RGPVNOTES.IN

Please do not share these notes on apps like WhatsApp or Telegram.

The revenue we generate from the ads we show on our website and app funds our services. The generated revenue **helps us prepare new notes and improve the quality of existing study materials**, which are available on our website and mobile app.

If you don't use our website and app directly, it will hurt our revenue, and we might not be able to run the services and **have to close them**. So, it is a humble request for all to **stop sharing the study material** we provide on various apps. Please **share the website's URL instead.**

CS-802 (B) Cloud Computing
Subject Notes

Unit - 4 **CO4**

Cloud security fundamentals, Vulnerability assessment tool for cloud, Privacy, and Security in cloud: Cloud computing security architecture, General Issues, Trusted Cloud computing, Security challenges: Virtualization security management-virtual threats, VM Security Recommendations, VM-Specific Security techniques, Secure Execution Environments and Communications in the cloud.

CLOUD SECURITY FUNDAMENTALS

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 customer's privacy as well as setting authentication rules for individual users and devices.

Protection measures:

- No single person should accumulate all these privileges.
- A provider should deploy stringent security devices, restricted access control policies, and surveillance mechanisms to protect the physical integrity of the hardware.
- By enforcing security processes, the provider itself can prevent attacks that require physical access to the machines.
- The only way a system administrator would be able to gain physical access to a node running a customer's VM is by diverting this VM to a machine under his/her control, located outside the IaaS's security perimeter.
- The cloud computing platform must be able to confine the VM execution inside the perimeter and guarantee that at any point a system administrator with root privileges remotely logged to a machine hosting a VM cannot access its memory.
- TCG (trusted computing group), a consortium of an industry leader to identify and implement security measures at the infrastructure level proposes a set of hardware and software technologies to enable the construction of trusted platforms suggests the use of "remote attestation" (a mechanism to detect changes to the user's computers by authorized parties).

VULNERABILITY ASSESSMENT TOOL FOR CLOUD

- **Qualys** makes public cloud deployments are secure and compliant. Quays' continuous security platform enables customers to easily detect and identify vulnerable systems and apps, helping them better face the challenges of growing cloud workloads.
- **Proof point** focuses specifically on email, with cloud-only services tailored to both enterprises and small to medium-sized businesses. Not only does it make sure none of the bad stuff gets in, but it also protects any outgoing data.
- **Zscaler** calls its product the "Direct to Cloud Network" and like many of these products, boasts that it's much easier to deploy and can be much more cost-efficient than traditional appliance security.
- **Cipher Cloud** is here to secure all those other "as a service" products used, such as Salesforce, Chatter, Box, Office 365, Gmail, Amazon Web Services, and more.
- **Centrify** aims at identity management across several applications and devices. The main goal is to make users, employers, and customer's look-alike as a central area to be viewed and accessed through company

policies. It gives an alarm when a person tries to sign in from on premise cloud software or cloud applications.

PRIVACY AND SECURITY IN CLOUD

Privacy in cloud:

- One of the main concerns regarding the security and privacy in cloud computing is the protection of data. Millions of users have stored up their important data on these clouds, which is what makes it riskier to secure each and every bit of information.
- In cloud computing, data security has become a serious issue different data is distributed in different storage devices and machines including PCs, servers and different mobile devices such as smart phones and wireless sensor networks.
- If the security and privacy in cloud computing is neglected, then the private information of each user is at risk, allowing easy cyber breaches to hack into the system and exploit any users' private storage data.
- Security and privacy in cloud computing needs to take action if users are to trust the system again.

Security in cloud:

- The cloud computing environment has various functions— some of the major ones involve data storage and computing.
- The data protection and its security regarding stored information of individual users, therefore many consumers use the cloud so much and that is exactly why it has prospered through its use of trustful functions.
- The cloud has become a very important tool for large scale purposes, such as for business and companies to prosper and on the lower scales where it is used by almost every individual as a necessary part of their everyday life.
- It makes sense why a lot of people are fond of using it and are willing to trust the cloud system with their valuable information. But a data breach may break this trust. Therefore, it is extremely crucial that the security and privacy in cloud computing must create a solid line of defense against these cyber-attacks.

CLOUD COMPUTING SECURITY ARCHITECTURE

Cloud security starts with cloud security architecture. An organization should first understand its current cloud security posture, and then plan the controls and cloud security solutions it will use to prevent and mitigate threats.

