Luis Joyanes Aguilar
Professor of Languages and Information Systems
Engineering and Architecture Faculty
Pontificia University of Salamanca

CLOUD COMPUTING
NOTES FOR A SPANISH *CLOUD COMPUTING* STRATEGY

Towards a national cloud computing strategy for administration and companies

*Cloud Computing** is a buzzword that we are hearing more and more. Organizations see this technology as providing the solution to many economic and technology infrastructure problems.

Cloud computing (**SaaS, PaaS** and **IaaS)** is growing rapidly, and the cloud delivery and implementation models (**private, public, hybrid and community)** offered by a multitude of providers **have become** a common part of business strategy and research centre terminology

In this article we seek to analyze these models, which have become *almost* standard in the industry. We assess their advantages and disadvantages, and the main problems associated with cloud computing, such as **security, data protection** and **privacy.**

The USA has already published a federal *cloud computing* strategy, and the European Union is developing a similar strategy. Spain should be involved in developing this European strategy. In this paper we will examine the main *strategies* and propose some ideas for how organizations, companies and the public administrations might adopt the cloud:

digital agenda, *cloud computing*, IaaS, PaaS, SaaS, privacy, data protection, security.

* This concept is being translated into Spanish in two ways: either as "computación en nube" or "computación en la nube", and event as "informática en nube" or "informática en la nube". There is no unanimity about this in Spain and Latin America, with all of these forms being used indistinctly. However, there is agreement in organizations, companies and the media about how to represent this new model in simple terms.

1. HOW HAS *CLOUD COMPUTING* COME ABOUT?

Practically all large ICT (information and communication technology) companies have developed *cloud computing* strategies this decade. Leading telecommunications and internet companies, which are *per se* cloud companies, have done likewise.

And other sectors are gradually migrating in this direction.

The concept of the Cloud and its associated technologies emerged in 2008 and 2009, and took off as it reached the general public. Two of the world's leading magazines -*Business Week* and *The Economist*- had already foreseen the arrival of this architecture in 2008, analyzing cloud computing and its impact on corporations in depth[1].

We are facing a paradigm shift that IT departments are going to have to deal with. Managers need to consider how to acquire and distribute information in this environment, whilst protecting the interests of their companies. Innovative companies must take advantage of these new resources and reinvent themselves in their markets. Any who fail to do so may soon be left behind and, perhaps, out of business.

However, *cloud computing raises some major problems and controversial issues, such as data protection and user privacy.* Social and technology analysts are also asking whether *the computer as we know it will disappear, and whether it might be replaced by mobile phones, tablets or other devices.*

1 JOYANES, Luis . *Icade,* nº 76, January-April, 2009, p.96.

Is the PC dying?[2] ***Is the Web dying?***[3] ***Are we entering a post-PC world as the genius Steve Jobs and others have declared?***

Data and applications are stored in clouds of machines, hundreds of thousands of computer servers belonging to the Internet giants. This approach is gradually being adopted by hundreds of large companies, universities and public administrations, who want to have their own data centres available to their employees, researchers and graduates[4]. Cloud servers have made it possible for email to be read and stored remotely on servers, whilst photos and videos can be uploaded and downloaded and music can be listened to with '*audiostreaming*'. It is also used in *business* administration, using CRM (customer relationship management) software; these services are provided on payment of a fee.

We will also finally mention some of the technological innovations associated with the Cloud; these will lead to social transformations and unpredictable technological developments: the ***Web in real time, geolocation, augmented reality, fourth generation (4G) LTE mobile phone communications***, wireless technologies, **QR (bar) codes, NFC, RFID,** wireless sensors, USB standards, Bluetooth and the implementation of *Wifi* and *WiMax* networks. These will configure the future ***Internet of things.***

2. CLOUD COMPUTING DEFINED

This is not just a '*buzzword*': it represents a new IT model, which some analysts regard as being as significant as the Internet once was. It is also the best synonym of the Web itself. *Cloud Computing* is the evolution of a set of technologies impacting on the approaches organizations and companies take in setting up their IT infrastructure. As with the development of the Internet -with Web 2.0 and the Semantic Web- cloud computing is not about incorporating new technology. It is about powerful and innovative technologies being brought together to create this new Web model and architecture.

Reese states "whilst the Internet is a necessary basis, the cloud is something more important. It is a place where technology is used when it is necessary, and whilst it is necessary, not a minute more". You do not install anything on your desktop, and you do not pay for technology when you are not using it.

The cloud can be infrastructure or software. In other words, it can be either an application accessed from the desktop and run immediately after downloading, or it can be a server that is invoked as necessary. In practice, cloud computing provides either a *software* or *hardware* service.

