Trechos para organização:

Cloud computing is a collection of IT services provided to customer over a network along with the ability to scale up down the service requirements. Cloud computing has the potential to eliminate the requirements for setting up of high cost infrastructure for IT-based solutions and services that industry uses. This promises to provide a flexible IT architecture, accessible through internet and portable devices. But despite the gain achieved from cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hinder the growth of cloud. This research paper analyzes the architecture of cloud along with definition of cloud computing, the various cloud models and brief overview of cloud contain any reference citations or displayed equations.

In order to define Cloud Computing, it is first necessary to explain what is mean by the phrase “The Cloud”. The first reference to “The Cloud” originated from the telephone industry in 1990s, when Virtual Private Network (VPN) service was first offered. This VPN service was used By providers along with customer, telephone companies despite of using hard wire data circuits to transmit data. This allowed provides and customers to offer the same amount of band width at a lower cost by rerouting the network traffic in real time to accommodate ever-changing network utilization. The term “Cloud” in phrase Cloud Computing refers to the internet and its infrastructure.

The advantages of cloud computing includes:

i. Reduced hardware and maintenance cost,

ii. Accessibility around the world, and

iii. Flexibility and highly automated processes wherein the customers need not to worry about software up-gradation.

In early days, the mainframe computer was very large or bulk in size and the computing platform was centralized with limited power and resources, CPU, memory so used by limited **number** of users. As origin of mainframe computer was 1920s so it gives the concept of Cloud Computing as all the data of user stored on server and user access the data from anywhere at any time. No hard drive or special system required only its account is necessary. From the example we understand the overall concept of “Cloud Computing”. When we store our photos or data online (internet) instead of our home PC or we use our webmail or social networking site then it is “CLOUD COMPUTING”. There are three service models of Cloud Computing SaaS, PaaS, and IaaS. SaaS refers to Software as a Service in this a system with operating systems, hardware and network provided or we can say a pre developed system. PaaS refers to Platform as a Service in this the operating system, hardware and network are provided and customer/user installs or develops its own software. And IaaS refers to Infrastructure as a Service in this the customer has the knowledge about all the stuff. There are no publically available standards specific to cloud computing security. In this paper we propose the following standards for maintaining security in an unsafe environment.

**Main characteristics include:**

i. Broad network access: Ability to access the service via standard platform like desktop, laptop, mobile etc.

ii. Resource pooling: Resources are pooled across multiple customers.

iii. Rapid elasticity: capability to cope with demand peaks.

iv. Measured service: Billing delivered as utility service.

The history of term “Cloud” ” is originated from telecommunications world, where telecom companies started offering Virtual Private Network (VPN) services along with comparable quality of service at a much lower cost. Before invention of VPN, they provided dedicated point-to-point data circuits which are nothing thing but wastage of bandwidth. But by using VPN services they able to switch traffic to balance utilization of overall network. Cloud computing now extends this to cover servers and network infrastructure. Many players in industries have jumped into cloud computing and implemented it. For example Amazon has played a important role and launched the Amazon Web Service (AWS) in 2006. Along with this Google and IBM also started research projects in Cloud Computing. Eucalyptus become the first open source platform for deploying the private clouds.

**ARCHITECTURE**

Cloud Computing is a collection of all IT services that are provided to a customer over a network on leased basis and with the ability to scale up or down their service requirements. Most of the time cloud computing services are delivered by third party provider who owns the infrastructure.

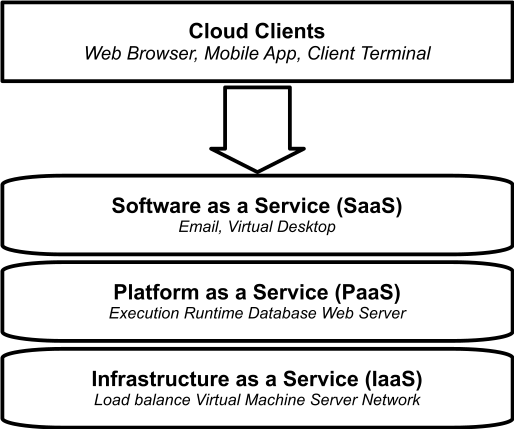
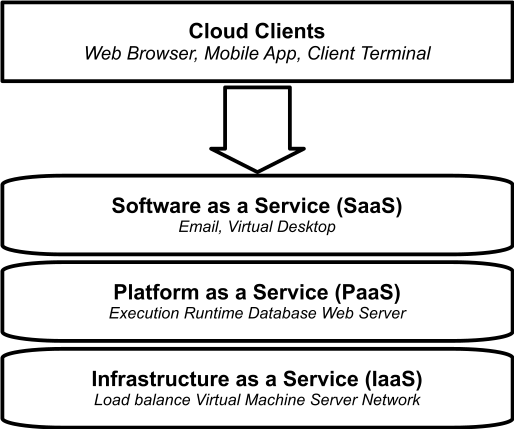
There are two basic cloud models, first the Cloud Service Model and Cloud Deployment Model

