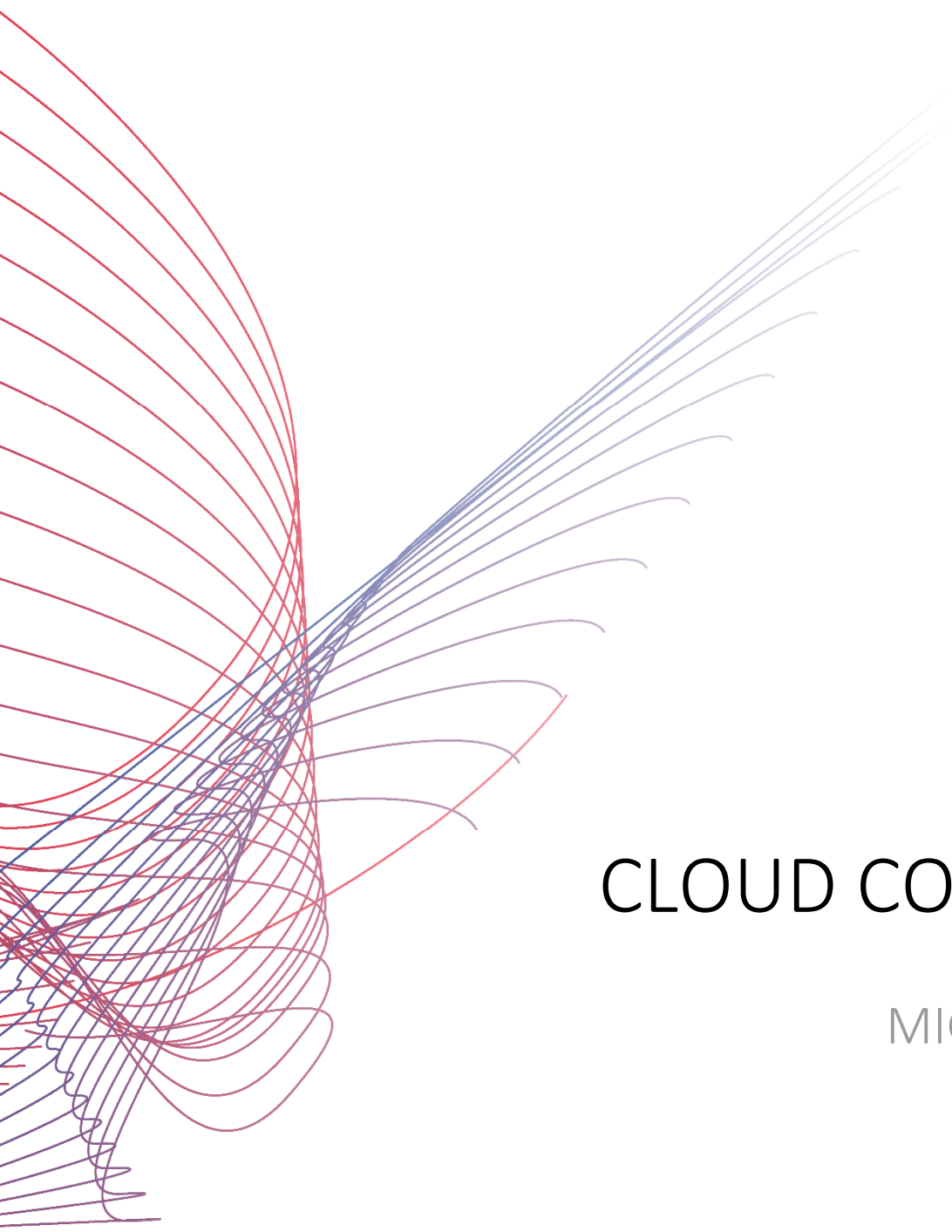
en
cs de
sk es

TECH
pedia



CLOUD COMPUTING

MIGUEL SORIANO

Title: Cloud computing
Author: Miguel Soriano
Published by: Czech Technical University of Prague
Faculty of electrical engineering
Contact address: Technicka 2, Prague 6, Czech Republic
Phone Number: +420 224352084
Print: (only electronic form)
Number of pages: 31
Edition: 1st Edition, 2017

ISBN 978-80-01-06212-8

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Explanatory Notes

	Definition
	Interesting
	Note
	Example
	Summary
	Advantage
	Disadvantage

ANNOTATION

This module contains some necessary information for the basic orientation of students in the field of cloud computing. It includes an overview of the history of this technology, the architecture, services and deployment models. Moreover, the pros and cons of cloud computing versus previous schemes or computing architectures are also presented.

OBJECTIVES

This module provides some basic information about cloud computing. Cloud computing is one of the hottest buzzwords in technology; this module aims to clarify the meaning and the different models and possibilities offered by this technology. This document tries to clarify the possible range of offerings and the terminology used to describe them in cloud computing

The main objective of this module is that readers can identify whether this type of solution can be useful for an organization, and if that is the case, which are the most suitable service and deployment model taking into account the company requirements. Finally, the reader will identify the general benefits and the major concerns about using cloud computing

LITERATURE

[1] U.S. National Institute of Standards and Technology (NIST) The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Sept. 2011. http://www.nist.gov/itl/cloud

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia "Above the Clouds: A Berkeley View of Cloud Computing" University of California at Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS

[3] Cary Landis, Dan Blacharski *Cloud Computing Made Easy: An Easy to Understand Reference About Cloud Computing*. Virtual Global Inc, 2013, ISBN 978-1482779424

