|  |
| --- |
| Moscow State UniversityFaculty of Computational Mathematics and Cybernetics |
| Cloud computing |
|  |
|  |
| **Vasilenko Anatoly**  |
| **02.10.2011** |

|  |
| --- |
|  |

**Contents**

1. Overview
2. Characteristics
3. Layers
* 3.1 Client
* 3.2 Application
* 3.3 Platform
* 3.4 Infrastructure
* 3.5 Server
1. Deployment models
* 4.1 Public cloud
* 4.2 Community cloud
* 4.3 Hybrid cloud
* 4.4 Private cloud
1. Architecture
* 5.1 The Intercloud
* 5.2 Cloud engineering
1. Issues
* 6.1 Privacy
* 6.2 Open source
* 6.3 Open standards
* 6.4 Security
* 6.5 Abuse
1. Research
2. Sources

**Cloud computing**

**Cloud computing** is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).

**Overview**

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

The concept of cloud computing fills a perpetual need of IT: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personal, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities.

Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers.

Cloud computing providers deliver applications via the internet, which are accessed from a web browser, while the business software and data are stored on servers at a remote location. In some cases, legacy applications are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location; in other cases, entire business applications have been coded using web-based technologies such as AJAX.

Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies.

**Characteristics**

Cloud computing exhibits the following key characteristics:

* **Agility** improves with users' ability to re-provision technological infrastructure resources.
* **Application programming interface (API)** provides accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.
* [**Cost**](http://en.wikipedia.org/wiki/Cost) is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house).
* **Device and location independence** enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.
* **Multi-tenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
	+ **Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
	+ **Peak-load capacity** increases (users need not engineer for highest possible load-levels)
	+ **Utilization and efficiency** improvements for systems that are often only 10–20% utilized.
* **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
* **Scalability** **and Elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.
* **Performance** is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.
* **Security** could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than under traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
* **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer.

**Layers**

Once an internet protocol connection is established among several computers, it is possible to share services within any one of the following layers: client, application, platform, infrastructure, server.

**Client**

A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery and that is in essence useless without it. Examples include some computers, phones and other devices, operating systems, and browsers.

**Application**

Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.

**Platform**

Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.

**Infrastructure**

Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Suppliers typically bill such services on a utility computing basis; the amount of resources consumed (and therefore the cost) will typically reflect the level of activity.

**Server**

The servers layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

**Deployment models**

**Public cloud**

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned to the general public on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis.

**Community cloud**

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the benefits of cloud computing are realised.

**Hybrid cloud**

Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

**Private cloud**

Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from lower up-front capital costs and less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

**Architecture**

*Cloud architecture*, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple *cloud components* communicating with each other over a loose coupling mechanism such as a messaging queue.

**The Intercloud**

The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based.

**Cloud engineering**

**Cloud engineering** is the application of [engineering](http://en.wikipedia.org/wiki/Engineering) disciplines to cloud computing. It brings a systematic approach to the high level concerns of commercialization, standardization, and governance in conceiving, developing, operating and maintaining cloud computing systems. It is a multidisciplinary method encompassing contributions from diverse areas such as systems, software, web, performance, information, security, platform, risk, and quality engineering.

**Issues**

**Privacy**

The cloud model has been criticized by privacy advocates for the greater ease in which the companies hosting the cloud services control, and, thus, can monitor at will, lawfully or unlawfully, the communication and data stored between the user and the host company. Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million phone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity. While there have been efforts (such as US-EU Safe Harbor) to "harmonize" the legal environment, providers such as [Amazon](http://en.wikipedia.org/wiki/Amazon_Web_Services) still cater to major markets (typically the United States and the European Union) by deploying local infrastructure and allowing customers to select "availability zones."

**Open source**

Open-source software has provided the foundation for many cloud computing implementations, one prominent example being the Hadoop framework. In November 2007, the Free Software Foundation released the Affero General Public License, a version of GPLv3 intended to close a perceived legal loophole associated with free software designed to be run over a network.

