Challenges In Cloud Security

More and more organizations are moving their applications and associated data to cloud to reduce costs and reduce the operational and maintenance overheads, and one of the important considerations is that of security of the data in the cloud. Most cloud service providers implement advanced security features similar to those that exist in in-house IT environments. However, due the out-sourced nature of the cloud, resource pooling and multi-tenanted architectures, security remains an important concern in adoption of cloud computing. In addition to the traditional vulnerabilities that exist for web applications, the cloud applications have additional vulnerabilities because of the shared usage of resources and virtualized resources. Key security challenges for cloud applications include:

Authentication

Authentication refers to digitally confirming the identity of the entity requesting access to some protected information. In a traditional in-house IT environment authentication polices are under the control of the organization and the process of confirming identity is usually restricted to the employees of the organization. Even in scenarios where users outside an organization need to be authenticated, the authentication policies are always under the organization's control and can be altered at their own convenience. However, in cloud computing environments, where applications and data are accessed over the internet, the complexity of digital authentication mechanisms increases rapidly. Alteration of authentication and authorization policies requires the involvement of the cloud service provider's systems and services.

Authorization

Authorization refers to digitally specifying the access rights to the protected resources using access policies. In a traditional in-house IT environment, the access policies are controlled by the organization and can be altered at their convenience. An organization, for example, can provide different access policies for different departments. Authorization in a cloud computing environment requires the use of the cloud service providers services for specifying the access policies.

Security of data at rest

Due to the multi-tenant environments used in the cloud, the application and database servers of different applications belonging to different organizations can be provisioned side-by-side increasing the complexity of securing the data. Appropriate separation mechanisms are required to ensure the isolation between applications and data from different organizations.

Security of data in motion

In traditional in-house IT environments all the data exchanged between the applications and users remains within the organization's control and geographical boundaries. Organizations believe that they have complete visibility of all the data exchanged and control the IT infrastructure. With the adoption of the cloud model, the applications and the data are moved out of the in-house IT infrastructure to the cloud provider. In such a scenario, organizations have to access their applications with the data moving in and out of the cloud over the internet. Therefore, appropriate security mechanisms are required to ensure the security of data in, and while in, motion.

Data Integrity

Data integrity ensures that the data is not altered in an unauthorized manner after it is created, transmitted or stored. Due to the outsourcing of data storage in cloud computing environments, ensuring integrity of data is important. Appropriate mechanisms are required for detecting accidental and/or intentional changes in the data.

Auditing

Auditing is very important for applications deployed in cloud computing environments. In traditional in-house IT environments, organizations have complete visibility of their applications and accesses to the protected information. For cloud applications appropriate auditing mechanisms are required to get visibility into the application, data accesses and actions performed by the application users, including mobile users and devices such as wireless laptops and smartphones.

CSA Cloud Security Architecture

The Cloud Security Alliance (CSA) provides a Trusted Cloud Initiative (TCI) Reference Architecture [46] which is a methodology and a set of tools that enable cloud application developers and security architects to assess where their internal IT and their cloud providers are in terms of security capabilities, and to plan a roadmap to meet the security needs of their business. The Security and Risk Management (SRM) domain within the TCI Reference Architecture provides the core components of an organization's information security program to safeguard assets and detect, assess, and monitor risks inherent in operating activities. Figure 12.1 shows the SRM domain within the TCI Reference Architecture of CSA. The sub-domains of SRM include:

Governance, Risk Management, and Compliance

This sub-domain deals with the identification and implementation of the appropriate organizational structures, processes, and controls to maintain effective information security governance, risk management and compliance.

Information Security Management

This sub-domain deals with the implementation of appropriate measurements (such as capability maturity models, capability mapping models, security architectures roadmaps and risk portfolios) in order to minimize or eliminate the impact that security related threats and vulnerabilities might have on an organization.

Privilege Management Infrastructure

The objective of this sub-domain is to ensure that users have access and privileges required to execute their duties and responsibilities with Identity and Access Management (IAM) functions such as identity management, authentication services, authorization services, and privilege usage management.

