UNIT-5

Lacking trust between service providers and cloud users has hindered the universal acceptance of cloud computing as a service on demand.

In the past, trust models have been developed to protect mainly e-commerce and online shopping provided by eBay and Amazon.

For web and cloud services, trust and security become even more demanding, because leaving user applications completely to the cloud providers has faced strong resistance by most PC and server users.

A healthy cloud ecosystem is desired to free users from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations.

The security demands of three cloud service models, IaaS, PaaS, and SaaS,.

These security models are based on various SLAs between providers and users.

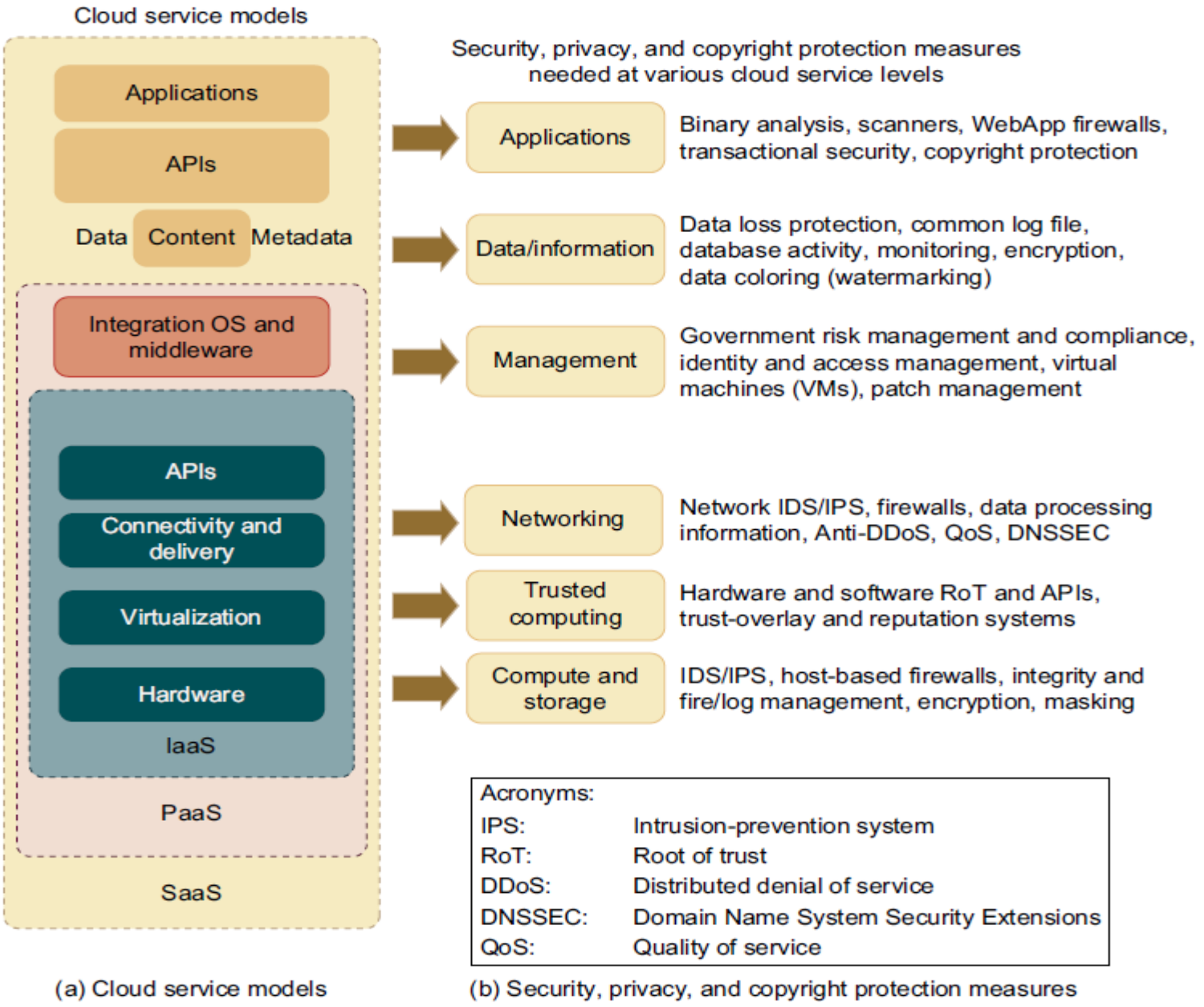
Basic Cloud Security

Three basic cloud security enforcements are expected.

- First, facility security in data centers demands on-site security year round. Biometric readers, CCTV (close-circuit TV), motion detection, and man traps are often deployed.

- Network security demands fault-tolerant external firewalls, intrusion detection systems (IDSes), and third-party vulnerability assessment.

- Finally, platform security demands SSL and data decryption, strict password policies, and system trust certification.



(a) Cloud service models

(b) Security, privacy, and copyright protection measures

Software as a Service - Security

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

In SaaS environments the security controls and their scope are negotiated into the contracts for service; service levels, privacy, and compliance are all issues to be dealt with legally in contracts.

In Software as a Service (SaaS) model, the client needs to be dependent on the service provider for proper security measures of the system.

The service provider must ensure that their multiple users don‘t get to see each other‘s private data.

So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed

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. Forensics tasks will become much more difficult since it will be very hard or maybe not possible for investigators may to access the system hardware physically.

Data 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. Whenever a business, an individual, a government agency, or any other entity wants to shares information over cloud, confidentiality or privacy is a questions nay need to be asked

Availability The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability is one of the big concerns of cloud service providers, since if the cloud service is disrupted or compromised in any way; it affects large no. of customers than in the traditional model.

Information Security In the SaaS model, the data of enterprise is stored outside of the enterprise boundary, which is at the SaaS vendor premises. Consequently, these SaaS vendor needs to adopt additional security features to ensure data security and prevent breaches due to security vulnerabilities in the application or by malicious employees. This will need the use of very strong encryption techniques for data security and highly competent authorization to control access private data.

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. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization.

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. H.

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. Aria 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.

Security Governance

Effective governance and enterprise risk management in Cloud Computing environments follows from well-developed information security governance processes, as part of the organization's overall corporate governance obligations of due care.

