UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Lecture 14 – Cloud Security

Prof. Esposito Christian

::.. Summary

- Attacks and Vulnerabilities
  - Modelling security in cloud computing;
  - Cloud security countermeasures.
- Cloud Security Assurance.

::.. Key Lectures

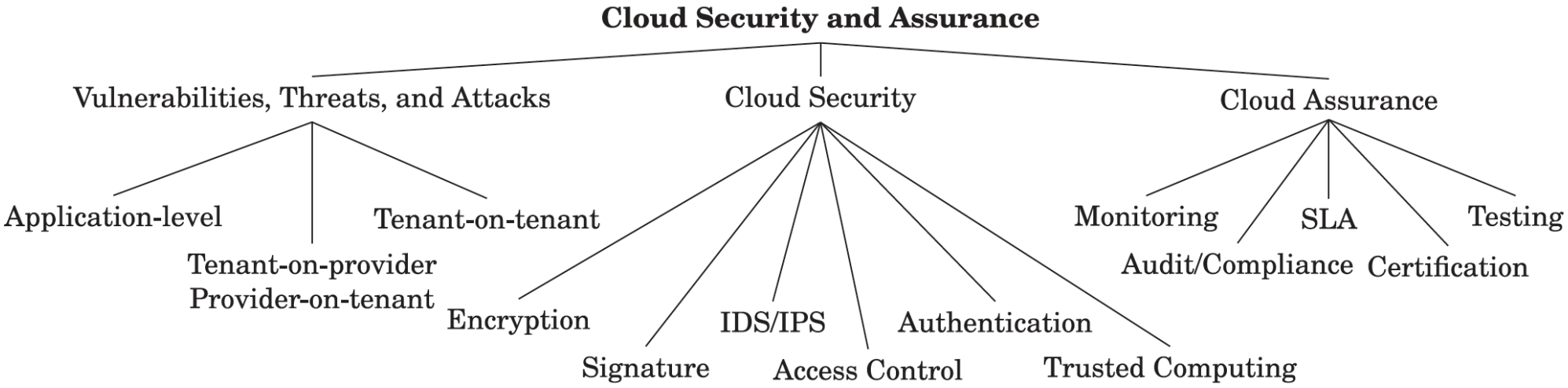
- C. A. Ardagna, R. Asal, E. Damiani, Q. H. Vu, “From security to assurance in the cloud: A survey”, ACM Computing Surveys (CSUR), 48(1): 1-50, July 2015.
- A. Singh, K. Chatterjee, “Cloud security issues and challenges: A survey”, Journal of Network and Computer Applications 79: 88-115, 2017.
- R. Kumar, R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey”, Computer Science Review 33: 1-48, 2019.

::.. Introduction (1/4)

Cloud computing in fact makes service providers and customers lose, at least partly, control over the status of their data and applications, impairing their ability to assess risks. The perceived lack of security is one of the main reasons discouraging customers and business owners from adopting cloud solutions.

The security research community has worked hard to improve the security of the cloud and the trust of cloud users that their applications and information are correctly managed and protected. However, we have witnessed the proliferation of ad hoc security solutions that target a very small part of the whole problem. This is why it is also important the cloud security assurance, which can be defined as the way to gain justifiable confidence that infrastructure and/or applications will consistently demonstrate one or more security properties, and operationally behave as expected despite failures and attacks.

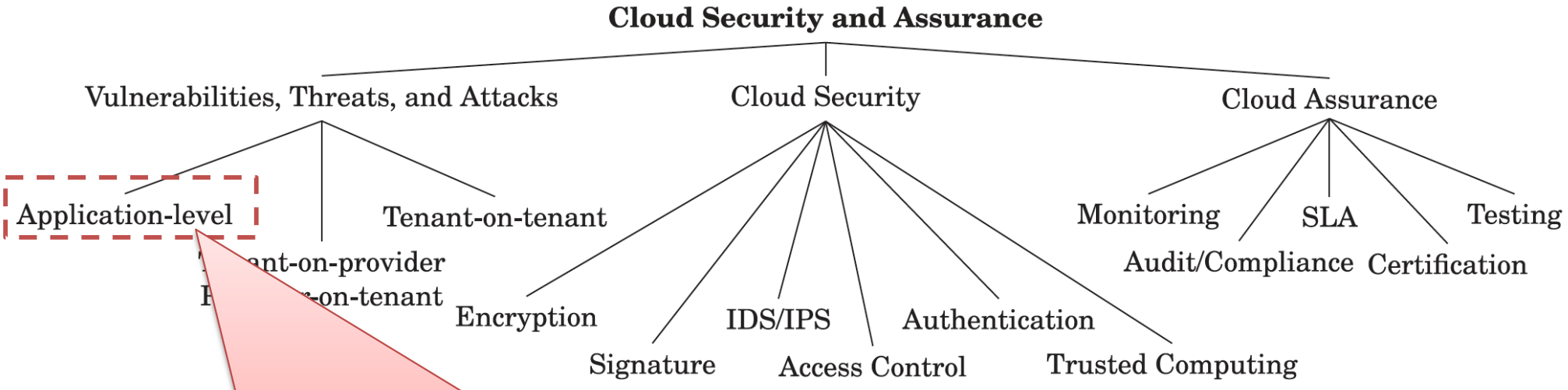
::.. Introduction (2/4)



The current literature on the topic can be partitioned in

- Studies presenting new security vulnerabilities, threats, and attacks in the cloud;
- Studies presenting novel security techniques and mechanisms protecting data and application security in the cloud;
- Studies presenting original assurance techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

::.. Introduction (2/4)



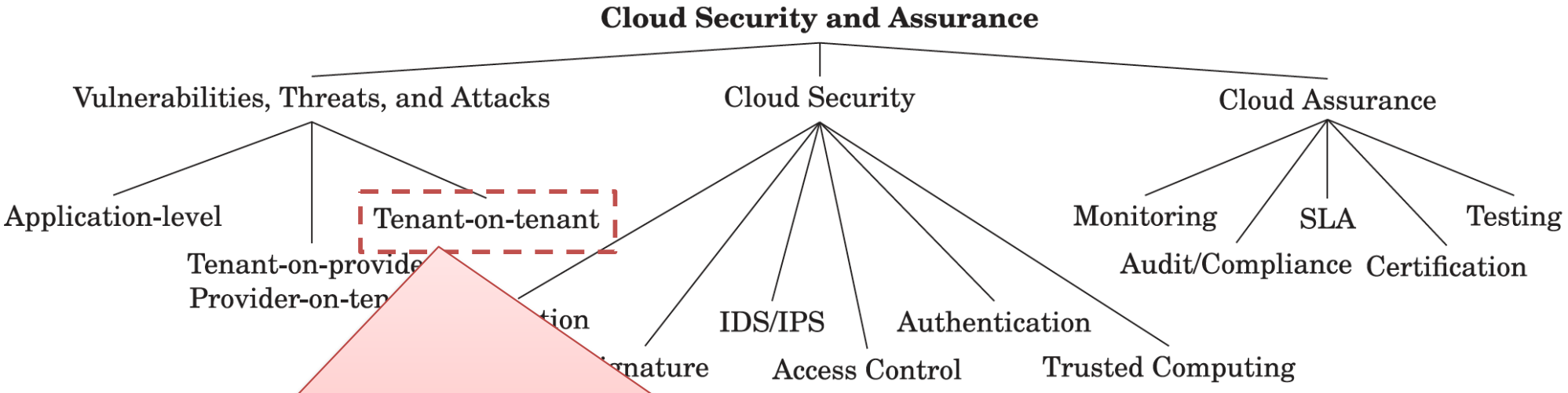
Attacks can be made by any cloud actor and target the SaaS level, including its services and data.

T …tioned in

…rabilities, threats, and attacks in the cloud;

- Studies presenting novel security techniques and mechanisms protecting data and application security in the cloud;
- Studies presenting original assurance techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

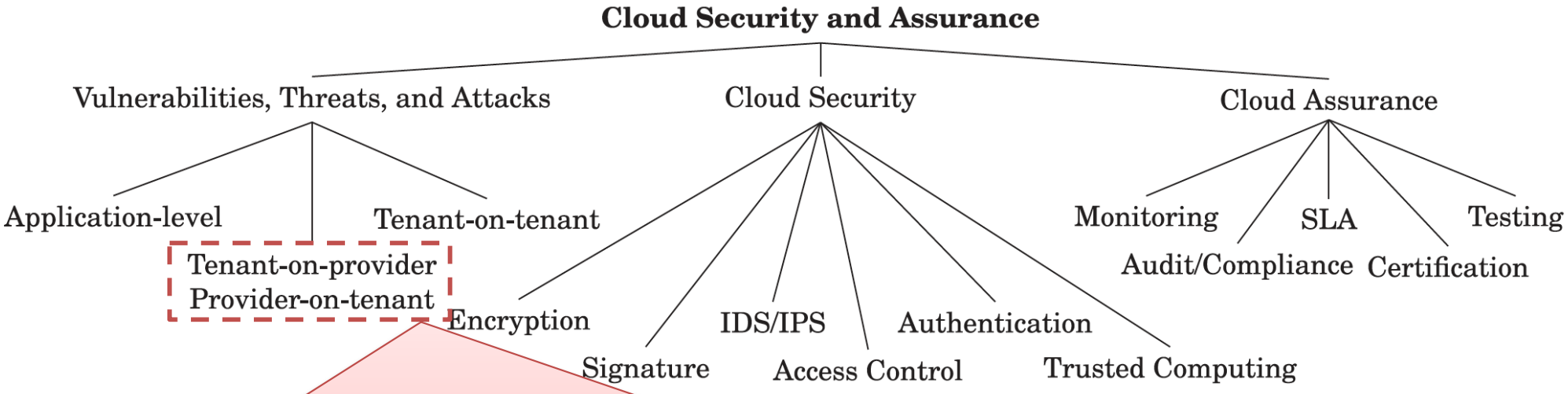
::.. Introduction (2/4)



Attacks are made by malicious cloud tenants on other cloud tenants, and target the PaaS and IaaS levels, including their resources, processes, and data. They are typical of virtualized environments where different tenants share a common infrastructure and may reside on the same physical hardware. A malicious tenant tries to attack other tenants colocated on the same hardware, exploiting misconfiguration and vulnerabilities on the virtualization infrastructure (e.g., Virtual Machine (VM) isolation).