Threat and Vulnerability Management

This sub-domain deals with core security such as vulnerability management, threat management, compliance testing, and penetration testing.

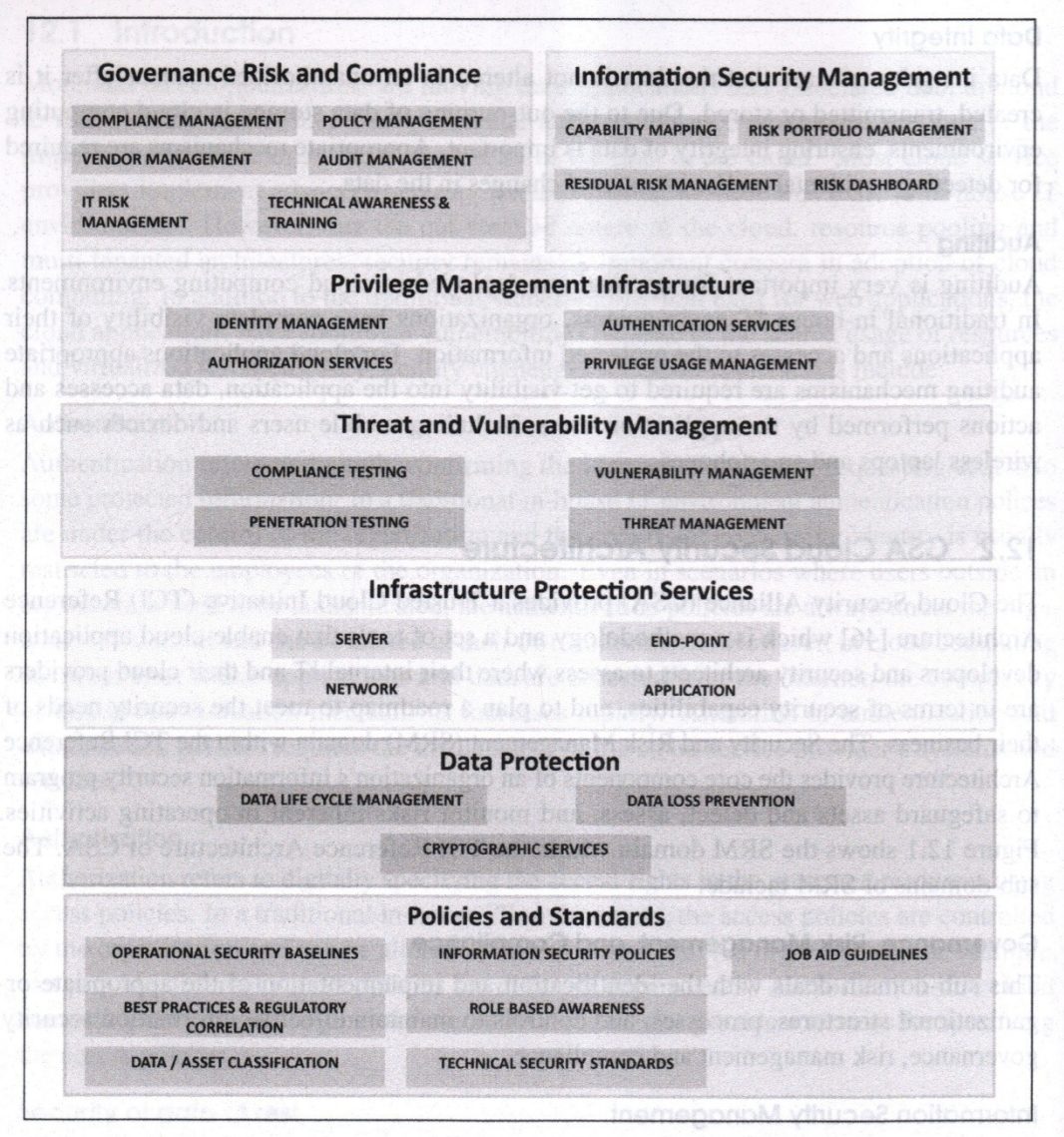
Infrastructure Protection Services

This objective of this sub-domain is to secure Server, End-Point, Network and Application layers.