3.1 Cloud Service Model

Cloud Computing is delivery of computing where massively scalable IT-based capabilities are provided, as service across the internet clients. This term effectively focus the different aspects of Cloud Computing paradigm which can be found at different levels of infrastructure. There are three types of services provided by Cloud Computing architecture namely SaaS, PaaS, IaaS. The figure 3.1 shows the hierarchy of services.

[International Journal of Advent Research in Computer and Electronics (IJARCE) (E-ISSN: 2348-5523) Special Issue National Conference “CONVERGENCE 2015”, 28 March 2015   
Cloud Computing: History, Architecture, Security Issues Swati I. Bairagi, Ankur O. Bang - https://ijarce.org/downloads/convergence2015/Convergence-26.pdf]

Desenho 1: Cloud Computing Services



**IBM:**

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote [data center](https://www.ibm.com/topics/data-centers) managed by a cloud services provider (or CSP). The CSP makes these resources available for a monthly subscription fee or bills them according to usage.

Compared to traditional on-premises IT, and depending on the cloud services you select, cloud computing helps do the following:

* ****Lower IT costs:****Cloud lets you offload some or most of the costs and effort of purchasing, installing, configuring, and managing your own on-premises infrastructure.
* ****Improve agility and time-to-value:****With cloud, your organization can start using enterprise applications in minutes, instead of waiting weeks or months for IT to respond to a request, purchase and configure supporting hardware, and install software. Cloud also lets you empower certain users—specifically developers and data scientists—to help themselves to software and support infrastructure.
* ****Scale more easily and cost-effectively:****Cloud provides elasticity—instead of purchasing excess capacity that sits unused during slow periods, you can scale capacity up and down in response to spikes and dips in traffic. You can also take advantage of your cloud provider’s global network to spread your applications closer to users around the world.

The term ‘cloud computing’ also refers to the technology that makes cloud work. This includes some form of *virtualized IT infrastructure—*servers, operating system software, networking, and other infrastructure that’s abstracted, using special software, so that it can be pooled and divided irrespective of physical hardware boundaries. For example, a single hardware server can be divided into multiple virtual servers.

[Virtualization](https://www.ibm.com/topics/virtualization) enables cloud providers to make maximum use of their data center resources. Not surprisingly, many corporations have adopted the cloud delivery model for their on-premises infrastructure so they can realize maximum utilization and cost savings vs. traditional IT infrastructure and offer the same self-service and agility to their end-users.

If you use a computer or mobile device at home or at work, you almost certainly use some form of cloud computing every day, whether it’s a cloud application like Google Gmail or Salesforce, streaming media like Netflix, or cloud file storage like Dropbox. Industry analyst [Gartner projected recently that worldwide end-user public cloud spending to reach nearly USD 600 billion in 2023](https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023) (link resides outside ibm.com).

[https://www.ibm.com/topics/cloud-computing]

## The concept of “cloud computing” has been around much longer than you think. Let’s dive into its history.

## The humble beginnings of cloud

Believe it or not, the modern day idea of “[cloud computing](https://www.ibm.com/cloud/learn/cloud-computing)” dates back to the 1950s, when large-scale mainframes were made available to schools and corporations. The mainframe’s colossal hardware infrastructure was installed in what could be called a “server room” (since the room would generally only be able to hold a single mainframe). Multiple users were able to access the mainframe via “dumb terminals”—stations with the sole function of facilitating access to the mainframes.

