BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXV No. 3/2013	13 - 20	Seria Tehnică

Cloud Computing PaaS Application

Otilia Cangea

Universitatea Petrol-Gaze din Ploieşti, Bd.Bucureşti, nr. 39, Ploieşti
e-mail: ocangea@upg-ploiesti.ro

Abstract

Nowadays, technology is in a continuous process of renewal, that leads to improving every activity; in this respect, one may define cloud computing – a modern concept that combines computers and informatics. The aim of this paper is to build a PaaS private cloud computing application, emphasizing the specific features of the system and the security requirements for data storage,management, and transfer in the given particular environment.

Key words: *cloud computing, platform as a service application, security risks.*

Introduction

The concept of „cloud" came into sight early on in the 60's, when in the specialty literature one discussed about using computing power as a public service, but it was in 1997, when Ramnath Chellapp, a well-known computer science professor, used for the first time the notion of „cloud computing"[1]. He defined the term „cloud" as a *computing paradigm where the boundaries of computing will be determined rational rather than by technical limits*. Since then, an increasingly number of business activities have oriented to cloud computing, considering the benefits of transparency and costs reduction.

A "cloud" may, practically, be defined as a set of hardware equipments, networks, storage spaces, services, and interfaces that deliver computing power. Cloud services comprise delivering software, infrastructure, and storage space on the Internet, considered either as separate components, or as a complete platform, based upon the user requests [4].

From an economic perspective, the main highlight of cloud computing is the one reffering to the fact that clients access only the needed resources, and, consequently, pay only what they really use; the resources are available any time and any place in the cloud. This is the reason why cloud computing is also known as „utility computing" or „IT at request".

A classification of the models that implement cloud computing includes the public cloud, the cloud for a communion, the private cloud, and the hybrid cloud.

Public cloud

A public cloud is based upon the standard model of cloud computing, where a service provider produces resources, such as applications or storage space, available to the public at large on the Internet. The public cloud services may be offered free of charge or of pay-per-usage manner. Figure 1 presents some examples of public cloud for Amazon Web Services, Microsoft Windows Azure and Google App Engine.

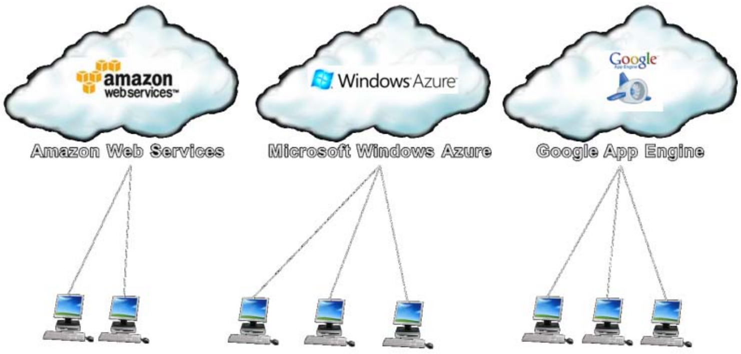


Fig. 1. Public cloud [4].

Cloud for a communion

The cloud for a communion (fig. 2) divides the infrastructure among many organizations from a particular communion having mutual interests (security, jurisdiction). The costs are shared by less users than in a public cloud, but by more users than in a private cloud, so that the resulted savings of the cloud computing potential are not so impressive [5].

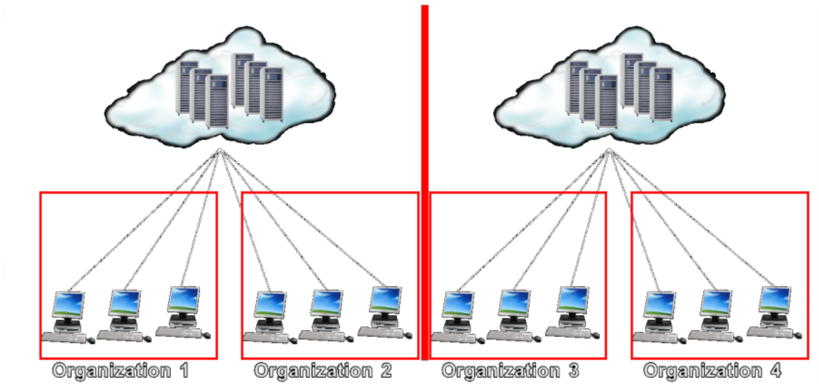


Fig. 2. Cloud for a communion [5].