This planning is critical to secure hyper-complex environments, which may include multiple public clouds, SaaS and PaaS services, on premise resources, all of which are accessed from both corporate and unsecured personal devices.

The cloud security architecture model is usually expressed in terms of:

- **Security controls:** It includes technologies and processes. Controls should take into account the location of each Service Company, cloud provider, or third party.
- **Trust boundaries:** The different services and components deployed on the cloud
- **Standard interfaces and security protocols:** Such as SSL, IPsec, SFTP, LDAPS, SSH, SCP, SAML, OAuth, etc.)
- **Techniques used for token management:** Authentication and authorization
- **Encryption methods:** Including algorithms like 128-bit AES, Triple DES, RSA, and Blowfish.
- **Security event logging:** Ensuring all relevant security events are captured, prioritized, and delivered to security teams.

The security services consumed by the cloud application:

- Logical location: Protocol
- Service function: Input/output
- Control description
- Actor

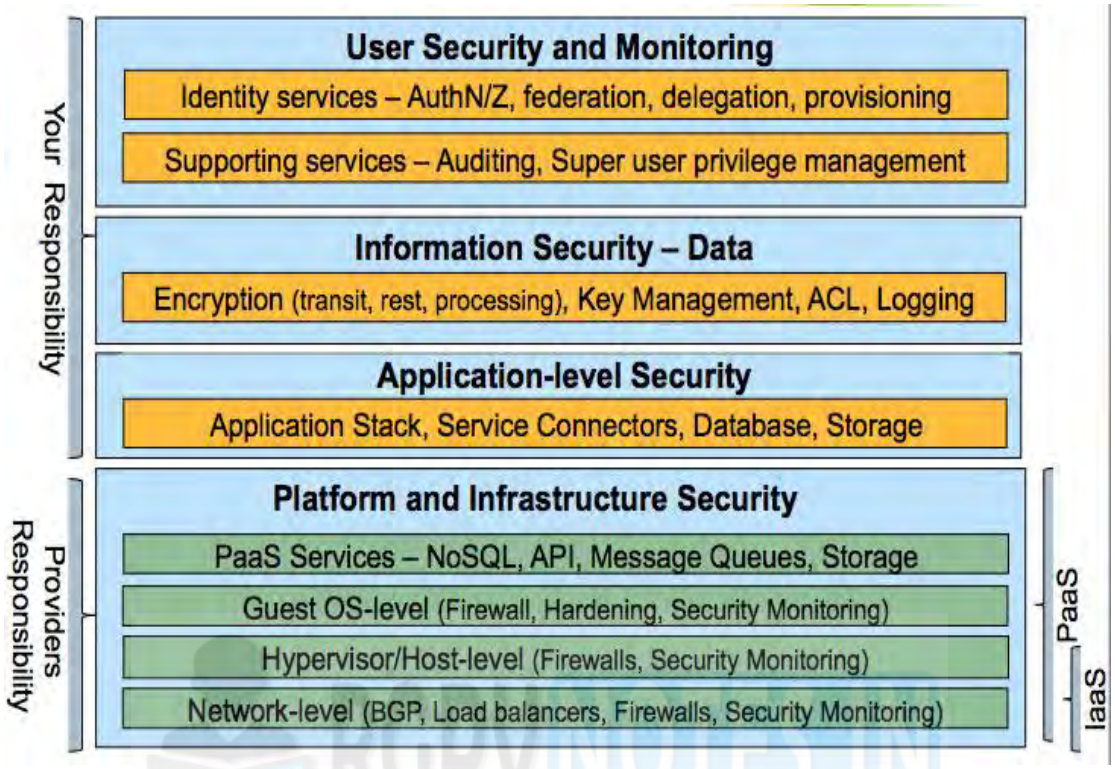

Figure 4.1: Cloud Security Architecture

ARCHITECTURAL CONSIDERATIONS- GENERAL ISSUES

The following table illustrates the dependencies which should be taken into consideration when architecting security controls into applications for cloud deployments:

	Public/Hybrid Cloud –Threats	Private Cloud -Threats	Mitigation
IaaS	• OWASP Top 10 • Data leakage(inadequate ACL) • Privilege escalation via management console mis-configuration • Exploiting VM weakness • DoS attack via API • Weak protection of privileged keys • VM Isolation failure	• OWASP Top 10 • Data theft (insiders) • Privilege escalation via management console mis-configuration	• Testing apps and API for OWASP Top 10 vulnerabilities • Hardening of VM image • Security controls including encryption, multi-factor authentication, fine granular authorization, logging • Security automation-Automatic provisioning of firewall policies, privileged accounts, DNS, application identity
PaaS	• Privilege escalation via API • Authorization weakness in platform services such as Message Queue, NoSQL, Blob services • Vulnerabilities in the run time engine resulting in tenant isolation failure	• Privilege escalation via API	

Table 4.1: Architectural dependencies

TRUSTED CLOUD COMPUTING

Trusted computing is a broad term that refers to technologies and proposals for resolving computer security problems through hardware enhancements and associated software modifications. Several major hardware manufacturers and software vendors, collectively known as the Trusted Computing Group (TCG), are cooperating in this venture and have come up with specific plans.

The TCG develops and promotes specifications for the protection of computer resources from threats posed by malicious entities without infringing on the rights of end-users. Microsoft defines trusted computing by breaking it down into four technologies, all of which require the use of new or improved hardware at the personal computer (PC) level:

- Memory curtaining -- prevents programs from inappropriately reading from or writing to each other's memory.
- Secure input/output (I/O) -- addresses threats from spyware such as key loggers and programs that capture the contents of a display.
- Sealed storage -- allows computers to securely store encryption keys and other critical data.
- Remote attestation -- detects unauthorized changes to software by generating encrypted certificates for all applications on a PC.

To be effective, these measures must be supported by advances and refinements in the software and operating systems (OSs) that PCs use.

The trusted computing base (TCB) encompasses everything in a computing system that provides a secure environment. This includes the OS and its standard security mechanisms, computer hardware, physical locations, network resources, and prescribed procedures.

The term trusted PC refers to the industry ideal of a PC with built-in security mechanisms that place minimal reliance on the end-user to keep the machine and its peripheral devices secure. The intent is that, once effective mechanisms are built into the hardware, computer security will be less dependent on the vigilance of individual users and network administrators than it has historically been.

CLOUD COMPUTING SECURITY CHALLENGES

- **DDOS and DDoS attacks:** A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests.
  If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.
- **Data breaches:** Data breaches can be the main goal of an attack through which sensitive information such as health, financial, personal identity, intellectual, and other related information is viewed, stolen, or used by an unauthorized user.
- **System vulnerability:** Security breaches may occur due to exploitable bugs in programs that stay within a system. This allows a bad actor to infiltrate and get access to sensitive information or crash the service operations.
- **Account or service hijacking using stolen passwords:** Account or service hijacking can be done to gain access and abuse highly privileged accounts. Attack methods like fraud, phishing, and exploitation of software vulnerability are carried out mostly using the stolen passwords.
- **Data loss:** The data loss threat occurs in the cloud due to interaction with risks within the cloud or architectural characteristics of the cloud application. Unauthorized parties may access data to delete or alter records of an organization.
- **Shared technology vulnerabilities:** Cloud providers deliver their services by sharing applications, or

infrastructure. Sometimes, the components that make up the infrastructure for cloud technology-as-a-service offers are not designed to offer strong isolation properties for a multi-tenant cloud service.

Risks to Cloud Environments:

- **Isolation failure:** Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing, and reputation between different tenants.
  It should be considered that attacks on resource isolation mechanisms are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.
- **Management interface compromise:** Customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
- **Data protection:** Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled lawfully.
- **Malicious insider:** while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

Overcoming Challenges in Cloud Computing:

1. **Security and Privacy:** Security is arguably the biggest challenge in cloud computing. Cloud security refers to a set of technologies or policies to protect data. Remember, violating privacy can cause havoc to end-users.
- Implementing security applications, encrypted file systems, and data loss software to prevent attacks on cloud infrastructures.
- Using security tools and adopting a corporate culture that upholds data security discreetly.

2. **Cloud Costs:** Costing is a significant challenge in the adoption, migration, and operation of cloud computing services, especially for small and medium-sized businesses.
- Prepare a cost estimate budget right from the start. It involves experts who will help for cloud cost management. An additional measure is creating a centralized team to oversee budget details.