**Open standards**

Most cloud providers expose APIs that are typically well-documented (often under a Creative Commons license) but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, with a view to delivering interoperability and portability.

**Security**

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model differ widely from those of traditional architectures.

The relative security of cloud computing services is a contentious issue that may be delaying its adoption. Issues barring the adoption of cloud computing are due in large part to the private and public sectors unease surrounding the external management of security based services. It is the very nature of cloud computing based services, private or public, that promote external management of provided services. This delivers great incentive among cloud computing service providers in producing a priority in building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solution to various cloud security issues vary through cryptography, particularly public key infrastructure (PKI), use of multiple cloud providers, standardization of APIs, improving virtual machine support and legal support.

**Abuse**

As with privately purchased hardware, crackers posing as legitimate customers can purchase the services of cloud computing for nefarious purposes. This includes password cracking and launching attacks using the purchased services. In 2009, a banking [trojan](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) illegally used the popular Amazon service as a command and control channel that issued software updates and malicious instructions to PCs that were infected by the malware.

**Research**

Many universities, vendors and government organizations are investing in research around the topic of cloud computing:

* In October 2007 the Academic Cloud Computing Initiative (ACCI) was announced as a multi-university project designed to enhance students' technical knowledge to address the challenges of cloud computing.
* In April 2009, the St Andrews Cloud Computing Co-laboratory was launched, focusing on research in the important new area of cloud computing. Unique in the UK, StACC aims to become an international centre of excellence for research and teaching in cloud computing and will provide advice and information to businesses interested in using cloud-based services.
* In June 2011, the Telecommunications Industry Association developed a Cloud Computing White Paper, to analyze the integration challenges and opportunities between cloud services and traditional U.S. telecommunications standards.

**Sources**

<http://en.wikipedia.org/wiki/Cloud_computing>

<http://www.linuxjournal.com/content/cloud-computing-good-or-bad-open-source>

<http://www.firstlinesoftware.com/solutions/cloud/>

Summary

**Cloud computing** is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network.

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.

Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies.

Cloud computing exhibits the following key characteristics: agility, application programming interface, cost, device and location independence, multi-tenancy (centralization, peak-load capacity, utilization and efficiency), reliability, scalability and elasticity, performance, security, maintenance.

I would like to explain some of these characteristics:

* **Application programming interface (API)** provides accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.
* **Multi-tenancy** enables sharing of resources and costs across a large pool of users thus allowing for:
	+ **Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
	+ **Peak-load capacity** increases (users need not engineer for highest possible load-levels)
	+ **Utilization and efficiency** improvements for systems that are often only 10–20% utilized.
* **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
* **Maintenance** of cloud computing applications is easier, because they do not need to be installed on each user's computer. The maintenance is one of the most important parameters of cloud computing, because without this feature nobody will never start to use it.

Once an internet protocol connection is established among several computers, it is possible to share services within any one of the following layers: client, application, platform, infrastructure, server.

* There is four types of deployment models: public cloud, community cloud, hybrid cloud, private cloud. Public cloud describes cloud computing in the traditional mainstream sense.
* Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.)
* Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.
* Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

*Cloud architecture*, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple *cloud components* communicating with each other over a loose coupling mechanism such as a messaging queue.

Cloud computing has many important issues: privacy, open source, open standarts, security. Firstly, the privacy, the cloud model has been criticized by privacy advocates for the greater ease in which the companies hosting the cloud services control, and, thus, can monitor at will, lawfully or unlawfully, the communication and data stored between the user and the host company. Secondly, open-source software has provided the foundation for many cloud computing implementations. Thirdly, most cloud providers expose APIs that are typically well-documented (often under a Creative Commons license) but also unique to their implementation and thus not interoperable. And finally, security, as cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model differ widely from those of traditional architectures.

At last, I would like to say that many universities, vendors and government organizations are investing in research around the topic of cloud computing