5 Cloud Security

5.1 Introduction to Security

- Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.
- The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.
- Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from leakage, theft, and data loss. Protection includes data from cloud infrastructure, applications, and threats. Security applications uses software the same as SaaS (Software as a Service) model.

❖ Why is cloud security important?

- For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

❖ Benefits of Cloud Security System

- **Centralized security:** Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with shadow IT or BYOD. Managing these entities centrally enhances traffic analysis and web filtering, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and auctioned easily when they are managed in one place.
- **Reduced costs:** One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.
- **Reduced Administration:** When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.
- **Reliability:** Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

5.2 Cloud security challenges

- Here are the major security challenges that companies using cloud infrastructure have to prepare for.
    - **Data breaches**
        - A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices. It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual

property. An organization's cloud-based data may have value to different parties for different reasons.

- **Access management**
  - Since cloud enables access to company's data from anywhere, companies need to make sure that not everyone has access to that data. This is done through various policies and guardrails that ensure only legitimate users have access to vital information, and bad actors are left out.
- **Data encryption**
  - Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.
- **Denial of service (DoS/DDoS attacks)**
  - Distributed denial-of-service attack (DDoS), like any denial-of-service attack (DoS), has as its final goal to stop the functioning of the targeted site so that no one can access it. The services of the targeted host connected to the internet are then stopped temporarily, or even indefinitely.
- **Advanced persistent threats (APTs)**
  - APTs are a parasitical form of cyber-attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them.

5.3 Cloud security risks and solutions

- Cloud computing is continually transforming the way companies store, use, and share data, workloads, and software. The volume of cloud utilization around the globe is increasing, leading to a greater mass of sensitive material that is potentially at risk.
- The market for worldwide cloud computing is projected to grow to $191 billion in two years. There are many pros of cloud computing, which are driving more firms and individuals to the cloud. The benefits include low costs, improved employee productivity, and faster to market, among many more.
- Regardless of the great advantages, saving a firm's workloads to a cloud service that is publicly hosted exposes the organization to new data security risks which cause unease for some firms' IT departments and clients. With more and more data and software moving to the cloud, unique info-security challenges crop up. Here are the top cloud computing security risks that every firm faces.

❖ Cloud security risks

- **Theft or loss of intellectual property**
  - An outstanding 21% of data uploaded by companies to cloud-based file management services contain sensitive data. The analysis that was done by Skyhigh found that companies face the risk of having their intellectual property stolen.
  - The Ponemon Institute and Surveying 409 IT investigated the risk posed by BYOC (bring your own cloud). The analysis revealed that most of the interviewees had no idea of the threat posed by bringing their own cloud storage devices to their organization. Employees unwittingly help cybercriminals access sensitive data stored in their cloud accounts. Weak cloud security measures within an organization include storing data without encryption or failing to install multi-factor authentication to gain access to the service.
- **Compliance violations**

