CLOUD COMPUTING SECURITY ISSUES

Florin OGIGAU-NEAMTIU

IT Specialist
The Regional Department of Defense Resources Management Studies,
Brasov, Romania

The term "cloud computing" has been in the spotlights of IT specialists the last years because of its potential to transform this industry. The promised benefits have determined companies to invest great sums of money in researching and developing this domain and great steps have been made towards implementing this technology. Managers have traditionally viewed IT as difficult and expensive and the promise of cloud computing leads many to think that IT will now be easy and cheap. The reality is that cloud computing has simplified some technical aspects of building computer systems, but the myriad challenges facing IT environment still remain. Organizations which consider adopting cloud based services must also understand the many major problems of information policy, including issues of privacy, security, reliability, access, and regulation. The goal of this article is to identify the main security issues and to draw the attention of both decision makers and users to the potential risks of moving data into "the cloud".

Key words: *cloud computing, security risks, IT security, cloud models, services, cloud standards, risk assessment*

1. WHAT IS CLOUD COMPUTING

According to specialists [1] cloud computing is one of the most significant transformation in information technology with many advantages to both companies and end users. This technology promises to release the client from the burden of administering more and more complex and expensive systems by offering him the possibility of using systems with state of art computing capabilities, high availability and scalability.

Given the theorists', network architects', developers', managers', consumers', etc. constant scrutiny over this subject, there is a plethora of definitions that attempt to address the concept of *cloud computing*. Therefore, this article will use a generic definition which, even if not a comprehensive one, it will include the most important dimensions and variables. Thus, cloud computing is *a model of organizing computers for enabling convenient, ubiquitous, on-demand network access to a shared pool of configurable IT resources.* Cloud computing has the potential

to enhance collaboration, agility, scaling and availability and provides opportunities for cost reduction through optimized and efficient use of computing resources. The cloud model is a way of organizing computers so that resources can be quickly orchestrated, provisioned, implemented and decommissioned, scaled up or down to provide an on-demand service allocation.

The term **cloud** is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to represent the Internet in computer network diagrams as an abstraction of the complex infrastructure it represents. The unknown cloud is used here to represent the data center hardware and software which will be transparent to the client offering him the capability of focusing his efforts on the main activity.

This computing model appeared as a consequence of the development of parallel computing, distributed computing, grid computing, utility computing, all of them oriented on outsourcing computational needs.

2. THE CLOUD DELIVERY MODEL

The technology of cloud computing is based on a modern approach to software engineering called service oriented architecture (SOA). The technique focuses on the delivery of an integrated and orchestrated suite of functions to an end-user trough the use of different functions or services. These services are well defined functionalities that are built as software components and that can be used in different combinations to achieve different goals.

Cloud computing providers offer services built around three fundamental models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), as displayed in the **Figure 1.**

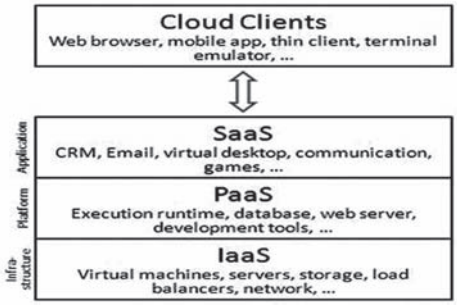

Figure 1: Cloud computing fundamental models
Source: www.wikipedia.com[2]

Infrastructure as a Service (IaaS) is the capability provided to the cloud user that provisions the processing, storage, networks, and other fundamental computing resources. All of the above enable the user to deploy and run arbitrary applications and even operating system software. The cloud user does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, etc. In this model, it is the cloud user who is responsible for patching and maintaining the operating systems and application

software. Infrastructure-as-a-Service is a platform through which businesses can avail equipment in the form of hardware, servers, storage space etc. at pay-per-use service. Examples include Amazon EC2, Terremark Enterprise Cloud, Rackspace, Microsoft Azure, etc.

Platform as a Service (PaaS) is the capability provided to the cloud user to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (e.g. Java, Python, .Net). In such a case the cloud user can develop and run its own software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. He cannot manage or control the underlying cloud infrastructure, network, servers, operating systems, or storage. Examples of such platforms are Google AppEngine, IBM SmartCloud Application Services, Amazon Web Services, etc.

Software as a Service (SaaS) represents the capability provided to the cloud user to use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin-client interface such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities, but only some limited user-specific application configuration settings. Examples include online word processing and spreadsheet tools, customer relationship management (CRM) services and web content delivery services (Salesforce CRM, Google Docs, Yahoo Email, Gmail, etc).