Private cloud

The private cloud, also known as internal cloud or corporation cloud (fig. 3), reports to particular computing architectures that host services for a restricted number of users, usually protected by a firewall structure [4].

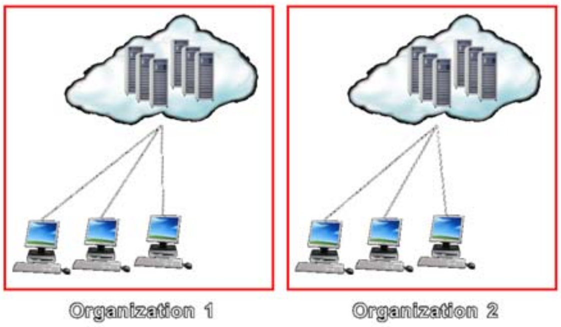


Fig. 3. Private cloud [4]

Hybrid cloud

A hybrid cloud, represented in Figure 4, is composed of at least a private cloud and at least a public cloud [4]. This type of cloud is usually provided in two manners: a distributor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a distributor that offers private cloud platforms.

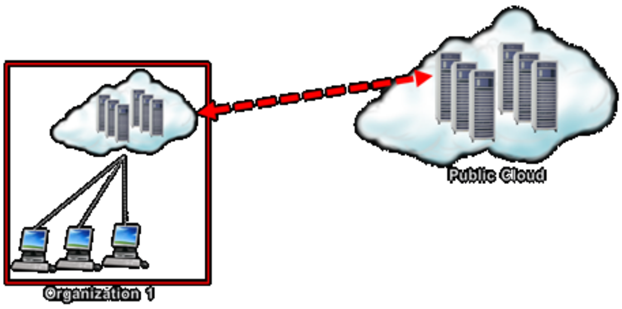


Fig. 4. Hybrid cloud [4].

Cloud Services

Cloud computing providers offer their services by means of three fundamental models, that are: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), where IaaS is the simplest, and the upper models inherit characteristics of the lower ones [3, 5].

Infrastructure as a service (IaaS)

IaaS is the simplest model: the IaaS providers offer computers – physical or virtual machines – and other resources, as well as data storage, firewalls, IP addresses, local virtual networks, and software packages [2]. These resources are provided upon request, from the own stores installed in data centers. In order to insure a good connectivity, clients may use Internet or mobile phone networks, that have integrated cloud services. The IaaS model is presented in Figure 5.

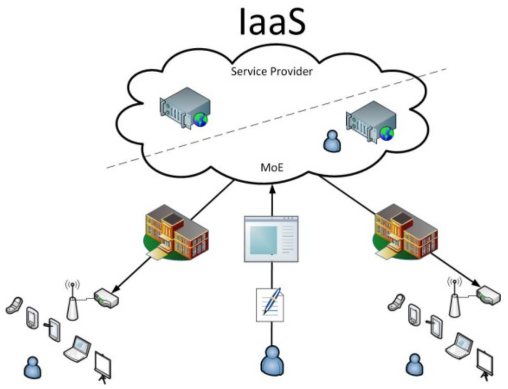


Fig. 5. IaaS model [2].

Platform as a service (PaaS)

In the PaaS model (fig. 6), the cloud providers offer a computing platform that contains an operating system, a programming environment, a data base, and a web server, so that the applications programmers can create and run their own software solutions on a cloud platform, without the costs and complexity implied by buying and managing the basic hardware and software levels.

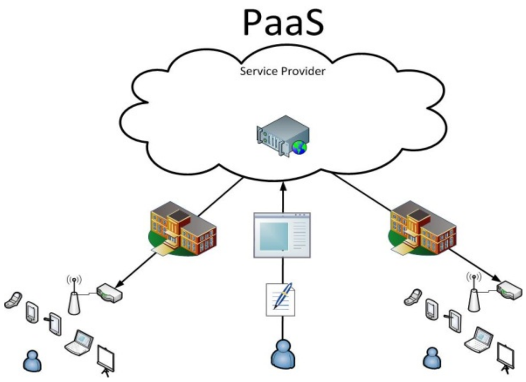


Fig. 6. PaaS model [2].

