13

Security in Cloud Computing

Learning Objectives

The main objective of this chapter is to provide an overview of security issues in cloud computing. After reading this chapter, you will

- Understand the different security aspects
- Understand the security issues in cloud service models
- Understand identity management and access control issues related to security
- Understand audit and compliance in security

Preamble

Security is an important aspect to be considered in the cloud computing environment. This chapter focuses on different aspects of security. We begin with the introduction to cloud security. Subsequent sections talk about data security; virtualization security; security issues in Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) models; etc. This chapter also considers privacy challenges and identity and access management issues in cloud. After reading this chapter, the reader can get an overview of security issues in different service models in cloud. The reader can also get an idea of challenges in these security issues.

13.1 Introduction

Cloud computing has entered everyone's life today irrespective of technology or any other aspect. Every tech magazine or every information technology (IT) organization website speaks about cloud computing. What exactly is

this cloud computing? What does it do to make our lives more easier? To answer all these questions, let us look into the details of cloud computing with respect to technology more precisely.

13.1.1 Cloud in Information Technology

Cloud computing has revolutionized the IT industry for the past decade and is still developing creative ways to solve current problems. Companies and research institutes are slowly moving to the cloud to address their computing needs.

So, why is the cloud attractive to the public and private sectors? To answer this question, let us see what is put into cloud by an organization.

To make cloud more user friendly for computing, the industry has invested a lot into the following aspects:

1. *Time and finance*: The cloud is a centralized system and updates real-time information. Businesses with time-sensitive data are quick to grab this opportunity and harness the efficiency of the cloud. For example, medical researches that needed months of in-house number crunching moved to distributed systems, significantly reducing computing time and expenses.
2. *People and association*: With the advent of cloud, an online collaboration between distributed teams became easy. It is now easier to communicate and work with people located in different areas, sometimes different countries, during office hours. Teams now consist of members distributed across large geographic areas. As mentioned, the capability of the cloud to update information in real time enables teams to address issues immediately. Working together no longer means meeting up in the boardroom. Internet Protocol (IP) telephony, such as Skype and Google Hangout, provides a platform that allows team members to discuss tasks without stepping a foot outside their cubicles.
3. *Replacing hardware*: Relocating information and data systems to the cloud not only saves money but also reduces wasted resources. Companies no longer need to purchase hardware and systems that need installation and maintenance. Data centers on the cloud can reallocate these resources to clients by saving company dollars only by paying what is used and avoiding the purchase of machines that will not be useful in the long run. Cloud service providers (CSPs) also have the ability to optimize their systems to reduce waste. They also have the capability of upgrading their systems according to service demands. This is usually very expensive for businesses to do and results in wasted resources. Fewer in-house machines means that companies could redirect funds toward improving other aspects of business operations.

4. *Energy efficient*: A study reports that clients of Salesforce produced 95% less carbon compared to companies with systems in their premises.
5. *Study from Accenture, Microsoft, and WSP Environment and Energy*: A 2010 study from Accenture, Microsoft, and WSP Environment and Energy reported a huge impact of the cloud on CO_2 emissions. They found out that businesses with systems and applications on the cloud could reduce per-user carbon footprint by 30% for large companies and 90% for small businesses.
6. *Going green*: Greenpeace pointed out in a recent study that while efficiency is increasing, the energy source is also varying. The internal operations of data centers are *green,* but it is superficial if the power source is nonrenewable. With the increasing demand for cloud computing, energy consumption is expected to increase by 12% each year. An analysis of Greenpeace showed that out of the 10 leading tech companies—Akamai, Amazon, Apple, Facebook, Google, HP, IBM, Microsoft, Twitter, and Yahoo!—Akamai and Yahoo! are the most environment friendly and Apple the least. The report also highlighted Google's effort in *greening* its energy sources.
7. *The future of the cloud and the environment*: Two companies in Iceland, Green Earth Data and GreenQloud, both claim to offer 100% renewable energy by powering their data centers with geothermal and hydropower resources, which are abundant in the country. "The internet with cloud computing is becoming a big contributor to carbon emissions because of dirty energy usage," GreenQloud aims to set an example to cloud computing giants in creating environment-friendly cloud services. As the cloud industry expects to grow to a $150 billion market by the end of the year, users are increasingly demanding green services. Cloud technologies are quickly taking off, and it is a chance for companies and businesses to think of creative ways of harnessing its power while saving the environment.

13.1.2 Cloud General Challenges

The use of the cloud provides a number of opportunities like enabling services to be used without any understanding of their infrastructure. Cloud computing works using economies of scale. Vendors and service providers claim costs by establishing an ongoing revenue stream. Data and services are stored remotely but accessible from anywhere.