Data Protection

This sub-domain deals with data lifecycle management, data leakage prevention, intellectual property protection with digital rights management, and cryptographic services such as key management and PKI/symmetric encryption.

Policies and Standards: Security policies and standards are derived from risk-based business requirements and exist at a number of different levels including Information Security policy, Physical Security Policy, Business Continuity Policy, Infrastructure Security Policies, Application Security Policies as well as the over-arching Business Operational Risk Management Policy.



Network level security

Network-level encryption is best suited for cases where the threats to data are at the network or storage level and not at the application or host level. Network-level encryption is performed when moving the data form a creation point to its destination using a specialized hardware that encrypts all incoming data in real-time. The application and host levels remain unencrypted. Network-level encryption is operating system independent. The advantage of this network- level encryption is that it is simple to implement and requires no changes in the existing data infrastructure. Keys are managed in hardware. However, the disadvantage of this encryption level is that it is the least scalable of all the levels. As the data volume increases, a single encryption appliance can become abottleneck.

Host level security

In host-level encryption, encryption is performed at the file-level for all applications running on the host. Host level encryption can be done in software in which case additional computational resource is required for encryption or it can be performed with specialized hardware such as a cryptographic accelerator card. The advantage of host-level encryption is that it is highly secure and suited well for active data files across all applications running on a host. However, like application-level encryption, key management can be challenging. Keys are stored in the host memory or a separate key server.

Application level security

Application level encryption involves encrypting application data right at the point where it originates i.e. within the application. Application level encryption provides security at the level of both the operating system and from other applications. Therefore one application cannot decrypt data of another application. An application encrypts all data generated in the application before it flows to the lower levels and presents decrypted data to the user. The advantage of application level encryption is that it provides security against operating system and network attacks and also data theft. However, key management is challenging task for application level encryption. Keys can be stored either in memory or a file or on a separate key server. The application performance is affected in case of key rotation, where the application reads and decrypts the data using an old key and then encrypts the data using the new key, while it is processing other requests.

Data Privacy

A risk assessment and gap analysis of controls and procedures must be conducted. Based on this data, formal privacy processes and initiatives must be defined, managed, and sustained. As with security, privacy controls and protection must an element of the secure architecture design.

Depending on the size of the organization and the scale of operations, either an individual or a team should be assigned and given responsibility for maintaining privacy.

A member of the security team who is responsible for privacy or a corporate security compliance team should collaborate with the company legal team to address data privacy issues and concerns. As with security, a privacy steering committee should also be created to help make decisions related to data privacy.

Typically, the security compliance team, if one even exists, will not have formalized training on data privacy, which will limit the ability of the organization to address adequately the data privacy issues they currently face and will be continually challenged on in the future.

The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

For example, customer contractual requirements/agreements for data privacy must be adhered to, accurate inventories of customer data, where it is stored, who can access it, and how it is used must be known, and, though often overlooked, RFI/RFP questions regarding privacy must answered accurately.

This requires special skills, training, and experience that do not typically exist within a security team.

As companies move away from a service model under which they do not store customer data to one under which they do store customer data, the data privacy concerns of customers increase exponentially.

This new service model pushes companies into the cloud computing space, where many companies do not have sufficient experience in dealing with customer privacy concerns, permanence of customer data throughout its globally distributed systems, cross-border data sharing, and compliance with regulatory or lawful intercept requirements.

Data Security

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider.

Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the United States.

It can also force encryption of certain types of Payment Card Industry Data Security Standard (PCI DSS). True unified end-to-end security in the cloud will likely requires an ecosystem of partners.

Application Security

Application security is one of the critical success factors for a world-class SaaS company. This is where the security features and requirements are defined and application security test results are reviewed.

Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams.

Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement.

This should be a collaborative effort between the security and product development team. External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly.

Fragmented and undefined collaboration on application security can result in lower-quality design, coding efforts, and testing results.