  - Organizations can quickly go into a state of non-compliance, which puts them in the risk ofserious repercussions. BYOC is one of the ways companies often violate one of the tenets and regulations instituted by the government or Industrial Corporation. Whether it is FERPA for confidential student documents or HIPAA for private patient records, most firms operate under a regulatory body.
  - A state of non-compliance with any of these bodies lands companies in a lot of trouble. To mitigate this risk, companies should always use authentication systems for all the sensitive data in the firm. Even tech giants like Facebook have been victims of resource exploitation due to user error or misconfigurations. Keeping employees informed about the dangers and risks of data sharing is of at most importance.
- **Malware attacks**
  - Cloud services can be a vector for data exfiltration. As technology improves, and protection systems evolve, cyber-criminals have also come up with new techniques to deliver malware targets. Attackers encode sensitive data onto video files and upload them to YouTube. Skyhigh reports that cyber-criminals use private twitter accounts to deliver the malware. The malware then exhilarates sensitive data a few characters at a time. Some have also been known to use phishing attacks through file-sharing services to deliver the malware.
- **End-user control**
  - When a firm is unaware of the risk posed by workers using cloud services, the employees could be sharing just about anything without raising eyebrows. Insider threats have become common in the modern market. For instance, if a salesman is about to resign from one firm to join a competitor firm, they could upload customer contacts to cloud storage services and access them later.
  - The example above is only one of the more common insider threats today. Many more risks are involved with exposing private data to public servers.
- **Contract breaches with clients and/or business partners**
  - Contracts restrict how business partners or clients use data and also who has the authorization to access it. Employees put both the firm and themselves at risk of legal action when they move restricted data into their cloud accounts without permission from the relevant authorities. Violation of business contracts through breaching confidentiality agreements is common. This is especially when the cloud service maintains the right to share all data uploaded with third parties.
- **Shared vulnerabilities**
  - Cloud security is the responsibility of all concerned parties in a business agreement. From the service provider to the client and business partners, every stakeholder shares responsibility in securing data. Every client should be inclined to take precautionary measures to protect their sensitive data.
  - While the major providers have already taken steps to secure their side, the more delicate control measures are for the client to take care of. Dropbox, Microsoft, Box, and Google, among many others, have adopted standardized procedures to secure your data. These measures can only be successful when you have also taken steps to secure your sensitive data.
- Key security protocols such as protection of user passwords and access restrictions are the client's responsibility. According to an article named "Office 365 Security and Share Responsibility" by Skyfence, users should consider high measures of security as the most delicate part of securing their data is firmly in their hands.
- **Attacks to deny service to legitimate users**
  - You are most likely well aware of cyber-attacks and how they can be used to hijack information and establish a foothold on the service provider's platform. Denial of service attacks, unlike cyber-attacks, do not attempt to bypass your security protocol. Instead, they make your servers unavailable to illegitimate users.
  - However, in some cases, DoS is used as a smokescreen for a variety of other malicious activities. They can also be used to take down some security appliances like web application firewalls.
- **Insecure APIs**

- API or Application Programming Interfaces offer users the opportunity to customize their cloud service experience. APIs can, however, be a threat to cloud security due to their very nature. Apart from giving firms the ability to customize the features on their cloud service provider, they also provide access, authenticate, and effect encryption.
- As APIs evolve to provide better service to users, they also increase their security risk on thedata client's store. APIs provide programmers with the tools to integrate their programs with jobcritical applications. YouTube is one of the sites with an API that allows users to embed YouTube videos into their apps or websites.
- Despite of this great opportunity that the technology presents the user, it also increases the level of vulnerability to their data. Cyber-criminals have more opportunities to take advantage of thanks to these vulnerabilities

- **Loss of data**
  - Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider. Losing sensitive data is devastating to firms, especially if they have no recovery plan. Google is an example of the big tech firms that have suffered permanent data loss after being struck by lightning four times in its power supply lines.
  - Amazon was another firm that lost its essential customer data back in 2011.
  - An essential step in securing data is carefully reviewing the terms of service of your provider and their back up procedures. The backup protocol could relate to physical access, storage locations,and natural disasters.
- **Diminished customer trust**
  - It is inevitable for customers to feel unsafe after data breach concerns at your firm. There have been massive security breaches that resulted in the theft of millions of customer credit and debit card numbers from data storage facilities.
  - The breaches reduce customer trust in the security of their data. A breach in an organization's data will inevitably lead to a loss of customers, which ultimately impacts the firm's revenue.
- **Increased customer agitation**

  A growing number of cloud service critics are keen to see which service providers have weak security protocols and encourage customers to avoid them. Most of these critics are popular around the internet and could lead to a poor impression of your firm in a few posts. If your customers suspect that their data is not safe in your hands, they not only move to competitor firms but also damage your firm's reputation.
- **Revenue losses**
  - Customers of a store will avoid buying from the store in the wake of news of data breach in the organization. A well-known company as Target estimated a data breach in its platform to cost around $128 million. The CEO of the company resigned, and the company's directors remain under oversight by cyber security com

❖ Managing cloud security

➢ To effectively mitigate the security risks brought by unmanaged cloud usage, firms need to understand the data that is being uploaded to cloud servers and who is uploading the data. The cloud storage and sharing services are here to stay, and firms must be able to balance the risks posed by using the service. The following steps will aid business decision-makers and enterprise IT managers to analyze cloud security of company data.