Software as a service (SaaS)

In the SaaS model, users have access to applications and data bases, and cloud providers manage the infrastructure and the platforms that run the applications (fig. 7). SaaS is usually known as „ software upon request” and the users have to pay a subscription.

The cloud providers set up and manage the software applications in the cloud. As the cloud users do not manage the cloud infrastructure and the platform on which the application runs, there is no need to use the personal computer of the client. The activity is shared by multiple virtual machines, so that the process is transparent to the user, that sees only one access point.

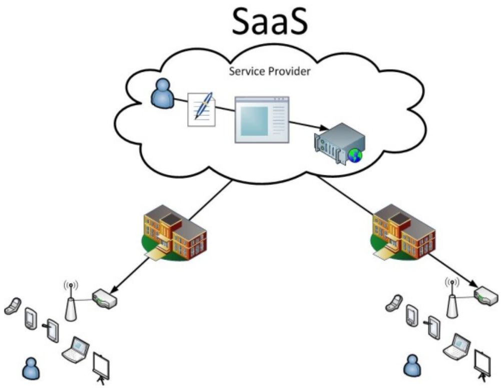


Fig. 7. SaaS model [2].

Security Risks in Cloud Computing

The development of cloud services model offers more efficient private business oriented technologies and changed the way IT departments think, design and provide computing technologies and applications. Nevertheless, these improvements created a new security vulnerability, with a significant impact. In this respect, studies [5] offer organizations up-to-date information regarding the security threats, the most important being briefly follow-up presented.

Data security violation

If the data base of a cloud service having several clients is not very well designed, a failure in one client application may allow an attacker to access the data of all the other clients. Unfortunately, even if data can be encrypted in order to reduce the risks of information leakage, the menace of losing the encryption key is significant. In the reverse order, one may keep offline copies of the data, with dangerous consequences regarding data security.

Data loss

Under the new data protection settlements of the European Union, data loss and private data alteration are considered forms of data security violation and would require specific notifications. In addition, many concordance politics demand the custody of audit recordings and other documents, so that, if these data are kept in a non-secure cloud, their loss could endanger the status of the organization.

Account piracy

Account or service piracy, usually by using stolen connection data, is a top threat. Thus, attackers can access critical areas of the installed cloud computing services, compromising the confidentiality, the integrity and the availability of these services.

Denial of Service- DoS

DoS attacks are meant to restrict the cloud service users to access its own data or applications. By forcing the cloud service of the "victim" to use immoderate system resources (processor power, memory, space disk or network band width), the attacker determines an intolerable lagging of the system, with major consequences upon the proper operation of the entire system.

Cloud service abuse

One of the major benefits of cloud computing is that it allows even a small company to access big amounts of processed information. Nevertheless, not everyone fairly uses this feature. An attacker may need a long time to break an encryption key, but using a matrix of cloud servers, could do this in a couple of minutes, or could use that matrix in order to create a DoS attack.

Cloud Computing PaaS Application

The Cloud Computing PaaS application consists in designing a private cloud composed of two servers (one for data storage, one for security purposes), where the connected clients can save their data, but cannot interact; the information is hidden for the non-authorized ones.

