CHAPTER 6

SECURITY IN CLOUD COMPUTING

CHAPTER OUTLINE

After studying this chapter, students will be able to understand the:

- Introduction to Cloud Security, Cloud Information Security Objectives
- Cloud Privacy, Security, And Trust, Cloud Security Services , Cloud Security Challenges and Risks
- Widely Seen Security Issues, Cloud Computing Risk Issues
- Software-As-A-Service Security, Important Actions For A Security Team, Secure Software Development Life Cycle (SecSDLC)
- Security Monitoring And Incident Response, Cloud Computing Security Architecture, Security Architecture Design, High Availability And Fault Tolerance, Scalability and Fault Tolerance
- Disaster Recovery, Cloud Disaster Recovery (Cloud DR), Options To Disaster Recovery In The Cloud, Four Steps To Achieving High Availability In The Cloud, Qos Issues in Cloud,
- Identity management and access Control, Importance Of IAM For Cloud Computing,
- Types of Digital Authentication

INTRODUCTION TO CLOUD SECURITY

Cloud computing security refers to a collection of control-based technologies and policies meant to comply with regulatory compliance regulations while also protecting information, data applications, and infrastructure involved with cloud computing use. Because the cloud is a shared resource, identity management, privacy, and access control are particularly important. With more enterprises turning to cloud computing and associated cloud providers for data operations, adequate security in these and other potentially susceptible areas has become a top responsibility for enterprises working with a cloud computing provider.

Cloud computing security, or simply cloud security, refers to a comprehensive range of rules, technologies, and procedures used to safeguard data, applications, and the related cloud computing infrastructure. It is a subdomain of computer security, network security, and information security in general.

Cloud computing security processes should address the security controls that the cloud provider will implement to ensure the security, privacy, and compliance with the applicable legislation of the customer's data. In the event of a cloud security breach, the processes will almost certainly involve a business continuity and data backup strategy.

CLOUD INFORMATION SECURITY OBJECTIVES

One of the most critical considerations when establishing cloud projects is security. It necessitates those businesses to recognize and comprehend the risks associated with digitalization, public networks, and the outsourcing of infrastructure components. Companies continue to be concerned about the security of their data while using cloud-based technologies. IT professionals want to protect their cloud installations with the same level of security as they do their internal resources. Many corporate executives believe that cloud security is only the provider's responsibility, yet genuine cloud security necessitates a joint effort.

Confidentiality

Confidentiality is the safeguarding of personal information, which entails keeping a client's information between the provider and the client and not disclosing it to outsiders, such as coworkers, friends, relatives, and so on. Confidentiality implies the prevention of unauthorized disclosure of information, whether deliberate or inadvertent. In cloud systems, confidentiality is connected to intellectual property rights, hidden channels, traffic analysis, encryption, and inference.

1. **Intellectual property rights**: Inventions, designs, and creative, musical, and literary works are all examples of intellectual property (IP). Copyright laws, which protect mental works, and patents, which are given for innovative innovations, safeguard intellectual property rights.
2. **Covert channels**: A covert channel is an unlawful and unexpected communication link that allows information to be exchanged. Covert channels can be established by timing messages or making an incorrect use of storage systems.
3. **Traffic analysis**: A type of confidentiality breach that may be done by evaluating the amount, rate, source, and destination of message traffic, even if it is encrypted, is traffic analysis. Increased message activity and strong bursts of traffic might signal the presence of a large event. Countermeasures against traffic analysis include maintaining a near-constant flow of message traffic and concealing the traffic's origin and destination locations.
4. **Encryption**: Encryption involves scrambling communications so that an unauthorized entity cannot read them, even if they are intercepted. The amount of effort (work factor) required to decrypt the message is determined by the encryption key's strength as well as the resilience and quality of the encryption method.

Inference: Typically, the inference is related to database security. The inference is an entity's capacity to utilize and correlate information protected at one degree of security to discover information protected at a higher degree of protection.

Examples of maintaining confidentiality include:

- Individual files are locked and secured.
- support workers do not tell other people what is in a client's file unless the client gives permission.
- information about clients is not disclosed to people who do not need to know.
- and clients have the right to keep any information about themselves confidential, including that information being disclosed.

Integrity

The guarantee that digital information is uncorrupted and may only be accessed or updated by those authorized to do so is known as data integrity. Maintaining the consistency, correctness, and trustworthiness of data through its entire lifespan is what integrity entails. It must not be modified in transit to maintain integrity, and efforts must be taken to guarantee that data cannot be manipulated by an unauthorized person or program. Implementing user access restrictions to prevent erroneous modifications or inadvertent deletion by authorized users is one example of such a safeguard. Documenting system administration methods, parameters, and maintenance operations, as well as preparing disaster recovery plans for eventualities like power outages, server failure, or security assaults, are examples of network administration practices to maintain data integrity. Backups or redundancies must be accessible if data becomes damaged to restore the impacted data to its original condition.

One of the most fundamental cornerstones of information assurance is integrity (IA). Because users must be able to trust information, integrity is a critical component of IA. Untrusted data lacks integrity. Data must be kept intact within an information system (IS) and throughout data transit. Hackers, for example, may inflict harm by entering systems with malware, such as Trojan horses, which takeover computer systems, as well as worms and viruses. An employee may harm the organization by purposefully entering inaccurate data.

Measures must also be made to preserve integrity by managing the physical environment of networked terminals and servers because environmental dangers such as heat, dust, or electrical difficulties might jeopardize data consistency, correctness, and trustworthiness. There must be a method in place to identify any changes in data that may occur as a consequence of non-human-caused events such as an electromagnetic pulse or a server crash. Keeping transmission media (such as cables and connectors) covered and secured to ensure that they cannot be tapped is one practice used to safeguard data integrity in the physical environment, as does shielding hardware and storage media from power surges, electrostatic discharges, and so on.

The following three principles must be followed for the idea of cloud information integrity to be realized:

- Modifications are not made to data by unauthorized personnel or processes.
- Unauthorized modifications are not made to data by authorized personnel or processes.
- The data is internally and externally consistent – in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.

Availability

Another critical component of information assurance is availability (IA). When a system fails frequently, information availability suffers, which harms users. Furthermore, information security suffers when data is not secure and easily accessible. Time is another aspect that influences availability. If a computer system cannot efficiently send information, its availability is jeopardized. Data availability must be assured

through storage, which can be on-site or off-site. In the case of an offsite location, a business continuity strategy should specify the availability of this data if onsite data is unavailable. Those with clearance must have access to information at all times.

Availability guarantees that the right employees have consistent and timely access to cloud data or cloud computing resources. Availability ensures that the systems are operational when needed. Furthermore, this idea ensures that the cloud system's security services remain operational. A denial-of-service attack is an example of an availability threat.

Finally, high availability is the cloud's holy grail. It symbolizes the concept of having access to services, tools, and data from anywhere and at any time, and it is the facilitator of ideas of a future with no physical offices or global corporations with entirely connected and unified IT systems. Availability is also connected to reliability: a service that is available 24 hours a day, seven days a week but frequently goes out is meaningless. To be considered high-availability, a service must not only be always-on but also have many "nines" (99.999[...]) of reliability.

CLOUD PRIVACY, SECURITY, AND TRUST

Cloud computing refers to the underlying infrastructure enabling a new form of service delivery that has the benefit of lowering costs by sharing computer and storage resources, in conjunction with an on-demand provisioning mechanism based on a pay-per-use business model. These new characteristics have an immediate impact on IT spending, but they also influence conventional security, trust, and privacy processes. The benefits of cloud computing, such as its capacity to grow quickly, store data remotely, and share services in a dynamic environment, can become drawbacks in maintaining a degree of assurance necessary to preserve potential consumers' confidence. Some basic old mechanisms for managing privacy are no longer flexible or dynamic enough, necessitating the development of new ways to meet this new paradigm.

Privacy

For clients, privacy means the preservation and responsible use of their personal information, as well as matching their expectations regarding its usage. For enterprises, privacy comprises the implementation of laws, rules, standards, and practices for managing personal information. What is appropriate will be determined by the applicable laws, individuals' expectations regarding the collection, use, and disclosure of their personal information, and other contextual information; thus, one way to think about privacy is simply as "the appropriate use of personal information under the circumstances." Personal information refers to facts, messages, or ideas about a person that would be fair to expect him or her to perceive as intimate or sensitive, and hence concerning which he or she would desire to limit collection, use, or dissemination. The phrases 'personal information' and 'personal data' are sometimes used interchangeably.

Name, address, phone number, social security or national identity number, credit card number, email address, passwords, date of birth, religion or race, political beliefs, health, sexual orientation, trade-union membership, driver's license numbers, personal financial information, and medical records are all examples of important personal data.

Security

Security is defined as the preservation of information confidentiality, integrity, and availability; other attributes such as authenticity, accountability, non-repudiation, and dependability may also be included. Confidentiality is a security feature that ensures information is not made available or given to unauthorized people, companies, or processes. The total correctness, completeness, and consistency of data, entities, or processes throughout its lifecycle is referred to as integrity. The process of ensuring that data is available to end-users and applications when they need it is known as availability.

Security is a required but insufficient prerequisite for privacy. Security is, in fact, one of the fundamental foundations of privacy. Any entity that creates, maintains, uses, or disseminates data must guarantee that those records have not been tampered with and must take safeguards to prevent the information from being misused. To be more specific, to maintain the security of such information processing, data controllers must establish suitable technological and organizational safeguards to protect it against unauthorized access or disclosure, destruction, modification, and unauthorized use. Mechanisms for doing this include risk assessment, implementation of an information security program, and the implementation of effective, reasonable, and appropriate measures covering physical, administrative, and technological components of security.

Trust

Trust is a complicated term with no commonly recognized definition. Trust is a psychological condition that consists of the decision to accept vulnerability based on favorable expectations of another's intentions or behavior. As a trust is consisting of subjective criteria and experience, it is a larger concept than security. Similarly, there exists both hard (security-oriented) and soft (i.e., confidence that is not based on security) trust. 'Hard' trust entails elements including authenticity, encryption, and transaction security, whereas 'soft' trust entails human psychology, brand loyalty, and user-friendliness. People generally find it more difficult to trust internet services than offline services since there are no tangible indicators in the digital realm and there may not be established centralized authority. The distrust of Internet services can even have a damaging impact on the amount of confidence provided to firms that have long been regarded as trustworthy.

The online trust may be developed in a variety of ways, the most significant of which is security. People are more inclined to engage in e-commerce if they are convinced that their credit card information and personal data are cryptographically secure, which is an example of enhanced security leading to higher confidence. Building trust, a stable trust relationship, and declining trust are all possible stages in a partnership. Trust is difficult to establish and quick to destroy: a single breach of trust may demolish years of patiently acquired reputation.

When evaluating trust in the context of cloud computing, it may be useful to distinguish between social and technological ways of establishing persistent and dynamic trust. Trust in long-term underlying infrastructure originates through relatively unchanging social and technical factors. Dynamic trust refers to a trust that is specific to certain conditions, settings, or short-term or variable knowledge; it can occur as a result of context-based social and technical systems. Persistent social-based trust in a hardware or software component or system is an indication of confidence in technological-based trust since it assures the implementation and functioning of that component or system.

Cloud Security Services

Authentication, authorization, auditing, and accountability are further aspects that have a direct impact on cloud software assurance.

Authentication

Cloud computing is altering our way of interacting with devices, software, data, and processes. However, certain things never change, and one thing that stays constant throughout old and new computer paradigms is the significance of authentication to establish the identity of the person and/or system with which we are talking.

Authentication is the process of identifying whether or not someone or something is who or what it claims to be. Authentication technology controls system access by determining if a user's credentials match those in a database of authorized users or a data authentication server. Users are typically recognized by a user ID, and authentication occurs when the user offers a credential, such as a password, that corresponds to that user ID.

Identity management and authentication are critical components of security, whether in the cloud or on a local network. Managing identities has always been a concern within the corporate network, and it grew even more difficult as organizations created federations to share resources across organizational boundaries. Private, public, and hybrid clouds add another degree of complication.

Security should be seamless and visible to users. The first objective for users is access - the ability to receive the information they need to do their tasks as fast and comfortably as feasible. The difficulty is that security and convenience will always occupy opposite sides of the spectrum; the more of the one you have, the less of the other you have.

Authentication is crucial because it allows companies to keep their networks safe by allowing only authenticated users (or processes) to access protected resources such as computer systems, networks, databases, websites, and other network-based applications or services.