1. **Ensure governance and compliance is effective**
   - A majority of companies have already established privacy and compliance policies to protect their assets. In addition to these rules, they should also create a framework of governance that establishes authority and a chain of responsibility in the organization. A well-defined set of policies clearly describes the responsibilities and roles of each employee. It should also define how they interact and pass information.

2. **Auditing and business procedures**
   - Every system in an organization requires a regular audit. In fact, it is of utmost importance that firms keep their IT systems in check in case of malware and phishing attacks. An IT system audit must also check the compliance of IT system vendors and data in the cloud servers. These are the three crucial areas that need to be frequently audited by cloud service customers:
     i. Security in the cloud service facility,
     ii. Access to the audit trail, and
     iii. the internal control environment of the cloud service provider.
3. **Manage identities, people and roles**
   - Employees from the cloud service provider will inevitably have access to your firm's applications and data. The employees at your organization that carry out operations on the provider's system will also have access to this data. A firm must ensure that the cloud service provider has sufficient policies to govern who has access to sensitive data and software. The cloud service provider must give the customer the privilege to manage and assign authorization for the users. They must also ensure their system is secure enough to handle different types of attacks on client data.
4. **Enforcing privacy policies**
   - Privacy and protection of personal and sensitive information are crucial to any organization's success. Personal data held by an organization could face bugs or security negligence. If a provider is not offering adequate security measures, the firm should consider seeking a different cloud service provider or not uploading sensitive information on the cloud.
5. **Assess security vulnerabilities for cloud applications**
   - Organizations have different types of data that they store in the cloud. Different considerations should be made according to the kind of data the firm intends to secure. Cloud application security poses diverse challenges to both the provider and the firm. Depending on the deployment model of the cloud service provider e.g., IaaS, SaaS, or PaaS, there are different considerations for both parties.
6. **Cloud networks security**
   - Audits of the cloud networks should be able to establish malicious traffic that can be detected and blocked. However, the cloud service providers have no way of knowing which network traffic its users plan to send or receive. Organizations must then work together with their service providers to establish safety measures.
7. **Evaluating physical infrastructure and security controls**
   - The security of the physical infrastructure of an IT system determines its vulnerability at the onset of a malicious attack. The provider must assure its users that appropriate measures are in place. Facilities and infrastructure should be stored in secure locations and backed up to protect against external threats. It is becoming more critical to maintain privacy and security with more data and software being migrated to the cloud. The IT groups must consider the cloud security risks and implement solutions to ensure the security of client data stored and processed in the cloud.

5.4 What is SaaS Security?

- SaaS Security refers to securing user privacy and corporate data in subscription-based cloud applications. SaaS applications carry a large amount of sensitive data and can be accessed from almost any device by a mass of users, thus posing a risk to privacy and sensitive information.

❖ Software-as-a-service (SaaS) security issues

- Cloud computing models of the future will likely combine the use of SaaS (and other as a service as appropriate), utility computing, and Web 2.0 collaboration technologies to leverage the Internet to satisfy their customers' needs. New business models being developed as a result of the move to cloud computing are creating not only new technologies and business operational processes but also new security requirements and challenges as described previously. SaaS will likely remain the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside. Just as with a managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. Security issues which one should discuss 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?
- To address the security issues listed above along with others mentioned earlier in the topic, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.
- The baseline security practices for the SaaS environment as currently formulated are discussed in the following sections:
  - **Security Management:** Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals.Morale among the team and pride in the team is lowered, and security suffers as a result.
  - **Risk Management:** Effective risk management: entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of informationassets. Owners have authority and accountability for information assets including protectionrequirements, and custodians implement confidentiality, integrity, availability, and privacy controls. A formal risk assessment process should be created that allocates security resourceslinked to business continuity.
  - **Risk/ Vulnerability Assessmen**: Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals, and can lead to inefficient and ineffective selection of security controls that may not adequately mitigate

information security risks to an acceptable level. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis.

