Cloud Deployment Model

Related terms:

Risk, Cloud Computing, Community Cloud, Hybrid Cloud, Private Cloud, Cloud Service Model, Deployment Model, Federal Agency

View all Topics

Cloud Deployment Models

Derrick Rountree, Ileana Castrillo, in The Basics of Cloud Computing, 2014

Introduction

NIST defines four cloud deployment models: public clouds, private clouds, community clouds, and hybrid clouds. A cloud deployment model is defined according to where the infrastructure for the deployment resides and who has control over that infrastructure. Deciding which deployment model you will go with is one of the most important cloud deployment decisions you will make.

Each cloud deployment model satisfies different organizational needs, so it's important that you choose a model that will satisfy the needs of your organization. Perhaps even more important is the fact that each cloud deployment model has a different value proposition and different costs associated with it. Therefore, in many cases, your choice of a cloud deployment model may simply come down to money. In any case, to be able to make an informed decision, you need to be aware of the characteristics of each environment.

> Read full chapter

Migrating to the Cloud

Tom Laszewski, Prakash Nauduri, in Migrating to the Cloud, 2012

Cloud Computing Deployment Models

Cloud deployment models indicate how the cloud services are made available to users. The four deployment models associated with cloud computing are as follows:

- **Public cloud** As the name suggests, this type of cloud deployment model supports all users who want to make use of a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis. Most common uses of public clouds are for application development and testing, non-mission-critical tasks such as file-sharing, and e-mail service.
- **Private cloud** True to its name, a private cloud is typically infrastructure used by a single organization. Such infrastructure may be managed by the organization itself to support various user groups, or it could be managed by a service provider that takes care of it either on-site or off-site. Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them. However, private clouds are better able to address the security and privacy concerns of organizations today.
- **Hybrid cloud** In a hybrid cloud, an organization makes use of interconnected private and public cloud infrastructure. Many organizations make use of this model when they need to scale up their IT infrastructure rapidly, such as when leveraging public clouds to supplement the capacity available within a private cloud. For example, if an online retailer needs more computing resources to run its Web applications during the holiday season it may attain those resources via public clouds.
- **Community cloud** This deployment model supports multiple organizations sharing computing resources that are part of a community; examples include universities cooperating in certain areas of research, or police departments within a county or state sharing computing resources. Access to a community cloud environment is typically restricted to the members of the community.

With public clouds, the cost is typically low for the end user and there is no capital expenditure involved. Use of private clouds involves capital expenditure, but the expenditure is still lower than the cost of owning and operating the infrastructure due to private clouds' greater level of consolidation and resource pooling. Private clouds also offer more security and compliance support than public clouds. As such, some organizations may choose to use private clouds for their more mission-critical, secure applications and public clouds for basic tasks such as application development and testing environments, and e-mail services.

TIP

Using hypervisor-based virtualization software to provide isolation between different customer environments can lead to increased utilization of system resources such as CPU and memory. Using native virtualization technologies offered by hardware vendors, such as Solaris Zones when using the Oracle Solaris operating system, can be much more effective and efficient depending on the customer environment. Native virtualization technologies offered by hardware vendors are more restrictive in terms of what is supported than hypervisor-based virtualization software.

Figure 1.1 summarizes the computing architecture evolution.

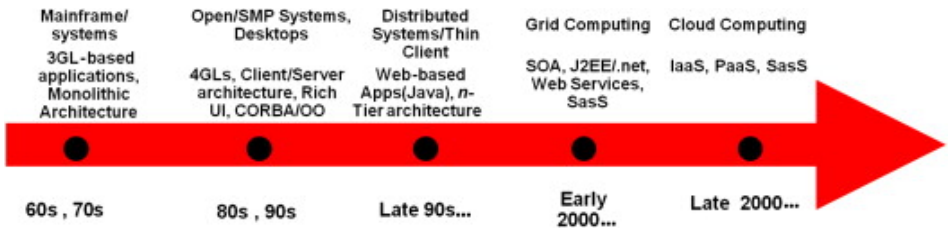

FIGURE 1.1. Evolution of Computing Architectures

As Figure 1.1 shows, cloud computing primarily impacts how IT infrastructure and platforms are set up, deployed, and provisioned from an end-user perspective. The applications running in a cloud environment should be able to seamlessly interact with the cloud ecosystem, including other applications within or outside the cloud environment.

Table 1.1 highlights the pros and cons of different computing architectures.