Single Sign-On (SSO) is the treasure of authentication. Federated Identity Management (FIDM) can bridge the gap by allowing users to connect to a public cloud service (such as SalesForce.com) using the same username and password that they use for their corporate credentials. Most IT/cloud professionals and end-users are still suffering from authentication, which means users must remember different passwords and usernames for various cloud services. Then there's the issue with passwords, which may be broken via brute force assaults and social engineering or disclosed via security breaches targeting large cloud sites and providers. Several customers have lately had to update many of their passwords due to concerns that they might have been hacked.

Multi-factor authentication increases security tremendously, but it is being deployed slowly, even inside local business networks, let alone in the cloud. Once the bugs are sorted out, biometric authentication has the potential to be the most secure type of single sign-on, and it eliminates some of the concerns inherent in other kinds of two-factor authentication. Users do not "forget," "lose," or "leave" their fingerprints at home.

Authentication Factors

Authenticating a user using a user ID and a password is the most basic sort of authentication, and it requires the user to know two pieces of information: the user ID or username and the password. This is a sort of single-factor authentication since it depends on only one authentication element.

Authentication elements that are currently in use include:

1. **Knowledge factor: "Something you know."** - Any authentication credentials that the user possesses, such as a personal identification number (PIN), a username, a password, or the solution to a secret question, can be used as the knowledge factor.
2. **Possession factor: "Something you have."** - Any credential based on the items that the user may own and carry about them, such as a security token or a mobile phone used to receive a text message or run an authentication software that may produce a one-time password or PIN, can be considered a possession factor.
3. **Inherence factor: "Something you are."** - The inherence factor is often dependent on biometric identification, such as finger or thumb prints, face recognition, retina scans, or any other type of biometric data.
4. **Location factor: "Where you are."** - While it may be less specific, the location factor is occasionally utilized in conjunction with the other elements. Devices equipped with GPS can detect locations with acceptable precision, or network paths may be checked with less precision. The location factor cannot generally stand alone as an authentication factor, but it can augment the other criteria by giving a way to rule out particular requests. It can, for example, prevent an attacker in a remote geographical location from impersonating a user who regularly logs in exclusively from their home or workplace in the organization's home nation.
5. **Time factor: "When you are authenticating."** - The time factor, like the location factor, is insufficient on its own, but it may be used as a supplement to clear attackers who attempt to access a resource at a time when that resource is not available to the authorized user. It can also be used in conjunction with the place. For example, if the user were last verified at noon in the United States, an attempt to log in from Asia one hour later would be refused due to the time and location combination.

Authorization

Cloud computing is a new service delivery paradigm that uses the Internet to offer services. Data security is one of the most important concerns in a cloud computing environment. Authentication is a critical method for information security that creates identity evidence to gain access to information in the system. To avoid unauthorized access to cloud resources, authorization is a critical identity service. The most essential security problems and difficult difficulties in cloud-based settings are access control and user authentication. Authentication and authorization mechanisms must be successfully implemented in this environment to prevent unauthorized access to dispersed system components.

Authorization is a security method used to define access levels or user/client rights for system resources such as files, services, computer programs, data, and application features. This is the process of allowing or refusing access to a network resource depending on the user's identification, which provides the user access to numerous resources.

The majority of online security technologies work in two steps. The first stage is authentication, which verifies the user's identification, and the second stage is authorization, which grants the user access to various resources depending on the user's identification. To enable application deployment and maintenance, modern operating systems rely on well-designed authorization mechanisms. Key considerations include user type, quantity, and credentials, as well as activities and responsibilities that require verification.

The practice of granting someone permission to do or have something is known as authorization. In multi-user computer systems, a system administrator specifies which users have access to the system and what rights they have (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). After a user logs in to a computer operating system or application, the system or application may wish to determine what resources the user may access during this session. As a result, authorization is sometimes seen as both the preparatory setting up of permissions by a system administrator and the actual validation of the permission values that have been put up when a user is granted access.

Auditing

Organizations utilize two key ways to maintain operational assurance: system audits and monitoring. Depending on asset design and deployment, these strategies can be used by the cloud client, the cloud provider, or both.

- A system audit is a one-time or periodic event to evaluate security.
- Monitoring refers to an ongoing activity that examines either the system or the users, such as intrusion detection.

Internal and external information technology (IT) auditors are frequently distinguished. Internal auditors are often employed by a single business, but external auditors are not. External auditors are often certified public accountants (CPAs), or other audit experts contracted to conduct an independent audit of an organization's financial statements. Internal auditors often have a considerably broader mission than external auditors, such as ensuring compliance and due care standards, assessing operational cost efficiency, and suggesting suitable controls.

IT auditors typically audit the following functions:

- System and transaction controls
- Systems development standards
- Backup controls
- Data library procedures
- Data center security
- Contingency plans

Furthermore, IT auditors may offer enhancements to controls, and they frequently engage in the development phase of a system to assist an organization in avoiding costly reengineering after the system's adoption.

An audit trail or log is a collection of records that offer documented proof of processing and are used to help in tracing from initial transactions to related records and reports, and/or backward from records and reports to their component source transactions. Audit trails might be restricted to certain events or might cover all of the activity on a system. Audit logs should record the following:

- The transaction's date and time
- Who processed the transaction?
- At which terminal the transaction was processed
- Various security events relating to the transaction

In addition, an auditor should examine the audit logs for the following:

- Amendments to production jobs
- Production job reruns
- Computer operator practices
- All commands directly initiated by the user
- All identification and authentication attempts
- Files and resources accessed

Accountability

Accountability is the capacity to determine and identify the acts and behaviors of a single individual within a cloud system. Audit trails and records help to ensure accountability and may be used to undertake postmortem examinations on past events and the people or processes involved. Accountability is linked to the notion of nonrepudiation, which states that an individual cannot effectively deny doing an activity.

CLOUD SECURITY CHALLENGES AND RISKS

Although virtualization and cloud computing can help businesses achieve more by breaking down the physical barriers that exist between an IT infrastructure and its customers, increased security dangers must be faced to fully benefit from this new computing paradigm. This is especially true for SaaS providers. Some security issues merit further consideration. For example, in the cloud, you lose some control over assets, thus your security approach must be reevaluated.

Enterprise security is only as good as its most untrustworthy partner, department, or vendor. Can you put your data in the hands of your service provider? Physical security is lost while using the cloud approach. You share computer resources with other businesses in a public cloud. You have no information or control over where the resources run in a common pool outside the organization. Exposing your data in a shared environment with other businesses may provide the authorities with "reasonable cause" to confiscate your assets because another firm broke the law. Simply because you share the cloud environment puts your data in danger of confiscation.

As more mission-critical activities are shifted to the cloud, SaaS providers will be required to offer log data in a real-time, simple manner, most likely for their administrators as well as their customers' people. Someone must be in charge of monitoring for security and compliance, and they will be unable to do so until the application and data are in the control of end-users. Will consumers have enough faith in the cloud provider to move mission-critical apps to the cloud? Monitoring is difficult since the SaaS provider's logs are internal and not always accessible externally or by clients or investigators.

Cloud apps are constantly updated with new features, and users must stay up to current on program updates to ensure their security. The rate at which apps evolve on the cloud will have an impact on both the SDLC and security. For example, Microsoft's SDLC believes that mission-critical software would not change significantly for three to five years, but the cloud may necessitate a change in the program every few weeks. Worse, a secure SLDC will not be able to provide a security cycle that keeps up with the rapid changes. This implies that users must regularly upgrade since an older version may not perform properly or adequately safeguard data.

If a non-mission-critical application goes down, the cloud service provider can survive; however, this may not be the case for mission-critical apps. Competitive distinctiveness is provided by core business processes. Security must be moved to the data level so that businesses can be certain that their data is secure wherever it travels. The organization, not the cloud computing provider, is in charge of sensitive data. Data-level security is one of the most difficult concerns in cloud computing.

Government policy will need to evolve in response to both the opportunities and challenges posed by cloud computing. This will most likely concentrate on the off-shoring of personal data and the protection of privacy, regardless of whether the data is owned by a third party or off-shored to another nation. As traditional controls such as virtual local-area networks and firewalls become less effective throughout the shift to a virtualized environment, security will suffer as a result. During the shift to server virtualization in commercial environments, security administrators will need to pay special attention to systems that hold vital data, such as company financial information or source code.

While surrendering significant control over data is not a smart idea from a security standpoint, the business's simplicity and financial savings will continue to encourage the use of these services. Security managers will need to collaborate with their company's legal team to ensure that suitable contract conditions are in place to secure corporate data while also providing acceptable service-level agreements. Because of cloud-based services, many mobile IT users will be able to access company data and services without having to connect to the corporate network. This will heighten the requirement for businesses to implement security controls between mobile users and cloud-based services. Placing enormous volumes of sensitive data in a globally accessible cloud exposes firms to enormous and dispersed threats—attackers no longer need to come on-site to steal data, and they can find it all in a single "virtual" place.

To achieve cloud virtualization efficiency, virtual computers from several enterprises must be co-located on the same physical resources. Physical segregation and hardware-based security cannot guard against assaults between virtual machines on the same server, even though traditional data center security still applies in the cloud environment. Administrative access is provided through the Internet rather than the traditional data center model's restricted direct or on-premises link. This raises the risk and exposure and necessitates close monitoring for changes in system control and access control restrictions.

The dynamic and fluid nature of virtual machines will make it difficult to maintain security consistency and assure record auditability. The ease with which physical servers may be cloned and distributed may result in the spread of configuration problems and other vulnerabilities. It will be difficult to demonstrate a system's security condition and locate an unsecured virtual machine. Regardless of where the virtual machine is located inside the virtual environment, intrusion detection and prevention systems must be able to identify malicious behavior at the virtual machine level. The co-location of numerous virtual machines expands the attack surface and raises the danger of virtual machine-to-virtual-machine compromise.

In a cloud server environment, localized virtual machines and physical servers share the same operating systems as well as corporate and online applications, raising the risk of an attacker or malware remotely exploiting weaknesses in these systems and applications. Virtual machines are susceptible when they transition between the private and public clouds. A completely or partially shared cloud environment is predicted to have a larger attack surface and hence to be more vulnerable than a dedicated resources environment.

Many organizations are likely rushing into cloud computing without giving any attention to the security implications to reap the benefits of cloud computing, not the least of which is significant cost reductions. To create trust zones in the cloud, virtual machines must be self-defending, thereby shifting the boundary to the virtual machine itself. Enterprise perimeter security (firewalls, demilitarized zones, network segmentation, intrusion detection and prevention systems, monitoring tools, and related security policies) solely controls data that resides and travels behind the perimeter. The cloud computing provider is responsible for client data security and privacy in the cloud computing industry.

cloud security issues

WIDELY SEEN SECURITY ISSUES

1. **Data breaches:** A data breach might be the primary goal of a targeted attack, or it might be the consequence of a human mistake, application flaws, or inadequate security policies. It might include any material that was not meant for public distribution, such as personal health information, financial information, personally-identifying information, trade secrets, and intellectual property. The cloud-based data of a business may be valuable to many parties for a variety of reasons. The danger of data breaches is not unique to cloud computing, but it remains a top issue for cloud consumers.
2. **Insufficient identity, credential, and access management:** Bad actors impersonating genuine users, operators, or developers can access, edit, and delete data; issue control plane and management functions; eavesdrop on data in transit, or distribute harmful software that looks to come from a genuine source. As a result, inadequate identity, credentials, or key management can allow for illegal data access and possibly catastrophic damage to companies or end-users.
3. **Insecure interfaces and application programming interfaces (APIs):** Customers employ a collection of software user interfaces (UIs), or APIs exposed by cloud providers to control and interact with cloud services. These interfaces are used for provisioning, management, and monitoring, and the security and availability of generic cloud services are all dependent on the security of APIs. They must be built to guard against both inadvertent and deliberate attempts to evade rules.
4. **System vulnerabilities:** System vulnerabilities are exploitable faults in programs that allow attackers to penetrate a system to steal data, take control of the system, or disrupt service operations. Vulnerabilities in the operating system's components jeopardize the security of all services and data. With the introduction of cloud multi-tenancy, systems from diverse companies are put nearby to one other and given access to shared memory and resources, resulting in the creation of a new attack surface.
5. **Account hijacking:** Account or service hijacking is not a new issue, but cloud services bring a new wrinkle to the mix. If an attacker gains access to a user's credentials, they can listen in on activities and transactions, modify data, return false information, and divert clients to malicious websites. Account or service instances might serve as a new base of operations for attackers. With stolen credentials, attackers may frequently get access to vital parts of cloud computing services, jeopardizing the confidentiality, integrity, and availability of such services.
6. **Malicious insiders:** A malicious insider, such as a system administrator, can get access to potentially sensitive information and subsequently get access to more essential systems and data. Systems that rely primarily on cloud service providers for security are more vulnerable.
7. **Advanced Persistent Threats (APTs):** APTs are a parasitical type of cyber-attack that infiltrates networks to get a foothold in target firms' IT infrastructure, from which they steal data. APTs operate invisibly over long periods, frequently adapting to the security mechanisms designed to counter them. Once installed, APTs can move laterally via data center networks and blend in with normal network traffic to accomplish their goals.
8. **Data loss:** Data saved in the cloud might be lost for causes other than hostile attacks. An inadvertent deletion by the cloud service provider, or a physical disaster such as a fire or earthquake, might result in the permanent loss of client data unless the provider or cloud consumer takes proper backup mechanisms, according to best practices in business continuity and disaster recovery.
9. **Insufficient due diligence:** Cloud technology and service providers must be considered by executives when developing corporate plans. Creating a clear plan and checklist for due diligence when assessing technologies and suppliers is critical for success. Organizations that rush to embrace cloud technology and select providers without conducting enough due diligence expose themselves to a range of hazards.
10. **Abuse and nefarious use of cloud services:** Cloud computing models are vulnerable to harmful attacks due to poorly protected cloud service installations, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud. Bad actors may utilize cloud computing resources to