Due to the cost of buying and maintaining mainframes, an organization wouldn’t be able to afford a mainframe for each user. It became practice to allow multiple users to share access to the same data storage layer and CPU power from any station. By enabling shared mainframe access, an organization would get a better return on its investment in this sophisticated piece of technology.

### Virtualization changes everything

Twenty years later in the 1970s, IBM released an operating system called [VM](https://en.wikipedia.org/wiki/VM_(operating_system)) that permitted admins on its System/370 mainframe systems to have multiple virtual systems, or “[virtual machines (VMs)](https://www.ibm.com/cloud/learn/virtual-machines)” on a single physical node. The VM operating system took the 1950s application of shared access of a mainframe to the next level by allowing multiple distinct compute environments to live in the same physical environment.

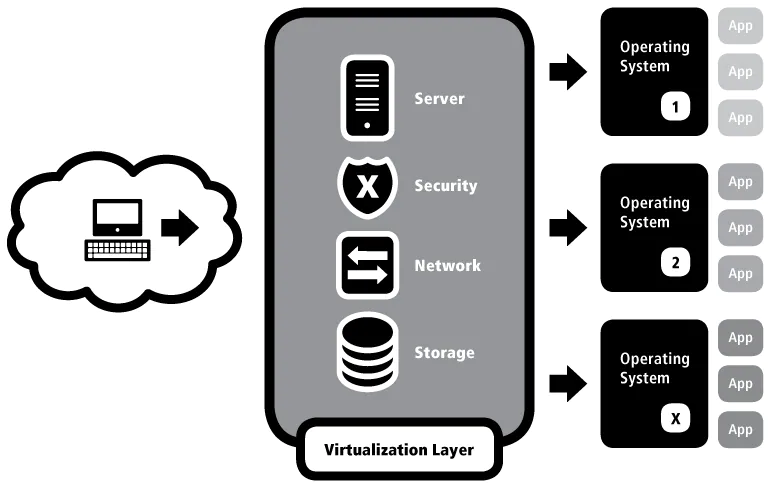
Most of the basic functions of any virtualization software that you see nowadays can be traced back to this early VM OS. Every VM ran custom operating systems or guest operating systems that had their own memory, CPU, and hard drives, along with CD-ROMs, keyboards, and networking—despite the fact that those resources were shared. “[Virtualization](https://www.ibm.com/cloud/learn/virtualization-a-complete-guide)” became a technology driver, and it became a huge catalyst for some of the biggest evolutions in communications and computing.

In the 1990s, telecommunications companies that historically only offered single dedicated point-to-point data connections began offering virtualized private network connections—with the same service quality as dedicated services at a reduced cost. Rather than building out physical infrastructure to allow more users to have their own connections, telecommunications companies provided users with shared access to the same physical infrastructure. This change allowed telecommunications companies to shift traffic as necessary, leading to better network balance and more control over bandwidth usage.

Virtualization meets the Internet

Meanwhile, virtualization for PC-based systems started in earnest. As the Internet became more accessible, the next logical step was to take virtualization online. If you were in the market to buy servers 10 or 20 years ago, you know that the costs of physical hardware—while not at the same level as the mainframes of the 1950s—were pretty outrageous. As more and more people expressed the demand to be online, the costs had to come out of the stratosphere and into reality.

One of the ways that happened was through—you guessed it—virtualization. Servers were virtualized into shared hosting environments, virtual private servers, and virtual dedicated dervers using the same types of functionality provided by the VM OS in the 1950s.

What did this look like in practice? Let’s say your company required 13 physical systems to run your sites and applications. With virtualization, you can take those 13 distinct systems and split them up between two physical nodes. Obviously, this kind of environment saves on infrastructure costs and minimizes the amount of actual hardware you would need to meet your company’s needs.

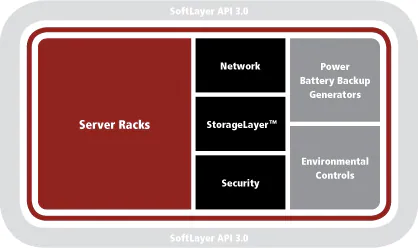
As the costs of server hardware slowly came down, more users could afford to purchase their own dedicated servers. But they ran into a different kind of problem: One server isn’t enough to provide the necessary resources. The market shifted from a “These servers are expensive; let’s split them up” belief to a “These servers are cheap; let’s figure out how to combine them” mentality. Because of that shift, the most basic understanding of “cloud computing” was born online.