- Studies presenting original assurance techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

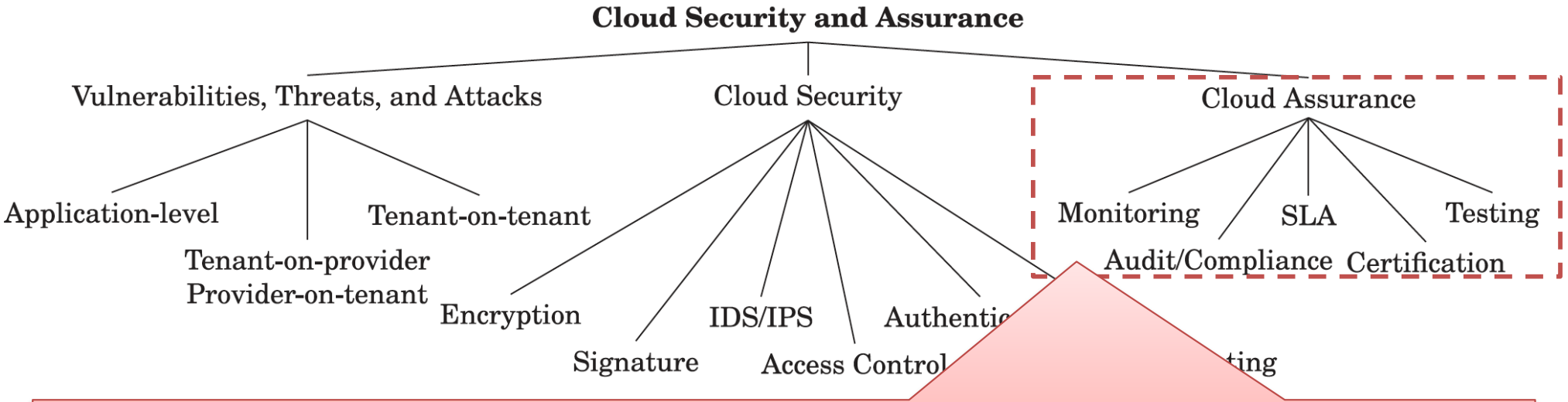
::.. Introduction (2/4)



Attacks are made by malicious cloud providers (tenants, respectively) on target tenants (cloud providers, respectively) and target the IaaS level, including its resources, processes, and data. They are specific of the cloud where users, enterprises, and business owners move their assets to an untrusted infrastructure. The cloud provider is malicious (or at least honest but curious) and attacks its tenants (provider-on-tenant), or one or more compromised tenants (e.g., botnets for denial of service attacks) are used to attack the cloud infrastructure (tenant-on-provider).

- Studies presenting original assurance techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

::.. Introduction (2/4)



Assurance techniques can be used at all layers of the cloud stack to prove the security claims made by a provider on its security mechanisms.

- Studies presenting new security vulnerabilities, threats, and attacks in the cloud;
- Studies presenting novel security techniques and mechanisms protecting data and application security in the cloud;
- Studies presenting original assurance techniques, which are used to verify, prove, and guarantee the properties provided by the implemented security techniques and mechanisms.

::.. Introduction (3/4)

Cloud security problems are very challenging, due to

1. the heterogeneity of cloud stacks,
2. the lack of formal and semantically equivalent security requirements,
3. the lack of a stable categorization of techniques,
4. the need of balancing between security, flexibility, and high performance,
5. the lack of transparency on activities and events happening in the cloud back-end.

In the cloud, it is perfectly possible to have good security and poor assurance. Many times, however, poor assurance goes hand in hand with poor security. More importantly, poor assurance usually prevents proving that security and privacy properties of a process comply with laws and regulations.

::.. Introduction (4/4)

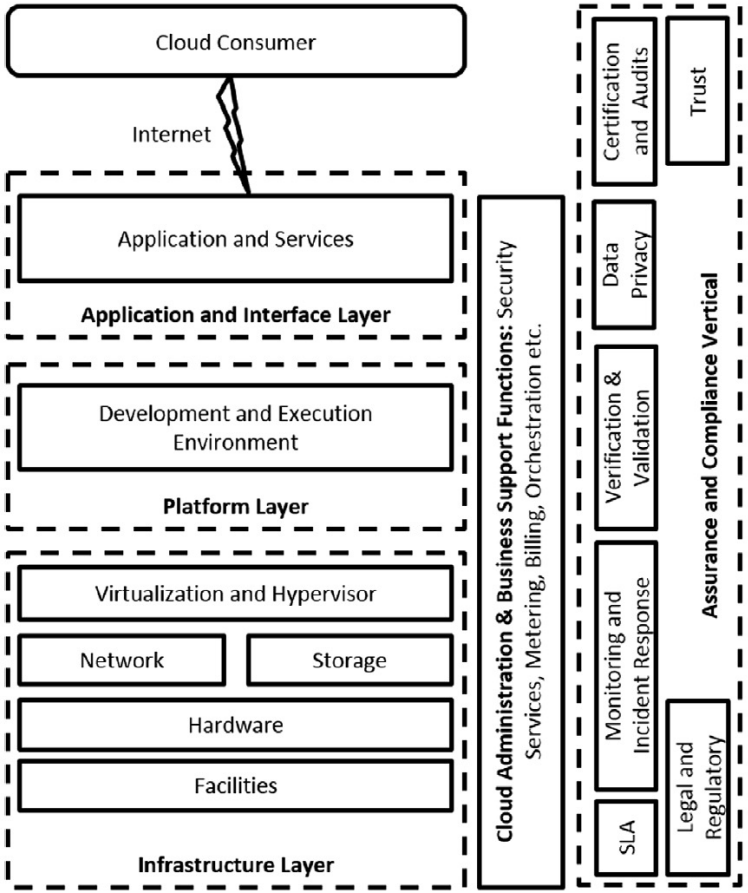
The concept of transparency, that is, higher access to low-level (back-end) data produced by the cloud infrastructure and to evidence collected on the security of cloud data and applications, has been recognized as the basis for an effective approach to cloud assurance.

Cloud providers, following the transparency requirement, should not only show their compliance to standards/regulations and the supported policies, but also explain how they achieve and maintain their compliance levels under the “comply-or-explain” principle.

Transparency is fundamental to support both introspection, that is, the capability of a cloud provider of examining and observing its internal processes, and outrospection, that is, the ability of customers and service providers to examine and observe cloud’s internal processes, involving their activities, data, and applications, for security purposes.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.

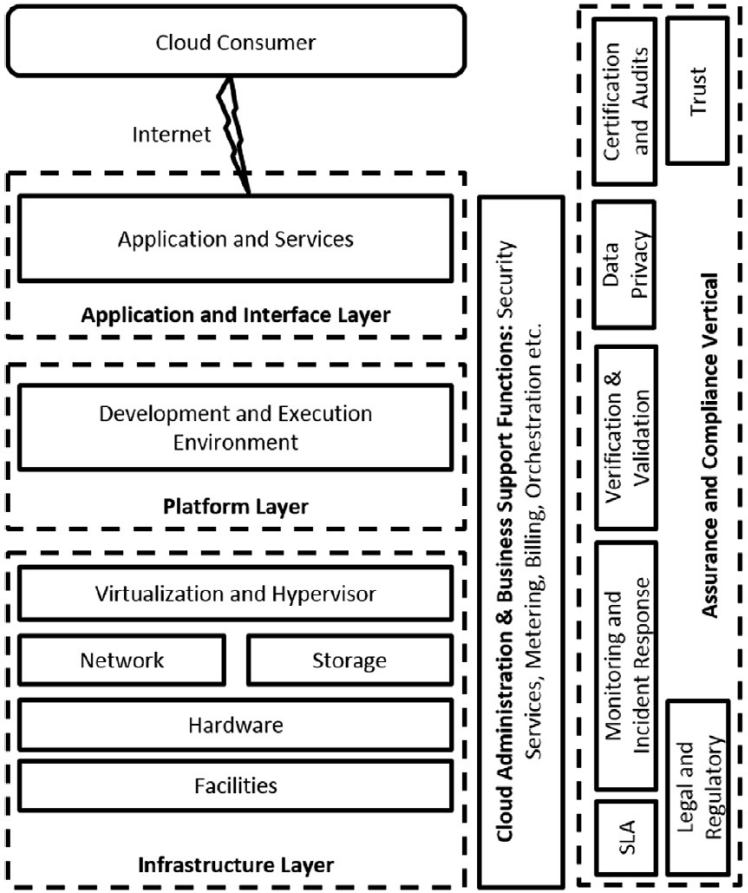


It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill cloud security and privacy requirements.

To understand the security aspects of cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.

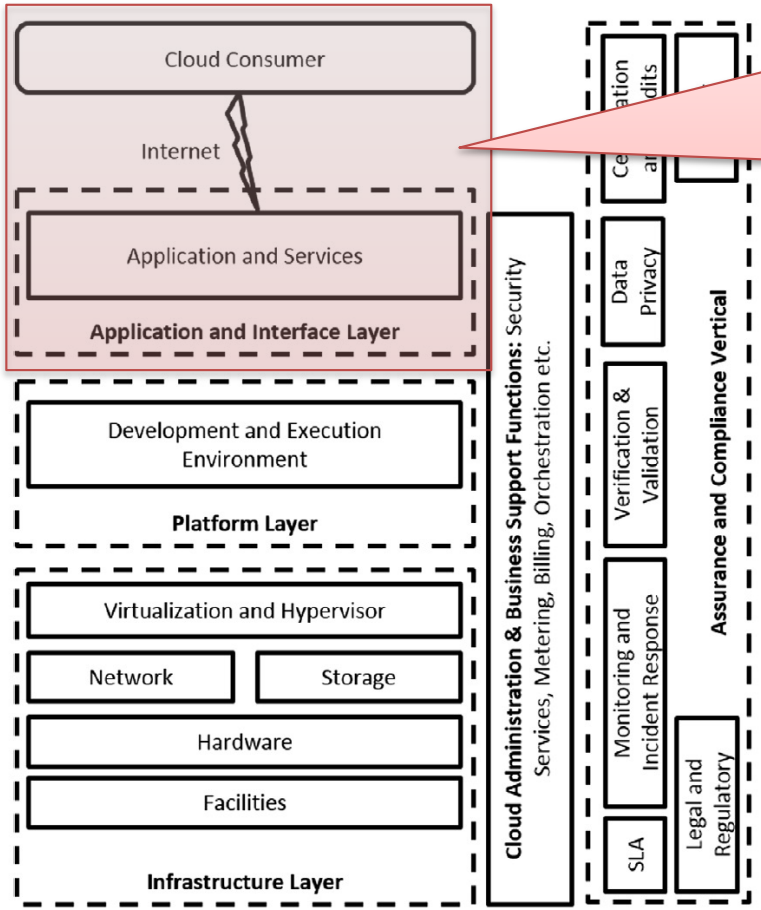


One of the widely used representations of the cloud architecture components is the multi-layered stack model that allows depicting technology associated with each layer representing as-a-service delivery model.
Each layer's component forms an attack surface.

To understand the security aspects of cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.

