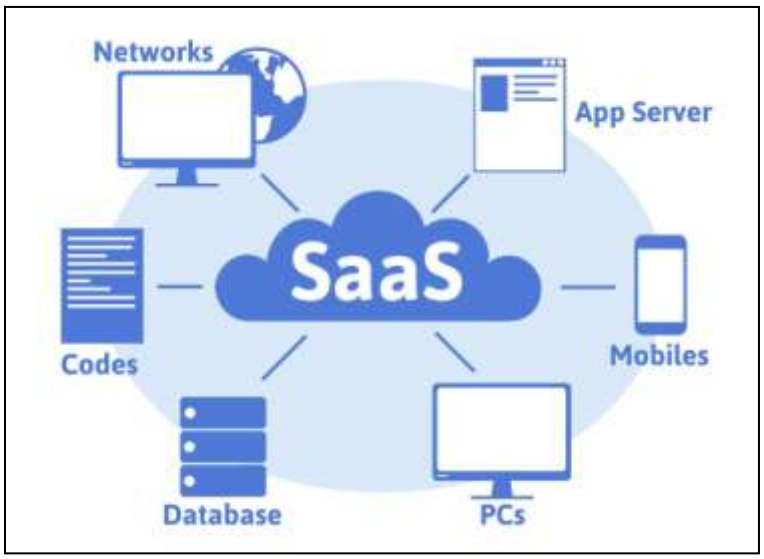
AIM : Study Software as a Service and Cloud Security

THEORY :

1. Prepare a detailed study of Software as a Service.

Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software", and was formerly referred to as "software plus services" by Microsoft. SaaS applications are also known as on-demand software and Web-based/Web-hosted software.

SaaS is considered to be part of cloud computing, along with infrastructure as a service (IaaS), platform as a service (PaaS), desktop as a service (DaaS), managed software as a service (Dancing Numbers)(MSaaS), mobile backend as a service (MBaaS), datacenter as a service (DCaaS), and information technology management as a service (ITMaaS).



Features:

- Multi-tenancy Model : Multi-tenancy is a kind of software architecture in which a single deployment of a software application serves multiple customers.
- Automated Provisioning : The users should be able to access the SaaS applications on the fly, which means the process of provisioning the users with the services needs to be automated. SaaS applications are typically used by B2B/B2C customers and this requirement demands creating companies/users just by invoking web services and provide the access credentials.
- Single Sign On :An enterprise organization would want to have a single identity system in place in order to authenticate the various systems which are going to be consumed by users.

- Subscription-based Billing : SaaS applications pricing do not involve the complexity of license cost & upgrade cost etc. Generally, the Software as a Service applications are subscription based, and this enables customers to buy the SaaS applications whenever they require them and discontinue whenever the enterprise decides that they are not needed any more.
- High Availability : SaaS applications are shared by multiple tenants and the availability of kind of applications are expected to be really high throughout. Applications should be accessible 24x7 across globe. Also SaaS applications should expose management & monitoring API to continuously check the health/availability factor.
- Elastic Infrastructure : SaaS applications usage is generally not predictable, consumption can dramatically vary in some months. The infrastructure on the applications deployed should really have an ability to expand/shrink the resources used behind the show.
- Data Security : Ensuring that the data/business information is protected from corruption and unauthorized access is very important in today's world. Since the Software as a Service applications are designed to be shared by different tenants, it becomes extremely important to know how well the data is secured. So, having a good Key Management Framework or ability to integrate/interface with external Key Management Frameworks becomes essential part of SaaS applications.
- Application Security : SaaS applications should be equipped with protection against vulnerabilities.
- Rate Limiting/QoS : These days, in order to provide better service to all class of customers, rate limiting is a good feature to have. The number of hits/ number of transaction can be technically limited to ensure the smooth business transactions.

2. Advantages and Limitation of SaaS.

Advantages :

1. Lower up-front cost - SaaS is generally subscription-based and has no up-front licence fees resulting in lower initial costs. The SaaS provider manages the IT infrastructure that is running the software, which brings down fees for hardware and software maintenance.
2. Quick set up and deployment
3. Easy upgrades - The SaaS providers deal with hardware and software updates, deploying upgrades centrally to the hosted applications and removing this workload and responsibility from you.
4. Accessibility - All you need to access a SaaS application is a browser and an internet connection.
5. Scalability - SaaS providers generally offer many subscription options and flexibility to change subscriptions as and when needed, eg when your business grows, or more users need to access the service.

