Course: Cloud Computing

Week 9: **Security in the Cloud**

Lecturer: Ikwap Flavia Agatha
MSc. Computer Forensic
PHD in IT (Candidate)

Lecture Learning Out come

- At the end of this lecture, you will be able to;
- 1. Understand Cloud Security
- 2. Comprehend the business need for information security
- 3. Understand Key Security Requirements in Cloud computing
- 4. Understand the different security threats in cloud computing
- 5. Understand the different attacks in cloud computing
- 6. Understand the different mitigation techniques adopted by different cloud players

What is Cyber/Cloud Security?

- Cyber security is primarily about people, processes, and technologies working together to Encompass the full range of threat reduction, vulnerability reduction, deterrence, international Engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.

  OR

What is Cyber/Cloud Security?

- Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks.

Business Need for Security

- Information security performs four important functions for an organization:

1. Protecting the organization's ability to function
2. Enabling the safe operation of applications running on the organization's IT systems
3. Protecting the data the organization collects and uses
4. Safeguarding the organization's technology assets

Protecting the Functionality of an Organization

- Any security breach can paralyze the activities ability to run its normal operations, it's there very vital that security mechanisms are provided to mitigate attacks
- Both general management and IT management are responsible for implementing information security that protects the organization's ability to function. IT Security has more to do with *management* than with *technology*, managing information security has more to do with policy and its enforcement than with the technology of its implementation

Enabling the Safe Operation of Applications

- Today's organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications. A modern organization needs to create an environment that safeguards these applications, particularly those that are important elements of the organization's
- Infrastructure—operating system platforms, electronic mail (e-mail), and instant messaging (IM) applications. Organizations acquire these elements from a service provider or they build their own.

Protecting Data that Organizations Collect and Use

- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Any business, educational institution, or government agency operating within the modern context of connected and responsive services relies on information systems.

Protecting Data that Organizations Collect and Use

- Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services. Therefore, protecting *data in motion* and *data at rest* are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization's data.

Safeguarding Technology Assets in Organizations

- To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool. When an organization grows, it must develop additional security services. For example, it could require a public key infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

Key Security Requirements in Cloud computing

- The International Standards Organization (ISO) defines Information Security concerns which can also be guided in regard to the cloud computing key security requirements for an effective and secure technology solution. These are defined as follows:
- **Confidentiality** means keeping users' data and allowing privileged entities only to have access to data.
- **Integrity** means to assure that there is no alteration or modification in data while it is stored or being transported and only authorized users have access to change, modify, copy or delete data.

Key Security Requirements in Cloud computing

- **Authentication** means to assure the identity of the user before giving access to data and this can be done by employing certain protections to their profiles.
- **Availability** means to assure that data which is requested by the user or the services he needs are constantly accessible at any time and at any place.
- Authorization means to assure that the users who have requested the particular information have the rights to access it

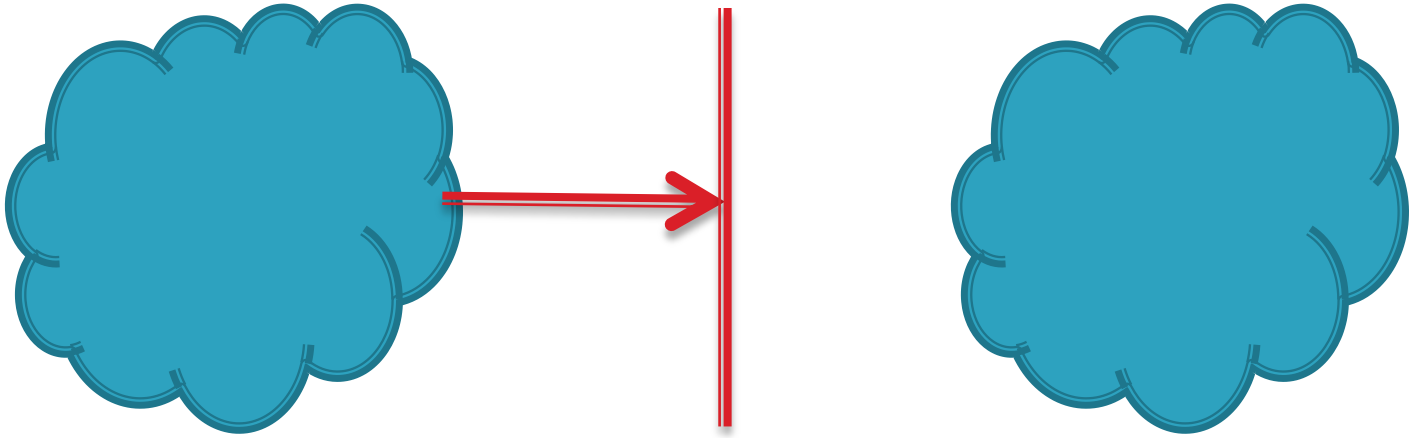
Attacks

- Any action that compromises the security of information owned by an organization
- **Demonstration of an attack occurrence**
- Normal Traffic flow without any Attack

