system on the basis of the job role. Roles were assigned to the user based on the concept of least privileges, i.e., the role is assigned with the least amount of permissions required for the job to be done. If, at any time, the privileges for a role changed, then it was possible to add or delete the permissions. Hence, any time a user needed to access the cloud, he would be authenticated by his identity and would be allowed to access the data or the resources on the basis of the assigned privileges to the role assigned to him. This resulted in easier overall system maintenance and also, very effective in the verification of security policies.
Disadvantage: This method is suitable for a system with a limited number of users and roles and also, where the user's roles seldom change. However, when this method was extended across administrative domains, problems arose, as it was difficult to decide a role's privileges.

The identity-based access control methods, namely, ACL, MAC, DAC, and RBAC have sometimes been known as the authentication based control methods and require a tight coupling among domains. These methods provide coarse-grained access control and are effective in unchangeable distributed system where there are only a set of users with a known set of services.
Since the growth of the networks as well as the users is always on the rise, identity-based access control was found to lack the strength to support such a large development.

Furthermore, IBAC was problematic for the distributed systems due to the difficulty in managing access to the system and the resources and also, due to the vulnerability to errors. In order to provide fine-grained access control in a large, distributed and dynamic environment such as the cloud, the attribute-based access control (ABAC) was proposed.

**Attribute-based Access Control (ABAC):** In ABAC, users are assigned attributes and access is granted to those users with a certain set of attributes required to access the data or the resources. Users need to be able to prove that they possess the attributes that they claim to own. For this purpose, the access control method relies on authenticating the user at the site as well as at the time of a request. In a way, the ABAC is an extension of the RBAC with features such as delegation of attribute authority, decentralization of attributes and interference of attributes. This makes the ABAC more suitable for the cloud environment that consists of an enormous number of dynamic users, massive amount of storage and also, dynamic and flexible constructions of networks.

ABAC consists of four entities, namely, the requestor, the resource, the service and the environment.

Requestor: one who sends requests to the cloud and invokes actions on the service.

Resource: One or more services act upon it.

Service: software and hardware with a network-based interface and predefined set of operations.

Environment: contains information that might be useful for taking access decisions.

The access policies are specified based on the attributes of all these four entities. With this approach, the access control will be flexible enough to have multiple policies in multiple domains, which is, otherwise, not the case with the traditional access control models, such as, the ACLs, which have their own security policy. In addition, it also provides scalability essential to large scale distributed system.

Role-based access control (RBAC) and Attribute-based access control (ABAC) use the cryptographic primitive known as Attribute Based Encryption (ABE), which enables the data and the information to be encrypted under some access policy and then stored in the cloud. Here, the users possess a set of attributes and are given the corresponding keys. Only those users having the matching set of attributes will be able to decrypt the data and the information stored in the cloud.

## TRUST IN CLOUD COMPUTING SECURITY

Trust is a vital factor, especially for service oriented systems in the area of Information Technology and Security. Several issues have been raised by enterprises and individuals concerning the reliability of the cloud resources. In cloud computing, trust helps the consumer to choose the service of a cloud service provider for storing and processing their sensitive information.

Trust in cloud computing is a measure of reputation of the specific cloud service provider (CSP) which has some set of resources for users. Trust in cloud plays a vital role to make the cloud business grow and the provider can get more profit. To make the provider trustable, some criteria are needed to help the user in selecting a CSP. Thus trust model

acts as a security strength evaluator and ranking service for cloud application and services. It can be used as a benchmark to setup the cloud service security and to find the shortcomings and improvements in cloud infrastructure.

Trust comprises of three factors;

- Expectancy
- Belief
- Willingness to take risks

**Expectancy:** It is when the trustor expects a particular behavior from the trustee party such as providing legal content or efficiently performing cooperative procedures.

**Belief:** The trustor considers that the behavior he has expected would occur based on the information evidence of capability of the trustee, reliability and helpfulness.

**Willingness of taking risk:** For that belief the trustor is prepared to take risk.

It is essential to note that the trustor cannot control the expected behavior of trustee; the trustor's faith in those predictable actions of trustee is dependent on the ability of trustee, capability and integrity.

The truthfulness of the trustee gives the trustor an assurance with reference to the expectedness of the trustee's behavior.