Since many connections between companies and their SaaS providers are through the web, providers should secure their web applications by following Open Web Application Security Project (OWASP)[1] guidelines for secure application development and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks in the cloud, just as you would on-premises.
LAMP is an open-source web development platform, also called a web stack, that uses Linux as the operating system, Apache as the web server, MySQL as the relational database management system RDBMS, and PHP as the object-oriented scripting language. Perl or Python is often substituted for PHP.

1

Virtual Machine Security

In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers.

Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.

By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely.

To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources.

Integrity monitoring and log inspection software must be applied at the virtual machine level.

This approach to virtual machine security, which connects the machine back to the mother ship, has some advantages in that the security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings for both the service provider and the enterprise.

Identity & Access Management

Identity management provides consistent methods for digitally identifying persons and maintaining associated identity attributes for the users across multiple organizations. Access management deals with user privileges. Identity and access management deal with user identities, their authentication, authorization and access policies. Authentication and authorization approaches were described in the previous section. Let us look at the Federated Identity Management approach. Federated identity management allows users of one domain to securely access data or systems of another domain seamlessly without the need for maintaining identity information separately for multiple domains. Federation is enabled through the use single sign-on mechanisms such as SAML token and Kerberos. With federated identify management the identity credentials stay with the identity provider at a trusted place and multiple applications from different organizations can use the identity credentials for user authentication.

Standardized access control policies ensure confidentially of data. Role-based access control approaches are used for restricting access to confidential information to authorized users. These access control policies allow defining different roles for different users. For example all users from a specific department within an organization can be put under one role and there can be different roles for different departments. Figure 12.5 shows an example of a the role based access control framework in the cloud. A user who wants to access the application data in the cloud is required to send his/her data to the system administrator who assigns permissions and access control policies which are stored in the User Roles and Data Access Policies databases respectively. The role based access control framework provides access to application data to the users based on the assigned roles and data access policies.

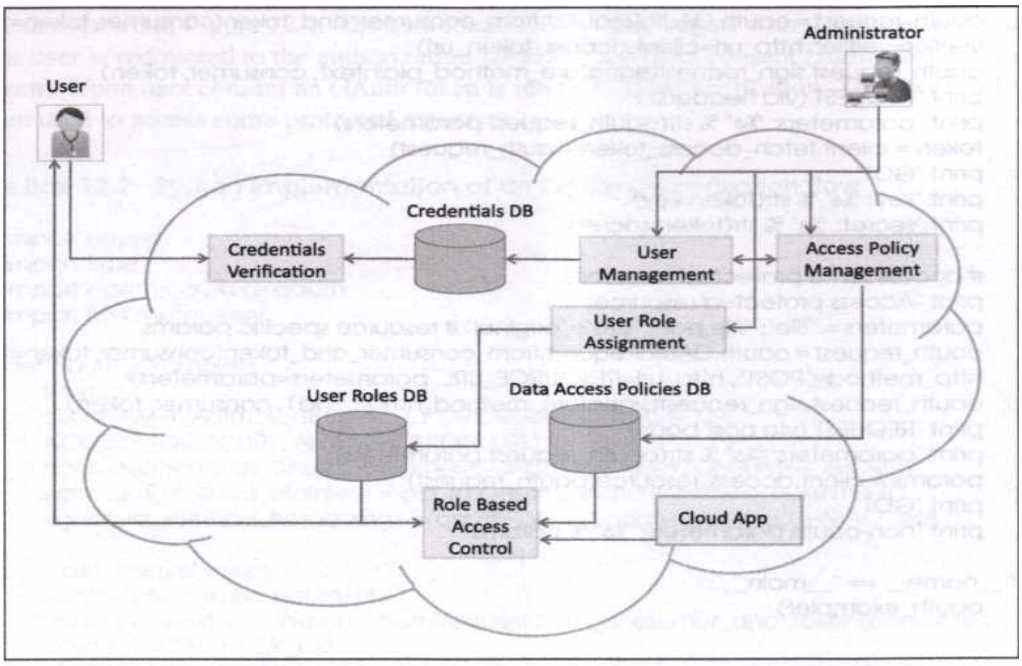


Figure 12.5: Role-based access control in the cloud

CLOUD CONTRACTING MODELS

Licensing Agreements Versus Services Agreements

Summary of Terms of a License Agreement. A traditional software license agreement is used when a licensor is providing a copy of software to a licensee for its use (which is usually non-exclusive). 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 forth 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 (among other things) 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. Additionally, the software license usually offers the licensee protection from the software's violation of the third party's intellectual property rights (i.e., intellectual property infringement). In the case of infringement the license agreement provides a mechanism for the licensor to repair, replace, or remove the software from the licensee's possession.