- Source Destination

Demonstration of an attack occurrence

- Security Attack Causing an INTERRUPT in Communication
- An asset of a system can be destroyed or becomes unavailable or unusable. It is an attack on **Availability**

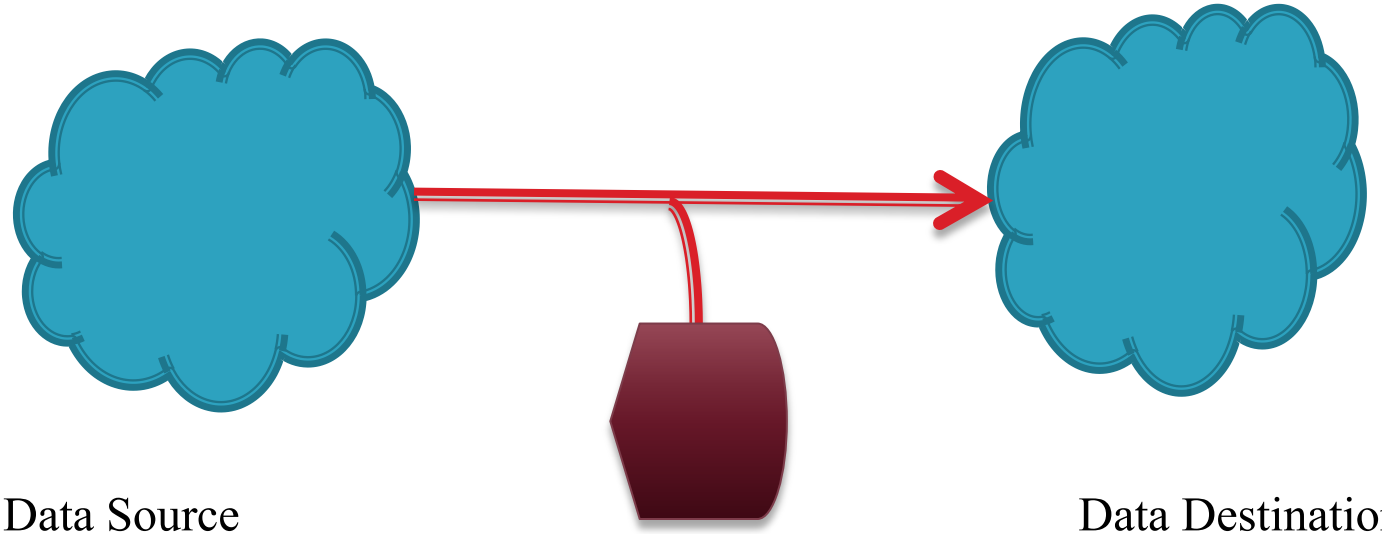


- Data Source

Data Destination

Demonstration of an attack occurrence

- Security Attack-INTERCEPTION



- Data Source

Data Destination

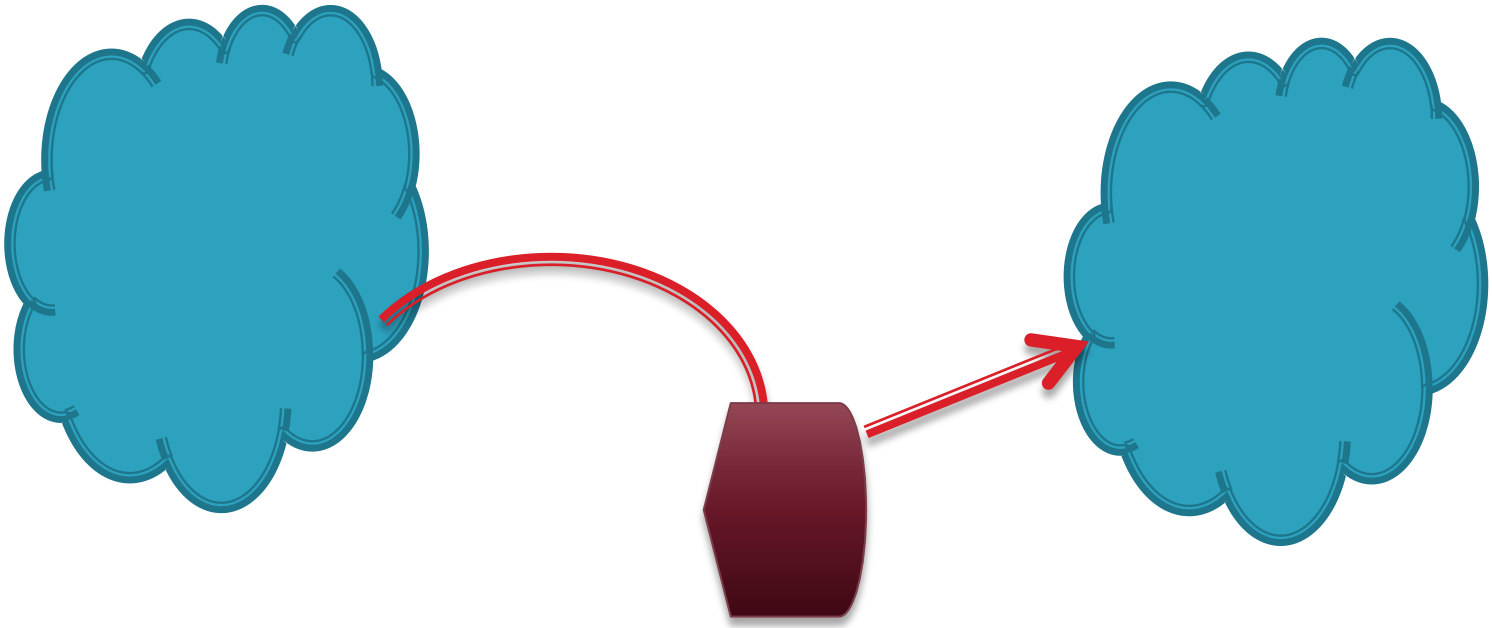
Security Attack-INTERCEPTION

- An unauthorized party gains access to an asset. Attack on confidentiality.
- Examples: Wiretapping to capture data in a network.
- Illicitly copying data or programs, Eavesdropping, Capture data in a network, copying file

Demonstration of an attack occurrence