Well-developed information security governance processes should result in information security management programs that are scalable with the business, repeatable across the organization, measurable, sustainable, defensible, continually improving, and cost-effective on an ongoing basis.

The fundamental issues of governance and enterprise risk management in Cloud Computing concern the identification and implementation of the appropriate organizational structures, processes, and controls to maintain effective information security governance, risk management, and compliance.

Governance Recommendations

- A portion of the cost savings obtained by Cloud Computing services must be invested into increased scrutiny of the security capabilities of the provider, application of security controls, and ongoing detailed assessments and audits, to ensure requirements are continuously met.
- Both Cloud Computing service customers and providers should develop robust information security governance, regardless of the service or deployment model.
- Information security governance should be a collaboration between customers and providers to achieve agreed-upon goals which support the business mission and information security program. The service model may adjust the defined roles and responsibilities in collaborative information security governance and risk management .
- User organizations should include review of specific information security governance structure and processes, as well as specific security controls, as part of their due diligence for prospective provider organizations.
- The provider's security governance processes and capabilities should be assessed for sufficiency, maturity, and consistency with the user's information security management processes. The provider's information security controls should be demonstrably risk-based and clearly support these management processes.

- Collaborative governance structures and processes between customers and providers should be identified as necessary, both as part of the design and development of service delivery, and as service risk assessment and risk management protocols, and then incorporated into service agreements.

- Security departments should be engaged during the establishment of Service Level Agreements and contractual obligations, to ensure that security requirements are contractually enforceable.

- Metrics and standards for measuring performance and effectiveness of information security management should be established prior to moving into the cloud. At a minimum, organizations should understand and document their current metrics and how they will change when operations are moved into the cloud, where a provider may use different (potentially incompatible) metrics.

- Wherever possible, security metrics and standards (particularly those relating to legal and compliance requirements) should be included in any Service Level Agreements and contracts. These standards and metrics should be documented and demonstrable (auditable).

Risk Management

A **cloud** provider needs to manage the **cloud computing** environment **risks** in order to identify, assess, and prioritize the **risks** in order to decrease those **risks**, improve **security**, increase confidence in **cloud** services, and relieve organizations' concerns on the issue of using a **cloud** environment

The practices should be proportionate to your particular usages of cloud services, which may range from innocuous and transient data processing up through mission critical business processes dealing with highly sensitive information.

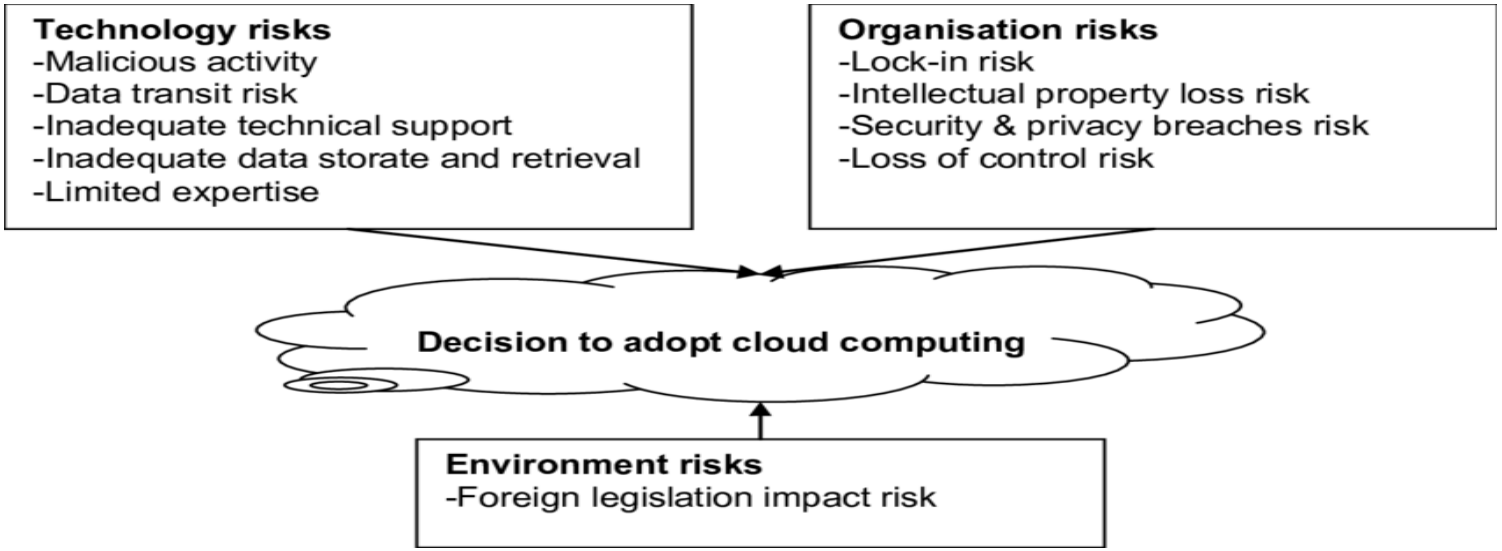
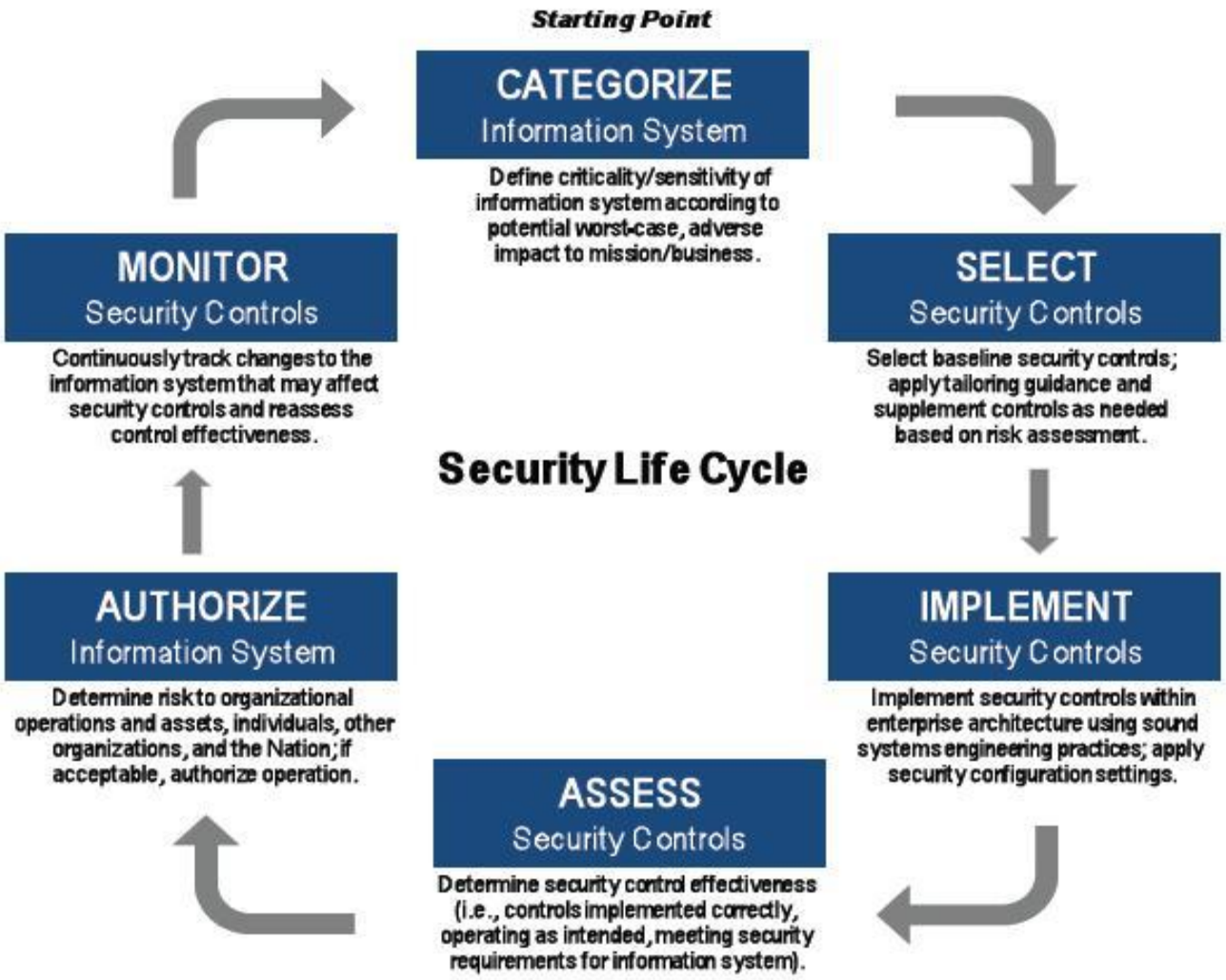