Though cloud is the hotcake technology today, there are many issues related with it. The following four major issues stand out with cloud computing:

1. *Threshold policy*: To test if the program works, develops, or improves and implements, a threshold policy is a pilot study before moving the program to the production environment. Check how the policy

detects sudden increases in the demand and results in the creation of additional instances to fill in the demand. Also, check to determine how unused resources are to be deallocated and turned over to other work.

2. *Interoperability issues*: The problems of achieving interoperability of applications between two cloud computing vendors. The need to reformat data or change the logic in applications.
3. *Hidden costs*: Cloud computing does not tell you what hidden costs are. In an instance of incurring network costs, companies who are far from the location of cloud providers could experience latency, particularly when there is heavy traffic.
4. *Unexpected behavior*: The tests to be made to show unexpected results of validation or releasing unused resources. The need to fix the problem before running the application in the cloud.

13.2 Security Aspects

Security concerns in the cloud are not that different from noncloud service offerings although they are exasperated—because in a single-tenant, noncloud environment, you generally know where information is and how it is being kept. There are many different customers and there is no mechanism followed to isolate each other's data.

Cloud computing places business data into the hands of an outside provider and makes regulatory compliance inherently riskier and more complex than it is when systems are maintained in-house. Loss of direct oversight means that the client company must verify that the service provider is working to ensure that data security and integrity are ironclad. The following are the current security-related research areas in cloud computing:

1. Reliable, distributed applications based on the Internet, such as the e-commerce system, rely heavily on the trust path among involved parties.
2. The skyrocketing demand for a new generation of cloud-based consumer and business applications is driving the need for a next generation of data centers that must be massively scalable, efficient, agile, reliable, and secure. In order to scale cloud services reliably to millions of service developers and billions of end users, the next-generation cloud computing and data center infrastructure will have to follow an evolution similar to the one that led to the creation of scalable telecommunication networks.

3. In the future, network-based CSPs will leverage virtualization technologies to be able to allocate just the right levels of virtualized compute, network, and storage resources to individual applications based on real-time business demand while also providing full service-level assurance of availability, performance, and security at a reasonable cost.

13.2.1 Data Security

Due to huge infrastructure, cost organizations are slowly switching to cloud technology. Data are stored in the CSP's infrastructure. As data do not reside in organization territory, many complex challenges arise. Some of the complex data security challenges in cloud include the following:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the European Union (EU) Data Privacy Directive
- Lack of standards about how CSPs securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company but may have control and visibility into your data

Such issues raise the level of anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data.

There is also an ongoing concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another CSP.

Unquestionably, virtualized environments and the private cloud involve new challenges in securing data, mixed trust levels, and the potential weakening of separation of duties and data governance. The public cloud compounds these challenges with data that are readily portable, accessible to anyone connecting with the cloud server, and replicated for availability. And with the hybrid cloud, the challenge is to protect data as it moves back and forth from the enterprise to a public cloud.

However, security and privacy are still cited by many organizations as the top inhibitors of cloud services adoption, which has led to the introduction of cloud encryption systems in the past 18 months.

The issues that must be addressed are as follows:

Breach notification and data residency: Not all data require equal protection, so businesses should categorize data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions.

Gartner also recommends that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities. The plan should take stakeholders into account, such as legal, contract, and business units, security, and IT.

Data management at rest: Businesses should ask specific questions to determine the CSP's data storage life cycle and security policy.

Businesses should find out if

- Multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants
- Mechanisms such as tagging are used to prevent data being replicated to specific countries or regions

Storage used for archive and backup is encrypted and the key management strategy includes a strong identity and access management policy to restrict access within certain jurisdictions.

Gartner recommends that businesses use encryption to implement end-of-life strategies by deleting the keys to digitally shred the data while ensuring that keys are not compromised or replicated.

Data protection in motion: As a minimum requirement, Gartner recommends that businesses ensure that the CSP will support secure communication protocols such as Secure Socket Layer (SSL)/Transport Layer Security (TLS) for browser access or virtual private network (VPN)–based connections for system access for protected access to their services.

The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data are unencrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches.

In IaaS, Gartner recommends that businesses favor CSPs that provide network separation among tenants, so that one tenant cannot see another's network traffic.

13.2.1.1 Data Center Security

Data are stored in outside territory of the user in a location called as *data center*, which is unknown to the user. As the location of the data center is unknown to the user, it becomes a virtual data center. The backbone of this

virtual data center is virtual infrastructure, or the virtual machine (VM); however, virtual platforms are dependent on many other, often forgotten components of both the physical and virtual data centers.

There are typically seven areas of concern that accompany any major virtual platform implementation or migration. Often, these issues are not seen during staging and testing and only appear when the VMs take on the same amount of load as physical machines. The critical points represent two cornerstones of the data center: network and storage.