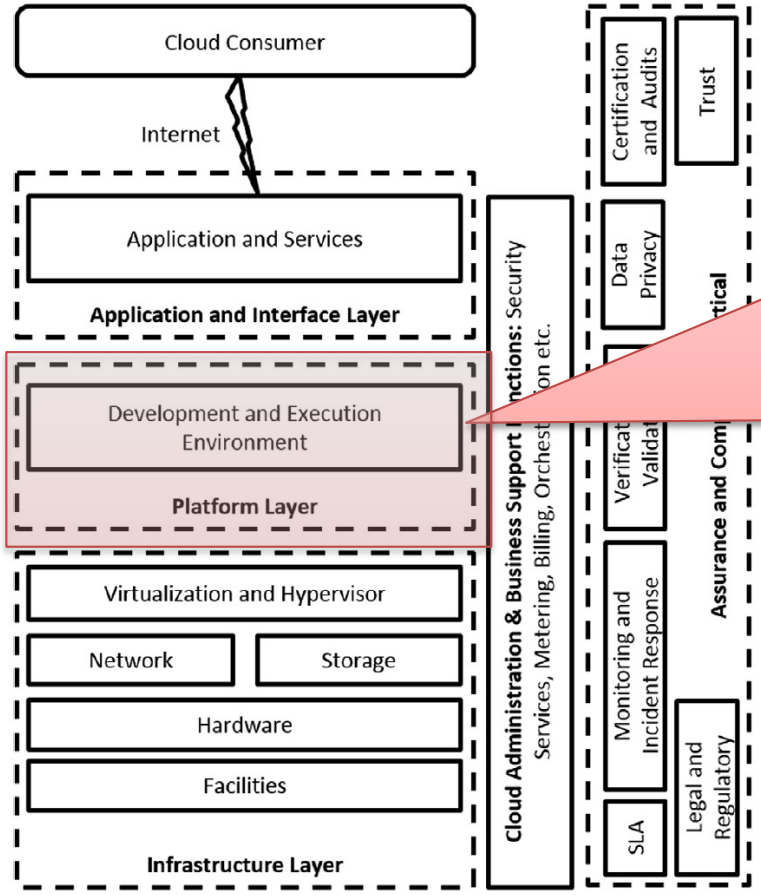


This layer primarily enables SaaS offerings through web services accessed by customers through the Internet. Access to services is secured through user identification, authentication, and authorization, and secure data communication between the service provider and the consumer using appropriate encryption techniques.

To understand the security aspects of cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.

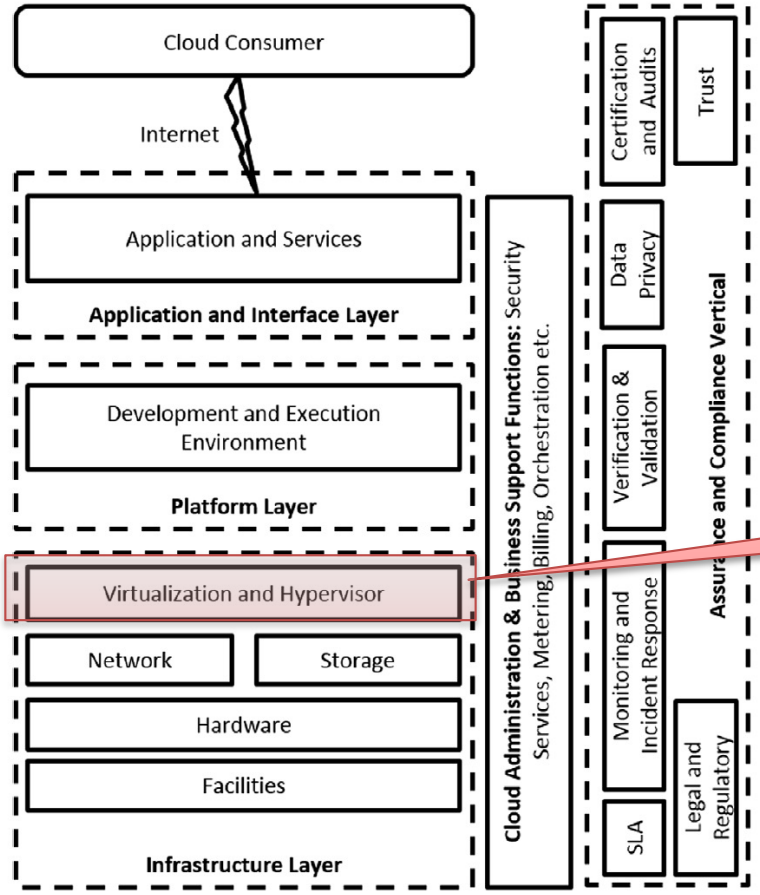


This layer provides software development, testing, deployment, and run-time execution environment to the cloud consumer to develop and deploy its customized application or to install off-the-shelves software applications, customized to suit the end user's requirements. This layer equips the end user with the required operating system and integrated development environment.

cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



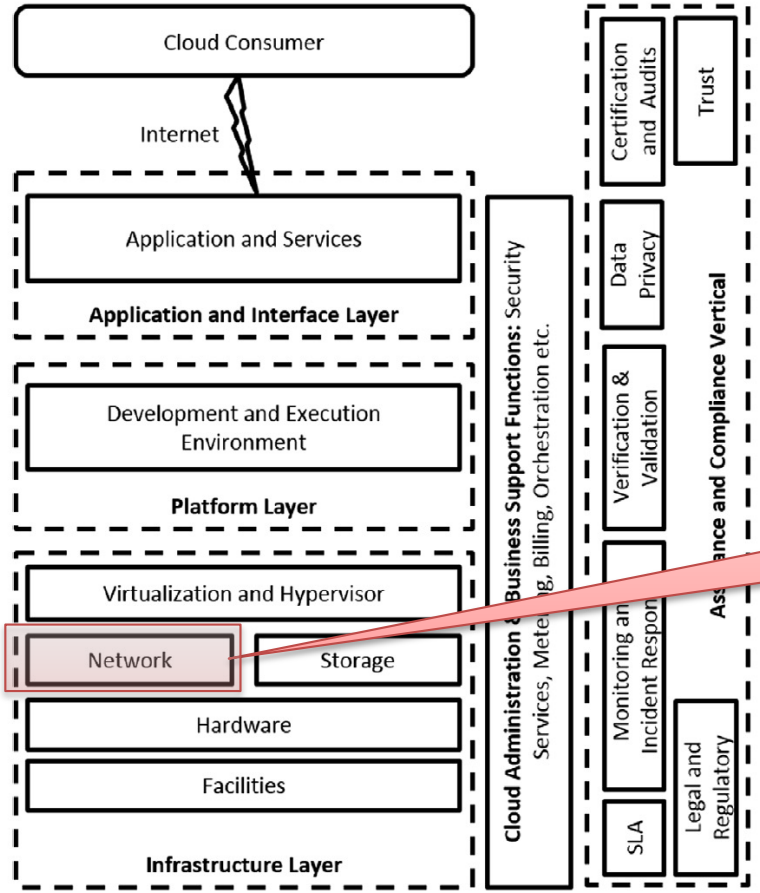
It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill

The hypervisor is a software that works as an abstraction layer to provide a unified and transparent view of underlying physical pooled resources to hosted virtual machines utilizing multiplexing.

cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



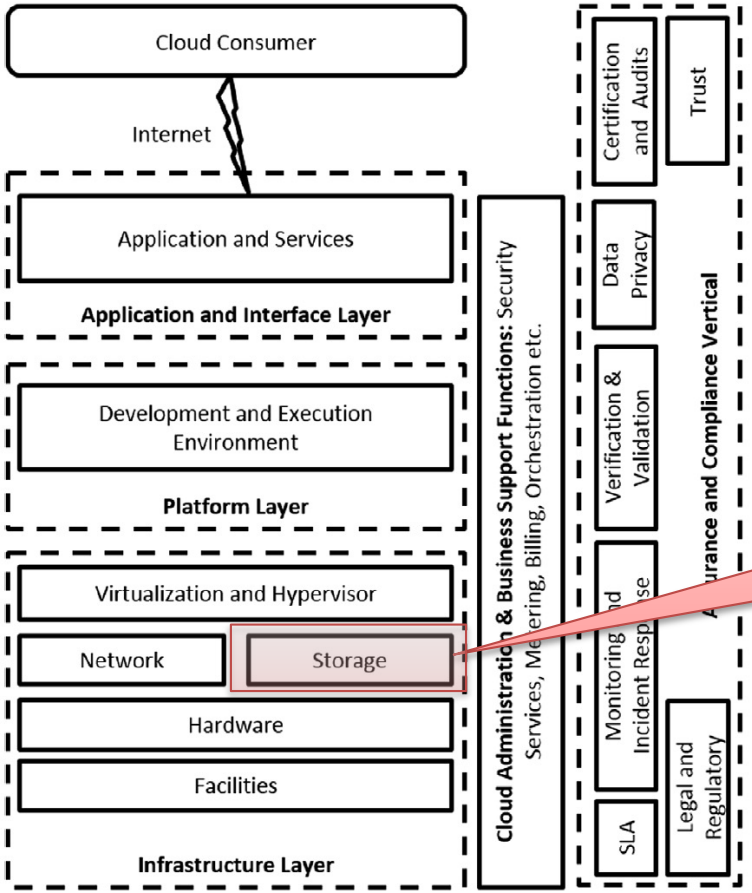
It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill cloud security and privacy requirements.

This component provides services for internal communication among virtualized components.

cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



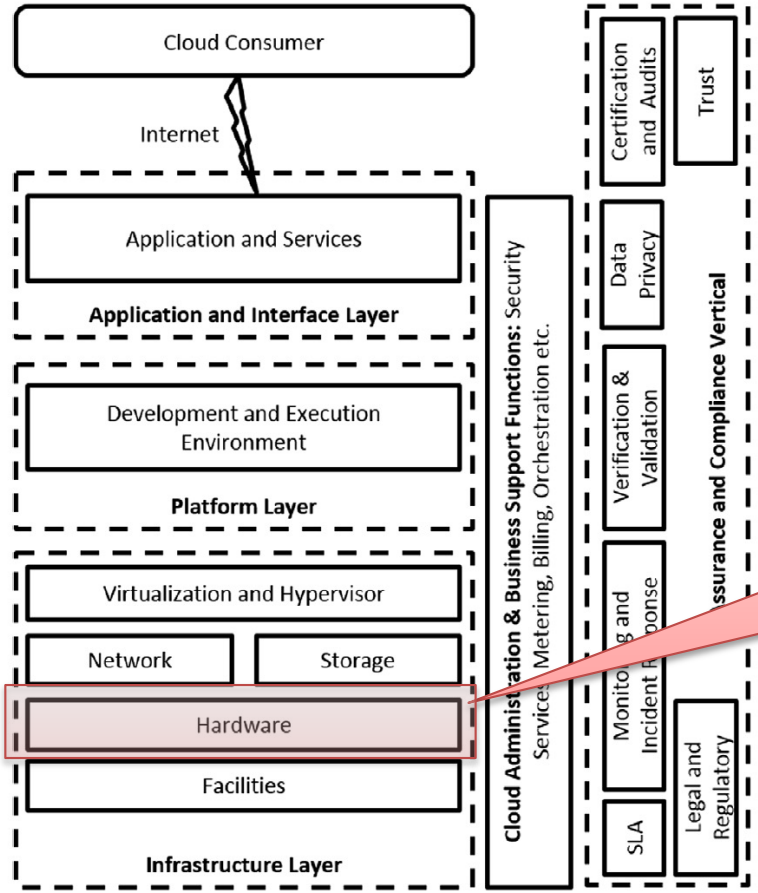
It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill

This component provides services for data storage for user data life cycle management. It is one of the most cared about component of the cloud computing environment.

computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



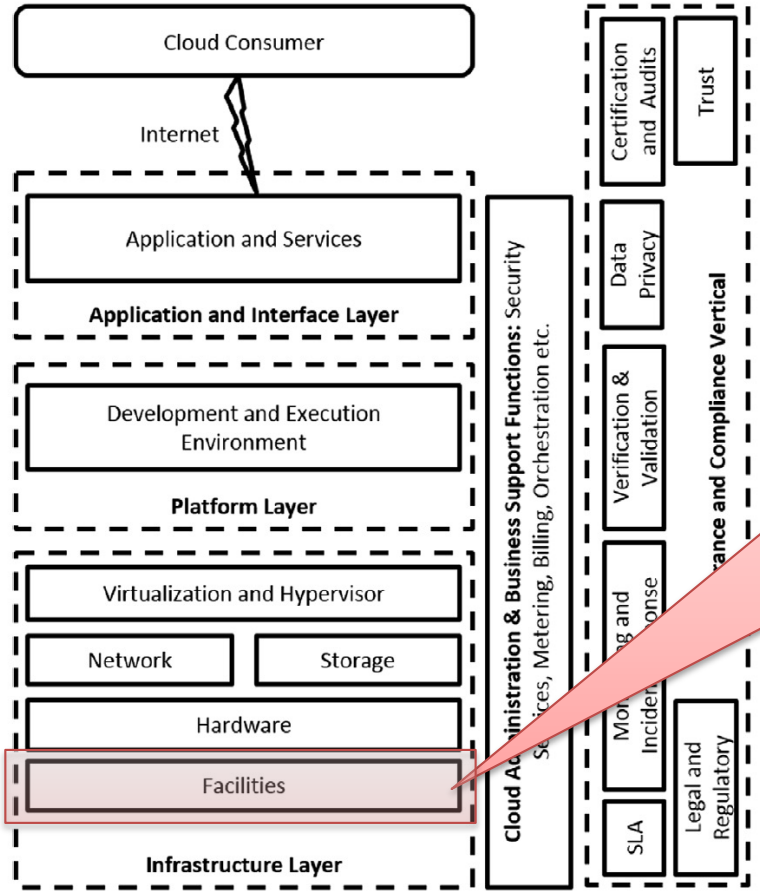
It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill

This layer consists of all the raw computing hardware. Generally, a cloud provider has distributed and heterogeneous set of hardware resources.

computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



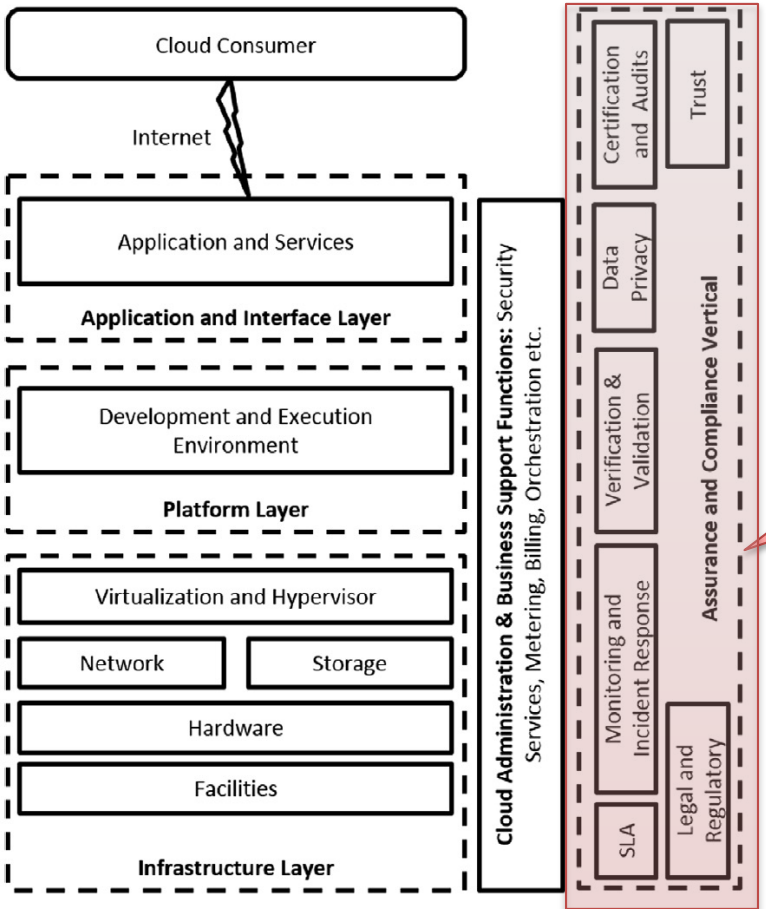
It involves determining countermeasures to address these known vulnerabilities to reduce or eliminate attack vectors to fulfill

This layer is all about the data center and its physical environment management. These aspects do have an impact on data availability and service continuity. At this layer, network access of the installed hardware is controlled by defining appropriate network firewall access control policies.

with the cloud computing system.

::.. Cloud Security Modeling (1/4)

Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.

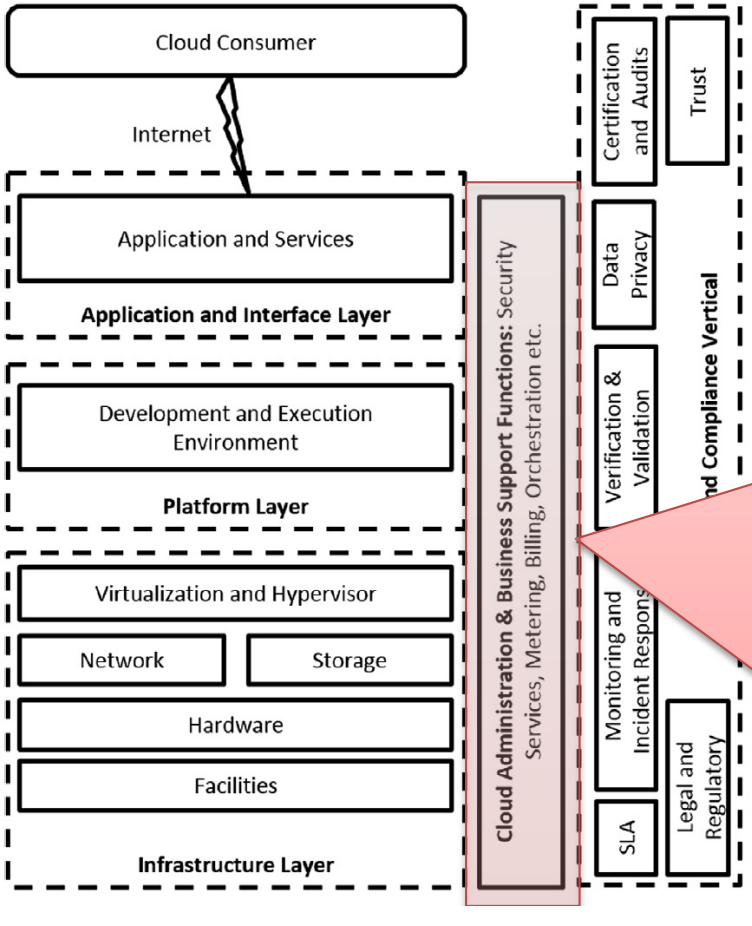


This vertical layer provides critical functionalities to ensure and support the well-functioning of the offered cloud services and cloud environment in totality. It enables to initiate appropriate corrective actions for deviation from expected behavior.

T understand the security aspects of cloud computing, it is required to know the architectural component associated with the cloud computing system.

::.. Cloud Security Modeling (1/4)

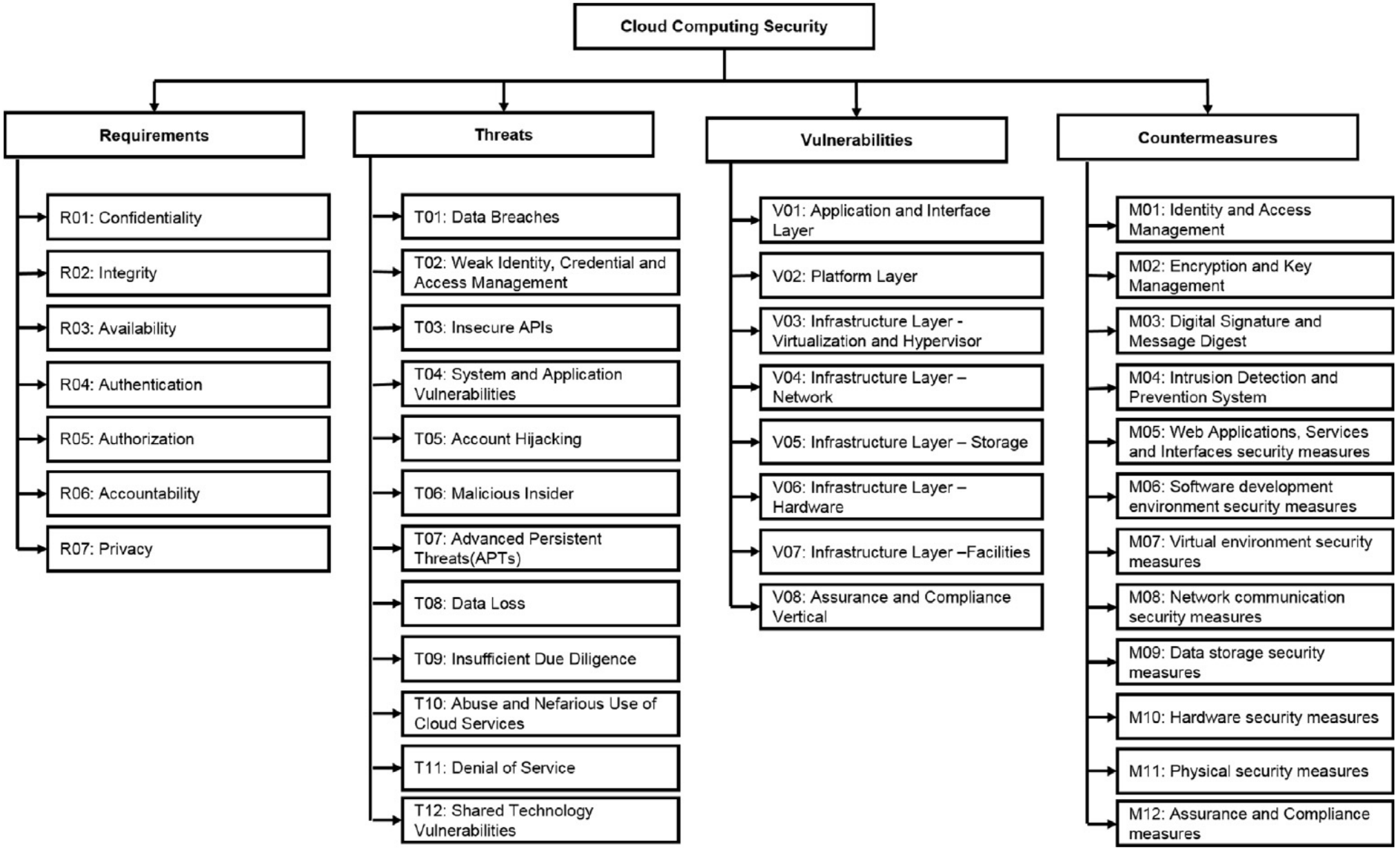
Modeling security involves identifying security requirements, associated threats due to vulnerabilities in cloud architectural components that form the attack vectors and affects the fulfillment of these requirements.