[4] Douglas F. Parkhill *The Challenge of the Computer Utility*. Addison-Wesley Publishing Company, (1966), ASIN: B000O121OS, ISBN : 0240507177

[5] Antonio Regalado, Who coined "Cloud Computing"? MIT Technology Review, USA, Oct. 2011

[6] M. N.O. Sadiku, S. M. Musa, O.D. Momoh "Cloud computing: Opportunities and challenges" IEEE Potentials 02/2014; 33(1):34-36

[7] Jinesh Varia *Architecting for the Cloud: Best Practices* January 2010

[8] Peter Mell, Tim Grance “Effectively and Securely Using the Cloud Computing Paradigm”

[9] Eugene Gorelik *Cloud Computing Models,* January 2013

[10] The cloud tutorial http://thecloudtutorial.com

[11] D. Catteddu and G. Hogben, “Cloud Computing: Benefits, Risks and Recommendations for Information Security,” ENISA, 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[12] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” http://www.cloudsecurityalliance.org/csaguide.pdf.

Index

1 Introduction. What is cloud computing

According to NIST, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]

A complementary definition is provided by the RAD Lab at the University of Berkeley [2]. The authors consider that cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services.

Basically, cloud computing is a distributed computing paradigm that focuses on providing a wide range of users with distributed access to scalable, virtualized hardware and/or software infrastructure over Internet.

Cloud computing refers to the delivery of computing resources over the Internet. It consists of a collection of technologies that ensure, typically in the form of a service offered by a provider to the customer, a consistency storage or high performance data processing capabilities through the use of hardware/software distributed and virtualized network. The cloud provider can both own and house the hardware and software necessary to run the home or business applications.

Cloud computing is a complex and rapidly evolving concept. Cloud computing may be regarded as a distributed system that offers computing services via a computer communication network, usually the Internet. Resources in the cloud are transparent to the users, and the users do not need to know their exact location. They can be shared among a large number of users, who should be able to access applications and data from anywhere at anytime. A simple example of cloud computing is webmail. The webmail provider maintains the server space and provides access; the webmail user just plugs a web address into a browser and submits user information to access an account. The software and storage for her account does not exist on her computer – it's on the service's computer cloud.

The main objective of cloud computing is to make better use of these distributed resources and solve large-scale computation problems. The word "cloud" is a metaphor for describing the Web as a space where computing has been preinstalled and exists as a service [1]. Operating systems, applications, storage, data, and processing capacity all exist on the Web, ready to be shared among users.

The use of cloud computing entails that a user can benefit from data processing resources and storage that a company offers her as a service over the Internet, instead of using only the hardware and software of her computer or servers located within the corporate network. Generally, these services are offered in a completely transparent manner; the platforms hide the complexity and details of the underlying infrastructure from users and applications.

In the cloud computing model, computing power, software, storage services, and platforms are delivered on demand to external customers over the Internet.

Potentially, all kind of applications from word processing software to customized computer programs could work on a cloud computing system. The access that this technology provides to resources and services can be scaled up or down to meet demand. Cloud computing providers typically charge customers on a pay-per-use model.

While the benefits of cloud computing are many, its disadvantages are just as numerous. If used properly, cloud computing is a technology with great opportunity for businesses of all sizes.

The major advantages of cloud computing are on-demand self-service, ubiquitous network access, location-independent resource pooling, and transference of risk. Additional advantages include lower running costs, ease of utilization, quality of service, and reliability, no large scale infrastructure investment, better agility and scalability and better peak demand management. For example, cloud computing can focus the power of thousands of computers on one problem, enabling researchers to do their work faster than ever.

Nowadays, the greatest challenges with cloud computing are privacy and security. Other disadvantages are the lack or limited control, the implicit dependency on the provider also known as “vendor lock-in“. It is difficult to migrate from a provider to another once a user have rolled with it

Vivek Kundra, Federal CIO and formerly technology chief of District of Columbia said: "The cloud will do for government what the Internet did in the '90s," [3]

2 History

Information Technology has always been considered a major pain point of enterprise organizations, from the perspectives of both cost and management. However, the information technology industry has experienced a dramatic shift in the past decade – factors such as hardware commoditization, open -source software, virtualization, workforce globalization, and agile IT processes have supported the development of new technology and business models.

Cloud computing is a natural evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic and utility computing. In fact, cloud computing is a new term for a long-held dream of computing as a utility, which has recently emerged as a commercial reality. This evolution started in the fifties with mainframe computing allowing that multiple users were able of accessing a central computer through very limited terminals. Later, in the seventies, the concept of virtual machines was created. The development of cloud computing gathered momentum in the nineties, when the Internet started to provide significant bandwidth and telecommunications companies started offering virtualized private network connections.

Some experts attribute the cloud concept to John McCarthy, professor at Stanford University and inventor of Lisp, who proposed in 1961 the idea of computation being delivered as a public utility, similar to the service bureau.

In 1966 Douglas F. Parkhill published the book “The Challenge of the Computer Utility”[4] that provides a vision for the future of computing, predicting that the computer industry would come to resemble a public utility "in which many remotely located users are connected via communication links to a central computing facility”. Many characteristics of cloud computing (elastic provision, provided as a utility, online, illusion of infinite supply) are included in this book.

A. Regalado, in his paper “Who coined “Cloud Computing” [5] states that “many believe the first use of “cloud computing” in its modern context occurred on August 9, 2006, when then Google CEO Eric Schmidt introduced the term to an industry conference. “What’s interesting [now] is that there is an emergent new model,” Schmidt said, “I don’t think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing—they should be in a “cloud” somewhere.”