5.5 Security Monitoring and Incident Response

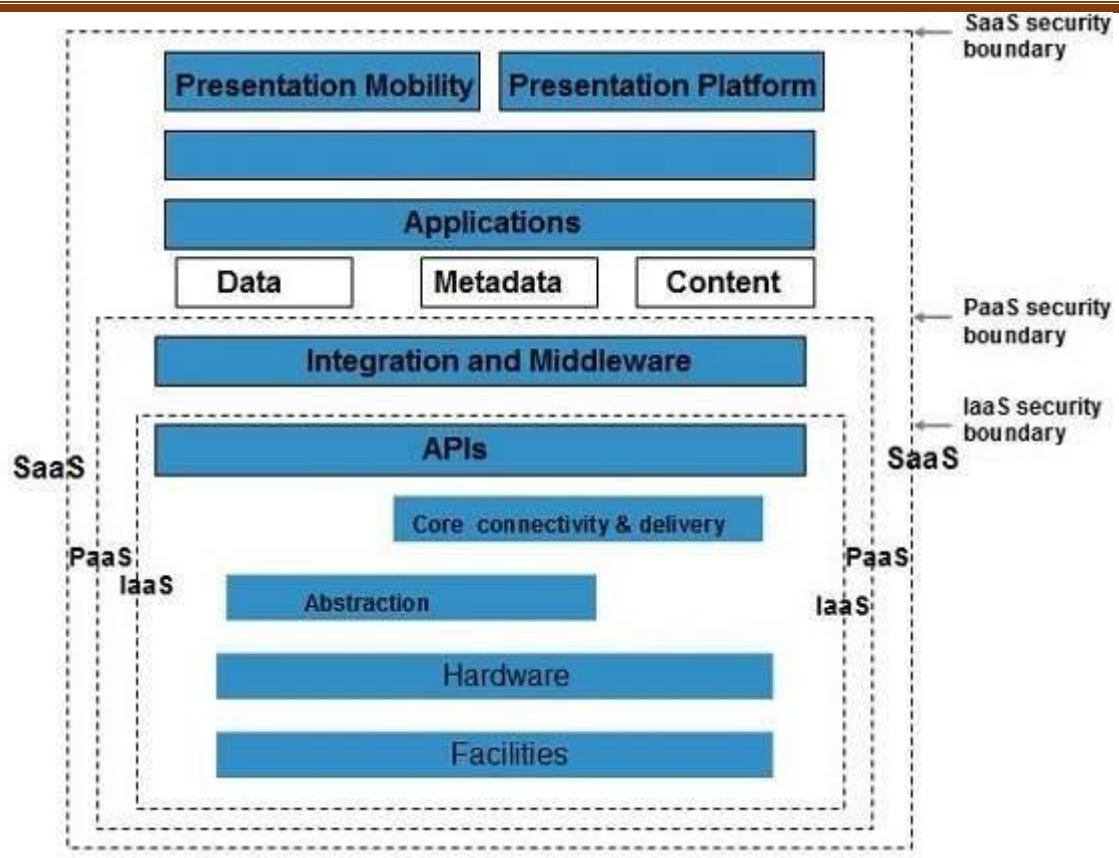
- Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring).
- Management of periodic, independent third-party security testing should also be included. Many of the security threats and issues in SaaS center around application and data layers, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and datalevel activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threat and attacks to its customer data and service stability.
- Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. An organization's incident response is conducted by the computer incident response team, a carefully selected group that, in addition to security and general IT staff, may include representatives from legal, human resources, and public relations departments.

5.6 Security Architecture Design

- Security Architecture is one component of a products/systems overall architecture and is developed to provide guidance during the design of the product/system.
- A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, nonrepudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.
- A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance.
- The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

❖ Security Boundaries

- A particular service model defines the boundary between the responsibilities of service provider and customer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the CSA stack model:



❖ **Key Points to CSA Model**

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
- Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

5.7 Vulnerability Assessment

- Vulnerability assessment classifies network assets to more efficiently prioritize vulnerabilitymitigation programs, such as patching and system upgrading. It measures the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and faster mitigation.
- Vulnerability management should be integrated with discovery, patch management, and upgrade management processes to close vulnerabilities before they can be exploited.
- A vulnerability assessment attempts to identify the exposed vulnerabilities of a specific host, or possibly an entire network. The vulnerabilities may be due to configuration problems or missing software patches.
- Vulnerability Assessment in cloud should be done in periodic basis with predefined service level agreement. Customers should be allowed to test cloud infrastructure before and after they outsource their infrastructure to cloud.

