University of Piraeus

Department of Digital Systems

Postgraduate Programme «Techno-Economic Management & Digital Systems Security»

"Security and Privacy in Billing Services in Cloud Computing"

Master Thesis

Name: Eleni - Laskarina Makri (mte0915)

Supervisor: Konstantinos Lambrinoudakis, Assistant Professor

Piraeus, 8-12-2011

Acknowledgements

I am heartily thankful to my supervisor, Konstantinos Lambrinoudakis, Assistant Professor, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

I would also like to offer my regards and blessings to all of those who supported me in any respect during the completion of the project.

Eleni-Laskarina Makri

Table of Contents

Abstract

The purpose of this master thesis is to define cloud computing and to introduce its basic principles.

Firstly, the history of cloud computing will be briefly discussed, starting from the past and ending up to the current and future situation. Furthermore, the most important characteristics of cloud computing, such as security, privacy and cost, will be analyzed. Moreover the three service and three deployment models of cloud computing will be defined and analyzed with examples. Finally, the advantages and disadvantages of cloud computing will be evaluated so as to help understand why the structure of cloud computing is worth using.

When referring to cloud computing, the first thing that comes to mind is the matter of security. So, in the second part of my master thesis, the security in the service models Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) will be analyzed. Security benefits as well as security risks will be thoroughly examined.

Cloud computing is a new internet-based technology enabling users to access resources via the Internet. To do so, Internet users have to pay for the services they receive depending on the use. There are two pricing models. The first pricing model is based on pay per use while the second on subscription. As a result, many billing factors play a really important role in the way a user is charged.

Charging customers for a cloud service, automatically makes the billing system vulnerable to malicious users, who will possibly take advantage of the vulnerabilities of the service in order to attack and use it for free. Thus, privacy is violated.

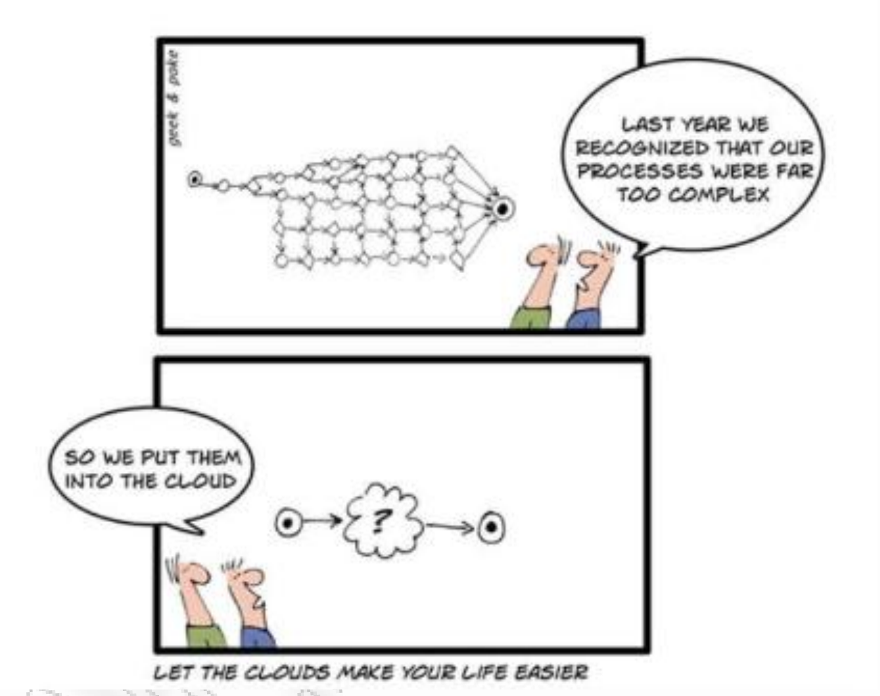
Keywords: security; privacy; cloud computing; billing services.

CHAPTER 1

Introduction

1.1 Defining Cloud Computing

Cloud Computing is a new technology based on the internet… so new that there has not been an official definition yet. In order for someone to understand what really cloud computing is a great deal of search is required. Many people and national organizations try to define with clarity what cloud computing represents, some with success and others not. As a result, there is a great number of definitions in many papers and book bibliography that explain the meaning of cloud computing, its special characteristics, its architecture and its provided services.

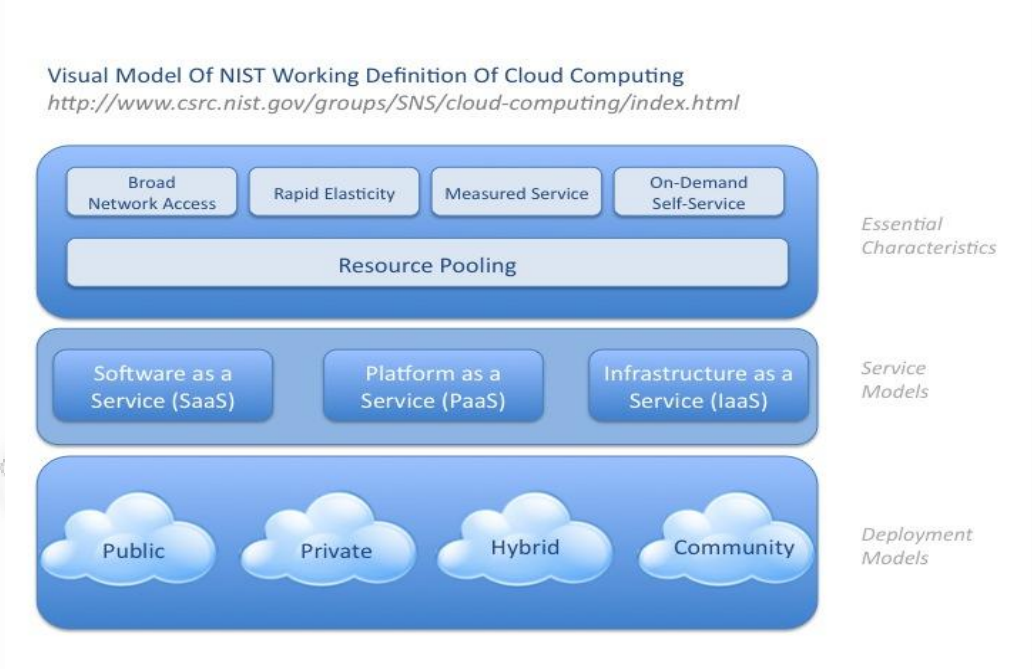

geek & poke
LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX
SO WE PUT THEM INTO THE CLOUD
?
LET THE CLOUDS MAKE YOUR LIFE EASIER

Source: ADVA Optical Networking [2]

Google was first to introduce and promote the idea of cloud computing. Kevin Marks supported that the idea of cloud computing was first introduced from the early days of the Internet, where the network was depicted as a cloud. We did not care about where the messages went—they came in one side and out the other, and we did not have to worry about the network because the cloud hid it from us. It was a 'cloud' around network buckets [1]. By this definition, Marks tried to explain the origin of cloud computing as the trend to draw the internet as a cloud.

Inside the cloud the procedures that occur are of little importance compared to the input and output in and out of the cloud respectively. The result is of greatest significance to the users.

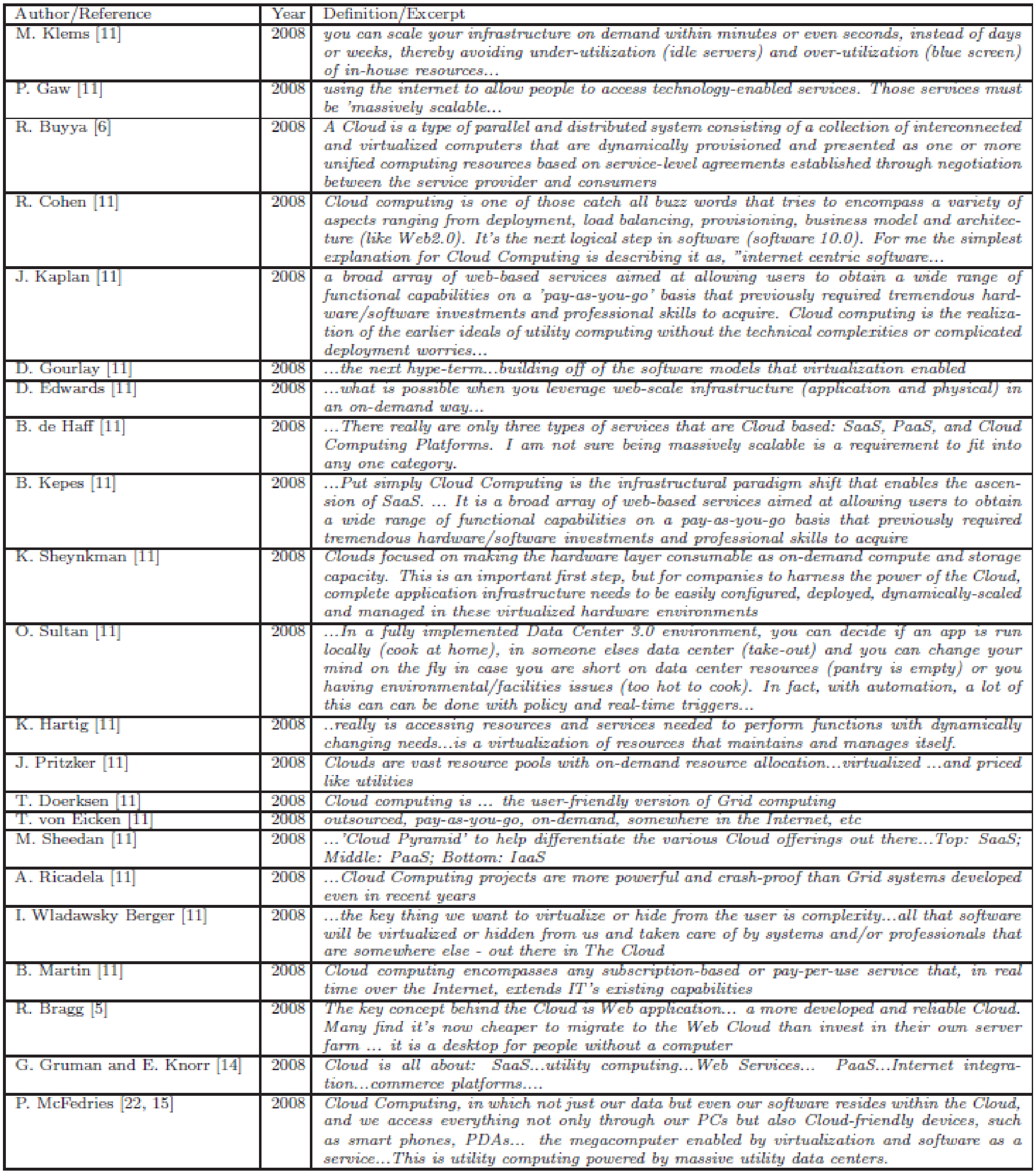
The “National Institute of Standards and Technology” (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [3]. In other words, according to the NIST, cloud computing is a technology that uses the internet in order to share the computing resources and software whenever the users wish. The service providers “make the whole management job”, “relieving” the users of the responsibility of managing their own servers, networks, applications, services, etc. NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models, all summarized below.


Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

The “European Network and Information Security Agency” (ENISA) defines that cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies [5]. According to ENISA, the idea of cloud computing is supported in virtualization and distributed technologies. That means that cloud computing architectures are scalable and flexible and they can use highly abstracted resources. The resources are shared among users, which use service on demand and pay only for what they use.

According to the “International Business Machines” (IBM), cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned “on demand,” regardless of the user location or device [13]. IBM emphasizes on the flexible and cost-effective services that are provided over the Internet, for the first time. In addition, the resources are provided according to the users’ needs and location.

Cloud computing definitions are listed in the table below by Luis et al in 2008 [14]:



Author/Reference	Year	Definition/Excerpt
M. Klems [11]	2008	*you can scale your infrastructure on demand within minutes or even seconds, instead of days or weeks, thereby avoiding under-utilization (idle servers) and over-utilization (blue screen) of in-house resources...*
P. Gaw [11]	2008	*using the internet to allow people to access technology-enabled services. Those services must be 'massively scalable...*
R. Buyya [6]	2008	*A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers*
R. Cohen [11]	2008	*Cloud computing is one of those catch all buzz words that tries to encompass a variety of aspects ranging from deployment, load balancing, provisioning, business model and architecture (like Web2.0). It's the next logical step in software (software 10.0). For me the simplest explanation for Cloud Computing is describing it as, "internet centric software...*
J. Kaplan [11]	2008	*a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a 'pay-as-you-go' basis that previously required tremendous hardware/software investments and professional skills to acquire. Cloud computing is the realization of the earlier ideals of utility computing without the technical complexities or complicated deployment worries...*
D. Gourlay [11]	2008	*...the next hype-term...building off of the software models that virtualization enabled*
D. Edwards [11]	2008	*...what is possible when you leverage web-scale infrastructure (application and physical) in an on-demand way...*
B. de Haff [11]	2008	*...There really are only three types of services that are Cloud based: SaaS, PaaS, and Cloud Computing Platforms. I am not sure being massively scalable is a requirement to fit into any one category.*
B. Kepes [11]	2008	*...Put simply Cloud Computing is the infrastructural paradigm shift that enables the ascension of SaaS. ... It is a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a pay-as-you-go basis that previously required tremendous hardware/software investments and professional skills to acquire*
K. Sheynkman [11]	2008	*Clouds focused on making the hardware layer consumable as on-demand compute and storage capacity. This is an important first step, but for companies to harness the power of the Cloud, complete application infrastructure needs to be easily configured, deployed, dynamically-scaled and managed in these virtualized hardware environments*
O. Sultan [11]	2008	*...In a fully implemented Data Center 3.0 environment, you can decide if an app is run locally (cook at home), in someone elses data center (take-out) and you can change your mind on the fly in case you are short on data center resources (pantry is empty) or you having environmental/facilities issues (too hot to cook). In fact, with automation, a lot of this can can be done with policy and real-time triggers...*
K. Hartig [11]	2008	*..really is accessing resources and services needed to perform functions with dynamically changing needs...is a virtualization of resources that maintains and manages itself.*
J. Pritzker [11]	2008	*Clouds are vast resource pools with on-demand resource allocation...virtualized ...and priced like utilities*
T. Doerksen [11]	2008	*Cloud computing is ... the user-friendly version of Grid computing*
T. von Eicken [11]	2008	*outsourced, pay-as-you-go, on-demand, somewhere in the Internet, etc*
M. Sheedan [11]	2008	*...'Cloud Pyramid' to help differentiate the various Cloud offerings out there...Top: SaaS; Middle: PaaS; Bottom: IaaS*
A. Ricadela [11]	2008	*...Cloud Computing projects are more powerful and crash-proof than Grid systems developed even in recent years*
I. Wladawsky Berger [11]	2008	*...the key thing we want to virtualize or hide from the user is complexity...all that software will be virtualized or hidden from us and taken care of by systems and/or professionals that are somewhere else - out there in The Cloud*
B. Martin [11]	2008	*Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities*
R. Bragg [5]	2008	*The key concept behind the Cloud is Web application... a more developed and reliable Cloud. Many find it's now cheaper to migrate to the Web Cloud than invest in their own server farm ... it is a desktop for people without a computer*
G. Gruman and E. Knorr [14]	2008	*Cloud is all about: SaaS...utility computing...Web Services... PaaS...Internet integration...commerce platforms....*
P. McFedries [22, 15]	2008	*Cloud Computing, in which not just our data but even our software resides within the Cloud, and we access everything not only through our PCs but also Cloud-friendly devices, such as smart phones, PDAs... the megacomputer enabled by virtualization and software as a service...This is utility computing powered by massive utility data centers.*

Less sophisticated, yet clear definitions are provided by Wikipedia and Whatis.com respectively.

According to the Wikipedia, cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, as with the electricity grid [15]. That means, that the users need to have an Internet connection to use cloud computing. The services are provided to users only when the resources are requested. For example, when they ask for a service, it is provided immediately and only to users that need it.

According to Whatis.com, cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [16, 27]. In other words, Whatis.com defines cloud computing more thoroughly compared to the Wikipedia definition, using the three hosted services IaaS, PaaS and SaaS that will be later analyzed.

Taking all the above definitions into consideration, it can be clearly understood that cloud computing is a new technology which offers users a great deal of conveniences, all via the internet. They can use a lot of remote resources and share them with other users at the same time. They are not responsible for the management of services, because it is the service providers’ job. Users have the ability to access their data and services through the internet and edit them as they wish. In other words, cloud computing defines a new architecture different from the one existing so far. Many data centers are there to provide services to users. One really important characteristic is that the users have to pay only for the services they use.

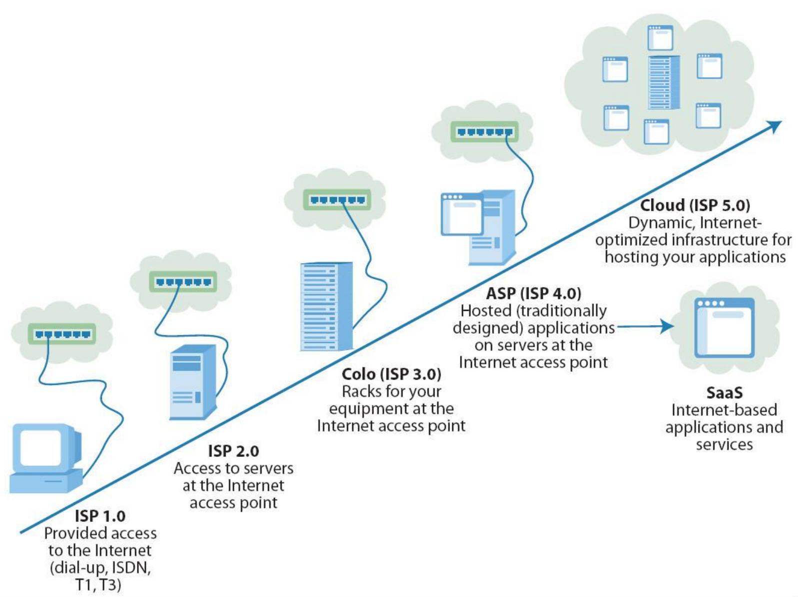
1.2 Cloud Computing Evolution

There has been a lot of discussion around cloud computing over the last years. There are plenty of researches that show that cloud computing is an upcoming new technology and more and more companies turn to this direction. Yet, there are other researches that consider cloud computing as a “bubble” that will soon blow off.

The Forrester Reasearch [17, 18] supports the notion that cloud computing has not been able to meet the needs of large companies yet and it is only temporary. According to Staten, the services are offered through hosting providers like Amazon Web Services.

"Cloud computing looks very much like the instantiation of many vendors' visions of the data center of the future; it's an abstracted, fabric-based infrastructure that enables dynamic movement, growth, and protection of services that is billed like a utility. It also has all the earmarks of a disruptive innovation: It is enterprise technology packaged to best fit the needs of small businesses and start-ups--not the enterprise," Staten supports.

Figure 3 Cloud Computing: The Latest Evolution Of Hosting


Cloud (ISP 5.0)
Dynamic, Internet-optimized infrastructure for hosting your applications
ASP (ISP 4.0)
Hosted (traditionally designed) applications on servers at the Internet access point
Colo (ISP 3.0)
Racks for your equipment at the Internet access point
SaaS
Internet-based applications and services
ISP 2.0
Access to servers at the Internet access point
ISP 1.0
Provided access to the Internet (dial-up, ISDN, T1, T3)

44229

Source: Forrester Research, Inc.

1.3 Cloud Computing Characteristics

Cloud computing has a great number of characteristics that make it a unique technology. According the US National Institute of Standards and Technology (NIST) these essential characteristics are of great importance and are analyzed below [3, 19].

- **On Demand Self-Service:** The computing resources such as storage, memory and network bandwidth, software, process, etc can be provided on an independent and automatical basis without human intervention being required. That means that the service providers “do the whole job” depending on the needs arising per case.
- **Broad Network Access:** Access to computing resources is conducted over the network through standard mechanisms with different client platforms such as personal computers, mobile phones and PDAs.
- **Resource Pooling:** The cloud resources of service providers can be pooled to serve all different clients using a multi-tenant model, with different physical and virtual resources in a dynamic way. The assigning or reassigning of these resources depends on the consumer needs that are often changing. The customer has no idea as to where the exact location of the provided resources is. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid Elasticity:** The cloud recourses can be rapidly and elastically scaled in and scaled out (i.e., provisioned and released) at any given time. To the consumer, the resources available for rent often seem to be unlimited and can be purchased on demand, which practically means at any quantity or time.
- **Measured Service:** This characteristic is often referred to as “pay per use”. The customer’s use of cloud resources can be transparently monitored, controlled, and reported. In other words, the use of recourses is charged according to a billing system which measures the storage, the network bandwidth as well as a number of other resources. The charge depends on the number of active user accounts per month.

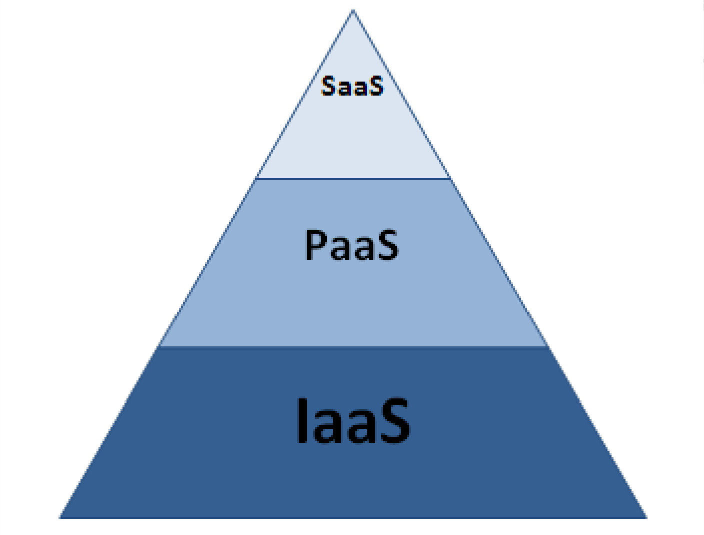
In conjunction with these characteristics that are defined by NIST, when searching the internet one is likely to find a lot of other characteristics related to cloud computing [15, 20, 21, 22, 23]. Some of these are listed below:

- flexibility
- scalability
- automation
- independency
- reliability
- homogeneity
- interoperability among several clouds
- use of virtualization technology
- pay-as-you-go model
- massive scale
- resilient computing
- low cost software
- geographic distribution
- service orientation
- advanced security technologies
- IT service-centric approach
- infrastructure that provided by third party
- standardized interfaces
- immature technology

All the above characteristics make cloud computing really useful and attractive to many customers, as well as companies to use and promote.