WIDELY SEEN SECURITY ISSUES

1. **Data breaches:** A data breach might be the primary goal of a targeted attack, or it might be the consequence of a human mistake, application flaws, or inadequate security policies. It might include any material that was not meant for public distribution, such as personal health information, financial information, personally-identifying information, trade secrets, and intellectual property. The cloud-based data of a business may be valuable to many parties for a variety of reasons. The danger of data breaches is not unique to cloud computing, but it remains a top issue for cloud consumers.
2. **Insufficient identity, credential, and access management:** Bad actors impersonating genuine users, operators, or developers can access, edit, and delete data; issue control plane and management functions; eavesdrop on data in transit, or distribute harmful software that looks to come from a genuine source. As a result, inadequate identity, credentials, or key management can allow for illegal data access and possibly catastrophic damage to companies or end-users.
3. **Insecure interfaces and application programming interfaces (APIs):** Customers employ a collection of software user interfaces (UIs), or APIs exposed by cloud providers to control and interact with cloud services. These interfaces are used for provisioning, management, and monitoring, and the security and availability of generic cloud services are all dependent on the security of APIs. They must be built to guard against both inadvertent and deliberate attempts to evade rules.
4. **System vulnerabilities:** System vulnerabilities are exploitable faults in programs that allow attackers to penetrate a system to steal data, take control of the system, or disrupt service operations. Vulnerabilities in the operating system's components jeopardize the security of all services and data. With the introduction of cloud multi-tenancy, systems from diverse companies are put nearby to one other and given access to shared memory and resources, resulting in the creation of a new attack surface.
5. **Account hijacking:** Account or service hijacking is not a new issue, but cloud services bring a new wrinkle to the mix. If an attacker gains access to a user's credentials, they can listen in on activities and transactions, modify data, return false information, and divert clients to malicious websites. Account or service instances might serve as a new base of operations for attackers. With stolen credentials, attackers may frequently get access to vital parts of cloud computing services, jeopardizing the confidentiality, integrity, and availability of such services.
6. **Malicious insiders:** A malicious insider, such as a system administrator, can get access to potentially sensitive information and subsequently get access to more essential systems and data. Systems that rely primarily on cloud service providers for security are more vulnerable.
7. **Advanced Persistent Threats (APTs):** APTs are a parasitical type of cyber-attack that infiltrates networks to get a foothold in target firms' IT infrastructure, from which they steal data. APTs operate invisibly over long periods, frequently adapting to the security mechanisms designed to counter them. Once installed, APTs can move laterally via data center networks and blend in with normal network traffic to accomplish their goals.
8. **Data loss:** Data saved in the cloud might be lost for causes other than hostile attacks. An inadvertent deletion by the cloud service provider, or a physical disaster such as a fire or earthquake, might result in the permanent loss of client data unless the provider or cloud consumer takes proper backup mechanisms, according to best practices in business continuity and disaster recovery.
9. **Insufficient due diligence:** Cloud technology and service providers must be considered by executives when developing corporate plans. Creating a clear plan and checklist for due diligence when assessing technologies and suppliers is critical for success. Organizations that rush to embrace cloud technology and select providers without conducting enough due diligence expose themselves to a range of hazards.
10. **Abuse and nefarious use of cloud services:** Cloud computing models are vulnerable to harmful attacks due to poorly protected cloud service installations, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud. Bad actors may utilize cloud computing resources to

target consumers, companies, or other cloud providers. Launching distributed denial-of-service assaults, email spam, and phishing campaigns are all examples of how cloud-based services are being abused.

11. **Denial of service (DoS):** DoS attacks are intended to prohibit service users from accessing their data or apps. Attackers can induce a system slowdown and prevent all legitimate service users from accessing services by causing the targeted cloud service to use excessive quantities of finite system resources such as CPU power, memory, disk space, or network bandwidth.

12. **Shared technology vulnerabilities:** Cloud service providers provide scalable services by sharing infrastructure, platforms, or applications. Cloud computing splits the "as-a-service" offering without significantly altering off-the-shelf hardware/software—sometimes at the price of the security. The underlying infrastructure components that facilitate cloud services deployment may not have been designed to provide strong isolation features for a multi-tenant architecture or multi-customer applications. This might result in shared technical vulnerabilities that can be exploited across all delivery modes.

VARIOUS SECURITY CONCERNS IN A CLOUD COMPUTING ENVIRONMENT

- **Security concern #1**: Control over physical security is lost with the cloud model due to the sharing of computer resources with other businesses. There is no information or control over where the resources run.
- **Security concern #2**: Companies breaking the law (risk of data seizure by a (foreign) government).
- **Security concern #3**: If a user decides to switch from one Cloud Service Provider (CSP) to another, the storage services supplied by one may be incompatible (e.g., Microsoft cloud is incompatible with Google cloud).
- **Security concern #4**: Who has access to the encryption/decryption keys?
- **Security concern #5**: Ensuring data integrity (transmission, storage, and retrieval) requires that the data changes only in response to approved transactions. There is currently no uniform standard for ensuring data integrity.
- **Security concern #6**: Data logs must be given to security managers and authorities in the event of the Payment Card Industry Data Security Standard.
- **Security concern #7**: Users must stay up to date on application improvements to ensure their safety.
- **Security concern #8**: Some government restrictions place severe constraints on what data on its inhabitants can be held and for how long, while some bank authorities require customers' financial data to be kept in their native nation.
- **Security concern #9**: The dynamic and fluid nature of virtual machines will make it difficult to maintain security, consistency, and assure records can be audited.
- **Security concern #10**: Customers may be able to sue cloud service providers if their privacy rights are breached, and cloud service providers may incur reputational harm in any scenario. Concerns emerge when consumers are unsure why their personal information is being obtained or how it will be used or passed on to other parties.

CLOUD COMPUTING RISK ISSUES

1. **The effect on a company's return on investment (ROI):** While migration to the cloud may appear to be the most cost-effective choice, businesses should carefully evaluate the expenses of owning software and equipment against the price of "rent" IT technology. Speed, security, utilization, quality of service, scalability, and support must all be addressed.

2. **Compatibility:** Migration to the cloud may cause compatibility issues with an existing IT infrastructure, as well as with a company's security needs and organizational regulations. Pre-planning is essential once again in examining all of these factors before committing to the change.
3. **Trust:** Not all service providers are created equal. Unforeseen incidents may cause disruptions to cloud computing services. Service provider outages, for example, can occur. Because providers cannot guarantee that no service outages will occur, data may not be available 24 hours a day, seven days a week. During a disaster, communications may be slowed or shut down for an extended length of time. Once again, a thorough evaluation of the cloud service provider is essential. Businesses must examine the dangers of entrusting all of their operations to a third party, as well as what would happen in the event of a default and service disruption. What assurances the cloud service provider provides in the event of a disaster is something a corporation should think about.
4. **Confidentiality:** Confidentiality is frequently cited as a justification for not adopting cloud computing as the primary worry. When a company's activities need the management of sensitive data, data protection becomes a priority and a problem. A company may be hesitant to share sensitive information with a third party. When data is handled and exchanged between two parties, assigning responsibility for a data breach may be difficult.
5. **Compliance:** There are dangers associated with noncompliance with current rules and predetermined responsibilities about the handled data or company operations. The legal implications of utilizing an outside IT supplier should be thoroughly investigated.
6. **Security:** Not just confidentiality, but the entire structure should be evaluated. Where will your data be stored? Who will have access to the data? What security and protection does the cloud provider provide? Is all information (even non-sensitive information) delivered in plaintext or encrypted at all times?
7. **Lack of control over performance:** There is always the possibility that the system quality is insufficient or that a cloud service provider is unable to deliver excellent services at all times. It should be obvious what assurances the provider can give in terms of system performance and, in particular, how quick its corrective action is in the event of a service outage. Because a firm does not have direct access to the infrastructure, it must rely on the provider's fast action when something goes wrong.
8. **Lack of control over the quality:** A company must have faith in the quality standards that a provider can supply over time. At the same time, the company should know the answer of 'How simple would it be to transfer providers if there was a clear deterioration in quality?' in case they needed to change the provider due to quality issues.

SOFTWARE-AS-A-SERVICE SECURITY

Future cloud computing models will most likely integrate the usage of SaaS, utility computing, and Web 2.0 collaborative technologies to harness the Internet to meet the demands of their consumers. As a result of the shift to cloud computing, new business models are emerging that include not just new technology and business operating procedures, but also new security requirements and concerns.

As the most recent evolutionary step in the cloud service model, SaaS will most certainly remain the dominant cloud service model in the future, as well as the sector with the most demand for security standards and monitoring. To avoid losing or not being able to access their data, companies or end-users will need to examine vendor rules on data security before employing vendor services, just as they would with a managed service provider.

Gartner, technology research, and consultancy firm, has identified seven security risks that should be discussed with a cloud computing vendor:

2. **Compatibility:** Migration to the cloud may cause compatibility issues with an existing IT infrastructure, as well as with a company's security needs and organizational regulations. Pre-planning is essential once again in examining all of these factors before committing to the change.
3. **Trust:** Not all service providers are created equal. Unforeseen incidents may cause disruptions to cloud computing services. Service provider outages, for example, can occur. Because providers cannot guarantee that no service outages will occur, data may not be available 24 hours a day, seven days a week. During a disaster, communications may be slowed or shut down for an extended length of time. Once again, a thorough evaluation of the cloud service provider is essential. Businesses must examine the dangers of entrusting all of their operations to a third party, as well as what would happen in the event of a default and service disruption. What assurances the cloud service provider provides in the event of a disaster is something a corporation should think about.
4. **Confidentiality:** Confidentiality is frequently cited as a justification for not adopting cloud computing as the primary worry. When a company's activities need the management of sensitive data, data protection becomes a priority and a problem. A company may be hesitant to share sensitive information with a third party. When data is handled and exchanged between two parties, assigning responsibility for a data breach may be difficult.
5. **Compliance:** There are dangers associated with noncompliance with current rules and predetermined responsibilities about the handled data or company operations. The legal implications of utilizing an outside IT supplier should be thoroughly investigated.
6. **Security:** Not just confidentiality, but the entire structure should be evaluated. Where will your data be stored? Who will have access to the data? What security and protection does the cloud provider provide? Is all information (even non-sensitive information) delivered in plaintext or encrypted at all times?
7. **Lack of control over performance:** There is always the possibility that the system quality is insufficient or that a cloud service provider is unable to deliver excellent services at all times. It should be obvious what assurances the provider can give in terms of system performance and, in particular, how quick its corrective action is in the event of a service outage. Because a firm does not have direct access to the infrastructure, it must rely on the provider's fast action when something goes wrong.
8. **Lack of control over the quality:** A company must have faith in the quality standards that a provider can supply over time. At the same time, the company should know the answer of 'How simple would it be to transfer providers if there was a clear deterioration in quality?' in case they needed to change the provider due to quality issues.

SOFTWARE-AS-A-SERVICE SECURITY

Future cloud computing models will most likely integrate the usage of SaaS, utility computing, and Web 2.0 collaborative technologies to harness the Internet to meet the demands of their consumers. As a result of the shift to cloud computing, new business models are emerging that include not just new technology and business operating procedures, but also new security requirements and concerns.