Summary of Terms of a Service Agreement

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. Since there is no transfer of possession of a copy of software and the service is controlled by the company providing it, a service agreement does not necessarily need to cover infringement risk, nor does it need to set forth the scenarios and manner in which a copy of software is to be returned to the vendor when a relationship is terminated. Since the software service is controlled by the provider, the attendant risks and issues associated with transferring possession of software without transferring ownership do not exist.

Value of Using a Service Agreement in Cloud Arrangements

In each of the three permutations of cloud computing (SaaS, PaaS, and IaaS), the access to the cloud-based technology is provided as a service to the cloud user. The control and access points are provided by the cloud provider. There is no conveyance of software to the cloud user. A service agreement covers all the basic terms and conditions that provide adequate protection to the cloud user without committing the cloud provider to risk and liability attendant with the licensing of the software.

On-Line Agreements Versus Standard Contracts

There are two contracting models under which a cloud provider will grant access to its services. The first, the on-line agreement, is a click wrap agreement with which a cloud user will be presented before initially accessing the service. A click wrap is the agreement the user enters into when he/she checks an "I Agree" box, or something similar at the initiation of the service relationship. The agreement is not subject to negotiation and is generally thought to be a contract of adhesion (i.e., a contract that heavily restricts one party while leaving the other relatively free). There is complete inequality in bargaining power in click wrap agreements because there is no ability to negotiate them. The click wrap is currently the most commonly used contracting model. The second model,the standard, negotiated, signature-based contract will have its place as well— over time. As larger companies move to the cloud (especially the public cloud),or more mission-critical

applications or data move to the cloud, the cloud user will most likely require the option or a more robust and user-friendly agreement. This will be the case notwithstanding the economies associated with resource pooling, multi-tenancy, and virtualization offered by the cloud (that are maximized when the cloud provider uses a one-size-fits-all approach—even at the contracting level), as increasingly complex or sensitive information begins to be process in the cloud; the cloud user will push for a negotiated agreement.

The Importance of Privacy Policies Terms and Conditions

The privacy policy of a cloud provider is an important contractual document for the cloud user to read and understand. Why? In its privacy policy the cloud provider will discuss, in some detail, what it is doing (or not doing, as the case may be) to protect and secure the personal information of a cloud user and its customers. The cloud user may get a sense of how the cloud provider is complying with various privacy laws by reviewing the privacy policy. Even if the cloud provider is in full compliance with laws, a data compromise could still occur. The privacy policy may be where one finds the limits the cloud provider is placing on its liability in such an event. It is not negotiated, but a potential cloud user should be particularly interested in its terms. If the privacy protections appear inadequate or insufficient, the cloud user may wish to consider other cloud providers with more desirable or robust protections. The cloud provider should be explicit in its privacy policy and fully describe what privacy security, safety mechanisms, and safety features it is implement- ing. As further incentive for the cloud provider to employ a “do what we say we do” approach to the privacy policy, the privacy policy is usually where the FTC begins its review of a company’s privacy practices as part of its enforcement actions. If the FTC discovers anomalies between a provider’s practices and its policies, then sanctions and consent decrees may follow.