- Security Attack-Modification When an unauthorized party gains access and tampers an asset. Attack is on Integrity.
- Changing value of data, modify message
- Examples: Changing data file, Altering a program and the contents of a message

Security Attack-Modification



- Data Source

Data Destination

Security threats in cloud computing

Security Issues in hypervisor

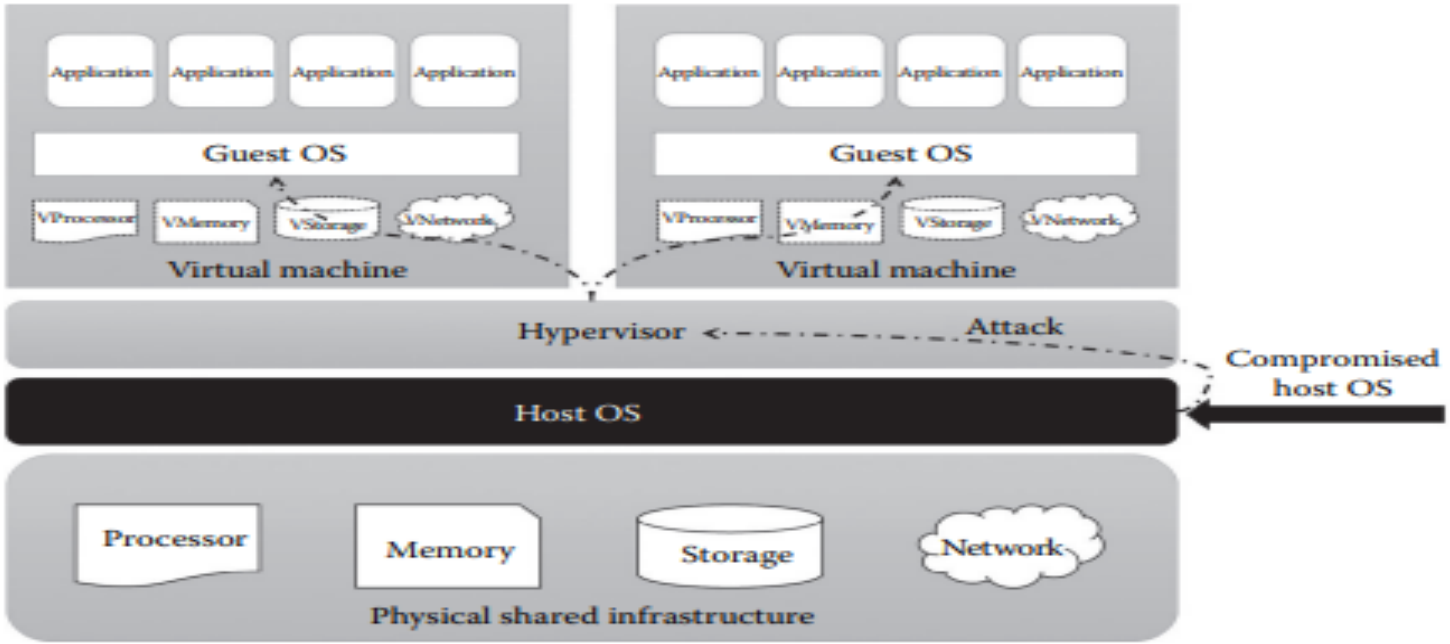
- The hypervisor creates a virtual environment in the data centers and can be attacked through malicious code written by any attacker to disrupt or corrupt the whole server. Hypervisor is the higher authority entity that has the direct access to the hardware hence attracting attackers.
- There are two possibilities of attacking the hypervisor: 1. through the host OS. 2. Through the guest OS