Lack of performance and availability: Virtualization moves many I/O (Input/Output) tasks tuned for hardware to software via the hypervisor. The virtualization translation layer is responsible for translating the optimized code for the software chip to the physical chip or CPU running on the underlying hardware. I/O intensive applications, like cryptographic processing applications for SSL, do not fare well when virtualized because of this translation layer.

VM saturation caused by virtualization sprawl can cause unanticipated resource constraints in all parts of the data center. With a physical machine running a network application, that application can have access to the full resources of the network card. This can lead to overall network performance issues, reduced bandwidth, and increased latency; the application might not be able to deal with all these issues. Even smaller issues such as IP address availability can be impacted by virtualization sprawl.

Lack of application awareness: One of the limitations of hypervisor- and kernel-based virtualization solutions is that they only virtualize the operating system (OS). OS virtualization does not virtualize nor is it even aware of applications that are running on the OS. Even the same applications do not realize that they are using virtual hardware on top of a hypervisor. By inserting this extra software management layer between the application and the hardware, the applications might encounter performance issues that are beyond control.

Virtual infrastructure platforms typically include software that can migrate live VM instances from one physical device to another; VMware Distributed Resource Scheduler (DRS) and VMotion are examples of live migration solutions. Like basic OS virtualization, these migration tools are unaware of the application state and also have no insight into the application delivery network.

Additional, unanticipated costs: Two of the primary drivers for virtualization are cost reduction and data center consolidation; however, implementing a complete VM solution in the data center and migrating physical machines to VMs do not come cheap. Once virtualization hardware and software are acquired, operational expenses can grow unbounded. Management of these new tools can be a long-term recurring cost, especially if the virtualization is done in-house. There can be additional growth requirements for the application and storage networks as these VMs begin to burden the existing infrastructure. Unexpected and unplanned costs can be a serious problem when implementing or migrating from physical to VMs, hindering or even completely halting deployment.

Unused virtualization features: New virtual platforms include many advanced networking technologies, such as software switching and support for virtual local area network (VLAN) segmentation. Often, new technologies perform flawless in development and staging, but they are unable to scale to production levels once deployed. These new platforms may have problems integrating with existing application and storage networks, requiring a redesign of the data center.

Storage integration issues tend to arise as soon as VMs are moved into production environments. First and foremost, network storage is a requirement for virtual platforms that implement live machine migration; direct-attached and local storage will only work for running local VMs. While many enterprise storage networks include technologies for data replication that span multiple geographic data centers, VM migration tools are often limited to local storage groups.

Overflowing storage network: Although converting physical machines to VMs is an asset for building dynamic data centers, hard drives become extremely large flat file virtual disk images. Consequently, file storage becomes unmanageable.

Congested storage network: Due to the portable nature of OS virtualization, there can be a dramatical increase in data traversing the storage network. For the same reason that VM disk files can overrun physical storage, once these images are made portable, it becomes trivial to move these VM images across the network from one host to another or from one storage array to another. It can be a challenge to prevent flooding of the storage network when planning a large VM migration or move. And as virtual sprawl and unmanaged VMs begin to appear in the data center, unplanned VM migrations can literally bring the network to a standstill, even on a LAN.

Management complexity: Throughout all areas of the data center, managing VMs as part of the complete management solution can be a struggle at best. VMs will report the metrics such as latency and response time of all physical machines. The management challenge with VMs appears in two forms:

1. The addition of two new components that need to be managed: The hypervisor and the host system. Neither one of these devices that exist in the physical server world is not part of existing data center management solutions, but they do have a major impact on the performance of VMs. Managing these devices and insight into these performance differences are critical.
2. Managing VMs, application network, and storage network together: Many VM platforms include built-in management tools, some of them highly sophisticated, such as VMware's Virtual Server.

While these tools do provide essential management tasks, such as live migration of virtual guests from one host to another, they do not take into account

any external information. With physical servers, there is a line segregating ownership and management responsibilities. The network team owns the network fabric (switches, routers, VLANs, IPs), and the server team owns the servers (hardware, OS, application, uptime). OS virtualization blends these responsibilities onto one platform, blurring the lines of ownership and management.

13.2.1.2 Access Control

As the data are stored in the data center, accessing these critical data is a major concern. Being a web-based platform, the cloud acts according to the access rights reserved for the users to access the data. These access rights though well defined by individual firms still pose problems in the cloud. Gartner recommends that businesses require the CSP to support IP subnet access restriction policies so that enterprises can restrict end user access from known ranges of IP addresses and devices.

The enterprise should demand that the encryption provider offers adequate user access and administrative controls, stronger authentication alternatives such as two-factor authentication, management of access permissions, and separation of administrative duties such as security, network, and maintenance.