Figure 5: NIST Risk Management Framework



Some cloud-specific recommendations you can incorporate into your existing risk management processes.

- Due to the lack of physical control over infrastructure in many Cloud Computing deployments; Service Level Agreements, contract requirements, and provider documentation play a larger role in risk management than with traditional, enterprise owned infrastructure.

- Due to the on-demand provisioning and multi-tenant aspects of Cloud Computing, traditional forms of audit and assessment may not be available, or may be modified. For example, some providers restrict vulnerability assessments and penetration testing, while others limit availability of audit logs and activity monitoring.

- Relating to the use of cloud services for functions critical to the organization, the risk management approach should include identification and valuation of assets, Identification and analysis of threats and vulnerabilities and their potential impact on assets (risk and incident scenarios), analysis of the likelihoods of events/scenarios, management-approved risk acceptance levels and criteria, and the development of risk treatment plans with multiple options (control, avoid, transfer, accept). The outcomes of risk treatment plans should be incorporated into service agreements.

- The user and provider should jointly develop risk scenarios for the cloud service; this should be intrinsic to the provider's design of service for the user, and to the user's assessment of cloud service risk.

- a provider cannot demonstrate comprehensive and effective risk management processes in association with its services, customers should carefully evaluate use of the vendor as well as the user's own abilities to compensate for the potential risk management gaps.

- Adopt a Information risk management (IRM)framework model to evaluate it, and a maturity model to assess the effectiveness of your IRM model.

- Establish appropriate contractual requirements and technology controls to collect necessary data to inform information risk decisions

- Adopt a process for determining risk exposure before developing requirements for a Cloud Computing project.

- When utilizing SaaS, the overwhelming majority of information will have to be provided by the service provider. Organizations should structure analytical information gathering processes into contractual obligations of the SaaS service.

- When utilizing PaaS, build in information gathering as per SaaS above, but where possible include the ability to deploy and gather information from controls as well as creating contractual provisions to test the effectiveness of those controls.

- When utilizing an IaaS service provider, build information transparency into contract language for information required by risk analysis.

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.

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 CLOUD SECURITY MONITORING

- One of the most effective ways to mitigate cloud security risks is to gain strict controls over data at all endpoints.

- Solutions that scan, analyze, and take action on data before it leaves the enterprise network provide a good first line of defense against data loss via the cloud and can avoiding the introduction of vulnerabilities, such as a sensitive file being uploaded to an unprotected cloud repository.

- 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.