One of the first milestones in cloud computing history was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications available from a website. This company paved the way for both specialist and mainstream software firms to deliver applications over the Internet and played a very important role in the introduction of the Software as a Service (SaaS). The SaaS subscription model enables companies to access software online and only pay for the services and applications used.

The next development was Amazon Web Services in 2002, which provided a suite of cloud-based services including storage, computation and even human. Third-party sites could search and display products from the web site of Amazon and add

items to Amazon shopping carts. The initial version of AWS in 2002 was focused more on making information available from Amazon to partners through a web services model with programmatic and developer support and was very focused on Amazon as a retailer.

In August 2006 Amazon launched as a commercial web service its Elastic Compute cloud (EC2). This solution gives the users a new way to store data offsite, rent compute cycles as a service, and provides online services for other web sites or client-side applications. Probably, EC2 was the first widely accessible cloud computing with infrastructure as a service model.

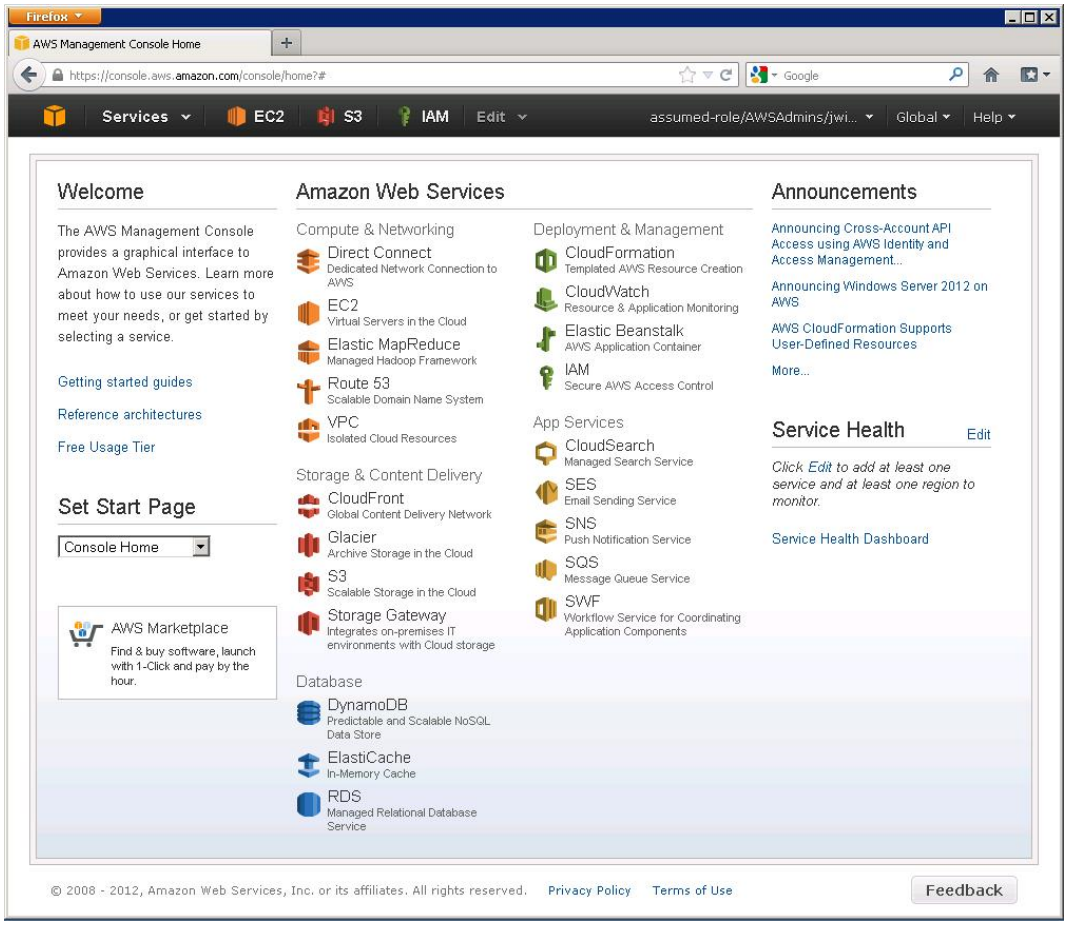


Fig. 1 – Amazon Web Services Management Console

The launch of Google App Engine in April 2008 was the entry of the first pure play technology company into the Cloud Computing market. Google Apps services allow this company started to offer browser-based enterprise applications.

Microsoft for several years did not accept the web as a significant market and continued to focus on the desktop market. Nevertheless, in November 2009, Microsoft changed this criterion and launched its Windows Azure cloud computing platform. This platform provides both PaaS and IaaS services and supports many different programming languages, tools and frameworks. It was renamed to Microsoft Azure in 2014.

In December 2013 Google Compute Engine was launched. This infrastructure enables users to create and run virtual machines on demand with a variety of configurations.

In 2009-2010, the open source cloud movement gained influence. There are numerous cloud computing services that are either written entirely in open source code, or at least incorporating open source into the final application. The use of open source code in cloud computing allows developers to build applications on top of an existing application infrastructure, gaining a lower cost, greater flexibility and probably more robust applications (with fewer flaws) than these ones entirely built from scratch. Across the many cloud computing service models, there are a large and diverse number of applications to choose from and both commercial and free open source offerings. Some examples are Apache CloudStack, Eucalyptus, OpenNebula and OpenStack [6].

The emergence of killer apps from Microsoft, Google, Amazon, Apple, Adobe, Cisco and other big IT companies results in a wider acceptance of online services and constitutes a very relevant contribution for the deployment of cloud computing.