13.2.1.3 Encryption and Decryption

As the data are stored in cloud out of the territory of the user, it is recommended that users store data in encrypted form. Enterprises should always aim to manage the encryption keys, but if they are managed by a cloud encryption provider, enterprises must ensure that access management controls are in place that will satisfy breach notification requirements and data residency.

If keys are managed by the CSP, then businesses should require hardware-based key management systems within a tightly defined and managed set of key management processes. When keys are managed or available in the cloud, it is imperative that the vendor provides tight control and monitoring of potential snapshots of live workloads to prevent the risk of analyzing the memory contents to obtain the key.

Businesses should also require

- Logging of all user and administrator access to cloud resources and to provide these logs to the enterprise in a format suitable for log management or security information and event management systems
- The CSP to restrict access to sensitive system management tools that might *snapshot* a live workload, perform data migration, or back up and recover data
- That images captured by migration or snapshotting tools are treated with the same security as other sensitive enterprise data.

13.2.2 Virtualization Security

Virtualization is technology that drives server consolidation and data center operations to a key ingredient in creating a flexible, on-demand infrastructure. When adopting virtualization for cloud computing, it becomes evident that the management tools used in a physical server-based deployment will not suffice in a highly dynamic virtualized one. To begin with, in a physical server deployment model, provisioning automation is generally not as heavily used unless there is a significant enough number of server OSs to warrant doing so.

Virtualization mainly focuses on three different areas: virtual networks (network virtualization), storage virtualization, and server virtualization. In network virtualization, the available resources are pooled into a network and the network bandwidth is split up into multiple channels where each individual channel is independent of one another. Storage virtualization combines the physical storage from multiple network storage devices, and this available storage is viewed as multiple different singular storage devices. In server virtualization, the identity of individual server devices is masked from the users, and the servers are designed to view as individual servers where the resource sharing and maintenance complexity are managed in a balanced way. The combination of these three virtualization components provides a self-managing capability to the resources, and this self-managing plays a major role in cloud computing.

The typical strategy for provisioning physical servers involves repetitive steps. In a heavily virtualized environment like the cloud, OS provisioning will rapidly transition to being a highly automated process. The critical areas of concern during virtualization are as follows.

A new threat: Virtualization alters the relationship between the OS and hardware. This challenges traditional security perspectives. It undermines the comfort you might feel when you provision an OS and application on a server you can see and touch. Some already believe that this sense of comfort is misplaced in most situations. For the average user, the actual security posture of a desktop PC with an Internet connection is hard to realistically discern.

Virtualization complicates the picture but does not necessarily make security better or worse. There are several important security concerns you need to address in considering the use of virtualization for cloud computing.

One potential new risk has to do with the potential to compromise a VM hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target. At the scale of the cloud, such a risk would have a broad impact if not otherwise mitigated. This requires an additional degree of network isolation and enhanced detection by security monitoring.

In examining this concern, first consider the nature of a hypervisor. It is observed that "Hypervisors are purpose-built with a small and specific set of functions. A hypervisor is smaller, more focused than a general

purpose operating system, and less exposed, having fewer or no externally accessible network ports. A hypervisor does not undergo frequent change and does not run third-party applications. The guest operating systems, which may be vulnerable, do not have direct access to the hypervisor. In fact, the hypervisor is completely transparent to network traffic with the exception of traffic to/from a dedicated hypervisor management interface."

Storage concerns: Another security concern with virtualization has to do with the nature of allocating and deallocating resources such as local storage associated with VMs. During the deployment and operation of a VM, data are written into physical memory. If it is not cleared before those resources are reallocated to the next VM, there is a potential for exposure.

These problems are certainly not unique to virtualization. They have been addressed by every commonly used OS. Not all OSs manage data clearing. Some might clear data upon resource release; others might do so upon allocation.

The bottom line is to clear the data yourself, carefully handle operations against sensitive data, and pay particular attention to access and privilege controls. Another excellent security practice is to verify that a released resource was cleared.

A further area of concern with virtualization has to do with the potential for undetected network attacks between VMs collocated on a physical server. Unless you can monitor the traffic from each VM, you cannot verify that traffic is not possible between those VMs.

In essence, network virtualization must deliver an appropriate network interface to the VM. That interface might be a multiplexed channel with all the switching and routing handled in the network interconnect hardware. Most fully featured hypervisors have virtual switches and firewalls that sit between the server physical interfaces and the virtual interfaces provided to the VMs.

Traffic management: Another theoretical technique that might have potential for limiting traffic flow between VMs would be to use segregation to gather and isolate different classes of VMs from each other. VMs could be traced to their owners throughout their life cycle. They would only be colocated on physical servers with other VMs that meet those same requirements for colocation.

One actual practice for managing traffic flows between VMs is to use VLANs to isolate traffic between one customer's VMs and another customer's VMs. To be completely effective, however, this technique requires extending support for VLANs beyond the core switching infrastructure and down to the physical servers that host VMs.