### The cloud is born

By installing and configuring a piece of software called a [hypervisor](https://www.ibm.com/cloud/learn/hypervisors) across multiple physical nodes, a system would present the environment’s entire resources as though those resources were in a single physical node. To visualize that environment, technologists used terms like “utility computing” and “cloud computing,” since the sum of the parts seemed a nebulous blob of computing resources you could then segment out as needed (like telecommunications companies did in the 1990s). In these cloud computing environments, it adding resources to the “cloud” was easy—add another server to the rack and configure it to become part of the bigger system.

As technologies and hypervisors improved upon reliably sharing and delivering resources, many enterprising companies decided to carve up the bigger environment. They wanted to make the cloud’s benefits available to users who didn’t have an abundance of physical servers available to create their own cloud computing infrastructure. Those users could order “cloud computing instances” (also known as “[cloud servers](https://www.ibm.com/cloud/learn/cloud-server)”) by ordering the resources they needed from the larger pool of available cloud resources. Because the servers were already online, the process of “powering up” a new instance or server is almost instantaneous. Because little overhead is involved for the owner of the cloud computing environment when a new instance is ordered or cancelled (since it’s handled by the cloud’s software), management of the environment is much easier.

### Go beyond the standard cloud computing environment

Most companies today operate with the aforementioned definition of “the cloud” as the end-all, be-all—but IBM Cloud isn’t “most companies.” IBM Cloud took the idea of a cloud computing environment and pulled it back one more step. Instead of installing software on a cluster of machines to let users grab pieces, we built a platform that automated the manual aspects of bringing a server online without a hypervisor on the server. We call this platform “IMS.” What hypervisors and virtualization do for a group of servers, IMS does for an entire data center. As a result, you can order a bare metal server with the resources you need and without any unnecessary software installed—and that server will be delivered to you in a matter of hours.

Without a hypervisor layer between your operating system and the bare metal hardware, your servers perform better. Because we automate almost everything in our data centers, you’re able to spin up load balancers and firewalls and storage devices on demand and turn them off when you’re done with them.

Other providers have cloud-enabled servers. We have [cloud-enabled data centers](https://www.ibm.com/cloud-computing/bluemix/data-centers).

IBM Cloud is leading the drive toward wider adoption of innovative cloud services. We have ambitious goals for the future. If you think we’ve come a long way from the mainframes of the 1950s, you ain’t seen nothin’ yet.

### The most open and secure public cloud for business

Today, the IBM Cloud is the most open and secure [public cloud](https://www.ibm.com/cloud/public/?cm_mmc=OSocial_Linkedin-_-Cloud+and+Data+Platform_Cloud+Platform+F2F-_-WW_WW-_-CDAIS+Fall+Momentum+Day+1+&cm_mmca1=000036KM&cm_mmca2=10003590&linkId=76040022) for business. Open architectures, based on [Kubernetes](https://www.ibm.com/cloud/learn/kubernetes) and [containers](https://www.ibm.com/cloud/learn/containers), are driving the next wave of cloud-based business innovation. That’s why IBM has just completed a two-year journey to enhance its public cloud on a foundation of open source software, security leadership and enterprise grade infrastructure. It delivers trusted and secure solutions and access to innovation backed by deep industry expertise. It’s a brand-new cloud—that’s also battle-tested, trusted and proven—for running your core business.

[A Brief History of Cloud Computing - <https://www.ibm.com/cloud/blog/cloud-computing-history>]

Traditionally, security concerns have been the primary obstacle for organizations considering cloud services, particularly public cloud services. In response to demand, however, the security offered by cloud service providers is steadily outstripping on-premises security solutions.