3 Characteristics of cloud computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to NIST, this cloud model is composed of five essential characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service). Moreover, there are several common characteristics such as scalability, virtualization, service orientation, resilient coStoramputing, advanced security, geographic distribution, …

Next, the five essential characteristics are shortly described

- On-demand self-service. Cloud computing provides resources, such as server time and network storage, on demand, i.e. when the consumer wants it. Examples of resources include storage, processing, memory, and network bandwidth. The consumer can unilaterally provision computing capabilities automatically. This is possible by self-service and automation. Self-service means that the consumer performs all the actions needed to acquire the service herself. Her request is automatically processed by the cloud infrastructure, without human interaction on the service provider's side. This characteristic implies a high level of planning, since a consumer can request a new resource (i.e. a virtual machine) at any time, and expects to have it working in few minutes. The cloud provider should monitor trends in resource usage and plan for future situations well in advance.

- Broad network access. Capabilities are available over the network and accessed through different client platforms thanks to the use of standard mechanisms. This not only includes the most common devices (laptops, workstations, etc.) but also this includes mobile phones, thin clients and so on. Contrast "broad network access" with access to compute and network resources during the mainframe era. Network, storage and compute resources were scarce and costly several years ago. Over time costs associated with these resources have decreased due to manufacturing scalability and commoditization of associated technologies. As network bandwidth has increased, network access and scalability has increased accordingly. "Broad network access" can be seen both as a trait of cloud computing and as an enabler.

  Resource pooling. The resources of the service provider are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. This concept is a fundamental premise of scalability in the cloud. Multi-tenant environments, where multiple customers share adjacent resources in the cloud with their peers, are the basis of public cloud infrastructures. With multi-tenancy, there is an inherent increase in operational expenditures, which can be mitigated by certain hardware configurations and software solutions, such as application and server profiles.

The resource pooling characteristic provides the feeling of location independence; the customer generally has no control or knowledge over the location of the provided resources. Without resource pooling and multi-tenancy the economics of cloud computing do not make financial sense.

- Rapid elasticity. Elasticity is basically a ‘rename’ of scalability, that is, the ability to add or remove capacity, mostly processing, memory, or both, when this is needed. The rename of the concept is due to the Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. Most implementations of scalability are based on adding or removing nodes, servers or instances to or from a pool like a cluster or farm. A well-known example is adding a load balancer in front of a farm of web servers that distributes the requests.

- Measured service indicates that resource usage is monitored, controlled and reported to the consumer, providing visibility and transparency to consumption rates and costs for both the provider and consumer of the utilized service. This is crucial for billing, access control, resource optimization, capacity planning and other tasks.

4 Cloud computing components and architecture

Many authors emphasize the use and access of multiple server-based computational resources when they refer to cloud computing architecture.

Nevertheless, the architecture of a cloud solution is the structure of the system, which typically comprises cloud resources (back end platforms, servers and storage), services, network, middleware, and software components, the externally visible properties of those, and the relationships between them [7].

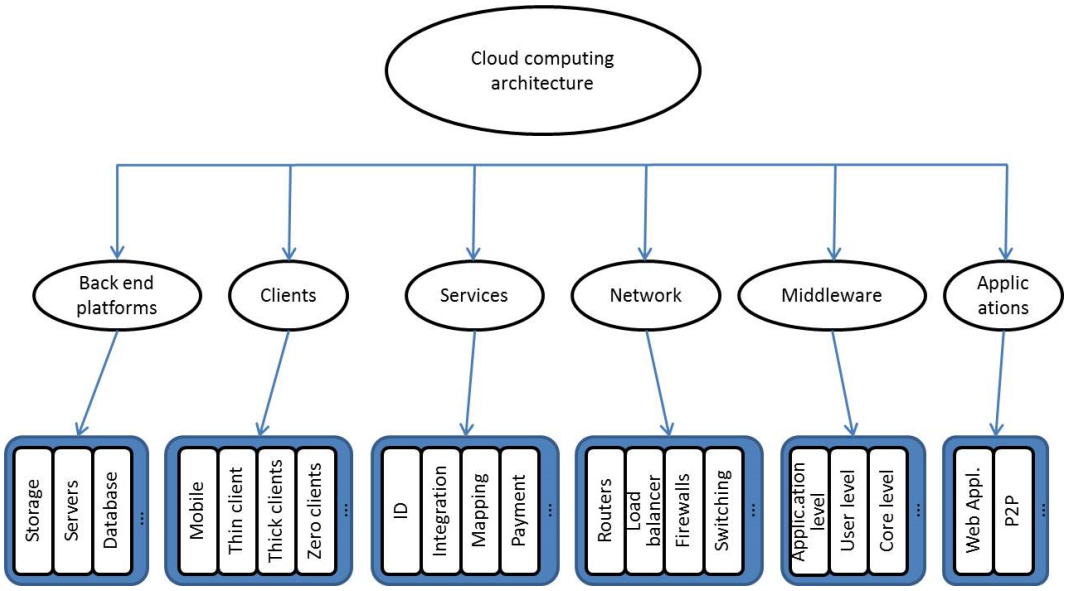


Fig. 2 – Cloud computing components

Next, the different components are introduced.

- Back end platforms. These servers are very large, can hold massive amounts of data and can be housed (distributed) anywhere in the world. Often servers are in geographically different places, but they act as if they are working next to each other. Moreover, usually there is a central server that manages the system while at the same time is used for monitoring traffic and client demands to ensure everything properly runs.

