UNIT -3

Cloud Computing Risk Issues and Security Challenges:

Despite the initial success and popularity of the cloud computing paradigm and the extensive availability of providers and tools, a significant number of challenges and risks are inherent to this new model of computing. Providers, developers, and end users must consider these challenges and risks to take good advantage of cloud computing. Issues to be faced include user privacy, data 34 INTRODUCTION TO CLOUD COMPUTING security, data lock-in, availability of service, disaster recovery, performance, scalability, energy-efficiency, and programmability

security as a main issue: “current cloud offerings are essentially public ... exposing the system to more attacks.” For this reason there are potentially additional challenges to make cloud computing environments as secure as in-house IT systems. At the same time, existing, well understood technologies can be leveraged, such as data encryption, VLANs, and firewalls. Security and privacy affect the entire cloud computing stack, since there is a massive use of third-party services and infrastructures that are used to host important data or to perform critical operations. In this scenario, the trust toward providers is fundamental to ensure the desired level of privacy for applications hosted in the cloud [38]. Legal and regulatory issues also need attention. When data are moved into the Cloud, providers may choose to locate them anywhere on the planet. The physical location of data centers determines the set of laws that can be applied to the management of data. For example, specific cryptography techniques could not be used because they are not allowed in some countries. Similarly, country laws can impose that sensitive data, such as patient health records, are to be stored within national borders.

The CIA Triad

Confidentiality, integrity, and availability are sometimes known as the CIA triad of information system security, and are important pillars of cloud software assurance.

Confidentiality
Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference:
- Intellectual property rights — Intellectual property (IP) includes inventions, designs, and artistic, musical, and literary works. Rights to intellectual property are covered by copyright laws, which protect creations of the mind, and patents, which are granted for new inventions.
- Covert channels — A covert channel is an unauthorized and unintended communication path that enables the exchange of information. Covert channels can be accomplished through timing of messages or inappropriate use of storage mechanisms.
- Traffic analysis — Traffic analysis is a form of confidentiality breach that can be accomplished by analyzing the volume, rate, source, and destination of message traffic, even if it is encrypted. Increased message activity and high bursts of traffic can indicate a major event is occurring. Countermeasures to traffic analysis include maintaining a near-constant rate of message traffic and disguising the source and destination locations of the traffic.
- Encryption — Encryption involves scrambling messages so that they cannot be read by an unauthorized entity, even if they are intercepted. The amount of effort (work factor) required to decrypt

the message is a function of the strength of the encryption key and the robustness and quality of the encryption algorithm.

- Inference — Inference is usually associated with database security. Inference is the ability of an entity to use and correlate information protected at one level of security to uncover information that is protected at a higher security level.

Integrity

The concept of cloud information integrity requires that the following three principles are met:

- Modifications are not made to data by unauthorized personnel or processes.
- Unauthorized modifications are not made to data by authorized personnel or processes.
- The data is internally and externally consistent — in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.

Availability

Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. A denial-of-service attack is an example of a threat against availability. The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (DAD).

Privacy and Compliance Risks

One area that is greatly affected by cloud computing is privacy. It's important to remember that although the control of cloud computing privacy has many threats and vulnerabilities in common with non cloud processes and infrastructure, it also has unique security issues. For example, a successful identity theft exploit can result in a privacy loss that has a huge impact on an enterprise. The organization can suffer short-term losses due to remediation, investigation, and restitution costs. It can also incur longer term problems for the organization due to loss of credibility, confidence, and negative publicity. Another mistake organizations often make is in assigning responsibility for privacy controls to the IT dept, rather than a business unit that owns the data. Information systems security frameworks have defined, standardized processes that apply to cloud computing — and its potential privacy breaches. This section examines the legal and standard processes that affect privacy control in the cloud. An individual's right to privacy is embodied in the fundamental principles of privacy:

- Notice — Regarding the collection, use, and disclosure of personally identifiable information (PII)
- Choice — To opt out or opt in regarding disclosure of PII to third parties
- Access — By consumers to their PII to permit review and correction of information
- Security — To protect PII from unauthorized disclosure
- Enforcement — Of applicable privacy policies and obligations Privacy definitions vary widely, especially when we start to wander out of the United States. The definition of personally identifiable information (PII) as described by the Office of Management and Budget (OMB) is as follows: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.1 Variations of this definition are used by compliance regulations such as HIPAA and EU directive 95/46/EC:

. . . "*personal data*" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. . .

Threats to Infrastructure

To properly understand the threats that cloud computing presents to the computing infrastructure, it's important to understand communications security techniques to prevent, detect, and correct errors so that integrity, availability, and the confidentiality of transactions over networks may be maintained. This includes the following:

- Communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access networks
- Internet/intranet/extranet in terms of firewalls, routers, gateways, and various protocols

Common Threats and Vulnerabilities

A threat is simply any event that, if realized, can cause damage to a system and create a loss of confidentiality, availability, or integrity. Threats can be malicious, such as the intentional modification of sensitive information, or they can be accidental — such as an error in a transaction calculation or the accidental deletion of a fi le. A vulnerability is a weakness in a system that can be exploited by a threat. Reducing the vulnerable aspects of a system can reduce the risk and impact of threats on the system. For example, a password-generation tool, which helps users choose robust passwords, reduces the chance that users will select poor passwords (the vulnerability) and makes the password more diffi cult to crack (the threat of external attack). Common threats to both cloud and traditional infrastructure include the following:

- Eavesdropping — Data scavenging, traffic or trend analysis, social engineering, economic or political espionage, sniffing, dumpster diving, keystroke monitoring, and shoulder surfing are all types of eavesdropping to gain information or to create a foundation for a later attack. Eavesdropping is a primary cause of the failure of confidentiality.
- Fraud — Examples of fraud include collusion, falsified transactions, data manipulation, and other altering of data integrity for gain.
- Theft — Examples of theft include the theft of information or trade secrets for profi t or unauthorized disclosure, and physical theft of hardware or software.
- Sabotage — Sabotage includes denial-of-service (DoS) attacks, production delays, and data integrity sabotage.
- External attack — Examples of external attacks include malicious cracking, scanning, and probing to gain infrastructure information, demon dialing to locate an unsecured modem line, and the insertion of a malicious code or virus.

Logon Abuse

Logon abuse can refer to legitimate users accessing services of a higher security level that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who might be legitimate users of a different system or users who have a lower security classification.

Inappropriate System Use

This style of network abuse refers to the nonbusiness or personal use of a network by otherwise authorized users, such as Internet surfi ng to inappropriate content sites (travel, pornography, sports, and so forth). As per the International Information Systems Security Certification Consortium (ISC) Code of Ethics and the Internet Advisory Board (IAB) recommendations, the use of networked services for other than business purposes can be considered abuse of the system. While most employers do not enforce extremely strict Websurfing rules, occasional harassment litigation may result from employees accessing pornography sites and employees operating private Web businesses using the company's infrastructure.

Eavesdropping

This type of network attack consists of the unauthorized interception of network traffic. Certain network transmission methods, such as satellite, wireless, mobile, PDA, and so on, are vulnerable to eavesdropping attacks. Tapping refers to the physical interception of a transmission medium (like the splicing of a cable or the creation of an induction loop to pick up electromagnetic emanations from copper). Eavesdropping can take one of two forms:

Passive eavesdropping
Active eavesdropping

Network Intrusion

This type of attack refers to the use of unauthorized access to break into a network primarily from an external source. Unlike a logon abuse attack, the intruders are not considered to be known to the company. Most common hacks belong to this category. Also known as a penetration attack, it exploits known security vulnerabilities in the security perimeter.

Data and Cloud Access Control Issues

The cost of access control in the cloud must be commensurate with the value of the information being protected. The value of this information is determined through qualitative and quantitative methods. These methods incorporate factors such as the cost to develop or acquire the information, the importance of the information to an organization and its competitors, and the effect on the organization's reputation if the information is compromised. Proper access controls enable full availability. Availability ensures that a system's authorized users have timely and uninterrupted access to the information in the system. The additional access control objectives are reliability and utility. Access control must offer protection from an unauthorized, unanticipated, or unintentional modification of information. This protection should preserve the data's internal and external consistency. The confidentiality of the information must also be similarly maintained, and the information should be available on a timely basis. These factors cover the integrity, confidentiality, and availability components of information system security. Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on both the system and the network. Audit trails can be used for intrusion detection and for the reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at logon time should notify the user of any monitoring being conducted. The following measures compensate for both internal and external access violations:

- Backups
- RAID (Redundant Array of Independent Disks) technology
- Fault tolerance
- Business continuity planning
- Insurance

Security Challenges- Security Policy Implementation

Security policies are the foundation of a sound security implementation. Often organizations will implement technical security solutions without fi rst creating this foundation of policies, standards, guidelines, and procedures, unintentionally creating unfocused and ineffective security controls. A policy is one of those terms that can mean several things. For example, there are security policies on

firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global information security policy. A good, well-written policy is more than an exercise created on white paper — it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a governmental or regulatory function. A policy can also provide protection from liability due to an employee's actions, or it can control access to trade secrets.