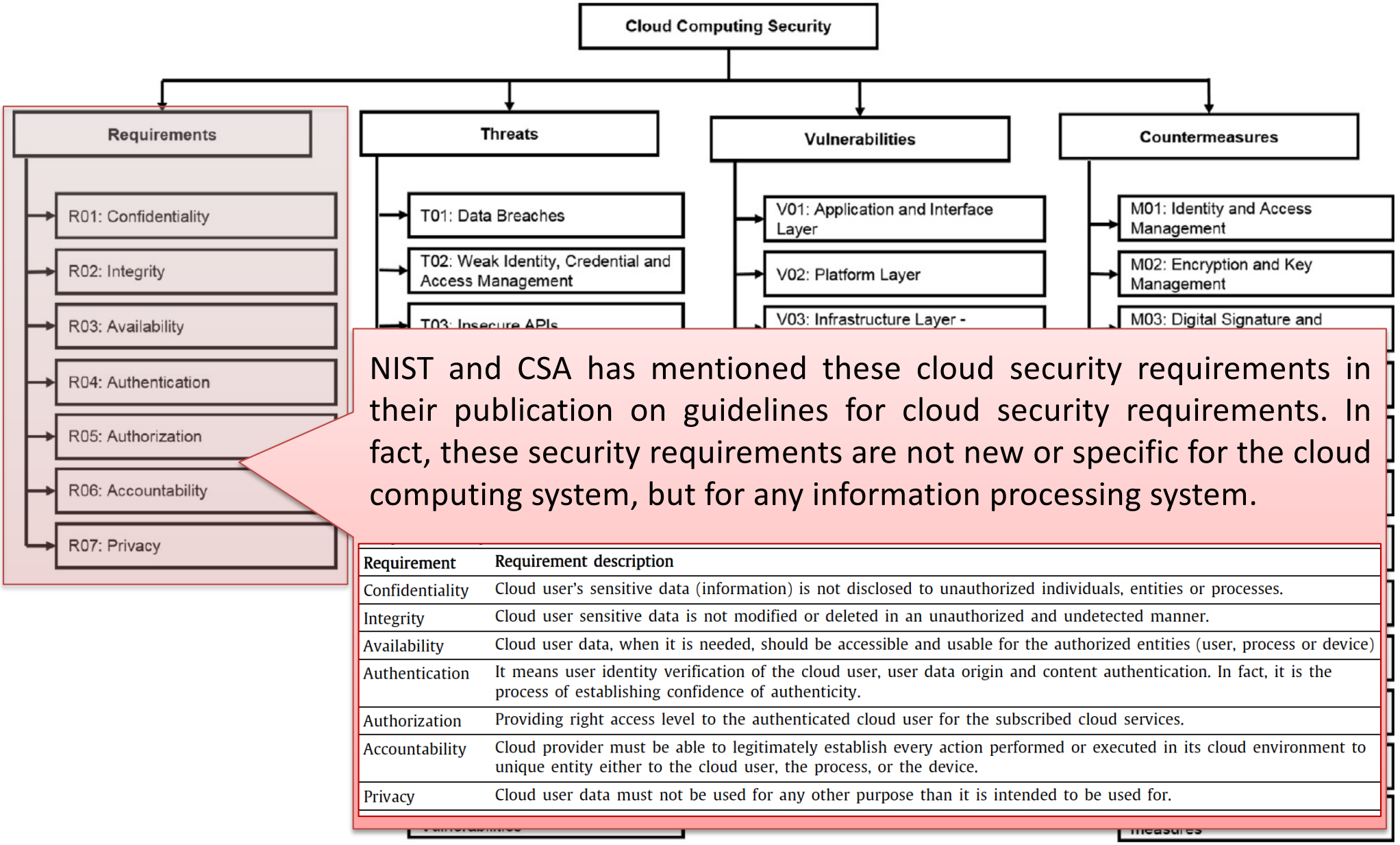
This vertical layer provides shared services to perform cloud administration and business support activities.

- user identification, authentication, and authorization;
- services for cloud orchestration which is primarily a composition of cloud resources in an optimal way to provide best value propositions of services offered to the cloud consumers.
- measuring the service usages and performing the charging and billing for consumed services.
- administrative functions like cloud service deployments, configuration and provisioning apart from needed support for load balancing of the offered services.

::.. Cloud Security Modeling (2/4)



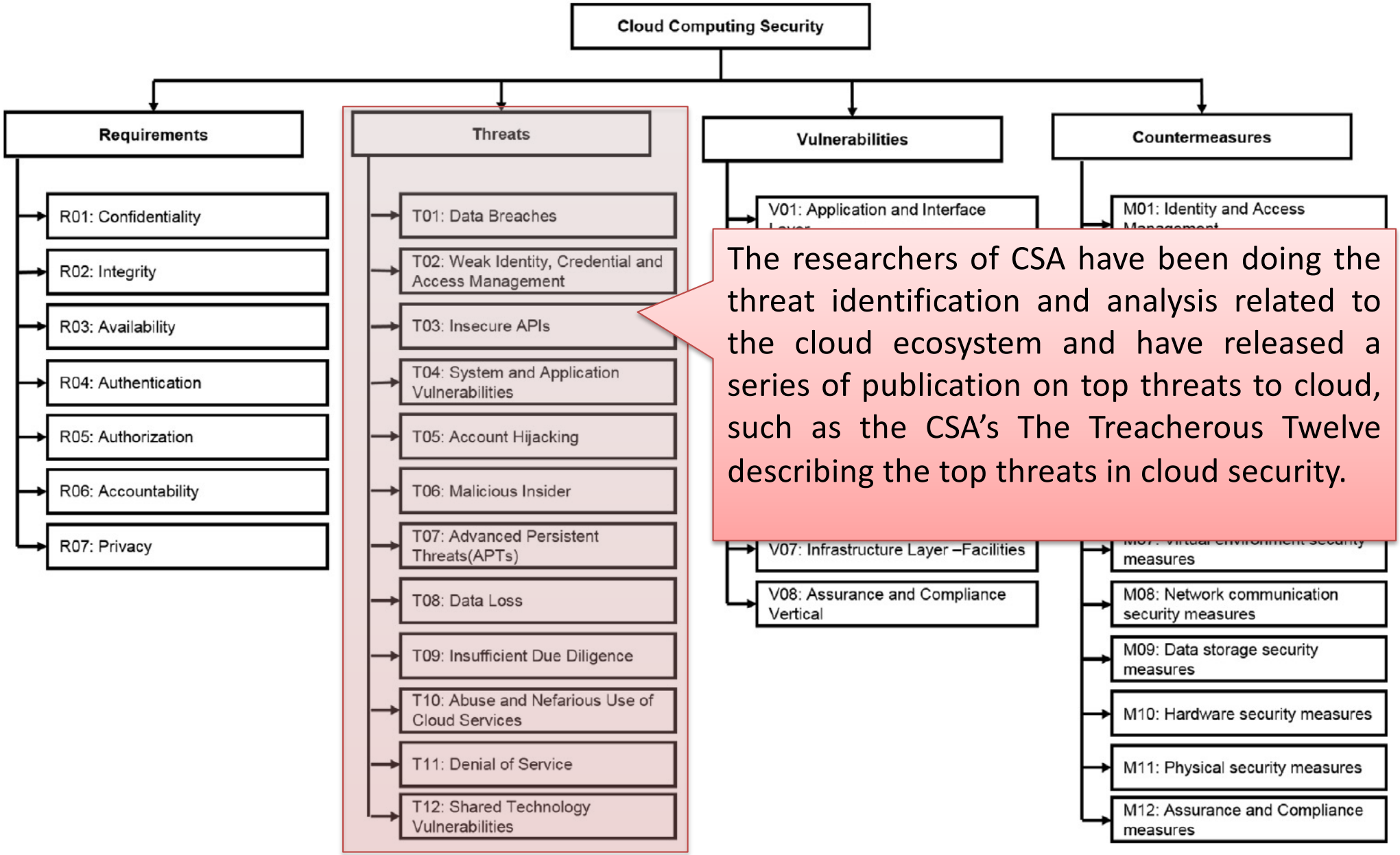
::.. Cloud Security Modeling (2/4)



NIST and CSA has mentioned these cloud security requirements in their publication on guidelines for cloud security requirements. In fact, these security requirements are not new or specific for the cloud computing system, but for any information processing system.

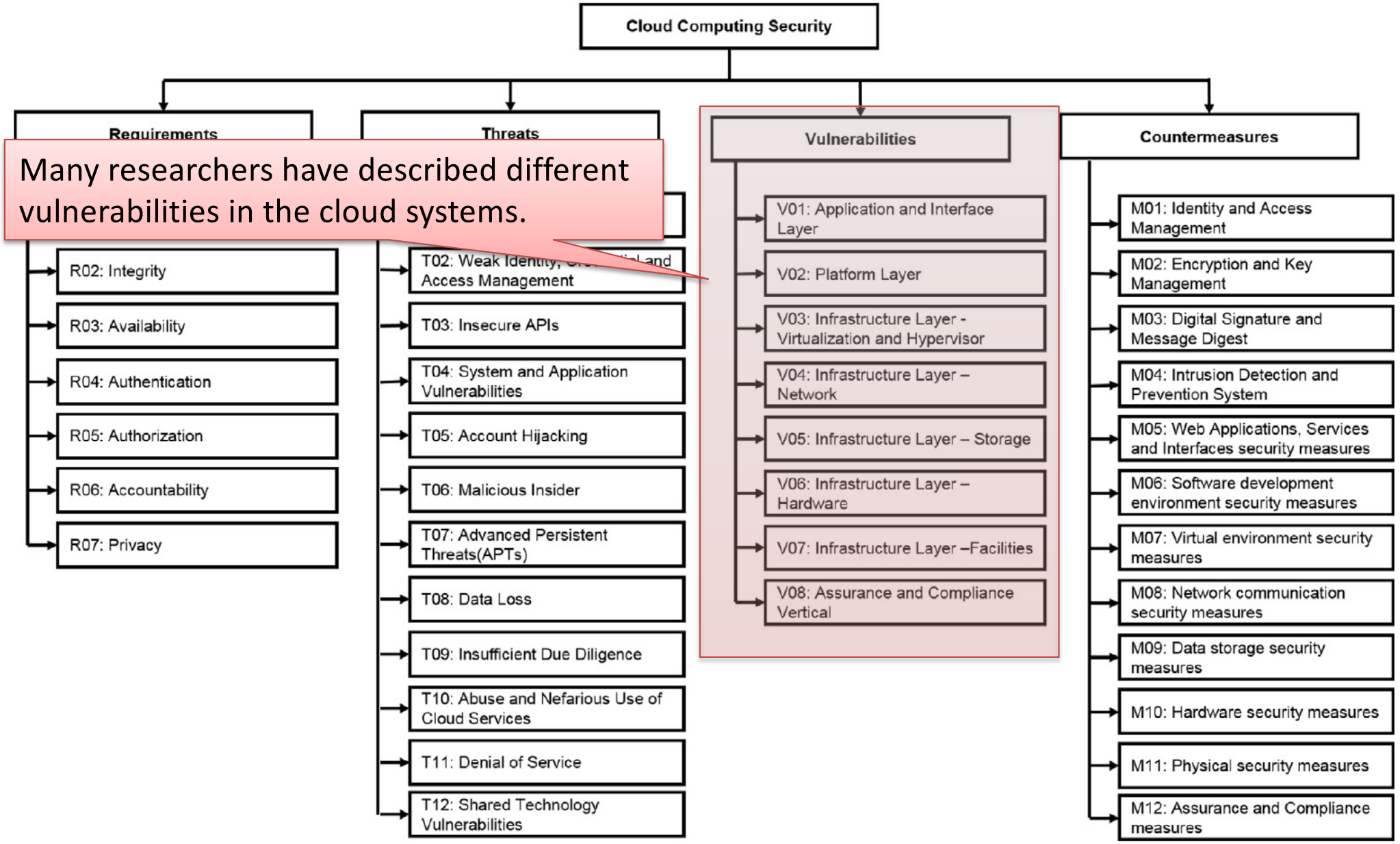
Requirement	Requirement description
Confidentiality	Cloud user's sensitive data (information) is not disclosed to unauthorized individuals, entities or processes.
Integrity	Cloud user sensitive data is not modified or deleted in an unauthorized and undetected manner.
Availability	Cloud user data, when it is needed, should be accessible and usable for the authorized entities (user, process or device)
Authentication	It means user identity verification of the cloud user, user data origin and content authentication. In fact, it is the process of establishing confidence of authenticity.
Authorization	Providing right access level to the authenticated cloud user for the subscribed cloud services.
Accountability	Cloud provider must be able to legitimately establish every action performed or executed in its cloud environment to unique entity either to the cloud user, the process, or the device.
Privacy	Cloud user data must not be used for any other purpose than it is intended to be used for.