- Cloud users may access the server resources using cloud clients, including fat (or thick) clients, thin clients, zero clients, tablets and mobile devices. These client platforms interact with the cloud data storage via an application (middleware), via a web browser, or through a virtual session.

- Network: Regarding the client side, the exploitation of cloud computing services by enterprises threatens to take IT server and server management challenges and exchange them for network and network management challenges. Therefore, there are more network requirements. By the other side,

regarding the service provider, the network capabilities must ensure that all the communications happen seamlessly, efficiently and in a secure manner. It is critical to have an intelligent, reliable and functional network that provides next generation innovations .

- Middleware is the software that makes possible the connection between any two clients, servers, databases or even applications. Cloud middleware provides a number of functionalities to the user, helping her in the creation of business applications; facilitating concurrency, transactions, threading and messaging.

- Services. Cloud services are services that support cloud-based solutions, such as identity management, service-to-service integration, mapping, billing/payment systems, search, ...

- Applications. A cloud application (or cloud app) is an application program that functions in the cloud, with some characteristics of a pure desktop app and some characteristics of a pure Web app. Usually, these applications are built over a high-level integrated environment; an example is Google's App Engine, which enables users to build Web applications on the same scalable systems that power Google applications.

5 Service models

Cloud computing offers organizations new choices regarding how to run infrastructures, save costs, and delegate liabilities to third-party providers. It has become an integral part of technology and business models, and has forced businesses to adapt to new technology strategies. Accordingly, the demand for cloud computing has forced the development of new market offerings, representing various cloud service and delivery models. These models significantly expand the range of available options and task organizations with dilemmas over which cloud computing model to employ

Cloud service models describe how cloud services are available to clients. According to NIST, there are three service models: SaaS (Software as a Service), PaaS (platform as a Service and IaaS (Infrastructure as a Service) that are described in the following sections. In fact, most fundamental service models include a combination of IaaS, PaaS and SaaS. These service models may have synergies between each other and be interdependent; for example, PaaS is dependent on IaaS because application platforms require physical infrastructure.

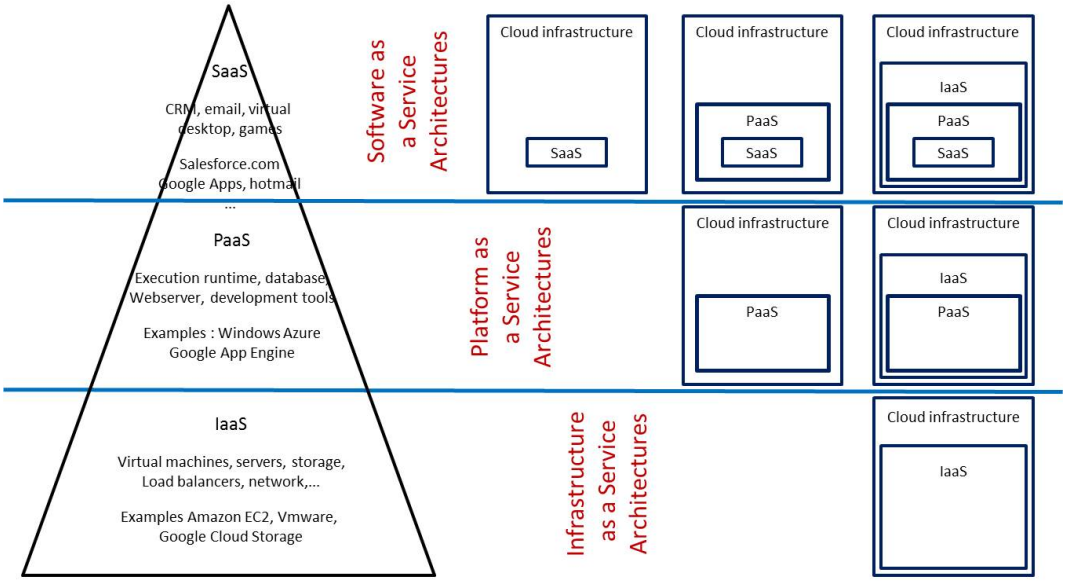


Fig. 3 – Service models. Adapted from [8]

Today, companies realize more value and resource-savings from software and platform services rather than infrastructure. Therefore IaaS service delivery model is likely to keep losing market share to PaaS and SaaS. It is expected that in the near future significant number of market consolidations with few large players retaining market control at the end [9].

5.1 Software as a Service

SaaS (Software as a service): is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. This capability eliminates the need to install software on users' computers, and it can be helpful for mobile or transient workforces.

E-mail is a simple example for SaaS. If a user has a service provider, she requires a desktop or mobile app to access the e-mail; otherwise she can host it on individual servers. It is important to point out that the user does not manage or control the underlying cloud infrastructure, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Some benefits of SaaS are:

- Cost savings: Little or no capital investment
- Flexible: Offered as an on-demand service
- Stable: SaaS applications are installed on reputed, protected, and redundant hardware
- Rapid deployment: Little to no time to provision and deploy
- Accessible: Only thing needed is an Internet access
- New releases (upgrade): Service providers upgrade the solution and it becomes available for their customers; the associated costs and efforts are lower than the traditional model

Besides the lack of control, one of the main disadvantages is that SaaS applications may not have the same features as non-SaaS applications. The functionality is often not as refined or as full. Nevertheless, this problem will diminish over time. Development tools for SaaS applications are becoming much more capable. Finally, the speed can be other disadvantage; generally SaaS applications are slower than the corresponding non SaaS equivalents.