As the most recent evolutionary step in the cloud service model, SaaS will most certainly remain the dominant cloud service model in the future, as well as the sector with the most demand for security standards and monitoring. To avoid losing or not being able to access their data, companies or end-users will need to examine vendor rules on data security before employing vendor services, just as they would with a managed service provider.

Gartner, technology research, and consultancy firm, has identified seven security risks that should be discussed with a cloud computing vendor:

Privileged user access—Inquire about who has specialized access to data, and about the hiring and management of such administrators.

Regulatory compliance— Make sure that the vendor is willing to undergo external audits and/or security certifications.

Data location— does the provider allow for any control over the location of data?

Data segregation—Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

Recovery—Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?

Investigative support—Does the vendor have the ability to investigate any inappropriate or illegal activity?

Long-term viability— what will happen to data if the company goes out of business? How will data be returned, and in what format?

Because determining data security is increasingly difficult nowadays, data security functions have grown more important than in the past. To address the security challenges outlined above, as well as others stated previously in the chapter, SaaS providers will need to include and improve on security techniques established by managed service providers, as well as develop new ones as the cloud computing environment matures.

IMPORTANT ACTIONS FOR A SECURITY TEAM

Security management

Creating a written charter for the security organization and program is one of the most critical tasks for a security team. This will establish a common vision across the team of what security leadership is aiming for and expecting, as well as "ownership" in the collective team's performance. The charter should correspond to the strategic strategy of the organization or firm for whom the security team works. A lack of clearly defined duties and duties, as well as agreement on expectations, can lead to a general sense of loss and uncertainty within the security team on what is expected of them, how their talents and expertise may be exploited, and fulfilling their performance objectives.

Risk Management

Identification of technological assets; identification of data and its relationships to business processes, applications, and data repositories; and assignment of ownership and custodial obligations are all part of effective risk management. Maintaining a repository of information assets should also be part of the action plan. Owners have responsibility and accountability for information assets, including security needs, and custodians apply controls for confidentiality, integrity, availability, and privacy. A structured risk assessment approach that distributes security resources tied to business continuity should be developed.

Risk Assessment

Security risk assessment is essential for assisting the information security organization in making educated decisions when balancing the competing requirements of business usefulness and asset protection. Inattention to completing formalized risk assessments can contribute to an increase in information security audit findings, jeopardize certification goals, and result in inefficient and ineffective security control selection that may not adequately mitigate information security risks to an acceptable level. A structured information security risk management approach should identify information security threats proactively and plan and manage them on a regular or as-needed basis. Threat modeling should be used for more extensive and technical security risk assessments of apps and infrastructure. This allows product managers and engineers to be more proactive in developing and testing application and system security, as well as engage more closely with the internal security team. Threat modeling necessitates the understanding of IT and business processes, as well as the technical expertise of the applications or systems under consideration.

Security Awareness

People will continue to be the weakest link in security. Knowledge and culture are two of the few effective strategies for managing people-related hazards. Failure to provide enough knowledge and training to those who may require it can expose the firm to a range of security concerns, threats, and points of entry of which are people rather than system or application vulnerabilities. Social engineering attacks delayed reporting and reaction to potential security events, and unintended customer data breaches are all conceivable and likely dangers that can be caused by a lack of an effective security awareness program. For SaaS firms, a one-size-fits-all approach to security awareness is not always the best strategy; instead, it is more vital to establish an information security awareness and training program that tailors the information and training to the individual's job in the business. For example, development engineers can receive security awareness training in the form of secure code and testing, whilst customer service representatives can receive data privacy and security certification awareness training. In an ideal world, both a generic and an individual-role approach would be applied.

Education and Training

Programs should be established to offer a foundation for teaching the security team and their internal partners' essential security and risk management skills and knowledge. This comprises a structured procedure for assessing and aligning skill sets to the needs of the security team, as well as providing proper training and mentorship—offering a comprehensive foundation of core security knowledge, including data privacy and risk management. The security concerns that a company faces will alter as the cloud computing business model and its associated services evolve. The security staff may not be equipped to fulfill the demands of the company if proper, current training and mentorship programs are not in place.

Policies, Standards, and Guidelines

There are several tools and templates available to assist in the creation of information security policies, standards, and guidelines. A cloud computing security team should begin by identifying the information security and business needs that are specific to cloud computing, SaaS, and collaborative software application security. Policies, as well as supporting standards and guidelines, should be defined, recorded, and applied. These rules, standards, and guidelines should be evaluated regularly (at least yearly) or whenever significant changes occur in the business or IT environment. As a cloud computing organization's business model develops, outdated rules, standards, and guidelines may result in the unintended disclosure of information. As business goals, the business environment, and the risk landscape evolve, it is critical to maintaining the correctness and relevance of information security policies, standards, and guidelines. Such rules, standards, and guidelines also serve as the foundation upon which an organization may assure consistency of performance and knowledge continuity throughout periods of resource turnover.

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SECSDLC)

The SecSDLC entails identifying specific threats and the risks they represent, then designing and implementing specific controls to fight those threats and aid in controlling the risks they pose to the company and/or its customers. The SecSDLC must be consistent, repeatable, and conformant. The SDLC is divided into six phases, each of which includes processes unique to the SecSLDC:

Phase 1. **Investigation**: Define project processes and objectives and include them in the program security policy.

Phase 2. **Analysis**: Analyze current security policies and programs, current threats and controls, legal challenges, and risk analysis.

Phase 3. **Logical design**: Create a security blueprint, prepare incident response activities, business catastrophe responses, and assess the viability of continuing and/or outsourcing the project.

Phase 4. **Physical design**: Develop a definition of a successful solution, establish physical security measures to support technical solutions, and evaluate and approve plans.

Phase 5. **Implementation**: Purchase or create security solutions. Present a tested package to management for approval at the end of this phase.

Phase 6. **Maintenance**: To respond to evolving dangers, constantly monitor, test, adjust, update, and repair.

Security Monitoring And Incident Response

Centralized security information management systems should be utilized to offer security vulnerability notification and to continually monitor systems using automated methods to identify possible concerns. They should be integrated with network and other system monitoring procedures (for example, security information management, security event management, security information and event management, and security operations centers that rely on these systems for dedicated 24/7/365 monitoring). Management of independent third-party security testing regularly should also be incorporated. Because many security risks and challenges in SaaS revolve around the application and data layers, the variety and sophistication of threats and assaults in a SaaS business necessitate a different approach to security monitoring than traditional infrastructure and perimeter monitoring. As a result, the organization's security monitoring capabilities may need to be expanded to encompass application- and data-level operations. Subject-matter specialists in application security and the special issues of protecting privacy in the cloud may also be required. A corporation may be unable to detect and prevent security risks and assaults on its customer data and service stability if it lacks this skill and competence.

Cloud Computing Security Architecture

Cloud security architecture encompasses all of the hardware and technology used to safeguard data, workloads, and systems on cloud platforms. Creating a cloud security architecture should begin during the initial phase, and it should be integrated into cloud platforms from the ground up. Secure cloud computing architecture encompasses three core capabilities: confidentiality, integrity, and availability which were already discussed at the beginning of this chapter.

There are several technologies available in cloud platforms to handle confidentiality, integrity, and availability, with the ultimate objective of building a trusted execution environment. These are just a few of the tools that cloud security architects and professionals use to help protect systems and data.

- Encryption safeguards text and data by converting them into ciphers that only authorized parties may decipher, access, and alter.
- Firmware resilience not only assists in the prevention of attacks on the firmware layer but also includes recovering from an attack and returning the system to a known good condition.
- Creating a root of trust includes ensuring boot integrity, which protects the system against malware injections during system startup.
- Stack validation tries to show that all components and software inside a system stack have been validated and are neither corrupted nor modified, either before delivery, in transit to cloud architects, or during deployment.
- As a best practice, secure systems are meant to segregate virtual machines (VMs), containers, data, and applications from one another.

On-Premises (for reference)	IaaS (infrastructure-as-a-service)	PaaS (platform-as-a-service)	SaaS (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Customer Responsibility — Cloud Provider Responsibility

Figure 6.1: Shared responsibility model for security in the cloud

The cloud, whether private, public, or hybrid, offers the promise of agility, efficiency, and cost-effectiveness. These are transformative characteristics for any business, allowing it to respond to market changes through quick service delivery and the capacity to make data-informed decisions. Businesses, on the other hand, may be unable to use cloud resources without putting themselves and their data in danger. Cloud security architecture enables enterprises to take advantage of all the cloud has to offer, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), while reducing exposure and susceptibility. Without cloud security design, the hazards of cloud computing may outweigh any possible benefits.

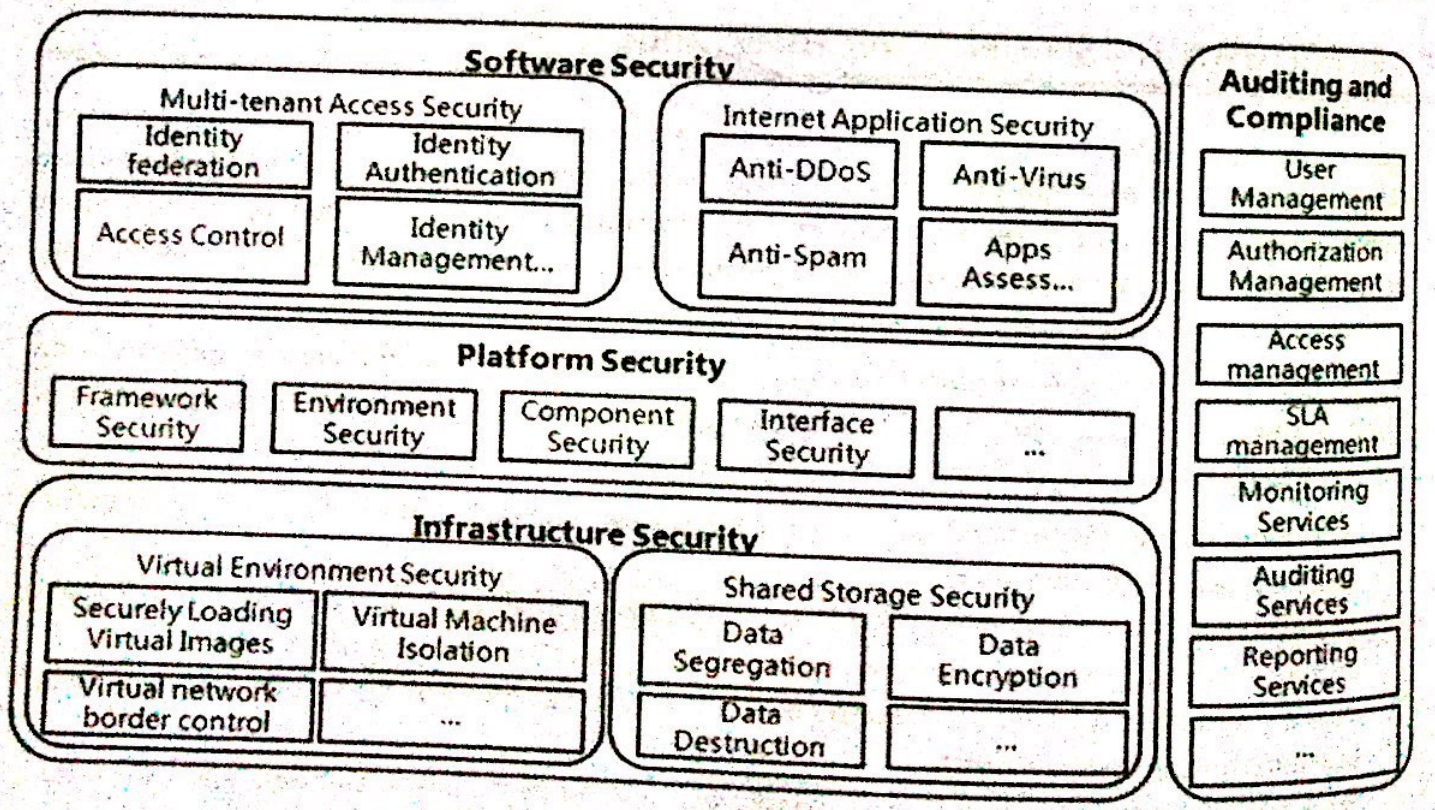

Figure 6.2. Cloud computing security architecture

You should plan for typical dangers such as malware and privilege-based attacks while planning the cloud implementation. We have already discussed the security issues which are widely being seen in the cloud environment so the cloud security architecture should focus to mitigate the risk as much as possible.

