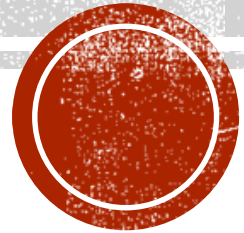
CLOUD SECURITY

Dr. Manjunath Hegde
Dept. of Computer Applications
Manipal Institute of Technology, Manipal



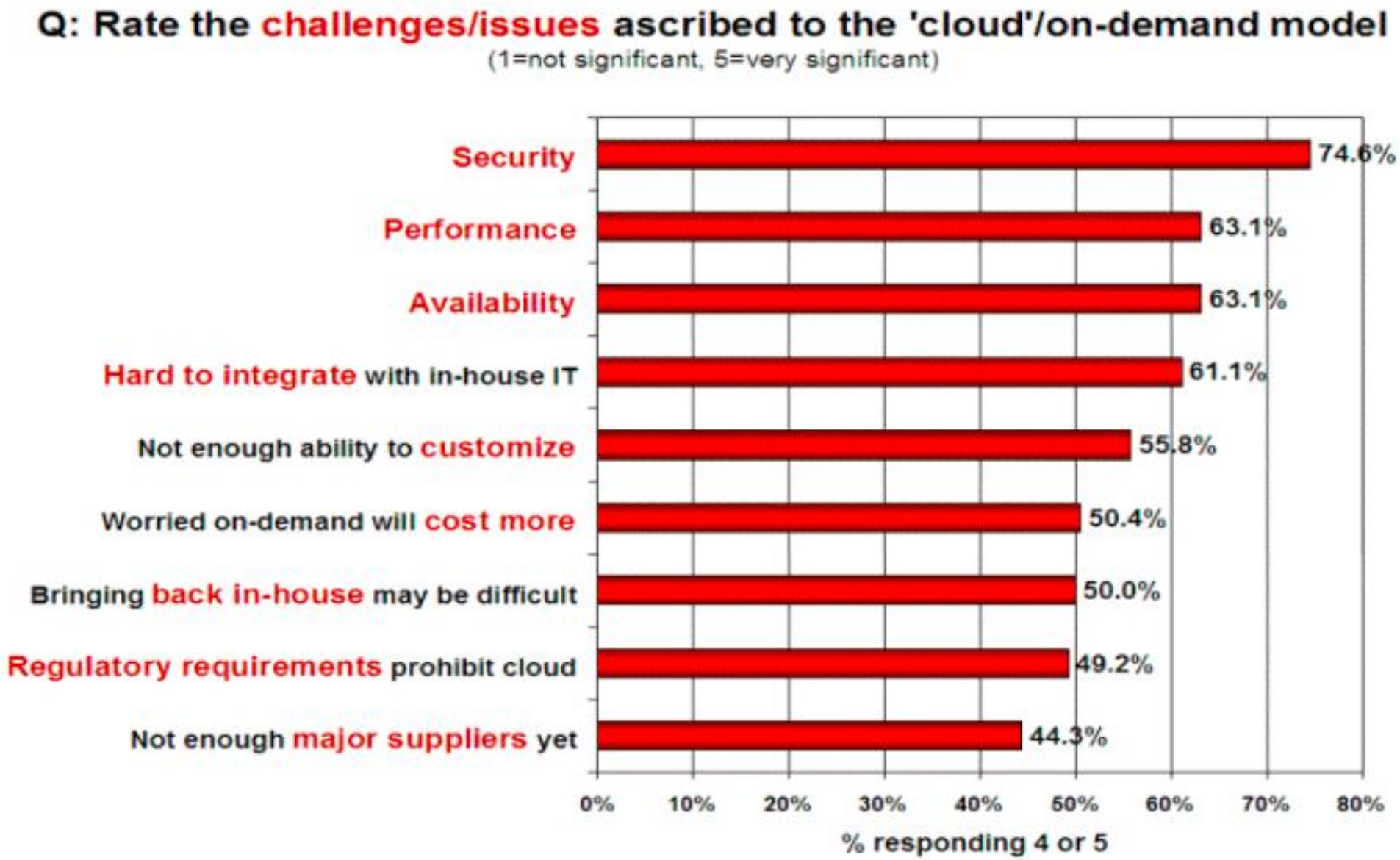
CLOUD BREACHES OF 2019

- April 2: Facebook (Cultura Colectiva)
- Breach size: 540,000 records, 146 GB of data

- April 25th: Docker Hub
- Breach size: 190,000 accounts

- May 20th: Instagram (Chtrbox)
- Breach size: 49 Million Records

- July 29: Capital One
- Breach size: 80,000 Bank Account Numbers, Over 1 Million Government ID Numbers


Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)
Security
74.6%
Performance
63.1%
Availability
63.1%
Hard to integrate with in-house IT
61.1%
Not enough ability to customize
55.8%
Worried on-demand will cost more
50.4%
Bringing back in-house may be difficult
50.0%
Regulatory requirements prohibit cloud
49.2%
Not enough major suppliers yet
44.3%
0%
10%
20%
30%
40%
50%
60%
70%
80%
% responding 4 or 5

THREE BASIC COMPONENTS OF SECURITY

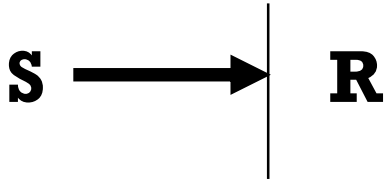
- Confidentiality
  - Keep data and Resources hidden
- Integrity
  - Data Integrity (Integrity)
  - Origin integrity (Authentication)
- Availability
  - Enabling access to data and resources