5.8 Data Privacy and Security

- Cloud computing has transformed the way organizations approach IT, enabling them to become more agile, introduce new business models, provide more services, and reduce IT costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches.
- Maintaining control over the data is paramount to cloud success. A decade ago, enterprise data typically resided in the organization's physical infrastructure, on its own servers in the enterprise's data center, where one could segregate sensitive data in individual physical servers.
- Today, with virtualization and the cloud, data may be under the organization's logical control, but physically reside in infrastructure owned and managed by another entity. This shift in control is the number one reason new approaches and techniques are required to ensure organizations can maintain data security. When an outside party owns, controls, and manages infrastructure and computational resources, how can you be assured that business or regulatory data remains private and secure, and that your organization is protected from damaging data breaches—and feel you can still completely satisfy the full range of reporting, compliance, and regulatory requirements?
- Some of the points to keep data private and secure in cloud infrastructure are as below:
    - Avoid storing sensitive information in the cloud.
    - Read the user agreement to find out how your cloud service storage works.
    - Password sensitivity
    - Encrypt your data
    - Use Encrypted cloud services

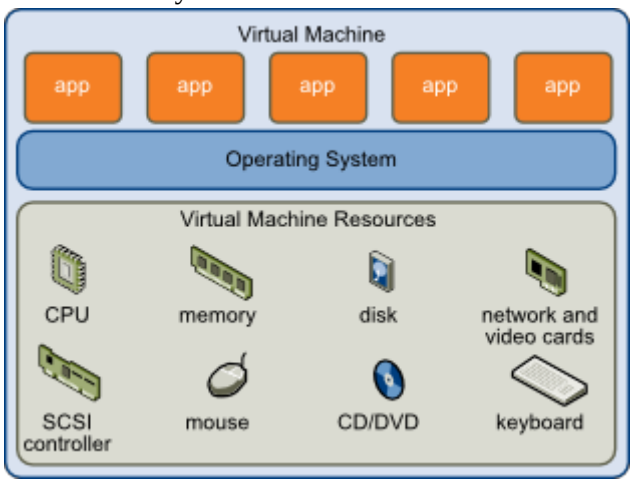
5.9 Application Security

- Application security is one of the critical success factors for SaaS company. This is where the security features and requirements are defined and application security test results are reviewed.
- Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development team.
- Although product engineers will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement.
- This should be a collaborative effort between the security and product development team.
- External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly. Fragmented and undefined collaboration on application security can result in lower-quality design, coding efforts, and testing results.
- Some of the things that we should consider while moving to cloud application are:
    - Risks associated with cloud application
    - The fact that someone is managing and controlling your critical application
    - The perimeter of cloud is different and multitenant
    - Application should be protected with industry standard firewall and security products e.
    - Insecure Interfaces and Application Program Interface (API's)
    - Denial of Service (DOS) attack

5.10 Virtual Machine Security

- Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

- Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it,



❖ **Virtual Machine Isolation**

- In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.
- Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.
- By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely. To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include abbidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from onpremises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.
- A further area of concern with virtualization has to do with the potential for undetected network attacks between VMs collocated on a physical server. Unless you can monitor the traffic from each VM, you can't verify that traffic isn't possible between those VMs.
- In essence, network virtualization must deliver an appropriate network interface to the VM. That interface might be a multiplexed channel with all the switching and routing handled in the network interconnect hardware.