Security threats in cloud computing

- Attacks from the host OS can be performed by exploiting the vulnerabilities of the host OS
- Once the attacker gets full control over the hypervisor through the compromised OS, the attacker will be able to run all the privileged instructions that can control the actual hardware, he can then carry out malicious activities:
- Denial of service attack
- Stealing the confidential information
- Malicious script.

Security Issues in hypervisor

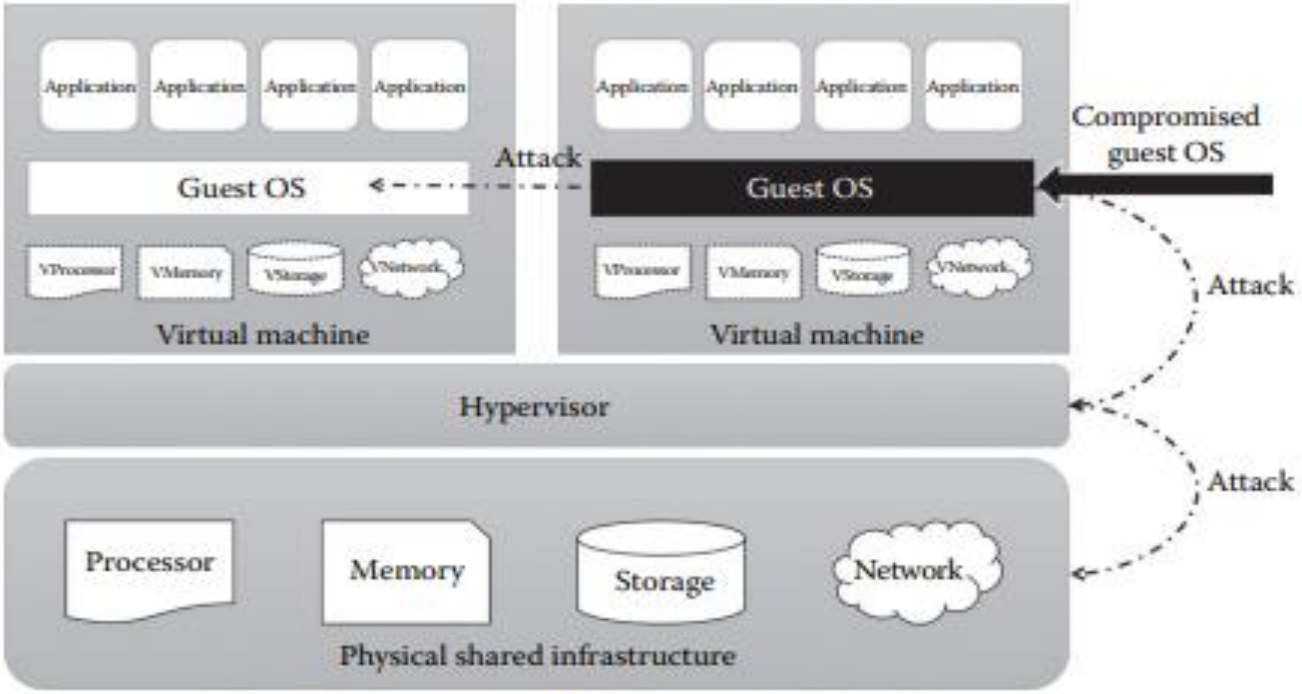
- Through the Host OS



- **(K.Chandrasekaran, 2015)**

Security Issues in hypervisor

- Through the guest OS



- (K.Chandrasekaran, 2015)