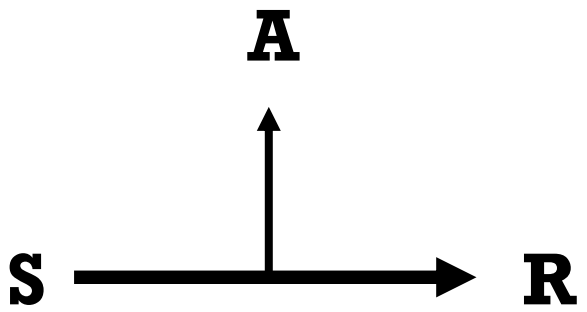
SECURITY ATTACKS

- Any action that compromises the security of information
- Four types of attack
  - Interruption - Obstruction during the communication process between the systems.
  - Interception - The data or message which is sent by the sender is stolen by an unauthorized individual where the message will be changed to the different form or it will be used by the malicious process
  - Modification - Message which is sent by the sender is modified and sent to the destination by an unauthorized user.
  - Fabrication - A fake message is inserted into the network by an unauthorized user as if it is a valid user.

Basic Model

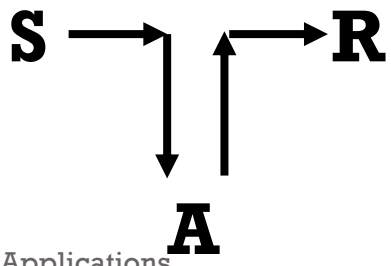
Interruption – Attack on availability

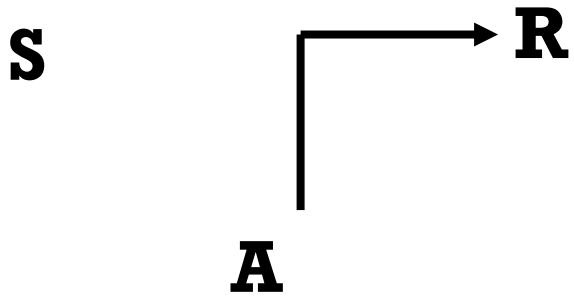




Interception – Attack on Confidentiality

Modification – Attack on Integrity





Fabrication – Attack on Authenticity

KEY TERMS

- **Threat** – is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets.
- **Vulnerability** – is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques.
- **Attack** – is an action that exploits a vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.

What are the differences between Attack and Threat?

CLASSES OF THREATS

- Disclosure
  - Snooping*
- Deception
  - Modification, Spoofing**, Repudiation of origin, Denial of receipt
- Disruption
  - Modification
- Usurpation***
  - Modification, Spoofing, Delay, Denial of service

*snooping is unauthorized access to another person's or company's data
**Spoofing is pretends to be something else in an attempt to gain the confidence to access the system/service
***Unauthorized control of some part of a system

GOALS OF SECURITY

- Prevention
  - Prevention attack from violating the security policies
- Detection
  - Prevention attackers who violating the security policies
- Recovery
  - Stop attack, asses and repair damage
  - Continue to function correctly even if attack succeeds

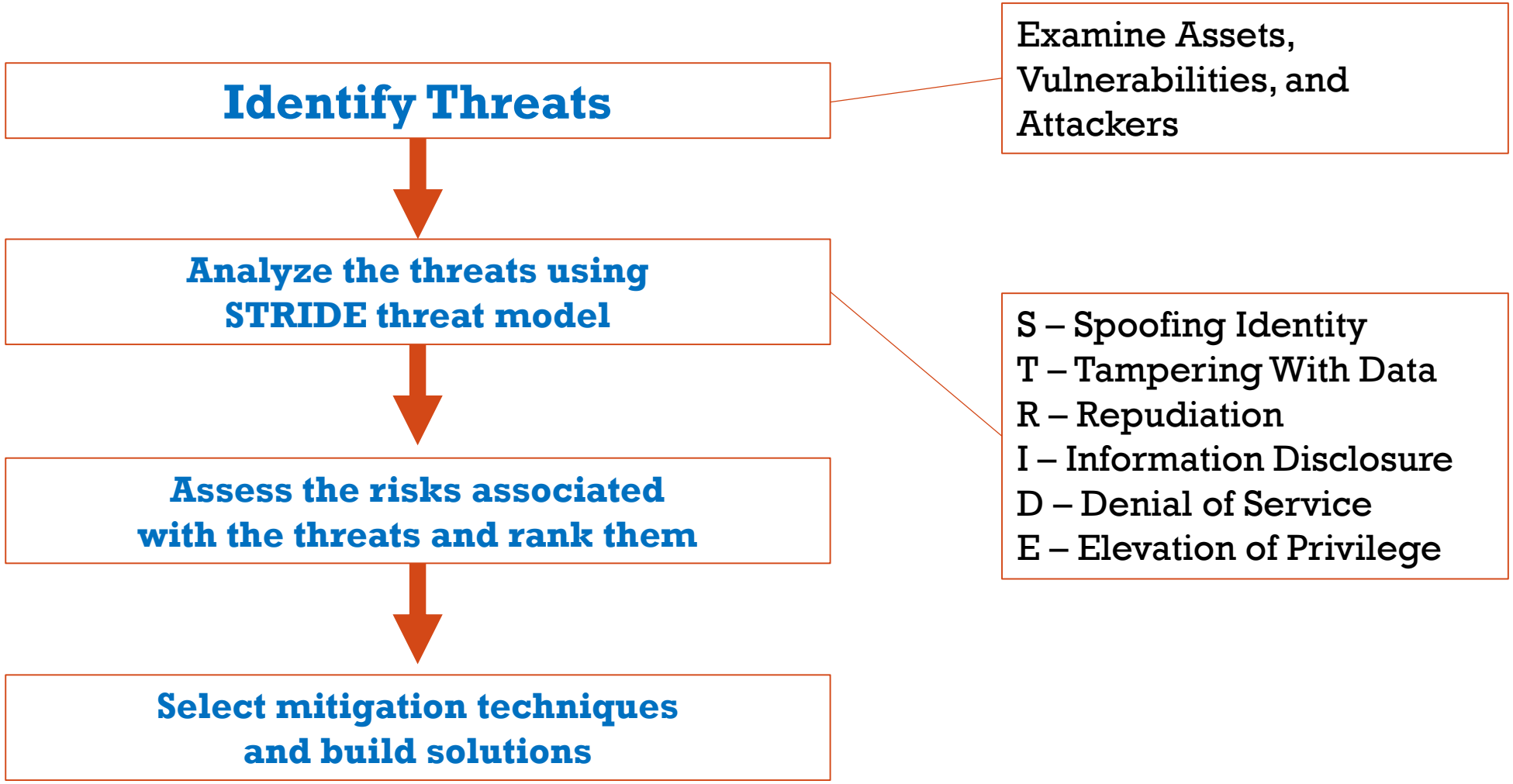
WHAT IS CLOUD SECURITY?