5.11 Disaster Recovery

- A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function.
- The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate - even possibly at a minimal level.
- A disaster recovery plan (DRP) documents policies, procedures and actions to limit the disruption to an organization in the wake of a disaster. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of actions intended to minimize the negative effects of a disaster and allow the organization to maintain or quickly resume mission-critical functions.
- To better understand and evaluate disaster recovery strategies, it is important to define two terms: **recovery time objective (RTO)** and **recovery point objective (RPO)**.

- **RTO**
  - The recovery time objective (RTO) is the maximum amount of time allocated for restoring application functionality. This is based on business requirements and is related to the importance of the application. Critical business applications require a low RTO.

- **RPO**
  - The recovery point objective (RPO) is the acceptable time window of lost data due to the recovery process. For example, if the RPO is one hour, you must completely back up or replicate the data at least every hour. Once you bring up the application in an alternate datacenter, the backup data may be missing up to an hour of data. Like RTO, critical applications target a much smaller RPO.
- **Some of the points why Disaster Recovery is needed?**
  - Machines, hardware and even data centers fail.
  - Much like machines, humans are not perfect. They make mistakes. In case of mistakes, DR may help resume business from back date.
  - Customers expect perfection as they don't want disruption in services
  - DR enabled organizations will attract more customers.

❖ **Disaster Recovery Management/ Planning Steps**

- Count the costs. Although data center downtime is harmful to any company that relies on its IT services, it costs some companies more than others. Your disaster recovery plan should enable a fast return to service, but it shouldn't cost you more than you are losing in downtime costs.
- Evaluate the types of threats you face and how extensively they can affect your facility. Malicious attacks can occur anywhere, but you may also face threats peculiar to your location, such as weather events (tornadoes, hurricanes, floods and so on), earthquakes or other dangers. Part of preparing for a disaster is to know what is likely to occur and how those threats could affect your systems. Evaluating these situations beforehand allows you to better take appropriate action should one of these events occur.
- Know what you have and how critical it is to operations. Responding to a disaster in your data center is similar to doing so in medicine: you need to treat the more serious problems first, then the more minor ones. By determining which systems are most critical to your data center, you enable your IT staff to prioritize and make the best use of the precious minutes and hours immediately following an outage. Not every system need be functional immediately following a disaster.
- Identify critical personnel and gather their contact information. Who do you most want to be present in the data center following an outage? Who has the most expertise in a given area and the greatest ability to oversee some part of the recovery effort? Being able to get in touch with these people is crucial to a fast recovery. Collect their contact information and, just as importantly, keep it up to date. If it's been a year or more since you last checked, some of that contact information is likely out of date. Every minute you spend trying to find important personnel is time not spent on recovery.
- Train your employees. Knowledge of how to implement disaster recovery procedures is obviously important when an outage occurs. To this end, prepare by training personnel and not just in their respective areas of expertise. Everyone should have some broad- based knowledge of the recovery process so that it can be at least started even if not everyone is present.
- Ensure that everyone knows the disaster recovery plan and understands his or her role. Announcing the plan and assigning roles is not something you should do after a disaster strikes; it should be done well in advance, leaving time for personnel to learn their roles and to practice them. Almost nothing about a disaster event should be new (aside from some contingencies of the moment, perhaps): the IT staff should implement disaster recovery as a periodic task (almost) like any other.
- Practice. Needless to say, this is perhaps the most critical part of preparation for a downtime event. The difference between knowing your role and being able to execute it well is simply practice. You may not be able to shut down your data center to simulate precisely all of the conditions you will face in an outage, but you can go through many of the procedures nevertheless. Some recommendations prescribe semiannual drills,

at a minimum, to practice implementing the disaster recovery plan. If there's one thing you take from this article, it's that you should practice your disaster recovery plan—don't expect it to unfold smoothly when you need it (regardless of how well laid-out a plan it is) if you haven't given it a trial run or two.

- Automate where possible. Your staff is limited, so it can only do so much. The more that your systems can do on their own in a recovery situation, the faster the recovery will generally be. This also leaves less room for human error—particularly in the kind of stressful atmosphere that exists following a disaster.
- Follow up after a disaster. When a downtime event does occur, evaluate the performance of the personnel and the plan to determine if any improvements can be made. Update your plan accordingly to enable a better response in the future.
- Furthermore, investigate the cause of the outage. If it's an internal problem, take necessary measures to correct equipment issues to avoid the same problem occurring again.