Table 1.1. Pros and Cons of Different Computing Architectures

Architecture	Pros	Cons
Mainframe/proprietary systems	•Mostly third-generation language (3GL)-based applications•Very efficient•Easier to secure/manage (only one large server)•Fewer moving parts	•Outdated/proprietary technology•Difficult to maintain due to declining skill sets•Expensive•Less agile
Client/server computing	•Supports different operating systems (including open source)•Different languages, fourth-generation languages (4GLs) used for application development•Many options for software and	•Many systems to manage and secure•Performance bottlenecks•Unique environment for each application, resulting in silos of systems

	hardware vendors•Cheaper than mainframes	
Internet computing (*n*-tier) architecture	•Separation between applications, business process orchestration, rules, and data and applicationservices•Agility•Interoperability using standard mechanism such as Web services•Support for compliance requirements•Globalization	•Many servers to manage•Many software components to integrate
Cloud computing	•Self-contained environment•Interoperability between applications and environments using standard interfaces•Cheaper to acquire and operate for end users	•Security•Compliance•Performance (public clouds)•Emerging patterns•Mostly used for development and testing environments•Most legacy client/server applications need to be rewritten and/or adapted to make them cloud-ready

To take advantage of cloud computing, legacy applications such as those developed using mainframe client/server technologies need to be adapted or migrated to modern languages and APIs so that they can interact with other applications regardless of where they are deployed. Cloud-enabling an application requires that the application be able to interact with databases, middleware, and other applications using standards-based mechanisms such as Web services. Most legacy and client/server applications today do not have this capability natively. Typically, these legacy applications require adapters and wrapper software to make them accessible via Web services.

> Read full chapter

Making the Decision

Derrick Rountree, Ileana Castrillo, in The Basics of Cloud Computing, 2014

Choosing a Cloud Deployment Model

After you have chosen the cloud service model that best fits your need, you need to determine your cloud deployment model. You can choose from among public, private, community, and hybrid. Most people believe that the hybrid cloud model is the model that will be used in most organizations. However, you still must consider which model is best for your organization.

User Experience

The cloud offers different user experiences depending on which deployment model you choose.

If you choose to go with a private cloud, you will complete control over the user experience. You will be able to control the application, the network, and, in most cases, the client systems. This allows you to tune everything for best performance and usability.

If you go with a public cloud, in some cases you might have no control over the user experience. In a community cloud environment, your control over the user experience depends on the agreement you have in place with the other members of the community.

Security

Security is always a complicated topic. It's even more complicated when you're dealing with the cloud. It mainly comes down to trust. Whom do you trust with your security? Many organizations would rather trust a third party than trust themselves. There is absolutely nothing wrong with that. Security is such an important concern that you need to go with what you trust.

Responsibilities

Responsibilities vary greatly depending on which cloud model you intend to go with. This can be another key factor in your decision. In fact, one of the big drivers of public clouds is organizations' desire to reduce their internal responsibilities.

The following tables outline who is responsible for what in each environment configuration. Table 5.1 outlines SaaS provider responsibilities.

Table 5.1. SaaS Responsibilities by Cloud Deployment Model

Public	Private	Community	Hybrid
Provider	Consumer	Consumer	Varies

Application Updates				
OS Updates	Provider	Consumer	Consumer	Varies
Antivirus	Provider	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

Table 5.2 outlines PaaS provider responsibilities.

Table 5.2. PaaS Responsibilities by Cloud Deployment Model

	Public	**Private**	**Community**	**Hybrid**
Application Updates	Consumer	Consumer	Consumer	Varies
OS Updates	Provider	Consumer	Consumer	Varies
Antivirus	Varies	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

Table 5.3 outlines IaaS provider responsibilities.

Table 5.3. IaaS Responsibilities by Cloud Deployment Model

	Public	**Private**	**Community**	**Hybrid**
Application Updates	Consumer	Consumer	Consumer	Varies
OS Updates	Varies	Consumer	Consumer	Varies

Antivirus	Consumer	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

> Read full chapter

FedRAMP primer

Matthew Metheny, in Federal Cloud Computing (Second Edition), 2017

Change Control

Changes to an operational environment are inevitable as a system undergoes routine maintenance. However, some changes may cause significant impacts to the security posture of the cloud service.[63] Therefore, the CSP is required to report "changes in the CSP's point of contact with FedRAMP, changes in the CSP's risk posture, changes to any applications residing on the cloud system, and/or changes to the cloud system infrastructure" [6], and submit any residual artifacts associated with significant changes such as the SSP, security impacts analysis, and a re-assessment by a 3PAO to the FedRAMP PMO.