Although cloud computing provides numerous advantages, there are still several real-world issues that must be addressed. Cloud computing is a promising sector, but weaknesses in the cloud paradigm will

raise security risks. According to service delivery methods, deployment patterns, and critical cloud computing capabilities, data security and privacy protection are the major challenges that must be addressed as soon as possible. Issues with data security and privacy arise at all levels of Software, Platform, Infrastructure (SPI) service delivery architectures.

SECURITY ARCHITECTURE DESIGN

Processes such as enterprise authentication and authorization, access control, confidentiality, integrity, nonrepudiation, security management, etc. should be considered when developing a security architecture framework, as should operational procedures, technology specifications, people and organizational management, and security program compliance and reporting. To fulfill business objectives, a security architecture document should be created that defines security and privacy standards. Asset classification and control, physical security, system access restrictions, network and computer administration, application development and maintenance, business continuity, and compliance all necessitate documentation. A design and implementation program that includes a business case, requirements definition, design, and implementation strategies should be linked with the formal system development life cycle. Technological and design approaches, as well as the security processes required to deliver the following services across all technology levels, should be included in the security architecture.

- Authentication
- Authorization
- Availability
- Confidentiality
- Integrity
- Accountability
- Privacy

The development of a secure architecture gives engineers, data center operations staff, and network operations staff a standardized blueprint for designing, building, and testing the security of applications and systems. Design reviews of new modifications may be more effectively examined against this architecture to ensure that they adhere to the principles outlined in the architecture, allowing for more consistent and effective design reviews.

VULNERABILITY ASSESSMENT

Vulnerability assessment categorizes network assets to better prioritize vulnerability-mitigation initiatives such as patching and system upgrades. It assesses the success of risk mitigation by establishing objectives such as reduced vulnerability exposure and faster mitigation. To close vulnerabilities before they may be exploited, vulnerability management should be linked with discovery, patch management, and upgrade management procedures.

DATA PRIVACY

A risk assessment, as well as a gap analysis of controls and processes, must be conducted. Formal privacy processes and activities must be defined, maintained, and perpetuated based on this data. Privacy controls and protection, like security, must be incorporated into the secure architectural design. Depending on the size of the business and the scope of activities, an individual or a team should be allocated and charged with safeguarding privacy. To handle data privacy issues and concerns, a member of the security team responsible for the privacy or a corporate security compliance team should engage with the business legal team. As with security, a privacy steering group should be formed to assist in making data privacy choices. Typically, the security compliance team, if one exists at all, will lack formalized data privacy training, limiting the organization's capacity to effectively handle the data privacy concerns it already faces and will be repeatedly challenged in the future. The solution is to employ a consultant in this field, a privacy specialist, or have one of your current staff members adequately taught. This ensures that your firm is ready to satisfy the data privacy requirements of its customers and regulators.

DATA SECURITY

Data-level security is the ultimate difficulty in cloud computing because sensitive data is the province of the organization, not the cloud computing provider. Enterprises will need to bring security to the data level to ensure that their data is secure wherever it travels. For example, using data-level security, the company can indicate that this data is not permitted to leave the United States. It can also compel the encryption of particular types of data and restrict access to the data to only specific people.

APPLICATION SECURITY

One of the crucial success elements for a world-class SaaS firm is application security. The security features and requirements are defined here, and the application security test results are examined. Application security methods, secure coding rules, training, and testing scripts and tools are often developed together by the security and development teams. Although product engineering will most likely focus on the application layer, the application's security design, and the infrastructure layers that interact with the application, the security team should give the security requirements for the product development engineers to implement.

The security and product development teams should work together on this. For application source code reviews, external penetration testers are utilized, and attack and penetration tests give an objective examination of the program's security as well as assurance to clients that attack and penetration tests are done regularly. Collaboration on application security that is fragmented and undefined might result in lower-quality design, development, and testing results.

Because many connections between businesses and their SaaS providers are made via the web, providers should secure their web applications in the cloud by following Open Web Application Security Project guidelines for secure application development and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks, just as they would on-premises. LAMP stands for 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. PHP is frequently replaced with Perl or Python.

VIRTUAL MACHINE SECURITY

Physical servers in the cloud are aggregated to numerous virtual machine instances on virtualized servers. Data center security teams may not only duplicate conventional security policies for the data center as a whole to safeguard virtual machines, but they can also advise their clients on how to prepare these machines for transfer to a cloud environment when suitable. Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection may all be implemented as software on virtual machines to boost server and application protection and compliance integrity when virtual resources migrate from on-premises to public cloud settings. By applying this conventional line of protection to the virtual machine itself, you can safeguard the migration of essential programs and data to the cloud. To enable 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, allowing for tighter policy and the flexibility to move the virtual machine from on-premises to cloud resources. At the virtual machine level, integrity monitoring and log inspection software must be used. As a significant approach to virtual machine security, the software can be put into a single software agent that provides consistent control and management throughout the cloud while seamlessly integrating back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings.

HIGH AVAILABILITY AND FAULT TOLERANCE

An effective IT infrastructure must function even in the event of a rare network loss, device failure, or power loss. When the system fails, one or more of the three major availability techniques will kick in: high availability, fault tolerance, and/or disaster recovery. While each of these infrastructure design solutions contributes to the availability of your key applications and data, they do not fulfill the same goal. Simply because you run a High Availability infrastructure does not mean you need not set up a disaster recovery site – and doing so risks disaster.

DATA SECURITY

Data-level security is the ultimate difficulty in cloud computing because sensitive data is the province of the organization, not the cloud computing provider. Enterprises will need to bring security to the data level to ensure that their data is secure wherever it travels. For example, using data-level security, the company can indicate that this data is not permitted to leave the United States. It can also compel the encryption of particular types of data and restrict access to the data to only specific people.

APPLICATION SECURITY

One of the crucial success elements for a world-class SaaS firm is application security. The security features and requirements are defined here, and the application security test results are examined. Application security methods, secure coding rules, training, and testing scripts and tools are often developed together by the security and development teams. Although product engineering will most likely focus on the application layer, the application's security design, and the infrastructure layers that interact with the application, the security team should give the security requirements for the product development engineers to implement.

The security and product development teams should work together on this. For application source code reviews, external penetration testers are utilized, and attack and penetration tests give an objective examination of the program's security as well as assurance to clients that attack and penetration tests are done regularly. Collaboration on application security that is fragmented and undefined might result in lower-quality design, development, and testing results.

Because many connections between businesses and their SaaS providers are made via the web, providers should secure their web applications in the cloud by following Open Web Application Security Project guidelines for secure application development and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks, just as they would on-premises. LAMP stands for 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. PHP is frequently replaced with Perl or Python.

VIRTUAL MACHINE SECURITY

Physical servers in the cloud are aggregated to numerous virtual machine instances on virtualized servers. Data center security teams may not only duplicate conventional security policies for the data center as a whole to safeguard virtual machines, but they can also advise their clients on how to prepare these machines for transfer to a cloud environment when suitable. Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection may all be implemented as software on virtual machines to boost server and application protection and compliance integrity when virtual resources migrate from on-premises to public cloud settings. By applying this conventional line of protection to the virtual machine itself, you can safeguard the migration of essential programs and data to the cloud. To enable 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, allowing for tighter policy and the flexibility to move the virtual machine from on-premises to cloud resources. At the virtual machine level, integrity monitoring and log inspection software must be used. As a significant approach to virtual machine security, the software can be put into a single software agent that provides consistent control and management throughout the cloud while seamlessly integrating back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings.

HIGH AVAILABILITY AND FAULT TOLERANCE

An effective IT infrastructure must function even in the event of a rare network loss, device failure, or power loss. When the system fails, one or more of the three major availability techniques will kick in: high availability, fault tolerance, and/or disaster recovery. While each of these infrastructure design solutions contributes to the availability of your key applications and data, they do not fulfill the same goal. Simply because you run a High Availability infrastructure does not mean you need not set up a disaster recovery site — and doing so risks disaster.

High Availability

A High Availability system is meant to be up and running 99.99 percent of the time, or as close to it as feasible. Typically, this entails creating a failover system capable of handling the same workloads as the original system. HA works in a virtualized environment by generating a pool of virtual computers and related resources inside a cluster. When one of the hosts or virtual machines dies, it is resumed on another VM in the cluster. HA is done in physical infrastructure by designing the system with no single point of failure; in other words, redundant components are required for all key power, cooling, compute, network, and storage infrastructure.

Hosting two identical web servers with a load balancer distributing traffic between them and an extra load balancer on standby is one example of a basic HA approach. If one of the servers fails, the balancer may route traffic to the other.

Fault Tolerance

The ability of a system (computer, network, cloud cluster, etc.) to continue working without interruption when one or more of its components fail is referred to as fault tolerance. The goal of developing a fault-tolerant system is to reduce interruptions caused by a single point of failure, while also assuring the high availability and business continuity of mission-critical applications or systems.

Fault-tolerant systems employ backup components that automatically take the place of failing components, ensuring that there is no interruption in service. These are some examples:

- Hardware systems that are supported by the same or analogous hardware systems. A server, for example, can be made fault-tolerant by operating an identical server in parallel, with all processes mirrored to the backup server.
- Software systems that are backed up by other instances of software. A database containing customer information, for example, can be continually copied to another system. If the primary database fails, operations can be immediately diverted to the backup database.
- Power sources that have been made fault-tolerant through the use of alternate sources. Many firms, for example, have backup generators that can take over if the main power supply fails.

Similarly, any system or component that has a single point of failure can be made fault-tolerant through the use of redundancy.

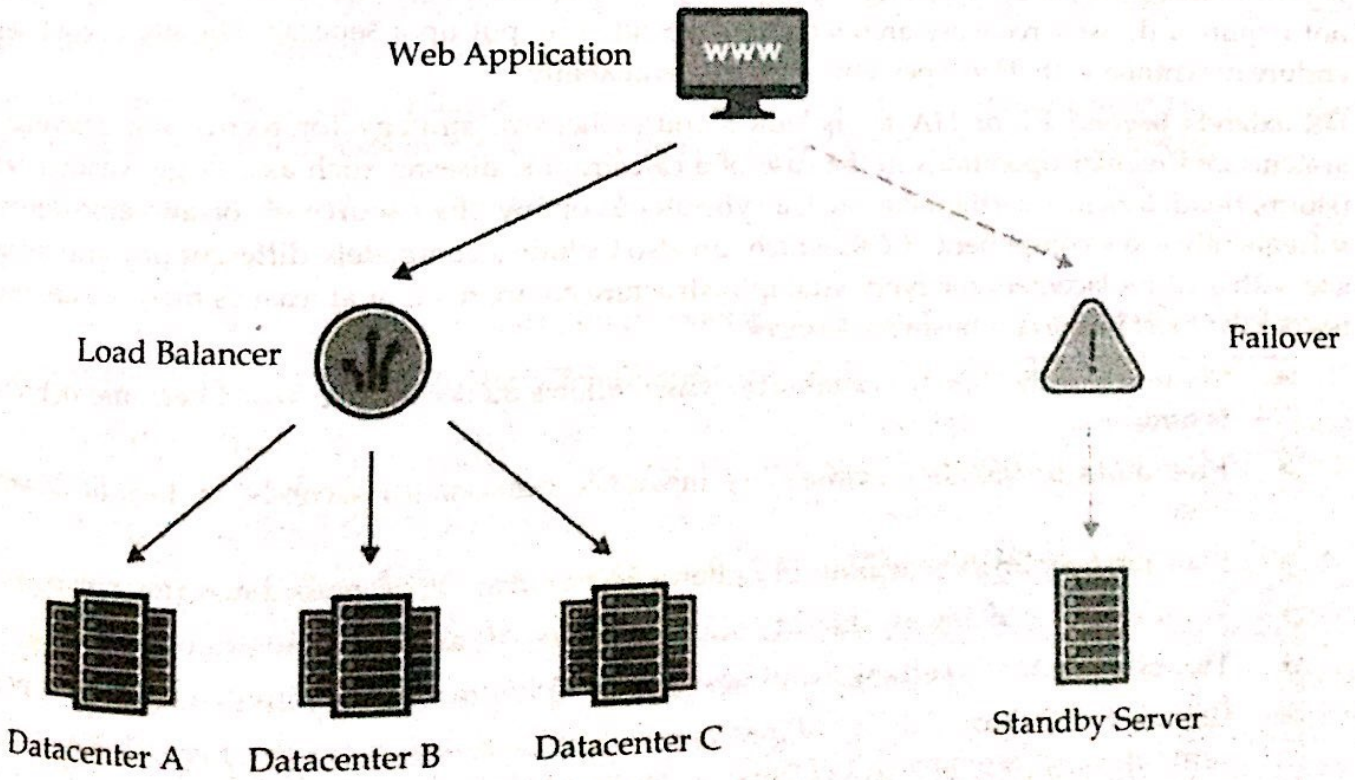

Figure 6.3: Load balancing and failover are both integral aspects of fault tolerance.