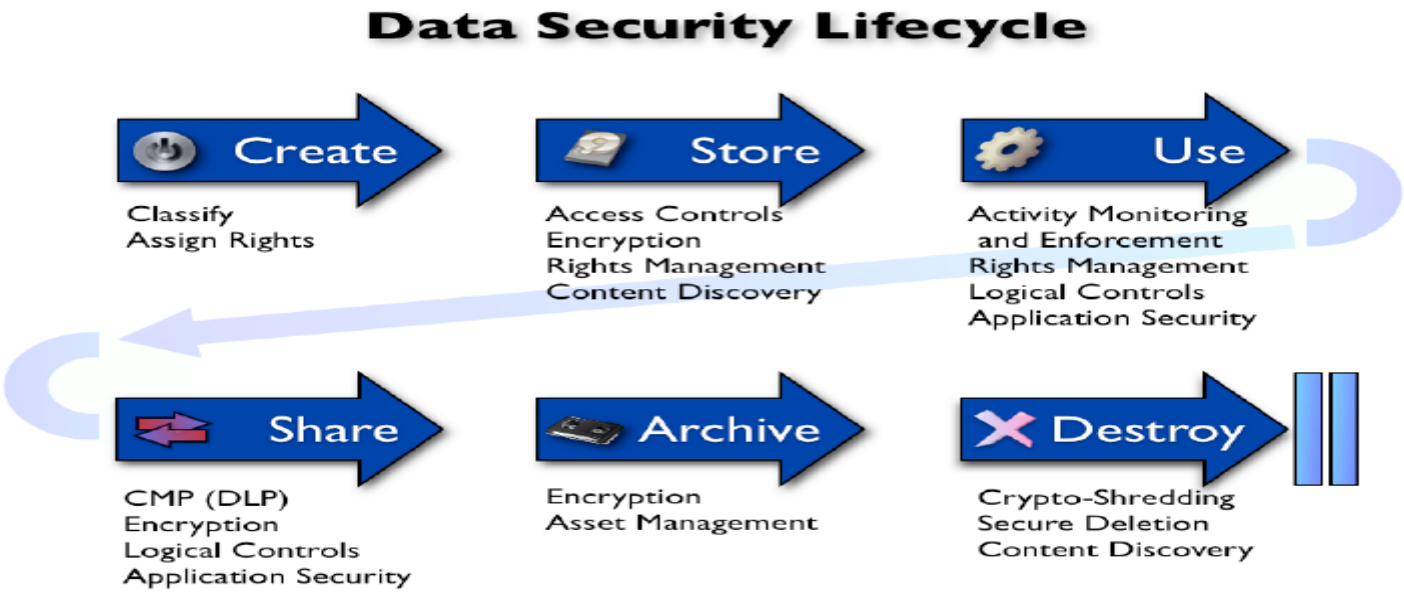
- Coupled with the scanning and auditing of data already stored in the cloud, real-time monitoring at the point of exit and entry is highly effective for enterprises that require comprehensive security while still utilizing the benefits of the cloud.

Data Security

One of the primary goals of information security is to protect the fundamental data that powers our systems and applications.

In case of Cloud Computing, our traditional methods of securing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies.

The Data Security Lifecycle is different from Information Lifecycle Management, reflecting the different needs of the security audience. The Data Security Lifecycle consists of six phases:



Key challenges regarding data lifecycle security in the cloud include the following:

Data security. Confidentiality, Integrity, Availability, Authenticity, Authorization, Authentication, and Non-Repudiation.

Location of the data. There must be assurance that the data, including all of its copies and backups, is stored only in geographic locations permitted by contract, SLA, and/or regulation.

Data remanance or persistence. Data must be effectively and completely removed to be deemed 'destroyed.' Therefore, techniques for completely and effectively locating data in the cloud, erasing/destroying data, and assuring the data has been completely removed or rendered unrecoverable must be available and used when required.

Commingling data with other cloud customers. Data – especially classified / sensitive data must not be commingled with other customer data without compensating controls while in use, storage, or transit. Mixing or commingling the data will be a challenge when concerns are raised about data security and geo-location.

Data backup and recovery schemes for recovery and restoration. Data must be available and data backup and recovery schemes for the cloud must be in place and effective in order to prevent data loss, unwanted data overwrite, and destruction. Don't assume cloud-based data is backed up and recoverable.

Data aggregation and inference. With data in the cloud, there are added concerns of data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information. Hence practices must be in play to assure the data owner and data stakeholders that the data is still protected from subtle "breach" when data is commingled and/or aggregated, thus revealing protected information (e.g., medical records containing names and medical information mixed with anonymous data but containing the same "crossover field").

Recomendations

- Understand how integrity is maintained and compromise of integrity is detected and reported to customers. The same recommendation applies to confidentiality when appropriate.
- The Cloud Computing provider must assure the data owner that they provide full disclosure (aka 'transparency') regarding security practices and procedures as stated in their SLAs.

- Ensure specific identification of all controls used during the data lifecycle. Ensure there specifications of to which entity is responsible for each control between the data owner and cloud services provider.
- Maintain a fundamental philosophy of knowing where your data is. Ensure your ability to know the geographical location of storage. Stipulate this in your SLAs and contracts. Ensure that appropriate controls regarding country location restrictions are defined and enforced.
- Understand circumstances under which storage can be seized by a third party or government entity. Ascertain that your SLA with the cloud provider includes advance notification to the data owner (if possible) that the data owner's information has been or will be seized.
- A system of service penalties should be included in the contract between the data owner and the cloud service provider. Specifically, data that would be subject to state and international data breach laws
- It is the data owner's responsibility to determine who should access the data, what their rights and privileges are, and under what conditions these access rights are provided.

- Encrypt data in the “. Encrypt data at rest and encrypt data in transit

- Identify trust boundaries throughout the IT architecture and abstraction layers. Ensure subsystems only span trust boundaries as needed and with appropriate safeguards to prevent unauthorized disclosure, alteration, or destruction of data.

- Understand what compartmentalization techniques are employed by a provider to isolate its customers from one another. A provider may use a variety of methods depending upon the types and number of services offered.

- Data owners should require cloud service providers to ensure that their backed-up data is not commingled with other cloud service customer data.

- Data retention and destruction schedules are the responsibility of the data owner. It is the cloud service provider’s responsibility to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures and on media. The data owner should enforce and audit this practice if possible.

- Perform regular backup and recovery tests to assure that logical segregation and controls are effective.

Application Security

Cloud environments — by virtue of their flexibility, openness, and often public availability — challenge many fundamental assumptions about application security.

Cloud Computing is a particular challenge for applications across the layers of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Cloud-based software applications require a design rigor similar to applications residing in a classic DMZ. This includes a deep up-front analysis covering all the traditional aspects of managing information confidentiality, integrity, and availability.

Applications in cloud environments will both impact and be impacted by the following major aspects:

Application Security Architecture – Consideration must be given to the reality that most applications have dependencies on various other systems.

With Cloud Computing application dependencies can be highly dynamic, even to the point where each dependency represents a discrete third party service provider.

Cloud characteristics make configuration management and ongoing provisioning significantly more complex than with traditional application deployment. The environment drives the need for architectural modifications to assure application security.