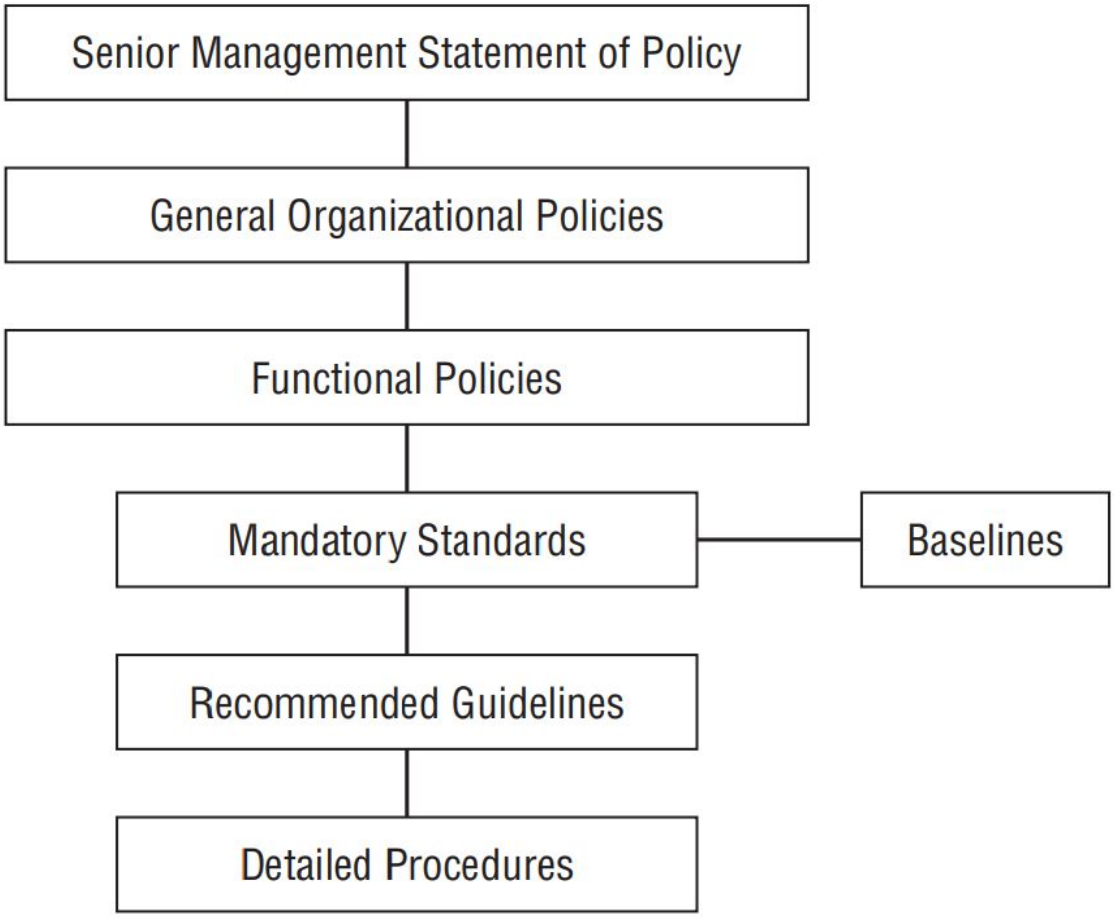


Figure 5-1: Security policy hierarchy

Virtualization Security Management

Although the global adoption of virtualization is a relatively recent event, threats to the virtualized infrastructure are evolving just as quickly. Historically, the development and implementation of new technology has preceded the full understanding of its inherent security risks, and virtualized systems are no different. The following sections examine the threats and vulnerabilities inherent in virtualized systems and look at some common management solutions to those threats.

VIRTUALIZATION TYPES

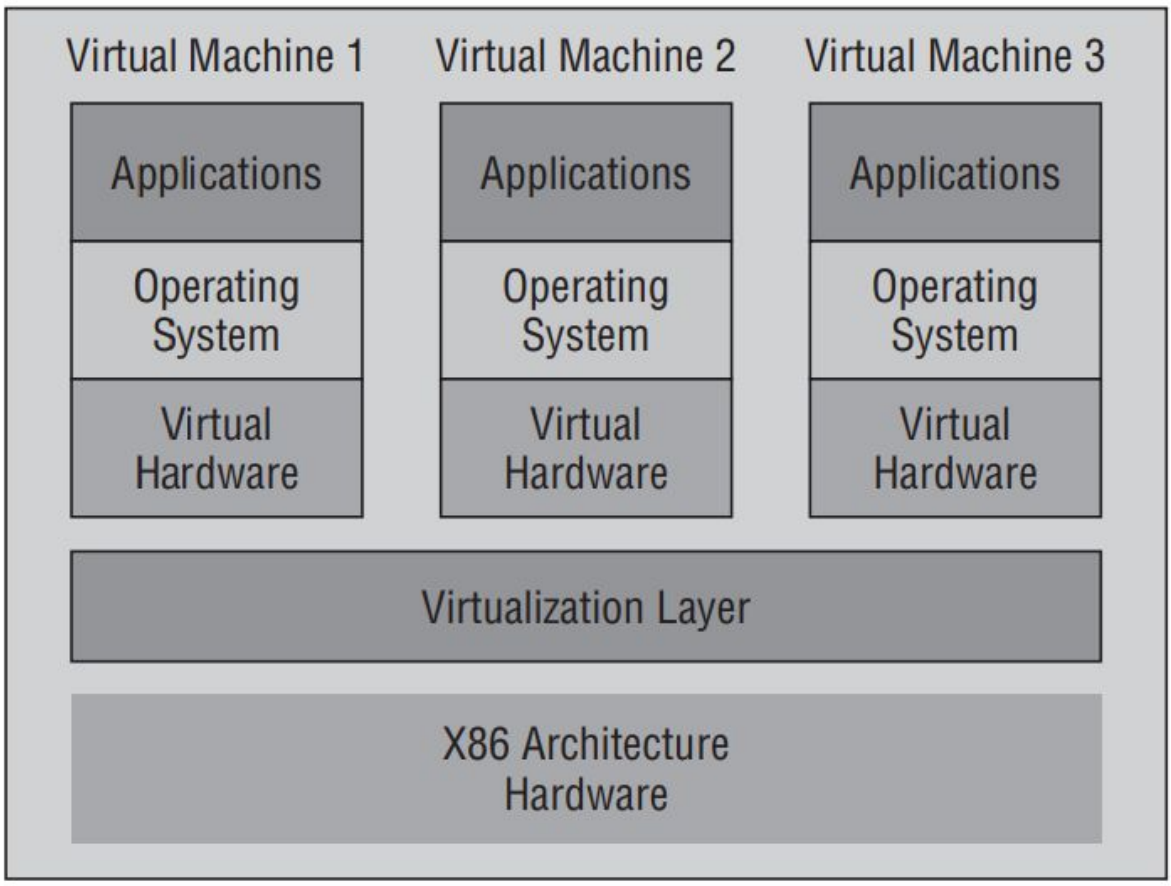
The Virtual Machine (VM), Virtual Memory Manager (VMM), and hypervisor or host OS are the minimum set of components needed in a virtual environment. They comprise virtual environments in a few distinct ways:

👁 Type 1 virtual environments are considered “full virtualization” environments and have VMs running on a hypervisor that interacts with the hardware.
👁 Type 2 virtual environments are also considered “full virtualization” but work with a host OS instead of a hypervisor.
👁 Para-virtualized environments offer performance gains by eliminating some of the emulation that occurs in full virtualization environments.
👁 Other type designations include hybrid virtual machines (HVMs) and hardware-assisted techniques.

VIRTUALIZATION MANAGEMENT ROLES

Typically, the VMware Infrastructure is managed by several users performing different roles. The roles assumed by administrators are the Virtualization Server Administrator, Virtual Machine Administrator, and Guest Administrator. VMware Infrastructure users may have different roles and responsibilities, but some functional overlap may occur. The roles assumed by administrators are configured in VMS and are defined to provide role responsibilities:
👁 Virtual Server Administrator — This role is responsible for installing and configuring the ESX Server hardware, storage, physical and virtual networks, service console, and management applications.
👁 Virtual Machine Administrator — This role is responsible for creating and configuring virtual machines, virtual networks, virtual machine resources, and security policies. The Virtual Machine Administrator creates, maintains, and provisions virtual machines.
👁 Guest Administrator — This role is responsible for managing a guest virtual machine or machines. Tasks typically performed by Guest Administrators include connecting virtual devices, adding system updates, and managing applications that may reside on the operating system.

VM Security Recommendations



As we’ve just

described a host of security issues inherent in virtualized computing, let's examine some ways to protect the virtual machine. First we'll look at standard best practice security techniques that apply to traditional computer systems, and then we'll examine security techniques that are unique to virtualized systems.