The next problem is scaling VLAN-like capabilities beyond their current limits to support larger clouds. That support will also need to be standardized to allow multivendor solutions. It will also need to be tied in with network management and hypervisors.

13.2.3 Network Security

Cloud is based on networking of many things together like the network of infrastructure. While the network is the backbone of the cloud, many challenges are encountered in this network. Some of the challenges in the existing cloud networks are discussed in the following.

Application performance: Cloud tenants should be able to specify bandwidth requirements for applications hosted in the cloud, ensuring similar performance to on-premise deployments. Many tiered applications require some guaranteed bandwidth between server instances to satisfy user transactions within an acceptable time frame and meet predefined service-level agreements (SLAs). Insufficient bandwidth between these servers will impose significant latency on user interactions. Therefore, without explicit control, variations in cloud workloads and oversubscription can cause delay and drift of response time beyond acceptable limits, leading to SLA violations for the hosted applications.

Flexible deployment of appliances: Enterprises deploy a wide variety of security appliances in their data centers, such as deep packet inspection (DPI) or intrusion detection systems (IDSs), and firewalls to protect their applications from attacks. These are often employed alongside other appliances that perform load balancing, caching, and application acceleration. When deployed in the cloud, an enterprise application should continue to be able to flexibly exploit the functionality of these appliances.

Policy enforcement complexities: Traffic isolation and access control to end users are among the multiple forwarding policies that should be enforced. These policies directly impact the configuration of each router and switch. Changing requirements, different protocols (e.g., Open Shortest Path First [OSPF], LAG (Link Aggregation Group), Virtual Router Redundancy Protocol [VRRP]), and different flavors of L2 spanning tree protocols, along with vendor-specific protocols, make it extremely challenging to build, operate, and interconnect a cloud network at scale.

Topology-dependent complexity: The network topology of data centers is usually tuned to match a predefined traffic requirement. For instance, a network topology optimized for east–west traffic (i.e., traffic among servers in a data center) is not the same as a topology for north south (traffic to/from the Internet). The topology design also depends on how L2 and/or L3 is utilizing the effective network capacity. For instance, adding a simple link and switch in the presence of a spanning tree–based L2 forwarding protocol may not provide additional capacity. Furthermore, evolving the topology based on traffic pattern changes also requires complex configuration of L2 and L3 forwarding rules.

Application rewriting: Applications should run *out of the box* as much as possible, in particular for IP addresses and network-dependent failover mechanisms. Applications may need to be rewritten or reconfigured before deployment in the cloud to address several network-related limitations.

Two key issues are (1) lack of a broadcast domain abstraction in the cloud network and (2) cloud-assigned IP addresses for virtual servers.

Location dependency: Network appliances and servers (e.g., hypervisors) are typically tied to a statically configured physical network, which implicitly creates a location-dependent constraint. For instance, the IP address of a server is typically determined based on the VLAN or the subnet to which it belongs. VLANs and subnets are based on physical switch port configuration. Therefore, a VM cannot be easily and smoothly migrated across the network. Constrained VM migration decreases the level of resource utilization and flexibility. Besides, physical mapping of VLAN or subnet space to the physical ports of a switch often leads to a fragmented IP address pool.

Multilayer network complexity: A typical three-layer data center network includes a TOR (Top of Rack) layer connecting the servers in a rack, an aggregation layer, and a core layer, which provides connectivity to/from the Internet edge. This multilayer architecture imposes significant complexities in defining boundaries of L2 domains, L3 forwarding networks and policies, and layer-specific multivendor networking equipment. Providers of cloud computing services are currently operating their own data centers. Connectivity between the data centers to provide the vision of *one cloud* is completely within the control of the CSP. There may be situations where an organization or enterprise needs to be able to work with multiple cloud providers due to locality of access, migration from one cloud service to another, merger of companies working with different cloud providers, cloud providers who provide the best-of-class services, and similar cases. Cloud interoperability and the ability to share various types of information between clouds become important in such scenarios. Although CSPs might see less immediate need for any interoperability, enterprise customers will see a need to push them in this direction. This broad area of cloud interoperability is sometimes known as cloud federation.

13.3 Platform-Related Security

CSPs offer services in various service models like SaaS, PaaS, and IaaS where the user is offered varied services based on his or her requirements. Every service model offered brings with it many security-related challenges like secured network, locality of resources, accessing secure data, data privacy, and backup policy.

13.3.1 Security Issues in Cloud Service Models

Cloud computing uses three delivery models such as SaaS, PaaS, and IaaS through which different types of computing services are provided to the

end user. These three delivery models provide infrastructure resources, application platform, and software as services to the cloud customer. These service models place a different level of security requirement in the cloud environment. IaaS is the basis of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in terms of integrated features, complexity versus extensibility, and security. If the CSP takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities.