Risk Allocation and Limitations of Liability

Simply stated, the limitation of liability in an agreement sets forth the maximum amount the parties will agree to pay one another should there be a reason to bring some sort of legal claim under the agreement. As a practical matter, contractual risk (e.g., provision of warranties, assuming liability for third parties under the provider’s control, covenants to implement certain industry standards, service level agreements, etc.) is not distributed evenly between the parties. This is due inpart because the performance obligations primarily fall on the provider. This sets up the traditional thinking that the contractual risk should follow the party with the most significant performance obligations. In reality, the cloud provider may have the bulk of the performance obligations, but may seek to take a “we bear no responsibility if something goes wrong” posture in its contracts, especially if those contracts are click wrap agreements. In fact, some cloud providers disclaim all liability in their agreements, even disclaiming liability if they are at fault or negligent in their performance. Over time, cloud services will be provided under both types of contracts. For mission-critical deployments the cloud provider will likely take on much more significant financial liability and contractual risk as part of the deal. This risk and liability will be reflected in the negotiated contract. The cloud user will pay a fee premium for shifting the liability and contractual risk to the cloud provider. The cloud provider’s challenge, as it sees the risk and liability profile shift requiring it to assume heightened provider obligations, will be to appropriately mitigate contract risk using technological or other types of solutions where possible. Examples of mitigation could include implementation of robust and demonstrable informa- tion security programs, implementing standards or best practices, developing next generation security protocols, and enhancing employee training.

Business Continuity and Disaster Recovery

In the SaaS environment, customers rely heavily on 24/7 access to their services, and any interruption in access can be catastrophic. The availability of your software applications is the definition of your company's service and the life blood of your organization.

Given the virtualization of the SaaS environment, the same technology will increasingly be used to support business continuity and disaster recovery, because virtualization software effectively "decouples" application stacks from the underlying hardware, and a virtual server can be copied, backed up, and moved just like a file.

A growing number of virtualization software vendors have incorporated the ability to support live migrations. This, plus the decoupling capability, provides a low-cost means of quickly reallocating computing resources without any downtime.

Another benefit of virtualization in business continuity and disaster recovery is its ability to deliver on service-level agreements and provide high-quality service.

Code escrow is another possibility, but object code is equivalent to source code when it comes to a SaaS provider, and the transfer and storage of that data must be tightly controlled.

For the same reason that developer will not automatically provide source code outside their control when they license their software, it will be a challenge for SaaS escrow account providers to obtain a copy of the object code from a SaaS provider.

Of course, the data center and its associated physical infrastructure will fall under standard business continuity and disaster recovery practices.

The Business Continuity Plan

A business continuity plan should include planning for non-IT-related aspects such as key personnel, facilities, crisis communication, and reputation protection, and it should refer to the disaster recovery plan for IT- related infrastructure recovery/continuity.

The BC plan manual typically has five main phases: analysis, solution design, implementation, testing, and organization acceptance and maintenance.

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure.

Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

Security challenges present in cloud computing.

Security Issues Within The Cloud

Cloud vendors provide a layer of security to user's data. However, it is still not enough since the confidentiality of data can often be at risk. There are various types of attacks, which range from password guessing attacks and man-in-the-middle attacks to insider attacks, shoulder surfing attacks, and phishing attacks. Here is a list of the security challenges which are present within the cloud:

Data Protection and Misuse: When different organizations use the cloud to store their data, there is often a risk of data misuse. To avoid this risk, there is an imminent need to secure the data repositories. To achieve this task, one can use authentication and restrict access control for the cloud's data.

Locality: Within the cloud world, data is often distributed over a series of regions; it is quite challenging to find the exact location of the data storage. However, as data is moved from one country to another, the rules governing the data storage also change; this brings compliance issues and data privacy laws into the picture, which pertain to the storage of data within the cloud. As a cloud service provider, the service provider has to inform the users of their data storage laws, and the exact location of the data storage server.

Integrity: The system needs to be rigged in such a manner so to provide security and access restrictions. In other words, data access should lie with authorized personnel only. In a cloud environment, data integrity should be maintained at all times to avoid any inherent data loss. Apart from restricting access, the permissions to make changes to the data should be limited to specific people, so that there is no widespread access problem at a later stage.

Access: Data security policies concerning the access and control of data are essential in the long run. Authorized data owners are required to give part access to individuals so that everyone gets only the required access for parts of the data stored within the data mart. By controlling and restricting access, there is a lot of control and data security which can be levied to ensure maximums security for the stored data.