Viewed in terms of data security the three ways of service provision differ radically because of the extent to which the user has access to the software used and its settings.

3. CLOUD DEPLOYMENT MODELS

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways :

a. Private Cloud — the cloud infrastructure has been deployed, and is maintained and operated only for a specific organization. The cloud may be hosted within the organization or externally and is managed internally or by a third-party. This model does not benefit from the less hands-on management, nor from the economic advantages that make cloud computing such an intriguing concept.

b. Public Cloud — the cloud infrastructure is made available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial implications compared to the capital expenditure requirements normally associated with other deployment options.

c. Community Cloud — the cloud infrastructure is shared among a number

of organizations with similar interests and requirements. It can be managed internally or by a third party and hosted within the organization or externally. The costs are shared among fewer users than a public cloud. Hence a community cloud benefits from medium costs as a result of a sharing policy. By means of comparison, with the private cloud the costs increase alongside the level of expertise needed.

d. Hybrid cloud is a combination of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without being entirely dependent on third party services. Hybrid Cloud architecture requires both on-premises resources and off-site (remote) server based cloud infrastructure. Hybrid clouds lack the flexibility, security and certainty of in-house applications. However, they provide the flexibility of in-house applications with the fault tolerance and scalability of cloud based services.

4. THE RISKS OF ADOPTING CLOUD COMPUTING TECHNOLOGY

The process of creating and managing a secure cloud space is a more challenging task than creating a secure classical IT environment. Given the immaturity of this technology the new resources and the reallocation of traditional ones are not fully tested and come with new risks that are still under research.

The main risks of adopting cloud computing identified by this paper are:

a. Misunderstanding responsibilities.

If in a traditional scenario the security of data is entirely the burden of the company owning data. In the cloud computing scenario the responsibilities are divided between the two actors: the cloud provider and the client. There is a tremendous potential for misguided risk management decisions if cloud providers do not disclose the extent to which the security controls are implemented and the consumer knows which controls are further needed to be adopted.

Different kinds of cloud services adopted mean different responsibilities for the service provider and the customer. If an IaaS service model is adopted, then the provider is responsible for physical security, environment security and the virtualization software security, whereas the consumer is responsible for securing everything else above this layer including operating system, applications and data. However, in an SaaS cloud service model the provider is responsible not only for the physical and environmental security but also for all the software services he uses in order to provide that particular software service to the client. In this case, the responsibilities of the consumer in the field of security are much lowered.

b. Data security and confidentiality issues

One of the biggest security concerns people have when moving to the cloud is related to the problem of keeping data

secure and confidential. In this respect, some particular problems arise: who can create data, where the data is stored, who can access and modify data, what happens when data is deleted, how the back-up is done, how the data transfer occurs, etc. All of this is known as data security lifecycle and it is displayed in **Figure 2**.

Figure 2: The data security lifecycle
Source: www.securosis.com [4]

This lifecycle exists also in the classic architecture but in a cloud environment its stages are much more complex, posing higher security risks and requiring a more careful management. Worth reminding in this respect is that it is much more difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus be sure that the data is handled in a proper way.

To counter such a risk, strategies like data encryption, particular public key infrastructure, data dispersion, standardization of APIs, etc are proposed to customers as security measures to create a trusted and secure environment.

c. Lack of Standards

The immaturity of this technology makes it difficult to develop a comprehensive and commonly accepted set of standards. As a result, many standard development organizations were established in order to research and develop the specifications. Organizations like *Cloud Security Alliance, European Network and Information Security Agency, Cloud Standards Customer Council*, etc. have developed best practices regulations and recommendations. Other establishments, like Distributed Management Task Force, The European Telecommunications Standards Institute, Open Grid Forum, Open Cloud Consortium, National Institute of Standards and Technology, Storage Networking Industry Association etc., centered their activity on the development of working standards for different aspects of the cloud technology. The excitement around cloud has created a flurry of standards and open source activity leading to market confusion. That is why certain working groups like Cloud Standards Coordination, TM Forum, etc. act to improve collaboration, coordination, information and resource sharing between the organizations acting in this research field.

d. Interoperability issues

The cloud computing technology offers a degree of resource scalability which has never been reached before. Companies can benefit from additional computational needs, storage space, bandwidth allocation, etc. whenever they need and without great investments to support peak

load demands. If the demand falls back the additional capacity can be shut down just as quickly as it was scaled up without any hardware equipment sitting idle.