SaaS is a software deployment model in which applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet. The SaaS model offers the customers with significant benefits, such as improved operational efficiency and reduced costs. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. PaaS is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the *view* of the developers.

13.3.2 Software-as-a-Service Security Issues

In a traditional on-premise application deployment model, the sensitive data of each enterprise continue to reside within the enterprise boundary and are subject to its physical, logical, and personnel security and access control policies. The architecture of SaaS-based applications is specifically designed to support many users concurrently (multitenancy). SaaS applications are accessed through the web, and so web browser security is very much important. Information security officers will need to consider various methods of securing SaaS applications. Web services (WS) security, Extensible Markup Language (XML) encryption, SSL, and available options used in enforcing data protection transmitted over the Internet. In the SaaS model, the enterprise data are stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and to prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. The pain points of concern in SaaS are as follows.

Network security: In an SaaS deployment model, sensitive data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as the SSL and TLS for security.

Resource locality: In an SaaS model of a cloud environment, the end users use the services provided by the cloud providers without knowing exactly where the resources for such services are located. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture.

The directive prohibits transfers of personal data to countries that do not ensure an adequate level of protection. For example, the recent Dropbox users have to agree to the *Terms of Service* that grant the providers the right to disclose user information in compliance with laws and law enforcement requests.

Cloud standards: To achieve interoperability among clouds and to increase their stability and security, cloud standards are needed across organizations. For example, the current storage services by a cloud provider may be incompatible with those of other providers. In order to keep their customers, cloud providers may introduce so-called sticky services that create difficulty for the users if they want to migrate from one provider to the other.

Data segregation: Multitenancy is one of the major characteristics of cloud computing. In a multitenancy situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. An SaaS model should, therefore, ensure a clear boundary for each user's data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users.

Data access: Data access issue is mainly related to security policies provided to the users while accessing the data. The organizations will have their own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations, wherein some of the employees are not given access to a certain amount 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. The model must also be able to provide organizational boundary within the cloud because multiple organizations will be deploying their business processes within a single cloud environment.

Data breaches: Since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. Thus, the cloud becomes a high-value target.

Backup: The SaaS vendor needs to ensure that all sensitive enterprise data are regularly backed up to facilitate quick recovery in case of disasters. Also, the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information. In the case of cloud vendors such as Amazon, the data at rest in S3 are not encrypted by default. The users need to separately encrypt their data and backups so that it cannot be accessed or tampered with by unauthorized parties.

Identity management (IdM) and sign-on process: IdM deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. When an SaaS provider has to know how to control who has access to what systems within the enterprise, it becomes all the more challenging task. In such scenarios, the provisioning and deprovisioning of the users in the cloud become very crucial.

13.3.3 Platform-as-a-Service Security Issues

PaaS provides a ready-to-use platform, including OS that runs on vendor-provided infrastructure. As the infrastructure is of the CSP, various security challenges of the focused architecture are caused mainly by the spread of the user objects over the hosts of the cloud. Stringently allowing access of objects to the resources and defending the objects against malicious or corrupt providers reasonably reduce possible risks. Network access and service measurement bring together concerns about secure communications and access control. Well-known practices, object scale enforcement of authorization, and undeniable traceability methods may alleviate the concerns.

Apart from the aforementioned problems, user privacy must be protected in a public, shared cloud. Therefore, proposed solutions must be privacy aware. Service continuity is another concern for many enterprises that consider cloud adoption. Accordingly, fault-tolerant reliable systems are required.

13.3.4 Infrastructure-as-a-Service Security Issues

Cloud computing makes a lot of promises in the areas of increased flexibility and agility, potential cost savings, and competitive advantages for developers so that they can stand up an infrastructure quickly and efficiently to enable them to develop the software to drive business success. There are a lot of problems that cloud, especially private cloud, solves, but it is not that much good in solving problems related to security.

However, in a private cloud environment, some of the traditional problems faced are as follows:

1. *Hypervisor security*: In private cloud, most or all of services will run in a virtualized environment and the security model used by the hypervisor cannot be taken for granted. A need to evaluate the security models and the development of hypervisors becomes necessary.

2. *Multitenancy*: Although all the tenants in the multitenancy environment will be from the same company, not all tenants may be comfortable sharing infrastructure with other users within the same company.
3. *Identity management and access control (IdAM)*: In a traditional data center, we were comfortable with the small handful of authentication repositories we had to work with—Active Directory being one of the most popular. But with private cloud, handling authentication and authorization for the cloud infrastructure, handling tenants, and handling delegation of administration of various aspects of the cloud fabric are the major tasks to be addressed.
4. *Network security*: In private cloud, we are likely to have many components of a service communicate with each other over virtual network channels only. Assessing the traffic, employing some powerful access controls for physical networks, and control quality of service, which is a key issue in the *availability* aspect of the confidentiality, integrity and availability (CIA) security model, are major concerns.