Best Practice Security Techniques

The following security implementation techniques are required for most computer systems, and are still best practices for virtualized systems. These areas include physical security, patching, and remote management techniques.

Hardening the Host Operating System

Vulnerabilities inherent in the operating system of the host computer can fl ow upward into the virtual machine operating system. While a compromise on the VM OS would hopefully only compromise the guest domain, a compromise of the underlying host OS would give an intruder access to all services on all virtual machines hosted by the machine. Therefore, best practice hardening techniques must be implemented to maintain the security posture of the underlying technology. Some of these techniques include the following:

- Use strong passwords, such as lengthy, hard to guess passwords with letters, numbers, and symbol combinations, and change them often.
- Disable unneeded services or programs, especially networked services.
- Require full authentication for access control.
- The host should be individually firewalled.
- Patch and update the host regularly, after testing on a non production unit.

Use vendor-supplied best practice configuration guides for both the guest and host domains, and refer to some of the published standards in this area, such as the following:

- NIST Computer Resource Center (http://csrc.nist.gov)
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) (http://iase.disa.mil/stigs/index .html)
- Center for Internet Security (http://cisecurity.org)
- SANS Institute (http://www.sans.org)
- National Security Agency (NSA) (http://www.nsa.gov) We'll describe some of these techniques in detail.

Limiting Physical Access to the Host Basic physical host security is required to prevent intruders from attacking the hardware of the virtual machine

Using Encrypted Communications Encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used to provide secure communications links between the host domain and the guest domain, or from hosts to management systems. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking.

Disabling Background Tasks Most traditional server operating systems have multiple low-priority processes that are scheduled to run after primary business hours, when the server is expected to be less busy. Disabling, limiting, or off-loading these processes to other servers may be advisable if the host is beginning to suffer from resource contention.

Updating and Patching Most standards organizations enforce the concept of timely patching and updating of systems. Unfortunately, the proliferation of VMs in an organization adds complexity to the

patch control process. This means that not only must you patch and update the host OS promptly, but each of the virtual machines requires the same patching schedule. This is one reason standardization of an operating system throughout an enterprise is very important, if at all possible.

Enabling Perimeter Defense on the VM Perimeter defense devices are some of the oldest and most established ways of enforcing the security policy, by regulating data traffic ingress and egress. In fact, a common error of IT management is allocating too many resources (time and money) to purely perimeter defense, in the form of firewalls and hardened DMZ routers, while neglecting hardening the internal, trusted network. This often creates what's referred to as an M&M network security posture: crunchy on the outside but soft on the inside. The network is difficult to get into, but it lacks adequate controls once an intruder succeeds in penetrating the perimeter.

Implementing File Integrity Checks One of the tenets of information systems security is the preservation of fi le integrity — that is, the guarantee that the contents of a fi le haven't been subjected to unauthorized alterations, either intentionally or unintentionally. File integrity checking is the process of verifying that the fi les retain the proper consistency, and serves as a check for intrusion into the system.

Maintaining Backups We shouldn't even have to tell you this, but unfortunately we do. Perform image backups frequently for all production VMs. This will aid recovery of both individual fi les or the complete server image.

VM-Specific Security Techniques

A fundamental requirement for a successful virtualization security process is recognizing the dynamic nature of virtual machines. Therefore, many of the following security techniques are fairly unique to virtualized systems, and should be implemented in addition to the traditional best practice techniques just described.

Hardening the Virtual Machine Virtual machines need to be configured securely, according to vendor-provided or industry best practices. Because this hardening may vary according to the

vendor's implementation of virtualization, follow the vendor recommendations for best practice in this area. This hardening can include many steps, such as the following:
- Putting limits on virtual machine resource consumption
- Configuring the virtual network interface and storage appropriately
- Disabling or removing unnecessary devices and services
- Ensuring that components that might be shared across virtual network devices are adequately isolated and secured
- Keeping granular and detailed audit logging trails for the virtualized infrastructure It's important to use vendor supplied best practice confi guration guides for both the guest and host domains, and refer to some of the published standards in this area, such as:
- NIST Computer Resource Center (http://csrc.nist.gov/)
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) (http://iase.disa.mil/stigs/index.html)
- Center for Internet Security (http://cisecurity.org)
- SANS Institute (http://www.sans.org/)
- National Security Agency (NSA) (http://www.nsa.gov/) Let's look at some important VM hardening techniques.

Harden the Hypervisor It is critical to focus on the hypervisor as an attack vector, and strive to ensure that the hypervisor is deployed securely. Even before this stage, when you are evaluating various vendors' virtualization technology, place a premium on a vendor's track record of identifying vulnerabilities to its technology and the frequency of patch distribution.

Root Secure the Monitor Because most operating systems can be compromised through privilege escalation, the VM monitor should be "root secure." This means that no level of privilege within the virtualized guest environment permits interference with the host system.

Implement Only One Primary Function per VM While contemporary servers and virtual machines are adept at multi-tasking many functions, it's a lot easier to maintain secure control if the virtual machine is confi gured with process separation. It greatly complicates the hacker's ability to compromise multiple system components if the VM is implemented with one primary function per virtual server or device.

Firewall Any Additional VM Ports The virtual machine may open multiple ports linked to the host's external IP address, besides the usual ports opened by the host. These ports are used to connect remotely to the virtual machine layer to view or confi gure virtual machines, share drives, or perform other tasks.

The Center for Internet Security (CIS) recently published a Xen benchmark study11 that incorporates a lot of valuable security advice for hardening the host domain: "Before any virtual machines can be secure, the Host Domain of the host Linux operating system must be secure. A compromise of the Host Domain makes compromising the Guest Domains a simple task.

Use Unique NICs for Sensitive VMs If possible, VMs that contain confi dential databases and encrypted or sensitive information should have their network interface address bound to distinct and separate physical network interfaces (NICs). This external NIC would be the primary attack vector for intrusion, and isolation can help protect the VM.

Disconnect Unused Devices It's advisable to disconnect the unneeded default virtual machine device connections when configuring the VM. Because the VM can control physical devices on the host, it's possible to insert media with undesired code into the device, enabling the code to execute when the VM mounts. Enable host access to devices only when explicitly required by the VM.

UNIT-4

Securing the cloud

The Internet was designed primarily to be resilient; it was not designed to be secure. Any distributed application has a much greater attack surface than an application that is closely held on a Local Area Network. Cloud computing has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from pooled, virtualized, and outsourced resources.
In the report “Assessing the Security Risks of Cloud Computing,” Jay Heiser and Mark Nicolett of the Gartner Group (http://www.gartner.com/DisplayDocument?id=685308) highlighted the following areas of cloud computing that they felt were uniquely troublesome:
• Auditing
• Data integrity
• e-Discovery for legal compliance
• Privacy
• Recovery
• Regulatory compliance

Your risks in any cloud deployment are dependent upon the particular cloud service model chosen and the type of cloud on which you deploy your applications. In order to evaluate your risks, you need to perform the following analysis:
1. Determine which resources (data, services, or applications) you are planning to move to the cloud.
2. Determine the sensitivity of the resource to risk. Risks that need to be evaluated are loss of privacy, unauthorized access by others, loss of data, and interruptions in availability.
3. Determine the risk associated with the particular cloud type for a resource. Cloud types include public, private (both external and internal), hybrid, and shared community types. With each type, you need to consider where data and functionality will be maintained.
4. Take into account the particular cloud service model that you will be using. Different models such as IaaS, SaaS, and PaaS require their customers to be responsible for security at different levels of the service stack.
5. If you have selected a particular cloud service provider, you need to evaluate its system to understand how data is transferred, where it is stored, and how to move data both in and out of the cloud. You may want to consider building a flowchart that shows the overall mechanism of the system you are intending to use or are currently using.

One technique for maintaining security is to have “golden” system image references that you can return to when needed. The ability to take a system image off-line and analyze the image for vulnerabilities or compromise is invaluable. The compromised image is a primary forensics tool. Many cloud providers offer a snapshot feature that can create a copy of the client's entire environment; this includes not only machine images, but applications and data, network interfaces, firewalls, and switch access. If you feel that a system has been compromised, you can replace that image with a known good version and contain the problem.
Many vendors maintain a security page where they list their various resources, certifications, and credentials. One of the more developed offerings is the AWS Security Center, shown in Figure 12.1, where you can download some backgrounders, white papers, and case studies related to the Amazon Web Service's security controls and mechanisms.