5.12 Identity and Access management (IAM)

- Identity and access management (IAM or IdAM for short) is a way to tell who a user is and what they are allowed to do. IAM is like the bouncer at the door of a nightclub with a list of who is allowed in, who isn't allowed in, and who is able to access the VIP area. IAM is also called identity management (IdM).

- In more technical terms, IAM is a means of managing a given set of users' digital identities, and the privileges associated with each identity. It is an umbrella term that covers a number of different products that all do this same basic function. Within an organization, IAM may be a single product, or it may be a combination of processes, software products, cloud services, and hardware that give administrators visibility and control over the organizational data that individual users can access.

❖ What is identity in the context of computing?

- A person's entire identity cannot be uploaded and stored in a computer, so "identity" in a computing context means a certain set of properties that can be conveniently measured and recorded digitally.
- Think of an ID card or a passport: not every fact about a person is recorded in an ID card, but it contains enough personal characteristics that a person's identity can quickly be matched to the ID card.
- To verify identity, a computer system will assess a user for characteristics that are specific to them. If they match, the user's identity is confirmed. These characteristics are also known as "authentication factors," because they help authenticate that a user is who they say they are.
- The three most widely used authentication factors are:
  - Something the user knows
  - Something the user has
  - Something the user is

- **Something the user knows:** This factor is a piece of knowledge that only one user should have, like a username and password combination. Imagine that John wants to check his work email from home. To do so, he will first have to log into his email account by establishing his identity, because if somebody who wasn't John accessed John's email, then company data would be compromised.
  John logs in by entering his email, john@company.com, and the password that only he knows –for example, "5jt*2)f12?y". Presumably, no one else besides John knows this password, so the email system recognizes

John and lets him access his email account. If someone else tried to impersonate John by entering their email address as "john@company.com," they wouldn't be successful without knowing to type "5jt*2)f12?y" as the password.

- **Something the user has:** This factor refers to possession of a physical token that is issued to authorized users. The most basic example of this authentication factor is the use of a physical house key to enter one's home. The assumption is that only someone who owns, rents, or otherwise is allowed into the house will have a key. In a computing context, the physical object could be a key fob, a USB device, or even a smartphone. Suppose that John's organization wanted to be extra sure that all users really were who they said they were by checking two authentication factors instead of one. Now, instead of just entering his secret password – the something the user knows factor – John has to show the email system that he possesses an object that no one else has. John is the only person in the world who possesses his personal smartphone, so the email system texts him a one-time code, and John types in the code to demonstrate his possession of the phone.
- **Something the user is:** This refers to a physical property of one's body. A common example of this authentication factor in action is Face ID, the feature offered by many modern smartphones. Fingerprint scanning is another example. Less common methods used by some high-security organizations include retina scans and blood tests. Imagine John's organization decides to tighten security even more by making users verify three factors instead of two (this is rare). Now John has to enter his password, verify possession of his smartphone, and scan his fingerprint before the email system confirms that he really is John. To summarize: In the real world, one's identity is a complex mix of personal characteristics, history, location, and other factors. In the digital world, a user's identity is made up of some or all of the three authentication factors, stored digitally in an identity database. To prevent impostors from impersonating real users, computer systems will check a user's identity against the identity database.

❖ **What is access management?**

- "Access" refers to what data a user can see and what actions they can perform once they log in. Once John logs into his email, he can see all the emails he has sent and received. However, he should not be able to see the emails sent and received by Tracy, his coworker.
- In other words, just because a user's identity is verified, that doesn't mean they should be able to access whatever they want within a system or a network. For instance, a low-level employee within a company should be able to access their corporate email account, but they should not be able to access payroll records or confidential HR information.
- Access management is the process of controlling and tracking access. Each user within a system will have different privileges within that system based on their individual needs. An accountant does indeed need to access and edit payroll records, so once they verify their identity, they should be able to view and update those records as well as access their email account.