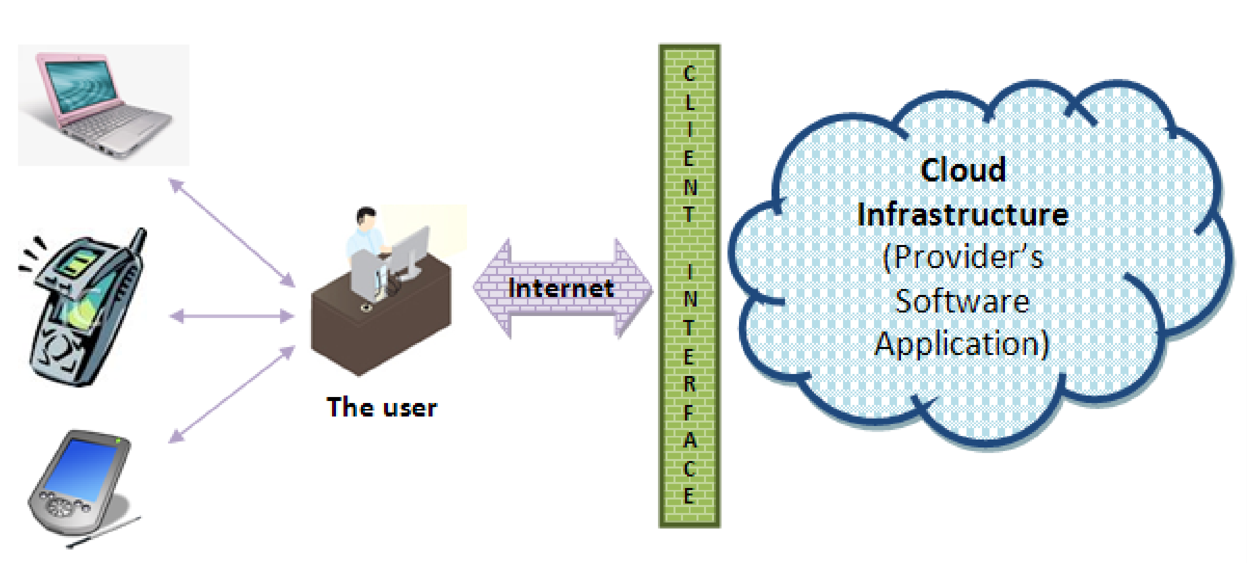
1.4 Cloud Computing Service Models

Cloud computing is described as a model whose services are hosted on the Internet for computational purposes. Cloud computing refers to three (or four according to Wlter F. Witt [4]) different types of computing services, Software-as-a-Service (SaaS), Platforms-as-a-Service (PaaS), Infrstructure-as-a-Service (IaaS) and Communications-as-a-Service (CaaS). The three of them are shown below [4]:



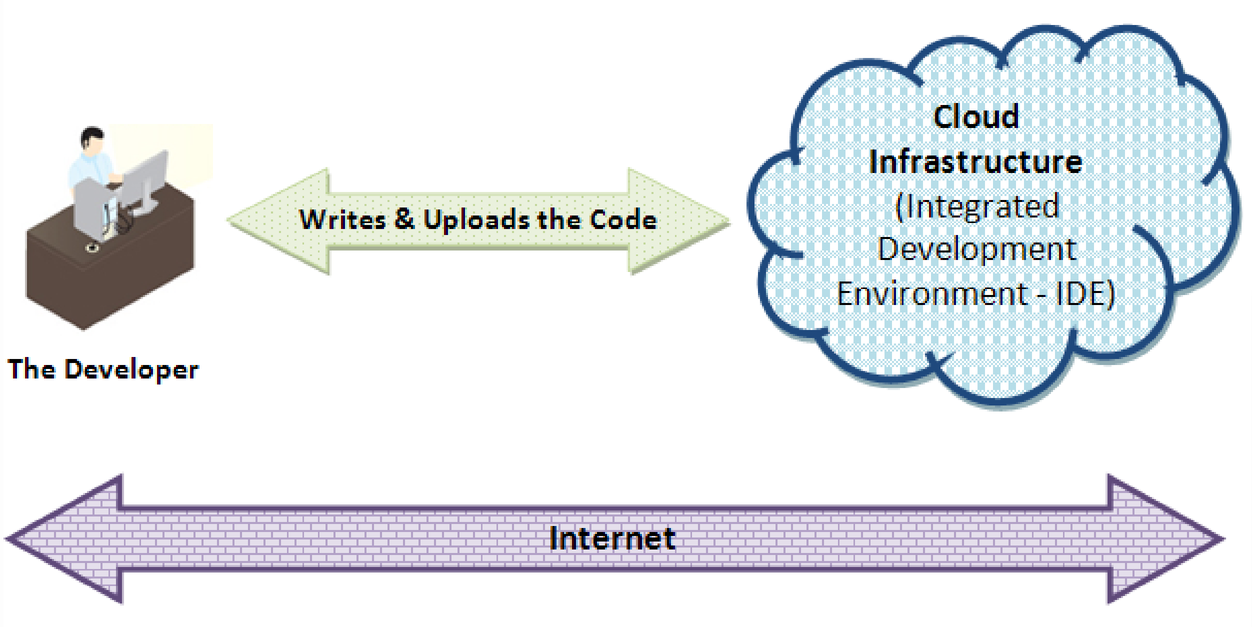
Among the three service models there are lots of differences [24]. The SaaS service model is at the top, offering applications on-demand. The PaaS service model follows in the middle including the operating system and application services. Finally, the IaaS service model with its hardware provided via a virtualized interface is shown in the lowest level. In the sections below the above service models will be analyzed.

1.4.1 Software-as-a-Service (SaaS)



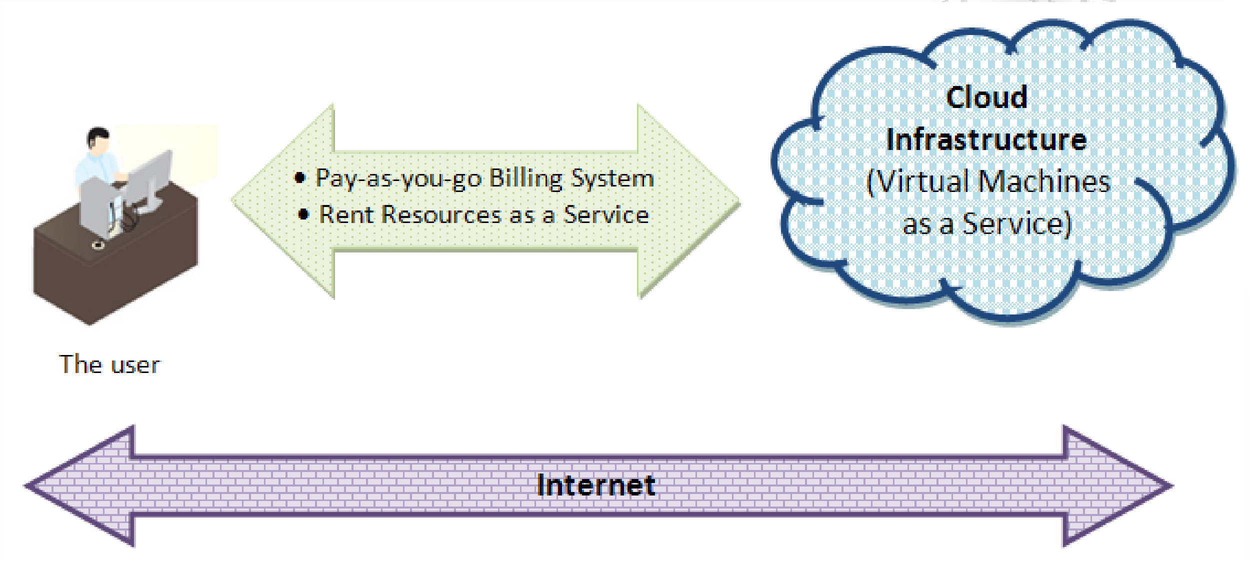
Software-as-a-Service (SaaS) is the service most clearly understood by common users. The application runs in an unknown server and people use it, via an internet connection, without knowing further details. This service model offers cloud users access to the provider's software application running on a server inside the cloud infrastructure [25]. That means that the cloud users can access different applications from various devices (e.g. net books, mobile phones, laptops, etc) through a client interface such as a Web browser. The cloud provider manages the applications, operating systems and underlying infrastructure, while the cloud user can only control some user-specific features. Examples of this service model are Google Docs, Salesforce CRM, SAP Business by Design, Facebook, Wikipedia, Gmail.

1.4.2 Platforms-as-a-Service (PaaS)


The Developer
Writes & Uploads the Code
Cloud Infrastructure (Integrated Development Environment - IDE)
Internet

Platforms-as-a-Service (PaaS), a service that practically facilitates programmers, is an integrated development environment (IDE) where development platforms are hosted on the web and are accessed by a browser. "Developers write their application to a more or less open specification and then upload their code into the cloud where the app is run magically somewhere, typically being able to scale up automatically as usage for the app grows." [4] The cloud developers focus on building the application without caring about the complex platform and they use programming languages and tools supported by cloud providers in order to develop their applications [25]. "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 application hosting environment configurations." [3] The cloud developers do not need to worry about environment configuration, as this is the cloud provider's job. They only develop their application depending on what the provider offers. Examples of this service model are Mosso, Force.com, Google App Engine, Windows Azure (Microsoft).

1.4.3 Infrastructure-as-a-Service (IaaS)



Pay-as-you-go Billing System
Rent Resources as a Service
Cloud Infrastructure (Virtual Machines as a Service)
The user
Internet

Infrastructure-as-a-Service (IaaS) is pay-as-you-go model and companies are only billed for the amount of service they have access to. "This service basically delivers virtual machine images as a service and the machine can contain whatever the developers want. Instead of purchasing servers, software, data center resources, network equipment, and the expertise to operate them, customers can buy these resources as an outsourced service delivered through the network cloud." [25] In other words, cloud users can actually rent resources as a service and companies are not obliged to spend money on buying servers or other types of infrastructure. Examples of this service model are IBM Blue house, VMWare, Amazon EC2, Sun Parascale, SQL Azure, Zimory, Elastichosts.

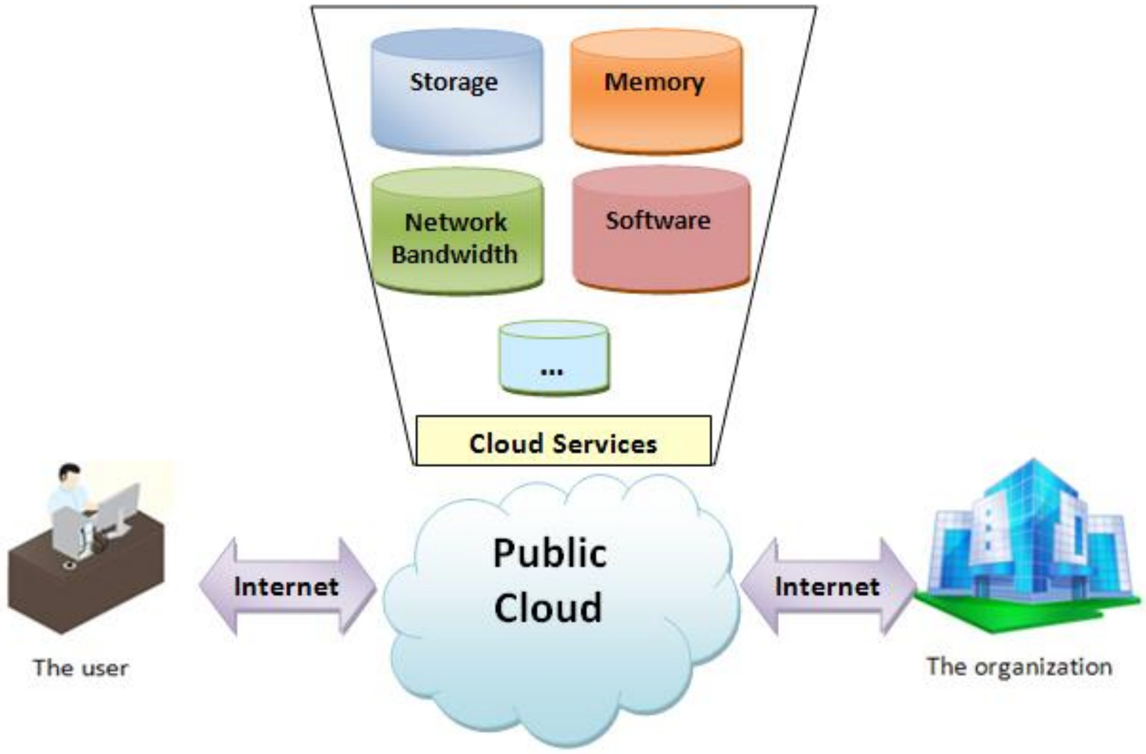
1.4.4 Communication-as-a-Service (CaaS)

According to Walter F. Witt [4] there is another service model called Communication-as-a-service (CaaS). It is a service similar to SaaS refering to communication services such as Voice over Internet Protocol (VoIP), blogs, instant messaging and video conferencing. Several of the SaaS and CaaS services are referred to as Web 2.0. Services.

1.5 Cloud Computing Deployment Models

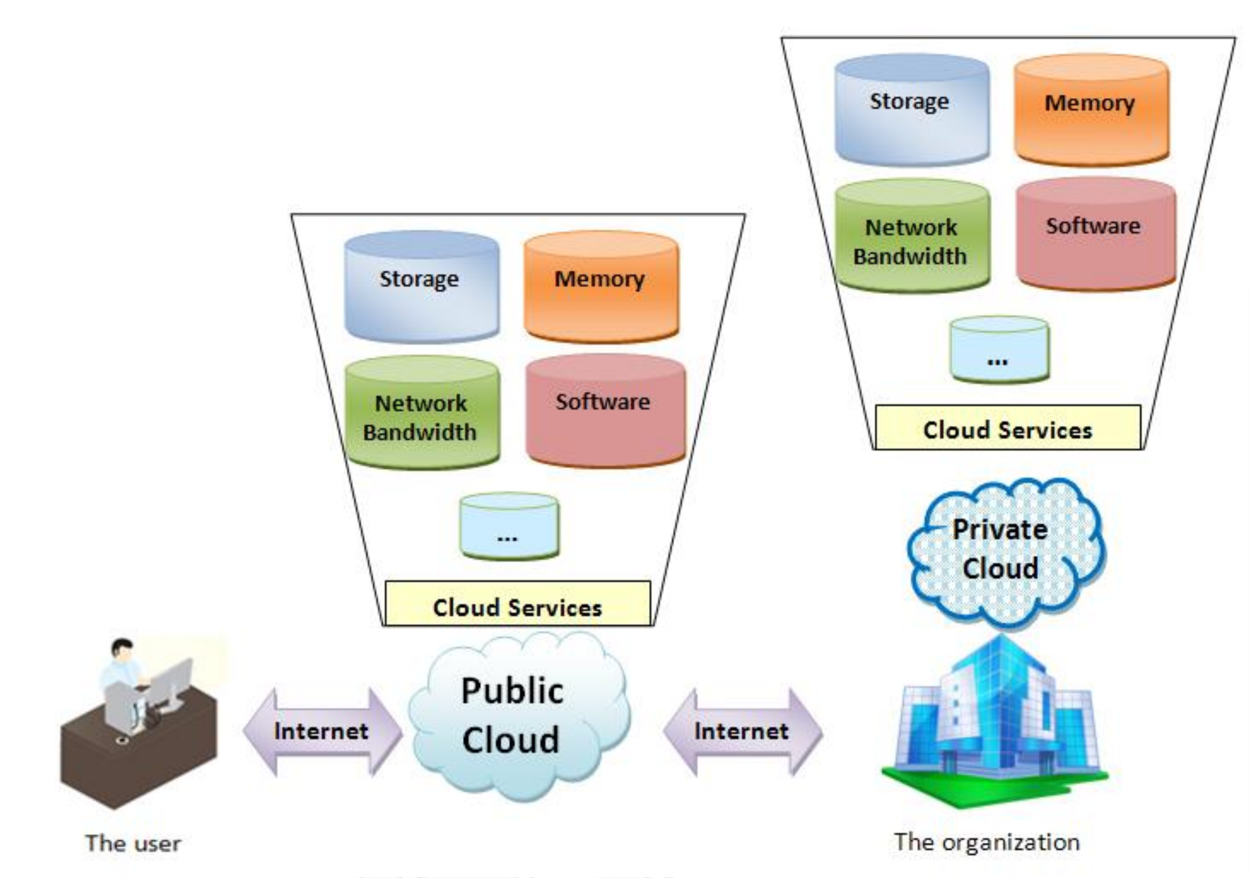
According to the US National Institute of Standards and Technology (NIST) there are four deployment models: the public cloud (sold to the public, mega-scale infrastructure), the private cloud (enterprise owned or leased), the hybrid cloud (composition of two or more clouds), and finally the community cloud (shared infrastructure for specific community) [3].

1.5.1 Public Cloud Model



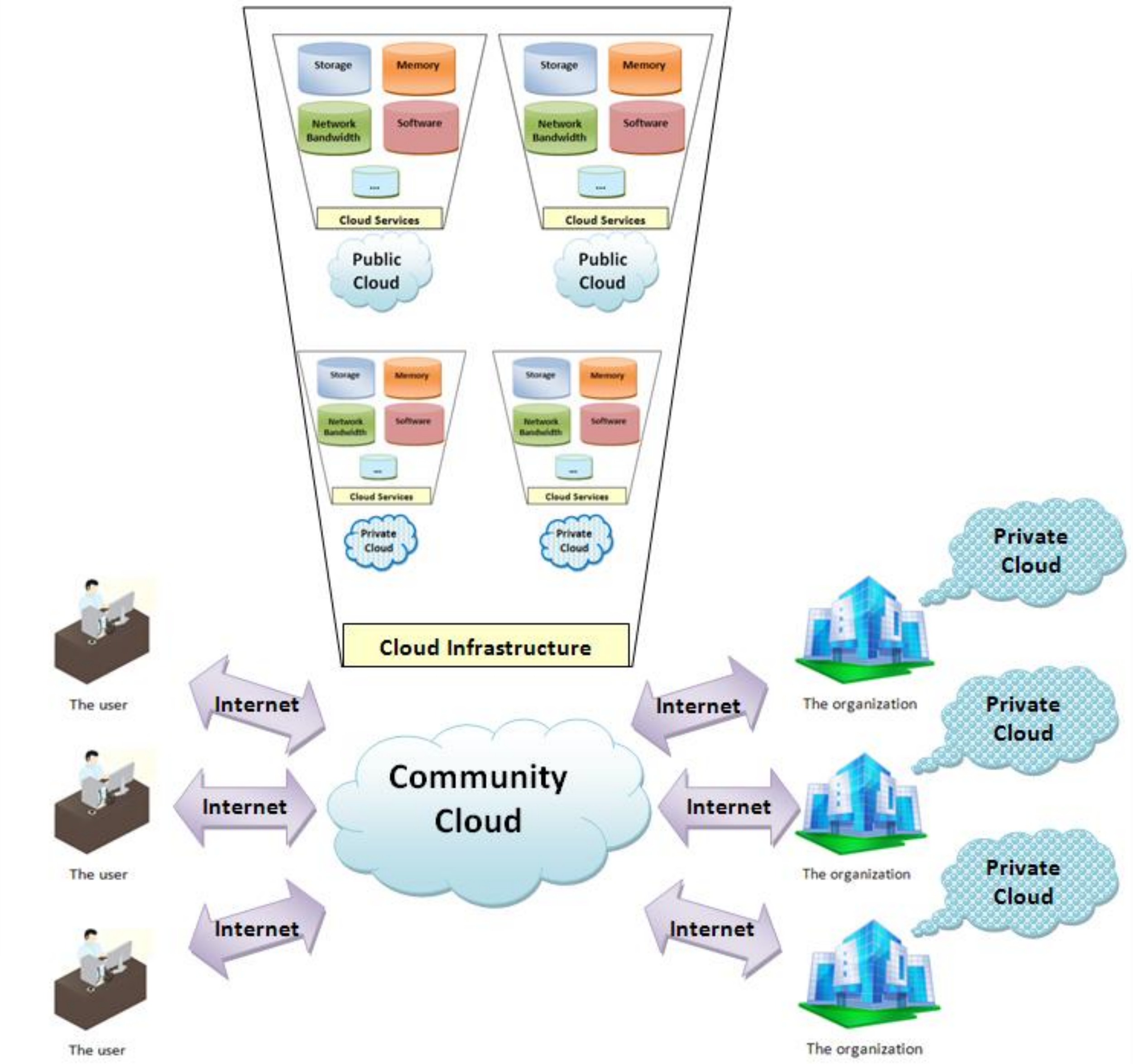
In a public cloud (known as external cloud or multi-tenant cloud), the cloud infrastructure is a mega-scale infrastructure, which is owned by a huge organization. This enterprise is able to sell all the cloud computing services to the general public or to a large industry group. The cloud services are shared through a pay-as-you-go model of payment. That means that the cloud users do not work for the organization which manages the cloud infrastructure, yet they are able to use the cloud services, as they are not “tied” by a contract. According to Walter F. Witt [4], public clouds are third-party providers of on-demand pay-as-you-go cloud services over the internet outside the company‘s firewall. Examples of public clouds are the Amazon Web Services EC2, the Google Apps and the Microsoft Azure.