The trust in cloud computing is divided into various categories namely;

- Reputation Based Trust
- SLA verification based trust
- Policy-based trust
- Evidence-based trust
- Societal trust

**In Reputation Based Trust**, the reputation of an entity is the collected estimation of public's trust towards that entity. Generally, many entities in a community trust an entity that has high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee. The reputation of cloud affects the selection process of cloud services; therefore, CSPs try to construct and preserve higher reputation. Reputation is classically represented by a broad score reflecting the overall outlook, or a small number of scores on numerous foremost aspects of performance.

**In SLA verification based trust**, after establishing the preliminary trust and accessing a cloud service, the cloud user is required to validate and re-examine the trust value. SLA is a lawful agreement between the two communicating parties: user and provider. Therefore, monitoring the QoS parameters and verification of SLA document are essential source of trust management for cloud computing. A third CSP party is required to provide these types of services.

**In Policy-based trust**, it is required to construct a "formal". In a related area, Public Key Infrastructure (PKI) is an extensively used technology that utilizes "formal" trust methodologies to support key certification, digital signature and validation. It also supports data attribute certification and validation. In this, the trust in a Certification

Authority (CA) is dependent on the CA's confirmation with definite certificate policies. It is taken w.r.t to delivering and retaining public key certificates which are validated. Certificate policies play a main role in PKI trust.

**In Evidence-based trust**, a belief of trustor in the predictable behavior of trustee is based on the proof about attributes of adaptness, helpfulness and honesty.

**Societal trust** consists of any individual and a company. In cloud also, each entity must be trusted. In Information security service sector, trust plays a vital role between the supplier and the client to help the business grow.

**TRUST MODEL:** The trust model is defined as the scale of trust among two parties on each other (between customer and CSP). Such relation has some scope defined which is security threats. When the service provider monitors the actions of cloud system, the user or the clients generate ratings. There are two outlooks to define a trust model in computing world:

Customer's outlook - what security does the service provider have?

Provider's outlook – what type of customer does it have?

The clients must be informed about the security faults and vulnerabilities that exists in the system or that have the possibilities. Trust model is nothing but some set of protocols which are to be followed by the service provider and their users or customers. Users also have the facility to provide some rules to overpower the activities on cloud according to their choices. The syntax of the protocol must be in understandable and standard form.

Trust models are classified based on trust management;

Types of Trust management based on flow of control

| **Type of Management** | **Main Policy** |
|---|---|
| Centralized trust management | After one transaction completion the client report rating to the trusted party. |
| Decentralized trust management | A peer to peer system is present. |
| Distributed trust management | Data is shared among different brokers |

Types of Trust management based on flow of transaction

| **Type of Management** | **Management Strategy** |
|---|---|
| Static trust management | Rules are defined by trust administration system |
| Dynamic trust management | Profiles are as a trust model engine which defines trust. |

Static trust model have a predefined design and flow of the process of transaction. Dynamic model works with future activities and unidentified process flow. The static model works according to system manner but dynamic model adjusts with different parameters and progress based on the previous cached data stored in a data store.

## REPUTATION IN CLOUD SECURITY

**Reputation** is gained through trust which might be through self-experience or through existing user's recommendation. Reputation is the assessment of the tasks which ensures the derived trust based services in cloud.

Trust and reputation are related, but different. Basically, trust is between two entities; but the reputation of an entity is the aggregated opinion of a community towards that entity. Usually, an entity that has high reputation is trusted by many entities in that community.

In the cloud computing environment, reputation can be used to the trust assessment between consumers and cloud providers. Thus, the reputation is seen as a collective measure calculated through several values related to the historical behavior of participants in a community.

Cloud users basically require the reputed system to guarantee the security in cloud services. Thus the reputation which gains the trusted users might be able to access very cheaper services especially in Infrastructure as a service (Iaas), Platform as a service (Paas) and Software as a service (Saas) with a secure cloud environment.

Generally, the reputation can be reported to the user by means of two approaches:

**Qualitative:** that refers to a set of categorical values, such as trustable or very trustable.

**Quantitative:** that refers to a numerical value in a given range.

Cloud providers' reputation is assumed as an aggregated value generated through a two historical trust indicators:

- Objective (QoS indicators)
- Subjective (users' ratings)

Thereby, a user who needs to interact with a cloud provider uses the reputation to establish a trust relationship in order to use the available cloud resources.