Maintaining cloud security demands different procedures and employee skillsets than in legacy IT environments. Some cloud security best practices include the following:

* ****Shared responsibility for security:****Generally, the cloud provider is responsible for securing cloud infrastructure and the customer is responsible for protecting its data within the cloud—but it's also important to clearly define data ownership between private and public third parties.
* ****Data encryption:****Data should be encrypted while at rest, in transit, and in use. Customers need to maintain full control over security keys and hardware security module.
* ****User identity and access management:****Customer and IT teams need full understanding of and visibility into network, device, application, and data access.
* ****Collaborative management:**** Proper communication and clear, understandable processes between IT, operations, and security teams will ensure seamless cloud integrations that are secure and sustainable.
* ****Security and compliance monitoring:**** This begins with understanding all regulatory compliance standards applicable to your industry and setting up active monitoring of all connected systems and cloud-based services to maintain visibility of all data exchanges between public, private, and hybrid cloud environments.

What is cloud security?

In modern-day enterprises, there has been a growing transition to cloud-based environments and IaaS, Paas, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring a number of challenges to enterprises when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud.

Security threats have become more advanced as the digital landscape continues to evolve. These threats explicitly target cloud computing providers due to an organization's overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information, regardless of where it is stored.

Cloud security should be an important topic of discussion regardless of the size of your enterprise.  Cloud infrastructure supports nearly all aspects of modern computing in all industries and across multiple verticals.

However, successful cloud adoption is dependent on putting in place adequate countermeasures to defend against modern-day cyberattacks. Regardless of whether your organization operates in a public, private, or hybrid cloud environment, cloud security solutions and best practices are a necessity when ensuring business continuity.

****Lack of visibility****  
It's easy to lose track of how your data is being accessed and by whom, since many cloud services are accessed outside of corporate networks and through third parties.

****Multitenancy****  
Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses.

****Access management and shadow IT****  
While enterprises may be able to successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that don't deploy bring-your-own device (BYOD) policies and allow unfiltered access to cloud services from any device or geolocation.

****Compliance****  
Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

****Misconfigurations****  
Misconfigured assets accounted for 86% of breached records in 2019, making the inadvertent insider a key issue for cloud computing environments. Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.

****Identity and access management (IAM)****  
[Identity and access management (IAM)](https://www.ibm.com/verify) tools and services allow enterprises to deploy policy-driven enforcement protocols for all users attempting to access both on-premises and cloud-based services. The core functionality of IAM is to create digital identities for all users so they can be actively monitored and restricted when necessary during all data interactions

****Data loss prevention (DLP)****  
Data loss prevention (DLP) services offer a set of tools and services designed to ensure the security of regulated cloud data. DLP solutions use a combination of remediation alerts, data encryption, and other preventative measures to protect all stored data, whether at rest or in motion.

****Security information and event management (SIEM)****  
[Security information and event management (SIEM)](https://www.ibm.com/products/qradar-siem) provides a comprehensive security orchestration solution that automates threat monitoring, detection, and response in cloud-based environments. Using artificial intelligence (AI)-driven technologies to correlate log data across multiple platforms and digital assets, SIEM technology gives IT teams the ability to successfully apply their network security protocols while being able to quickly react to any potential threats.

****Business continuity and disaster recovery****  
Regardless of the preventative measures organizations have in place for their on-premise and cloud-based infrastructures, data breaches and disruptive outages can still occur. Enterprises must be able to quickly react to newly discovered vulnerabilities or significant system outages as soon as possible. [Disaster recovery solutions](https://www.ibm.com/cloud/disaster-recovery) are a staple in cloud security and provide organizations with the tools, services, and protocols necessary to expedite the recovery of lost data and resume normal business operations.

[<https://www.ibm.com/topics/cloud-security>]

## Introduction to History of Cloud Computing

Cloud computing has now become an ideal way to deliver solutions and enterprise applications for different businesses across the globe. The History of Cloud Computing started in the early 1960s. During this period the concepts of time-sharing took a rise via Remote Job Entry. This terminology was associated with IBM and DEC (Digital Equipment Corporation). Due to this growth, full time-sharing systems were available by the early 1970s. By the 1990’s, few telecommunication giants started offering VPN (Virtual private network) services at affordable costs. As they could do by switching traffic with proper server use, it made them use the overall network more effectively. By 1994, the cloud metaphor was started to be used for virtualized services.