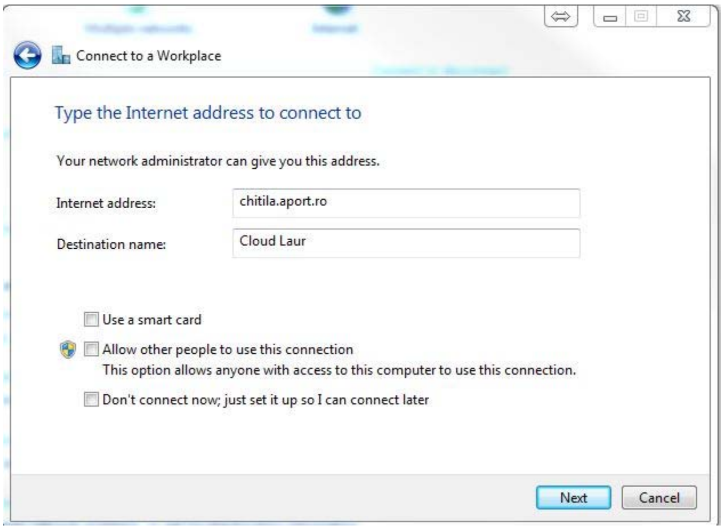
The application has a VPN (Virtual Private Network) connection, highly secured, that comprises a FTP (File Transfer Protocol) connection, in order to insure the security requirements for a data transfer in cloud computing.

The methodology of obtaining an user account in a cloud application is as follows:

- one sends an e-mail to a particular address, specifying the complete name, e-mail address, telephone number;
- one receives the confirmation, containing user name, password for the VPN server connection and for the FTP server, VPN and FTP servers addresses, information about the maximum amount of data that can be stored, and the folders that may be accessed;
- one creates and tests the VPN server connection and the FTP server, as presented in Figure 8.

The application provides information regarding the VPN server, as seen in Figure 9.

MS CHAP V2 is an authentication protocol and MPPE 128 is a protocol for data encryption in private networks that uses a RSA RC4 encryption algorithm. MPPE uses 40 bit, 56 bit, and 128 bit keys for a session, frequently changed in order to improve the security.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: chitila.aport.ro

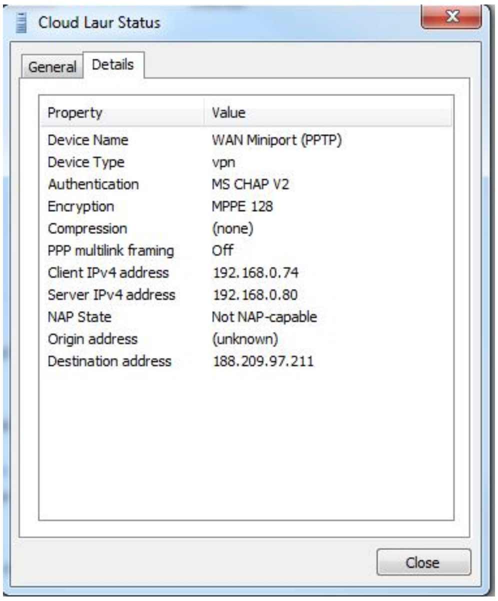
Destination name: Cloud Laur

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later

Fig. 8. VPN server connection.



Cloud Laur Status

Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.0.74
Server IPv4 address	192.168.0.80
NAP State	Not NAP-capable
Origin address	(unknown)
Destination address	188.209.97.211

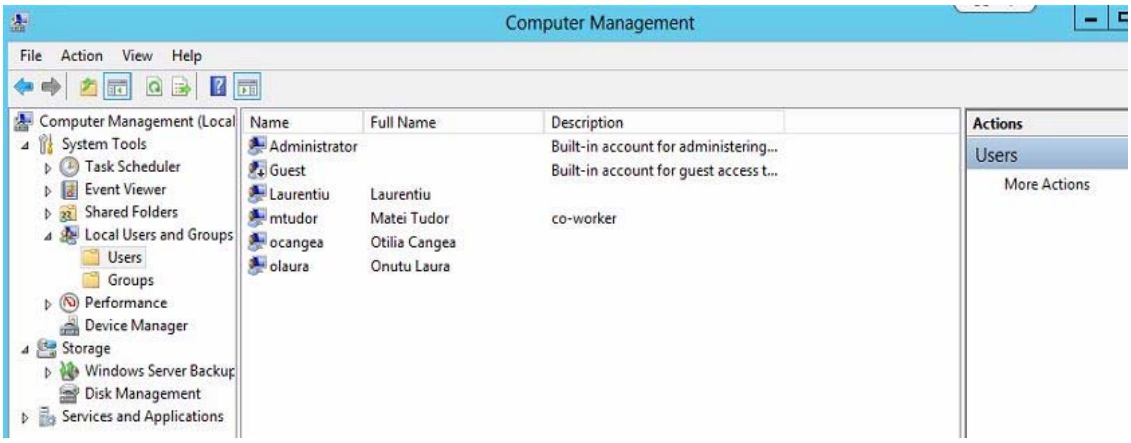
Fig. 9. VPN server information.