Reputation systems are widely used in Peer-to-Peer Networks (P2P) and E-Commerce systems. Peer-Trust is a P2P reputation system, where the reputation of a peer is based on the given feedbacks from others who interacted with it. Also, the reputation considers several factors: feedback from other peers; amount of transactions; credibility factor, and community and context factor. The Beta Reputation System is a e-commerce reputation system that calculates the entities reputation using a beta distribution probability, where the entities reputation is based on the amount of positive and negative transactions.

The reputation architecture comprises following modules, namely:

- Monitoring module
- Reputation Manager (RM)
- Data Repository
- Reputation Broker Service (RBS)
- Aggregation Module

**The Monitoring Module** is responsible for monitoring and updating QoS indicators of each CSP, during the operation stage. The QoS monitoring represents an important role during the verification of the promised QoS in the SLA.

**The Reputation Manager (RM)** is an external interface that offers the architecture's operations and communicates with other members, for example, a user wants to know the reputation of a cloud provider or evaluates a cloud provider. Also, RM module collects users' feedback.

**The Data Repository** stores historical and current values for QoS values and the subjective historical evaluations from users to cloud providers (member's feedbacks).

**The Reputation Broker Service Module** is the inter-face through which communication occurs with others members. It receives service specifications and QoS values from cloud service providers, in order to each cloud provider participate in the proposed architecture.

**The Aggregation Module** uses the historical objective and subjective data to calculate the cloud provider's reputation based on QoS indicators and users feedbacks.

## SECURITY RISK

In spite of security advantages such as improved collaboration, excellent accessibility, Mobility, Storage capacity, etc., cloud computing paradigm also introduces some key security challenges/risks.

Some most common Security Risks of Cloud Computing are given below-

1. **Data Loss/Leakage**

   Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices.

2. **Data Breach**

   Data breach is an incident that exposes confidential or protected information. A data breach might involve the loss or theft of your Social Security number, bank account or credit card numbers, personal health information, passwords or email.

   A data breach can be intentional or accidental. A cybercriminal may hack the database of a company where you've shared your personal information. Or an employee at that company may accidentally expose your information on the Internet. Either way, criminals may access your key personal details and profit from them at your expense. Retailers, hospitals, corporations, government offices and colleges have all been targets of data breaches.

3. **Insecure APIs and Interfaces**

   As we all know, cloud computing is completely depends on Internet and some services are available in the public domain. Cloud Service Providers provide these services and set of application programming interfaces (APIs) that customers use to manage and interact with cloud services. Organizations/customers use these

APIs to provision, manage, coordinate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc. Unlike management APIs for on-premises computing, CSP APIs are accessible via the Internet exposing them more broadly to potential exploitation.

Threat actors look for vulnerabilities in management APIs. If discovered, these vulnerabilities can be turned into successful attacks, and organization cloud assets can be compromised. From there, attackers can use organization assets to execute further attacks against other CSP customers.

4. **Account Hijacking**

Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen or hijacked by an attacker/hacker. Cloud account hijacking is a common tactic in identity theft schemes in which the attacker uses the stolen account information to conduct malicious or unauthorized activity. When cloud account hijacking occurs, an attacker typically uses a compromised email account or other credentials to impersonate the account owner.

5. **Malicious Insiders**

Malicious insiders can be current or former employees, contractors or business partners that gains access to an organizations network, system or data and release this information without permission by the organization. Malicious insiders are the members who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems. It does not include well-meaning staff that accidentally put your cyber security at risk or spill data.

There are many reasons an insider can be or become malicious including revenge, coercion, ideology, ego or seeking financial gain through intellectual property theft or espionage.

6. **Increased Complexity Strains IT Staff**

Migrating to the cloud can introduce complexity into IT operations. Managing, integrating, and operating in the cloud may require that the agency's existing IT staff have to learn a new model. IT staff must have the extra capability and skill level to manage, integrate, and maintain the migration of assets and data to the cloud in addition to their current responsibilities for on-premises IT.

7. **Insufficient Due Diligence**

Organizations migrating to the cloud often perform insufficient due diligence. They move data to the cloud without understanding the full scope of doing so, the security measures used by the CSP, and their own responsibility to provide security measures. They make decisions to use cloud services without fully understanding how those services must be secured.