Some examples of SaaS providers are

- Google Apps: provides web-based office tools such as e-mail, calendar and document management
- salesforce.com: provides a full customer relationship management (CRM) application
- zoho.com: provides a large suite of web-based applications, mostly for enterprise use

5.2 Platform as a Service

PaaS (Platform as a service): is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the Internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser. Basically, it is a way to rent hardware, operating systems, storage and network capacity over the Internet.

The service delivery model allows the customer to rent virtualized servers and associated services for running acquired or consumer-created applications developed using programming languages, libraries, services, and tools supported by the provider. The application development platforms allow users to create and host applications of a larger scale than an individual or small business would be able to handle. PaaS providers can assist developers from the conception of their original ideas to the creation of applications, and through to testing and deployment. This is all achieved in a managed mechanism.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. They benefit from the economies of scale that arise from the sharing of the underlying physical infrastructure between users, and that results in lower costs; PaaS services are generally paid for on a subscription basis with clients ultimately paying just for what they use.

Some examples of the features that can be included with a PaaS are:

- Operating system
- Server-side scripting environment
- Database management system
- Server Software
- Support
- Storage
- Network access
- Tools for design and development
- Hosting

Some benefits of PaaS are:

- Regarding software developers, they can use individual PaaS environments at every stage of the process to develop, test and ultimately host their applications.
- Teams Can Collaborate From Afar. Anyone in any location has the ability to work on software projects.

- Flexibility; customers can have control over the tools that are installed within their platforms and can create a platform that suits their specific requirements.
- Cost savings: there is no need to invest in physical infrastructure
- Maximize uptime: PaaS vendors should have the tools, technologies, and experience to help the user to avoid the unplanned outages that cause downtime
- Scale easily. Features can be changed if circumstances dictate that they should.

One of the cons of PaaS is that depending on the offerings of the company providing the PaaS, the user could be locked into a specific software environment, language or interface. This can affect some, not all, providers.

Some PaaS examples are:

- Google App Engine: provides users with a complete development stack and allows them to run their applications on Google's infrastructure
- Akamai EdgePlatform: provides a large distributed computing platform on which organizations can deploy their web applications; has a large focus on analysis and monitoring
- Microsoft Azure Services Platform: provides users with on-demand compute and storage services as well as a development platform based on Windows Azure
- Yahoo! Open Strategy (Y!OS): provides users with a means of developing web applications on top of the existing Yahoo! Platform and in doing so leveraging a significant portion of the Yahoo! resources

5.3 Infrastructure as a Service

IaaS (Infrastructure as a service): is a provision model in which an organization outsources the underlying operating systems, security, networking, storage and servers for developing such applications, services, and for deploying development tools, databases, etc. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Instead of ready-made applications or services, just network is provided; some of the most common uses of IaaS include virtual servers, load balancers, and network connections

IaaS allows organizations and developers to extend their IT infrastructure on an on-demand basis. The cloud provider has pool of virtualized computing resources and storage which the customer organization can take advantage of. This is on demand computing and takes care of the variation in computing peaks. Physically, the pool of hardware resource is pulled from a multitude of servers and networks usually distributed across numerous data centers, all of which the cloud provider is responsible for maintaining. The client, on the other hand, is given access to the virtualised components in order to build their own IT platforms. She does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Some benefits of IaaS are:

- Quick and easy access to enterprise class capabilities,
- Scalability; resource is available as and when the client needs it and, therefore, there are no delays in expanding capacity or the wastage of unused capacity
- Simplicity: the provider assumes the facilities management, hardware/software procurement, provisioning, patching, and all the other complex details involved with infrastructure.
- No investment in hardware; the underlying physical hardware that supports an IaaS service is set up and maintained by the cloud provider, saving the time and cost of doing so on the client side
- Location independence; the service can usually be accessed from any location as long as there is an internet connection and the security protocol of the cloud allows it
- Physical security of data centre locations; services available through a public cloud, or private clouds hosted externally with the cloud provider, benefit from the physical security afforded to the servers which are hosted within a data centre
- Rapid deployment: Little to no time to provision and deploy.

In bigger businesses, the main advantage is the last one; it is more related with timely deployment in supporting short term and unforeseen needs

The main disadvantage of the IaaS is the business risk. Even with extensive diligence, ongoing audits and proactive management, IaaS still requires trust in the vendor infrastructure/operations for availability, data security etc.

Some examples of IaaS providers are

- Amazon Elastic Compute Cloud (EC2): provides users with a special virtual machine (AMI) that can be deployed and run on the EC2 infrastructure
- Amazon Simple Storage Solution (S3): provides users with access to dynamically scalable storage resources
- Microsoft Live Mesh: provides users with access to a distributed file system; targeted at individual use
- IBM Computing on Demand (CoD): provides users with access to highly configurable servers plus value-added services such as data storage

In common with the other two forms of cloud hosting, IaaS can be utilised by enterprise customers to create cost effective and easily scalable IT solutions where the complexities and expenses of managing the underlying hardware are outsourced to the cloud provider. If the scale of a business customer's operations fluctuate, or they are looking to expand, they can tap into the cloud resource as and when they need it rather than purchase, install and integrate hardware themselves.

6 Deployment models

There are four commonly-used cloud deployment models: private, public, hybrid and community. The last one is less-commonly used.

- A private cloud is built and managed within a single organization. Organizations use software that enables cloud functionality, such as VMWare.
- A public cloud is a set of computing resources provided by third-party organizations. The most popular public clouds include Amazon Web Services, Google AppEngine, and Microsoft Azure.
- A hybrid cloud is a mix of computing resources provided by both private and public clouds.
- A community cloud shares computing resources across several organizations, and can be managed by either organizational IT resources or third-party providers

Public cloud deployment model is likely to stay dominant and keep expanding further. Private and Hybrid deployment models are going to stay for years ahead but their market share is going to continuously drop. In the long-term private and hybrid cloud models most probably will be used only for specific business cases.