Confidentiality: There is a lot of sensitive data which might be stored in the cloud. This data has to have extra layers of security on it to reduce the chances of breaches and phishing attacks; this can be done by the service provider, as well as the organization. However, as a precaution, data confidentiality should be of utmost priority for sensitive material.

Breaches: Breaches within the cloud are not unheard. Hackers can breach security parameters within the cloud, and steal the data which might otherwise be considered confidential for organizations. On the contrary, a breach can be an internal attack, so organizations need to lay particular emphasis in tracking employee actions to avoid any unwanted attacks on stored data.

Storage: For organizations, the data is being stored and made available virtually. However, for service providers, it is necessary to store the data in physical infrastructures, which makes the data vulnerable and conducive to physical attacks.

Data security,data privacy and application security

Data Security

Data Security is a process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption.

Data security is an essential aspect of IT for organizations of every size and type.Data security is also known as information security (IS) or computer security.

Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers.

One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Data privacy

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations.

Data privacy relates to how a piece of information—or data—should be handled based on its relative importance.

When data that should be kept private gets in the wrong hands, bad things can happen. A data breach at a government agency can, for example, put top secret information in the hands of an enemy state. A breach at a corporation can put proprietary data in the hands of a competitor.

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.

Application security

Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

Application security is the process of making apps more secure by finding, fixing, and enhancing the security of apps. Much of this happens during the development phase, but it includes tools and methods to protect apps once they are deployed. This is becoming more important as hackers increasingly target applications with their attacks.

Application security is getting a lot of attention. Hundreds of tools are available to secure various elements of your applications portfolio, from locking down coding changes to assessing inadvertent coding threats, evaluating encryption options and auditing permissions and access rights. There are specialized tools for mobile apps, for network-based apps, and for firewalls designed especially for web applications.

Write a short notes on i)Infrastructure Security ii)Host Level Security iii)Identity Access management iv)Virtual machine security v)Application level security vi)Data privacy

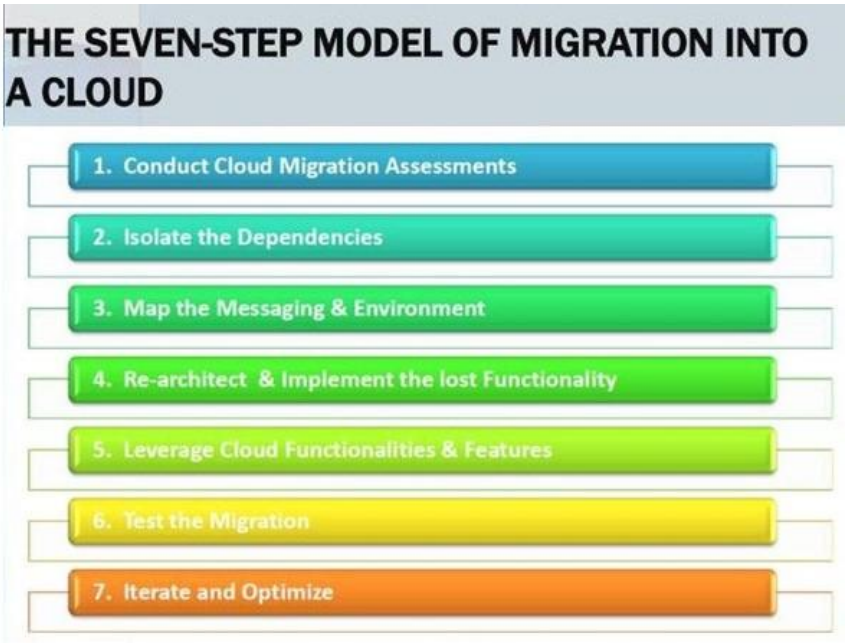
Infrastructure Security

Infrastructure security is the security provided to protect infrastructure, especially critical infrastructure, such as airports, highways, rail transport, hospitals, bridges, transport hubs, network communications, media, the electricity grid, dams, power plants, seaports, oil refineries, and water systems.

Infrastructure security seeks to limit vulnerability of these structures and systems to sabotage, terrorism, and contamination.