8. **Abuse and Nefarious Use**

The threat of abusing cloud services is somewhat unique in that it involves the risk of insider threat as well as the risk posed by cyber criminals to join the cloud and

misuse its services. Abuse and nefarious use of cloud computing is considered as the top security threat to cloud computing because cloud providers do not enforce any strong registration process where any person with a valid credit card can register to receive cloud services.

Some cloud service providers offer readily available free limited trial period of cloud services which presents a perfect opportune time for cyber criminals to join the cloud and possibly misuse and abuse their access privilege to cloud services. Attackers can exploit this threat and launch an attack called "cloud computing malware injection attack" by creating their own implementation module (e.g. PaaS or SaaS) within the cloud environment and trick the cloud system to treat that malicious instance as a valid instance for the particular service module.

**9. Vendor Lock-in**

Vendor lock-in is one of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another. If a selected service provider goes out of business, it becomes a major problem since data can be lost or cannot be transferred to another CSP in a timely manner.

**10. System Vulnerabilities**

System vulnerabilities are closely related to the insecure APIs threats. Basically, "system vulnerabilities" is the term used for any exploitable bugs or features in a program that hackers can use to compromise a computer system or program. There are many different common vulnerabilities and exposures. The damage caused by system vulnerability exploits can vary depending on the nature of the exploit, but common consequences include loss of data/service, data breaches, and heavy recovery/repair expenses.

**11. Denial of Service (DoS) attacks**

Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

In cloud computing, a DoS attack can be described as an attack designed to prevent some cloud computing service or resource from providing its normal services for a period of time. DoS attacks compromise the availability of the cloud resources and services and often target the computer networks' bandwidth or connectivity. The bandwidth attacks are aimed to forward large traffic to consume all the available network resources. Moreover, connectivity attacks flood the victim by sending a high volume of connection requests that cause all the available operating system resources in the victim to be consumed and as a result the legitimate user requests cannot be handled.

**12. Insufficient Identity, Credential, and Access Management**

We have all gotten those emails from Visa, LinkedIn, or the like, stating you need to reset your password. This is usually due to a security breach or stolen user information, such as credentials. Your Username and Passwords are sacred, and can be used against you when in the wrong hands. This is why multi-factor authentication is vital to any business. Two-factor takes information the user knows, such as a password, and matches it with a single-use encrypted key. Multi-factor authentication also includes identity verification such as biometric verification. When the systems for managing access to an application are lacking, it's easier for hackers to fake their way past protection protocols by imitating the identities of authorized users with stolen account credentials.

**13. Data Deletion is Incomplete**

Threats associated with data deletion exist because the consumer has reduced visibility into where their data is physically stored in the cloud and a reduced ability to verify the secure deletion of their data. This risk is concerning because the data is spread over a number of different storage devices within the CSP's infrastructure in a multi-tenancy environment. In addition, deletion procedures may differ from provider to provider. Organizations may not be able to verify that their data was securely deleted and that remnants of the data are not available to attackers. This threat increases as an agency uses more CSP services.

## AUTHENTICATION IN CLOUD COMPUTING

Cloud computing is helping organizations to store a large amount of data at relatively low costs but it is essential these service providers offer methods to ensure users are authenticated. Authentication is the process that allows the user to provide proof of his identity. Authentication serves as a protection against different sorts of attacks where the goal is to confirm the identity of a user. It is often done through the login method, based on the using of a username and a password. This static mechanism leaves the system vulnerable to attacks, since hackers can use many techniques, such as sniffing and guessing, to steal user passwords. So, to alleviate the problems associated with identity theft, it is essential to adopt a strong form of authentication techniques.

Multiple authentication technologies (username and password, multi-factor authentication, mobile trusted module, public key infrastructure, single sign-on, and biometric authentication) have been put forward so far that confirm user identity before giving the permit to access resources.

The user authentication is generally based on three factors;

- Something he knows
- Who is he and
- What he possesses

**Something he knows** may be a password, a pass phrase, a pin number or a secret question. Face recognition, iris scan or the other authentication methods based on body parts allow to identify **who is the user**. Finally, **something that the user possesses** may be a smart card, software token or even a mobile phone. When authentication is

performed by combining two or more of these factors, it is named a two or a multiple factor authentication.