Architecture and Data Security

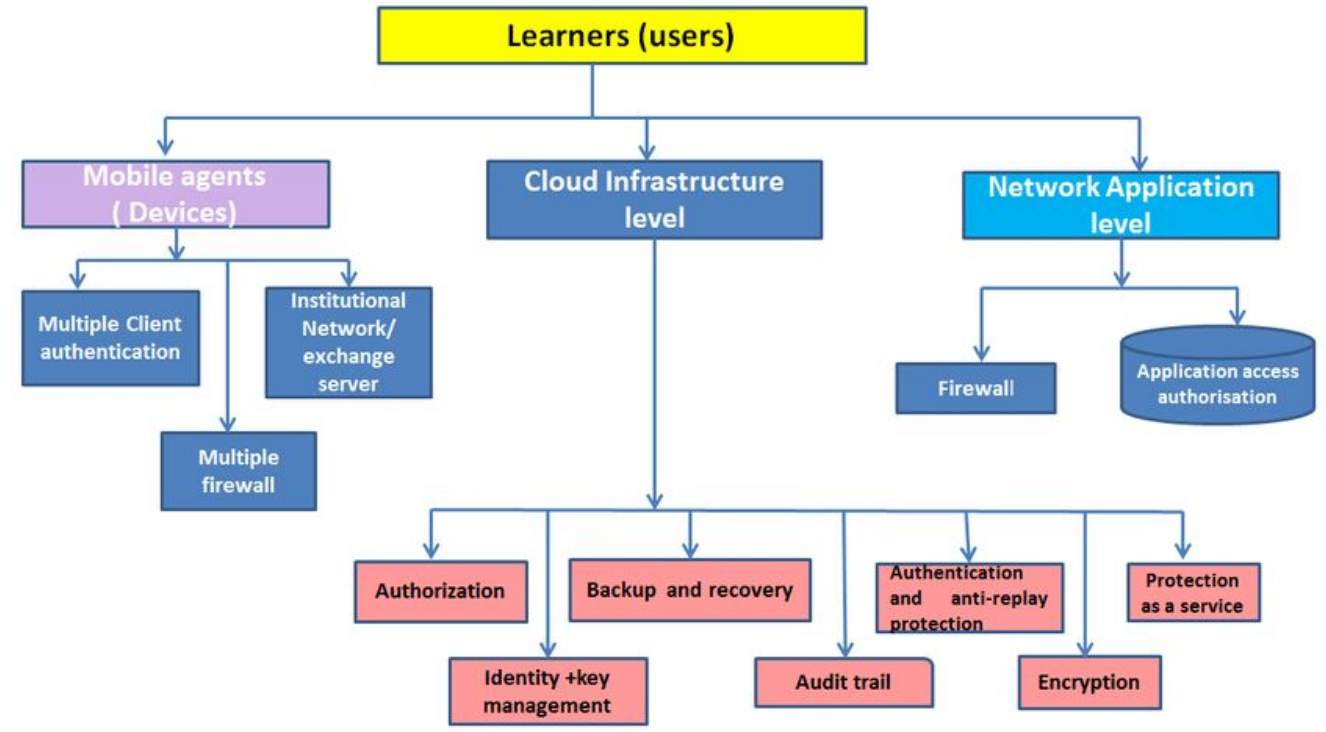
Taking information and making it secure, so that only yourself or certain others can see it, is obviously not a new concept. However, it is one that we have struggled with in both the real world and the digital world. In the real world, even information under lock and key, is subject to theft and is certainly open to accidental or malicious misuse. In the digital world, this analogy of lock-and-key protection of information has persisted, most often in the form of container-based encryption. But even our digital attempt at protecting information has proved less than robust, because of the limitations inherent in protecting a container rather than in the content of that container. This limitation has become more evident as we move into the era of cloud computing: Information in a cloud environment has much more dynamism and fluidity than information that is static on a desktop or in a network folder, so we now need to start to think of a new way to protect information.

Before we embark on how to move our data protection methodologies into the era of The cloud, perhaps we should stop, think, and consider the true applicability of information security and its value and scope. Perhaps we should be viewing the application of data security as less of a walled and impassable fortress and more of a sliding series of options that are more appropriately termed “risk mitigation.”

The reason that I broach this subject so early on is that I want the reader to start to view data security as a lexicon of choices, as opposed to an on/off technology. In a typical organization, the need for data security has a very wide scope, varying from information that is set as public domain, through to information that needs some protection (perhaps access control), through to data that are highly sensitive, which, if leaked, could cause catastrophic damage, but nevertheless need to be accessed and used by selected users.

One other aspect of data security that I want to draw into this debate is the human variable within the equation. Computer technology is the most modern form of the toolkit that we have developed since human prehistory to help us improve our lifestyle. From a human need perspective, arguably, computing is no better or worse than a simple stone tool, and similarly, it must be built to fit the hand of its user. Technology built without considering the human impact is bound to fail. This is particularly true for security technology, which is renowned for failing at the point of human error.

If we can start off our view of data security as more of a risk mitigation exercise and build systems that will work with humans (i.e., human-centric), then perhaps the software we design for securing data in the cloud will be successful.



Security Requirements for the Architecture

One goal for architecture is that it should be appropriate in meeting needs. This section surveys key architectural requirements for a typical cloud implementation. Several factors serve as the underlying motivation for requirements; these include:

Costs and Resources The cloud provider's financial resources will act to constrain investment in technology, security controls included. But it is important to recognize that the absence of unlimited resources can be very motivating to how one designs, architects, and builds. For instance, if you know that your staff will be small, then this can force you toward process improvement and greater automation. Likewise, cost is also a motivation for the consumer of cloud services. The nature of these constraints tends toward the development of services with operating characteristics that are not ideal for all consumers

Reliability This is a quality that refers to the degree you can depend on a system to deliver its stated services. Reliability can be described as a guarantee that the underlying technology can provide delivery of services.

Performance A measure of one or more qualities that have to do with the usefulness of a system. By example, common measures include responsiveness to input and the amount of throughput the system can handle.

The Security Triad The essential security principles of confidentiality, integrity, and availability apply to most systems; the responsibility of a security architect is to match security controls with security requirements that sometimes must be derived from the need to assure the other three drivers (reliability, performance, and cost).

Legal and regulatory constraints (we have covered these to some extent in Chapter 3) Legal and regulatory constraints can lead to the need for many additional requirements having to do with technical security controls, access policies, and retention of data among many others.

We begin with an unusual area of requirements for system security requirements: Physical security. But, by the time we are done you will see what motivates this.

Security Patterns and Architectural Elements

This section examines several patterns and elements that support or contribute to cloud security. Investing effort to develop such patterns will pay dividends during the build process, during operations and will often contribute to better security.

Defense In-depth:
The term Defense in-depth in computer and network security was first documented in a 1996 paper Information Warfare and Dynamic Information Defense, 3 and was adopted from military operations. This approach has been used for system and network security under a number of names, including layered defense. Essentially, this is a strategy that accounts for the fact that individual security controls are typically incomplete or otherwise not sufficient, and that multiple reinforcing mechanisms or controls will compose a more complete and robust security solution. Such reinforcing controls can be similar and redundant, but can also be implemented or layered at different levels throughout the implementation. When using a series of layers consisting of even the same type of mechanism, residual risk can be significantly reduced.

Honeypots
A honey pot is a well-known and sophisticated network decoy technique. In an enterprise network, the goal of a honeypot is to create a false or non production system that appears enticing for an attacker to target. After the attacker is lured to that target, the honeypot is used to observe, distract, and potentially alarm on the attacker's network penetration. In any event, the objective is that if the attacker is wasting time in the honeypot, they aren't in your production systems

Sandboxes
Sandboxing, at the software layer, by its very definition uses a form of virtualization or abstraction between the software or code being executed from the OS in which it is running. As a result, it's very similar to hypervisor-based virtualization, running one layer up between the OS and the hardware, instead of between the OS and the application. One of the goals of the defense in-depth model is to add layers of security. Without a doubt, a sandboxed environment adds such a layer of security between the applications running within a guest virtual machine and the hypervisor.

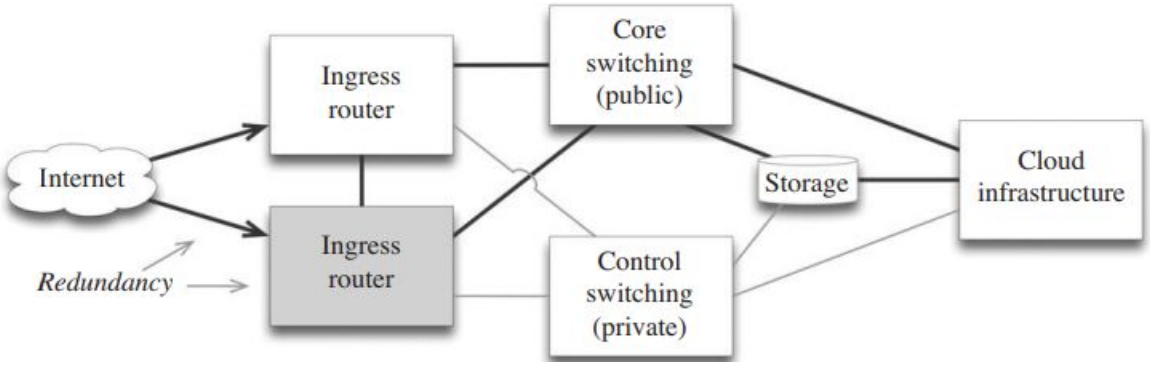
Network Patterns
Cloud infrastructure deviates from traditional IT infrastructure at many levels, including networking. Public clouds face several challenges in terms of ensuring sufficient network isolation between tenants, especially when VMs that are assigned to different tenants are colocated on a physical server.