### Who Invented Cloud Computing?

Cloud Computing was invented in the early 1960s by J.C.R Licklider (Joseph Carl Robnett Licklider), an American Psychologist and Computer Scientist. During his network research work on ARPANet (Advanced Research Project Agency Network), trying to connect people and data all around the world, gave an introduction to Cloud Computing technique which we all know today. Born on March 11th, 1915 in St. Louis, Missouri, US, J.C.R Licklider pursued his initial studies from Washington University in 1937 and received a BA Degree with three specializations including physics, maths, psychology. Later in the year 1938, Licklider completed his MA in psychology and received his Ph.D. from the University of Rochester in the year 1942. His interest in Information Technology and looking at his years of service in different areas and achievements, made his appointed as Head of IPTO at ARPA (US Department of Defense Advanced Research Project Agency) in the Year 1962. His aim led to ARPANet, a forerunner of today’s Internet.

The beauty of the cloud computing phase went on running throughout the era of the 21st Century. By mid-2000s probably 2006 Amazon created [AWS (Amazon web services)](https://www.educba.com/what-is-aws/) and also noted its Elastic Computing Cloud (EC2). By 2008, Google too introduced its beta version of the search engine. Earlier announced by Microsoft in the year 2008, it released its cloud computing service named Microsoft Azure for testing, deployment and managing applications and services. In the year 2012, Google compute engine was released but was rolled to the public by the end of Dec 2013. Oracle introduced Oracle Cloud with three primary services for business (IaaS, PaaS and SaaS). Currently, as per records, Linux and [Microsoft Azure](https://www.educba.com/what-is-azure/) share most of their work parallel.

### Why Cloud Computing was Invented?

The Defense Advanced Research Project Agency in the year 1963, funded $2 million for a project which included developing a technology that allows a computer to be used by two or more persons simultaneously. Here giant computers were used, where reels of magnetic tape for memory and a forerunner, currently named “cloud computing” were taken into consideration. It acted as a cloud giving access to max 3 peoples to connect. In the vision of expansion, J.C.R Licklider in the year 1969, developed the ARPANet (known as the primitive version of the internet). He advanced his vision named Intergalactic Computer Network, in which anyone on the globe can be interconnected by means of computers and also access the information from anywhere and anytime. The term coined virtualization in the year 1970s made a shift, which now describes the creation of a virtual machine that acts like a fully functional real computer system. The most use of virtual computers in the 1990’s and business offering virtual service led to the development of cloud computing infrastructure.

### Advantages Behind Cloud Computing

Cloud Computing has gained wide popularity in the last few years. With the increase in data security and storing vital information, Cloud has gained its place for business requirements. Cloud works as the same phenomenon as web-based email services for storing the data in bulk and accessing it at any corner around the world. Some of the few cloud-based applications are Facebook, Instagram and Google Cloud, etc. Such an application provides cloud-hosted servers where the user personal data are been stored for later access.

Below are listed a few advantages of Cloud Computing in businesses:

1. Implementing a Cloud-based server or being on the cloud makes you cost-effective as it will easier to access organization data and information which saves time and investment in the early phase. Moreover, the cloud has facilities for storage area too, which means pay only for the storage you have installed. Revenue growth also increases investing in cloud applications.
2. Security Concern is a big issue when it comes to onsite viewing and storage of files and documents. As its cybercrime doing the same thing for remotely accessing data. The Key to enhance security is one by encrypting the data that is being transmitted over networks. Moreover, different security features are available to the users too.
3. Rather than hosting an application in Local Server, Cloud gives a lot of flexibility on hosting on its platform. It increases the overall efficiency of the organization.
4. Cloud computing provides greater mobility and connectivity to connect with people and information. It allows to access data from anywhere, anyplace and anytime.
5. Clouds based applications update and upgrade their software versions without being manually functioned.
6. [Cloud storage helps](https://www.educba.com/what-is-cloud-storage/) in loss prevention from data. If any valuable data is stored in local hardware and due to any viral infections, malware or malfunctions the data gets corrupted. To prevent loss, it’s better to dump all data in the cloud which gives better flexibility and access anytime.

### Conclusion

Cloud computing offers alternatives to IT departments for improved flexibility and lower cost. Cloud Computing profits in market demands by improving resource utilization and providing tremendous benefits to customers of all sizes. It promises increased reliability and scalability. Despite the potential gains, few companies are still having a concern in accepting it due to some application security issues which may hamper the cloud in the long run. As per the ongoing research and development activities, cloud computing holds the potential to stand out at the top but with a few challenges to come alongside which it should take care of for its future growth.