6.1 Public cloud

Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure. Generally, public cloud providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access over the Internet for open use by the general public. With this model, customers have no visibility or control over where the infrastructure is located. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.

In public clouds, resources are offered as a service. Users can scale their use on demand and do not need to purchase hardware to use the service. Public cloud providers manage the infrastructure and pool resources into the capacity required by its users.

Public Cloud customers benefit from economies of scale, because infrastructure costs are spread across all users, allowing each individual client to operate on a low-cost, “pay-as-you-go” model. Another advantage of public cloud infrastructures is that they are typically larger in scale than an in-house enterprise cloud, which provides clients with seamless, on-demand scalability. These clouds offer the greatest level of efficiency in shared resources.

A public cloud is the obvious choice when:

- The standardized workload for applications is used by lots of people, such as e-mail.
- It is needed to test and develop application code.
- An incremental capacity is required (the ability to add compute resources for peak times).
- Collaboration projects are being done.

6.2 Private cloud

In a private cloud, the cloud infrastructure is a proprietary operated solely for a single client or organization. It is not shared with other organizations but it can comprise multiple consumers (e.g., business units). The infrastructure may be hosted internally or externally and it can be managed by the organization, by a third party or by some combination of them. It allows organizations to host data and applications in the cloud, in a more secure and controlled environment regarding public clouds. The resources are deployed behind a firewall and may be accessed across private leased lines or secure encrypted connections via public networks to get the specified clients (and only they) can operate. The objective of these mechanisms is to minimize security concerns and limit access to specific clients.

There are two variations of private clouds according to the place where it is hosted [10]:

On-Premise Private Cloud: This type of cloud is hosted within an organization's own facility. This option is suitable for organizations that have invested in substantial server and storage hardware and want to leverage that investment and repurpose some of such equipment in a private cloud, either for applications that require complete control and configurability of the infrastructure and security.

Externally Hosted Private Cloud: Externally hosted private clouds are hosted by a third party specializing in cloud infrastructure. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources.

Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment. Private clouds are more expensive but also more secure when compared to public clouds. An important part of IT decision-makers will focus exclusively on the private cloud, as these clouds offer the greatest level of security and control.

As a summary, a private cloud is the best option when

- A high control level is needed.
- Data security and privacy are critical.
- Data sovereignty is required but cloud efficiencies are desired

6.3 Community cloud

A community cloud is a multi-tenant cloud service model that is shared among several organizations from a specific group with common computing concerns (e.g., mission, security requirements and compliance considerations). These organizations or communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives. Community Cloud has its own challenges like allocation of costs, responsibilities, governance and security

The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized. The cloud may be managed by the organisations or by a third party and can be either on-premise or off-premise.

In general, public cloud services are likely to be more cost efficient and scalable than private clouds, but less secure.

The goal of community clouds is to have participating organizations realize the benefits of a public cloud with the added level of privacy, security, and policy compliance usually associated with a private cloud.

Government, healthcare, telco community, and some regulated private industries are leveraging the added security features within a community cloud environment. Instead of just provisioning space in a public cloud, organizations can test and work on a cloud platform which is secure, “dedicated,” and even compliant with certain regulations.

6.4 Hybrid cloud

Hybrid Cloud or combined Cloud is a combination of different methods of resource pooling (for example, combining public and community clouds. Also, hybrid clouds can be seen as a composition of two or more clouds (private, community or public) that are bound together, offering the advantages of multiple deployment models, by standardized or proprietary technology that enables data and application portability. These entities can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. The idea of hybrid cloud is to combine several cloud models to create a customized solution based on the organization requirements

Hybrid cloud architecture requires both on-premise resources and off-site server based cloud infrastructure and can be implemented in a number of ways. For instance, it is possible for an entity to have its data and applications in cloud maintaining control over organizational network topology and polices, and at the same time keeping its existing physical infrastructure (although this infrastructure does not scale) and borrow additional resources when required.

Hybrid clouds allow a company to keep each aspect of its business in the most efficient environment possible. Moreover, these models are easily scalable, cost efficient (it is possible to reduce the demand on a private cloud by moving non-sensitive data or applications to the public cloud), secure and flexibles.

The downside is that they have to keep track of multiple cloud security platforms and ensure that all aspects of the business can communicate with each other.

Hybrid cloud is a good option when:

- A company might use a public cloud for test and development while using a hosted private cloud inside the organization for production deployment.
- A company that uses public clouds for external facing applications while using a hosted private cloud for internal applications.
- A company that wants to use a public cloud to interact with the customers but keep their sensitive data secured within a private cloud.

7 Uses and applications

Cloud computing can support nearly any application. But some workloads are a better fit for cloud from a organization or technical perspective. The two killer use cases for cloud computing are:

Managing big data. Cloud computing is a natural fit for big data analytics, since elastic computing capacity and on-demand provisioning make analytics accessible to more teams within an organization. Moreover, cloud is also a useful solution when lots of computations are required for solving complex problems, or when collaboration among developers is needed. Cloud computing allows much more efficient computation by centralizing storage memory processing and bandwidth

Test and developments in the cloud. Development teams will benefit from the agility of creating virtual machines in minutes. Cloud computing avoids that organizations need to set up an environment through physical assets, significant manpower and time. Moreover, an organization can quickly get applications into production and to scale them as required

Other relevant uses are:

- File storage and sharing
- Backup and disaster recovery
- CRM
- Web site hosting

Typical applications are:

- Social networks sites
- E-mail sites
- Search engines
- Communications facilities (i.e. Skype)
- Time-tracking applications
- Notes organizer (like evernote)
- Creating and sharing office documents (google apps)

8 Benefits and disadvantages of cloud computing

Many users, businesses large and small use cloud computing today either directly (e.g. Google or Amazon) or indirectly (e.g. Twitter) instead of traditional alternatives.