Isolation of VMs Switching infrastructure in the cloud can't isolate traffic between VMs that reside on a single hardware platform because this traffic is limited to a shared physical machine and does not enter the cloud network. Without use of encryption for this traffic, VMs could observe traffic that belongs to an adjacent VM—but the ability to do this will be a function of how the hypervisor implements networking. The use of encryption for VM network traffic can result in effective network

isolation between adjacent VMs. The overall security in this case heavily depends on the security controls of each VM and on the isolation between VMs that the hypervisor affords.

Isolation of Subnets

There are other network patterns that can be followed for cloud architecture. By segregating the network into physically separate networks, you can improve isolation between public-accessed subnets and infrastructure control subnets (as depicted in Figure 4.4). Network isolation can be achieved to a point by use of network virtualization, but this is subjected to vulnerabilities and misconfiguration. Physical separation is also prone to error, but process controls can be used to minimize the probability.



Cloud Security Architecture:

The first part of this chapter identified requirements for security and patterns to architect cloud security. Taking that material and composing some of those elements into representative security architectures is our goal for this section. To some, the security of a cloud computing architecture can be summarized in one phrase: Everything in a cloud is at scale. Cloud providers deploy massive amounts of infrastructure to capture economies at scale, tenants and users adopt that infrastructure at scale, and some believe that the threats that occur at the cloud level are threats that may be realized at scale and by everyone in the cloud. The cloud security space is still evolving, as is the technology used to implement clouds. It appears that the technology that powers the cloud is progressing at a rate that is faster than the technology used to secure clouds. In part, this goes far beyond any particular vendor or software and reflects on the state of systems and security in general.

Planning Key Strategies for Secure Operation:

The process of architecting a cloud can benefit from planning for the activities of operating the cloud. Understanding eventual operational processes and constraints can lead to better architecture and to a cloud that is more effectively operated and more secure. This section explores several areas that can offer key strategies that will pay off later in the cloud life cycle.

Classifying Data and Systems

Knowing what you have and having a formal structure for it is a great advantage when planning for how to protect it. To begin, one can identify categories of information that can be processed with lesser security concern and fewer controls than other kinds of data. That sort of information classification would lend itself to a public cloud, to hybrid cloud processing, or to a community cloud.

Various types of data bring with them the need for higher security concern, regulatory handling requirements, and even national security level processing requirements (you know who you are). National security information, be it Federal, military, or intelligence data will generally fall under the following hierarchical classification levels: Unclassified, Sensitive But Unclassified, Confidential, Secret, and Top Secret. These levels are hierarchical in terms of entailing increasing levels of security and additional handling requirements. Users are vetted before they can obtain a clearance to access data at a given classification level, and then access is generally granted on a need-to-know basis. Additional subcategories of classification can be as sedimented within a classification level and entail the need to maintain separation even from users who are cleared at the same, say Top Secret level but who have not been read into the category in question. The national security information classification scheme is very mature and quite effective in managing control over and access to classified information. However, it also tends toward over classifying information based on the consequences of data exposure.

Define Valid Roles for Cloud Personnel and Customers:
This section discusses two broad kinds of roles. Some define authorization classes for operational segregation, whereas the other roles define authority for policy, design, and standards. There will be several roles for internally infrastructure-focused personnel, system-focused personnel, security-focused personnel, management-focused personnel, externally service consumer-focused personnel as well as end user roles. Understanding these various roles is critical for policy, operations, and developing an effective and well-run cloud. The following list is derived from the Open Security Architecture 6, and serves as an example for such roles

• End Users Will require security awareness training and access agreements. To support users, need: Access management, access enforcement, user identification and authentication, device identification and authorization, cryptographic keys.
• Architect Information flow enforcement, acquisitions, information system documentation.
• Business Manager Responsible for risk assessment, risk assessment updates, allocation of resources.
• IT Manager Access control policies and procedures, supervision and review of access controls, security awareness and training policy, among many similar functions.
• Other Other roles include Independent Auditors, Developers, Security Administrators, Server Administrators, and Network Administrators.

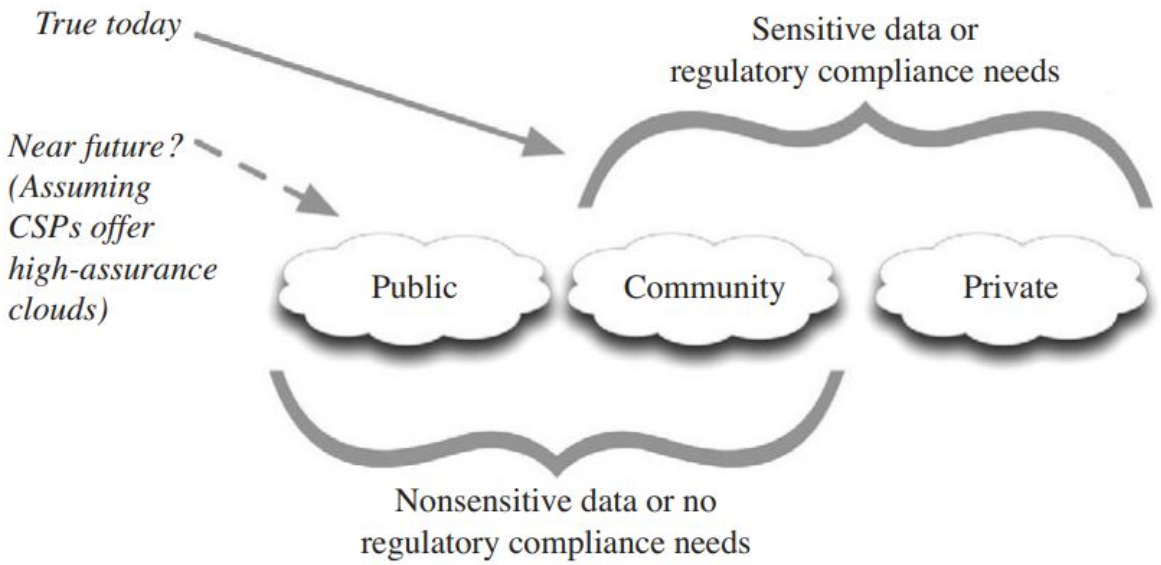
Overview of Data Security in Cloud Computing
It is understandable that prospective cloud adopters would have security concerns around storing and processing sensitive data in a public or hybrid or even in a community cloud. Compared to a private data center, these concerns usually center on two areas:

- Decreased control by the owning organization when data is no longer managed within an organization’s premises
- Concern by the owning organization that multitenancy clouds inherently pose risks to sensitive data

Control over Data and Public Cloud Economics
In contrast to use of a public cloud, maintaining organizational physical control over stored data or data as it traverses internal networks and is processed by on-premises computers does offer potential advantages for security. But the fact is that while many organizations may enforce strict on-premises-only data policies, few organizations actually follow through and implement the broad controls and the disciplined practices that are necessary to achieve full and effective control.

Organizational Responsibility:

Ownership and Custodianship While an organization has responsibility for ensuring that their data is properly protected as discussed above, it is often the case that when data resides within premises, appropriate data assurance is not practiced or even understood as a set of actionable requirements.

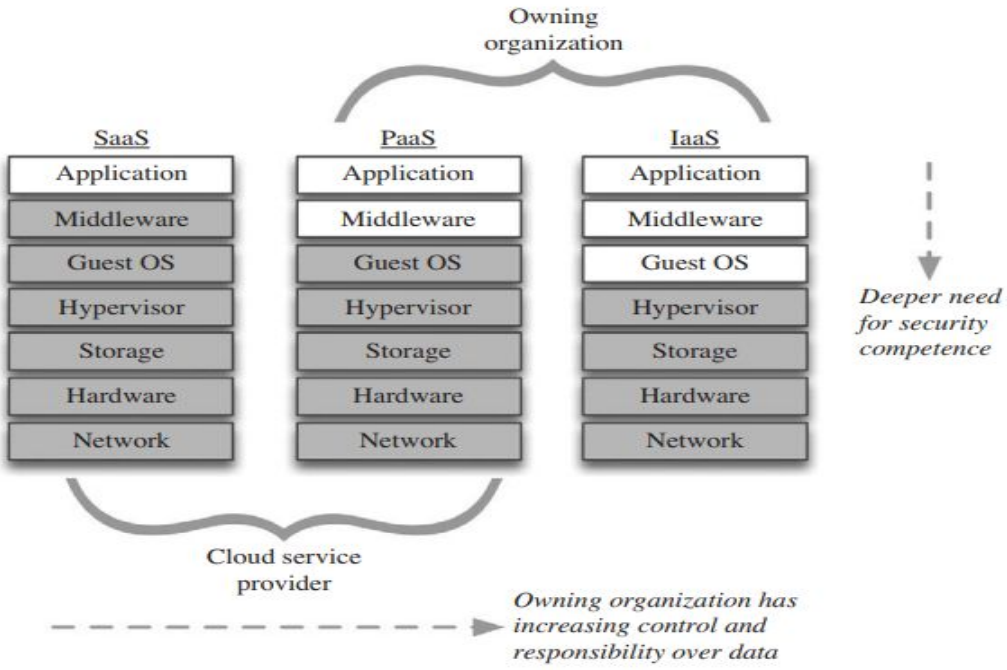


Data at Rest

Data at rest refers to any data in computer storage, including files on an employee's computer, corporate files on a server, or copies of these files on off-site tape backup. Protecting data at rest in a cloud is not radically different than protecting it outside a cloud. Generally speaking, the same principles apply. As discussed in the previous section, there is the potential for added risk as the data owning enterprise does not physically control the data. But as also noted in that discussion, the trick to achieving actual security advantage with on-premises data is following through with effective security.