[Priya Pedamkar - <https://www.educba.com/history-of-cloud-computing/>]

**Brief History of Cloud Computing**

**By Keith D. Foote on December 17, 2021**

**Cloud Computing**

In 1963, DARPA (the Defense Advanced Research Projects Agency) presented MIT with $2 million for Project MAC. The funding included a requirement for MIT to develop technology allowing for a “computer to be used by two or more people, simultaneously.” In this case, one of those gigantic, archaic computers using reels of magnetic tape for memory became the precursor to what has now become collectively known as cloud computing. It acted as a primitive cloud with two or three people accessing it. The word “virtualization” was used to describe this situation, though the word’s meaning later expanded.

In 1969, J. C. R. Licklider helped develop the ARPANET (Advanced Research Projects Agency Network), a “very” primitive version of the Internet. JCR, or “Lick,” was both a psychologist and a computer scientist, and promoted a vision called the “Intergalactic Computer Network,” in which everyone on the planet would be interconnected by way of computers, and able to access information from anywhere. (What could such an unrealistic, impossible-to-pay-for, fantasy of the future look like?) The Intergalactic Computer Network, otherwise known as the internet, is necessary for access to the cloud.

The meaning of virtualization began shifting in the 1970s, and now describes the creation of a virtual machine, that acts like a real computer, with a fully functional operating system. The concept of virtualization has evolved with the internet, as businesses began offering “virtual” private networks as a rentable service. The use of virtual computers became popular in the 1990s, leading to the development of the modern cloud computing infrastructure.

Cloud Computing in the Late 1990s

In its early stages, the cloud was used to express the empty space between the end user and the provider. In 1997, Professor Ramnath Chellapa of Emory University defined cloud computing as the new “computing paradigm, where the boundaries of computing will be determined by economic rationale, rather than technical limits alone.” This somewhat ponderous description rings true in describing the cloud’s evolution.

The cloud gained popularity as companies gained a better understanding of its services and usefulness. In 1999, Salesforce became a popular example of using cloud computing successfully. They used it to pioneer the idea of using the Internet to deliver software programs to the end users. The program (or application) could be accessed and downloaded by anyone with Internet access. Businesses could purchase the software in an on-demand, cost-effective manner, without leaving the office.

Cloud Computing in the Early 2000s

In 2002, Amazon introduced its web-based retail services. It was the first major business to think of using only 10% of its capacity (which was commonplace at the time) as a problem to be solved. The cloud computing infrastructure model allowed them to use their computer’s capacity much more efficiently. Soon after, other large organizations followed their example.

In 2006, Amazon launched Amazon Web Services, which offers online services to other websites, or clients. One of Amazon Web Services’ sites, called Amazon Mechanical Turk, provides a variety of cloud-based services including storage, computation, and “human intelligence.” Another of Amazon Web Services’ sites is the Elastic Compute Cloud (EC2), allowing individuals to rent virtual computers and use their own programs and applications.

In the same year, Google launched Google Docs services. Google Docs was originally based on two separate products, Google Spreadsheets and Writely. Google purchased Writely, which offers renters the ability to save documents, edit documents, and transfer them into blogging systems. (These documents are compatible with Microsoft Word.) Google Spreadsheets (acquired from 2Web Technologies, in 2005) is an Internet-based program allowing users to develop, update, and edit spreadsheets, and to share the data online. An Ajax-based program is used, which is compatible with Microsoft Excel. The spreadsheets can be saved in an HTML format.

In 2007, IBM, Google, and several universities joined forces to develop a server farm for research projects needing both fast processors and huge data sets. The University of Washington was the first to sign up and use resources provided by IBM and Google. Carnegie Mellon University, MIT, Stanford University, the University of Maryland, and the University of California at Berkeley, quickly followed suit. The universities immediately realized computer experiments can be done faster and for less money, if IBM and Google were supporting their research. Since much of the research was focused on problems IBM and Google had interests in, they also benefitted from the arrangement. 2007 was also the year when Netflix launched it’s streaming video service, using the cloud, and provided support for the practice of “binge-watching.”

Eucalyptus offered the first AWS API compatible platform, which was used for distributing private clouds, in 2008. In the same year, NASA’s OpenNebula provided the first open-source software for deploying private and hybrid clouds. Many of its most innovative features focused on the needs of major businesses.