In the firewall there are performed the following set-up operations, in order to allow the VPN traffic:

- for PPTP: 1723 TCP and the 47 GRE protocol (PPTP Pass-through);
- for L2TP over IPSEC: 1701 TCP and 500 UDP;
- for SSTP: 443 TCP.

The application allows static IP settings for each user, for a better security control, as a major concern in cloud computing applications is the one regarding the protection of the VPN server. In addition, clients that use laptop for establishing a VPN connection must have an updated anti-virus that runs every time the computer is turned on and a personal firewall software. The firewall may insure that the VPN client is the right one, not a Trojan programme.

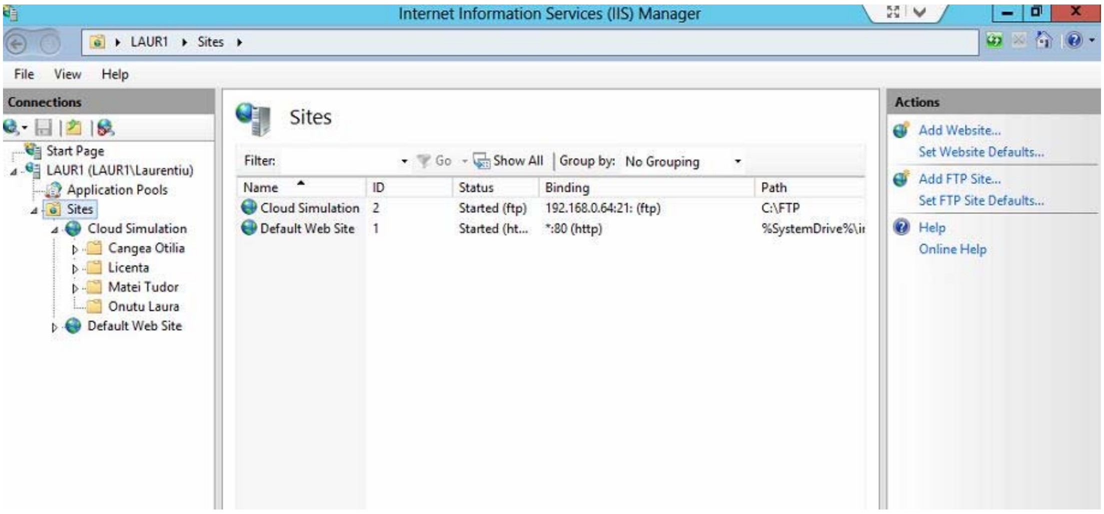
Both servers have the same users, with different passwords, with respect to the resources, VPN or FTP (fig. 10). The passwords may be changed only by the Administrator.



Name	Full Name	Description
Administrator		Built-in account for administering...
Guest		Built-in account for guest access t...
Laurentiu	Laurentiu	
mtudor	Matei Tudor	co-worker
ocangea	Otilia Cangea	
olaura	Onutu Laura	

Fig. 10. Clients that are allowed to use VPN and FTP.