Data in Motion

Data in motion refers to data as it is moved from a stored state as a file or database entry to another form in the same or to a different location. Any time you upload data to be stored in the cloud, the time at which the data is being uploaded data is considered to be data in transit. Data in motion can also apply to data that is in transition and not



necessarily permanently stored. Your username and password for accessing a Web site or authenticating yourself to the cloud would be considered sensitive pieces of data in motion that are not actually stored in unencrypted form.

Common Risks with Cloud Data Security

Several risks to cloud computing data security are discussed in this section. None of these are unique to the cloud model, but they do pose risk and must be considered when addressing data security. They include phishing, CSP privileged access, and the source or origin of data itself.

Phishing

One indirect risk to data in motion in a cloud is phishing. Although it is generally considered unfeasible to break public key infrastructure (PKI) today (and therefore break the authentication and encryption), it is possible to trick end users into providing their credentials for access to clouds. Although phishing is not new to the security world, it represents an additional threat to cloud security.

Provider Personnel with Privileged Access

Another risk to cloud data security has to do with a number of potential vectors for inappropriate access to customer sensitive data by cloud personnel. Plainly stated, outsourced services—be they cloud-based or not—can bypass the typical controls that IT organizations typically enforce via physical and logical controls. This risk is a function of two primary factors: first, it largely has to do with the potential for exposure with unencrypted data and second, it has to do with privileged cloud provider personnel access to that data.

Data Encryption: Applications and Limits

Bruce Schneier discussed how the information age practice of encrypting data at rest deviates from the historical use of cryptography for protecting data while it is communicated or in transit. One of Schneier's key points is that for data in motion, encryption keys can be ephemeral, whereas for data at rest, keys must be retained for as long as the stored data is kept encrypted. As Schneier points out, this does not reduce the number of things that must be stored secretly; it just makes those things smaller (the size of a key is far smaller than a typical data file). As Schneier states: "This whole model falls apart on the Internet. Much of the data stored on the Internet is only peripherally intended for use by people; it's primarily intended for use by other computers. And therein lies the problem. Keys can no longer be stored in people's brains. They need to be stored on the same computer, or at least the network, that the data resides on. And that is much riskier."2 In meeting this challenge, there has been a recent rise in the number of security appliances that are intended to address this and related security implementation issues for data security in clouds.

Overview of Cryptographic Techniques

Cryptography is a complex and esoteric field. In modern times, cryptography has expanded from protecting the confidentiality of private communications to including techniques for assuring content integrity, identity authentication, and digital signatures along with a range of secure computing techniques. Given that range of functional utility, cryptography has been recognized as being a critical enabling technology for security in cloud computing. Focusing on data security, cryptography has great value for cloud computing.

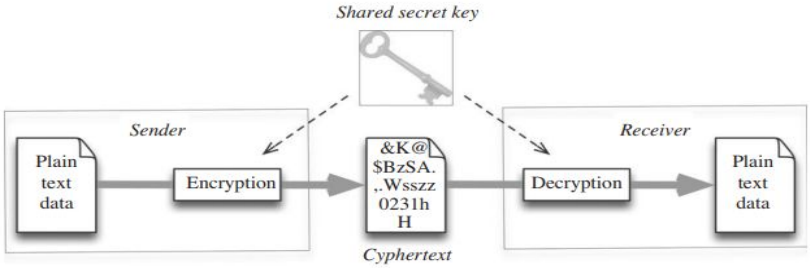


FIGURE 5.3
Symmetric encryption.

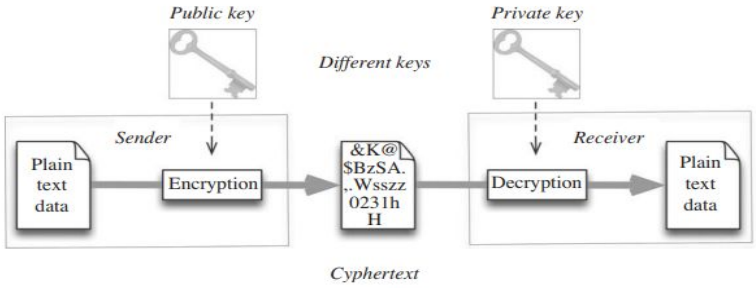


FIGURE 5.4
Asymmetric encryption.

This use of public–private keys is a great enabler for confidentiality in cloud computing, and not just for encryption of content. A private key can be used to authenticate a user or computational component, and it can also be used to initiate the negotiation of a secure channel or connection between communicating parties. Going one level deeper in our background treatment of cryptography, for the purpose of this book, there are four basic uses of cryptography:

• **Block Ciphers** These take as input a key along with a block of plaintext and output a block of cyphertext. Because messages are generally larger than a defined block, this method requires some method to associate or knit together successive cyphertext blocks.
• **Stream Ciphers** These operate against an arbitrarily long stream of input data, which is converted to an equivalent output stream of cyphertext.
• **Cryptographic Hash Functions** Hash functions take an arbitrarily long input message and output a short, fixed length hash. A hash can serve various purposes, including as a digital signature or as a means to verify the integrity of the message.
• Authentication Cryptography is also widely used within authentication and identity management systems.

Common Mistakes or Errors with Data Encryption

Cryptography has become pervasive and broadly accessible for even the average computer users to secure their digital files on local or remote storage, as well as for communication. But as commonly available as cryptography is, it is too often either not used when it should be or it is implemented or used in insecure or ineffective ways. The most obvious example of the ineffective use of cryptography might well be using cryptography to achieve secure communications and authentication with an Internet service, only to do so from a PC that is hopelessly out-ofdate in security patches or that harbors spyware and is otherwise compromised. In such a case, the dedicated use of strong cryptography from this platform amounts to affixing a bank vault door on a cardboard box

i

Cloud Data Security: Sensitive Data Categorization

When it comes to cloud data protection methods, no particularly new technique is required. Protecting data in the cloud can be similar to protecting data within a traditional data center. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing. This section will briefly review these methods and will note anything that is particularly unique to when these are deployed in a cloud.

Authentication and Identity

Maintaining confidentiality, integrity, and availability for data security is a function of the correct application and configuration of familiar network, system, and application security mechanisms at various levels in the cloud infrastructure. Among these mechanisms are a broad range of components that implement authentication and access control. Authentication of users and even of communicating systems is performed by various means, but underlying each of these is cryptography. Authentication of users takes several forms, but all are based on a combination of authentication factors: something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them (such as a fingerprint). Single factor authentication is based on only one authentication factor. Stronger authentication requires additional factors; for instance, two factor authentication is based on two authentication factors (such as a pin and a fingerprint).

Access Control Techniques Access control mechanisms are a key means by which we maintain a complex IT environment that reliably supports separation and integrity of different levels or categories of information belonging to multiple parties. But access controls do not stand on their own; they are supported by many other security capabilities. In addition, as we will discuss in Chapter 7 (Security Criteria: Building an Internal Cloud), access control is dependent on an identity management capability that meets the needs for the implementation.

• Discretionary Access Control (DAC) In a system, every object has an owner. With DAC, access control is determined by the owner of the object who decides who will have access and what privileges they will have. Permission management in DAC can be very difficult to maintain; furthermore, DAC does not scale well beyond small sets of userss

• Role Based Access Control (RBAC) Access policy is determined by the system. Where with MAC access is based on subject trust or clearance, with RBAC access is based on the role of the subject. A subject can access an object or execute a function only if their set of permissions—or role—allows it.

• Mandatory Access Control (MAC) Access policy is determined by the system and is implemented by sensitivity labels, which are assigned to each subject and object. A subject's label specifies its level of trust, and an object's label specifies the level of trust that is required to access it. If a subject is to gain access to an object, the subject label must dominate—be at least as high as—the object label.