1.5.2 Private Cloud Model



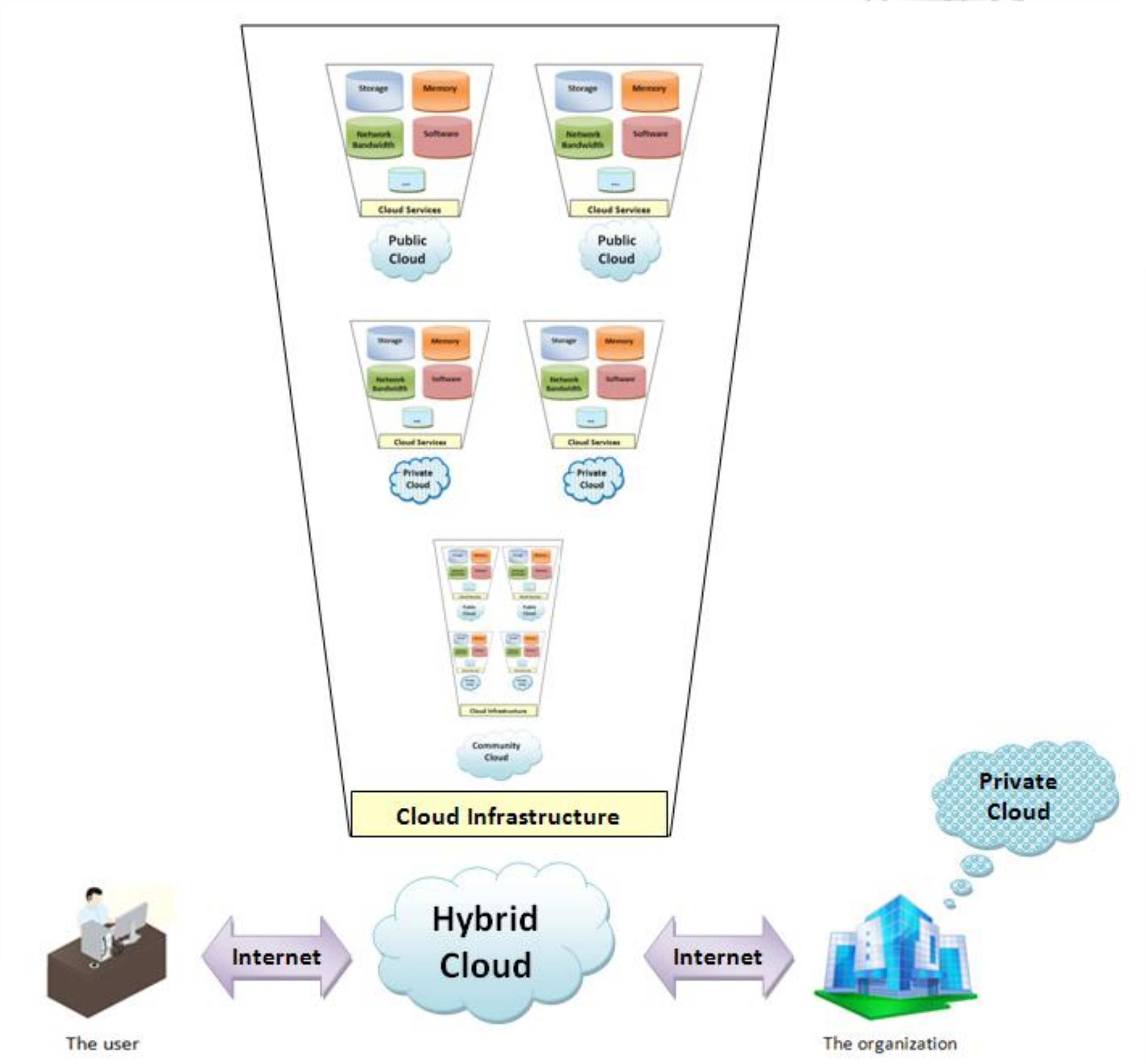
The private cloud (known as internal cloud) is a deployment model which allows an enterprise to own or lease the cloud services existing in the cloud. That means that the cloud infrastructure is owned or rented only by one organization and is run only for the specific organization without the resources being shared by other organizations. The cloud infrastructure may be managed by the organization or a third party, and may be located on-premise (in the organization's datacenter) or off-premise [26]. The private cloud users work for the organization and are able to use the cloud services. According to Walter F. Witt [4], the private clouds emulate cloud computing on private networks behind the company's firewall. The drawback of this type of cloud is that the company still needs to build, manage and buy the infrastructure. An example of private cloud is eBay.

1.5.3 Community Cloud Model



According to the NIST, another deployment model is the community cloud. This is a shared infrastructure for a specific community. In other words, the cloud infrastructure is shared by multiple organizations and supports a specific community with common interests such as security requirements, policy and compliance considerations. This cloud model may be managed by the organization or by a third party and may be located on-premises or off-premises. Community users are usually part of the community.

1.5.4 Hybrid Cloud Model



The hybrid cloud is the forth deployment model and it is a composition of two or more clouds such as public, private or community clouds. According to Walter F. Witt [4], the hybrid cloud combines aspects of both public and private clouds from multiple internal and/or external providers. The hybrid cloud seems to be the most common cloud model.

1.5.5 Comparing Deployment Models

The deployment models are made available to users to offer them cloud services in a pay-as-you-go model. There are some characteristics that distinguish them from each other [27].

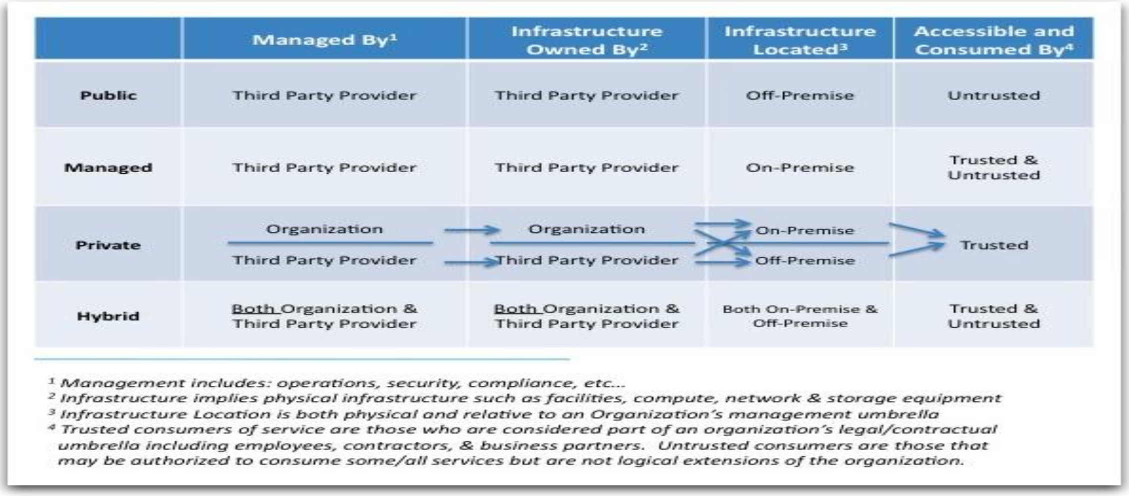
Starting with the public clouds, the resources are dynamically provided on a self-service basis over the Internet, via web applications, from an off-site third-party provider [15]. Some essential characteristics are that they include an homogeneous infrastructure, common policies, shared resources and multi-tenant, leased or rented infrastructure, operational expenditure cost model and economies of scale. What is really important, is that public clouds can host individual services or collections of services, allowing the deployment of service compositions or even entire service inventories.

On the other hand, the private clouds include an heterogeneous infrastructure, customized and tailored policies, dedicated resources, in-house infrastructure (capital expenditure cost model) and end-to-end control.

As far as the community clouds are concerned, the main characteristic is that they offer a higher level of privacy, security and policy compliance. In addition, they can be economically attractive as the resources (storage, workstations) utilized and shared in the community are already exploited and have reached their return of investment [15].

Finally, the hybrid cloud is a model that combines all deployment models concentrating all the above characteristics.

Yet, according to Bardin [26], there are deployment model characteristics that do not belong to some of the above four categorizations. It is worth having a look at the table below.



	Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Managed	Third Party Provider	Third Party Provider	On-Premise	Trusted & Untrusted
Private	Organization Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: operations, security, compliance, etc...*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

1.6 Cloud Platforms

1.6.1 Amazon Elastic Compute Cloud (EC2)

The Amazon Elastic Compute Cloud (Amazon EC2) is a central part of Amazon Web Services (AWS), the Amazon.com's cloud computing platform. It provides resizable compute capacity in the cloud and it allows users to rent virtual computers to run their applications [28]. Each user can create an image which is loaded when he starts the service. EC2 offers users a web interface in order to launch instances with a lot of operating systems, load them with their custom application environment, manage their network's access permissions, and run their image using as many or few systems as they desire [29]. Users have the ability to pay only for what they use. The Amazon's EC2 provides users the IaaS service model.

1.6.2 IBM Computing on Demand or Blue Cloud

The Blue Cloud is a highly enterprise-focused cloud computing related to and built with the same technology sold to enterprises. [30]. It allows corporate data centers to operate more like the Internet by enabling computing across a distributed, globally accessible fabric of resources, rather than on local machines or remote server farms. Blue Cloud, built on IBM's expertise in leading massive-scale computing initiatives, is based on open standards and open source software supported by IBM software, systems technology and services [31]. IBM provides users the SaaS, PaaS and IaaS service models [32].

1.6.3 Windows Azure Platform

The Windows Azure and SQL Azure enable users to build, host and scale applications in Microsoft datacenters. They require no up-front expenses, no long term commitment, and enable users to pay only for the resources they use [33]. Microsoft Windows Azure platform is a group of cloud technologies, each providing some services to application developers. The Windows Azure platform is consisted of four components: Windows Azure (a Windows environment for running applications and storing data on computers in Microsoft data centers), SQL Azure (relational data services in the cloud based on SQL Server), Windows Azure AppFabric (cloud-based infrastructure services for applications running in the cloud or on premises) and Windows Azure Marketplace (an online service for purchasing cloud-based data and applications. [34]. The Microsoft Azure provides users the PaaS and IaaS service models.

1.6.4 Google App Engine

The Google App Engine is a cloud computing platform that allows users to run their web applications on the Google's infrastructure. The applications are really easy to built, to maintain and to scale when the traffic and capacity increase. In addition, the users just upload their application without worrying about the server [35]. The Google App Engine provides users the PaaS service model.

1.6.5 Salesforce.com, Force.com

The Force.com is a cloud computing platform as a service system provided by Salesforce.com. The developers use it to build multi tenant applications that are hosted on their servers as a service [36]. The platform allows external developers to create add-on applications that integrate into the main salesforce.com application and are hosted on salesforce.com infrastructure [37]. The Salesforce.com provides users the SaaS and PaaS service models.

Platforms	SaaS	IaaS	PaaS
Amazon Elastic Compute Cloud (EC2)		✓	
IBM Blue Cloud	✓	✓	✓
Windows Azure Platform		✓	✓
Google App Engine			✓
Salesforce.com	✓		✓

1.7 Advantages and Disadvantages of Cloud Computing

Cloud computing is a new technology based on the internet. Because of the fact that it is yet under development, many issues arise. Some people agree that cloud computing can offer a lot to the “web” society, supporting its advantages, such as the reduced cost, the scaling and elasticity, the portability and the productivity as well as the collaboration. On the other hand, there are those who support that cloud computing has nothing exciting to offer as on the one hand there is a lack of appropriate infrastructures and on the other hand there are several security issues that have not yet been solved. Some of the disadvantages are the data migration, the potential data loss, the stability and reliability, the licensing as well as a number of legal issues. In this section we will analyze some of positive and negative aspects of cloud computing [4].

1.7.1 Advantages

- **Reduced Cost**

  The first and really significant advantage of cloud computing is its low cost. That means that there is no need to maintain the physical hardware related to the infrastructure. The cloud services are running “somewhere” in the cloud without the cloud users worrying about the hardware requirements. Also, the low cost software is important, because users do not need to waste their time installing the software and its updates.

- **Scaling and Elasticity**

  The cloud services offered to users are charged in two ways. The users either have to pay a monthly fee for the services or pay only for what they use. In contrast to the first, the second way of billing is actually better, especially in the case where for some reason the user does not use the cloud service on a monthly basis. Scalability ensures that the cloud platform can handle an increased load of users working on a cloud application.

This scaling capacity up and down for a cloud service is commonly called elasticity. In other words, the cloud data centers are able to be resized or downsized in order to serve the needs of end-users in the best way.

- **Portability**

  Another major advantage is that the end-user is not limited to accessing these applications from a traditional computer and can use almost any device with a web connection. Most of the computing and storage is done in the cloud so this diminishes the need for high-powered computing devices which makes many of these services accessible from most any device. That means that all the end-users have the ability to connect and access the cloud services remotely from any place, even home. Moreover, the remote access helps the organizations, because the employees can work from home without commuting on a daily basis. As a result, portability is really useful, provided that there is an internet connection.

- **Productivity and Collaboration**

  Last but not least, collaboration and productivity of multiple cloud users are advantages worth mentioning. The cloud computing permits plenty of cloud users to collaborate from distance and share documents and projects. Because of the fact that the documents are not located at a traditional computer, cloud users can use them at work, through the process of downloading. Collaboration results to productivity, because when the users in a business collaborate on a project they are more effective when working all together.

In a different approach by Aymerich, Fenu and Surcis [38] the advantages are divided into four categories; technical advantages, advantages for users, architectural advantages and advantages for companies.

The first technical advantage is that there is no need for additional hardware infrastructure as resources can be virtualized. Also, the ability to use the processing power of the cloud to do things that traditional productivity applications cannot do (such as search over GBs of e-mail online) is offered. A third technical advantage is that the use of servers and traditional computers are easy to be maintained and recovered, therefore the scalability is increased.

The cloud user can benefit, too. That means that the cloud users can use the cloud applications from every computer, wherever they are located provided that there is an internet connection. Moreover, there is no need to worry about issues like storage capacity or compatibility.

As far as the architectural advantages are concerned, cloud computing launches innovation. That means that innovators can find new resources to develop, test and make their innovations available to the user community. A second benefit is portability, which enables organizations to use their IT hardware and software investments more efficiently. In addition, cloud computing infrastructure can be located in areas with lower costs of space and electricity.

Finally, there are two really important advantages when an organization uses a cloud. The first is that the organizations, especially not the large ones, become more productive as they use the IT tools inside the cloud without wasting their money on technical equipment. The second is that more and more enterprises use the cloud because of the cost savings, remote access, ease of availability and real-time collaboration capabilities.

1.7.2 Disadvantages

- **Data Migration**

  Organizations possess huge amounts of data and despite the fact that they are easy to transfer in the cloud storage, there may be some serious limits in the capacity of the network connections to the cloud, which can create challenges for enterprises with multiple terabytes of data to move back and forth. So, the data transfer is still done manually.

- **Potential Data Loss**

  One of the most important drawbacks of cloud computing is the danger of a potential data loss. Organizations manage a great number of data and in no way do they wish to lose them as that may lead to chaos. As a result, the idea of losing data may cause companies to keep systems with sensitive customer data which are strategic to the business in a private cloud behind a firewall under their control.

- **Security and Legal Issues**

  As cloud computing is a new internet technology, a lot of security as well as legal issues have to be considered. For instance, there are challenges related to the protection of the data belonging to different companies which share the same disk within the cloud. In such cases, access must be secured. Another point worth mentioning is that cloud users are not aware of the fact that since they use the cloud services, thus accepting the terms of the service, they automatically allow the provider to manage their personal information as he wishes.

- **Stability and Reliability**

  Stability and reliability are both critical issues. That is because the data center cannot always provide them. For example, there will obviously be a problem in the case where a data center goes bankrupt and the creditors come in and take the equipment without caring about the users’ data. As far as reliability is concerned, nobody can warranty that a web service that runs on a data center will always be available as a number of misfortunes (e.g. a distributed denial-of-service attack - DDoS attack) can occur.

- **Licensing**

  In order to use software on single computers and servers, organizations sell licenses. Yet, in the imminent era of cloud computing, this has to be different. That means that vendors (e.g. Oracle, Siebel, SAP) will have to change their licensing to support three weeks running on three servers, then one week per month expanding to ten and only paying for the capacity used, something which is really difficult to be achieved.

CHAPTER 2

Security & Privacy in Cloud Computing

2.1 Security Requirements in Cloud Computing

When using cloud computing services, there are specific issues concerning security. Before selecting a cloud vendor, Gartner proposes some really important security issues, customers should focus on [6]:

- **Privileged User Access**

  Data access has to be controlled systematically and in depth. Users have to know who manages their data and what kind of privileges he has over them.

- **Regulatory Compliance**

  The users, who are the ones to decide on the management of their data by the service providers, are responsible for the security and integrity of their data. So, they are the ones who actually decide if they trust their data to cloud providers who do not follow the regulations.

- **Data Location**

  When the users “locate” their data within a cloud, they cannot possibly know where their data is hosted. To ensure safety, Gartner suggests that users ask their cloud providers if they are in compliance with the local privacy requirements.

- **Data Segregation**

  In a cloud environment, a lot of data from different users is gathered, therefore its protection via encryption cannot be ensured. According to Gartner, cloud providers should give evidence that encryption schemes are controlled by specialists for their correct operation.

- **Recovery**

  A cloud provider should be able to recover the data when a disaster occurs. Therefore, the users should be informed by the cloud provider about the procedures required for a complete recovery.

- **Investigative Support**

  Cloud services are really difficult to be investigated, because data from different customers can be located in the same data center. Cloud providers should be able to support specific forms of investigation.

- **Long-term Viability**

  Users have to make sure that in case of a potential change in the cloud providers management (merger, bankruptcy, etc) their data will be safe, as well as usable in the future.

According to Michael Gregg, the cloud provider is obliged to offer a better level of security than a company on its own, so that the users will move their sensitive data inside the cloud. He mentions ten top security concerns for cloud computing, which are analyzed below [39].

- **Data Location**

  The data in a cloud may be physically located in a number of locations. So, cloud providers should provide users the appropriate level of security, as different countries have different requirements and controls regarding access.

- **Data Access**

  Cloud computing users should be really cautious about people who have access to their data. The kind of rights and privileges people with access are entitled to, should always be considered.

- **Regulatory Requirements**

  There are plenty of legal issues within a cloud environment. A user should know what exactly his regulatory requirements are. Cloud providers have to ensure that they are in accordance with the requirements among different countries, providing a number of security certifications.

- **Audit**

  Another important issue is the user's right to audit. In each case, the cloud provider should deal with the terms of audit.

- **Training Provider Employees**

  Cloud providers have to train their employees on matters of security, because a lot of issues occur due to human errors. To avoid such incidents, the employee should obtain security awareness and training through training programs.

- **Data Classification System**

  The cloud provider has to keep the data in a good level of classification, so as other users cannot have access to sensitive information. Furthermore, encryption should be ensured when the data is in transit or at rest. In this way, users will trust the cloud providers and they will be sure their data is safe.

- **Service Level Agreement (SLA) Terms**

  The users should know what the SLA terms are, as they determine the level of services provided to the users.

- **Long-term Viability**

  The long-term viability of the cloud provider is another important issue. It is essential that the user know what happens with his data, if the cloud provider goes out of business. The provider should be able to return the data to his owner in the original format. This is really important to the user, as he wishes for the integrity of his data, therefore it is really difficult to trust the management of sensitive information to a third party.

- **Security Breach**

  A cloud environment is really attractive to attackers. That means that many attacks are likely to take place causing serious damages. The cloud provider is obliged to inform the user in case of security breach and the user has to be aware of the fact that his information can be attacked.

- **Disaster Recovery/Business Continuity Plan (DR/BCP)**

  Despite the fact that users do not know where their data is physically located, there are plenty of environmental threats such as fires, floods, earthquakes etc. The cloud provider has to protect the environment around the data center so as the equipment is safe. In addition, the user has to be sure that his data will be reusable after a potential disaster and that there is a BCP by the cloud provider.

It can be clearly inferred that the above researchers both agree on the security concerns regarding cloud computing. Data location, data access, long-term viability, data classification, recovery and legal issues are some of the most important requirements. So, a potential user should always have in mind the following list:

Security Requirements	InfoWorld, Gartner	Global Knowledge, Michael Gregg
Data Location	✓	✓
Data Access	✓	✓
Regulatory Compliance	✓	✓
Audit	✓	✓
Disaster Recovery / Business Continuity Plan (DR/BCP)	✓	✓
Long-term Viability	✓	✓
Data Classification / Data Segregation	✓	✓
Training of Provider Employees		✓
Service Level Agreement (SLA) Terms		✓
Security Breach		✓
Investigative Support	✓	

David Chou analyzes some of the most common distinct security considerations concerning cloud computing. These are data privacy, shared and virtualized resources, multi-tenancy, heterogeneity, Internet transit, lack of both control and standards [40]. He focuses on all the above security considerations in order to emphasize on the fact that the services are sensitive to environments such as cloud computing, therefore they should be protected.

2.2 Privacy Requirements in Cloud Computing

Privacy has always been a major concern, as cloud users have to upload, and in most cases, store their data in publicly accessible data enters [7]. The protection of privacy is really important. Pearson mentions and analyzes a number of key privacy requirements [8, 42], which are listed below:

- **Notice, openness and transparency**

  In a cloud environment, a lot of information is located. If someone wishes to use this information in any way, he has to inform the data' owners on the kind of information he intends to use, as well as the duration and the way of use. In order for the privacy to be protected, cloud providers have to familiarize cloud users with the privacy policies and terms of use.

- **Choice, consent and control**

  Cloud users should be the ones to choose whether for different reasons they wish their data to be collected or not and give their consent so as the management of their data is held by the cloud providers.