Cloud Security Threats

- Losing control over data: Outsourcing means losing significant control over data. Amazon Simple Storage Service (S3) APIs provide both bucket- and object level access controls, with defaults that only permit authenticated access by the bucket and/or object creator.
- Data Integrity: Data integrity is assurance that data changes only in response to authorized transactions, in the cloud there is possibility of compromising data integrity.

Cloud Security Threats

- Risk of Seizure: Exposing your data in an environment shared with other companies could give the government “reasonable cause” to seize your assets because another company has violated the law.

Cloud Security Threats

- Incompatibility Issue: Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating "sticky services" – services that an end user may have difficulty transporting from one cloud vendor to another
- Constant Feature Additions: Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected however, this could have security implications.

Cloud Security Threats

- Failure in Provider's Security: Failure of cloud provider to properly secure portions of its infrastructure results in the compromise of subscriber systems.
- Abusive Use of Cloud Services can be described as consumer's unethical and illegal actions to misuse the services. Low-cost infrastructure, high-resource, provisioning, weak registration procedures have facilitated anonymity to spammers, criminals, and other malicious users to achieve their target in attacking the system.

Cloud Security Threats

- Insecure Interfaces and Application Programming Interfaces (API). As the security of cloud services depends on these APIs so these should have secure certification standards, proper access controls and activity monitoring mechanisms to avoid
- Malicious Insiders can be trusted people within an organization who can access organizational confidential assets. They can perform unprivileged activities to infiltrate organizational assets and can do brand damage, productivity and financial losses

Cloud Attacks

- Structured Query Language (SQL) Injection Attacks - In standard SQL code, the attacker inserts malicious code to access unauthorized database to gain sensitive data about the user. In this case, the website allows hacker’s data to be accessed by SQL Server considering it as user’s data

Cloud Attacks

- Cross Site Scripting (XSS) Attacks - The attacker inserts malicious code into the user's web page to redirect him to the attacker's website. Implemented by using Stored XSS (permanently stores malicious code into a resource managed by the web application) or Reflected XSS (immediately reflects back malicious code to the user and hence do not store it permanently)

Cloud Attacks

- Reused IP Address Attacks - Each node of a network has an IP address which is allocated to a particular user when that user leaves the network; the IP address associated with him is assigned to a new user. The chances of accessing previous user data by the new user exist as the address still exist in DNS cache and hence the data belonging to one person can be accessed by another

Cloud Attacks

- Cookie Poisoning Attacks: The contents of the cookie are changed to get access to an unauthorized application or web page. The cookie contains sensitive credentials about user's data and when the hacker gains access to these contents then he also gains access to the content within these and can perform illegal activities
- Man in the Middle Attack: This attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker

Cloud Attacks

- Distributed Denial of Service (DDOS) Attack: In this attack servers and networks are flooded by a huge amount of network traffic and users are denied the access to a certain Internet based Service.
- IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address. Intruder gain unauthorized access to computer, whereby he sends messages to a computer with an IP address indicating that the message is coming from a trusted host

Cloud Attacks

- Port Scanning: Since a port is a place where information goes into and out of the computer, port scanning identifies open doors to a computer, hence, opening the computer to possible attack
- Packet Sniffing: Packet sniffing is listening (with software) to the raw network device for packets that interest you. When that software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like “login” or “password”

Cloud Attacks

- Domain Name Server (DNS) Attacks- the attacker makes use of DNS to translate the domain name into an IP address to access user's confidential data
- Zombie Attacks - victim's Virtual Machines (VMs) is flooded by sending requests from other VMs in the network. Attackers can flood a large number of requests in relatively short time period causing DOS attacks or DDOS attacks.

Mitigation Techniques

Cloud providers

- The cloud provider plays a very key role in ensuring the safety of clients and the resources they access over the cloud by ensuring a secure and isolated environment for each of them.
- Security measures applied by Cloud Providers
- Physical data center security including building security (keycard protocols, biometric
- Scanning protocols and round-the-clock interior and exterior monitoring, access to data center only by the authorized personnel.