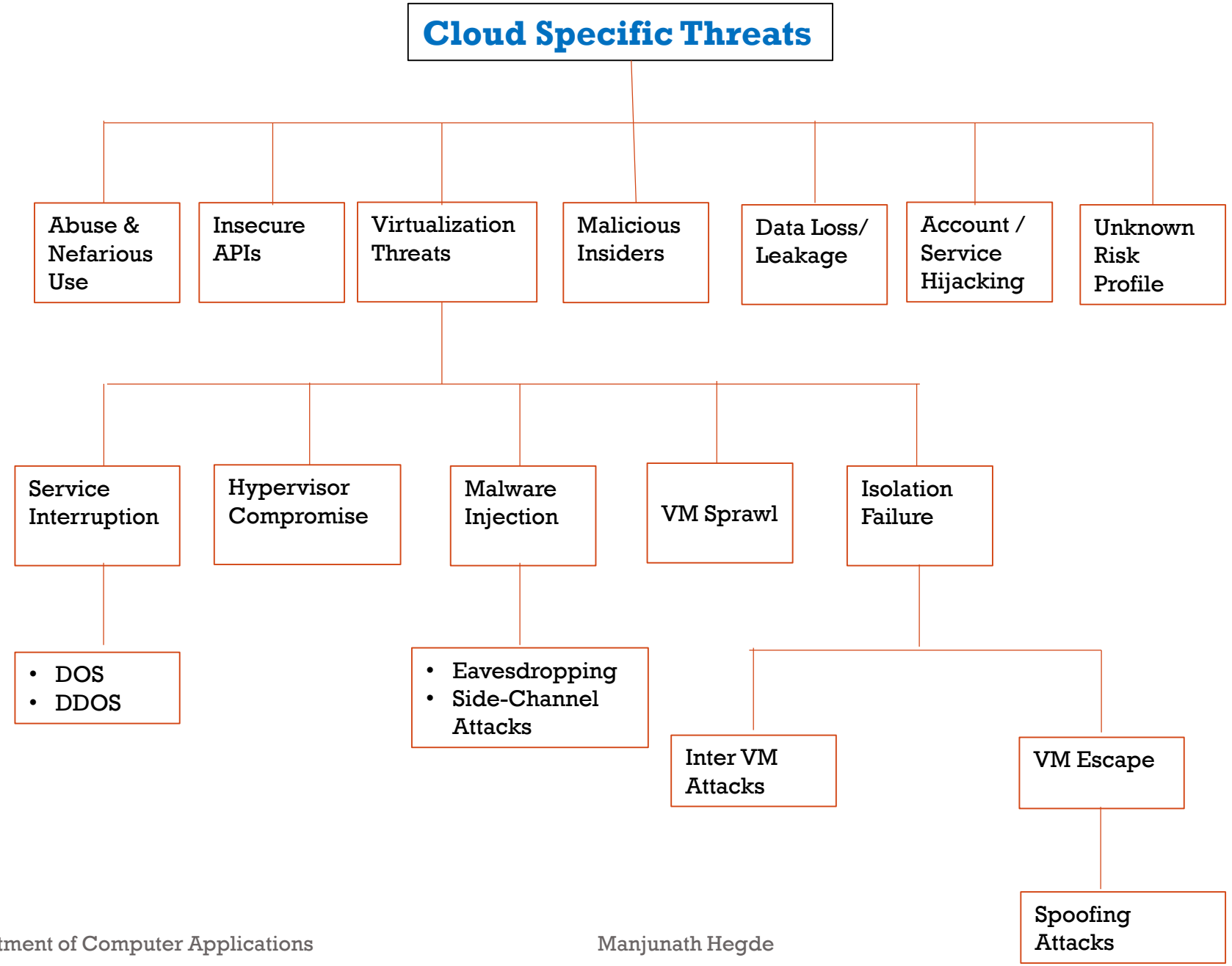
- Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion.
- Methods of providing cloud security include
  - Firewalls
  - Penetration testing
  - Tokenization, virtual private networks (VPN)
  - Avoiding public internet connections.
- Cloud security is a form of cybersecurity.