As a consolidation, platform-related security considers the previously said three service delivery models like SaaS, PaaS, and IaaS, and the concerned components are also mentioned individually.

Combining the three types of clouds (public cloud, private cloud, and hybrid cloud) together with the three service delivery models, we get a complete picture of a cloud computing environment interlinked by connectivity devices coupled with information security components. Virtualized physical resources, virtualized infrastructure, virtualized middleware platforms, and business-related applications are being provided as computing services in the cloud. Cloud providers and cloud consumers must be able to maintain and establish computing security at all levels of interfaces in the cloud computing architecture.

13.4 Audit and Compliance

It is a widely known fact that data protection and regulatory compliance are among the top security concerns for chief information officers (CIOs) of any organization.

According to the Pew Internet and American Life Project, an overwhelming majority of users of cloud computing services expressed serious concern about the possibility of a service provider disclosing their data to others. Ninety percent of cloud application users said that they would be very concerned if the company at which their data were stored sold them to another party.

A survey conducted by many firms expressed the view that security is the biggest challenge for the cloud computing model. Stakeholders, therefore, increasingly feel the need to prevent data breaches. In recent months, many newspaper articles have revealed data leaks in sensitive areas such as the financial and governmental domains and web community.

One of the missions of the data protection authorities is to prevent the so-called *Big Brother* phenomenon, which refers to a scenario whereby a public authority processes personal data without adequate privacy protection. In such a situation, end users may view the cloud as a vehicle for drifting into a totalitarian surveillance society.

The specificities of cloud computing, therefore, make the data protection incentive even greater. For example, the cloud provider should provide encryption to protect the stored personal data against unauthorized access, copy, leakage, or processing.

In a cloud environment, companies have no control over their data, which, being entrusted to third-party application service providers in the cloud, could now reside anywhere in the world. Nor will a company know in which country its data reside at any given point in time. This is a central issue of cloud computing that conflicts with the EU requirements whereby a company must at all times know where the personal data in its possession are being transferred to. Cloud computing thus poses special problems for multinationals with specific EU customers.

13.4.1 Disaster Recovery

Simple data backup as well as more comprehensive disaster recovery and business continuity planning is an essential part of business and personal life. Backup as a Service and Disaster Recovery as a Service is now available online through the cloud for every level of user, from personal, small business to large enterprise data storage and retrieval, either publicly through the Internet or via more secure dedicated access methods. As a result, traditional methods are becoming obsolete.

A few of the advantages include the following:

- No huge upfront costs for capital investment or infrastructure management or black boxes.
- Backups are physically stored in a different location from the original source of your data.
- Remote backup does not require user intervention or periodic manual backups.
- Unlimited data retention. You can get as much or as little data storage space as you need.
- Backups are automatic and *smart*. They occur continuously and efficiently back up your files only as the data change.

Cloud computing, based on virtualization, takes a very different approach to disaster recovery. With virtualization, the entire server, including the OS, applications, patches, and data, is encapsulated into a single software bundle or virtual server. This entire virtual server can be copied or backed up to an offsite data center and spun up on a virtual host in a matter of minutes.

Since the virtual server is hardware independent, the OS, applications, patches, and data can be safely and accurately transferred from one data center to a second data center without the burden of reloading each component of the server. This can dramatically reduce recovery times compared to conventional (nonvirtualized) disaster recovery approaches where servers need to be loaded with the OS and application software and patched to the last configuration used in production before the data can be restored.

13.4.2 Privacy and Integrity

The promise to deliver IT as a service is addressed to a large range of consumers, from small- and medium-sized enterprises (SMEs) and public administrations to end users. Users are creating an ever-growing quantity of personal data.

This expanding quantity of personal data will drive demand for cloud services, particularly if cloud computing delivers on the promises of lower costs for customers and the emergence of new business models for providers.

Among the main privacy challenges for cloud computing are as follows.

Complexity of risk assessment in a cloud environment: The complexity of cloud services introduces a number of unknown parameters. Service providers and consumers are cautious about offering guarantees for compliance-ready services and adopting the services. With service providers promoting a simple way to flow personal data irrespective of national boundaries, a real challenge arises in terms of checking the data processing life cycle and its compliance with legal frameworks.

To address the issues like stakeholders' roles and responsibilities, data replication, and legal issues compliance, the Madrid Resolution states that every responsible person shall have transparent policies with regard to the processing of personal data. Stakeholders need to specify requirements for cloud computing that meet the expected level of security and privacy. In Europe, the European Network and Information Security Agency (ENISA) provides recommendations to facilitate the understanding of the shift in the balance of responsibility and accountability for key functions such as governance and control over data and IT operations and compliance with laws and regulations.