Limitations :

1. Lack of control - in-house software application gives businesses a higher degree of control than hosted solutions where control resides with a third party. Typically everyone has to use the latest version of the software application and cannot defer upgrades or changes in the features.
2. Security and data concerns - access management and the privacy of sensitive information is a major consideration around cloud and hosted services.
3. Limited range of applications - while SaaS is becoming more popular, there are still many applications that don't offer a hosted platform.
4. Connectivity requirement - since the SaaS model is based on web delivery, if your internet service fails, you will lose access to your software or data
5. Performance - SaaS may run at somewhat slower speeds than on-premise client or server applications, so it's worth keeping performance in mind your software isn't hosted on a local machine.

3. Study security issues in cloud computing.

- Misconfiguration : Misconfigurations of cloud security settings are a leading cause of cloud data breaches.
- Unauthorized Access : Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization's knowledge.
- Insecure Interfaces/APIs : CSPs often provide a number of application programming interfaces (APIs) and interfaces for their customers. In general, these interfaces are well-documented in an attempt to make them easily-usable for a CSP's customers.
- Hijacking of Accounts : Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts.
- Cyberattacks : Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data.
- Denial of Service Attacks : The cloud is essential to many organizations' ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications.
- Lack of Visibility : An organization's cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own. As a result, many traditional tools for achieving network visibility are not effective for cloud

environments, and some organizations lack cloud-focused security tools. This can limit an organization's ability to monitor their cloud-based resources and protect them against attack.

- Data Loss/Leakage : Cloud-based environments make it easy to share the data stored within them. These environments are accessible directly from the public Internet and include the ability to share data easily with other parties via direct email invitations or by sharing a public link to the data.
- Data Privacy/Confidentiality
- Accidental Exposure of Credentials
- Malicious Insiders

4. Explain Server and Data Security in cloud computing.

Servers are powerful computers that provide one or more services (such as email, web or file servers) to users on a particular network. Cyber criminals frequently target servers because of the nature of sensitive data they often hold.

Server and data security focuses on the protection of data and resources held on the servers. It comprises tools and techniques that help prevent intrusions, hacking and other malicious actions.

Server security measures vary and are typically implemented in layers. They cover:

- The base operating system - focusing on security of critical components and services.
- Hosted applications - controlling the content and services hosted on the server.
- Network security - protecting against online exploits, viruses and attacks.

Data security in cloud computing is the practice of securing a company's data in a cloud environment, wherever that data is located, whether it's at rest or in motion, and whether it's managed internally by the company or externally by a third party.

To successfully protect and secure their data in cloud environments, companies must first know:

- Which data they have and where it's located.
- Which data is exposed, how it's exposed, and potential risks.
- Which applications are being accessed and by whom.
- What's happening inside their applications (e.g., how people are accessing and using them).
- Which data they need to protect and at what level.

Some ways for server and data security:
1. Network firewall security :A firewall is a piece of software or hardware that filters all incoming and outgoing traffic to your business. Firewall devices can:

- Block malicious email relaying
- Prevent malware being downloaded from untrusted websites
- Prevent access to blacklisted websites or unsecure services

1. Hardware firewall is a part of broadband routers. It protects your entire local network from unauthorised external access and is usually effective even with minimal configuration.
2. Software firewall is an application installed on individual computers and devices. It is often part of the operating system and usually needs greater configuration of settings and applications controls.

2. Server hardening : Regardless of what server software and operating system you run, their default configuration may not be fully secure. You should take steps to increase server security - this process is known as server hardening.

Some common server hardening methods include:

- Using data encryption for communication
- Removing unnecessary software from servers
- Regularly updating operating systems, and applying security patches
- Using security extensions
- Enforcing strong password complexity to protect all user accounts
- Account locking after repeated login failures
- Using brute force and intrusion detection systems
- Backing up data and systems regularly

Activity :

With the help of any suitable cloud service explain SaaS. Use owncloud to explain the security of the webserver and data directory.