Critical infrastructures naturally utilize information technology as this capability has become more and more available. As a result, they have become highly interconnected, and interdependent. Intrusions and disruptions in one infrastructure might provoke unexpected failures to others. How to handle interdependencies becomes an important problem.

Seven steps of cloud migration



It is best to first iterate through the Seven-Step model process for optimizing and migration is both comprehensive and robust. The seven stages of migration are outlined below.

- **Assess**

  Assessment is the first step of a seven-step model of cloud migration and also it is the most important of all the other steps. It includes assessment of issues and reasons related to migration and understanding the need to shift your technology and software on the cloud platform. This migration can be of application, design, code and architecture level.This is the most important and as migration starts with an assessment of the issues and strategies related to the migration. The assessment can be of tools being used, test cases as well as functionalities and configurations. The assessment can also be about the cost of migration and ROI (Return on Investment) that can be achieved in the case of the production version.

- **Isolate**

  In the second step of migration into the cloud environment, there is the isolation of all environmental and systematic dependencies of an enterprise application within the captive data center. The dependencies include the library, application and architectural.This step helps in better understanding of the complexity of the cloud migration. This step helps in isolation of run-time environment, applications dependencies, libraries dependencies and much more. Isolation of all the components is necessary to make the system more reliable and atomic.

- **Mapping**

  After complete isolation, the third step is to generate the mapping constructs between what data shall remain in the local captive data centers and what shall be shifted to the cloud. It is very important to first understand what exactly you need to shift on the cloud platform as there is no sense of shifting all the data and applications on the cloud environment.

- **Re-architect**

  This is the fourth step in cloud migration which includes understanding which part of the application is generally needed to be sifted and what not.Moreover, a substantial part of enterprise application is generally needed to be shifted as it is to be rearchitected, reimplemented and redesigned on the cloud. There are also chances that in this step of cloud migration process, some of the useful functionalities can be lost initially but later all of them can be regained.

- **Augment**

  Augmentation of cloud computing application is done in this application. In this, we leverage the intrinsic features of services of a cloud to augment our enterprise application in its own ways.

- **Test**

  After augmentation is complete, the applications needed to be tested and validated. This is done using a test suite for the applications on the cloud. The test results can be both positive and negative. In this step of cloud migration, new test cases due to augmentation and proofs-of-concept are also tested.

- **Optimize and Iterate**

  In this last step of cloud migration, we iterate and optimize as appropriate. After several other optimizing iterations, the migration process is successful. It is best to first iterate the seven-step model process for optimizing and ensuring that cloud migration is both robust and comprehensive.

Q.Explain broad approaches in migration.[W-17](7M)

Ans:

Once the IT department has fully addressed these risk factors, they can move on to plan the best cloud migration approach to meet the company's business objectives and requirements. While there are a number of approaches used in the industry, below are the most broad:

Lift and shift: This approach involves mapping the on-premises hardware and/or VMs to similar resource-sized cloud instances. For example, if a company's front-end application

server has 4 CPUs, 64GB of RAM, and 512GB of local storage, they would use a cloud instance that matches that configuration as closely as possible. The challenges with this approach is that on-premise solutions are typically over-provisioned with respect to resources in order to meet peak loads as they lack the elastic, auto-scaling features of cloud. This results in increased cloud costs, which may be fine if this is a short-term approach

Refactor and rearchitect: In order to best maximize the features of cloud, such as auto-scaling, migration can be the forcing function to take some time and re-architect the application to be more performant and also keep the costs under control. It is also a good time to re-evaluate technology choices, as a company may be able to switch some solutions from more expensive commercial ones, to open-source or cloud-native offerings.

Shelve and spend: This third approach involves retiring a monolithic on-premises application and moving to a SaaS solution. An example of this would be an HCM (Human Capital Management) application, which is often times a disparate set of code bases tied together with a relational database, migrating to an offering such as Workday HCM. This allows the modernisation of business logic and offloads the operational burden of the service and infrastructure to the SaaS provider.

Network security,Host level security and application level security in detail.

Network security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.