MOTIVATION

- Cloud provider - provides resources/services that can be accessed from anywhere in the world by the user.
- Cloud user - can be either a single person or any organization.
- Cloud computing has many benefits, but security is a big concern.
- Cloud provider should provide privacy and security to the user's data and applications.

Threat Model




Cloud Specific Threats
Abuse & Nefarious Use
Insecure APIs
Virtualization Threats
Malicious Insiders
Data Loss/ Leakage
Account / Service Hijacking
Unknown Risk Profile
Service Interruption
Hypervisor Compromise
Malware Injection
VM Sprawl
Isolation Failure
• DOS
• DDOS
• Eavesdropping
• Side-Channel Attacks
Inter VM Attacks
VM Escape
Spoofing Attacks

SHARED TECHNOLOGY VULNERABILITIES

- Cloud computing provides scalable services with shared infrastructure, computational power, storage, and cost-effectiveness over the Internet on user's demand basis.
- Virtualization plays a major role in cloud computing
  - Normal virtualization security techniques are not enough to handle virtualization security in cloud computing
  - Applying virtualization to cloud computing may cause additional security risks such as isolation failure, service interruption
- Multiple users share the cloud infrastructure
  - This co-tenancy also introduce vulnerabilities such as performing side-channel attacks to get another user's confidential information via information leakage

DATA PRIVACY

- The two issues lead to many privacy and security concerns:
  - User does not have control over the data
  - Dependence on the cloud provider
- Solution: Data encryption, but should consider the facts
  - How to encrypt the data
  - Who is responsible for encryption
- Choose a strong encryption mechanism to secure data in cloud computing.
- To ensure privacy, data should be encrypted by the user.

AUTHENTICATION

- How to authenticate the user?
  - Use Public Key Infrastructure (PKI) PKI provides Authentication, Integrity, Confidentiality.
- PKI is the strong authentication system, but does not replace the need for authentication.
- Use two-factor authentication – In combination with the other factors such as Smart cards or Biometrics, PKI can create solution for authentication

NEED

- Traditional security techniques are not capable enough to handle cloud specific threats.
- To secure cloud, cloud specific security mechanisms need to be investigated and developed.

ABUSE & NEFARIOUS USE

- It is considered as the top security threat to cloud computing.
- Cloud providers do not enforce any strong registration process where any person with a valid credit card can register to receive cloud services.
- Some cloud service providers offer readily available free limited trial period of cloud services which presents a perfect time for cyber criminals to join the cloud and possibly misuse and abuse their access privilege to cloud services.

CONT..

- Cloud computing model involves multiple data centers across multiple locations and each data center is dedicated to many customers and their data needs;
- This in turn makes investigating and detecting unauthorized or inappropriate activity significantly difficult in a cloud environment.
- Attackers can exploit this threat and launch an attack called "cloud computing malware injection attack" by creating their own implementation module (e.g. PaaS or SaaS) within the cloud environment.
- Once adversary is capable of doing this trick, the cloud system will automatically redirect valid user requests to the service module run by attackers
- Eg: Hackers can host malicious data and possibly convince users of Amazon Elastic Cloud Compute (EC2) to run images on a virtual machine by giving the image a name that sounds official such as "Fedora-core"

INSECURE APIS

- A Cloud API is what facilitates the cloud services by enabling the development of applications and services provisioning the cloud hardware, software, and platforms.
- Cloud API is a gateway that provides access to the direct and indirect cloud infrastructures and software as the services.
- The APIs are provided by the cloud service providers to software developers to design the interfaces and through these interfaces, they can interact with the cloud services.
- Another layer built on the framework raises the complexity of the cloud allowing the vulnerabilities to enter in the cloud.
- The treats of clear-text authentication or transmission of content, improper authorizations, anonymous access, reusable passwords or tokenization can arise, hampering the cloud services and customer access, limiting monitoring and logging capabilities, creating unknown services, and API dependencies resulting in leading to the repudiation and denial of services.

THE SECURITY RISKS OF VIRTUALIZATION

- In a Virtualized environment, each of the VMs is detached from the rest of the system by the hypervisor or Virtual Machine Monitor (VMM).
- A Strong accomplishment can break this confinement and thus point to various concerns respecting the Confidentiality, Integrity, Or Availability of the VMs.
- Virtualization Security Issues
  - **VM escape**- Enables a hacker/cracker to gain access to the primary hypervisor and its created virtual machines.
  - **Hyperjacking**- Hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine (VM) host.
  - **VM sprawl**- When the large number of virtual machines exist in the environment without proper management.

VIRTUALIZATION SECURITY ISSUES

- **VM footprint-** Used for gathering information about target VM like OS installed, packages installed and services running etc.
- **Inside-VM attack-** VM can get infected with malware or OS rootkits at run time.
- **Outside-VM attack-** Attacks from the host OS and co-located VMs are known as outside-VM attacks.
- **Cross VM side channel-** To maximize resource utilization, multiple VMs are usually placed on the same physical server in the cloud environment. The basic idea is a malicious VM penetrates the isolation between VMs, and then access the shared hardware and cache locations to extract confidential information from the target.

CONT..

- Oudated SW packages in VMs- Outdated software packages in virtual machines can pose serious security threats in the virtualized environment.
- Because of the low cost and the ease of creation, users tend to create new virtual machines for different tasks, branch new virtual machines based on the old ones, snapshot machines or even rollback machines to an earlier state.