Data Categorization and the Use of Data Labels

Putting in place effective and appropriate controls for information systems requires an understanding of the nature of the information. In this regard, sensitive or otherwise valuable data should be categorized to support data security. By identifying data according to sensitivity, one can implement various strategies to better protect such data. Unfortunately, understanding what other cloud data may require protection may not always be clear. Data that a user chooses to store in the

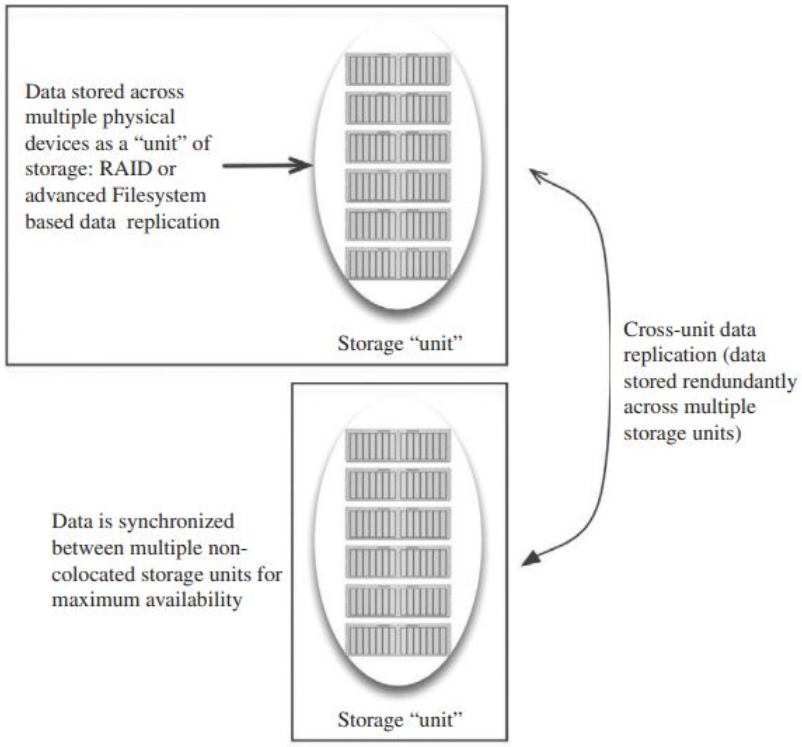
cloud may not require protection if it is not sensitive or if it can easily be recovered. But generally, protecting data is a universal requirement regardless of its value, if for no other reason than failing to do so leads to all manner of complexity, consequence, and mischief.

Cloud Data Storage

Among other advances, cloud computing has brought advantages in the form of online storage. In this section, we are referring to Storage-as-a-Service. The range of service offerings in this space is remarkable, and they are continuing to grow. Data security for such a cloud service encompasses several aspects including secure channels, access controls, and encryption. And, when we consider the security of data in a cloud, we must consider the security triad: confidentiality, integrity, and availability.

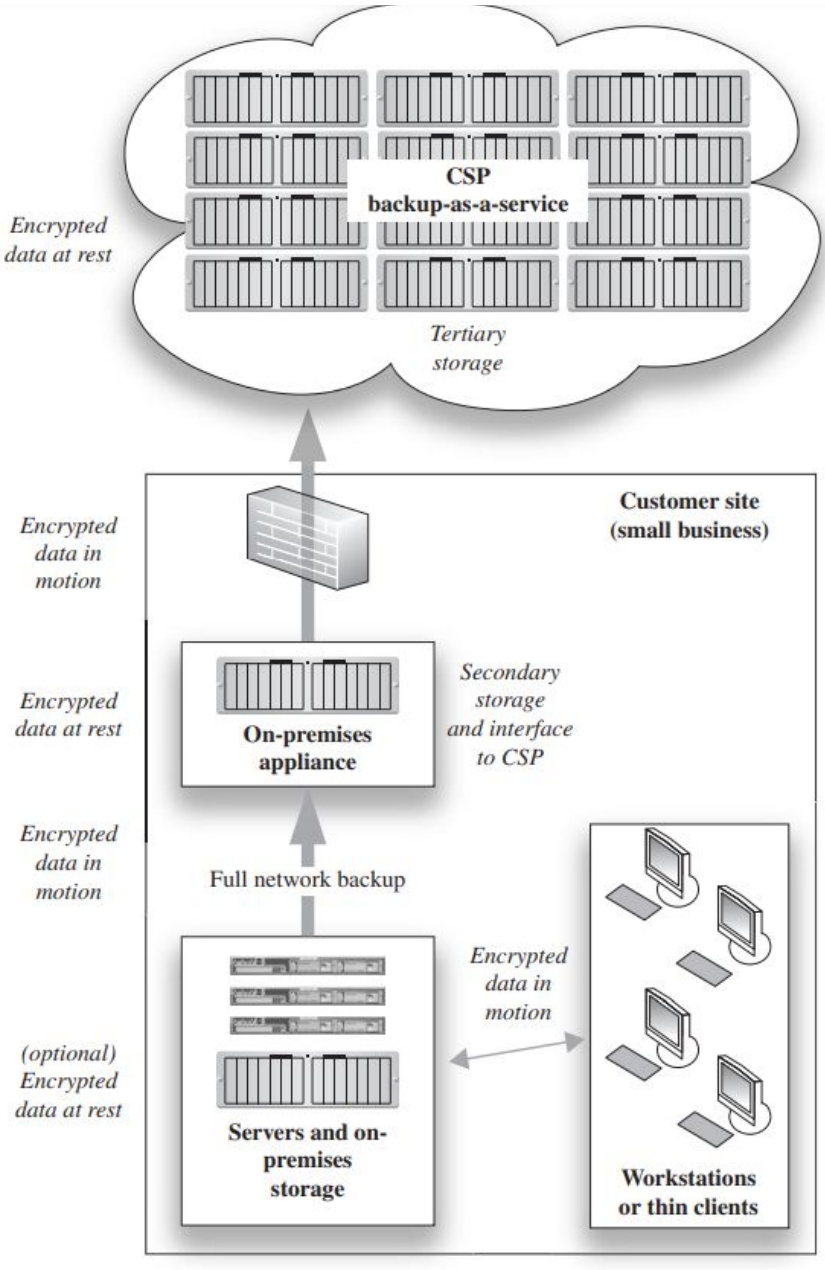
In the cloud storage model, data is stored on multiple virtualized servers. Physically the resources will span multiple servers and can even span storage sites. Among the additional benefits of such generally low-cost services are the storage maintenance tasks (such as backup, replication, and disaster recovery), which the CSP performs. The most notable provider in this space is Amazon with its S3 (Simple Storage Service). Amazon launched S3 in March of 2006.

A common aspect of many cloud-based storage offerings is the reliability and availability of the service. Figure 5.6 depicts an abstracted view of how many individual disks in many aggregated storage devices are composed into a virtualized unit of storage. Replication of data is performed at a low level by such mechanisms as RAID or by a file system. One such file system is ZFS, which was designed by Sun Microsystems as both a file system and a volume manager. ZFS supports high storage capacities and performs numerous security relevant functions including copy-on-write cloning and continuous integrity checking along with automatic repair.



Cloud Lock-in

A number of questions about adopting public clouds have to do with what might happen when an external cloud becomes business-critical for the organization. One of these questions involves concern over cloud lock-in. As George Harrison wrote in the song Stuck Inside a Cloud: “Talking to myself, Crying out loud,



Only I can hear me, I’m stuck inside a cloud.”C,4 The concern here is that once you become dependent on the services of a cloud provider, you may find it extremely difficult to switch providers due to any number of technical reasons.
In one lock-in example, a company may subscribe to a specific public CSP service as their customer relationship management tool. This service may consequently end up being used to house all of the company’s data relating to their customers. The company may invest significant effort in customizing rules or reporting routines in their use of this service. The service may also become the primary reporting engine that provides management insight to the health of the business. If the service entails proprietary formats or APIs, then the service subscriber may very well not own anything other than the data. If the company decides to discontinue the service, then the organization may retain no value for any effort they performed in tailoring the service for their needs. If the data formats are proprietary, the company could conceivably face serious challenges when migrating their data to a replacement system or service.

Metadata
Further questions in this lock-in scenario might include what happens to a customer’s data when they terminate their service? Who else might be able to access it? This is further complicated by the fact that if the organization used the cloud service over a considerable length of time, then it is almost guaranteed that there is a tremendous amount of data that was developed by simply using the cloud—sometimes referred to as cloud metadata. Metadata is simply data about data, or more precisely, it is highlevel information about such things as to where the data came from, who performed what operations against it, and when changes were made. But cloud metadata that is developed may include other very valuable information that records associative context based on users and their relationship with content. In a SaaS solution, this kind of information may be developed over time by the CSP’s software.