Software Development Life Cycle (SDLC) – Cloud computing affects all aspects of SDLC, spanning application architecture, design, development, quality assurance, documentation, deployment, management, maintenance, and decommissioning.

Compliance – Compliance clearly affects data, but it also influences applications (for example, regulating how a program implements a particular cryptographic function), platforms (perhaps by prescribing operating system controls and settings) and processes (such as reporting requirements for security incidents).

Tools and Services – Cloud computing introduces a number of new challenges around the tools and services required to build and maintain running applications.
These include development and test tools, application management utilities, the coupling to external services, and dependencies on libraries and operating system services, which may originate from cloud providers. Understanding the ramifications of who provides, owns,operates, and assumes responsibility for each of these is fundamental.

Vulnerabilities – These include not only the well-documented—and continuously evolving—vulnerabilities associated with web apps, but also vulnerabilities associated with machine-to-machine Service-Oriented Architecture (SOA) applications, which are increasingly being deployed into the cloud.

Recommendations

- Software Development Lifecycle (SDLC) security is important, and should at a high level address these three main areas of differentiation with cloud-based development: 1)updated threat and trust models, 2) application assessment tools updated for cloud environments, and 3) SDLC processes and quality checkpoints to account for application security architectural changes.

- IaaS, PaaS, and SaaS create different trust boundaries for the software development lifecycle; which must be accounted for during the development, testing, and production deployment of applications.

- For IaaS, a key success factor is the presence of trusted virtual machine images. The best alternative is the ability to provide your own virtual machine image conforming to internal policies.

- The best practices available to harden host systems within DMZs should be applied to virtual machines. Limiting services available to only those needed to support the application stack is appropriate.

- Securing inter-host communications must be the rule; there can be no assumption of a secure channel between hosts, whether in a common data center or even on the same hardware device.

- Managing and protecting application credentials and key material are critical.
- Extra care should be undertaken with the management of files used for application logging and debugging, as the locations of these files may be remote or unknown and the information could be sensitive.
- Account for external administration and multi-tenancy in the application's threat model.
- Metrics should be applied to assess effectiveness of application security programs. Among the direct application security-specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Indirect data handling metrics, such as the percentage of data encrypted, can indicate that responsible decisions are being made from an application architecture perspective.
- Cloud providers must support dynamic analysis web application security tools against applications hosted in their environments.
- Attention should be paid to how malicious actors will react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in the user context.

Identity and Access Management

Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today. While an enterprise may be able to leverage several Cloud Computing services without a good identity and access management strategy, in the long run extending an organization's identity services into the cloud is a necessary precursor towards strategic use of on-demand computing services.

following major IAM functions that are essential for successful and effective management of identities in the cloud:

- Identity provisioning/deprovisioning
- Authentication
- Federation
- Authorization & user profile management

Identity Provisioning: One of the major challenges for organizations adopting Cloud Computing services is the secure and timely management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. Furthermore, enterprises that have invested in user management processes within an enterprise will seek to extend those processes and practice to cloud services.

Authentication: When organizations start to utilize cloud services, authenticating users in a trustworthy and manageable manner is a vital requirement. Organizations must address authentication-related challenges such as credential management, strong authentication (typically defined as multi-factor authentication), delegated authentication, and managing trust across all types of cloud services.

Federation: In a Cloud Computing environment, Federated Identity Management plays a vital role in enabling organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP).

Authorization & user profile management: The requirements for user profiles and access control policy vary depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organization (such as an employer, university, hospital, or other enterprise). The access control requirements in SPI environments include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.

Identity Provisioning – Recommendations

- Capabilities offered by cloud providers are not currently adequate to meet enterprise requirements. Customers should avoid proprietary solutions such as creating custom connectors unique to cloud providers, as these exacerbate management complexity.
- Customers should leverage standard connectors provided by cloud providers to the extent practical, preferably built on SPML schema.

Authentication – Recommendations

- Both the cloud provider and the customer enterprises should consider the challenges associated with credential management and strong authentication, and implement cost effective solutions that reduce the risk appropriately.

SaaS and PaaS providers typically provide the options of either built-in authentication services to their applications or platforms, or delegating Authentication to the enterprise. Customers have the following options:

- Authentication for enterprises. Enterprises should consider authenticating users via their Identity Provider (IdP) and establishing trust with the SaaS vendor by federation.

- Authentication for individual users acting on their own behalf. Enterprises should consider using user-centric authentication such as Google, Yahoo, OpenID, Live ID, etc., to enable use of a single set of credentials valid at multiple sites.

For IaaS, authentication strategies can leverage existing enterprise capabilities.

- For IT personnel, establishing a dedicated VPN will be a better option, as they can leverage existing systems and processes.
- Some possible solutions include creating a dedicated VPN tunnel to the corporate network or federation. A dedicated VPN tunnel works better when the application leverages existing identity management systems
- Any local authentication service implemented by the cloud provider should be OATH compliant. With an OATH-compliant solution, companies can avoid becoming locked into one vendor's authentication credentials.

Federation Recommendations

- In a Cloud Computing environment, federation of identity is key for enabling allied enterprises to authenticate, provide single or reduced Sign-On (SSO), and exchange identity attributes between the Service Provider (SP) and the Identity Provider (IdP).

- Organizations considering federated identity management in the cloud should understand the various challenges and possible solutions to address them with respect to identity lifecycle management, authentication methods, token formats, and non-repudiation.

Access Control Recommendations

- Review appropriateness of the access control model for the type of service or data.
- Identify authoritative sources of policy and user profile information.
- Assess support for necessary privacy policies for the data.
- Select a format in which to specify policy and user information.
- Determine the mechanism to transmit user information from a Policy Information Point (PIP) to a Policy Decision Point (PDP).
- Request a policy decision from a Policy Decision Point (PDP).
- Enforce the policy decision at the Policy Enforcement Point (PEP).
- Log information necessary for audits.

Identity as a Service should follow the same best practices that an internal IAM implementation does, along with added considerations for privacy, integrity, and auditability.

For internal enterprise users, custodians must review the cloud provider's options to provide secured access to the cloud, either through a direct VPN or through an industry standard such as SAML and strong authentication.