MALICIOUS INSIDERS

- A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

DATA LOSS/ LEAKAGE

- The risk of data leakage increases as more employees use their personal devices for work without a strict and robust security policy in place.
- When employees use these devices to access storage services (like Dropbox or OneDrive) to work from home or on the train, there is an increased risk for a security breach, especially when older versions of operating systems are used.
- This potential risk is not entirely mitigated by company-supplied IT devices either, as connections to unsecured networks can easily lead to a data hack.
- Another way in which sensitive data can be leaked is due to an unintentional human error. Storing passwords and sensitive personal data in a plain text file or on memory sticks can mean it's susceptible if the wrong person gets their hands on it.

ACCOUNT / SERVICE HIJACKING

- Cloud account hijacking is a process in which an individual or organization's cloud account is stolen or hijacked by an attacker.
- Cloud account hijacking is a common tactic in identity theft schemes in which the attacker uses the stolen account information to conduct malicious or unauthorized activity.
- When cloud account hijacking occurs, an attacker typically uses a compromised email account or other credentials to impersonate the account owner.

UNKNOWN RISK PROFILE

- One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths.
- Information about who is sharing your infrastructure may be relevent, in addition to network intrusion logs, redirection attemptsand/or successes, and other logs.
- Security by obscurity may be low effort, but it can result in unknown exposures.
- It may also impair the in-depth analysis required highly controlled or regulated operational areas.

CLOUD SECURITY CHALLENGES

- Cloud computing attracts users with its great elasticity and scalability of resources with an attractive tag line pay-as-you-use at relatively low prices.
- Although this provides savings in terms of finance and manpower, it brings with new security risks.
- There are many research organizations, cloud vendors, product development enterprises and academic research institutes working on various security classifications of cloud computing and its solutions.

SECURITY CHALLENGES

- We analyze the current security challenges in cloud computing environment based on state-of-the-art under the following two categories.
- Category 1: Architectural & Technological aspects
  - T1 - Logical storage segregation & multi-tenancy security issues
  - T2 - Identity management issues
  - T3 - Insider attacks
  - T4 - Virtualization issues
  - T5 - Cryptography and key management
- Category 2: Process & regulatory-related aspects
  - T6 - Governance and regulatory compliance gaps
  - T7 - Insecure APIs
  - T8 - Cloud & CSP migration issues
  - T9 - SLA & trust management gaps

For more info:
https://dl.acm.org/doi/pdf/10.1145/2345396.2345474

SOFTWARE-AS-A-SERVICE SECURITY

More info:

https://www.mcafee.com/enterprise/en-in/security-awareness/cloud/what-is-saas.html

http://www.ijceronline.com/papers/Vol4_issue06/version-2/J3602068071.pdf

SAAS

- Software-as-a-service (SaaS) is an on-demand, cloud-based software delivery model that enables organizations to subscribe to the applications they need without hosting them in house.
- SaaS is one of several categories of cloud subscription services, including platform-as-a-service and infrastructure-as-a-service.
- SaaS has become increasingly popular because it saves organizations from needing to purchase servers and other infrastructure or maintain an in-house support staff.

BENEFITS OF SOFTWARE-AS-A-SERVICE

- **On-demand and scalable resources.** Organizations can purchase additional storage, end-user licenses, and features for their applications on an as-needed basis.
- **Fast implementation.** Organizations can subscribe almost instantly to a SaaS application and provision employees, unlike on-premises applications that require more time.
- **Easy upgrades and maintenance.** The SaaS provider handles patches and updates, often without the customer being aware of it.
- **No infrastructure or staff costs.** Organizations avoid paying for in-house hardware and software licenses with perpetual ownership. They also do not need on-site IT staff to maintain and support the application.

SAAS SECURITY

- SaaS providers handle much of the security for a cloud application.
- The SaaS provider is responsible for securing the platform, network, applications, operating system, and physical infrastructure.
- However, providers are not responsible for securing customer data or user access to it.
- Some providers offer a bare minimum of security, while others offer a wide range of SaaS security options.

SECURITY ISSUES

- Authentication and authorization
  - The authorization and authentication applications used in enterprise environments need to be changed, so that they can work with a safe cloud environment.
- Data confidentiality
  - Confidentiality may refer to the prevention of unintentional or intentional unauthorized disclosure or distribution of secured private information. Confidentiality is closely related to the areas of encryption, intellectual property rights, traffic analysis, covert channels, and inference in cloud system.

CONT..

- Availability
  - The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel.
- Information Security
  - In the SaaS model, the data of enterprise is stored outside of the enterprise boundary, which is at the SaaS vendor premises.
- Data Access
  - Data access issue is mainly related to security policies provided to the users while accessing the data. Organizations have their own security policies based on which each employee can have access to a particular set of data.

CONT..

- Network Security
  - In a SaaS deployment model, highly sensitive information is obtained from the various enterprises, then processed by the SaaS application and stored at the SaaS vendor‘s premises. All data flow over the network has to be secured in order to prevent leakage of sensitive information.
- Data breaches
  - Since data from various users and business organizations lie together in a cloud environment, breaching into this environment will potentially make the data of all the users vulnerable. Thus, the cloud becomes a high potential target.
- Identity management and sign-on process
  - Identity management (IdM) or ID management is an area that deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. Area of IdM is considered as one of the biggest challenges in information security. When a SaaS provider want to know how to control who has access to what systems within the enterprise it becomes a lot more challenging task.