- **Scope/minimization**

  Depending on the purpose the information is used, privacy can be violated. That means that only in the cases of a stated purpose, should information be collected. The concentration of user data should always be limited.

- **Access and accuracy**

  Cloud users must be able to have access to their data within the cloud environment. They should have the ability to check the integrity of their data. In that way they will be sure that their data is safe and not altered in any way. In other words, whether privacy is held or not will be ensured.

- **Security safeguards**

  When safeguards are implemented, certain “security actions” cannot be permitted. Unauthorized access, disclosure, copying, use and alteration are some of the forbidden security actions according to Pearson.

- **(Challenging) compliance**

  Each company follows a specific privacy procedure, which the users have the right not to agree with. However, every single transaction must be in compliance with the privacy legislation.

- **Purpose**

  The cloud data has to be used only for the purpose collected. It is essential, that cloud users be informed about the reason their data is concentrated, as well as the applications it is shared in. In this way, they will be aware of the location as well as use of their personal information.

- **Limited use – disclosure and retention**

  As mentioned above, data must be used only for specific purposes, therefore the use must be limited, in order to avoid possible revelation of personal data without delegation. This is a way data can be protected.

- **Accountability**

  Accountability is a really important privacy requirement. An appointed person by the company must check if privacy policies and practices are properly implemented, by monitoring all the procedures and intervening when necessary.

Privacy Requirements	HP Labs, Pearson
Notice, openness and transparency	✓
Choice, consent and control	✓
Scope/minimization	✓
Access and accuracy	✓
Security safeguards	✓
(Challenging) compliance	✓
Purpose	✓
Limiting use – disclosure and retention	✓
Accountability	✓

2.3 Security and Privacy Benefits

Several security benefits related to cloud computing are suggested by ENISA. Among the top ones are the following [5]:

- **Security and the benefits of scale**

  "Put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection." The security measures applied to large quantities of resources by organizations, can definitely be less expensive due to the massive scale of protection. In this way, organizations can achieve better protection. Other benefits of scale are the multiple locations, the edge networks, the improved timeliness of response as well as the threat management. By multiple locations we mean that cloud providers store their users' data

in a number of places, which practically induces redundancy and failure independence. By edge networks we mean that the data content within the cloud is processed near its destination, therefore lots of problems in local networks can be avoided. Another important benefit is that in case of an incident, the response time is increased, so the cloud providers can correspond more effectively. Finally, larger cloud providers, can easily hire specialists to deal with the most important security threats, whereas on smaller organizations cannot afford such services.

- **Security as a market differentiator**

  A great number of cloud users focus on the security of cloud services. In contrast to traditional services, reputable cloud providers offer a better level of security, so customers make their choice based on the confidentiality, integrity and resilience levels of the services to ensure better data protection.

- **Standardized interfaces for managed security services**

  Large cloud providers create open and easily accessible interface so that customers can be served easily at lower costs. Cloud users wish to handle their data quickly, safely and with minimal difficulties, so when security services are user friendly, through an easy interface, the choice to trust one's data to a cloud provider becomes easier.

- **Rapid and smart scaling of resources**

  As technology develops, the number of cloud resources is increased. A cloud provider has the ability to reallocate the resources in order to cope with attacks, thus increasing resilience levels.

- **Audit and evidence-gathering**

  Cloud providers have the ability to offer multiple virtual machines. In this way, when an incident occurs, the cloud user can create an image to store his data and protect it from an attack. When there are lots of virtual machines, the analysis of security incidents becomes quicker and easier, therefore valuable time is saved. In addition, log storage becomes more cost-efficient, so security incidents can be handled appropriately.

- **More timely, effective and efficient updates and defaults**

  In a cloud environment, updates of VMs images and software should regularly take place and all security settings have to be updated with the latest versions. Especially when there is no heterogeneity in the cloud platform, updating is achieved effectively and efficiently.

- **Audit and SLAs force better risk management**

  Internal audits and risk assessments have to be carried out on a regular basis so that risks that will provoke damages to both systems and data can be avoided. Through the process of risk assessment risks are estimated and threats are recognized, enabling the cloud provider to offer better levels of security.

- **Benefits of resource concentration**

  "It has the obvious advantage of cheaper physical perimiterisation and physical access control (per unit resource) and the easier and cheaper application of a comprehensive security policy and control over data management, patch management, incident management, and maintenance processes." That means that when more resources are gathered in just one place, the security procedures can be applied more effectively and in an easier way.

There are plenty of other analyses on the security benefits of cloud computing [42]. For example, it is worth mentioning that in SaaS applications the intruders cannot access the original source code of the application. That means that the intruder does not know what the vulnerabilities inside the code are, a frequent phenomenon in other applications. Another benefit is that the cloud provider has the main responsibility for the security of the services.

2.4 Security and Privacy Risks

Cloud computing is a new technology that involves a great number of security risks. ENISA analyzes the security issues related to cloud computing classifying them in four categories and listing them according to probability and impact level, reference to vulnerabilities and affected assets as well as level of risk. Within the top security risks the following are listed [5]:

- **Policy and organizational risks**
  - **Lock-in:** Due to the lack of tools, as well as the lack of procedures and standard data formats, service portability cannot possibly be guaranteed thus affecting sensitive or personal data, company reputation and service delivery.
  - **Loss of governance:** When a user locates his data within a cloud, he loses every single control over it. Security is the first thing affected because plenty of audits are not permitted (e.g. external penetration testing) and limited logs are available. Therefore, customer trust is at stake.
  - **Compliance challenges:** Neither cloud providers can possibly prove their compliance to standards and regulatory requirements, nor customers are allowed to control them.
  - **Loss of business reputation due to co-tenant activities:** If a malicious activity occurs within a cloud, it will affect all tenants, as there is a chain reaction within the infrastructure. So when a tenant behaves improperly, the reputation of other tenants is affected too. Spamming is a characteristic example.
  - **Cloud service termination or failure:** The cloud provider can go out of business, due to a number of reasons such as competitive pressure or lack of financial support. Such failure can have a huge impact on the customer who inevitably loses his data.
  - **Cloud provider acquisition:** The acquisition of a cloud provider can jeopardize non-binding agreements (e.g security investments) thus having a negative impact on security and privacy requirements.

- **Supply chain failure:** The cloud provider may outsource spesific tasks to third parties something that causes a number of security problems, as it depends on the level of security of each cloud provider. Sometimes, the customer ignores this situation, therefore he cannot possibly be aware of the risk his data is in.

- **Technical risks**
  - **Resource exhaustion:** The concentration of resources in a single cloud service poses a number of risks for both the cloud provider, as well as the cloud user. It can lead to service unavailability, compromised access control system and consequently economic losses. The risk of resource exhaustion can be caused by a denial of service (DoS) attack.
  - **Isolation failure:** In a cloud environment, resources are shared among cloud users. This can cause problems in isolating one user from another. The risk of not maintaining isolation in storage, memory, routing and reputation is present. In other words, lots of attacks can take place on resource isolation mechanisms.
  - **Cloud provider malicious insider-abuse of high privilege roles:** Occupied in data centers, certain employees who work within cloud environments, acquire high privilege roles, administrating or managing economic services. Therefore, they often become the targets of malicious insiders who wish to deprive them of their personal or sensitive data. Such attacks can even affect the reputation of the company, so the risk is classified as “high”.
  - **Management interface compromise:** The customer management interface is often accessible through the Internet, so the cloud provider has to handle the risks of both remote access and web browser vulnerabilities. The fact that the management is carried out via an Internet connection, facilitates malicious users who wish to attack for their profit.
  - **Intercepting data in transit:** Due to the fact that cloud computing is a huge and complex architecture, plenty of data is in transit among nodes, giving the “perfect chance” to attacks (e.g. sniffing, spoofing, and man-in-the-middle

attack) to create problems to the data in transit, especially to the communication among the nodes.

- **Data leakage on up/download:** Data leakage is possible between cloud providers and cloud users. Some of the most important assets affected by data leakage are personal and sensitive data, credentials, user directory, business reputation and customer trust.
- **Insecure or ineffective deletion of data:** The deletion of data within a cloud environment is really risky. When a cloud user asks his cloud provider to delete his data, two major problems arise. On the one hand, the cloud provider has already stored copies of the user’s data, possibly from previous backups. Therefore, while he assures the customer that his data does not exist anymore, in reality this is not the case. On the other hand, the data may be located in a disk shared with other users, so the deletion of data, cannot possibly take place. For the above reasons the deletion is a huge problem for the both cloud provider and the cloud users.
- **Distributed denial of service attacks (DDoS):** Due to the fact that cloud computing is a distributed architecture, the possibility of a DDoS attack is always present. A major asset affected by a DDoS attack is the network, as the traffic created can prove to be disastrous.
- **Economic denial of service (EDoS):** An EDoS attack is a kind of DDoS attack targeting the customer’s economic resources. As a result the customer may either lose some money or in the worst cases be economically destroyed.
- **Loss of encryption keys:** A malicious user can reveal the secret keys or passwords pretending to be someone else than in reality, thus acquiring access to unauthorized data without being delegated.
- **Undertaking malicious probes or scans:** Malicious probes or scans can be serious threats as hackers find it convenient to attack and create problems to the security of data and cloud services.

- **Compromise service engine:** The role of a service engine is to manage and organize the resources among customers. It can be compromised by attackers, who try to hack it through different service models (IaaS, PaaS and SaaS).
- **Conflicts between customer hardening procedures and cloud platforms:** Both cloud customers and cloud providers are responsible for the security of the customer's data. On the one hand, customers have to follow certain practice guidelines to secure their data and not just wait for the cloud provider to act. On the other hand, cloud providers have to offer the best level of security while being obliged to handle conflicts among customers and the different level of security selected by them. Satisfying the security and privacy requirements of all tenants, makes the role of a cloud provider a really challenging task.

- **Legal risks**
  - **Subpoena and e-discovery:** When the physical hardware is confiscated due to legal differences the risk of unwanted disclosure of the customers' data becomes obvious, thus inducing problems to the data security.
  - **Risk from changes of jurisdiction:** The data may be located in different countries therefore held in multiple jurisdictions. In some cases this may lead to mandatory disclosure or seizure, posing a number of legal risks to both customers and providers.
  - **Data protection risks:** The protection of data in a cloud infrastructure is essential and of high importance. The customer is responsible for the processing of his data, even in case the cloud provider is in charge of the process. Therefore, the customer has to be aware of the data protection law. The cloud providers have to inform the customers about the lawful processing procedures they use. The security of data can be easily breached, especially in case of hybrid clouds, leading to customers losing control of their data.
  - **Software licensing risks:** Software license often applies to a single computer or a limited number of computers. When software runs in a cloud environment there

are chances that the license terms are not applied. Therefore, applications that have been designed for the cloud may be at risk, as attackers are likely to try to use the application for free (without license) for their own profit.

- **Certain risks not specific to the cloud**, such as network problems, network management, modifying network traffic, privilege escalation, social engineering attacks, loss or compromise of security logs, backups lost/stolen, unauthorized access to data centers, theft of computer equipment and natural disasters can also be present. Such risks are not directly related to cloud computing, but ENISA analyzes them in an effort to present an integrated risk analysis.

Summarizing all the above security risks, it is quite obvious that the assets which are affected the most are the company reputation, the customer trust, the personal and sensitive data, as well as the service delivery.

According to Pearson [8, 42], there are certain privacy risks for cloud computing, divided into five main categories presented below:

- **Cloud service users privacy**
  In a cloud environment users are often obliged to give several personal data unwillingly. In some cases they even give their consent to be monitored without practically being aware of it.

- **Privacy of the organization using the cloud service**
  From the company’s perspective, there are lots of privacy risks. Non compliance to enterprise policies and legislation, loss of reputation and credibility are some of them. In other words, if the organization does not comply with the standards and the user’s data is lost, the company will inevitably lose both customers and consequently its reputation.

- **Implementers of cloud platforms privacy**

  The programmers and the people who manage cloud platforms have to tackle the exposure of sensitive information stored on the platforms, the legal liability, the loss of reputation and credibility, as well as the lack of user trust and take-up. That means that all these risks, which implementers have to cope with, have serious impacts on both cloud customers and cloud platforms.

- **Providers of applications on top of cloud platforms privacy**

  Such privacy risks involve legal non compliance and loss of reputation. Besides, when so much sensitive data is stored in the cloud, there is always the possibility that it is used for purposes other than the original purpose. In this way, customer trust is lost.

- **Data subject privacy risk**

  The exposure of personal information is the main privacy risk. That means that customers trust their personal data, in non-safe environments, therefore running the danger of being revealed.

2.5 Security Attacks in Cloud Computing

Due to the fact that cloud computing is a relatively new technology, there is a growing number of potential violators. The attackers find vulnerabilities in the security of a cloud environment and use them for their own profit. The main attacks concerning security in cloud computing as well as measures to combat such attacks are listed below [25]:

- **Distributed Denial of Service (DDOS) Attack**

  In a DoS attack legitimate users are prevented from using a specified network resource (e.g. websites, web service, computer system). When many computing systems launch a coordinated DoS attack against one or more targets, then the attack is called a DDoS attack, which intends to exhaust the resources of the target. In a cloud environment, a

DDoS attack is really feasible, as the attackers use botnets (zombie computers) to perform DDoS attacks resulting to disastrous effects. In a cloud infrastructure, there is a great number of computers linked together, therefore a DDoS attack is quite easy to be performed. However, the Amazon has managed to come up with DDoS mitigation techniques in order to tackle such attacks.

- **Man in the Middle Attack**

  In this kind of attack, a third party (e.g. the attacker) intervenes between two users and creates problems to their communication. To be more specific, the messages exchanged between the victims, are late to arrive their destination, as the attacker is the one who first receives the messages from one victim and then forwards them to the other victim, without the victims being aware of the fact. The Amazon Web Service (AWS) Application Programming Interface (API) uses SSL-protected endpoints in order to achieve server authentication, therefore ensuring customer safety.

- **IP Spoofing**

  IP spoofing is practically the creation of Internet Protocol (IP) packets with a forged source IP address. The aim of this attack is to conceal the identity of the sender or to impersonate another computing system. The Amazon Elastic Compute Cloud (EC2) protects its customers by not permitting traffic sent from a forged IP Address.

- **Port Scanning**

  When a user regulates all traffic from any source directed to a specific port, then that specific port becomes vulnerable to a port scan attack. The attacker takes advantage of the opening ports to access a computer via the Internet. The customers of the Amazon EC2 can be protected through the Amazon EC2 Acceptable use Policy (AUP), so when an attacker violates the AUP, then the Amazon makes sure that the case is investigated and dealt with, appropriately.

- **Packet Sniffing**

  Trough Packet Sniffing, the attacker observes packets that “travel” within a network. Sniffing is a way to trap data from a network, especially packets that include words like “login” or “passwords”, ID names etc. In this way the attacker gathers all the necessary information he needs about the network. Although the Amazon EC2 is able to prevent such attacks, yet customers should make sure that all sensitive traffic is encrypted.

2.6 Security Recommendations

According to ENISA [5], there are three top security recommendations related to cloud computing: assurance for cloud customers, legal recommendations as well as research recommendations.

To begin with, cloud customers need to be sure that cloud providers follow some standard security practices in order to offer assurance and protection to their data. ENISA recommends that customers have the ability to evaluate cloud providers as well as the risks included in the cloud services, through completion of check-lists.

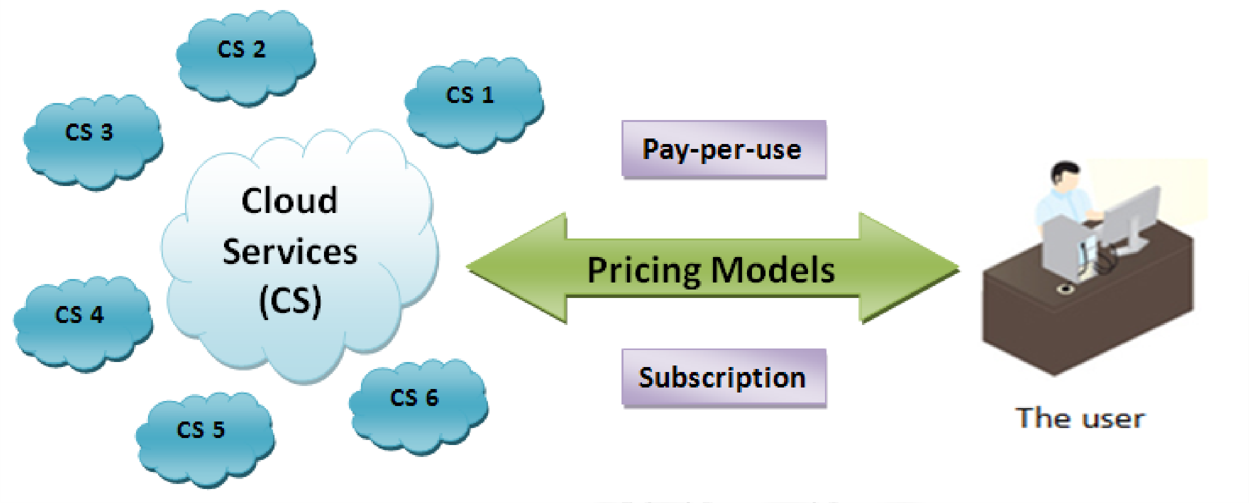
In addition, through the use of cloud computing, many legal issues arise. Therefore, both cloud customers and cloud providers have to make sure that the terms of their contract ensures protection against possible security issues. In that way, many legal issues are practically solved during contract evaluation or contract negotiations.

Finally, ENISA recommends that specific areas related to building trust in the cloud, data protection in large scale cross-organizational systems as well as large scale computer systems engineering be thoroughly measured. In this way, cloud computing technologies will improve security.

CHAPTER 3

Billing in Cloud Computing

3.1 Pricing Models

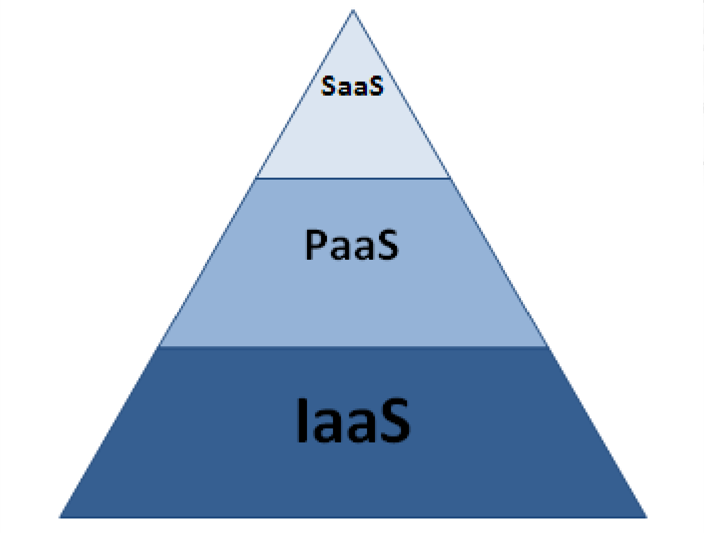


Cloud computing is a new internet-based technology enabling users to access resources via the Internet. To do so, Internet users have to pay for the services they receive depending on the use. There are two pricing models. The first, is based on pay per use. That means that people pay for the particular services they use. They can either increase or decrease the capacity of cloud resources on demand as their computing requirements change. The second pricing model is based on subscription. The users sign a contract and pay a fixed price, usually per month or per year, having access to a combination of recourses the way they wish.

When people use the resources they have to pay according to the use. The pay-per-use pricing model is simple: it associates units (or units per time) with fixed price values, and it is widely used for products (services) in which mass production and widespread delivery make price negotiation impractical. In other words, the pay-as-you-go pricing model is one of the basic components of the cloud computing environment and the users can increase or decrease the capacity of cloud resources on demand as their computing requirements change. Another pricing model is subscription, in which the customer subscribes (by signing a contract) to use a preselected combination of service units for a fixed price and a longer time frame, usually on a monthly or annually basis [9].

3.2 Cloud Billing in Service Models

Due to the fact that users pay for the recourses they need, a number of rules in the cloud services billing should be applied [43]:



3.2.1 Cloud Billing in IaaS

The IaaS service model provides customers different hardware resources such as CPUs, server type, system administration, storage, disaster recovery, SLAs and others (e.g. charges for space, power, network capacity, security, operating system). According to CGI Group, “Billing for IaaS may be done based on the quantity and quality of the infrastructure resources provided.” All these examples are charged accordingly. For instance, the cost of server type depends on whether the same CPU can be deployed either in a low cost server or in a top-of-the-range server with high availability. The cost may vary depending on the customer.