Avoiding Cloud Lock-in (the Roach Motel Syndrome) Fortunately, many of the large public cloud services organizations that exist today provide the ability to export not only data but also metadata generated by its subscribers. Any enterprise should seriously consider this as a vital feature to have before adopting any cloud service that could become critical to their business. It could be unrealistic to assume that you will always maintain a service with a particular cloud provider. If there is no mechanism to retrieve your data, then the resulting situation can present a dilemma of costly proportions.

Key strategies to secure the cloud

In the cloud, the segregation of duties will already be partially implemented by the nature of the model itself, namely IT will be responsible for managing all aspects of the physical infrastructure. Requests for changes by the cloud provider for the cloud itself will go through a configuration management process where they will be vetted by all the major business functions—security included. And, depending on the cloud deployment model—public, community, or private—the tenant will have a varying degree of responsibility for and opportunity to effect service, software, and other configuration changes. Likewise, the nature of the service models increasingly limit the scope of control the tenant or user has from IaaS to SaaS.

Especially sensitive functions should entail a two-person rule to assure that the function is not only properly invoked but done so under proper circumstances. Similarly, different roles should be defined to configure and manage computer and network security controls. By example, resetting a user's credentials or privileges. Where such actions are performed without organizational process controls, management over user access rights is not reliable. In addition, with cloud services, there are multiple areas of responsibility with the potential to mismanage resources (human error is legendary). These different areas include roles that lie with the CSP and roles that a tenant has responsibility for. By dividing the levers of control enables faster changes and also more informed decisions over privileged management operations. It does bear mentioning that many of the configuration changes that a tenant of a public IaaS service can make can have a significant impact on both the security of their service and on the metered costs.
There is another aspect to segregation of duties and different roles and responsibilities. Not all processes can be fully automated, and even for those that should be automated it is not always the case that this can be achieved given overall budgets, schedules, and competitive pressures. On the path toward automation one will often start by employing people following well-defined steps and processes, eventually converting these to automated processes. And it is also often the case that automated processes have backup manual procedures. Again—whether automated or manual—cloud administration and operational processes must be controlled to meet the goals of segregation of duties and maintain security.

Best practices for cloud computing

The Cloud Computing Use Case Discussion Group is focused on best practices for building clouds or IaaS and PaaS. In July 2010, they published version 4.0 of their Cloud Computing Use Cases White Paper. Besides detailing a number of use cases for cloud computing, this group also identified a number of security controls for cloud computing. The following summarizes these

• Asset Management All assets including hardware, network, and software that comprise the cloud infrastructure must be managed.
• Cryptography: Key and Certificate Management They advocate for an infrastructure to manage keys and certificates, and encourage the use of standards-based cryptography.
• Data/Storage Security They identify the need to support encrypted storage of data and they recognize that some users will need separate storage from others.
• Endpoint Security Secure endpoints for cloud resources, along with end point restrictions by protocol and device types.
• Event Auditing and Reporting This entails visibility by consumers into security-relevant events and breaches.
• Identity, Roles, Access Control, and Attributes Effective implementation of access controls and security policy enforcement depends on defined identity, roles, and privileges.
• Network Security Network traffic must be able to be secured at the level of switches, routers, and packets.
• Other controls listed by the Cloud Computing Use Case Discussion Group Service Automation, Workload and Service Management, and Security Practices.

Other Best Practices for Cloud Computing: Cloud Service Consumers

Beyond the CSA's Best Practices, NIST has offered a relatively short set as well. Distilling guidance from traditional security best practices, the CSA's list and a range of NIST sources the following is representative of practices for a cloud consumer:

• State-of-the-Practice Select a CSP based in part on their attention to security and how their overall security compares to current practices.
• Transparency Select a CSP based on their willingness to offer transparency into key security practices, including risk assessment and incident response. CSPs who meet this will also likely have a customer-facing CSO or CISO.
• Security Controls A CSP should furnish security control and practice information that the customer can use to map against their policy requirements.
• Security Standards and Practices A CSP should view many of their security efforts as not just good security, but also as competitive differentiation. This is especially the case with adherence to secure coding practices, use of security standards and products that have passed independent evaluation.

Security monitoring

It is a best practice to automate the collection of security events from all securityrelevant network devices, servers, and applications. These events should be archived in raw form to preserve a legal record of all security-relevant activity and being assessed via automated means to detect situations warranting alerts.
Security monitoring in cloud infrastructure and services is based on the generation, collection, analysis, and reporting of security-relevant event data. We can refer to the source events as security instrumentation data or security telemetry. This amounts to any security-relevant data that is generated by a system, network, or application, along with any other data that may be developed by observing the security-relevant behavior of a system. The scope of what can be collected is broad and the level of detail can be overwhelming. Collection probes can be used to instrument every aspect of a cloud, gathering information on user, application, and system activity, as well as observing data in motion as packets cross-observation points.

• Knowledge about the infrastructure, such as that which is maintained in a CMDB or similar information about the monitored infrastructure.
• Event data that is a form of output from the cloud infrastructure.
• Security rules and heuristics that are used to assess the event data.

These three kinds of information sources are used to some extent in modern security monitoring systems. Admittedly, there is no published use of a CMDB to illuminate monitoring and guide automated analysis, but this section (Security Monitoring) will discuss the potential for this in greater detail. Figure 6.6 also makes representations about the effectiveness of a security feedback loop. Again, although there are few published descriptions of using security monitoring with feedback loops, doing so is to embrace a forward edge of the field. What this figure seeks to convey is the relationship between cloud security, output from the cloud that enables security monitoring, the role of the CMDB as an additional source of monitoring input, and an automated means to effect feedback to control the cloud.

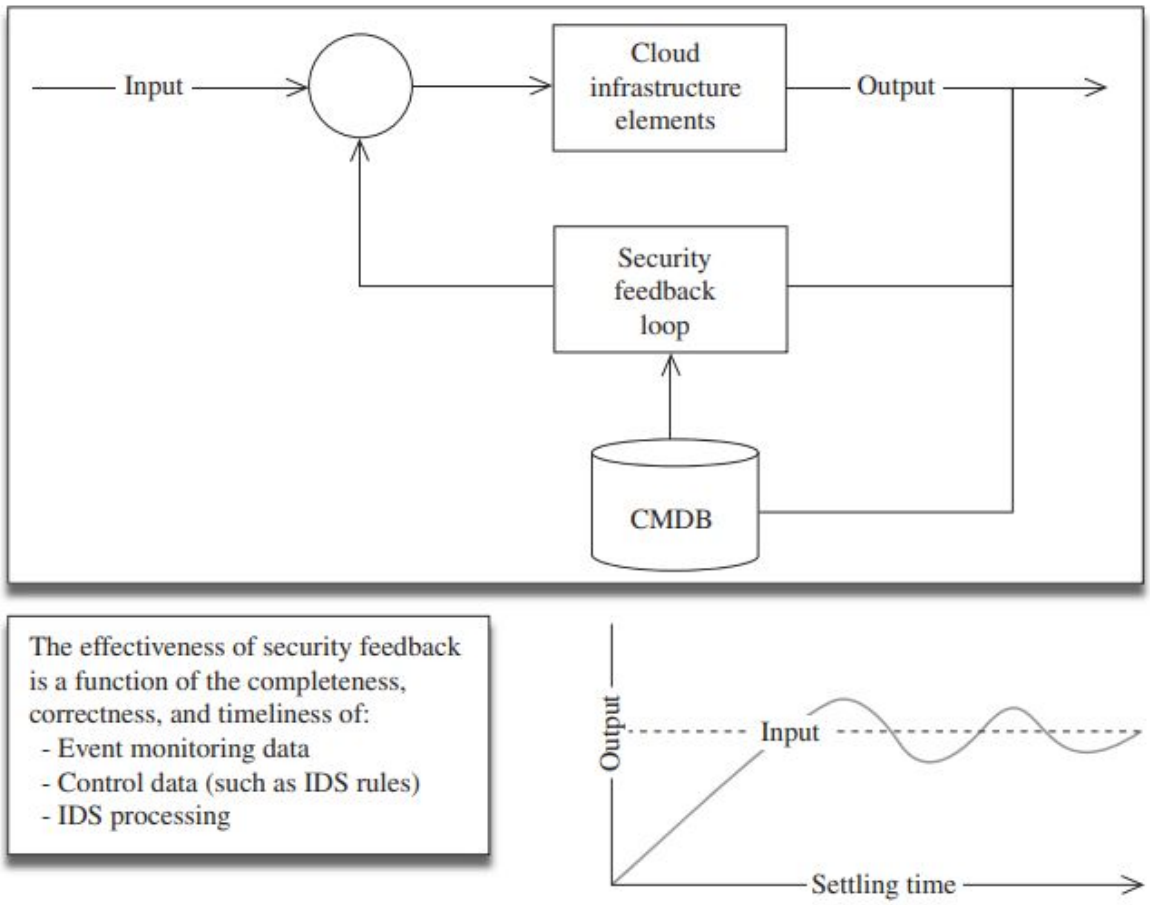


FIGURE 6.6

Security monitoring and security feedback.