For external users such as partners, the information owners need to incorporate interactions with IAM providers into their SDLC, as well as into their threat assessments. Application security – the interactions of the various components with each other, and the vulnerabilities created thereby (such as SQL Injection and Cross Site Scripting, among many others) – must also be considered and protected against.

Virtualization Security

In Cloud computing, virtualization is the basis of delivering Infrastructure as a Service (IaaS) that separates data, network, applications and machines from hardware constraints

Virtualization enables a single system to concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system (OS). However, there are still open challenges in achieving security for Cloud virtualization.

To secure the virtualization hardware, (Cloud) service provider must limit access of hardware resources to authorized person. Similarly, proper access control should be implemented in the management layer, so that each administrator has access only to its concerned data and software. The service provider also need to provide strong authentication mechanisms to users.

Programs that control the hypervisor must be secured using similar practices used for security of programs running on servers. Similarly access to the hyper visor must be restricted. Other security measures to secure hypervisor include installing updates to the hypervisor, restricting administrator access to the hypervisors management interfaces and analyzing hypervisors logs to see if it is functioning properly

Each component of virtualization layer can act as an attack vector to launch multiple attacks on the system. Attacks that target different components of virtualization environment may result in security issues such as compromise of complete Cloud infrastructure, stealing of customer data and system hacking.

- Limit on VM resource usage has to be assigned so that malicious VMs can be restricted from consuming extra resources of the system . Moreover, isolation between virtual machines should be provided to ensure that they run independently from each other.

- To secure the guest OS running in virtual machines, best practices for the security of physical machines must be followed that include updating the OS regularly for patches and updates, using anti-virus software, securing internet and email and monitoring of guest OS regularly

- Hypervisors use disk images (host files used as disk drive for guest OSs) to present guest OSs with virtual hard drives. Guest OS images can be moved and distributed easily, so they must be protected from unauthorized access, tampering and storage.

- To securely manage the guest OS images they must be examined and updated regularly according to the requirements. Unnecessary images must not be created and if any image is useless it must be removed from system

If the attacker has physical access to the Cloud hardware, he may run malicious application or code in the system to damage the VMs by modifying their source code and changing their functionality. With the help of physical access to system, attackers can also launch cross VM side channel attacks include CPU cache leakage to measure the load of other virtual web server on the network .

Moreover, if access control is not implemented properly, different administrators such as network admin and virtualization admin might access the customer data that they are not authorized to access. These activities will result in security compromises such as loss of data confidentiality and unauthorized traffic monitoring.

A Cloud customer can lease a guest VM to install a malicious guest OS, which attacks and compromises the hypervisor by changing its source code in order to gain access to the memory contents (data and code) of VMs present in the system

Another attack in which program running in one VM can get root access to the host machine is called VM Escape . It is done by crashing the guest OS to get out of it and running an arbitrary code on the host OS. Therefore, such malicious VMs can take complete control of the host OS.

If isolation is not properly implemented covert channels can be used for unauthorized communication with other VMs in the system. Attackers can use Trojans, malwares and botnets for traffic monitoring, stealing critical data, and tampering the functionality of guest OS

Recommendations

- Identify which types of virtualization your cloud provider uses, if any.
- Virtualized operating systems should be augmented by third party security technology to provide layered security controls and reduce dependency on the platform provider alone.
- Understand which security controls are in place internal to the VMs other than the built in hypervisor isolation — such as intrusion detection, anti-virus, vulnerability scanning, etc. Secure by default configuration must be assured by following or exceeding available industry baselines.
- Understand which security controls are in place external to the VMs to protect administrative interfaces (web-based, APIs, etc.) exposed to the customers.

Autonomic computing is a computer's ability to manage itself automatically through adaptive technologies that further **computing** capabilities and cut down on the time required by computer professionals to resolve system difficulties and other maintenance such as software updates.

The ability of a system to react consistently and correctly to situations ranging from benign but unusual events to outright attacks is key to the achievement of the goals of self-protection, self-healing, and self-optimization.

Because they are often built around the interconnection of elements from different administrative domains, autonomic systems raise additional security challenges, including the establishment of a trustworthy system identity, automatically handling changes in system configuration and interconnections, and greatly increased configuration complexity

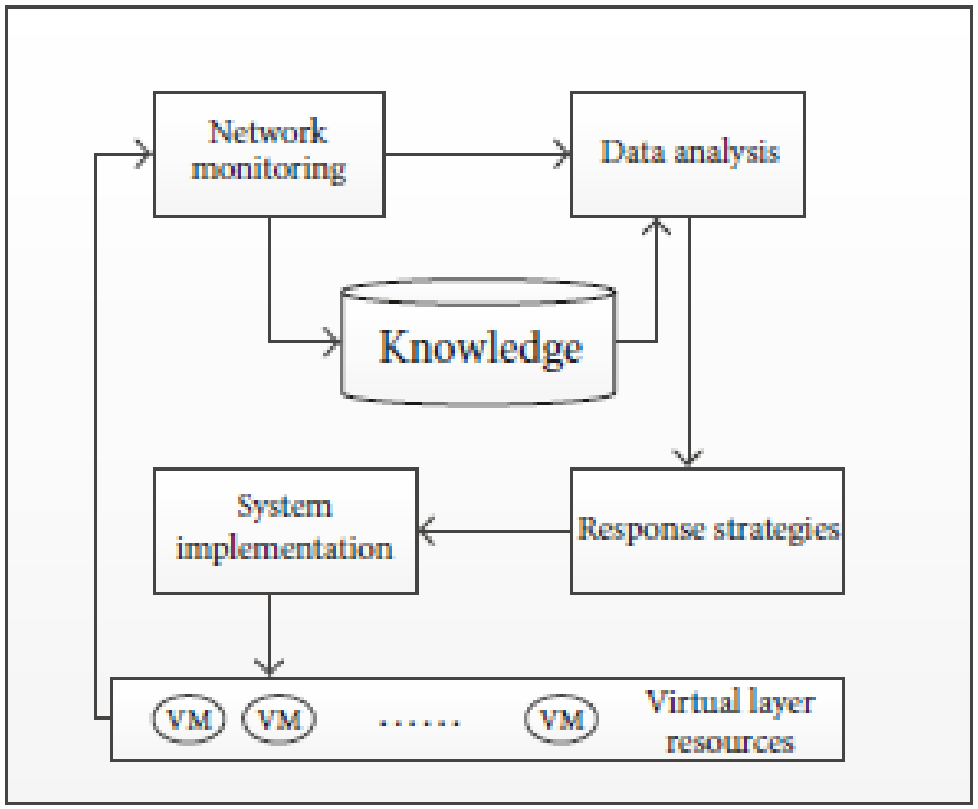
Autonomic computing provides an effective way to reduce the complexity of the system management, but what early autonomic computing system mostly considered is physical resource management of distributed heterogeneous environment.