3.2.2 Cloud Billing in PaaS

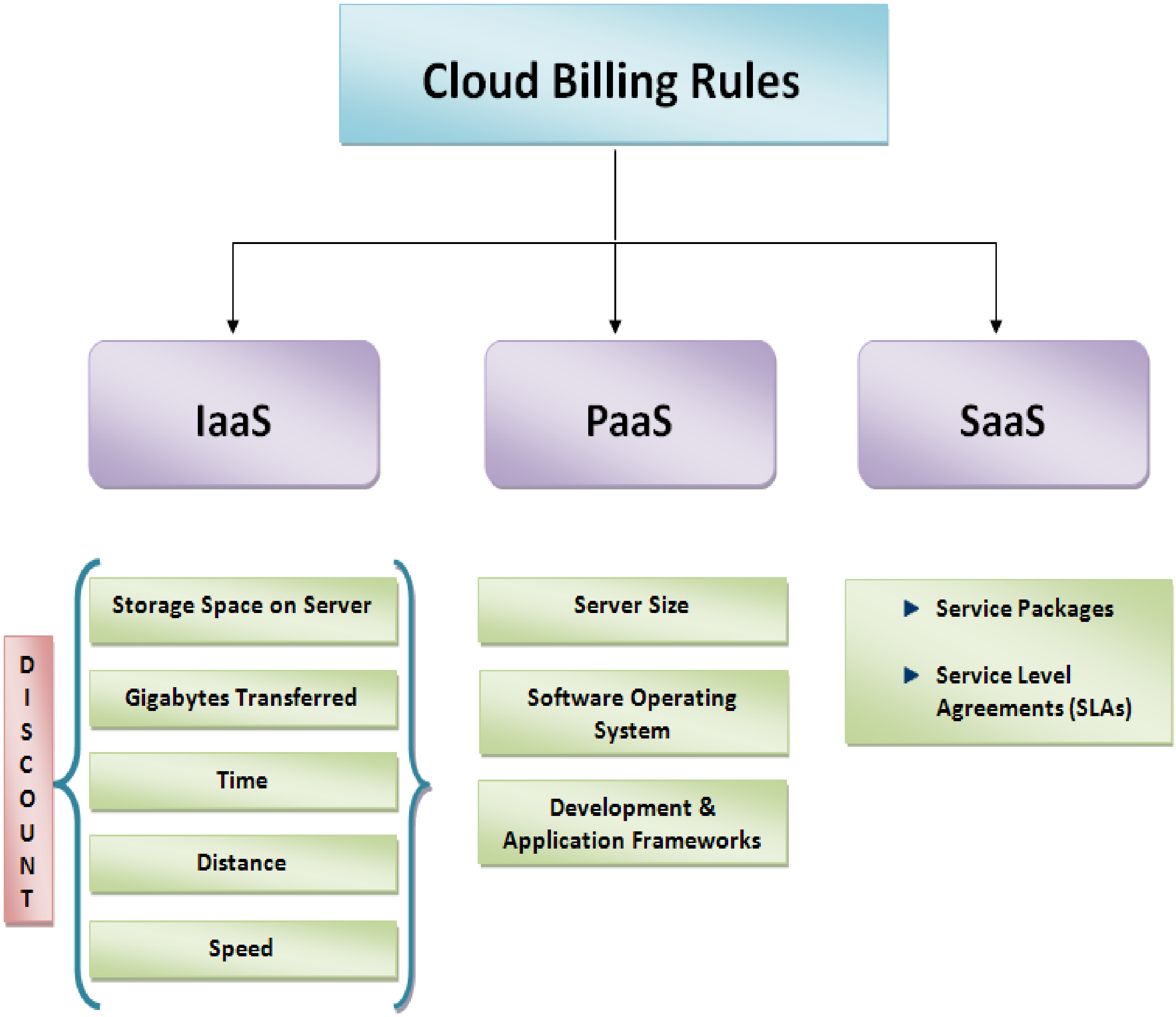
The PaaS service model includes software frameworks as well as the essential hardware for a developer to write and upload codes within a cloud for SaaS applications. Some examples of these frameworks are different hardware architectures with different server sizes, several software operating systems and lots of development and application frameworks. According to CGI Group, “Billing must take into account Infrastructure as a Service (IaaS) costs, as well as software features and product offerings provided in the PaaS layer. Different frameworks have different prices and may include different infrastructures.”

3.2.3 Cloud Billing in SaaS

The SaaS service model can be delivered either as a single cloud offering or as a multi cloud offering:

- The “single cloud offering” model includes different packages offered by different cloud providers. The packages consist of cloud services and their low price make them quite appealing to customers such as small and medium businesses (SMB). However, when it comes to large organizations the single cloud offering model does not work, because there is a great number of users who use numerous services. Therefore, it would be better if the enterprise paid only for the services used.
- The “multi cloud offering” model involves different clouds which include applications from different cloud suppliers.

3.3 Cloud Billing Rules in Service Models



Nowadays, more and more people use services through the cloud. All the services are provided by a data center at a specific cost and some billing policies have already been applied so that people can be charged accordingly. Below, we will define some billing rules based on some important factors [44].

3.3.1 Infrastructure-as-a-Service (IaaS)

- **Storage space on server**

Before someone uses the services from a data center, he has to be aware of the available space on the server, which he can use. Each user has to have a specific space on the server and be charged respectively. In other words, the user is actually "renting" the space on the server without buying it.

There are different ways in which the users of the cloud services can be charged. One way is for the user to pay depending on how much he uses the server over time. So, for instance, a server can charge the user with 5€ per month. Another way, is the user to be charged depending on the traffic on server, for example with 10€ per server/traffic or 4€ per server/user/traffic.

In case someone wishes to access a server at the same time with another user, who will finally be "the winner"? This question is quite difficult to answer. One way to handle such cases is according to priority. That means that the resources will become available to the user, whose process is the most critical. Another way is timing. The user, who "comes first", is preceded.

A server may offer backup services of the files of each user. The backup can be done on a daily basis, weekly or when necessary. The charges may vary depending on the type of backup. For instance, a fixed charge could be 10€ for each 256MB [45].

Examples:

- Each user can only use 20GB of storage for free.
- If the user exceeds the 20GB of storage, he has to pay 5€ for each additional 10GB of storage.
- If the total amount reaches 50€ a month, the user gets a bonus of an additional 15GB of storage and 5 hours of usage on a specific application.

Gigabytes transferred

Cloud services are provided through the resources, which are transferred from the data center to the machine of each user. The resources are usually estimated in gigabytes, which are transferred to the user's computers and the user, in turn, has to pay for them. The users have to be aware of the billing policy of each application based on the gigabytes transferred. Each service has its own way to charge the users, for example according to the hours of data transfer.

Example:

- If the use of resources exceeds the 20 hours of data transfer, the user has to pay the amount of 10 €.

Limit in resources

The resources have to be used in moderation. It is essential that a limit in the gigabytes transferred exists. More specifically, when users exceed the amount they have agreed to pay for a limited time (e.g. for a month), the system should be able to block the services provided. Moreover, the billing system should also have the ability to block, in real time, someone who does not follow the rules or even warn users before it is too late, so as they will be able to control and protect their data.

Examples:

- In order for the user not to exceed the limit of a monthly usage of 100€, the system blocks the services before the limit and informs the user.
- When the user violates the rules, he gets a limitation of resources probably for a period of time. If the violation is not very serious, he must pay a fine to continue his actions normally.

Maximum number of users

Each application has a maximum number of users, otherwise it crashes. When an application approaches the maximum number of users, it automatically sends warning in all registered members. In the case where the application has reached the maximum number of users, a user has to abandon and give his space to another user, as there is no space for both. That will inevitably cost the user who will finally access the service an additional amount charged by the application.

Examples:

- The "X" application can host 10.000 users at the same time. If a new user has to use the application urgently, another user has to quit the application. To do so, the first user has to pay the fixed amount of 15€ and the company has to guarantee the second user that he will be able to use his data another time without losing it.
- When the above "X" application approaches 9.000 users, it warns all the registered members by sending the following message: "The "X" application is approaching the limit of maximum users, so the system will not be directly available. If you do not need this application please quit! Thanks for your collaboration".

Time

Sometimes time plays a really important role in cloud computing. The most usual way to charge someone who uses the services in the cloud, is related to the time. So, some applications charge the customers based on an hour or monthly basis. There are users that prefer to pay depending on the hours they use the resources and others, who prefer to pay a fixed amount each month. The first way is the pay-per-use pricing model and the second is the subscription pricing model. Moreover, the billing system is responsible for charging in real time, so as not to miss any events. For instance, it is essential that real time monitoring and budget control be applied, so as the users can neither exploit the services nor feel lost.

Examples:

- The users should be charged depending on how much they use the server per month. They have to pay 50€ for a monthly subscription.
- Another way is for the users to pay 0.20€/hour. So, the users can calculate the hours they have access to an application. This way is better for people who do not work so much in the cloud and they only use certain applications especially for a few hours a month. So, it is more beneficial for them, because they are not forced to pay for something, which they actually do not need on a permanent basis.
- The ”Y” application sets specific privileges where the user gets a 15% discount for using the specific application off peak (from 24:00 – 6:00), or Sundays and Public Holidays.

Distance

Cloud services used by the registered members are located in numerous data centers all over the world. In most cases the same service is offered by different data centers so as to ensure that more users are served. The distance between the data center from where the service is offered and the area the user is located, is really important, especially, in the case of billing. In other words, the service provider should charge the user depending on the latter’s distance from the data center. The closer the data center the lower the cost.

Example:

- Supposing that someone lives in Greece and uses the “Z” application, he has to be charged by the closest to him data center. That means that if the “Z” application is offered by two data centers, one in Italy and one in California, the service must be able to provide the applications from the data center in Italy and charge the user accordingly. That will also be really better for the user, as the response time will be just a few seconds quicker, due to the fact that the data center is closer to him.

Speed

The speed of the cloud services response plays an important role in the process of billing. Speed levels scale up and so does the charge, so when the user exceeds the limits, he is charged accordingly.

Example:

- If someone wishes to use 1-10 Mbit/sec speed he will be charged 10€. If he wishes to use 10-100 Mbit/sec speed the cost will be 20€. The way of billing depends on the speed of the service that the user wishes to be provided. That can be beneficial for the user as he will be able to choose the speed according to his needs.

Discount

Frequent users of certain applications are encouraged to use the application more often by receiving special bonuses. In other words, the more they use the resources the more discounts they get. Such discounts can either be in the form of additional time in an application, or free use of another application and so on. Discounts can also be provided depending on the type of customer. That means that the billing policy will be different for someone who works alone in contrast to someone who is part of a company. Furthermore, another division of customers can be made among frequent and occasional users of the cloud services.

Examples:

- If someone uses the resources in large quantities, he benefits certain discounts. There are different types of customers, so there are levels of discounts. When someone exceeds the fixed amount of 80€ monthly, he “leaves” the first level and “enters” the second, which is set between 80€ and 160€. For each additional 80€ the user levels up.
- If a user completes the amount of 200€ within a month, he is given the benefit of using certain applications for free.
- If the use of resources exceeds the 40 hours of data transfer, the user benefits 30% discount on his monthly bill.
- If someone uses more than 40 applications he is charged with 1€ for each additional application.

3.3.2 Platform-as-a-Service (PaaS)

- **Server Size**

A cloud company often uses different hardware architectures with different server sizes. The server size plays a really significant role in the process of billing. Small (e.g. Intel-based servers), mid or even top-range servers and mainframes (e.g utilizing different chips) can be used [43].

Example:

- If someone uses a small framework to develop his application, the cost cannot possibly be the same with someone who has greater needs and wants to use a bigger server. In other words the server size is of great importance.

- **Software Operating Systems**

There is a big variety of software operating systems, which someone can use to develop his applications [43].

Example:

- If a developer develops an application which requires Windows, he should be charged at a different rate than someone who develops a similar application which requires another operating system such as Linux, Solaris, etc.

- **Development & Application Frameworks**

The development and application frameworks (e.g Java, .Net, etc) are really important, as the level of prerequisites as well as the knowledge required by the developer may vary and so will the cost [43].

3.3.3 Software-as-a-Service (SaaS)

- **Service Packages**

Many clouds offer service packages in order to be more appealing to the customers. In other words, a small or medium business can pay for a total number of services, even in case the business uses only a part of them [43]. That is mainly due to the fact that being interested in its own profit a business decides to pay for a vast number of services at a better price.

- **Service Level Agreements (SLAs)**

Each cloud provider uses different pricing models, based on “different contracts with different service level agreements (SLAs)” [43].

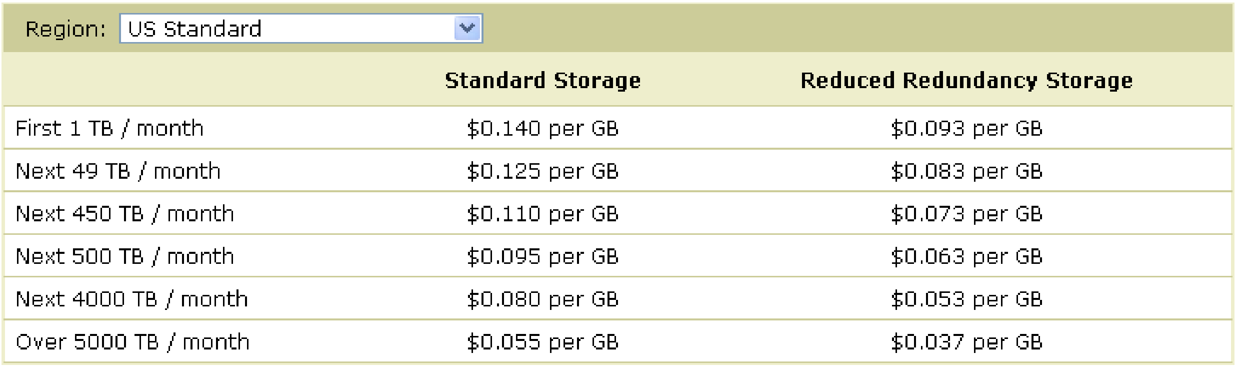
3.4 Examples of Pricing in two Online Storage Providers

Many cloud companies offer their customers disk space on data centers, based on the utility of services. The customers pay only for what they use, whereas the cloud providers charge taking some important factors (e.g. price, ease of use, 24/7 availability, customer service, security of the data, and long-term stability of the vendor) into account [46]. Two major companies offering the cloud environment to their customers are indicated below as characteristic examples. The way such large organizations charge for their services, will be examined through comparison.

3.4.1 Amazon

The Amazon uses the Amazon Simple Storage Service (Amazon S3), which is storage via the Internet, to charge its customers. The Amazon billing service is based on three types of pricing: storage pricing, request pricing and data transfer pricing [47]. In the figures below, the specific amounts are presented.

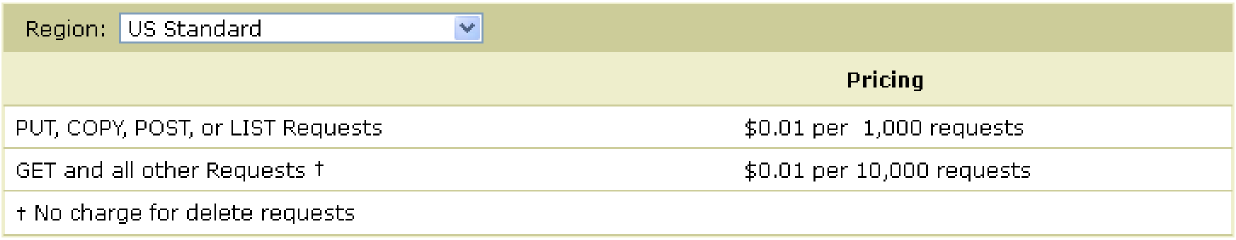
- **Storage Pricing**



Region: US Standard

	Standard Storage	Reduced Redundancy Storage
First 1 TB / month	$0.140 per GB	$0.093 per GB
Next 49 TB / month	$0.125 per GB	$0.083 per GB
Next 450 TB / month	$0.110 per GB	$0.073 per GB
Next 500 TB / month	$0.095 per GB	$0.063 per GB
Next 4000 TB / month	$0.080 per GB	$0.053 per GB
Over 5000 TB / month	$0.055 per GB	$0.037 per GB

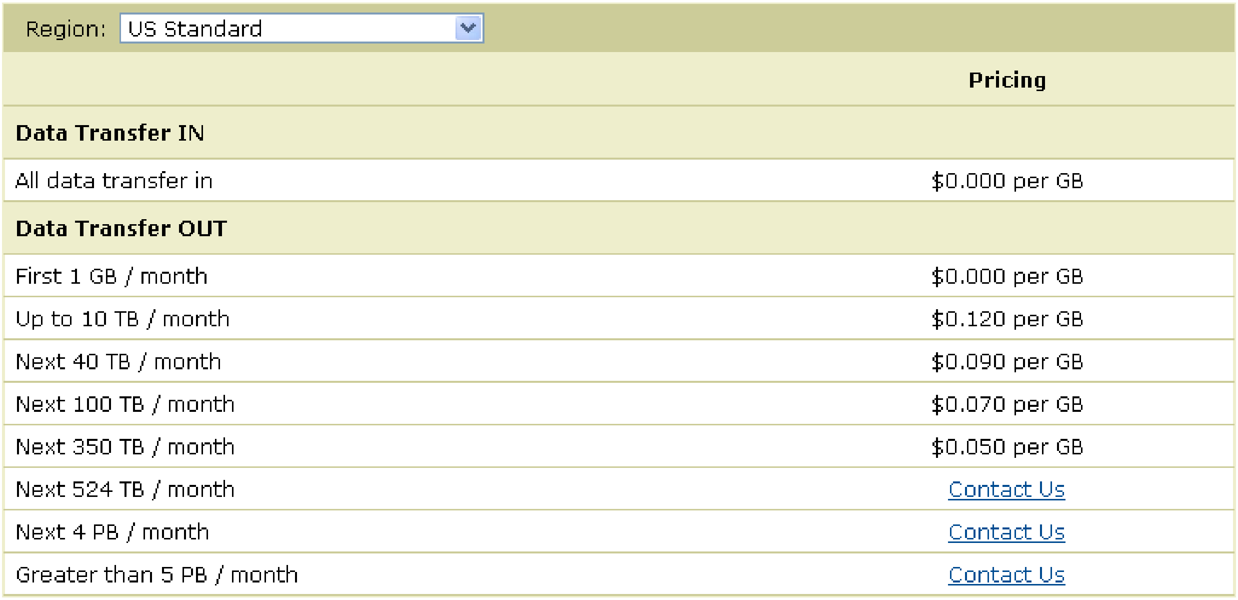
- **Request Pricing**



Region: US Standard

	Pricing
PUT, COPY, POST, or LIST Requests	$0.01 per 1,000 requests
GET and all other Requests †	$0.01 per 10,000 requests
† No charge for delete requests	

- **Data Transfer Pricing**



Region: US Standard

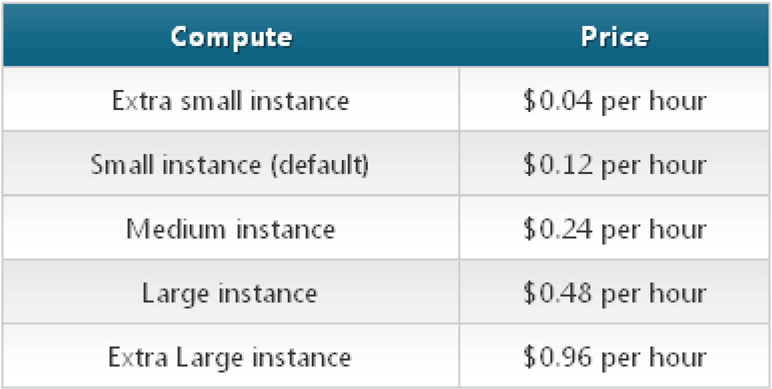
	Pricing
Data Transfer IN	
All data transfer in	$0.000 per GB
Data Transfer OUT	
First 1 GB / month	$0.000 per GB
Up to 10 TB / month	$0.120 per GB
Next 40 TB / month	$0.090 per GB
Next 100 TB / month	$0.070 per GB
Next 350 TB / month	$0.050 per GB
Next 524 TB / month	Contact Us
Next 4 PB / month	Contact Us
Greater than 5 PB / month	Contact Us

Furthermore, the Amazon provides its new customers with 5 GB of Amazon S3 storage, 20,000 Get Requests, 2,000 Put Requests, and 15GB of data transfer out, each month on an annual basis.

3.4.2 Microsoft

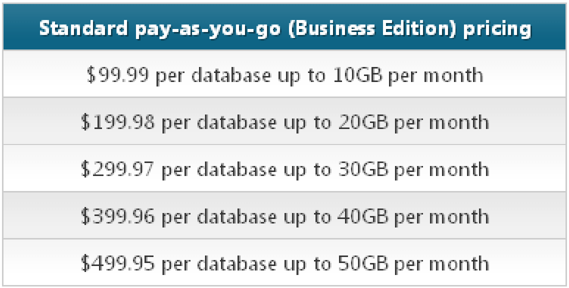
The Microsoft cloud computing platform is Windows Azure Platform. The way of pricing is quite flexible as Microsoft charges only for the resources its customers use. Storage, Database, Bandwidth, Caching and CDN features are charged on a per-GB/month usage basis, with per-transaction costs for some resources [48].