::.. Cloud Security Modeling (2/4)

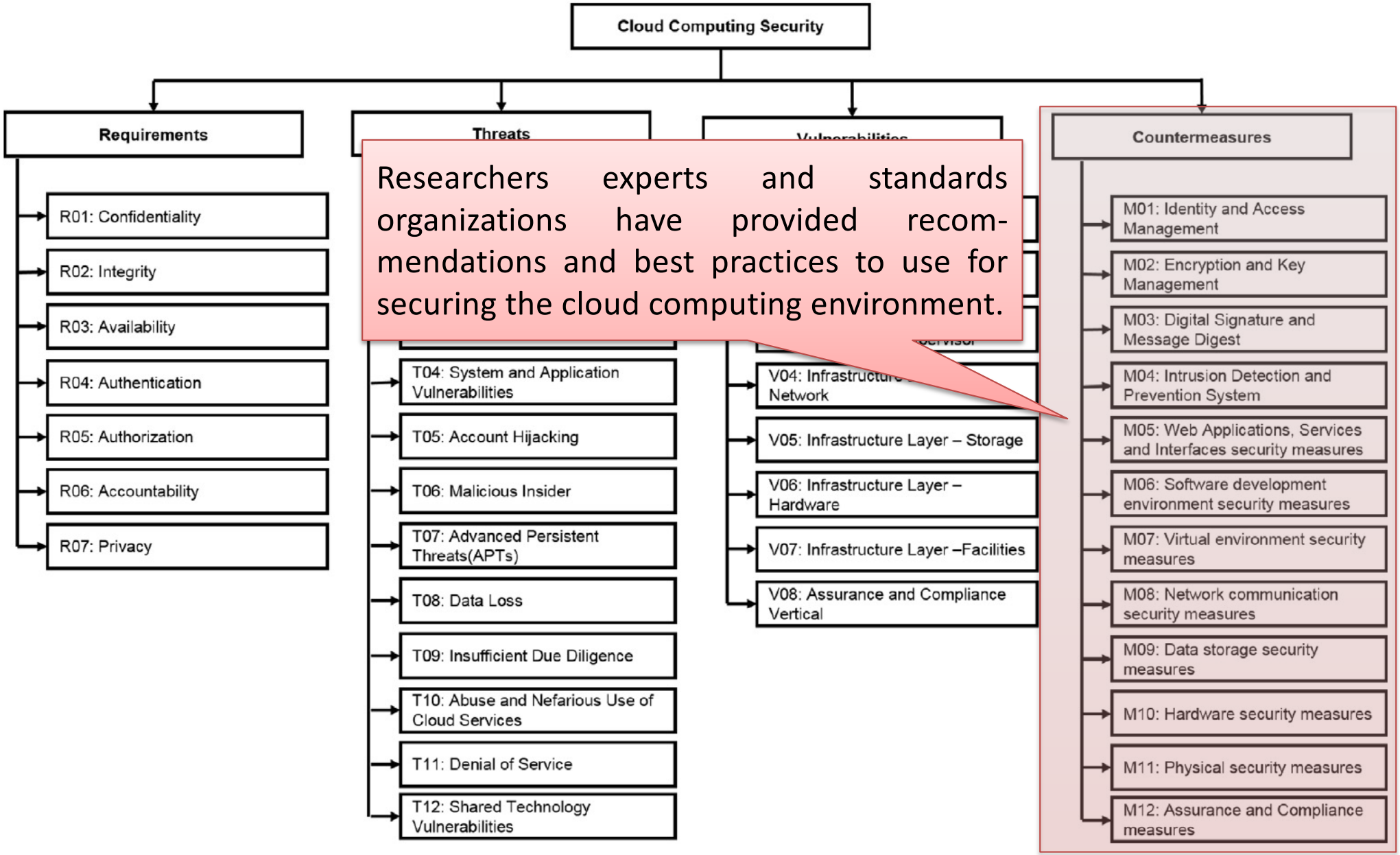


The researchers of CSA have been doing the threat identification and analysis related to the cloud ecosystem and have released a series of publication on top threats to cloud, such as the CSA's The Treacherous Twelve describing the top threats in cloud security.

::.. Cloud Security Modeling (2/4)



::.. Cloud Security Modeling (2/4)



::.. Cloud Security Modeling (3/4)

CSA top threats to cloud computing

Top threats	2010	2013	2016
1	Abuse and nefarious use of cloud computing	Data breaches	Data breaches
2	Insecure application programming interfaces	Data loss	Weak identity, credential and Access management
3	Malicious insiders	Account hijacking	Insecure APIs
4	Shared technology vulnerabilities	Insecure APIs	System and Application Vulnerabilities
5	Data loss/Leakage	Denial of Service	Account hijacking
6	Account, Service & Traffic hijacking	Malicious Insiders	Malicious Insiders
7	Unknown Risk Profile	Abuse of Cloud Services	Advanced Persistent Threats (APTs)
8	–	Insufficient Due Diligence	Data loss
9	–	Shared Technology Issues	Insufficient Due Diligence
10	–	–	Abuse and Nefarious Use of Cloud Services
11	–	–	Denial of service
12	–	–	Shared technology vulnerabilities

::.. Cloud Security Modeling (3/4)

CSA top threats to cloud computing

Top threats	2010	2013	2016
1	Abuse and nefarious use of cloud computing	Data breaches	Data breaches
2	Insecure application programming interfaces	Data loss	Weak identity, credential and Access management
3	Malicious insiders	Account hijacking	Insecure APIs
4	Shared technology vulnerabilities	Insecure APIs	System and Application Vulnerabilities
5	Data loss/Leakage	Denial of Service	Account hijacking
6	Account, Service & Traffic hijacking	Malicious Insiders	Malicious Insiders
7	Unknown Risk Profile	Abuse of Cloud Services	Advanced Persistent Threats (APTs)
8	–	Insufficient Due Diligence	Data loss
9	–	Shared Technology Issues	Insufficient Due Diligence
10	–	–	Abuse and Nefarious Use of Cloud Services
11	–	–	Denial of service
12	–	–	Shared technology vulnerabilities

Cloud computing treacherous 12 top threats

Rank	Threat	Threat description
1	Data breaches (T01)	It means releasing, viewing, stealing or using of sensitive, protected or confidential information by any party for any purpose which was not authorized to do so. Any information leaked that was not intended for public release may come under the purview of data breaches like personal health information, personally identifiable information (PII), etc. The extent of damage due to data breaches could be determined based on the sensitivity of the breached information.
2	Weak identity, Credential and Access Management (T02)	It results in attackers masquerading as legitimate users and getting unauthorized access to data resulting into data breaches which potentially damaging to the owner of data and associated stakeholders.
3	Insecure APIs (T03)	For monitoring, provisioning, orchestration, and managing the allocated resources, cloud consumers are provided with application programming interfaces (APIs) and/or user interfaces (UIs) which exposes the cloud computing environment to the external world and potentially to attackers. These UIs and APIs are generally designed and implemented using web services which have inherent vulnerabilities. These APIs can be further used to build value-added services which might further dilute the user's credentials to the third party.
4	System and Application Vulnerabilities (T04)	This threat appears due to bugs in the system and application software which could be exploited by the attackers to steal data and take control of the systems' operation. Vulnerabilities in libraries, kernel and application tools of an operating system put all services and data at the security risk. The feature like multi-tenancy creates yet another attack surface as it needs usage of shared memory and resources among different systems of organizations, hosted in the same cloud environment.

::.. Cloud Security Modeling (4/4)

Cloud computing treacherous 12 top threats

Rank	Threat	Threat description
5	Account Hijacking (T05)	This is the traditional threat of any computer system and so is in the cloud computing environment which means gaining access to a system by hacking credentials and password of a legitimate user. From the cloud perspective, if attackers hijacked a user's account, they can redirect clients to illegitimate sites, manipulate data, return falsified information, and eavesdrop on activities and transactions.
6	Malicious Insiders (T06)	A malicious insider is a current or former employee or any business partner that has or had authorized access to information system creates threat if he or she intentionally misused that access to negatively impact the security and privacy aspects of the information system.
7	Advanced Persistent Threats (APTs) (T07)	APTs refer to a higher degree of sophisticated attack which is of very much of specific purpose and aimed to specific target. These attacks are difficult to eliminate as they adapt to deployed security measures while pursuing their goals over an extended period.
8	Data loss (T08)	Data can be lost other than malicious attacks as well, like accidental deletion or unfortunate damage or physical catastrophe like fire, earthquake, flood, etc., which may lead to permanent loss of stored outsourced data unless it is backed up to some alternate safe location which can be made accessible to the legitimate consumer.
9	Insufficient Due Diligence (T09)	While making a choice and decision for selection for cloud technology to use and cloud provider to provide services to host business functions the selection committee must consider many factors. Lack of proper approach and plan for conducting due diligence leads to security risks.
10	Abuse and Nefarious Use of Cloud Services (T10)	It is potentially caused due to unaccounted, mismanaged, fraudulent, free trails user accounts and poorly secured cloud deployments that allows attackers to access the computing resources and misuses it to target victims. Launching distributed email spam, denial-of-service attacks, and phishing campaigns are some of the examples of misuse of cloud-based resources.
11	Denial of Service (T11)	It simply means legitimate users are prevented from accessing their data and application due to slow response or simply no availability of the cloud resources. An attacker causes system slowdown by forcing the target cloud service to consume more than allocated finite system resources and virtually resulting in no access to legitimate users.
12	Shared Technology Vulnerabilities (T12)	Sharing technology, either for infrastructure, platforms or applications, is the basic characteristics of the cloud computing system. The components which facilitate sharing of technology are, generally, not designed to offer an effective isolation property for a multi-tenant environment where applications of multiple customers are hosted together. This potentially can lead to shared technology vulnerabilities like flaws in hypervisors.