It did not include the cloud environment under various restricting factors, such as large-scale virtualized applications, service level agreements, diverse application, and dynamic changes in the deployment environment.

The original framework of autonomic computing application cannot be applied directly in the cloud environment

According to the data security problem of the cloud platform, the working mechanism of autonomic computing system model uses the abnormal data mining idea for reference. It contains four self-regulatory elements, which can transmit the monitoring information to one another.

The model framework is shown in Figure. The model consists of five modules: network monitoring module, data analysis module, response strategy module, system implementation module, knowledge base, and virtual machine (VM).


Network monitoring
Data analysis
Knowledge
System implementation
Response strategies
VM
VM
.....
VM
Virtual layer resources

Network monitoring module is the monitoring agent deployed on the physical host, virtual machine, or other containers. It is used to collect monitored data of system at all levels and its persistent storage.

Based on the historical monitored data, the data analysis module establishes the correlation of the data to form the metric correlation graph for evaluating the importance degree. It uses the PCA (Principal Component Analysis) to calculate the eigenvector of the monitored data and computes the linear regression equation of the data source in the cloud computing environment to quantitatively evaluate system anomalies.

The response strategy module selects the object to be monitored in the next stage according to the importance of the monitored object.

System implementation module is to use the monitoring agent to perform the dynamic adjustment of monitoring objects and monitoring cycle.

Knowledge base is the record of operation in the process of learning load patterns and corresponding eigenvectors, so that the system normal operation can be depicted.

Any Abnormal operation in VM or in any components can be verified by historical data and current data and appropriate decision can be taken.

Cloud Security Architecture design

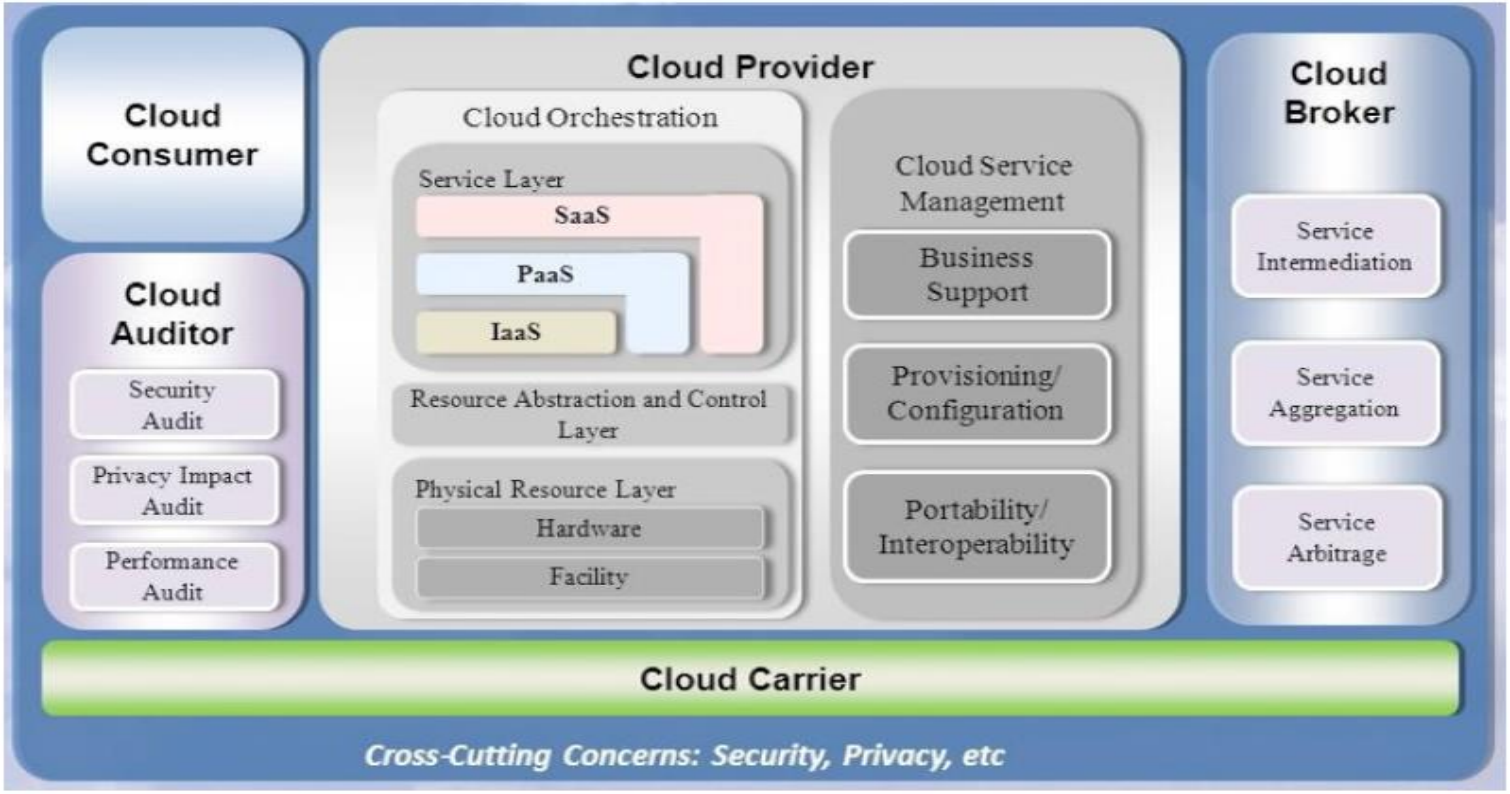


Figure 2: NIST Cloud Computing Security Reference Architecture Approach

Cloud computing security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud Ecosystem.