Emergence of new business models and their implications for consumer privacy: A report by the Federal Trade Commission (FTC) on *Protecting consumer privacy in an era of rapid change* analyzes the implications for consumer privacy of technological advances in the IT sphere. According to the FTC, users are able to collect, store, manipulate, and share vast amounts of consumer data for very little cost.

These technological advances have led to an explosion of new business models that depend on capturing consumer data at a specific and individual level and over time, including profiling, online behavioral advertising (OBA), social media services, and location-based mobile services.

13.5 Summary

Cloud being the efficient, low-cost computing platform for the IT industry is fast growing. With the tremendous growth comes the challenge of handling the critical data and offering quality of service to the users.

This chapter throws light on various security aspects related to cloud computing. The basic security elements related to various cloud deployment models and service delivery models are briefly explained here. The security aspects like data center security and security with respect to service models are also highlighted. As the IT industry is driven to the cloud for its computing capacities, it in turn needs to look into the security of the critical data stored in third-party providers. The various security-related issues, though addressed by IT industry, still are major concerns as no standard development procedure is defined for the development of the cloud model. As organizations follow their own model for development, security becomes more prominent for concentration.

Review Points

- *Threshold policy*: To test if the program works, develops, or improves and implements, a threshold policy is a pilot study before moving the program to the production environment (see Section 13.1.2).
- *Data security*: Data are stored in the CSP's infrastructure. As data do not reside in organization territory, many complex challenges arise (see Section 13.2.1).
- *Access control*: As the data are stored in the data center, accessing these critical data is a major concern. Being a web-based platform, the cloud acts according to the access rights reserved for the users to access the data (see Section 13.2.1.2).
- *Location dependency*: Network appliances and servers (e.g., hypervisors) are typically tied to a statically configured physical network, which implicitly creates a location-dependent constraint (see Section 13.2.3).

- *Resource locality*: In an SaaS model of a cloud environment, the end users use the services provided by the cloud providers without knowing exactly where the resources for such services are located (see Section 13.3.2).
- *IdM*: IdM deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities (see Section 13.3.2).
- *Disaster recovery*: Simple data backup as well as more comprehensive disaster recovery and business continuity planning is an essential part of business and personal life (see Section 13.4.1).

Review Questions

1. What are the issues to be addressed in data security? Explain.
2. What are the storage concerns in virtualization security?
3. Explain the challenges in cloud networks.
4. What are the security issues in SaaS? Explain.
5. What are the security issues in PaaS? Explain.
6. What are the security issues in IaaS? Explain.
7. What are the advantages of Disaster Recovery as a Service?
8. What are the privacy challenges for cloud computing? Explain.

Further Reading

An introduction to cloud computing in public sector. White Paper, APPTIS.

Bioh, M. and D. Earhart. Security issues that affect cloud computing data storage. www.slideshare.net, 2009. Accessed November 2, 2014.

Brodkin, J. Gartner: Seven cloud-computing security risks, 2008. www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853. Accessed November 23, 2014.

Cloud computing issues and impacts. White Paper, Ernst and Young.

Cloud computing security and privacy issues. White Paper, CEPIS.

Curran, K., S. Carlin, and M. Adams Security issues in cloud computing. *Journal of Network Engineering* 4069–4072, 2011.

Hamlen, K., M. Kantarcioglu, L. Khan, and B. Thuraisingham. Security issues for cloud computing. *International Journal of Information Security and Privacy* 4(2): 39–51, 2010.

Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications* 4: 5, 2013.

Cloud Computing, http://www.gartner.com/technology/research/cloud-computing/report. Accessed December 21, 2013.

http://www.hostway.com/resources/media/disaster-recovery-in-the-cloud.pdf. Accessed November 27, 2013.

Kuyoro, S. O., F. Ibikunle, and O. Awodele. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)* 3(5): 247–255, 2011.

Ma, M. and C. Meinel. A proposal for trust model: Independent trust intermediary service (ITIS). *Proceedings of IADIS International Conference WWW/Internet 2002*, Lisbon, Portugal, 2002, pp. 785–790.

More, J. J. Cloud computing: Information technology's answer to sustainability. www.ecoseed.org. Accessed November 9, 2013.

Murphy, A. Keeping your head above the cloud: Seven data center challenges to consider before going virtual. White Paper.

Rashmi, G. Sahoo, and S. Mehfuz. Securing software as a service model of cloud computing: Issues and solutions. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)* 3(4): 1–11, 2013.

Subashini, S. and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1): 1–11, 2011.

The ethics and security of cloud computing. White Paper, ILTA.

www.trustedcomputinggroup.org.

Xu, K., M. Song, X. Zhang, and J. Song. A cloud computing platform based on P2P. *Proceedings of the IEEE*, 2009.