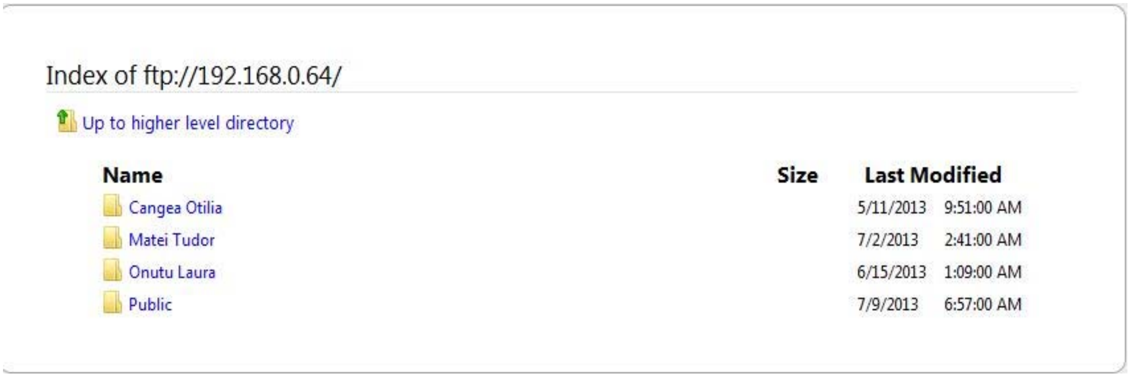
Each user has a personal folder that may be accessed, the other are blocked by IIS Manager, installed on FTP server, presented in Figure 11.



Name	ID	Status	Binding	Path
Cloud Simulation	2	Started (ftp)	192.168.0.64:21: (ftp)	C:\FTP
Default Web Site	1	Started (ht...	*:80 (http)	%SystemDrive%\i

Fig. 11. FTP manager

Access to FTP server can be done from the web browser (fig. 12). Data stored on these servers have a very high level of security due to the fact that the access to information can not be performed directly, all servers being virtual machines installed on a Windows Server 2012, and the information is distributed in RAID 10 on 12 HDD and virtually in RAID 5.


Index of ftp://192.168.0.64/

Up to higher level directory

Name	Size	Last Modified
Cangea Otilia		5/11/2013 9:51:00 AM
Matei Tudor		7/2/2013 2:41:00 AM
Onutu Laura		6/15/2013 1:09:00 AM
Public		7/9/2013 6:57:00 AM

Fig. 12. Private and public folders from FTP server in web browser

All data from the server that hosts virtual machines are encrypted using BitLocker, specific to Windows Server, that may be installed only by the system administrator. Once activated, a password is created in order to restrict the unauthorized access, as well as a password recovery key that is saved on USB memory. The data access can be performed only by using the accurate password.

Conclusions

The aim of this paper was to build the Cloud Computing PaaS application, that consists in designing a private cloud based on VPN and FTP technologies. There are presented the methodology of obtaining an user account in a cloud application, the protocols used for authentication and data encryption, the set-up operations performed in the firewall and the way clients may use the storage facilities managed by the FTP manager. The most important conclusion is that all the technologies that define this concept have to be designed very responsibly, in order to insure the security requirements regarding data protection.

As future directions, the designed cloud can be expanded for many different applications, for example operation on applications exclusively installed on servers, where the storage space and the processing power are not limited, as on personal computers.

References

1. Chellapp, R. – *Intermediaries in Cloud Computing: A new Paradigm*, presented at INFORMS meeting, Dallas, 1997.
2. Amies, A., Sluiman, H., Tong, Q., Liu, G. – Infrastructure as a Service. Cloud Concepts. Developing and Hosting Applications in the Cloud*, IBM Press*, July 2013.
3. Rajkumar, B., Broberg, J., Goscinsky, A. – Cloud Computing. Principles and Paradigms, *IBM Press*, March 2011, p.121-154, 251-275.
4. Sotomayor, B., Montero, R.B., Llorente, I.M. – Virtual Infrastructure Management in Private and Hybrid Clouds*, IEEE Internet Computing*, Sept/Oct. 2009.
5. Mell,P.,Grance,T. – *The NIST Definition of Cloud Computing,* National Institute of Standards and Technology, Technical Report, Version 15, USA, 2009.

Aplicație PaaS cloud computing

Rezumat

În prima parte a lucrării au fost prezentate noțiuni generale referitoare la conceptul de cloud computing, o clasificare a modelelor care realizează implementarea acestuia, precum şi cele mai importante riscuri de securitate cu care se confruntă. Aplicația PaaS cloud computing construieşte un nor privat pe baza tehnologiilor VPN şi FTP, detaliind trăsăturile specifice ale sistemului şi modalitățile de rezolvare a cerințelor de securitate asociate accesării serverelor şi gestiunii datelor.