::.. Cloud Vulnerabilities (1/13)

Vulnerabilities in application and interface layer reflect the issues related to the entry point to access the services of a cloud provider, mostly through the Internet. This is as vulnerable as the flaw and weaknesses in web technologies used, including the Internet.

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

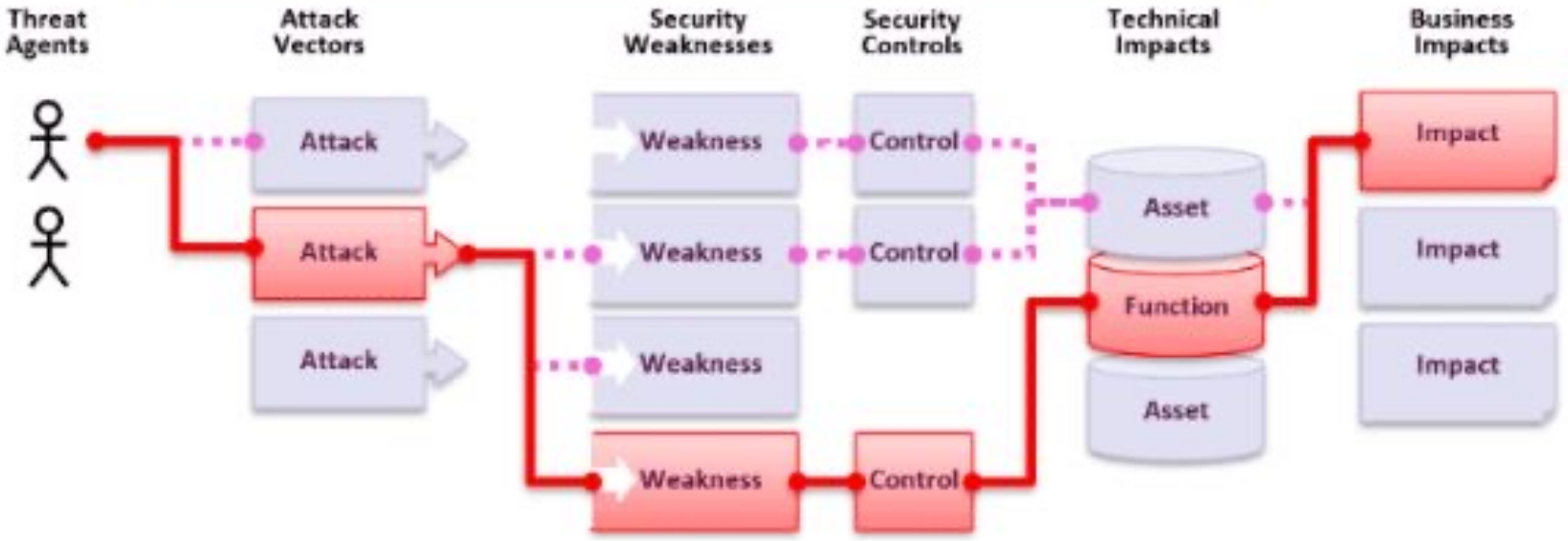
Ten most critical web application security threats identified by the Open Web Application Security Project (OWASP) is as well applicable to the cloud computing environment.

The ranking is based on data collected within the community, classifying the risks according to the OWASP Risk Rating Methodology and assigning a 3-level ranking.

::.. Cloud Vulnerabilities (2/13)

The raking criteria are for the following criteria: Attack Difficulty (Exploitability), Risk Prevalence, Risk Detection (Detectability), and Technical Impacts.

Threat Agents	Risk Exploitability	Risk Prevalence	Risk Detectability	Technical Impacts	Impacts in the Activity
Application Specific	Easy	Generalized	Easy	Severe	Activity /application specific
	Moderated	Common	Moderated	Moderated	
	Hard	Rare	Hard	Little	



::.. Cloud Vulnerabilities (3/13)

RISK	Threat Agents	Attack Vectors: Exploitability	Security Weakness: Prevalence	Security Weakness: Detectability	Impacts: Technical	Impacts: Business	Score
A1:2017-Injection	App Specific	EASY 3	COMMON 2	EASY 3	SEVERE 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY 3	COMMON 2	AVERAGE 2	SEVERE 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE 2	WIDESPREAD 3	AVERAGE 2	SEVERE 3	App Specific	7.0
A4:2017-XML External Entity (XXE)	App Specific	AVERAGE 2	COMMON 2	EASY 3	SEVERE 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE 2	COMMON 2	AVERAGE 2	SEVERE 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY 3	WIDESPREAD 3	EASY 3	MODERATE 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY 3	WIDESPREAD 3	EASY 3	MODERATE 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT 1	COMMON 2	AVERAGE 2	SEVERE 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE 2	WIDESPREAD 3	AVERAGE 2	MODERATE 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE 2	WIDESPREAD 3	DIFFICULT 1	MODERATE 2	App Specific	4.0

::.. Cloud Vulnerabilities (4/13)

Platform layer provides development and deployment tools, middleware and operating system, so that the vulnerabilities decide the security level of this layer in developed custom software and the underlying operating system.

- Insufficient and incomplete verification and validation of the software deployed at the platform layer leads to vulnerabilities. Most of the time security aspects are underestimated or ignored in the software development life cycle.
- Security issues in a software application are, generally, due to vulnerable programming codes and causes increased exploitation. Non compliance to best coding practices and guidelines by the programmers introduces vulnerabilities in code.
- Applications communicate with hardware through system calls, and thay may have access to all the data in a virtual machine. So, any malicious services running in the background may lead to data leakage.

::.. Cloud Vulnerabilities (5/13)

- Malicious system admin can bring down whole OS software. Inappropriate system resource allocation and monitoring adversely impact system performance and availability.
- Inappropriate memory isolation may lead to data leakage. Incomplete and insufficient OS monitoring leads to malicious actions to go un-noticed.

Virtualization and hypervisor technologies are critical enabling technologies for cloud systems, which may be affected by vulnerabilities. Apart from traditional vulnerabilities, cloud-specific characteristics and processes, like VM image, VM migration, VM rollback, and multitenancy as well have witnessed vulnerabilities.

::.. Cloud Vulnerabilities (6/13)

- The traditional data center perimeter-security measures like firewalls, network segmentation, Demilitarized Zones (DMZ), network monitoring tools and Intrusion Detection and Prevention Systems (IDS/IPS) are not enough to secure the virtual machines as each virtual machine has its OS and application hosted on a shared hardware with other co-located virtual machines.
- A publisher of VM image has a risk of releasing sensitive information and a retriever has a risk of running a vulnerable or malicious VM image as it might have contaminated while at rest.
- VM migration as the process of relocating a VM from one physical server to another without shutting down the VM. This important feature might result into man-in-the-middle (MiM) and insider attack and other related security vulnerabilities like information disclosure.

::.. Cloud Vulnerabilities (7/13)

- VMs could be rolled back to its previous state if needed so. However, this re-surface the previous security vulnerabilities patched out or restores disabled security credentials. A rollback can also revert to previous configuration error and outdated security policy. Also, to enable the rollback a copy of the VM image is maintained which can result in propagation of configuration errors and other vulnerabilities.
- In Multi-tenancy architectures, co-located services and hosts may result in targeted cyber-attacks which is a superset of advanced persistent threat (APT).
- Also, multi-tenancy may result in violation of integrity, as sharing computing resources to multiple tenants may allow malicious users to launch attacks on data under processing by another tenant.

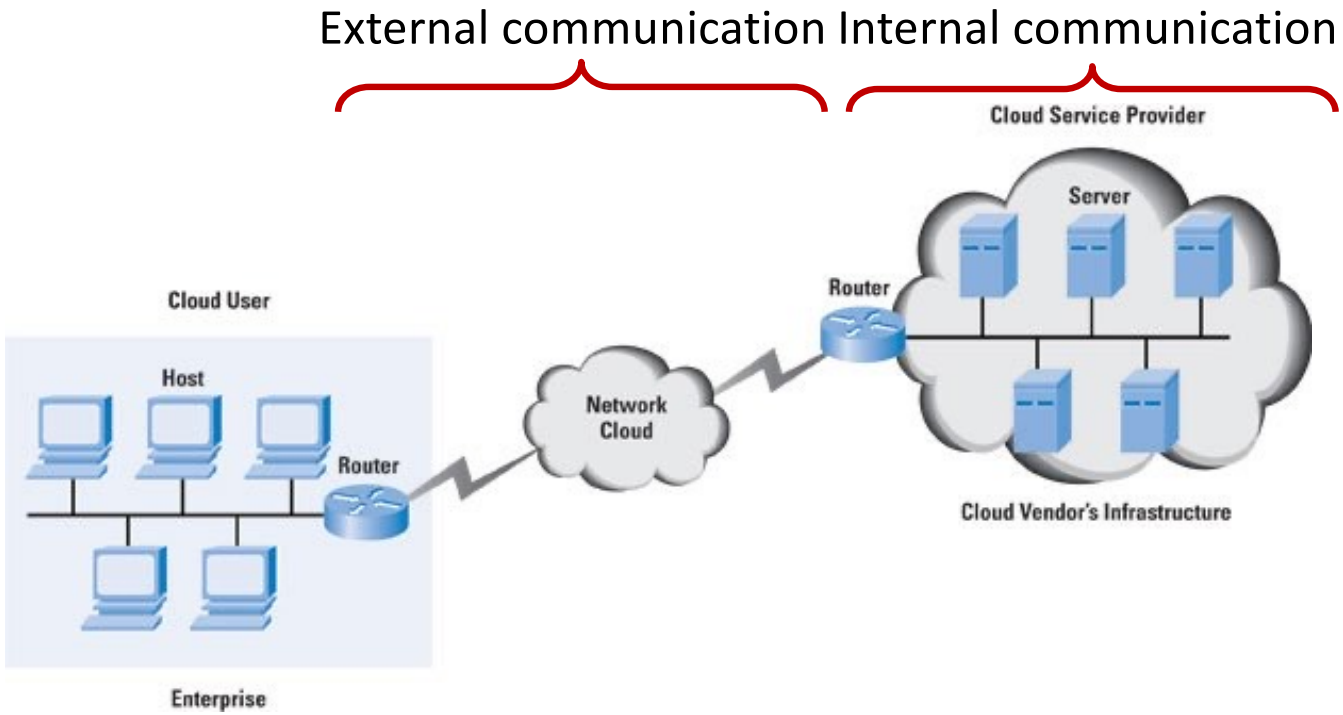
::.. Cloud Vulnerabilities (8/13)

- A hypervisor is a software that manages the VMs and enables multiple operating systems to run concurrently on the same hardware. A hypervisor, like any other cloud components, suffers through security and privacy challenges. A threat of VM escape can lead to bringing down the hypervisor itself and illegitimate access to other VMs.
- A compromised hypervisor can bring all the associated VMs to a halt or non-functioning as it exposes the larger attack surface. The large code base of hypervisors exposes them for the software related vulnerabilities, and isolation, inspection and interposition properties are yet to be achieved in hypervisors.