Clouds can provide users with a number of different benefits. One of the most relevant is the reduction of cost and complexity of owning and operating computers and networks. Cloud users do not need to invest in information technology infrastructure, purchase hardware, or buy software licences. Moreover, there are clouds providers specialized in particular areas (such as e-mail) that can bring advanced services very useful for a single company.

Some other benefits to clients include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development. In addition, information in the cloud is not as easily lost

Next, there is a list of some of the most important benefits derived of the use of cloud computing.

- Availability and universal access. Cloud computing can allow remotely located employees to access resources and applications resources at any time through a standard internet connection.

- Choice of applications. This allows flexibility for cloud users to experiment and choose the best option for their needs. Cloud computing also allows a business to use, access and pay only for what they use, with a fast implementation time

- Collaboration. Users begin to see the cloud as a way to work simultaneously on common data and information.

- Cost reduction. The pay-per-usage model, unlike on-site hosting, allows an organization to only pay for the resources they need with basically no investment in the physical resources available in the cloud.

- Elasticity. The provider transparently manages the clients resource utilization based on dynamically changing needs.

- Flexibility. Cloud computing allows clients to switch applications easily and rapidly, using the one that suits their needs best.

- Potential to be greener and more economical. The average amount of energy needed for a computational action carried out in the cloud is far less than the average amount for an on-site deployment. This is because different organisations can share the same physical resources.

- Risk reduction. Organizations can use the cloud to test ideas and concepts before making major investments in technology.
- Scalability. Users have access to a large amount of resources that scale based on their demand.
- Up to date software. A cloud provider will also be able to upgrade software keeping in mind feedback from previous software releases.
- Virtualization. Each user has a single view of the available resources, independently of how they are arranged in terms of physical devices. Therefore, there is potential from a provider perspective to serve a greater number of users with fewer physical resources.

Nevertheless, there are some problems that can act as a barrier when an organization wants to adopt cloud computing. Following there is a list of these concerns:

- Interoperability. A universal set of standards and/or interfaces have not yet been defined, resulting in a significant risk of vendor lock-in.
- Latency. All access to the cloud is done via the internet, introducing latency into every communication between the user and the provider.
- Platform or Language Constraints. Some cloud providers support specific platforms and languages only.
- Regulations. There are concerns in the cloud computing community over jurisdiction, data protection, fair information practices, and international data transfer, mainly for organizations that manage sensitive data.
- Reliability. Many existing cloud infrastructures leverage commodity hardware that is known to fail unexpectedly.
- Resource Control. The amount of control that the user has over the cloud provider and its resources vary greatly between providers.
- Security. The main concern is data privacy: users do not have control or knowledge of where their data is being stored. Nevertheless, regarding forensic security, the use of cloud computing (when using virtualisation) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down-time for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance [11]

9 Cloud security. Potential privacy risks

While there are benefits, there are privacy and security concerns too. Data is travelling over the Internet and is stored in remote locations. In addition, cloud providers often serve multiple customers simultaneously. All of this may raise the scale of exposure to possible breaches, both accidental and deliberate. It is needed to ensure that the personal information is appropriate handled [12]. Security concerns may be magnified by the dynamic nature of the cloud environment. One of the cloud key advantages is the speed with which the cloud vendors can adjust, develop and change their offerings. There is a tradeoff between this speed and flexibility requirements and the security level.

Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem increases in cases of multiple transfers of data, e.g., between federated clouds.

Privacy, including the need to protect identity information, is a core issue in the success of cloud computing deployment. Many organizations do not feel comfortable storing their data and applications on systems that reside outside of their on-premise data centers. The risk of exposure or unauthorized access of sensitive data increases when workloads migrate to a shared infrastructure.

Concerns have been raised by many that cloud computing may lead to “function creep” — uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware. Given how inexpensive it is to keep data, there is little incentive to remove the information from the cloud and more reasons to find other things to do with it

Cloud service providers must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy-protection mechanisms must be embedded in all security solutions.

10 Conclusions

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. Specifically, cloud computing usually refers to a cloud alternative to something that organizations would traditionally manage in-house, using dynamically scalable and often virtualized resources provided as a service over the Internet/Intranet. For example, a webmail service is a cloud-based alternative to hosting your own email server.

Most cloud computing services are accessed through a web browser using any connected device (mobile, tablet, personal computer, ...). Therefore, cloud services do not require users to have sophisticated computers that can run specialized software. A user-centric interface makes the cloud infrastructure supporting the applications transparent to users.

Cloud computing has the potential to be a disruptive force by affecting the deployment and use of technology; in fact cloud is changing the way that many organizations manage information technology. Depending on the perspective and situation of the organization or the individual, this represents both opportunity and crisis. Such change may be resisted, even if it is a good idea and it works. Companies have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services.

One of the main concerns is security and privacy. This concern depends on the kind of company. In the case of big organizations with significant resources to devote to a sophisticated information security program, it is needed to overcome a number of security, privacy, and compliance challenges. Nevertheless, in the case of a small to medium-size business (SMB), the security of cloud computing might look attractive, compared to the resources the company can afford to spend on information security today.