SCALABILITY AND FAULT TOLERANCE

Scalability refers to the capacity to scale facilities and services on-demand as needed by the user. Scaling is beyond the bounds, which implies we have no idea what the limit will be. Cloud middleware is built with scalability in mind across several dimensions, such as performance, size, and load. The cloud middleware controls a large number of resources and users who rely on the cloud to acquire resources that they cannot access on-premises without incurring administrative and maintenance fees. These expenses are borne by whoever creates, operates, and maintains the cloud middleware and provides the service to clients.

So, in this general scenario, the capacity to endure failure is typical, but it becomes more essential than delivering an efficient and optimized system at times. According to the general conclusion, 'it is a difficult challenge for cloud providers to design such highly scalable and fault-tolerant systems that can be maintained while still providing competitive performance.'

VMware vSphere Fault Tolerance (FT) creates a live shadow version of a virtual machine that replicates the original virtual machine to offer continuous availability for applications (with up to four virtual CPUs). If a hardware failure occurs, vSphere FT initiates a failover to reduce downtime and data loss. Following failover, vSphere FT builds a new, secondary virtual machine to provide ongoing protection for the application.

VMware Fault Tolerance ensures continuous availability for virtual machines by building and maintaining a Secondary VM that is identical to the Primary VM and is constantly available to replace it in the case of a failover emergency.

Most mission-critical virtual machines have Fault Tolerance enabled. The Secondary VM is a second virtual machine that operates in virtual lockstep with the Primary VM. VMware vLockstep records inputs and events on the Primary VM and forwards them to the Secondary VM, which is running on a different host. Using this information, the execution of the Secondary VM is similar to that of the Primary VM. Because the Secondary VM is in virtual lockstep with the Primary VM, it may take over execution at any time without interruption, providing fault tolerance.

DISASTER RECOVERY

If your systems are set up with High Availability (HA) or Fault Tolerance (FT), it may appear that you do not require a disaster recovery architecture. After all, why put up a separate DR site if your servers can endure downtime with 99.999 percent or greater availability?

DR extends beyond FT or HA to include a comprehensive strategy for recovering essential business systems and regular operations in the case of a catastrophic disaster such as a large weather catastrophe (storm, flood, tornado, earthquake, etc.), a cyberattack, or any other source of considerable downtime. HA is frequently a key component of DR, which can also include a completely different physical infrastructure site with a 1:1 replacement for every vital infrastructure component, or at least as many as are necessary to restore the most important business services.

- Six nines or 99.9999% availability, which allows 32 seconds or less downtime per year, which is ambitious.
- Five nines or 99.999% availability means 5 minutes, 15 seconds, or less of downtime in a year.
- Four nines or 99.99% availability allows 52 minutes, 36 seconds downtime per year.
- Three nines or 99.9% availability allows 8 hours, 46 minutes downtime per year.
- Two nines or 99% availability allows 3 days, 15 hours, and 40 minutes downtime per year.
- One nine or 9% availability allows over 332 days of downtime per year. You are only up and running about a month out of the year on average.
- Zero nines are useless. It is 100% downtime per year.

DR is set up with a Time to Recovery and Recovery Point, which indicate the time it takes to restore critical systems and the point in time before the catastrophe that is restored (you probably do not need to restore backup data from 5 years ago to come back to work during a catastrophe, for example).

A disaster recovery platform copies your chosen systems and data to a second cluster for storage. This mechanism is activated when downtime is detected, and your network pathways are rerouted. DR is frequently used to replace a whole data center, whether real or virtual, as opposed to HA, which often deals with problems in a single component such as a CPU or a single server rather than a full failure of all IT infrastructure, as would occur in the event of a disaster.

CLOUD DISASTER RECOVERY (CLOUD DR)

Cloud disaster recovery is a backup and restoration method that involves keeping and keeping copies of electronic documents as a security measure in a cloud computing environment. The purpose of cloud DR is to offer a method for an organization to recover data and/or enable failover in the case of a man-made or natural disaster. Cloud disaster recovery often offers the same services as an on-premises or company-managed off-premises disaster recovery plan (DRP) facility but on a more cost-effective, efficient, and provider-managed platform. A cloud DRP vendor assigns users and storage space, and updates selected computers with client software installed on each system regularly. Users may add, amend, and delete systems and storage space without having to worry about the back-end infrastructure.

A cloud-based disaster recovery solution allows users to scale up the complete cloud DRP system from one to many. The storage and client software licenses are generally invoiced to the customer monthly. Most Cloud DR services include backup and recovery for essential server machines that run enterprise-level programs such as MS-SQL, Oracle, and others.

Although the idea - and some of the goods and services - of cloud-based disaster recovery is still in its early stages, some businesses, particularly small and medium-sized businesses (SMBs), are finding and beginning to leverage cloud services for DR. Because the usage-based pricing of cloud services is ideally suited for DR where the secondary infrastructure is parked and idle most of the time, it might be an appealing choice for organizations that may be short on IT resources. Having disaster recovery sites in the cloud eliminates the requirement for data center space, IT equipment, and IT staff, resulting in considerable cost savings, allowing smaller businesses to adopt disaster recovery alternatives that were previously only available to bigger corporations.

Disaster recovery in the cloud is not a flawless solution, and its flaws and limitations must be thoroughly recognized before a company invests in it. Security is frequently at the top of the list of concerns:

- Is data securely transferred and stored in the cloud?
- How are users authenticated?
- Are passwords the only option or does the cloud provider offer some type of two-factor authentication?
- Does the cloud provider meet regulatory requirements?

Furthermore, because clouds are accessed over the Internet, bandwidth needs must be properly recognized. There is a danger in merely preparing for bandwidth needs to shift data onto the cloud without considering how to keep the data accessible in the event of a disaster:

- Do you have the bandwidth and network capacity to redirect all users to the cloud?
- If you plan to restore from the cloud to on-premises infrastructure, how long will that restore take?

Reliability of the cloud provider, its availability, and its ability to serve your users while a disaster is in progress are other key considerations. The choice of a cloud service provider or managed service provider (MSP) that can deliver service within the agreed terms is essential, and a wrong decision can even get you fired.

OPTIONS TO DISASTER RECOVERY IN THE CLOUD

Managed Applications And Managed Dr

A growing trend is to deploy both primary production and disaster recovery instances in the cloud and have them maintained by a managed service provider (MSP). By doing so, you gain all of the benefits of cloud computing, including usage-based pricing and the elimination of on-premises equipment. Instead of performing it yourself, you outsource disaster recovery to a cloud or managed service provider. The selection of a service provider and the process of drafting suitable service-level agreements (SLAs) are critical. By entrusting control to the service provider, you must be assured that it will supply uninterrupted service within the stated SLAs for both primary and DR instances. For email and certain other business applications, such as customer relationship management (CRM), where Salesforce.com has been a pioneer and is now leading the cloud-based CRM industry, a pure cloud approach is becoming increasingly attractive.

Backup to and Restore from the Cloud

In this strategy, applications and data stay on-premises, with data backed up to the cloud and restored to on-premises hardware in the event of a disaster. In other words, cloud backups take the place of tape-based off-site backups. When it comes to cloud backup and recovery, it's critical to grasp both the backup and the more difficult restore elements. Backing up to the cloud is simple, and backup software makers have been expanding their backup suites to include options for directly backing up to prominent cloud service providers such as AT&T, Amazon, Microsoft, and Rackspace.

The recovery process is the most difficult component of employing cloud-based backups for disaster recovery. With limited bandwidth and potentially terabytes of data to be recovered, getting data restored on-premises within stipulated RTOs might be difficult. Some cloud backup service providers allow customers to restore data on disks, which are subsequently delivered to the client for local on-premises recovery. A big on-premises cache of recent backups that may be utilized for local restoration is another possibility. However, depending on the data to be recovered, characteristics like compression and, more critically, data deduplication might enable restorations from cloud data to on-premises infrastructure a realistic alternative.

Back up to and Restore to the cloud

Data is not restored to on-premises infrastructure in this technique; rather, it is restored to virtual computers in the cloud. This necessitates the use of cloud storage as well as cloud computational resources, such as Amazon's Elastic Compute Cloud (EC2). The restoration might be done only when a catastrophe is proclaimed, or it can be done on an ongoing basis.

Replication to virtual machines in the cloud.

Replication is the data transportation solution of choice for applications that require aggressive recovery time and recovery point goals (RPOs), as well as application awareness. Cloud virtual machine replication may be used to safeguard both cloud and on-premises production instances.

FOUR STEPS TO ACHIEVING HIGH AVAILABILITY IN THE CLOUD

Building a high-availability application in the cloud might appear to be a difficult task. The idea is to prepare for the possibility that every component of a system will fail at some time. Then you may prepare for failure and automate methods to deal with it. In the cloud, fault-tolerant systems with high availability are possible. Many businesses are striving to handle high availability (HA) and disaster recovery (DR) plans.

1. **Build for Server Failure:** Instances in the cloud, like those in a traditional data center, are transient. You must be ready for server failure. Designing stateless applications that are robust via a server or service reboot or re-launch is the first step in preparing for server failure.

- Enable auto-scaling in your application so that it may adapt to dynamic traffic patterns based on a set of performance indicators.
- Configure database mirroring, master/slave setups, and/or priming to ensure data integrity and downtime minimization.
- Use dynamic DNS and static IP addresses to ensure that components of your application's architecture are always in the correct context.

2. **Build for Zone Failure:** Power outages, network outages, and lightning strikes can all cause several servers to fail at the same time. You must ensure that your apps are ready to handle zone failures. Zones (also known as "availability zones" by Amazon Web Services) are discrete places that are designed to be isolated from failures in other zones.

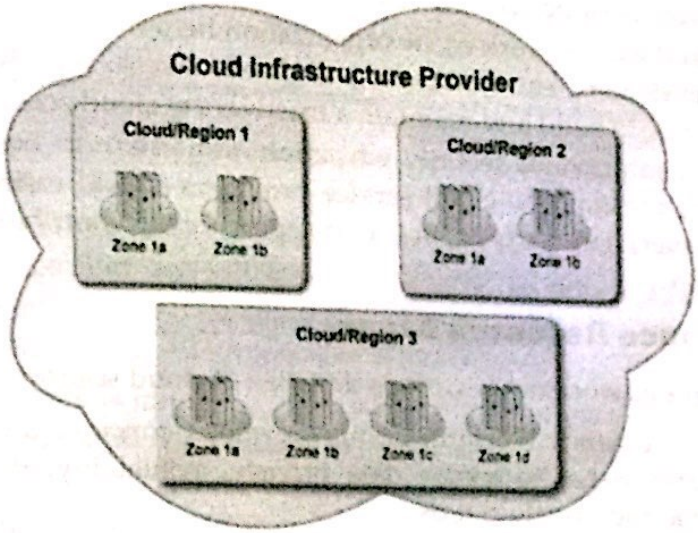

Figure 6.4: Cloud regions and Zones

- Spread the servers in each of your application tiers across at least two zones.
- Replicate data across zones. Note that this is usually cheap, though not free.

3. **Build for Cloud Failure:** Multiple zones in a region might encounter outages owing to system-wide faults on rare occasions; the April 2011 Amazon Web Services (AWS) outage is a prominent example. To achieve multiple 9s of availability, you must have a mechanism in place to deal with cloud problems. The building across clouds may be challenging since APIs, services, and settings vary. You must build your architecture using general notions (durable storage), but deploy it using cloud-specifics (EBS volumes).

By offering reusable building pieces, cloud management solutions abstract away these variations and make it easier to create a fault-tolerant strategy. These building components can be utilized to move not just between various areas of the same provider, but also between other infrastructure providers.

- Create a backup or duplicate data between regions or providers. As the traffic will transit the open Internet, ensure that your connections across these areas are safe and authenticated.
- Keep enough capacity to absorb zone or cloud outages and use reserved instances if required.
- Always remember to crawl first, then walk: Create high availability across zones before expanding to various clouds.