This great advantage has also a major drawback. It comes alongside with the risk of managing data within a shared environment (computation, storage, and network) with other cloud clients. Additionally, at one time one company may have multiple cloud providers for different services which have to be interoperable. In time, for different reasons, companies may decide to move their services to another cloud and in such a case the lack of interoperability can block or raise heavy obstacles to such a process.

Cloud providers may find the customer lock-in system attractive, but for the customers interoperability issues mean that they are vulnerable to price increases, quality of services not meeting their needs, closure of one or more cloud services, provider going out of business, disputes between with the cloud provider.

e. Reliability breakdowns

Another important aspect of the cloud computing is the reliability or availability of services. The breakdown of an essential service operating in a cloud has an impact on many clients. For example, in April 2012 there was a Gmail disruption that made Gmail services unavailable for almost 1 hour. The company first said that it affected less than 2 % of their customers, then they updated to 10 %, which sums around 35 million clients of a total of 350 million users. These incidents are not rare and evidence the customer lack of control over their data.

The irony is that, in terms of reliability, cloud providers have set high standards which are rarely achieved in an internal environment. However, because these outages affect large numbers of consumers it cast doubts in the minds of IT decision makers over the viability of replacing desktop functionality with the functionality offered by the cloud.

Also, in this industry, the leading companies have set some high level quality services. Those levels are not easy to be reached by the other cloud service providers which do not have such a well developed infrastructure. Unfortunately for the clients these quality services may come at higher costs and sometimes the decision makers, lured by the cheaper services, will be reluctant to collaborate with such a provider.

f. Malicious insider

A malicious insider is a person motivated to create a bad impact on the organization's mission by taking action that compromises information confidentiality, integrity, and/or availability. When sensitive data is processed outside the enterprise the organizational managers are less immediately aware of the nature and level of risk and they do not possess quick and direct capability to control and counter these risks.

Experienced security specialists are highly aware of the inverse

relationship between loyalty and risk. Even if trusted company employees can make mistakes or commit fraud and the outsiders are not automatically less ethical than them, it is prudent to invest company's long-term employees with higher trust.

The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data and services with impact on the internal activities, organization's reputation and customer trust. This is especially important in the case of cloud computing due to the fact that cloud architectures require certain roles, like cloud administrators, cloud auditors, cloud security personnel, which are extremely high-risk.

5. CONCLUSIONS

"Cloud" computing is based on technologies like virtualization, distributed computing, grid computing, utility computing, but also on networking, web and software services. The benefits of adopting this technology draw decision makers' attention and nowadays many companies are engaged in adopting or researching cloud adoption. Specialists who analyze this sector forecast that the global market for cloud computing will experience a significant increase in the next years and will replace traditional IT environment.

In the process of adopting cloud based services companies and IT organizations should evaluate the business benefits and risks. The cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The management of security risk involves users, the technology itself, the cloud service providers, and the legal aspects of the data and services being used. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective than traditional ones. To help reduce the threat, cloud computing stakeholders should invest in implementing security measures to ensure that the data is being kept secure and private throughout its lifecycle.

REFERENCES

[1] Bob Savage's speech delivered to Science Foundation Ireland's (SFI) forum, 'Science and Industry: Working Together for Economic Recovery',

http://www.siliconrepublic.com/cloud/item/24428-cloud-most-significant-tran, last retrieved 02.08.2012

[2]http://wikipedia.org/wiki/Cloud_computing last retrieved 04.08.2012

[3] http://www.vmware.com/solutions/cloud-computing/index.html, last retrieved 02.08.2012

[4] https://securosis.com/blog/data-security-lifecycle-2.0 last retrieved 15.08.2012

[5]http://www.redhat.com/solutions/cloud-computing/, last retrieved 15.08.2012

[6]http://softwarestrategiesblog.com/2012/01/17/roundup-of-cloud-

computing-forecasts-and-market-estimates-2012/, last retrieved 29.07.2012

[7] http://www.google.com/appsstatus, last retrieved 16.08.2012

[8] http://cloud-standards.org, last retrieved 10.08.2012

[9] http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview, last retrieved 13.08.2012

[10]http://royal.pingdom.com/2007/09/26/google-availability-differs-greatly-between-countries/, last retrieved 27.08.2012

[11]http://www.techrepublic.com/blog/datacenter/11-cloud-iaas-providers-compared/5285, last retrieved 05.08.2012