3. **Reliability and Availability:** cloud providers continue to improve their uptimes; service disruption is still an enrollment problem. Small-scale cloud service providers are more prone to downtime. This problem persists today even with well-developed backups and platform advancements.
- Cloud computing service providers have resorted to creating multiple redundancy levels in their systems. Also, they are developing disaster recovery setups and backup plans to mitigate outages.

VIRTUALIZATION SECURITY MANAGEMENT

- **Migration management:** VM migration is easy to attack and is a vulnerable process. Special security mechanisms should be applied when a VM is migrated from a place to somewhere else. It sounds like an easy process but it is not.
  When any of the organizations or an enterprise tries to use any of the automated tools such as live migration many other factors creep in. Two different VMs on a single machine may cause a violation to Payment Card Industry (PCI).

- **VM Image Management:** VM Image (VMI) is a type of file or the format of the data which is used to create the virtual machine in the environment of virtualization. Hence, the confidential data and the integrity of VMIs are very important when the VMs are migrating or starting.
- **Patch Management:** Patch management is acquiring, installing, or testing system management or inserting code changes to the computer system administration. It also includes on the available patches of the maintaining current knowledge ensuring the patches are installed properly. Patch management is built for identify and test the various types of code changes.
- **Audit:** In the lifecycle of the Virtual machines, the sensitive data and the behavior of the virtual machines should be monitored throughout the virtual system. This may be done with auditing which provides the mechanism to check the traces of the activities left by the virtual system.

VIRTUAL THREATS

Some of the virtual threats to Cloud computing security are:

1. Shared clipboard:

Shared clipboard technologies enable information to become transferred between VMs as well as the host, offering a means of moving information between malicious programs in VMs of various security realms.

2. Keystroke logging:

Some VM technologies allow the logging of keystrokes and screen updates to become passed across virtual terminals within the virtual machine, writing to host files and permitting the monitoring of encrypted terminal connections in the VM.

3. VM monitoring in the host:

Since all network packets coming from or planning to a VM pass with the host, the host may be able to impact the VM from the following this:

- Starting, stopping, pausing, and restart VMs
- Monitoring and configuring resources available to the VMs, including CPU, memory, disk, and network usage of VMs
- Adjusting the amount of CPUs, level of memory, quantity, and variety of virtual disks, and quantity of virtual network interfaces offered to a VM.
- Monitoring the applications running inside the VM.
- The viewing, copying, and modifying data stored about the VM's virtual disks.

4. Virtual machine monitoring from another VM:

VMs shouldn't have the ability to directly access one another's virtual disks around the host. Nevertheless, if the VM platform uses a virtual hub or switches for connecting the VMs to the host, then intruders may be able to use a hacker technique called "ARP poisoning" to redirect packets planning to or in the other VM for sniffing.

5. Virtual machine backdoors:

Virtual machine backdoors, covert communications channel between guest and host could allow intruders to execute potentially harmful operations.

VM SECURITY RECOMMENDATIONS

Following virtual machine security recommendations help ensure the integrity of the cloud:

- **General Virtual Machine Protection:** A virtual machine is, in most respects, the equivalent of a physical server. Employ the same security measures in virtual machines that for physical systems.
- **Minimize Use of the Virtual Machine Console:** The virtual machine console provides the same function for a virtual machine that a monitor provides on a physical server.
  Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls. Console access might therefore allow a malicious attack on a virtual machine.
- **Prevent Virtual Machines from Taking over Resources:** When one virtual machine consumes so much of the host resources that other virtual machines on the host cannot perform their intended functions, a Denial of Service (DoS) might occur.
  To prevent a virtual machine from causing a DoS, use host resource management features such as setting Shares and using resource pools.
- **Disable Unnecessary Functions Inside Virtual Machines:** Any service that is running in a virtual machine provides the potential for attack. By disabling system components that are not necessary to support the application or service that is running on the system, to reduce the potential.