4. **Automate and Test Everything:** You should automate your operations in the case of a server, zone, or cloud failure as you build your infrastructure to accommodate such failures. Cloud management tools enable you to automate failover operations across servers, zones, and clouds. Because speed is of the essence in an emergency, automate everything.

- Automate backups so that your data is always available in the event of a calamity.

- Set up monitoring and notifications to discover and pinpoint problems as they arise because your cloud providers may not offer timely information.
- Your disaster recovery plan will only be useful if you test it to ensure that it works. You may test your infrastructure's capacity to tolerate failure by pushing large loads to your production servers and deactivating your different servers, services, and zones.

Cloud Security Alliance (CSA) Stack Model

The Cloud Security Alliance (CSA) is a non-profit organization that encourages research into best practices for cloud computing security and the use of cloud technology to safeguard other types of computing. CSA draws on the knowledge of industry practitioners, associations, and governments, as well as corporate and individual members, to provide cloud security research, education, certification, events, and products. The actions, knowledge, and vast network of the organization help the whole cloud community, including cloud service providers, customers, entrepreneurs, and governments. The CSA also provides a venue for all stakeholders to collaborate to build and maintain a trustworthy cloud ecosystem. The industry association also provides security education and advice to businesses at various levels of cloud adoption, as well as assistance to cloud service providers in addressing security in their software delivery methods. Any interested party with the competence to contribute to the security of cloud computing can join the CSA.

Cloud Security Alliance Research Areas

There are CSA working groups working on various domains of cloud security including:

- The Cloud Data Governance Working Group develops concepts and applies them to develop technologies and approaches to ensure data privacy, availability, integrity, confidentiality, and security across public and private clouds.
- The Cloud Security Alliance IoT Working Group develops meaningful use cases for the Internet of Things (IoT) implementations as well as practical guidelines to help security practitioners safeguard their installations.
- The CSA Application Containers and Microservices Working Group research application container and microservice security. It is also in charge of establishing best practices and guidelines for the secure usage of application containers and microservices.
- The SaaS Governance Working Group seeks to encourage and establish procedures to promote collaboration and assist suppliers and customers in working closely together to manage software-as-a-service risks, ensure the security of customer data, and ensure the resilience of the SaaS cloud architecture.

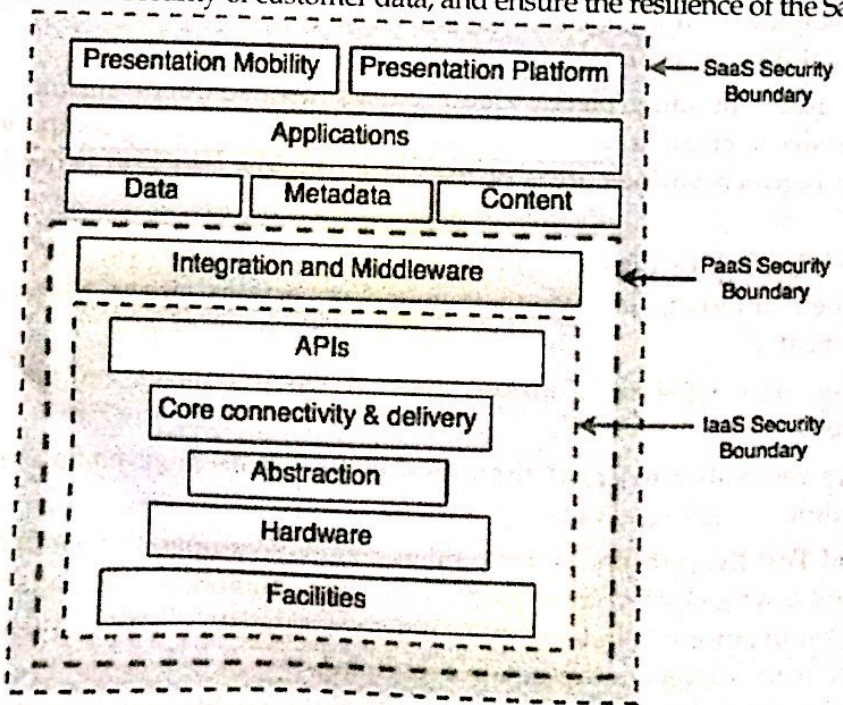

Figure 6.5: CSA Stack Model

The following are the key points in the CSA stack model:

- IaaS is the most basic level of service. PaaS and SaaS are the next levels of service.
- IaaS provides infrastructure, PaaS provides a platform development environment, and SaaS provides an operational environment.
- IaaS offers the fewest integrated functions and integrated security, whereas SaaS has the most.
- This model defines the security boundaries. The cloud service provider's duties cease at the security barrier, and the customer's duties begin.
- The security mechanism below the security border is required for the system to be built and should be maintained by the client.

QOS ISSUES IN CLOUD

In recent years, corporate applications have been implemented in the cloud environment. And with such development, Quality of Service (QoS) management is one of the issues posed by cloud applications. This issue deals with assigning resources to the mobile apps or web applications to provide a high quality of service increasing performance and accessibility. The degree to which a collection of fundamental characteristics meets the requirements. Fundamental characteristics are required components of the system and cannot be removed from it.

A system's or application's quality is influenced by a variety of things such as Flexibility, Maintainability, Performance and Efficiency, Scalability, Availability, Reliability, Usability and Accessibility, Platform Compatibility, and Security.

1. **Flexibility** refers to the system's capacity to control functionality without harming the system. The services can be altered according to the business needs of a company.
2. **Maintainability** focuses on changes related to system correction. Reducing complexity greatly improves the maintainability of the system. Good abstractions can help reduce complexity and make the system easier to modify and adapt for new use cases.
3. **Performance and efficiency** refer to the software's reaction time. Efficient cloud performance is crucial for assuring business continuity and providing access to cloud services to all relevant parties.
4. **Scalability** means having strategies for keeping performance good, even when load increases. In a scalable system, you can add processing capacity to remain reliable under high load.
5. **Availability** makes sure your products, services, and tools available to the consumers and workers at any time and from any location via any device with an Internet connection. Cloud availability and cloud reliability are interconnected.
6. **Reliability** means making systems work correctly, even when faults occur. Faults can be in hardware, software, and humans. The fault-tolerant system can be built with the help of extra resources which will be the backup system and will be active if any fault occurred in the main system.
7. **Usability and Accessibility**: Usability relates to how comfortable is the system to use. As the user interface is the most visible aspect of the system, it must be simple to use. Everyone can observe, comprehend, navigate, and interact with the system if it is accessible. The goal of accessibility is to ensure that there are no system-related impediments to normal individuals or individuals with impairments. Accessibility may also relate to people's desire for the system to be available in a language other than English.
8. **Platform Compatibility:** A good system should be able to run on as many different platforms as possible so that it will cover a large number of consumers who use the system. The term platform refers to the operating system and internet browsers.
9. **Security:** This is a key issue in determining software quality. You must implement a security policy, apply it appropriately to the program, and leave no entrance gaps. Security policies such as authentication and authorization mechanisms, data encryption with high-level algorithms, and network attack defense are examples of security policies.

IDENTITY MANAGEMENT AND ACCESS CONTROL

In enterprise, IT, identity, and access management (IAM) are concerned with establishing and controlling the roles and access rights of particular network entities (users and devices) to a range of cloud and on-premises services. Customers, partners, and workers are examples of users; computers, cellphones, routers, servers, controllers, and sensors are examples of devices. The discipline of managing access to business resources to keep systems and data safe is known as identity management and access control. It can assist validate your users' identities before providing them access to workplace systems and information as a critical component of your security architecture. While the phrases' identity management, authentication, and access control are sometimes used interchangeably, each of these functions as a separate layer for business security procedures.

Identity management, often known as identity and access management (IAM), is the primary discipline responsible for confirming a user's identity and degree of access to a specific system. Within that context, both authentication and access control—which govern each user's degree of access to a specific system—play critical roles in protecting user data. Every day, we engage with various authentication methods. Your identity is validated for authentication reasons when you enter a login and password, use a PIN, scan your fingerprint, or tap your bank card. After your identification has been validated, access control is used to decide your degree of access. This is critical for applications and services that require varying degrees of authorization for various users. For example, access control will allow program administrators to add users or change profiles while restricting lower-tier users' access to particular functions and information.

The primary goal of IAM systems is to provide one digital identity per human or thing. Once a digital identity has been created, it must be maintained, adjusted, and monitored throughout the access lifespan of each person or device. Identity management's main purpose is to enable access to company assets that people and devices have rights to in a particular environment. This comprises timely onboarding of users and systems, permission authorizations, and offboarding of users and devices.

IAM systems give administrators the tools and technology they need to modify a user's position, track user activity, generate reports on that activity, and enforce regulations on an ongoing basis. These systems are intended to provide a method of managing user access across a whole business while also ensuring compliance with company policy and government requirements.

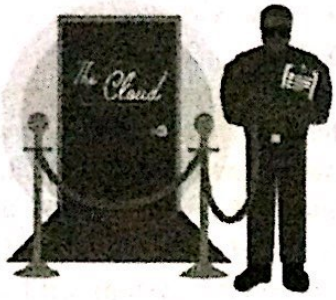

Figure 6.6: IAM is like the bouncer at a nightclub's entrance, with a list of who is permitted in, who is not permitted in, and who has access to the VIP section.

A person's full identity cannot be uploaded and kept on a computer, so "identity" in a computing context refers to a collection of traits that can be easily assessed and recorded digitally. Consider an ID card or a passport: an ID card does not carry every data about a person, but it does include enough personal features that a person's identification may be promptly linked to the ID card.

The three most widely used authentication factors are: 'Something the user knows' such as *username and password combination;* Something the user has' such as a USB device, or a smartphone with some authentication token and another is 'Something the user is' such as Face ID, Fingerprint, etc.

On a fundamental level, IAM encompasses the following components:

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

IMPORTANCE OF IAM FOR CLOUD COMPUTING

As we all know, data is stored remotely and accessed through the Internet in cloud computing. As customers may access the Internet from practically any place and device, most cloud services are device and location independent. To access the cloud, users no longer need to be at the office or on a company-owned device. Indeed, remote workforces are growing more prevalent. As a result, identification, rather than the network boundary, becomes the most essential point of control for access. The identity of the user, not their device or location, defines what cloud data they can access and if they may access it at all. Assume a cybercriminal trying to gain access to sensitive material stored in a corporate data center. Before the widespread use of cloud computing, a cybercriminal would have to breach the company firewall protecting the internal network or physically access the server by breaking into the building or paying an inside employee who will let him/her enter. The main objective of the criminal would be to breach the network's perimeter. With cloud computing, sensitive files are saved on a remote cloud server. Employees of the corporation who need to access the files need to sign in using a browser or an app. So, in the cloud environment, if a cybercriminal wants to access the data, they only require employee login credentials (*such as a username and password*) and an Internet connection; the criminal does not need to breach the network perimeter physically. In this context, identity management and access control mechanisms should be strong. IAM facilitates the prevention of identity-based threats and data breaches caused by privilege escalation. As a result, IAM solutions are vital for cloud computing.

BENEFITS OF IAM

IAM technology may be used to automate the creation, capture, recording, and management of user identities and their associated access rights. It provides the following benefits to an organization:

- All persons and services are properly authenticated, approved, and audited, and access privileges are provided following the policy.
- Companies that manage identities effectively have better control over user access, lowering the risk of internal and external data breaches.
- Automating IAM systems enables organizations to function more efficiently by reducing the effort, time, and money necessary to manage network access manually.
- In terms of security, using an IAM framework might make it easier to enforce regulations surrounding user authentication, validation, and privileges, as well as solve concerns with power creep.
- IAM systems assist businesses in better complying with regulatory rules by allowing them to demonstrate that company information is not being exploited. Companies can also demonstrate that any data required for audits is readily available.

TYPES OF DIGITAL AUTHENTICATION

1. **Unique Passwords:** The unique password is the most frequent method of digital authentication. Some businesses demand longer or more complicated passwords that include a mixture of characters, symbols, and numbers to make passwords safer. Users often find memorizing unique passwords onerous unless they can automatically aggregate their collection of passwords behind a single sign-on entry point.