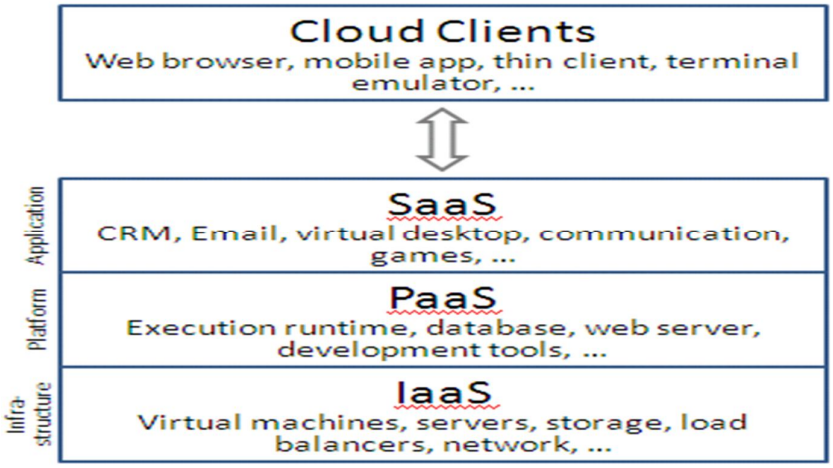
There are multiple authentication techniques in cloud computing suited for different applications and use cases when it comes to the cloud. The best cloud authentication method depends on your preferences but each is a supported method. These methods are typically employed to increase cloud security.

1. **Authentication via username and password**: The important point in authentication is to protect data from the access of unauthorized people. This entails that the servers reject visit requests from unknown people and manage the access of the confirmed users. In this authentication method, the user should enter the username and password to log in to the system and can then access the information in the cloud.
2. **Multi-factor authentication (MFA):** The traditional authentication method via password cannot sufficiently provide information security against the majority of modern attacks in a cloud computing environment. A secure method is multi-factor authentication. Not only does this method confirm any pair of username/password, but also it requires a secondary factor such as biometric authentication. Of course, the feasibility of the second factor is limited owing to deployment complexity and high expenditure.
3. **Public Key Infrastructure (PKI):** Old authentication systems are based on hidden key mainly supporting traditional asymmetrical encryption algorithms, such as RSA. It uses a private key to confirm user identity. PKI has been adopted in the design of security protocols such as SSL/TSL and the use of SET mainly to provide authentication. PKI success depends on the control of access to private keys similar to other types of encryption systems. PKI mechanism should provide data confidentiality, data comprehensiveness, non-repudiation, strong authentication, and permit issuance.
4. **Single sign-on (SSO):** SSO is an identity management system where a user may be validated in a single authentication and can then access other limited resources without a repeated authentication. In other words, authentication information is generated by using different programs in this method. SSO is a way to access an independent multiple software system where a user logs in to a system and accesses all systems without a need to log in again to a program.
5. **Biometric authentication:** Biometric authentication supports three factors of information security, namely authentication, identification, and non-repudiation. This mechanism is based upon the identification of physiological or behavioral characteristics of a person. There are several physical biometric authentication techniques such as hand geometry recognition, fingerprint recognition, palm print recognition, voice recognition, face recognition, retinal scan, and iris scan. The behavioral technique identifies the users according to their location, typing pattern, profile, etc. Two important types of behavioral biometrics are keystroke analysis, and signature recognition.

6. **Trusted Computing Group (TCG):** Trusted computing group introduces a set of properties to measure, store, and report software and hardware comprehensiveness via Root-of-Trust hardware that consist of TPM (Trusted Platform Module) and MTM (Mobile Trusted Module) modules. MTM is a security factor to be adopted in mobile devices. Contrary to TPM module that is used for PCs, MTM is used in mobile devices. However, in higher levels of isolated protection, an MTM can be executed as a slightly altered TPM.

## CLIENT ACCESS IN CLOUD

A *Cloud Client* consists of computer hardware and/or software that relies on cloud computing for application delivery. A Cloud Client could also be specifically designed for delivery of cloud services. In either case, the Cloud Client is essentially useless without Cloud Services. A cloud client is an interface of the cloud to the common computer user through web browsers and thin computing terminals. So the term cloud client describes a piece of hardware, a piece of software or both, that is specially designed for a cloud service. Examples of Cloud Clients include computers, phones and other devices, operating systems and browsers.