BEST PRACTICES

- By 2022, 95% of cloud security failures will be the customer's fault. To avoid security breaches, customers can implement improved security practices and technologies.
- There are SaaS security practices that organizations can adopt to protect data in their SaaS applications.
  - Detect rogue services and compromised accounts.
  - Apply identity and access management (IAM).
  - Encrypt cloud data.
  - Enforce data loss prevention (DLP).
  - Monitor collaborative sharing of data.
  - Check provider's security.

CLOUD SECURITY GOVERNANCE

CLOUD SECURITY GOVERNANCE

- Cloud security governance refers to the management model that facilitates effective and efficient security management and operations in the cloud environment so that an enterprise's business targets are achieved.
- Incorporates a hierarchy of executive mandates, performance expectations, operational practices, structures, and metrics that, when implemented, result in the optimization of business value for an enterprise.
- Cloud security governance helps answer leadership questions such as:
  - Are our security investments yielding the desired returns?
  - Do we know our security risks and their business impact?
  - Are we progressively reducing security risks to acceptable levels?
  - Have we established a security-conscious culture within the enterprise?

CLOUD SECURITY GOVERNANCE CHALLENGES

- Whether developing a governance model from the start or having to retrofit one on existing investments in cloud, these are some of the common challenges:
  - Lack of senior management participation and buy-in
  - Lack of embedded management operational controls
  - Lack of operating model, roles, and responsibilities
  - Lack of metrics for measuring performance and risk

LACK OF SENIOR MANAGEMENT PARTICIPATION AND BUY-IN

- The lack of a senior management influenced and endorsed security policy is one of the common challenges facing cloud customers.
- An enterprise security policy is intended to set the executive tone, principles and expectations for security management and operations in the cloud.
- Many enterprises tend to author security policies that are often loaded with tactical content, and lack executive input or influence.
- The result of this situation is the ineffective definition and communication of executive tone and expectations for security in the cloud.
- To resolve this challenge, it is essential to engage enterprise executives in the discussion and definition of tone and expectations for security that will feed a formal enterprise security policy.
- It is also essential for the executives to take full accountability for the policy, communicating inherent provisions to the enterprise, and subsequently enforcing compliance

LACK OF EMBEDDED MANAGEMENT OPERATIONAL CONTROLS

- Controls are often interpreted as an auditor's checklist or procedures, and as a result. Not effectively embedded into security operational processes.
- This lack of embedded controls may result in operational risks that may not be apparent to the enterprise.
- For example, the security configuration of a device may be modified (change event) by a staffer without proper analysis of the business impact (control) of the modification. The net result could be the exploitable security weaknesses that may not have been apparent with this modification.
- The enterprise would now have to live with an inherent operational risk that could have been avoided if the control had been embedded in the change execution process.

LACK OF OPERATING MODEL, ROLES, AND RESPONSIBILITIES

- Many enterprises moving into the cloud environment tend to lack a formal operating model for security, or do not have strategic and tactical roles and responsibilities properly defined and operationalized.
- This situation suffocate the effectiveness of a security management and operational function/organization to support security in the cloud.
- Establishing a hierarchy can help an enterprise to better manage and control security in the cloud, and protect associated investments in accordance with enterprise business goals.
- This hierarchy can be employed in an in-sourced, out-sourced, or co-sourced model depending on the culture, norms, and risk tolerance of the enterprise.

LACK OF METRICS FOR MEASURING PERFORMANCE AND RISK

- A problem that also stifles executive visibility into the real security risks in the cloud.
- For example, a metric that quantitatively measures the number of exploitable security vulnerabilities on host devices in the cloud over time can be leveraged as an indicator of risk in the host device environment.
- A metric that measures the number of user-reported security incidents over a given period can be leveraged as a performance indicator of staff awareness and training efforts.
- Metrics enable executive visibility into the extent to which security tone and expectations are being met within the enterprise and support prompt decision-making in reducing risks or rewarding performance as appropriate.

KEY OBJECTIVES FOR CLOUD SECURITY GOVERNANCE

- Strategic Alignment
  - Enterprises should mandate that security investments, services, and projects in the cloud are executed to achieve established business goals.
- Value Delivery
  - Enterprises should define, operationalize, and maintain an appropriate security function with appropriate strategic and tactical representation, and charged with the responsibility to maximize the business value from the pursuit of security initiatives in the cloud.
- Risk Mitigation
  - Security initiatives in the cloud should be subject to measurements that gauge effectiveness in mitigating risk to the enterprise. These initiatives should also yield results that progressively demonstrate a reduction in these risks over time.

CONT..

- Effective Use of Resources
  - It is important for enterprises to establish a practical operating model for managing and performing security operations in the cloud, including the proper definition and operationalization of due processes, the institution of appropriate roles and responsibilities, and use of relevant tools for overall efficiency and effectiveness.
- Sustained Performance
  - Security initiatives in the cloud should be measurable in terms of performance, value and risk to the enterprise (Key Performance Indicators, Key Risk Indicators), and yield results that demonstrate attainment of desired targets (Key Goal Indicators) over time.

CLOUD SERVICE RISKS

CLOUD SERVICE RISKS

- Security
  - Physical access to infrastructure, systems & data
  - Physical location of systems, data
  - Logical access to the network, OS, applications & databases
  - Network & data segregation
- Availability
  - Cloud provider service interruptions
  - Data location/availability for restoration
  - Network/connectivity interruptions
  - Failure of the provider to adhere to SLAs
  - Service provider disaster recovery

CONT..