2010 and Beyond

Although private clouds were initiated in 2008, they were still undeveloped, and not very popular. Concerns about poor security in public clouds was a strong driving force promoting the use of private clouds. In 2010, companies like AWS, Microsoft, and OpenStack had developed private clouds that were fairly functional. (2010 was also when OpenStack made an open-sourced, free, do-it-yourself cloud, which became very popular, available to the general public.)

The concept of hybrid clouds was introduced in 2011. A fair amount of interoperability is needed between a private and public cloud, and the ability to shift workloads back and forth between the two clouds. At this time, very few businesses had systems capable of doing this, though many wanted to, because of the tools and storage public clouds could offer.

In 2011, IBM introduced the IBM SmartCloud framework, in support of Smarter Planet (a cultural thinking project). Then, Apple launched the ICloud, which focuses on storing more personal information (photos, music, videos, etc.). Also, during this year, Microsoft began advertising the cloud on television, making the general public aware of its ability to store photos, or video, with easy access.

Oracle introduced the Oracle Cloud in 2012, offering the three basics for business, IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service), and SAAS (Software-as-a-Service). These “basics” quickly became the norm, with some public clouds offering all of these services, while other focused on offering only one. Software-as-a-service became quite popular.

CloudBolt was founded in 2012. This company gets credit for developing a hybridcloud management platform that helped organizations build, deploy and manage both private and public clouds. They resolved the interoperability problems between public and private clouds.

Multi-clouds began when organizations started using SaaS providers for certain services, such as human resources, customer relations management, and supply chain management. This started becoming popular in roughly 2013-2014. While this use of SaaS providers is still quite popular, a philosophy of using multiple clouds for their specific services and advantages has developed. This philosophy includes not becoming trapped into using a specific cloud because of “interoperability problems.”

By 2014, cloud computing had developed its basic features, and security had become a major concern. Cloud security has become a fast-growing service, because of its importance to customers. Cloud security has advanced significantly in the last few years, and now provides protection comparable to traditional IT security systems. This includes the protection of critical information from accidental deletion, theft, and data leakage. Having said that, security is, and may always be, the primary concern of most cloud users.

Currently, one of the primary users of cloud services are application developers. In 2016 the cloud began to shift from developer-friendly to developer-driven. Application developers began taking full advantage of the cloud for the tools it had available. A large number of services strive to be developer-friendly to draw more customers. Realizing the need, and the potential for profit, cloud vendors developed (and continue to develop) the tools apps developers want and need.

Containers

Although primitive containers have been around since 2004 (Solaris containers), these early containers were very limited, and restricted to certain computer systems. It wasn’t until 2013, when Docker came up with a container that was extremely functional, that these tools caught on. It is no coincidence that the growth of both Docker and container use and Docker happened simultaneously.

In 2017, hundreds of tools that had been around for years were modified and used to make working with containers easier. Kubernetes, developed by Google in 2014, and then made available as an open-source product, was one of these. Kubernetes is a container-orchestration system designed to automate application deployments, scaling, and management.

The Future of Cloud Computing

The coronavirus pandemic accelerated use of the internet for eCommerce and working remotely. Automated data governance software for dealing with a growing number of internet laws and regulations seems a reasonable prediction for the future of the cloud. For more on the future of the cloud, learn about the cloud computing trends of 2022.

[<https://www.dataversity.net/brief-history-cloud-computing/>]

# Deployment models of Cloud Computing

Created: Sep 27, 2022 07:45:39

****Private cloud****

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. Undertaking a private cloud project requires significant engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. It can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

****Public cloud****

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.[103] Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon Web Services (AWS), Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.

****Hybrid cloud****

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Gartner, Inc. defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.

Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that cannot be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization pays for extra compute resources only when they are needed. Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands. The specialized model of hybrid cloud, which is built atop heterogeneous hardware, is called "Cross-platform Hybrid Cloud". A cross-platform hybrid cloud is usually powered by different CPU architectures, for example, x86-64 and ARM, underneath. Users can transparently deploy and scale applications without knowledge of the cloud's hardware diversity. This kind of cloud emerges from the raise of ARM-based system-on-chip for server-class computing.