OwnCloud acts as a software for storage as a service wherein we can run the service on a server and access it through its public IP address. But here we need to address some security concerns.

OwnCloud specifically runs on LAMP(Linux Apache Mysql PHP) service where Mysql is the database, Linux is the operating system, Apache and PHP manage the webserver.

OwnCloud specific data directory is "`/var/www/owncloud/data`". This directory is used for the webserver to work properly.

Some Security Issues:

- Database Password
- Data in data directory
- Server firewall protection

OwnCloud provides Hardening and security guidance for giving proper security on cloud which are as follows:

- Limit on Password Length : ownCloud uses the bcrypt algorithm, and thus for security and performance reasons, e.g. Denial of Service as CPU demand increases exponentially, it only verifies the first 72 characters of passwords. This applies to all passwords that you use in ownCloud: user passwords, passwords on link shares, and passwords on external shares.
- Give PHP read access to /dev/urandom : ownCloud uses a RFC 4086 ("Randomness Requirements for Security") compliant mixer to generate cryptographically secure pseudo-random numbers. This means that when generating a random number ownCloud will request multiple random numbers from different sources and derive from these the final random number
  Thus it is highly recommended to configure your setup in such a way that PHP is able to read random data from /dev/urandom
- Enable hardening modules such as SELinux : Security-Enhanced Linux (SELinux) is a security architecture for Linux® systems that allows administrators to have more control over who can access the system. It was originally developed by the United States National Security Agency (NSA) as a series of patches to the Linux kernel using Linux Security Modules (LSM). Hence it can be helpful
- Place data directory outside of the web root : It is highly recommended to place your data directory outside of the Web root (i.e. outside of /var/www). It is easiest to do this on a new installation.
- Use a dedicated domain for ownCloud : Administrators are encouraged to install ownCloud on a dedicated domain such as cloud.domain.tld instead of domain.tld to gain all the benefits offered by the Same-Origin-Policy.
- Proper SSL configuration : Default SSL configurations by Web servers are often not state-of-the-art, and require fine-tuning for an optimal performance and security experience. The available SSL ciphers and options depend completely on your environment and thus giving a generic recommendation is not really possible.
  They recommend using the Mozilla SSL Configuration Generator to generate a suitable configuration suited for your environment, and the free Qualys SSL Labs Tests gives good guidance on whether your SSL server is correctly configured.
  Also it should be ensured that HTTP compression is disabled to mitigate the BREACH attack.

CONCLUSION :

- From this experiment we understood Software as a service and cloud security where we saw what is SaaS, its advantages and disadvantage and also so issues in cloud security.
- SaaS is required because it can provide notable savings in cost since it uses pay-as-you-go basis models, it saves time since installations are as simple as connecting to internet and logging in to the software.
- SaaS is important because it can also provide great scalability and accessibility since the software is hosted externally by a vendor, changing your usage plan is easy and can be done without advance notice.
- Cloud computing security is important because with cloud storage your data is backed up to the cloud rather than stored on-site or nearby.
- Organizations have ignored or lack knowledge of the emerging cloud security threats. As the Cloud evolves and transforms into sophisticated infrastructure and technology, so is the cloud security threats. Hackers are becoming more aggressive with honed techniques to take advantage of any slight breach to steal data.
- Hence cloud security measures have to be taken to protect the servers and the data of each organization.

REFERENCES :

1. https://en.wikipedia.org/wiki/Software_as_a_service

2. https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-software-service-saas

3. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

4. https://www.nibusinessinfo.co.uk/content/server-security#:~:text=What%20is%20server%20security%3F,are%20typically%20implemented%20in%20layers.

5. https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection#:~:text=Cloud%20data%20protection%20is%20the,externally%20by%20a%20third%20party.

6. https://technologyadvice.com/blog/information-technology/advantages-of-software-as-a-service-saas-2/#:~:text=SaaS%20can%20provide%20notable%20savings,be%20easily%20downloaded%20and%20maintained.

7. https://www.probrand.co.uk/it-services/cloud-computing-security