> Read full chapter

Introduction

Vic (J.R.) Winkler, in Securing the Cloud, 2011

Structure of the Book

We begin by examining cloud computing in light of the continuing evolution of IT. Later, we will build a set of guidelines and simple tools that we can use to plan or evaluate security in different cloud deployment models and for different service models—SaaS, PaaS, and IaaS. Together, we refer to these as the SPI service model.

Developing guidelines entails a review and understanding of security principles, security risks, and security architecture. What we aim to do is to describe the security issues associated with cloud computing and how to apply security to cloud computing.

We recognize that security requirements and solutions will vary greatly, and thus our underlying goal for the book is that the reader becomes better prepared to evaluate the conditions under which we should adopt Cloud Computing services and technologies.

Chapters in This Book

This book is organized in a top-down manner that begins with an introduction to cloud computing and security, progresses to an examination of cloud security architectures and issues, then presents a series of key strategies and best practices for cloud security, discusses the major security considerations for building or selecting a cloud provider, and concludes with an examination of what it means to securely operate a cloud.

Chapter 1: Introduction to Cloud Computing and Security

Chapter 1 "Introduction to Cloud Computing and Security" presents an overview to cloud computing along with its IT foundations, the historical underpinnings, and the cost benefits. Also covered are the essential qualities of clouds and a brief security and architecture background to support the remaining chapters. The bottom line with cloud computing is the combination of cost advantages it brings along with the pervasive changes it is unleashing.

Chapter 2: Cloud Computing Architecture

Chapter 2 "Cloud Computing Architecture" examines cloud computing, the NIST Cloud Computing Model, and identifies the essential characteristics of clouds. Also covered is the SPI cloud service model (SaaS, PaaS, and IaaS) along with the four cloud delivery models (public, private, hybrid, and community). The chapter also covers the relative degree of security control a tenant or consumer has with the different models.

Chapter 3: Security Concerns, Risk Issues, and Legal Aspects

Chapter 3 "Security Concerns, Risk Issues, and Legal Aspects" takes a closer look at the security concerns and issues with clouds along with surveying the legal and regulatory considerations of different types of clouds.

Chapter 4: Securing the Cloud: Architecture

Chapter 4 "Securing the Cloud: Architecture" identifies a number of security requirements for cloud computing. Proceeding from those requirements we identify common security patterns and architectural elements that make for better security. We then look at a few representative cloud security architectures and discuss several important aspects of those. This chapter also details several key strategies that if considered during design can present considerable operational benefits.

Chapter 5: Securing the Cloud: Data Security

Chapter 5 "Securing the Cloud: Data Security" examines data security in cloud computing along with data protection methods and approaches. Cloud security countermeasures must comprise a resilient mosaic that protects data at rest and data in motion. Security concerns around storing data in the cloud are not inherently unique compared to data that is stored within the premises of an organization; nonetheless there are important considerations for security when adopting the cloud model.

Chapter 6: Securing the Cloud: Key Strategies and Best Practices

Chapter 6 "Securing the Cloud: Key Strategies and Best Practices" presents an overall cloud security strategy for effectively managing risk. Also covered is a treatment of cloud security controls and a discussion of the limits of security controls in cloud computing. The chapter also includes a detailed treatment of best practices for cloud security and a discussion of security monitoring for cloud computing.

Chapter 7: Security Criteria: Building an Internal Cloud

Chapter 7 "Security Criteria: Building an Internal Cloud" discusses the various motivations for embarking on a private cloud strategy along with an overview of what adopting a private cloud strategy entails in terms of benefits to both the enterprise and to security. The remainder of the chapter details the security criteria for a private cloud.

Chapter 8: Security Criteria: Selecting an External Cloud Provider

Chapter 8 "Security Criteria: Selecting an External Cloud Provider" ties together the material from the previous chapters in providing guidance for selecting a cloud service provider (CSP). In doing so, it addresses the gaps between vendor claims and the various aspects of information assurance, including those elements that are critical in selecting a CSP. That discussion includes an overview of vendor *transparency* and the prudent limits of disclosure. The chapter includes a discussion

on the nature of risks in cloud computing along with the probability, impact affected assets, and factors that may be involved. The chapter concludes with a lengthy discussion of security criteria to enable selection of a CSP.

Chapter 9: Evaluating Cloud Security: An Information Security Framework

Chapter 9 "Evaluating Cloud Security: An Information Security Framework" builds on previous chapters and presents a framework for evaluating cloud security. This framework augments the security criteria identified in Chapter 8 and serves to provide a set of tools to evaluate the security of a private, community, or public cloud.