Mitigation Techniques -Cloud providers

- Isolating and securing networks – each isolated network has to have proper perimeter controls and policies to limit access to it.
- Host machine operating system security manages many guest virtual machines at once and any security hole might give the attacker an access to multiple customer environments.

Mitigation Techniques -Cloud providers

- ✓ Host machine protection should include
- ✓ Intrusion detection system monitoring network and system for any malicious activities.
- ✓ small number of user accounts as possible with limited administrator's access to them,
- ✓ policy on strong and complex access passwords,
- ✓ No publicly accessible network services and only necessary programs running on the machine

Mitigation Techniques -Cloud providers

- Performing regular vulnerability scanning of cloud infrastructure in order to find and identify any new or recurring vulnerability to prepare proper mitigation strategies.
- Strong authorization and authentication must be implemented to provide the customer with secure access to their data and resources.
- The principle of least privilege should be taken into consideration ensuring that the user can access only the resources he needs.

Mitigation Techniques -Cloud providers

- Ensuring auditing mechanisms are in place logging every time the customers or administrators access and use the resources.
- Frequent backups of data should be performed by the provider. It has to be transparent to the customer what backups the provider will perform and what should be done by the user
- Encrypting APIs through which the customers access the cloud resources with SSL, recommended to provide the secure communication over Internet

Mitigation Techniques -Cloud customers

- Cloud Customers are equally stakeholders in ensuring the safety of resources, best practices for customers:
- Proper firewall protection is required to analyze the incoming and outgoing traffic and Making sure any unauthorized access is blocked. User has to make sure that the hardware firewalls are properly configured to protect all the machines on local networks

Mitigation Techniques -Cloud customers

- Software firewalls have to be installed on individual's machines to prevent a third party from taking control of the machine and to protect the customer's virtual machines.
- Up-to-date software including anti-virus, operating system and browsers through which the users usually access the cloud services. Updating provides protection from the newest threats and any bugs.

Mitigation Techniques -Cloud customers

- Enforcing strong passwords policies since most attacks occur due to using the insecure passwords.
- Users should have backup policies which they can discuss with the service provider, third-party backup services to have the copies of the data in a case of sudden data loss in the cloud

Mitigation Techniques -Cloud customers

- Ensuring a firewall for virtual machines service ports
- using encryption for communication
- Making use of Intrusion Detection Systems to monitor system and network for any malicious activities.

Mitigation Techniques -Cloud customers

- Keep up to data with the latest cloud security developments and any changes made to the security policies or infrastructure by the provider.
- Limiting access to data by setting proper access privileges to limiting number of other users or employees.
- Encrypting sensitive data as it travels over the cloud

Standards for Security in Cloud Computing

- Security standards define the processes, procedures, and practices necessary for implementing a security program.
- Security Assertion Markup Language (SAML): SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners. It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal.

Standards for Security in Cloud Computing

- Open Authentication (OAuth): OAuth is an open protocol that allows secure API authorization in a simple, standardized method for various types of web applications. OAuth is a method for publishing and interacting with protected data.

Standards for Security in Cloud Computing

- OpenID: It is an open, decentralized standard for user authentication and access control. It allows users to log onto many services using the same digital identity. It is a singlesign-on (SSO) method of access control. OpenID replaces the common log-in process, i.e. a log-in name and a password, by allowing users to log in once and gain access to resources across participating systems.

Standards for Security in Cloud Computing

- SSL/TLS: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP. TLS and SSL encrypt the segments of network connections at the transport layer. The TLS protocol allows client/server applications to communicate across a network in a way specifically designed to prevent eavesdropping, tampering, and message forgery

Next Lecture

- Migrating to the Cloud

References

- Alani, M. M. (2014). Securing the Cloud: Threats, Attacks and Mitigation Techniques. *Journal of Advanced Computer Science and Technology*, 1-12.
- Amara, N. (2017). Cloud Computing Security Threats and Attacks with their Mitigation Techniques. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, (pp. 1-9). Nanjing.
- Chandrasekaran, K. (2015). *Essentials of Cloud Computing.* Newyork: CRC.
- Ertaul, L. (2010). *Security Challenges in Cloud Computing.* Istanbul.
- Poniszewska-Maranda, A. (2014). Selected aspects of security mechanisms for cloud computing – current solutions and development perspectives. *Journal of Theoretical and Applied Computer Science*, 1-15.