2. **Pre-shared Key (PSK):** PSK is a sort of digital authentication in which the password is shared among users who are permitted to access the same resources – think of it as a branch office Wi-Fi password. Individual passwords are more secure than this method of authentication. One issue with shared passwords, such as PSK, is that they must be changed regularly, which can be inconvenient.
3. **Behavioral authentication:** When working with extremely sensitive data and systems, businesses can employ behavioral authentication to go much more detailed and evaluate keyboard dynamics or mouse-usage patterns. Organizations can swiftly determine if the user or machine behavior deviates from the usual by utilizing artificial intelligence, a trend in IAM systems, and can automatically lock down systems.
4. **Biometrics:** It is a term used to describe the use of Biometrics used in modern IAM systems to provide more precise authentication. They capture fingerprints, irises, faces, palms, gaits, voices, and, in certain circumstances, DNA, among other biometric features. Passwords have been discovered to be less successful than biometrics and behavior-based analytics.

IMPORTANT IAM TERMS

Access Management: Access management refers to the methods and technology that are used to govern and monitor network access. Access management elements like authentication, authorization, trust and security auditing are included in both on-premises and cloud-based ID management solutions.

Microsoft Active Directory (AD): AD was created by Microsoft as a user-identity directory service for Windows domain networks. Despite being proprietary, AD is included in the Windows Server operating system and hence extensively used.

Biometric authentication: A method of authenticating users that is based on the user's unique traits. Fingerprint sensors, iris, and retina scanning, and face recognition are examples of biometric authentication technology.

Context-aware network access control: Context-aware network access control is a policy-based way of giving access to network resources depending on the user's present context. A user attempting to login from an IP address that has not been white listed, for example, would be banned.

Credential: An identification used by a user to acquire network access, such as a password, public key infrastructure (PKI) certificate, or biometric information (fingerprint, iris scan).

De-provisioning: The removal of identity from an ID repository and the termination of access privileges.

Digital identity: The ID comprising information on the user and his/her/its access privileges.

Entitlement: The set of attributes that define an authenticated security principal's access rights and privileges.

Identity as a Service (IDaaS): Cloud-based IDaaS provides identity and access management capability to an organization's on-premises and/or cloud-based systems.

Identity lifecycle management: This refers to the full set of procedures and technology for preserving and upgrading digital identities, similar to access lifecycle management. Identity lifecycle management includes identity synchronization, provisioning, and de-provisioning, as well as the continuing management of user characteristics, credentials, and entitlements.

Identity synchronization: The process of verifying that different identity stores, such as those created as a result of a merger, contain consistent data for a particular digital ID.

Lightweight Directory Access Protocol (LDAP): LDAP is an open standards-based protocol that is used to manage and access a distributed directory service, such as Microsoft's AD.

Multi-factor authentication (MFA): MFA is used when more than one factor, such as a username and password, is required for network or system authentication. At least one more step is also necessary, such as getting an SMS code on a smartphone, inserting a smart card or USB stick, or meeting a biometric authentication requirement, such as a fingerprint scan.

Password reset: It is a feature of an ID management system that allows users to re-establish their passwords, relieving administrators of the task and reducing support calls. The reset program is frequently used by the user via a browser. To authenticate the user's identity, the program requests a secret word or a series of questions.

Privileged account management: This refers to the management and auditing of accounts and data access depending on the user's rights. In general, a privileged user has administrative access to systems as a result of his or her employment or role. A privileged user, for example, might create and deactivate user accounts and roles. Provisioning is the process of establishing identities, specifying their access privileges, and registering them in an ID repository.

Risk-based authentication (RBA): Risk-based authentication increases authentication criteria dynamically based on the user's current status at the time when authentication is attempted. When users seek to authenticate from a geographic area or IP address that has not previously been linked with them, they may be subject to extra authentication procedures.

Security principal: A digital identity that includes one or more credentials that may be authenticated and used to communicate with the network.

Single sign-on (SSO): A kind of access control for several linked but distinct systems. A user may access a system or systems with a single username and password, eliminating the need for multiple credentials.

User behavior analytics (UBA): UBA systems monitor user activity patterns and employ algorithms and analysis to find significant abnormalities that may suggest possible security issues. UBA differs from other security solutions in that it is not concerned with tracking devices or security occurrences. UBA is sometimes referred to as UEBA when combined with entity behavior analytics.

OBJECTIVE QUESTIONS

1) **Which of the following service providers provides the least amount of built-in security?**
   a. SaaS b. PaaS c. IaaS d. All of the mentioned

2) **Point out the correct statement:**
   a. Different types of cloud computing service models provide different levels of security services
   b. Adapting your on-premises systems to a cloud model requires that you determine what security mechanisms are required and mapping those to controls that exist in your chosen cloud service provider
   c. Data should be transferred and stored in an encrypted format for security purpose
   d. All of the mentioned

3) **Which of the following services need to be negotiated in Service Level Agreements?**
   a. Logging b. Auditing
   c. Regulatory compliance d. All of the mentioned

4) **_____ is a framework tool for managing cloud infrastructure.**
   a. IBM Tivoli Service Automation Manager
   b. Microsoft Tivoli Service Automation Manager
   c. Google Service Automation Manager
   d. Windows Live Hotmail

5) **Which of the following areas of cloud computing is uniquely troublesome?**
   a. Auditing b. Data integrity
   c. e-Discovery for legal compliance d. All of the mentioned

6) **SaaS providers manage and secure all the following except:**
   a. Infrastructure b. OS c. Application stack d. Access controls

7) **Which data may not be suitable for public clouds?**
   a. Legacy application data b. Mission-critical workloads
   c. Sensitive data d. All of the above

8) **In which environment do admins have the most control over cloud app security?**
   a. PaaS b. SaaS c. IaaS d. CaaS

9) **Which is not a form of confidential computing?**
   a. Zero-trust networks b. Trust execution environments
   c. Fully homomorphic encryption d. Secure multiparty computation

10) **When is centralized cloud application monitoring most useful?**
   a. When applications must span hybrid architectures
   b. When applications are hosted solely in the cloud
   c. When an organization's applications are all on-premises
   d. When an organization uses a single cloud application

11) **During which phase of a cloud migration framework is security the most critical?**
a. Discovery phase b. Cloud migration phase
c. Operations phase d. All of the above

12) **Which of the following service providers provides the least amount of built-in security?**
a. SaaS b. PaaS c. IaaS d. All of the mentioned

13) **Point out the correct statement:**
a. Different types of cloud computing service models provide different levels of security services
b. Adapting your on-premises systems to a cloud model requires that you determine what security mechanisms are required and mapping those to controls that exist in your chosen cloud service provider.
c. Data should be transferred and stored in an encrypted format for security purpose
d. All of the above

14) **Which of the following services need to be negotiated in Service Level Agreements?**
a. Logging b. Auditing
c. Regulatory compliance d. All of the above

15) **Point out the wrong statement:**
a. You can use proxy and brokerage services to separate clients from direct access to shared cloud storage
b. Any distributed application has a much greater attack surface than an application that is closely held on a Local Area Network
c. Cloud computing does not have vulnerabilities associated with Internet applications a
d. All of the mentioned

16) **Which of the following areas of cloud computing is uniquely troublesome?**
a. Auditing b. Data integrity
c. e-Discovery for legal compliance d. All of the above

17) **Which of the following is the operational domain of CSA?**
a. Scalability b. Portability and interoperability
c. lexibility d. None of the above

18) **Which of the following is considered an essential element in cloud computing by CSA?**
a. Multi-tenancy b. Identity and access management
c. Virtualization d. All of the above

19) **Which of the following is a standard protocol for network monitoring and discovery?**
a. SNMP b. CMDB c. WMI d. All of the above

20) **Point out the correct statement:**
a. Cloud management includes not only managing resources in the cloud but managing resources on-premises
b. The management of resources in the cloud requires new technology
c. Management of resources on-premises allows vendors to use well-established network management technologies
d. All of the above

21) **Which of the following is a layer of protection for Security?**
a. Platform-level protection b. Application-level protection
c. Record-level protection d. All of the above

22) **What are security controls?**
a. Controls that are intended to ensure that attacks are unsuccessful
b. Controls that are intended to detect and repel attacks
c. Controls that are intended to support recovery from problems
d. All of the mentioned above

23) **Controls that are intended to repel attacks is analogous to _____ in dependability engineering.**
a. Fault avoidance b. Fault tolerance c. Fault detection d. None of the mentioned

24) **A system resource that has a value and has to be protected is known as**
a. Asset b. Control c. Vulnerability d. None of the mentioned

25) **Circumstances that have the potential to cause loss or harm is known as**
a. Attack b. Threat c. Vulnerability d. Control

26) A _____ view shows the system hardware and how software components are distributed across the processors in the system.
a. physical b. logical c. process d. all of the mentioned

27) Which of the following is not included in Architectural design decisions?
a. type of application b. distribution of the system
c. architectural styles d. testing the system

28) Which of the following patterns is the basis of interaction management in many web-based systems?
a. architecture b. repository pattern
c. model-view-controller d. different operating system

29) Cloud computing architecture is a combination of?
a. service-oriented architecture and grid computing
b. utility computing and event-driven architecture.
c. service-oriented architecture and event-driven architecture
d. virtualization and event-driven architecture.

30) Which of the following was one of the weaker aspects of early cloud computing service offerings?
a. Logging b. Integrity checking
c. Consistency checking d. None of the above

31) Which of the following is a common mean for losing encrypted data?
a. lose the keys b. lose the encryption standard
c. lose the account d. all of the mentioned

32) Which of the following is the key mechanism for protecting data?
a. Access control b. Auditing
c. Authentication d. All of the mentioned

33) For the _____ model, the security boundary may be defined for the vendor to include the software framework and middleware layer.
a. SaaS b. PaaS c. IaaS d. All of the mentioned

34) Which of the following service providers provides the highest level of service?
a. SaaS b. PaaS c. IaaS d. All of the mentioned above

35) Which of the following areas of cloud computing is uniquely troublesome?
a. Auditing b. Data integrity
c. e-Discovery for legal compliance d. All of the above

36) Which of the following service providers provides the least amount of built-in security?
a. SaaS b. PaaS c. IaaS d. All of the above

37) Which of the following monitors the performance of the major cloud-based services in real-time in Cloud Commons?
a. CloudWatch b. CloudSensor c. CloudMetrics d. All of the above

38) Which of the following is a workflow control and policy-based automation service by CA?
a. CA Cloud Optimize b. CA Cloud Orchestrate c. CA Cloud Insight d. CA Cloud Compose

40) Which of the following initiatives tries to provide a way of measuring cloud computing services along dimensions like cost?
a. CCE b. OCCI c. SMI d. All of the above

41) Which of the following is a core management feature offered by most cloud management service products?
a. Support of different cloud types
b. Creation and provisioning of different types of cloud resources, such as machine instances, storage, or staged applications
c. Performance reporting including availability and uptime, response time, resource quota usage, and other characteristics
d. All of the above

42) Which of the following is used for performance management for virtualized Java Apps with VMware integration?
a. Hyperic b. Internetseer c. RightScale d. All of the above

43) Which of the following is used for Web site monitoring and analytics?
a. Gomez b. Ganglia c. Elastra d. None of the above

44) Which of the following provides tools for managing Windows servers and desktops?
a. Microsoft System Center b. System Service
c. System Cloud d. All of the above

QUESTION

1. Analyze and explain the factors for successful cloud deployment.
2. How is Cloud Computing bringing new security threats and challenges? Explain different threats and vulnerabilities and probable ways to minimize them.
3. What are the steps for designing architectures for HA in the cloud?
4. Explain Confidentiality, integrity, and availability.
5. Explain cloud security services.
6. How scalability and fault tolerance is an important requirement of cloud computing. Explain the applications of Cloud Computing in various complex fields with proper examples.
7. What are the requirements for secure cloud software? Explain.
8. Explain policy implementation issues in cloud security.
9. Explain Cloud Computing Security Challenges.
10. Explain Cloud Computing Security Architecture in brief.
11. How Security is a major worry for cloud service providers as well as users? Explain the design principles of cloud information security.
12. List and describe the security challenges, which are threatening the cloud computing environment.
13. How Security is a major concern for cloud service providers as well as users? Explain the objectives of cloud information security.
14. **Explain** Web Service, resiliency, provisioning, asset management, high availability, and disaster recovery.
15. List and describe the security challenges, which are threatening the cloud computing environment.
16. What are the security issues which one should discuss with a cloud-computing vendor? Explain secure software development life cycle (SecSDLC).
17. **Write short notes on:**
    a. MapReduce and Cloud Governance
    b. High availability and Disaster recovery
    c. Cloud interoperability and analytics
18. **Explain**
    a. Security Architecture services across technology layers
    b. Grid Computing and Distributed Computing
    c. Uses of SOAP and REST for cloud-based application

❑❑❑