Cloud computing security addresses both physical and logical security issues across all the different service models of software, platform and infrastructure. It also addresses how these services are delivered in the Public, Private, Hybrid and Community delivery models

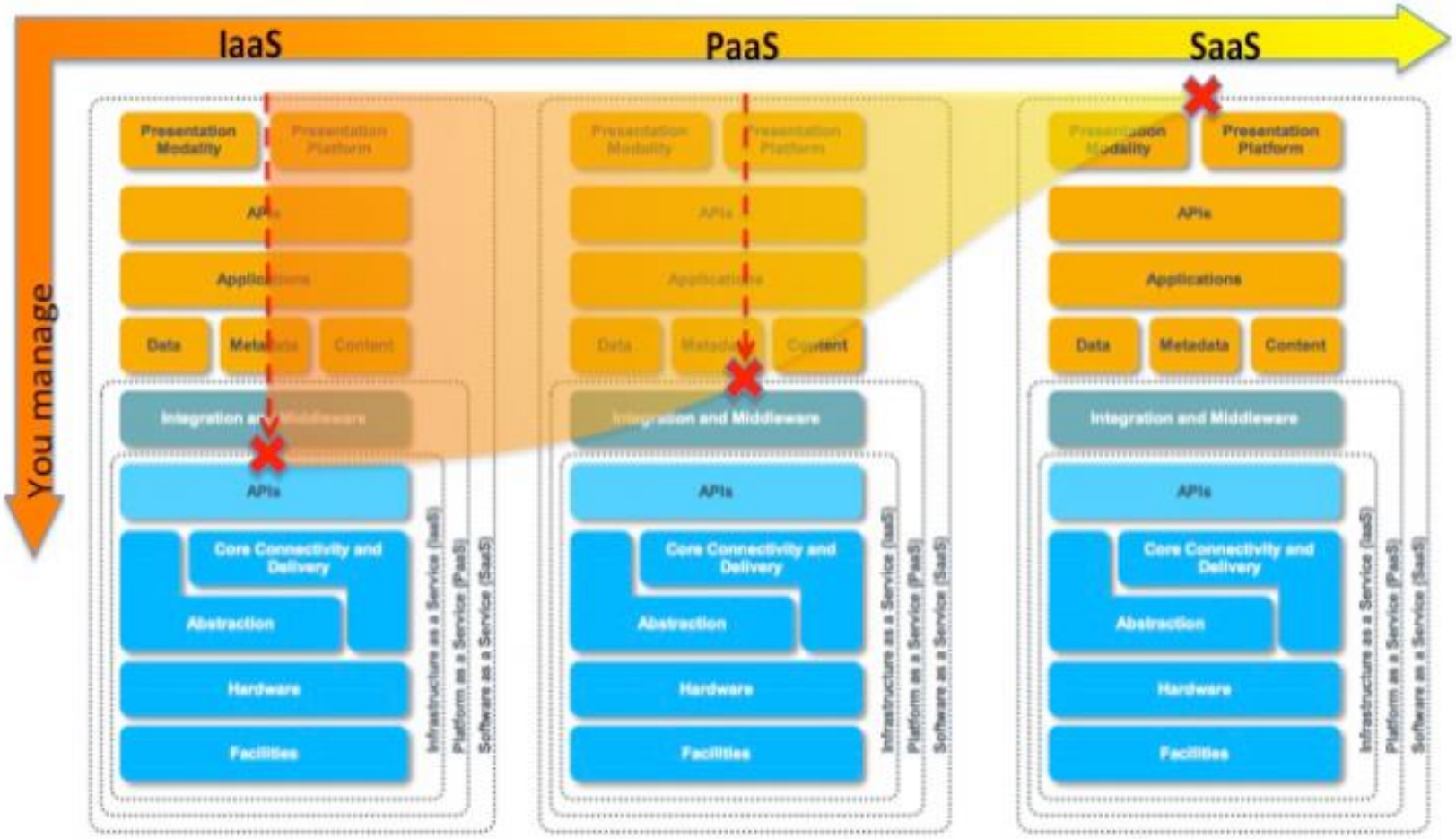
In a cloud environment, there are security threats and security requirements that differ for different cloud deployment models, and the necessary mitigations against such threats and cloud Actor responsibilities for implementing security controls depend upon the service model chosen and the service categories elected.

Many of the security threats can be mitigated with the application of traditional security processes and mechanisms, while others require cloud-specific solutions. Since each layer of the cloud computing Reference Architecture may have different security vulnerabilities and may be exposed to different threats, the architecture of a cloud-enabled service directly impacts its security posture and the system's key management aspects.

As the figure shows, in a IaaS service model, the cloud Consumer has high visibility into everything above the API layer, while the cloud Providers implement controls below the API layer (which are usually opaque to Consumers).

The cloud Consumer has limited visibility and limited key management control in a PaaS model, since the cloud Provider implements the security functions in all layers below the integration and middleware layer.

The cloud Consumer loses visibility and control in a SaaS model, and in general, controls below the presentation layer are opaque to the cloud Consumer, since the cloud Provider implements all security functions.



Stack image source: Cloud Security Alliance specification, 2009

The centralization of data and increase in security-focused resources can improve security, but concerns can persist about losing control of certain sensitive data, and the lack of security for stored kernels.

Security is often as good as or better than traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle.

However, the complexity of security greatly increases when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users.

In addition, user access to security audit logs may be difficult or impossible for cloud Providers to grant to cloud Consumers. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Cloud computing possesses privacy concerns because the service providers have access to the data that is stored on their infrastructure.

Cloud Providers could accidentally or deliberately alter or even delete information. Many cloud Providers can share information with third parties if necessary without a warrant.

The permission is granted in their privacy policy, which users agree to before they start using cloud services.

Privacy solutions include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

While all cloud Actors involved in orchestrating a cloud Ecosystem are responsible for addressing operational, security and privacy concerns, cloud Consumers retain the data ownership, and therefore remain fully responsible for:

- properly identifying data's sensitivity,
- assessing the risk from any exposure or misuse of the data and the impact to their business,
- identifying security requirements commensurable with the data sensitivity, and
- approving necessary risk mitigations.