- Processing Integrity
  - Adherence to change management procedures
  - Incident management
  - Failure of the provider to adhere to SLAs
    - Timeliness
    - Accuracy
    - Authorization
    - Completeness

CONT..

- Confidentiality
  - Comingling of data & other assets
  - Unauthorized access to sensitive or trade secret information
- Privacy
  - International laws affecting service provider location
  - Regulatory compliance/legal liability
  - Breach & incident management

RISK MANAGEMENT

- Data Flow Analysis
  - Understand life cycle
  - Develop data-flow schematics
  - Policies to review/update data flow documentation
- Managing Computing Risk
  - App & Tech Inventory
  - In conjunction with data flow analysis
  - Address each layer of cloud "stack" risk.
- Audit & Compliance
  - Regulatory implications
  - Use risk assessment tools and control frameworks
  - Assess control maturity
  - Vendor management

SECURITY MONITORING

CLOUD SECURITY MONITORING

- Monitoring is a critical component of cloud security and management.
- Typically relying on automated solutions, cloud security monitoring supervises virtual and physical servers to continuously assess and measure data, application, or infrastructure behaviors for potential security threats.
- This assures that the cloud infrastructure and platform function optimally while minimizing the risk of costly data breaches.

BENEFITS

- Cloud monitoring provides an easier way to identify patterns and pinpoint potential security vulnerabilities in cloud infrastructure.
- As there's a general perception of a loss of control when valuable data is stored in the cloud, effective cloud monitoring can put companies more at ease with making use of the cloud for transferring and storing data.
- When customer data is stored in the cloud, cloud monitoring can prevent loss of business and frustrations for customers by ensuring that their personal data is safe.
- Cloud monitoring is one initiative that enables companies to find the balance between the ability to mitigate risks and taking advantage of the benefits of the cloud.

CHALLENGES

- Virtualization poses challenges for monitoring in the cloud.
- Visibility can also be a concern when it comes to cloud monitoring. Many companies rely on third-party cloud services providers and may not have access to every layer in the cloud computing stack, and therefore can't gain full visibility to monitor for potential security flaws and vulnerabilities.
- Shifts in scope are another common challenge when dealing with cloud environments, as assets and applications may move between systems which may not necessarily have the same level of security monitoring.

HOW MONITORING WORKS

- There are several approaches to cloud security monitoring.
- Cloud monitoring can be done in the cloud platform itself, on premises using an enterprise's existing security management tools, or via a third party service provider.
- Some of the key capabilities of cloud security monitoring software include:
  - **Scalability:** tools must be able to monitor large volumes of data across many distributed locations
  - **Visibility:** the more visibility into application, user, and file behavior that a cloud monitoring solution provides, the better it can identify potential attacks or compromises
  - **Timeliness:** the best cloud security monitoring solutions will provide constant monitoring, ensuring that new or modified files are scanned in real time
  - **Integration:** monitoring tools must integrate with a wide range of cloud storage providers to ensure full monitoring of an organization's cloud usage
  - **Auditing and Reporting:** cloud monitoring software should provide auditing and reporting capabilities to manage compliance requirements for cloud security

BEST PRACTICES FOR MONITORING

- One of the most effective ways to mitigate cloud security risks is to gain strict controls over data at all endpoints.
- Effective cloud monitoring solutions can scan, evaluate, and classify data before it's downloaded to the enterprise network, avoiding the introduction of malware and other malicious elements that can create vulnerabilities and leave the enterprise open to data breaches.
- Coupled with the scanning and auditing of data already stored in the cloud, real-time monitoring at the point of exit and entry is highly effective for enterprises that require comprehensive security while still utilizing the benefits of the cloud.

DATA SECURITY

https://journals.sagepub.com/doi/pdf/10.1155/2014/190903

INTRODUCTION

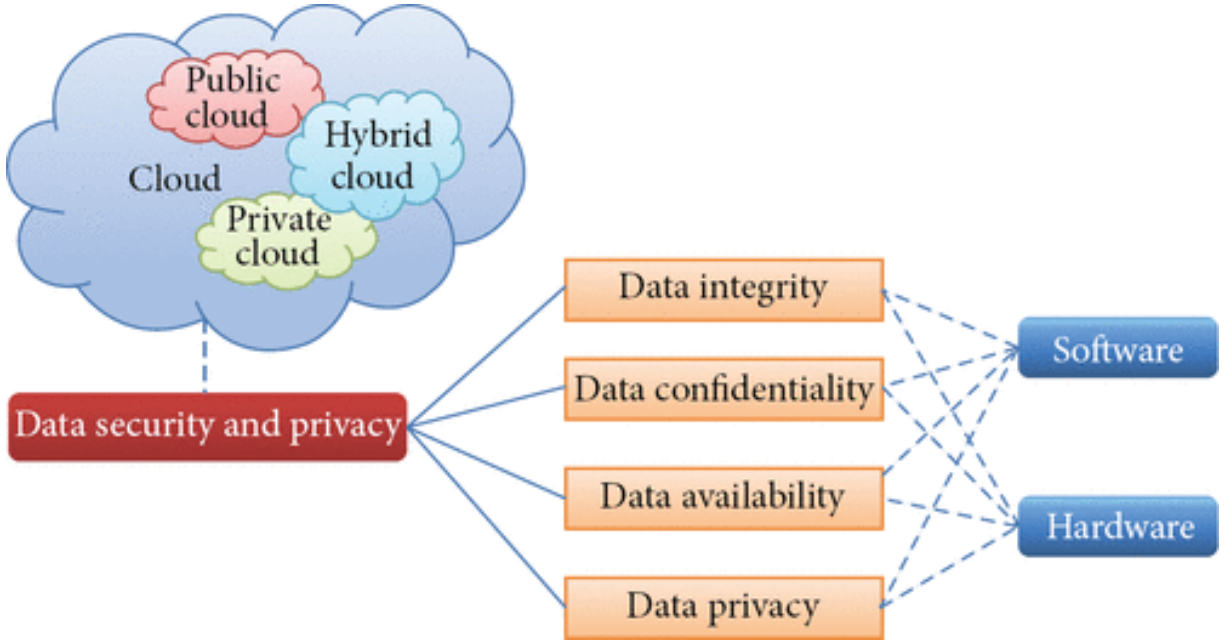
- Data security has consistently been a major issue in information technology.
- In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe.
- Data security and privacy protection are the two main factors of user's concerns about the cloud technology.
- Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