VM-SPECIFIC SECURITY TECHNIQUES

- **Protecting the VMM:**
  A hypervisor can be used to monitor the virtualized systems it is hosting. However, the hypervisor can in turn be targeted and modified by an attack. As the hypervisor possesses every privilege on its guest systems, it is crucial to preserve its integrity. However, while it is possible to ensure the integrity of a system during boot it is much harder to ensure runtime integrity.
  To ensure runtime integrity, one could think of installing a second hypervisor under the initial hypervisor dedicated to monitoring it, similar to one would have to guarantee that the most privileged hypervisor cannot, in turn, be corrupted. Several studies have therefore focused on using other means to ensure the integrity of the most privileged element.
- **Protecting the VMs against their VMM:**
  The purpose of CloudVisor is to ensure data confidentiality and integrity for the VM, even if some elements of the virtualization system (hypervisor, management VM, another guest VM) are compromised. The idea is that data belonging to a VM but accessed by something else than this VM appears encrypted.
- **Virtual Machine Encryption:**
  A virtual machine consists of a set of files, machine theft has now become much easier. Furthermore, stealing a virtual machine can be achieved with relative ease by simply snap shooting the VM and copying the snap shorted files.
- **Encryption under the hypervisor:**
  VMs can be encrypt the hypervisor. By using standard protocols such as NFS or iSCSI, the encryption is independent of the hypervisor platform. That means hypervisor features such as VMotion and LiveMigration continue to work unchanged. As VMs are copied into an encrypted data store, they will be encrypted according to the encryption policy.
- **Encryption within the VM:**
  In this model, for all devices encrypted, there is an encrypted path from the VM's operating system through the hypervisor and down to the storage layer. This prevents VM administrators from being able to view

sensitive data that resides within the VM. In this environment, as with the previous one described, the key server could reside anywhere.

- **Encryption of VM images and application data:**
  Another model combines encryption at the VM and storage layers. This combined option is superior because there's an encrypted path for sensitive data from the VM through the hypervisor. This prevents the VM administrator from seeing clear text data.

SECURE EXECUTION ENVIRONMENTS AND COMMUNICATIONS IN CLOUD

- An Execution Environment is an environment for executing code, in which those executing the code can have high levels of trust in that surrounding environment because it can ignore threats from the rest of the device.
  Execution Environment stands and distinguishes them from the uncertain nature of applications. Generally, the rest of the device hosts a feature Rich OS like Android, and so is generically known in this context as the REE (Rich Operating System Execution Environment).
- Cloud communications are the blending of multiple communication modalities. These include methods such as voice, email, chat, and video, in an integrated fashion to reduce or eliminate communication lag. Cloud communications are essentially internet-based communication.
- Cloud communications evolved from data to voice with the introduction of VoIP (voice over Internet Protocol). A branch of cloud communication is cloud telephony, which refers specifically to voice communications
- Cloud communications providers host communication services through servers that they own and maintain. The customers, in turn, access these services through the cloud and only pay for services that they use, doing away with maintenance associated with PBX (private branch exchange) system deployment.
- Cloud communications provide a variety of communication resources, from servers and storage to enterprise applications such as data security, email, backup and data recovery, and voice, which are all delivered over the internet. The cloud provides a hosting environment that is flexible, immediate, scalable, secure, and readily available.

The need for cloud communications has resulted from the following trends in the enterprise:

- Distributed and decentralized company operations in branch and home offices
- Increase in the number of communication and data devices accessing the enterprise networks
- Hosting and managing IT assets and applications

These trends have forced many enterprises to seek external services and to outsource their requirement for IT and communications. The cloud is hosted and managed by a third party, and the enterprise pays for and uses space on the cloud for its requirements. This has allowed enterprises to save on costs incurred for hosting and managing data storage and communication on their own.

The following are some of the communication and application products available under cloud communications that an enterprise can utilize:

- Private branch exchange
- SIP Trucking
- Call center
- Fax services
- Interactive voice response

- Text messaging
- Voice broadcast
- Call-tracking software
- Contact center telephony

All of these services cover the various communication needs of an enterprise. These include customer relations, intra-branch and inter-branch communication, inter-department memos, conference, call forwarding, and tracking services, operations center, and office communications hub.

Cloud communication is a center for all enterprise-related communication that is hosted, managed, and maintained by third-party service providers for a fee charged to the enterprise.

RGPVNOTES.IN

Thank you for using our services. Please support us so that we can improve further and help more people.
https://www.rgpvnotes.in/support-us

If you have questions or doubts, contact us on
WhatsApp at +91-8989595022 or by email at hey@rgpvnotes.in.

For frequent updates, you can follow us on
Instagram: https://www.instagram.com/rgpvnotes.in/.