Cloud network communication can be put under two classes:

::.. Cloud Vulnerabilities (9/13)

- External communication involves communication external to the cloud, i.e. between cloud components and consumers, which happens over the Internet.
- Internal communication involves communication within cloud components and VMs over virtual network communication channels.



So, vulnerabilities of protocols and technologies associated with the Internet and virtual network is inherent to the cloud network infrastructure.

::.. Cloud Vulnerabilities (10/13)

Huge storage capacity, high availability and stable performance make online storage services very exciting. At the same time, it poses security challenges due to lack of transparency and direct control over the data stored in the cloud environment.

- Poor key management, faulty, insecure and obsolete encryption algorithm makes data storage vulnerable to security attacks.
- Data stored within a cloud environment is always under threat of being tampered by outsiders and insiders. Data in cloud storage (data-in-rest) is vulnerable to unauthorized access due to a shared environment, compromised keys and application vulnerabilities.
- Cloud computing environment, generally, is distributed over multiple geographical locations to meet the cost-effectiveness, scalability, redundancy, disaster recovery, and other requirements. Local legal and regulatory policies affect the security and privacy of user data.

::.. Cloud Vulnerabilities (11/13)

- The backup storage is vulnerable for unauthorized access and tampering, and the dynamic allocation and sharing of the resources invite unique security challenge in terms of data recovery vulnerabilities, of the previous user by the newly allocated user.
- Data sanitization is about the destruction of media containing cloud user data, especially user sensitive data. Improper sanitization leads to security risks: it might not be feasible to destroy the storage media as the associated hardware might still be in use by other tenants, and so there are associated risk of information disclosure.

Virtualized hardware can lead to a partial or complete outage of the cloud system. There are more security risks in using the shared hardware than the dedicated hardware.

::.. Cloud Vulnerabilities (12/13)

Cloud computing resources are placed physically in facilities, known as data centers. These facilities are vulnerable to malicious insiders, natural disasters, poor infrastructure support (like bad cooling, power management, etc.) and inappropriate design.

Assurance and compliance provide a framework to evaluate the level of security a provider provides while delivering the cloud services. More the assurance level of security a user finds in its provider, more the trust relationship strengthens between them.

- A weak SLA may result in SLA violations which in turn negatively affects the trust in cloud services and its provider.
- From a security perspective, weakness in monitoring and audit of user activity logs might result in security incidents, and then prompt actions on those security incidents become inevitable.

::.. Cloud Vulnerabilities (13/13)

- Conventional testing methodology is not sufficient for cloud-based applications and services.
- There is a need for certifications of the cloud providers by a third party. Almost all the key characteristics of cloud poses problems for compliance with legal and regulatory obligations, mainly related to determining which jurisdiction's law applies to hosted data lifecycle and data privacy law.
- Most of the cloud solutions lack support for forensic investigations. Many challenges arise with respect to data provenance in the cloud to support forensic investigations. The availability of log files is essential for any audit compliance and forensic investigation to establish the accountability of any event that occurred within the identified scope of cloud computing environment

::.. Cloud Security Means (1/9)

Many solutions have been introduced so as to provide cloud security to countermeasure known vulnerabilities:

- Identity and access management involves management of user identity, user authentication and user authorization at all levels of cloud environment. User identity management mostly involves password management which involves enforcing a strong password with strict life-cycle management procedures, covering change, resetting and expiration policy for passwords.
- Encryption mechanisms are used to cater to data security and privacy requirements of confidentiality, integrity in combination with message digest, and both authentication and accountability in combination with a digital signature. There might be different encryption mechanisms for data in-store, data in-process and data-in-transit.

::.. Cloud Security Means (2/9)

- To process the encrypted data, a cloud provider needs to decrypt the ciphered data that raises privacy concerns. To address this, fully homomorphic encryption is used to perform arbitrary operations on encrypted data without decrypting it.
- Message Digest, Digital Signature and Message Authentication Code (MAC) are the mechanisms to ensure authenticity, integrity, and non-repudiation of data/messages exchanged between any communicating parties and so is recommended to be used in the cloud system.
- Intrusion detection and prevention is used for identifying anomalies based on the analysis of the traffic patterns and activities to detect the possibilities of different attacks. For cloud systems, intrusion detection and prevention system is required both at the network level and at VM instance level.

::.. Cloud Security Means (3/9)

- Cloud applications and operations (like service provisioning, administration, and orchestration) heavily rely on web services as a core enabling technologies and WS-Security is used to countermeasure the vulnerabilities in web services communication. The best way to counter web services and web client vulnerabilities is to develop a more security robust web applications and for that the software development teams must have adequate security training.
- To develop a consistent and high-quality software system, certain characteristics needs to be taken into consideration, right from concept formation to software delivery. Software development environment security measures must be religiously followed to achieve the functional and non-functional requirements.

::.. Cloud Security Means (4/9)

- Virtual machines and their images, shared hardware and other resources, hypervisors and virtual network for internal communications together form the virtual environment. All these components have the associated vulnerabilities, and cloud provider needs to implement countermeasures to secure them.
  - Virtual Trusted Platform Module provides cryptographic and secure storage functions of TPM to operating systems and applications running on virtual machines, and offers a closed, confidential execution environment to attest the cloud provider before launching the service execution.
  - The easiest approach to safeguard a guest VM is to allow hypervisor to know guest VMs's operating system so that it can monitor and analyze the activities at the guest VM. However, this may not be feasible always as provider might not get the guest VM details from the user.

::.. Cloud Security Means (5/9)

  - Virtual Image security can be provided by a management system, that has four measures for protection of VM Images – a framework for access control to regulate sharing of VM images, remove unwanted information in the image by applying appropriate image filters before putting it in use, a provenance tracking mechanism to track performed operations on an image and a set of repository maintenance services, like virus scanning and security patching, to ensure secured usability of the VM images.
- A series of recommendations have been done for the VM migration and rollback security, such as deletion of VM images, after migration, as attackers can recover data from old disks, remote attestation to verify the security requirements at destination host for migration and a trusted communication channel between the source and destination.

::.. Cloud Security Means (6/9)

- CSA guideline recommends cloud provider should take appropriate security measures to protect data in transit by using a combination of firewalls, IDS, IPS, and virtual LANs.
  - It should deploy firewalls to protect each external interface with only necessary ports opened and default settings as denial. An updated intrusion detection and prevention mechanism should be in place.
  - The virtual and conventional devices should be closely connected with a hypervisor for monitoring of traffic over the virtual network.
  - It recommends strict access management policies in place.
- Several researchers identified lack of control, multi-tenancy, virtualization and shared resources cause to data storage security issues in cloud computing model as compared to conventional computing model.

::.. Cloud Security Means (7/9)

- The user data outsourced to cloud storage, generally, have different degrees of confidentiality and sensitivity. So, the encryption mechanism and access control to the user data can be defined accordingly.
- Data confidentiality in cloud can be ensured through traditional encryption or secret sharing mechanism, and data authentication can ensure the integrity of data transmission. However, the integrity of stored data in the cloud is challenging. CSA recommends strict access management policies in place.
- The provider must be transparent to its user for backup related information like storage location, the frequency of backup, encryption mechanism used, access control used, and its availability during the recovery.

::.. Cloud Security Means (8/9)

- A storage service provider has to transparently attest the de-duplication patterns of the (encrypted) data being stored, to its customers.
- Secure data deletion is demanding in the cloud and several researchers have defined a taxonomy of adversaries having different capabilities and having different manners of access to the storage medium.
- Hardware availability, as per agreed SLA, is a key ingredient to build trust in a cloud computing environment. Hardware can be unavailable partially or fully. Partial unavailability happens due to limited resource allocation, and in that case, a load balancing mechanism is used to ensure hardware availability as per current need and SLA. Some works proposed the use of hardware-based encryption than software encryption for data integrity in the cloud.

::.. Cloud Security Means (9/9)

Physical security measures include preventing malicious insiders and outsiders from getting physical access to cloud physical resources. In the case of natural disasters measures should include minimal or no loss of data for the cloud user and business continuity is assured, such as by the implementation of standard Business Continuity Plan (for example BS25999, ISO22301) for the cloud providers.

::.. Cloud Assurance (1/5)

Assurance and compliance measures are a set of proactive actions that a provider executes to ensure necessary countermeasures are implemented to address known vulnerabilities in the cloud computing architectural components and used technologies and are sufficient to detect any malicious use of the cloud resources. Assurance and compliance measures are about monitoring and assessing implemented security solutions sufficiency for secured cloud operation.

- SLA document defines the contractual agreement between the cloud user and the cloud provider. It contains — minimum performance level of the cloud provider, counteractive actions, and consequences on SLA breach. The security requirement must be explicitly mentioned into the SLA along with monitoring and measurement mechanism.

::.. Cloud Assurance (2/5)

- Monitoring helps to increase transparency and trust in the cloud environment. Activity, event and traffic logs allow to establish accountability in the cloud and helps establishing proactive and reactive measures to secure the cloud.
- Verification and validation are the static and dynamic testing approach in a system or application software development life-cycle process. Security testing of the application software is generally focused around user authentication, system database, and network testing. Well tested software in use increases trust in a cloud-based solution. There are two aspects of verification and validation:
  - the use of verified and validated cloud infrastructure to gain the trust of the cloud user, and there are different solutions proposed wherein cloud infrastructure can be tested before putting in use.

::.. Cloud Assurance (3/5)

  - to use the cloud infrastructure to test any of the cloud system and application software and services. Cloud infrastructure can be used to provide Testing-as-a-Service (TaaS) to verify and validate any cloud-based application services before putting in use.
- Cloud system faces trust issue mostly because cloud heterogeneous infrastructure is located offsite, mostly multi-location, and is managed by another party and establishing trust is a multi-dimensional and multi-phased phenomenon. Establishing trust involves both infrastructure stability and human behavior responsible for managing the infrastructure.
- Certification process involves assessment, by accredited authorities, of security properties of cloud services and the underlying security mechanism to ensure the same. Certified services provide trust in the service and service provider.

::.. Cloud Assurance (4/5)

- Data audit is required to ensure the integrity of user data stored at a remote location which is being managed by a third party. The conventional integrity check methods, like hash functions, message digest, are not sufficient for the cloud environment as there is no local data available and downloading the entire data is a challenge. The design of remote data audit (RDA) technique must take care of the following aspects:

1. efficiency – use of least computational complexity;
2. public verifiability – permissible to delegate audit responsibility to a trustworthy Third Party Auditor (TPA);
3. frequency – permissible to repeat the audit any number of time with different input sets;
4. detection probability – probability of detection of potential corruption of stored data;

::.. Cloud Assurance (5/5)

5. recovery – probability of restoration of any corrupted data;
6. dynamic update — permissibility of updates in stored data while audit continues.

To optimize the audit process, only a fraction of stored data is taken for remote auditing purpose.

- In replication-based remote data auditing, same copy of the data is replicated over multiple distributed storage.
- In erasure-coding-based remote data auditing, Maximum Distance Separable (MDS) technique is used to achieve reliability for the same level of replication.
- In network-coding-based remote data auditing a new data block is created, at the time of repair, based on linear combination of the stored data blocks of the intact servers.