CONT..

- Cloud computing environment provides two basic types of functions: Computing
- Data storage.
- In the cloud computing environment, consumers of cloud services do not need anything and they can get access to their data and finish their computing tasks just through the Internet connectivity.
- During the access to the data and computing, the clients do not even know where the data are stored and which machines execute the computing tasks.

DATA SECURITY ASPECTS INCLUDES

- Data integrity,
- Data confidentiality
- Data availability
- Data privacy



DATA INTEGRITY

- Data integrity is one of the most critical elements in any information system.
- Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication.
- Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.

CONT..

- Data integrity is easily achieved in a standalone system with a single database.
- Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS).
- Transactions should follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity.
- Most databases support ACID transactions and can preserve data integrity.
- Authorization is used to control the access of data.
- It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

CONT..

- Data integrity in the cloud system means preserving information integrity.
- The data should not be lost or modified by unauthorized users.
- Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS.
- Data storage of large-scaled data, cloud computing environment usually provides data processing service.
- Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.
- By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity.
- The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity.

DATA CONFIDENTIALITY

- Data confidentiality is important for users to store their private or confidential data in the cloud.
- Authentication and access control strategies are used to ensure data confidentiality.
- The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness
- Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly.
- Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

HOW?

- **Homomorphic Encryption:** Homomorphic encryption is a form of encryption allowing one to perform calculations on encrypted data without decrypting it first. The result of the computation is in an encrypted form, when decrypted the output is the same as if the operations had been performed on the unencrypted data.
- **Encrypted Search and Database:** Which is concerned with the design and analysis of cryptographic techniques for searching on encrypted data.
- Distributive Storage
- **Hybrid Technique:** Uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes.
- **Data Concealment:** Concealment is the act of hiding
- **Deletion Confirmation:** Deletion confirmation means that data could not be recovered when users delete their data after the deletion confirmation.

DATA AVAILABILITY

- Data availability means the following:
- When accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

HOW?

- Reliable Storage Agreement
  - The most common abnormal behavior of untrusted storage is that the cloud service providers may discard part of the user's update data, which is hard to be checked by only depending on the simple data encryption.
  - A good storage agreement needs to support concurrent modification by multiple users.
- Reliability of Hard-Drive
  - Hard-drive is currently the main storage media in the cloud environment. Reliability of hard disks formulates the foundation of cloud storage.

DATA PRIVACY

- Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively Privacy has the following elements.
  I. When: a subject may be more concerned about the current or future information being revealed than information from the past.
  II. How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.
  III. Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

CONT..

- The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows:
  I. How to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,
  II. How to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,
  III. Which party is responsible for ensuring legal requirements for personal information,
  IV. To what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

APPLICATION SECURITY

http://ijcsit.com/docs/Volume%203/vol3Issue6/ijcsit20120306616.pdf

APPLICATION SECURITY

- The final level of security is application security in which the application can only be accessed by providing some kind of credentials.
- We can divide the application security in four types
- Identity based access
- Role based access
- Key based access
- Claim based access

IDENTITY BASED ACCESS

- In identity based access a username and password is provided by the user and if they matches with the records in the database then only the access is provided otherwise the access is denied.
- Username can ben uniquely identify that person. of many types for example, name, email address, id proofs like driving license number, pan card number, etc.
- In case of email id we have got additional advantage that in case of lost password we the issuing authority can send the new password to that email id.

ROLE BASED & KEY BASED

- Role based access
  - In role based identity a role is associated with the user like administrator, developer etc and the application changes the view according to the role of that user.
  - Other credentials are also stored while issuing the role based identity to that user for security purpose.
- Key based access
  - In key based identity the end user is provided a key and by using that key only the end user can access the services.
  - This key is also stored in the database for verification. This key is encrypted and is generally very long such that no one can guess it.
  - The level of security is very high with key based identity.
  - It is generally associated with a time stamp and the services can only be used generally for certain amount of time only like 1 day or 6 hours, 1 month etc.

CLAIM BASED ACCESS

- In claim based identity a live id is created for a particular brand and all other services provided by that particular brand are accessed by that id.
- This is done because the end user or customer does not want to or does not prefer to create a new id and remembering the credentials each time for using the different services of that particular brand.
- The end user never likes filling the form each time for different services of that particular brand. So in order to attract customer to use their services without any pain and at the same time not compromising with the security claim based identity has been introduced.
- Efforts and cost for maintain the data also reduce to great extent and at the same time we can track the data that how many services and what type of the services has been accessed by a particular type of person.
- Example of claim based identity is Google id which is same for Gmail, Google+, Blogspot, Google search etc. Similarly Windows live id which is common for downloading all kinds of software provided for Windows.