Users access cloud services by using networked cloud client devices, such as desktop computers, laptops, tablets and smartphones. Some cloud clients rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application. Some cloud applications, however, support specific client software dedicated to these applications (e.g., virtual desktop clients and most email clients). Some legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology.

## CLOUD CONTRACTING MODEL

Today it is possible to contract for 'on-demand' computing which is internet-based whereby shared resources and information are provided. Analogous to a utility, the advantages of the 'Cloud' allow the cost of the infrastructure, platform and service delivery to be shared amongst many users.

Contracting techniques for cloud services have matured since the early 2010s and continue to evolve rapidly, supporting the deep digital transformation and emerging business patterns that the cloud is enabling. Contracting for cloud services is one of a number of rapidly evolving areas of cloud computing law.

A cloud service contract sets out the legal basis upon which a customer for cloud-based services accesses and uses those services. Cloud contracts contrasted with outsourcing, software licenses and professional services agreements. Essentially, cloud services are generally provided on a 'one to many' basis (where a useful analogy is that the customer taking a room at the CSP's hotel) while outsourcing and professional services (typically implementation services) are provided 'one to one'.

'Notice' provisions are common in contracts. It follows that if you are contracting for computing resources delivered over the internet, you want clearly defined notice provisions that would require notice of any security breaches as well as any discovery requests made in the context of litigation. 'Storage' is also a key concept and term to be addressed and warrants special attention. From a risk management standpoint you also want to understand the physical location of the equipment and data storage. Perhaps geographical distance and diversity is both a challenge and an opportunity in terms of risk management.

Consider the type of contractual arrangement. Is the form of contract essentially a 'service', 'license', 'lease' or some other form of contractual arrangement? Service agreements, licenses and leases have different structures. Perhaps the contract for Cloud computing services contains aspects of all these different types of agreements, including ones for IT infrastructure. Yet, such considerations are common to all contracting efforts.

Although the issues are many, they are closely related to what any good negotiator or contract manager would consider early on.

### Cloud Contracting Model

**Licensing Agreements vs Services Agreements**

**A traditional software license agreement** is used when a licensor is providing a copy of software to a licensee for its use. This copy is not being sold or transferred to the licensee, but a physical copy is being conveyed to the licensee. The software license is important because it sets the terms under which the software may be used by the licensee. The license protects the licensor against the inadvertent transfer of ownership of the software to the person or company that holds the copy.

It also provides a mechanism for the licensor of the software to retrieve the copy it provided to the licensee in the event that the licensee;

(a) stops complying with the terms of the license agreement or

(b) stops paying the fee the licensee charges for the license.

**A service agreement,** on the other hand, is not designed to protect against the perils of providing a copy of software to a user. It is primarily designed to provide the terms under which a service can be accessed or used by a customer. The service agreement may also set forth quality parameters around which the service will be provided to the users.

Shrink-wrap, Click-wrap and Browse-wrap are common types of contracts used in electronic commerce.

***Shrink wrap* contracts** are license agreements or other terms and conditions which are packaged with the products. The usage of the product considers the acceptance of the contract by the consumer.

Shrink-wrap assertions are unsigned permit understandings which state that acknowledgment on the client of the terms of the assertion is demonstrated by opening the shrink-wrap bundling or other Bundling of the product, by utilization of the product, or by some other determined instrument.

A ***click-wrap agreement*** is mostly found as part of the installation process of software packages. It is also called a "click-through" agreement or click-wrap license. It is a take-it or leave-it contract which lacks bargaining power. A click-wrap assertion is a kind of agreement that is broadly utilized with programming licenses and online exchanges in which a client must consent to terms and conditions before utilizing the item or administration. Click-wrap agreements can be of the following types:

1. Type and Click where the user must type "I accept" or other specified words in an on-screen box and then click a "Submit" or similar button. This displays acceptance of the terms of the contract. A user cannot proceed to download or view the target information without following these steps.
2. Icon Clicking where the user must click on an "OK" or "I agree" button on a dialog box or pop-up window. A user indicates rejection by clicking "Cancel" or closing the window. The terms of service or license may not always appear on the same webpage or window, but they must always be accessible before acceptance.