Chapter 10: Operating a Cloud

Chapter 10 "Operating a Cloud" discusses the relationship between underlying architecture and numerous security-relevant decisions that are made during all phases of a system and their impact on security operations, associated costs, and agility in operation. The chapter covers the numerous activities that are part of security operations, including patching, security monitoring, and incident response.

> Read full chapter

Introduction to the Cloud

Derrick Rountree, Ileana Castrillo, in The Basics of Cloud Computing, 2014

Summary

There are five key cloud characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. A solution must exhibit these five characteristics to be considered a true cloud solution. There are four cloud deployment models: public, private, community, and hybrid. Each deployment model is defined according to where the infrastructure for the environment is located. There are three main cloud service models: Software as a Service, Platform as a Service, and Infrastructure as a Service. SaaS was the original cloud service model but the cloud has continued to grow and expand. Now a vast array of service models is available.

There are many factors pushing organizations toward the cloud, as well as many factors that are keeping organizations away. Each organization must evaluate cloud offerings for itself to see what best fits its needs.

> Read full chapter

Securing Cloud Computing Systems

Cem Gurkok, in Computer and Information Security Handbook (Third Edition), 2017

Managing the Risks of Public Clouds

Though a public cloud deployment is suitable for most uses that are nonsensitive, migrating sensitive, mission critical, or proprietary data into any cloud environment that is not certified and designed for handling such data introduces high risk. A customer should first select a cloud deployment model and then make sure that sufficient security controls are in place. These actions should be followed by a reasonable risk assessment:

- *Data and encryption*: If the data is stored unencrypted in the cloud, data privacy is at risk. There is the risk for unauthorized access either by a malicious employee on the cloud service provider side or an intruder gaining access to the infrastructure from the outside.
- *Data retention*: When the data is migrated or removed by the cloud provider or customer, there may be data residues that might expose sensitive data to unauthorized parties.
- *Compliance requirements*: Various countries have varying regulations for data privacy. Because some public cloud providers don't provide information about the location of the data, it is crucial to consider the legal and regulatory requirements about where data can be stored.
- Multitenancy risks: The shared nature of public cloud environments increases security risks, such as unauthorized viewing of data by other customers using the same hardware platform. A shared environment also presents resource competition problems whenever one of the customers uses most of the resources either due to need or due to being exposed to targeted attacks, such as DDoS.
- *Control and visibility*: Customers have restricted control and visibility over the cloud resources because the cloud provider is responsible for administering the infrastructure. This introduces additional security concerns that originate from the lack of transparency. Customers need to rethink the way they operate as they surrender the control of their IT infrastructure to an external party while utilizing public cloud services.
- *Security responsibility*: In a cloud the vendor and the user share the responsibility of securing the environment. The amount of responsibility shouldered by each party can change depending on the cloud model adopted.

> Read full chapter

Securing Cloud Computing Systems

Cem Gurkok, in Network and System Security (Second Edition), 2014

Managing the Risks of Public Clouds

Although a public cloud deployment is suitable for most uses that are nonsensitive, migrating sensitive, mission-critical, or proprietary data into any cloud environment that is not certified and designed for handling such data introduces high risk. A customer should first select a cloud deployment model and then make sure that sufficient security controls are in place. These actions should be followed by a reasonable risk assessment:

- *Data and encryption*: If the data is stored unencrypted in the cloud, data privacy is at risk. There is the risk for unauthorized access either by a malicious employee on the cloud service provider side or an intruder gaining access to the infrastructure from the outside.
- *Data retention*: When the data is migrated or removed by the cloud provider or customer, there may be data residues that might expose sensitive data to unauthorized parties.
- *Compliance requirements*: Various countries have varying regulations for data privacy. Because some public cloud providers don't offer information about the location of the data, it is crucial to consider the legal and regulatory requirements about where data can be stored.
- Multi-tenancy risks: The shared nature of public cloud environments increases security risks, such as unauthorized viewing of data by other customers using the same hardware platform. A shared environment also presents resource competition problems whenever one of the customers uses most of the resources due either to need or to being exposed to targeted attacks, such as DDoS (distributed denial of service).
- *Control and visibility*: Customers have restricted control and visibility over the cloud resources because the cloud provider is responsible for administering the infrastructure. This introduces additional security concerns that originate from the lack of transparency. Customers need to rethink the way they operate as they surrender the control of their IT infrastructure to an external party while utilizing public cloud services.
- *Security responsibility*: In a cloud the vendor and the user share responsibility forsecuring the environment. The amount of responsibility shouldered by each party can change depending on the cloud model adopted.