- **Compute time, measured in service hours**

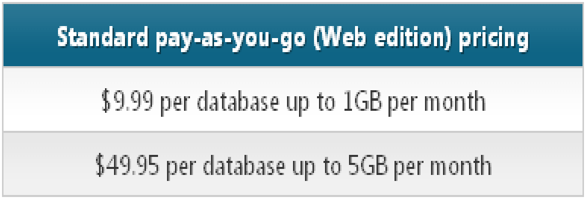


Compute	Price
Extra small instance	$0.04 per hour
Small instance (default)	$0.12 per hour
Medium instance	$0.24 per hour
Large instance	$0.48 per hour
Extra Large instance	$0.96 per hour

- **Database, based on size of the database**



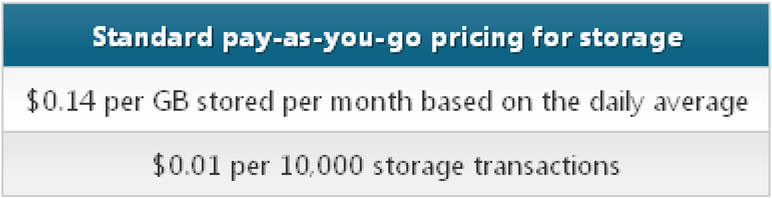
Standard pay-as-you-go (Business Edition) pricing
$99.99 per database up to 10GB per month
$199.98 per database up to 20GB per month
$299.97 per database up to 30GB per month
$399.96 per database up to 40GB per month
$499.95 per database up to 50GB per month



Standard pay-as-you-go (Web edition) pricing
$9.99 per database up to 1GB per month
$49.95 per database up to 5GB per month

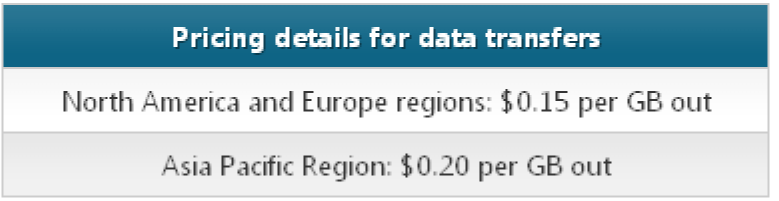
- **Virtual Machines**

- **Storage, measured in GB**



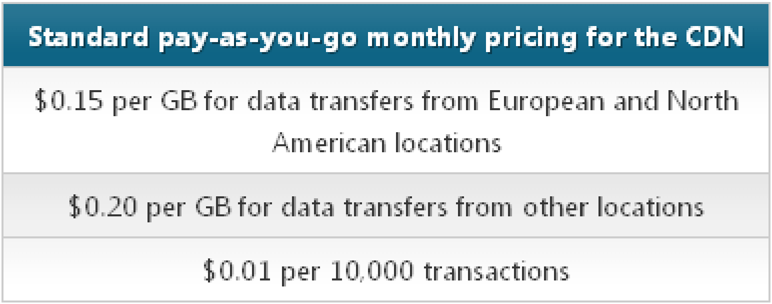
Standard pay-as-you-go pricing for storage
$0.14 per GB stored per month based on the daily average
$0.01 per 10,000 storage transactions

- **Data transfers measured in GB**



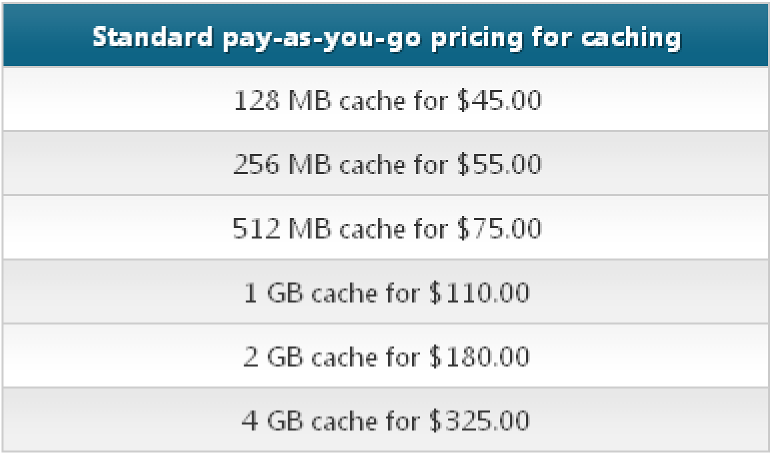
Pricing details for data transfers
North America and Europe regions: $0.15 per GB out
Asia Pacific Region: $0.20 per GB out

- **Content Delivery Network (CDN)**



Standard pay-as-you-go monthly pricing for the CDN
$0.15 per GB for data transfers from European and North American locations
$0.20 per GB for data transfers from other locations
$0.01 per 10,000 transactions

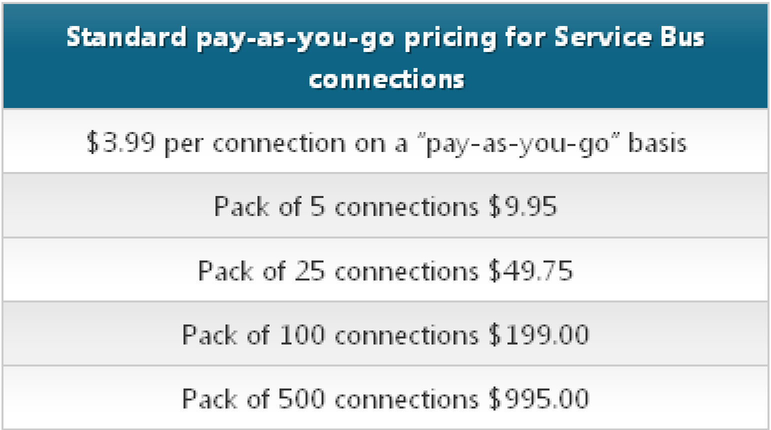
- **Caching, based on cache size per month**



Standard pay-as-you-go pricing for caching
128 MB cache for $45.00
256 MB cache for $55.00
512 MB cache for $75.00
1 GB cache for $110.00
2 GB cache for $180.00
4 GB cache for $325.00

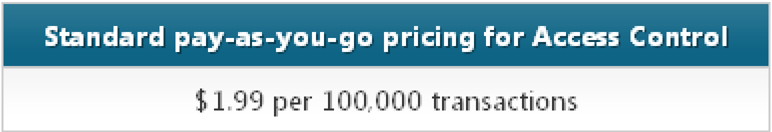
- **Virtual Network**

- **Service Bus**



Standard pay-as-you-go pricing for Service Bus connections
$3.99 per connection on a "pay-as-you-go" basis
Pack of 5 connections $9.95
Pack of 25 connections $49.75
Pack of 100 connections $199.00
Pack of 500 connections $995.00

- **Access Control**



Standard pay-as-you-go pricing for Access Control
$1.99 per 100,000 transactions

3.4.3 Comparing Pricing in Amazon & Microsoft

To sum up, from the above two important organizations, which offer cloud services, we can infer that they both charge according to the resources their customers consume. The common pricing factors they charge for are storage and data transfer, as we can see in the table below:

Cloud Platforms Pricing Factors	Amazon S3	Windows Azure Platform
Storage	✓	✓
Request	✓	
Data Transfer	✓	✓
Compute time		✓
Database		✓
Virtual Machines		✓
Content Delivery Network (CDN)		✓
Caching		✓
Virtual Network		✓
Service Bus		✓
Access Control		✓

3.5 Security & Privacy in Cloud Billing

Among the most important cloud computing characteristics is the measured service, something that is actually translated into billing. Therefore, the security and privacy requirements implemented in cloud computing in general, should be implemented in a cloud billing infrastructure too. The security and privacy requirements that have been presented in the previous section, are shown in the table below:

Security Requirements	Privacy Requirements
Data Location	Notice, openness and transparency
Data Access	Choice, consent and control
Regulatory Compliance	Scope/minimization
Audit	Access and accuracy
Disaster Recovery / Business Continuity Plan (DR/BCP)	Security safeguards
Long-term Viability	(Challenging) compliance
Data Classification / Data Segregation	Purpose
Training of Provider Employees	Limiting use – disclosure and retention
Service Level Agreement (SLA) Terms	Accountability
Security Breach	
Investigative Support	

3.6 Proposed Billing Architectures in Cloud Computing

The majority of papers only provide little information on the way the users are charged when they use the resources. More papers propose billing architectures and some of them mention the security challenges of the architectures.

According to Erik Elmroth, Fermın Galan Marquezy, Daniel Henriksson, David Perales Ferrera [11], a federated Cloud accounting and billing architecture is proposed for use within the RESERVOIR project, a research project partly funded by the European Union, focusing on the federation of Clouds at the infrastructural level. Two payment models are used, the postpaid and prepaid. The requirement is fulfilled in the proposed architecture. The billing for the execution of a service must be done on a per service basis, and not for each Virtual Execution Environment (VEE). The payment model of a service must be changeable without affecting components outside the accounting and billing system, and without enforcing any restarts or redeployments. In this billing architecture nothing is mentioned concerning security system.

Another system that provides a mutually verifiable resource usage and billing mechanism is THEMIS. THEMIS provides a level of security that is identical to that of a Public Key Infrastructure (PKI), minimizing the latency of billing transactions. In this paper some security-enhanced billing systems are listed and compared. THEMIS is a secure billing system because it offers protection from malicious cloud service providers (CSPs) or malicious users, from replay attacks and MITM attacks [12].

3.7 Attacks in Billing System

There are many security issues within cloud computing therefore, cloud services are vulnerable to attacks indeed. According to Rituik Dubey, Muhammad Asim Jamshed, Xiaohui Wang, Rama Krishna Batalla [10], many different attack scenarios and proposed solutions are defined. Some cloud service providers do not provide any kind of real time reporting or API for their cloud billing. This may lead to trust issues which arise when a client doubts whether the computation task provided by the cloud service was executed completely and correctly or whether the user was billed fairly for its service. Several critical security issues in cloud computing are studied in this project, including the metering problem, the problem of data backups as well as the solutions to the problems above.

3.8 Open and Legal Issues to Billing Services

Metering and Billing Evasion

Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker mention some serious vulnerabilities based on NIST's five essential cloud characteristics (on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity, and measured service). One of them is the metering and billing evasion. “The cloud characteristic of measured service means that any cloud service has a metering capability at an abstraction level appropriate to the service type (such as storage, processing, and active user accounts). Metering data is used to optimize service delivery as well as billing. Relevant vulnerabilities include metering and billing data manipulation and billing evasion.” [49].

Laws and Standards

Laws and standards play an important role in the cloud computing billing. They define the way cloud computing functions. Far too many issues are regulated by laws and standards and all users must follow them. Both the security and privacy of data in cloud services are of concern for the majority of the Internet “cloud” users. When constructing an application for cloud computing, each provider must be in accordance with national standards. So, the way of billing in cloud services is of outmost importance, as people, who use the services, want to be sure that providers follow certain guidelines in order to trust them. As a result, when a user violates the billing rules he is fined. Depending on the degree of violation the fines can be really “harsh”.

Moreover, those who wish to use resources from a data center based on a different country, must do so, in compliance with the billing rules of the country the data center is located in. Due to this, the providers need to deal with the fact that there are different taxes among countries. So, the billing may vary from one country to another. The violator will be forced to pay the fine set by the country the data center is located in.

Examples:

- If someone uses the “A” application for free while he is not eligible to do so, he will suffer the consequences, as he will be fined 10€. If he does not do so, he will not be able to use the application in the future.

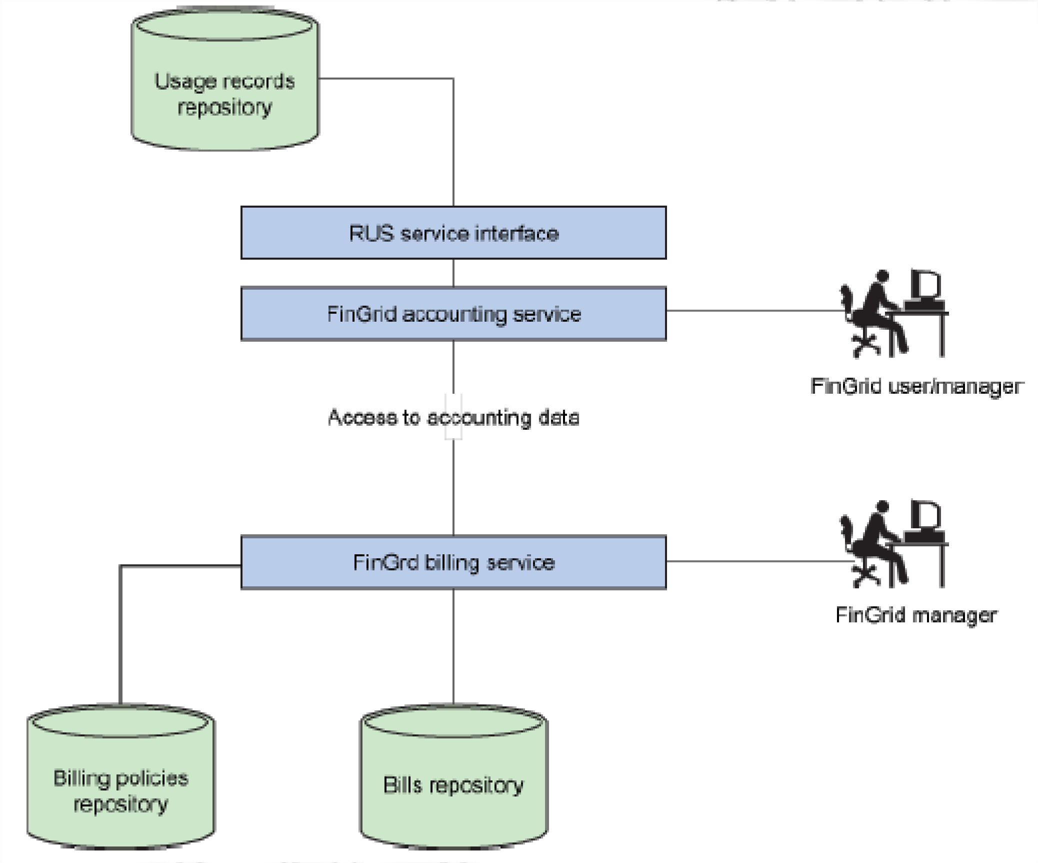
- If someone in Greece wishes to transfer data from a server in England, he should follow the billing rules that are valid in England. If the English provider charges 5€ per hour for the gigabytes transferred, then the Greek user will have to pay 5€ for each hour.
- A user in Greece has to pay 1€ per hour for the “Z” application. Because of the different taxes among the countries, the same user in England has to pay 1,5€ per hour for the same application.

CHAPTER 4

Case Study in Cloud Billing Policy

4.1 Proposed Cloud Billing Policy

IBM proposes a billing service module for the cloud environment [50] whose architecture is pictured in the diagram below.

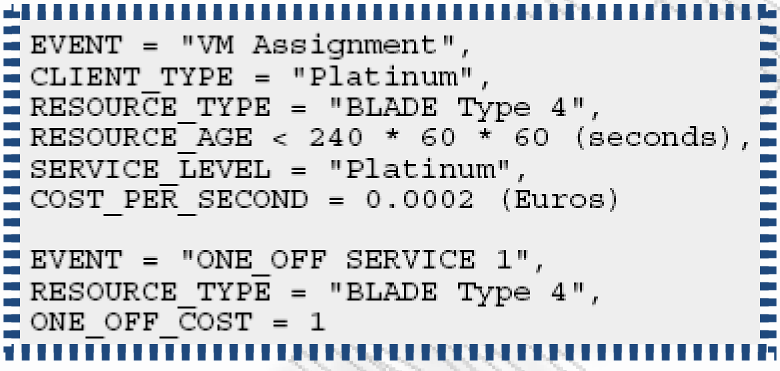


According to IBM, the aim of such cloud billing service module is to provide an interface in order for the bills to be generated based on some predefined billing policies. Yet, because of the fact that the person who sets the billing policies, is not aware of a programming language (like a programmer does), the billing policies have to be expressed in an understandable language. This needs to be done so that the billing policies can change.

For example, IBM uses an expression of rules in plain English and converts it in a specific language with concrete syntax.

Example:

“When the event is VM Assignment and the client's type is Platinum, then the cost per second is 0.0002 euros.”



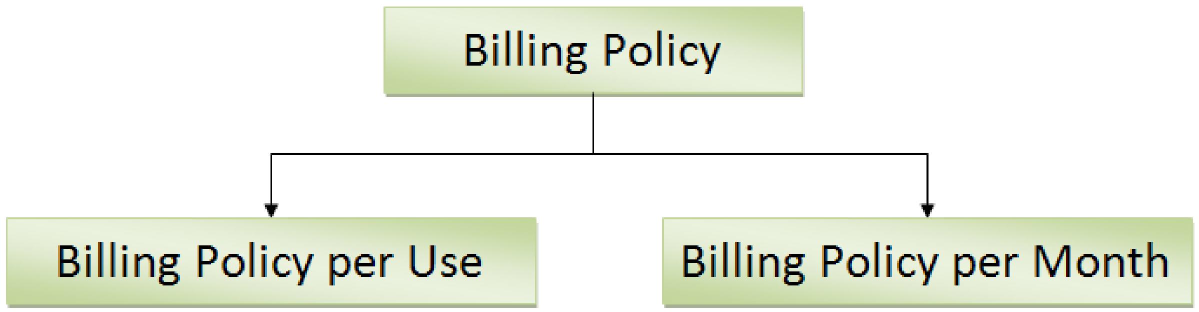
```
EVENT = "VM Assignment",
CLIENT_TYPE = "Platinum",
RESOURCE_TYPE = "BLADE Type 4",
RESOURCE_AGE < 240 * 60 * 60 (seconds),
SERVICE_LEVEL = "Platinum",
COST_PER_SECOND = 0.0002 (Euros)

EVENT = "ONE_OFF SERVICE 1",
RESOURCE_TYPE = "BLADE Type 4",
ONE_OFF_COST = 1
```

In addition, Wehle from IBM defines some functional requirements and non-functional yet essential requirements to provide an integrated research about the proposed cloud billing service module. In functional requirements he includes quote service, conversion functions and policies, payment schemes, and user identification. In non-functional requirements security, scalability, standards, and fault tolerance are included.

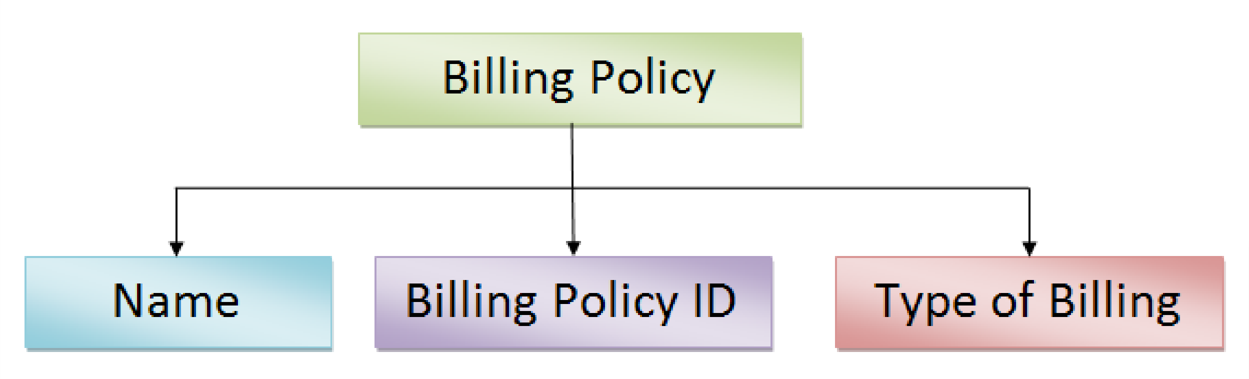
Through his research, he offers a way to understand how the billing module both operates and fits into a cloud infrastructure, something which is really important, especially, when wishing to set billing policies.

4.2 Cloud Billing Policy using Extensible Markup Language (XML)

As analyzed in the previous section, XML is an understandable and easy way to set billing policies in a cloud. Through XML, we will examine how the two ways of pricing (pay-per-use, monthly subscription) can be defined. In other words, the billing policy is divided into two "sub-policies", the billing policy per use and the billing policy per month.



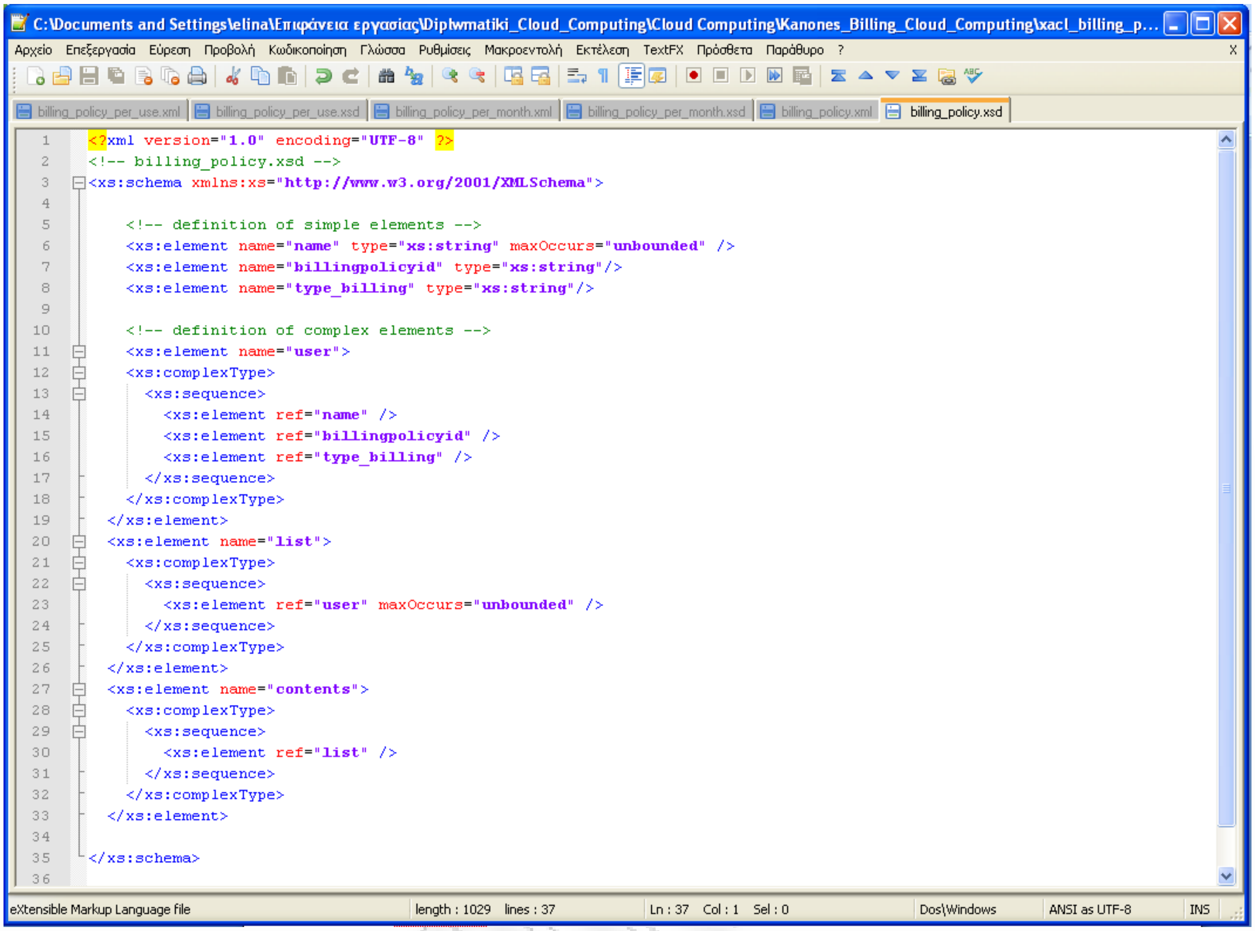
XML Schema: billing_policy.xsd



In the billing_policy.xsd, we define an element <billing_policy>, which contains a list with multiple users, who follow one of the two ways of pricing. Each element <user> has three sub elements:

- <name>: The <name> element defines the name of the user.
- <billingpolicyid>: The <billingpolicyid> element defines a unique identifier, which uniquely identifies the policy of a single user.
- <type_billing>: The <type_billing> element defines if a user uses the pay-per-use or monthly subscription model.