***Browse-wrap agreements*** cover the access to or use of materials available on a website or downloadable product. Only if the person agrees to the terms and conditions on the web page, then he can access the contents of the web page.

In most cases, the website or the browse-wrap includes a statement that the user's continued use of the website or the downloaded software manifests assents to those terms. Many times, the terms mentioned in the browse-wraps are explicitly displayed on the website but the existence of such browse wrap is hidden or not seen on the page.

## COMMERCIAL AND BUSINESS CONSIDERATIONS

Cloud computing can benefit businesses in many ways, from cutting costs, to increasing business efficiency, to guaranteeing data recovery in case of an accident. The cloud computing market has evolved in recent years. The commercial offerings of service providers have become more flexible, and we have also seen changes in providers' traditional 'take it or leave it' approach to cloud contract terms.

Moving to the Cloud can be complicated. Not all data, applications, and files are suited for cloud storage and security issues may arise if proper safeguards are not implemented properly.

As potential cloud users assess whether to utilize cloud computing, there are several commercial and business considerations that may influence the decision-making. Many of the considerations presented below may manifest in the contractual arrangements between the cloud provider and cloud user.

**Understand provider's terms**

Cloud computing services are generally implemented on the provider's terms - although it can often be a struggle to figure out exactly what those terms are. Contracts for private cloud solutions and with system integrators/resellers allow more scope for negotiation than contracts with public cloud providers. However, even in public cloud deals, terms are increasingly negotiable - although the degree of negotiability certainly pales in comparison with traditional outsourcing contracts. Some of the key issues that tend to recur in cloud contract negotiations include:

- Customer control and visibility over subcontracting
- Limitations on the provider's ability to change the nature of the services.
- Privacy and data security commitments
- Rights of the provider to suspend services, e.g., for non-payment or violation of an acceptable use policy
- Limitations of liability
- Exit provisions allowing the customer to extend service for a period after termination or expiry to allow migration to the replacement solution

**Due diligence**

Because of the constraints on your ability to negotiate the provider's cloud terms, it's essential to carry out appropriate due diligence on the provider. Areas of focus should include:

- Location of services
- Service performance and usability
- Existing customers (references)
- Data location, processing, portability and recovery
- Security
- Interoperability
- Business continuity
- Exit

**Data privacy remains center stage**

It's also vital to understand how responsibility for data privacy obligations will be allocated between you and the provider, including who is responsible for data security.

Typically, providers have been more willing to take on responsibility for network integrity. For example, there has been an increased willingness of providers to adopt the

EU model clauses for data transfer. In addition, many providers now offer European-based data centers, reacting to commercial pressures from Europe-based clients.

When evaluating cloud solutions:

• classify the data concerned (including its sensitivity), and consider what would happen if data was disclosed, lost or corrupted

• consider what the business impact would be if you were unable to use the data

• check whether the provider is compliant with ISO/IEC 27001/2 and, if a public cloud provider, ISO/IEC 27018

• ensure that your deployment of cloud will comply with applicable data protection law, taking into account all relevant regulatory guidance

**Performance commitments are hard to find**

Ensure that you are comfortable with the level of service performance commitment offered by the cloud provider. Most cloud contracts remain pretty light in terms of service levels, with availability being the typical measurement metric. Check the wording of the SLAs carefully – watch out for references to 'service levels designed to be available', 'target service levels', etc.

Also, identify the remedies available for service failure – it's common for providers to offer credit for additional services, despite the fact that it's hard to see 'more of the same' as a valuable remedy.

**Regulators are taking notice**

If you are a regulated entity, you will need to take account of relevant regulatory guidance. For example, the FCA published draft guidance on cloud computing in November 2015. This high level guidance is aimed at ensuring regulated firms appropriately identify and manage risks relating to the deployment of cloud-based solutions. Issues identified in the guidance include:

- Legal and regulatory considerations
- Oversight and audit
- Change management
- Exit
- Risk management
- Data privacy and security
- Business continuity

Ultimately, you need to approach cloud transactions with a large amount of practicality, accepting that it may be very difficult to negotiate material changes to a cloud provider's terms. You need to carry out a thorough risk/benefit analysis exercise in order to evaluate whether the particular cloud solution is right for your business. If you perceive the risks to be so great that significant contract negotiation seems essential before putting services in the cloud, it may be that cloud isn't the right solution for you after all.