The <billing_policy_id> is the common element in both pricing models. This is the element, from which the system can understand if a user follows the pay-per-use or the subscription model. So, a user cannot possibly access another user's resources.

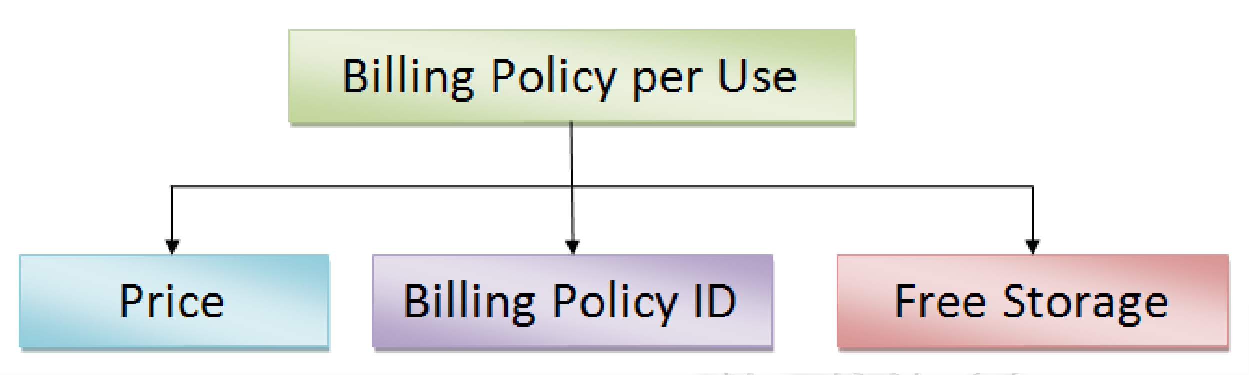

C:\Documents and Settings\elina\Επιφάνεια εργασίας\Diplwmatiki_Cloud_Computing\Cloud Computing\Kanones_Billing_Cloud_Computing\xacl_billing_p...
Αρχείο Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση TextFX Πρόσθετα Παράθυρο ?
billing_policy_per_use.xml
billing_policy_per_use.xsd
billing_policy_per_month.xml
billing_policy_per_month.xsd
billing_policy.xml
billing_policy.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- billing_policy.xsd -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

    <!-- definition of simple elements -->
    <xs:element name="name" type="xs:string" maxOccurs="unbounded" />
    <xs:element name="billingpolicyid" type="xs:string"/>
    <xs:element name="type_billing" type="xs:string"/>

    <!-- definition of complex elements -->
    <xs:element name="user">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="name" />
        <xs:element ref="billingpolicyid" />
        <xs:element ref="type_billing" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="list">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="user" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="contents">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="list" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

eXtensible Markup Language file
length : 1029 lines : 37
Ln : 37 Col : 1 Sel : 0
Dos\Windows
ANSI as UTF-8
INS

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- billing_policy.xsd -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

      <!-- definition of simple elements -->
      <xs:element name="name" type="xs:string" maxOccurs="unbounded" />
      <xs:element name="billingpolicyid" type="xs:string"/>
      <xs:element name="type_billing" type="xs:string"/>

      <!-- definition of complex elements -->
      <xs:element name="user">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="name" />
        <xs:element ref="billingpolicyid" />
        <xs:element ref="type_billing" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="list">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="user" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="contents">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="list" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

XML Schema: billing_policy_per_use.xsd



In the billing_policy_per_use.xsd, we define an element <contents>, containing a list of multiple entries, which include the users who follow the pay-per-use model of pricing. Each element <entry> has three sub elements:

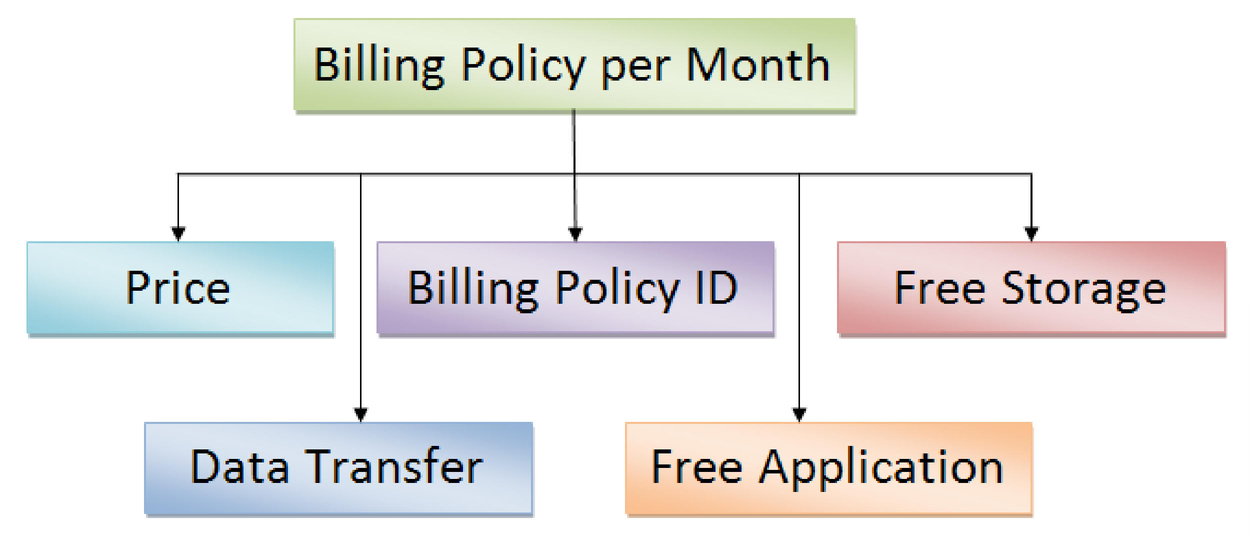
- <billingpolicyid>: The <billingpolicyid> element defines the unique identifier, which uniquely identifies the billing policy of a single user. From this element, the system "understands" who the user is and which way of pricing he follows. It recognizes that the user follows the pay-per-use model of pricing and not the monthly subscription.
- <price>: The <price> element defines the final total amount of money that a user has to pay.
- <freestorage>: The <freestorage> element defines the total free storage which is available to the user.

The <freestorage> element is used as an example, as it represents any resource a cloud company may offer its customers for free.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- billing_policy_per_use.xsd -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

      <!-- definition of simple elements -->
      <xs:element name="billingpolicyid" type="xs:string" />
```

```
    <!-- definition of complex elements -->
    <xs:element name="price">
          <xs:complexType>
            <xs:sequence>
                <xs:element name="amount" type="xs:positiveInteger"
                                  minOccurs="0" maxOccurs="unbounded" />
                <xs:element name="nomisma" type="xs:string"
                                                    default="euros"/>
            </xs:sequence>
          </xs:complexType>
    </xs:element>
    <xs:element name="freestorage">
          <xs:complexType>
            <xs:sequence>
                <xs:element name="memory" type="xs:positiveInteger"
                                                          default="20"/>
                <xs:element name="unit" type="xs:string" default="GB"/>
            </xs:sequence>
          </xs:complexType>
    </xs:element>
    <xs:element name="entry">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="name" />
      <xs:element ref="duration" />
      <xs:element ref="price" />
      <xs:element ref="freestorage" />
    </xs:sequence>
      <!-- definition of attribute -->
    <xs:attribute name="type" type="xs:string" use="required"
                                                    default="per use"/>
  </xs:complexType>
</xs:element>
<xs:element name="list">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="entry" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="contents">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="list" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

<u>XML Schema:</u> billing_policy_per_month.xsd



In the billing_policy_per_month.xsd, we define an element <contents>, containing a list of multiple entries, which include the users who follow the monthly subscrption model of pricing. Each element <entry> has the below sub elements:

- <billingpolicyid>: The <billingpolicyid> element defines the unique identifier, which uniquely identifies the billing policy of a single user. From this element, the system "understands" who the user is and which way of pricing he follows. It recognizes that the user follows the monthly subscription model of pricing instead of the pay-per-use.
- <price>: The <price> element defines the final total amount of money that a user has to pay. In this case, the amount of money is fixed.
- <freestorage>: The <freestorage> element defines the total free storage which is available to the user.
- <datatransfer>: The <datatransfer> element defines how many free hours of data transfer the user is entitled to.
- <freeapplication>: The <freeapplication> element defines how many hours of free usage on a specific application each user is allowed to use.

The <freestorage>, <datatransfer> and <freeapplication> elements are used as examples, as they represent any resource a cloud company may offer its customers for free.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- billing_policy_per_month.xsd -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

      <!-- definition of simple elements -->
      <xs:element name="billingpolicyid" type="xs:string" />
      <xs:element name="amount" default="30">
            <xs:simpleType>
              <xs:restriction base="xs:positiveInteger">
                  <xs:enumeration value="30"/>
              </xs:restriction>
            </xs:simpleType>
      </xs:element>

      <!-- definition of complex elements -->
      <xs:element name="price">
            <xs:complexType>
              <xs:sequence>
                  <xs:element ref="amount"/>
                  <xs:element name="nomisma" type="xs:string"
                                                     default="euros"/>
              </xs:sequence>
            </xs:complexType>
      </xs:element>
      <xs:element name="freestorage">
            <xs:complexType>
              <xs:sequence>
                  <xs:element name="memory" type="xs:positiveInteger"
                                                     default="25"/>
                  <xs:element name="unit" type="xs:string" default="GB"/>
              </xs:sequence>
            </xs:complexType>
      </xs:element>
      <xs:element name="datatrasfer">
            <xs:complexType>
              <xs:sequence>
                  <xs:element name="freehours" type="xs:positiveInteger"
                                                     default="100"/>
              </xs:sequence>
            </xs:complexType>
      </xs:element>
      <xs:element name="freeapplication">
            <xs:complexType>
              <xs:sequence>
                  <xs:element name="freehoursapp" type="xs:positiveInteger"
                                                      default="4"/>
              </xs:sequence>
            </xs:complexType>
      </xs:element>
      <xs:element name="entry">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="name" />
        <xs:element ref="duration" />
        <xs:element ref="price" />
        <xs:element ref="freestorage" />
        <xs:element ref="datatrasfer" minOccurs="0" />
        <xs:element ref="freeapplication" minOccurs="0" />
      </xs:sequence>
        <!-- definition of attribute -->
      <xs:attribute name="type" type="xs:string" use="required"
                                                      default="per month"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="list">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="entry" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="contents">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="list" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

The difference between the two cases is that in the pay-per-use model the user can use some standard resources (which a cloud provider may offer), while in the monthly subscription the user can use a total package of resources. For example, a cloud company can offer its users 10GB of storage for free, as a standard resource. In the first case, the user will have 10GB of free storage plus whichever service/application he uses from others resources. In the second case, the user will also have 10GB of free storage, as in the first case, but he will have the additional resources the cloud company offers in the "monthly package" subscription.

4.2.1 A Possible Cloud Billing Scenario

Taking all the above billing factors into account, a possible cloud billing scenario followed by a company, should be based on the way the billing is done in the cloud.

- Each user can use 20GB of storage for free.
- If the user exceeds 20GB of storage, he will have to pay 5€ for each additional 10GB.
- If a user chooses to pay only for the applications he uses, he has to be charged accordingly. That practically means that he will be charged with the application cost depending on the hours he uses the application.
    - If the user exceeds the amount of 100€ per month, he receives a 20% discount to all the applications he uses.
- If the user chooses to pay a total fixed amount of money on a monthly basis, he will have to sign a contract (monthly subscription).
    - The users should be charged depending on how much they use the server on a monthly basis. The cost for that will be 30€ per month. 25GB of free storage, 100 free hours of data transferred and 4 hours of free usage on a specific application are included in the cost. If the total amount reaches 30€ a month, the user "wins" an additional 15GB of storage for free and 5 hours of usage on a specific application.
    - When the user decides to renew his contract for the next year, he gets a number of bonuses. Every year the user levels up. In other words, every year the fixed charge of 30€ per month slightly increases but the user receives more services. His fixed amount reaches 35€ per month, for 50GB of free storage, 200 free hours of data transferred and 8 hours of free usage on a specific application.
- In all cases, if the user violates the laws and regulations he gets punished. The fine depends on the application he has violated and is defined in cooperation with the legislation that applies in the country the data center is located in.

4.2.2 Two Users, One Virtual Machine, One Company

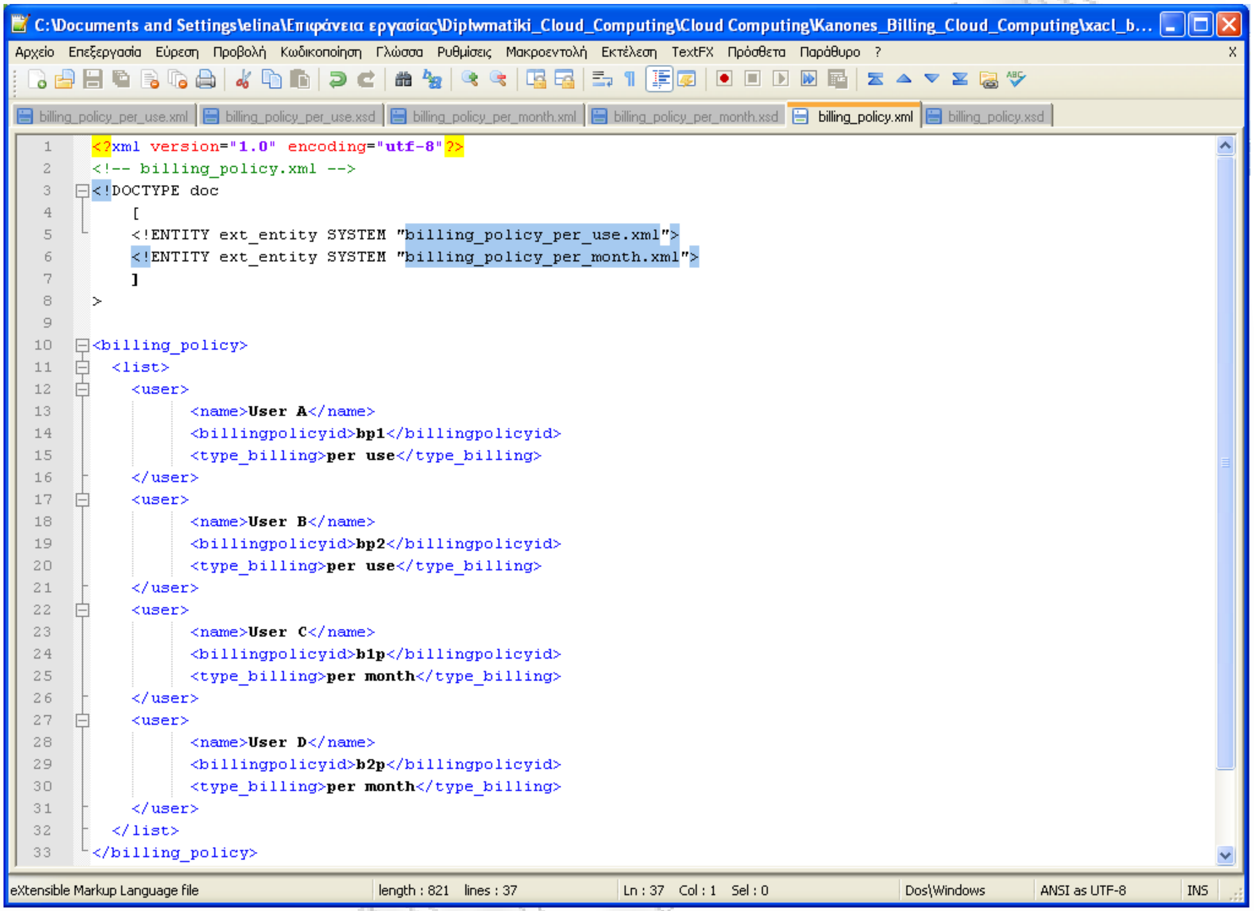
Supposing there are two users, who are in the same virtual machine, in the same cloud company but follow different billing policies according to the example billing policy from the previous section. More specifically, user A chooses to follow the pay-per-use model, while user B prefers the second way of charging, the monthly subscription. Comparing the two users during the period of a month, we come up with the below results:

User A (pay-per-use)	User B (monthly subscription)
The total cost is 25€ per month. Provisions: ✓ 20GB of free storage	The total cost is 30€ per month. Provisions: ✓ 25GB of free storage, ✓ 100 free hours of data transferred and ✓ 4 hours of free usage on a specific application

User A wishes to have the same provisions as user B, but he does not want to pay a lot of money. Therefore, he decides to attack user B so as to use his services for free. How should the cloud company deal with such incidents?

Based on the possible XML schemas defined previously, a cloud company could set billing policies through xml. According to the example, the produced XML files from the XML schemas are indicated below:

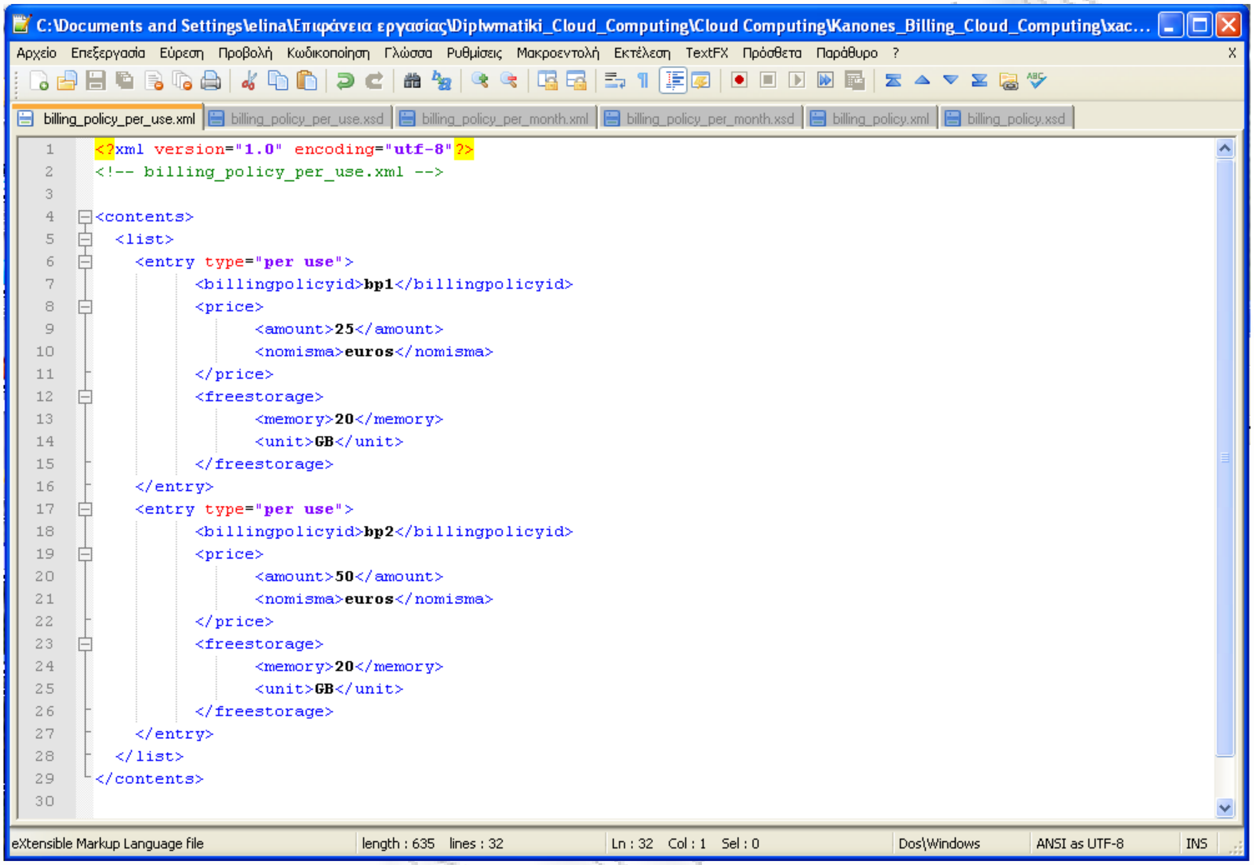
<u>XML file:</u> billing_policy.xml


C:\Documents and Settings\elina\Επιφάνεια εργασίας\Diplwmatiki_Cloud_Computing\Cloud Computing\Kanones_Billing_Cloud_Computing\xacl_b...
Αρχείο Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση TextFX Πρόσθετα Παράθυρο ?
billing_policy_per_use.xml
billing_policy_per_use.xsd
billing_policy_per_month.xml
billing_policy_per_month.xsd
billing_policy.xml
billing_policy.xsd
eXtensible Markup Language file
length : 821 lines : 37
Ln : 37 Col : 1 Sel : 0
Dos\Windows
ANSI as UTF-8
INS

```
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy.xml -->
<!DOCTYPE doc
    [
    <!ENTITY ext_entity SYSTEM "billing_policy_per_use.xml">
    <!ENTITY ext_entity SYSTEM "billing_policy_per_month.xml">
    ]
>

<billing_policy>
  <list>
    <user>
          <name>User A</name>
          <billingpolicyid>bp1</billingpolicyid>
          <type_billing>per use</type_billing>
    </user>
    <user>
          <name>User B</name>
          <billingpolicyid>bp2</billingpolicyid>
          <type_billing>per use</type_billing>
    </user>
    <user>
          <name>User C</name>
          <billingpolicyid>b1p</billingpolicyid>
          <type_billing>per month</type_billing>
    </user>
    <user>
          <name>User D</name>
          <billingpolicyid>b2p</billingpolicyid>
          <type_billing>per month</type_billing>
    </user>
  </list>
</billing_policy>
```

```
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy.xml -->
<!DOCTYPE doc
      [
      <!ENTITY ext_entity SYSTEM "billing_policy_per_use.xml">
      <!ENTITY ext_entity SYSTEM "billing_policy_per_month.xml">
      ]
>

<billing_policy>
  <list>
    <user>
              <name>User A</name>
              <billingpolicyid>bp1</billingpolicyid>
              <type_billing>per use</type_billing>
    </user>
      <user>
              <name>User B</name>
              <billingpolicyid>bp2</billingpolicyid>
              <type_billing>per use</type_billing>
    </user>
      <user>
              <name>User C</name>
              <billingpolicyid>b1p</billingpolicyid>
              <type_billing>per month</type_billing>
    </user>
      <user>
              <name>User D</name>
              <billingpolicyid>b2p</billingpolicyid>
              <type_billing>per month</type_billing>
    </user>
  </list>
</billing_policy>
```

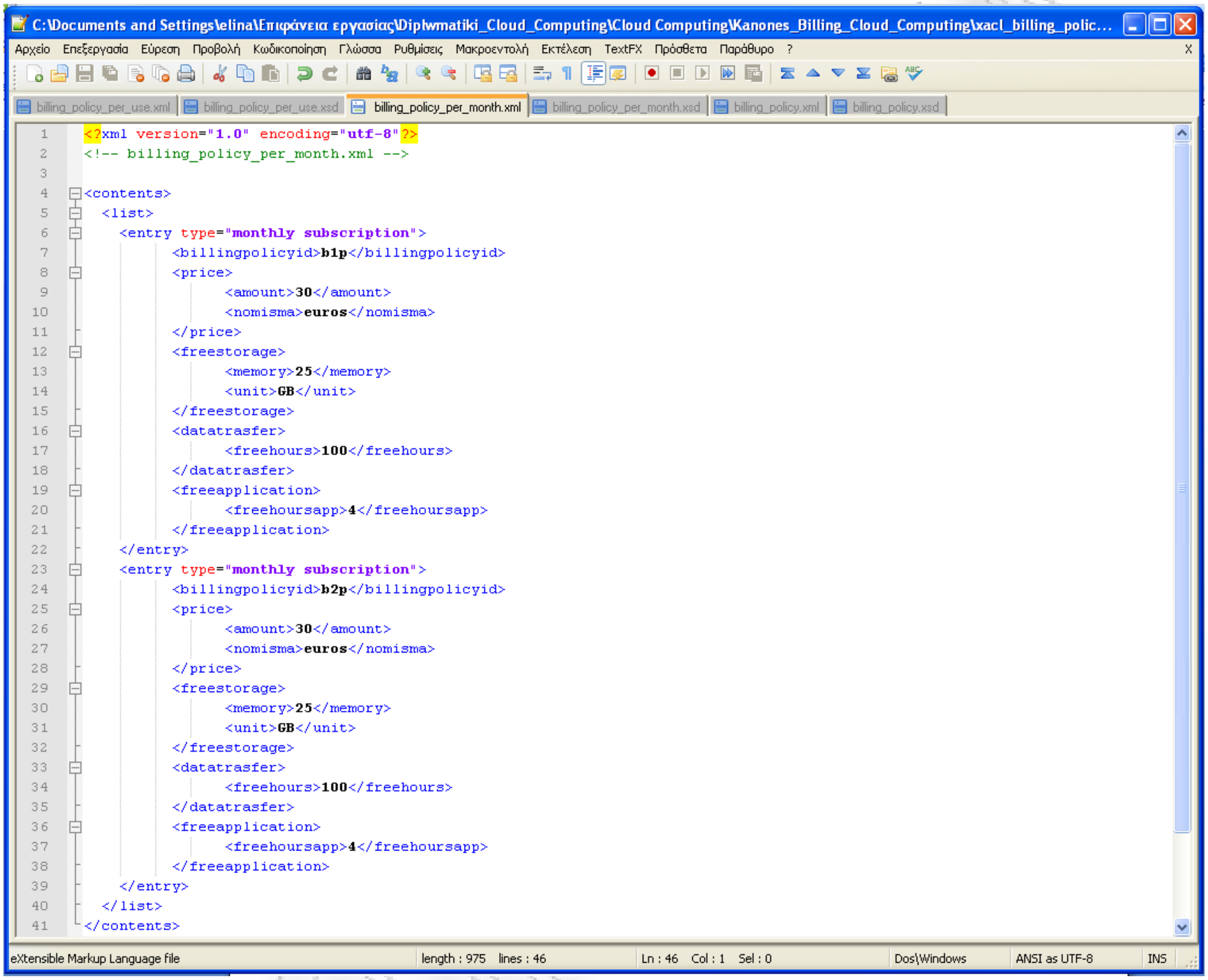
XML file: billing_policy_per_use.xml


C:\Documents and Settings\elina\Επιφάνεια εργασίας\Diplwmatiki_Cloud_Computing\Cloud Computing\Kanones_Billing_Cloud_Computing\xac...
Αρχείο Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση TextFX Πρόσθετα Παράθυρο ?
billing_policy_per_use.xml
billing_policy_per_use.xsd
billing_policy_per_month.xml
billing_policy_per_month.xsd
billing_policy.xml
billing_policy.xsd
eXtensible Markup Language file
length : 635 lines : 32
Ln : 32 Col : 1 Sel : 0
Dos\Windows
ANSI as UTF-8
INS

```xml
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy_per_use.xml -->

<contents>
  <list>
    <entry type="per use">
          <billingpolicyid>bp1</billingpolicyid>
          <price>
                <amount>25</amount>
                <nomisma>euros</nomisma>
          </price>
          <freestorage>
                <memory>20</memory>
                <unit>GB</unit>
          </freestorage>
    </entry>
    <entry type="per use">
          <billingpolicyid>bp2</billingpolicyid>
          <price>
                <amount>50</amount>
                <nomisma>euros</nomisma>
          </price>
          <freestorage>
                <memory>20</memory>
                <unit>GB</unit>
          </freestorage>
    </entry>
  </list>
</contents>

```

```xml
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy_per_use.xml -->

<contents>
  <list>
    <entry type="per use">
              <billingpolicyid>bp1</billingpolicyid>
              <price>
                        <amount>25</amount>
                        <nomisma>euros</nomisma>
              </price>
              <freestorage>
                        <memory>20</memory>
                        <unit>GB</unit>
              </freestorage>
    </entry>
    <entry type="per use">
              <billingpolicyid>bp2</billingpolicyid>
              <price>
                        <amount>50</amount>
                        <nomisma>euros</nomisma>
              </price>
              <freestorage>
                        <memory>20</memory>
                        <unit>GB</unit>
              </freestorage>
    </entry>
  </list>
</contents>
```

<u>XML file:</u> billing_policy_per_month.xml



C:\Documents and Settings\elina\Επιφάνεια εργασίας\Diplwmatiki_Cloud_Computing\Cloud Computing\Kanones_Billing_Cloud_Computing\xacl_billing_polic...
Αρχείο Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση TextFX Πρόσθετα Παράθυρο ?
billing_policy_per_use.xml
billing_policy_per_use.xsd
billing_policy_per_month.xml
billing_policy_per_month.xsd
billing_policy.xml
billing_policy.xsd
eXtensible Markup Language file
length : 975 lines : 46
Ln : 46 Col : 1 Sel : 0
Dos\Windows
ANSI as UTF-8
INS

```xml
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy_per_month.xml -->

<contents>
  <list>
    <entry type="monthly subscription">
          <billingpolicyid>b1p</billingpolicyid>
          <price>
                <amount>30</amount>
                <nomisma>euros</nomisma>
          </price>
          <freestorage>
                <memory>25</memory>
                <unit>GB</unit>
          </freestorage>
          <datatrasfer>
                <freehours>100</freehours>
          </datatrasfer>
          <freeapplication>
                <freehoursapp>4</freehoursapp>
          </freeapplication>
    </entry>
    <entry type="monthly subscription">
          <billingpolicyid>b2p</billingpolicyid>
          <price>
                <amount>30</amount>
                <nomisma>euros</nomisma>
          </price>
          <freestorage>
                <memory>25</memory>
                <unit>GB</unit>
          </freestorage>
          <datatrasfer>
                <freehours>100</freehours>
          </datatrasfer>
          <freeapplication>
                <freehoursapp>4</freehoursapp>
          </freeapplication>
    </entry>
  </list>
</contents>
```

```xml
<?xml version="1.0" encoding="utf-8"?>
<!-- billing_policy_per_month.xml -->

<contents>
  <list>
    <entry type="monthly subscription">
          <billingpolicyid>b1p</billingpolicyid>
          <price>
                <amount>30</amount>
                <nomisma>euros</nomisma>
          </price>
```

```
              <freestorage>
                        <memory>25</memory>
                        <unit>GB</unit>
              </freestorage>
              <datatrasfer>
                        <freehours>100</freehours>
              </datatrasfer>
              <freeapplication>
                        <freehoursapp>4</freehoursapp>
              </freeapplication>
    </entry>
    <entry type="monthly subscription">
              <billingpolicyid>b2p</billingpolicyid>
              <price>
                        <amount>30</amount>
                        <nomisma>euros</nomisma>
              </price>
              <freestorage>
                        <memory>25</memory>
                        <unit>GB</unit>
              </freestorage>
              <datatrasfer>
                        <freehours>100</freehours>
              </datatrasfer>
              <freeapplication>
                        <freehoursapp>4</freehoursapp>
              </freeapplication>
    </entry>
  </list>
</contents>
```

When we wish to manage and control the access that users have when they follow a specific billing policy we use XACL. XML Access Control Language (XACL) is an XML-based language. It is a standard for describing structured information and contents on the Internet and it provides authorization for XML documents [50]. It enables us to specify security policies such as if:

- a user is authorized to access confidential information, but the access must be logged
- a user is authorized to read sensitive information, but must sign a “terms and conditions” statement first
- unauthorized access is detected, therefore a warning message must be sent to the administrator

A possible XML document using XACL could be:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- billing_policy.xml -->

<contents>
  <list>
    <entry>
               ...
    </entry>
    <entry>
               ...
    </entry>
  </list>
<contents>

<policy>
  <xacl>
    <object href="/contents/list/entry"/>
    <rule>
      <!-- Αν το userID δεν είναι το ίδιο με του χρήστη κατά το login, δεν
      δίνει καθόλου πρόσβαση (read=deny, write=deny) -->
        <acl>
```

```
<action name="read" permission="deny"/>
<condition operation="and">
   <predicate name="compareStr">
           <parameter>neq</parameter>
           <parameter>
               <function name="getValue"/>
                       <parameter>./name</parameter>
               </function>
           </parameter>
           <parameter>
               <function name="getUid"/>
           </parameter>
   </predicate>
</condition>
<condition operation="not">
   <predicate name="logged">
           <parameter>
               <subject>
                       <uid>User A</uid>
               </subject>
           </parameter>
           <parameter>
               <object href="/contents/list/entry"/>
           </parameter>
           <parameter>
           <action name="write" permission="deny"/>
           </parameter>
   </predicate>
</condition>
<condition operation="not">
   <predicate name="logged">
           <parameter>
               <subject>
                       <uid>User B</uid>
               </subject>
           </parameter>
           <parameter>
               <object href="/contents/list/entry"/>
```

```
            </parameter>
            <parameter>
                 <action name="write" permission="deny"/>
            </parameter>
     </predicate>
  </condition>
  </acl>
<!-- Αν το userID είναι το ίδιο με του χρήστη κατά το login, δίνει MONO
πρόσβαση για read (read=grant) -->
  <acl>
  <action name="read" permission="grant"/>
  <condition operation="and">
     <predicate name="compareStr">
            <parameter>eq</parameter>
                 <parameter>
                    <function name="getValue"/>
                         <parameter>./name</parameter>
                    </function>
                 </parameter>
                 <parameter>
                    <function name="getUid"/>
                 </parameter>
     </predicate>
  </condition>
  </acl>
<!-- Αν το userID είναι το ίδιο με του χρήστη κατά το login, δίνει
πρόσβαση για read και write MONO αν το write είναι verify (read=grant,
write=grant) -->
  <acl>
  <action name="read" permission="grant"/>
  <action name="write" permission="grant">
     <provisional_action timing="before" name="log"/>
     <provisional_action timing="before" name="verify">
     <parameter>
        <SignedInfo>
         <CanonicalizationMethod
         Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"/>
         <SignatureMethod
```

```
          Algorithm="http://www.w3.org/2000/01/xmldsig/rsa-sha1"/>
          <Reference>
          <Transforms>
          <Transform
          Algorithm="http://www.w3.org/TR/1999/WD-xml-c14n-19991115"/>
          </Transforms>
          <DigestMethod
          Algorithm="http://www.w3.org/2000/01/xmldsig/sha1"/>
          </Reference>
          </SignedInfo>
      </parameter>
      </provisional_action>
   </action>
   <condition operation="and">
      <predicate name="compareStr">
          <parameter>eq</parameter>
          <parameter><function name="getUid"/></parameter>
          <parameter>
                  <function name="getValue">
                          <parameter>name</parameter>
                  </function>
          </parameter>
      </predicate>
   </condition>
</acl>
    <acl>
          <subject>
                  <uid>User A</uid>
          </subject>
          <action name="create" permission="deny"/>
          <action name="delete" permission="grant"/>
   </acl>
   <acl>
          <subject>
                  <uid>User B</uid>
          </subject>
          <action name="create" permission="deny"/>
          <action name="delete" permission="grant"/>
```

```
        </acl>
     </rule>
  </xacl>
</policy>
```

Conclusions

Cloud computing is a really rapidly widespread technology. It offers various benefits to its users but at the same time “hides” a great number of security risks, especially in the measured services (cloud billing system). There is an insufficient number of research papers which suggest both architectures and systems in the way the billing is implemented. Therefore, cloud billing still remains a big challenge for both customers and cloud providers as it is prone to exploitation, by malicious users who launch serious and dangerous attacks.

References

[1] S.E. Slack, Is there value in cloud computing?, March 2009, <http://www.ibm.com/developerworks/architecture/library/ar-valuecloudcomputing//?S_TACT=105AGX01&S_CMP=HP>.

[2] Adva Cloud Computing Final, ADVA Optical Networking FSP 3000 and cloud computing, February 2010, <http://www.slideshare.net/sc_online/adva-cloud-computing-final>.

[3] Peter Mell, Tim Grance, NIST, Effectively and Securely Using the Cloud Computing Paradigm, Information Technology Laboratory, July 2009, <http://www.cs.purdue.edu/homes/bb/cs590/handouts/Cloud_NIST.pdf>.

[4] Walter F. Witt, Keep Your Feet on the Ground When Moving Software into the Cloud, International Journal of Digital Content Technology and its Applications, Volume 4, Number 2, April 2010.

[5] Daniele Catteddu, Giles Hogben, ENISA, Cloud Computing: BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY, November 2009.

[6] Jon Brodkin, Gartner: Seven cloud-computing security risks, july 2008, <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0>.

[7] Haibo Yang, Mary Tate, Where are we at with Cloud Computing?: A Descriptive Literature Review, 20th Australasian Conference on Information Systems, Melbourne, December 2009.

[8] Ali Khajeh-Hosseini, Ian Sommerville, Ilango Sriram, Research Challenges for Enterprise Cloud Computing, <http://arxiv.org/ftp/arxiv/papers/1001/1001.3257.pdf>.

[9] Christof Weinhardt, Arun Anandasivam, Benjamin Blau, and Jochen Stößer, Business Models in the Service World, Germany, Published by the IEEE Computer Society, March/April 2009.

[10] Rituik Dubey, Muhammad Asim Jamshed, Xiaohui Wang, Rama Krishna Batalla, Addressing Security Issues in Cloud Computing, <http://www.contrib.andrew.cmu.edu/~rdubey/index_files/cloud%20computing.pdf>.

[11] Erik Elmroth, Fermın Galan Marquezy, Daniel Henriksson, David Perales Ferrera, Accounting and Billing for Federated Cloud Infrastructures, Spain, <http://www.computer.org/portal/web/csdl/doi/10.1109/GCC.2009.37>.

[12] Ki-Woong Park, Sung Kyu Park, Jaesun Han, Kyu Ho Park, THEMIS†: Towards Mutually Verifiable Billing Transactions in the Cloud Computing Environment, 2010 IEEE 3rd International Conference on Cloud Computing, July 2010, <http://www.computer.org/portal/web/csdl/doi/10.1109/CLOUD.2010.21>.

[13] IBM, IBM Point of View: Security and Cloud Computing, White Paper, November 2009.

[14] Luis M. Vaquero, Luis Rodero-Merino , Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, Volume 39, Number 1, January 2009.

[15] Wikipedia, the free encyclopedia, Cloud computing, <http://en.wikipedia.org/wiki/Cloud_computing>.

[16] Search Cloud Computing, Definition cloud computing, December 2007, <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>.

[17] James Staten, Is Cloud Computing Ready For The Enterprise?, Infrastructure & Operations Professionals, March 7, 2008.

[18] Martin LaMonica, Study: Cloud computing to brighten future of data centers, March 10, 2008.

[19] Tek-Tips, Defining Cloud Computing’s Key Characteristics, Deployment and Delivery Types, June 30, 2009, <http://tek-tips.nethawk.net/blog/defining-cloud-computings-key-characteristics-deployment-and-delivery-types>.

[20] Olafur Ingthorsson, Cloud Computing - What Are the Special Characteristics?, February 9, 2010, <http://ezinearticles.com/?Cloud-Computing---What-Are-the-Special-Characteristics?&id=3715149>.

[21] HPC Cloud Computing, What kinda apps are best suited for 'Cloud deployment' : 4 Solutions, <http://www.techpluto.com/cloud-computing-characteristics/>.

[22] Dave Malcolm Surgient, The five defining characteristics of cloud computing, April 9, 2009, <http://www.zdnet.com/news/the-five-defining-characteristics-of-cloud-computing/287001>.

[23] Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper, Cloud Computing Characteristics, Part of the Cloud Computing Cheat Sheet, <http://www.dummies.com/how-to/content/cloud-computing-characteristics.html>.

[24] Bob Tarzey, The difference between Saas, Paas and Iaas, 07 June 2010, <http://www.computerweekly.com/photostory/2240109268/The-Computer-Weekly-guide-to-Cloud-Computing/2/The-difference-between-Saas-Paas-and-Iaas>.

[25] L. Ertaul, S. Singhal, and G. Saldamli, Security Challenges in Cloud Computing.

[26] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009.

[27] WhatIsCloud.org, Cloud Deployment Models, <http://www.whatissoa.com/whatiscloud/p1.php>.

[28] Wikipedia, the free encyclopedia, Amazon Elastic Compute Cloud, <http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud>.

[29] Amazon Web Services, Amazon Elastic Compute Cloud (Amazon EC2), <http://aws.amazon.com/ec2/>.

[30] Tom Nolle, Introducing the key cloud computing platforms, May 2009, <http://searchcloudcomputing.techtarget.com/tip/Introducing-the-key-cloud-computing-platforms>.

[31] Armonk, N.Y. and Shanghai, IBM Introduces Ready-to-Use Cloud Computing, 15 November 2007, China, <http://www-03.ibm.com/press/us/en/pressrelease/22613.wss>.

[32] IBM cloud computing, <http://www.ibm.com/cloud-computing/us/en/>.

[33] Windows Azure platform, What is the Windows Azure platform?, <http://www.microsoft.com/windowsazure/>.

[34] David Chappell, Windows Azure platform, Introducing the Windows Azure Platform, October 2010, <http://www.microsoft.com/windowsazure/Whitepapers/introducingwindowsazureplatform/>.

[35] Google, What Is Google App Engine?, <http://code.google.com/appengine/docs/whatisgoogleappengine.html>.

[36] Wikipedia, the free encyclopedia, Force.com, <http://en.wikipedia.org/wiki/Force.com>.

[37] Wikipedia, the free encyclopedia, Salesforce.com, <http://en.wikipedia.org/wiki/Salesforce.com>.

[38] Francesco Maria Aymerich, Gianni Fenu, Simone Surcis, An Approach to a Cloud Computing Network, 2008.

[39] Expert Reference Series of White Papers, 10 Security Concerns for Cloud Computing, 2010.

[40] David Chou, Understanding Cloud Computing and Cloud-Based Security, March 9, 2010, <http://www.soamag.com/I37/0310-2.pdf>.

[41] Siani Pearson, Taking Account of Privacy when Designing Cloud Computing Services, May 23, 2009, Vancouver, Canada, <http://dl.acm.org/citation.cfm?id=1564628>.

[42] Ali Khajeh-Hosseini, Ian Sommerville and Ilango Sriram, Research Challenges for Enterprise Cloud Computing.

[43] CGI, Cloud billing: The missing link for cloud providers, White Paper, 2010.

[44] eVapt Monetization Platform : Billing & Metering, <http://www.evapt.com/products/products_billing&metering.php>.

[45] Rackspace Cloud Servers, How We Price Cloud Servers, <http://www.rackspace.com/cloud/cloud_hosting_products/servers/pricing/>.

[46] www.thecloudtutorial.com, Comparison of cloud computing organizations, <http://thecloudtutorial.com/cloudcomparison.html>.

[47] Amazon, Amazon Simple Storage Service (Amazon S3), Pricing, <http://aws.amazon.com/s3/#pricing>.

[48] Windows Azure Platform, Windows Azure Platform Consumption (Pay-As-You-Go), <http://www.microsoft.com/windowsazure/offers/MS-AZR-0003P?currency-locale=en-us>.

[49] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, Understanding Cloud Computing Vulnerabilities, MARCH/APRIL 2011.

[50] Hans-Dieter Wehle, Cloud billing service, An SOA-enabled billing service module for the cloud environment, IBM, 09 Feb 2011.

[51] Satoshi Hada and Michiharu Kudo, XML Access Control Language: Provisional Authorization for XML Documents, October 16, 2000, <http://www.trl.ibm.com/projects/xml/xacl/xacl-spec.html>.