2 GOMEZ, Lee and BULEY, Taylor (2009). "The PC is Dead" in *Forbes, 28* December 2009.

3 ANDERSON, Chris (2010). "The Web is dead. Long live the internet" in *Wired* (US, UK and Italian editions), October 2010, United Kingdom, pp. 125-131.

4 *Op. Cit.* pp. 95-111.

There is no universally accepted definition. However, there are several international bodies with responsibilities for standardizing information technology, particularly for *Cloud Computing*. One of the most prestigious of these is the National Institute of Standards and Technology (**NIST**)[5] and its Information Technology Laboratory, which defines *cloud computing*[6] as:

> "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to ... resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

The cloud is a combination of *hardware* and *software*, storage, services and interfaces that facilitate the provision of information as a service. There are many actors and participants in the world of the cloud. The stakeholders in cloud computing include: the *vendors or suppliers:* providing the applications and facilitating the corresponding technology, infrastructure, platforms and information; the *suppliers' partners:* these create *services* for the cloud, offering services to clients; *business leaders*: assess cloud services for implementation in their organizations and companies; and *end users,* who use cloud services, whether for free or on payment of a fee.

Cloud services are distributed (*multi-tenancy*); in other words, a number of companies can share the same basic resources. This is enabling companies to find new value, eliminating the complex restrictions inherent to traditional IT formats, such as issues of space, time, energy and costs.

2.2. The characteristics of *cloud computing*

NIST argues that the cloud model has five fundamental characteristics, three service models and four deployment models. The main characteristics are:

On-demand self-service. A consumer can supply themselves with server time and web storage as required, without needing any human communications with the service provider.

- **Ubiquitous web access.** Using standard devices, fostering usage of lightweight client systems (mobile phones, laptops, PDAs, tablets).
- **Resource distribution independent of position.** The supplier's computing resources are *"pooled"* to serve multiple consumers using a "*multi-tenant*" model, with different physical and virtual resources dynamically assigned and reas-

5 NIST is an Agency of the US Commerce Department. The NIST's Computer Security Resource Center (CSRC) is responsible for IT standards, particularly for Cloud Computing.

6 In October 2009, two NIST researchers, Peter Mell and Tim Grance, published a *draft* definition and guide for *cloud computing*, which they prepared working with the industry and government. This was entitled: "Effectively and Securely Using the Cloud Computing Paradigm", available on the NIST website at: http://crsc.nist.gov/groups/SN/cloud-computing/cloud-computing-v25.ppt.

signed in response to consumer demand. There is a sensation of independence of location, with the client normally having no control over or knowledge of the exact location of the resources provided. However, they may be able to specify this at a higher level of abstraction (country, geographic region or data centre). These resources include storage, processing capacity, memory, web bandwidth and virtual machines.

- **Rapid elasticity.** The *capabilities* can be provided rapidly and flexibly, often automatically. The way they are supplied makes them seem unlimited; that they can be acquired in any quantity at any time.
- **Measured service.** Cloud-computing systems automatically control and optimize resource usage, boosting capacity at an abstraction level suitable for the type of service (storage, processing, bandwidth and active user accounts). Resource usage may be monitored, controlled and reported on, providing transparency for both the provider and the consumer.

3. CLOUD MODELS

NIST classifies cloud computing models into two main categories:

- **Implementation models.** This refers to the position (location) and administration (management) of the cloud infrastructure (Public, Private, Community, Hybrid)
- **Service models.** This refers to specific services that can be accessed in a *cloud computing* set up (Software, Systems and Infrastructure as Services).

These technologies offer three *service models:*

1. ***Software.*** The user is offered the capacity of the applications supplied being implemented in a *cloud* infrastructure, with the applications being accessed using a web browser, as with webmail. This is perhaps the most widespread and representative example of this service model. The user has no control over the infrastructure or the applications, with the exception of any user configuration or personalization that is allowed.

2. ***System.*** The user can implement their own applications (whether acquired or developed by the user) in the supplier's *cloud* infrastructure, with the supplier offering the development platform and programming tools. In this case, the user has control of the applications, but not the underlying infrastructure.

3. ***Infrastructure.*** The supplier provides resources such as processing capacity, storage and communications that the user may use to run any *software,* from operating systems to applications.

The implementation models for cloud infrastructure and services can be classified as follows:

1. ***Private cloud.*** Services are not offered to the general public. The infrastructure is fully managed by an organization.

2. ***Public cloud.*** The infrastructure is operated by a supplier that offers services to the general public.

3. ***Hybrid cloud.*** A combination of two or more individual *clouds* that may be private, shared or public. This allows data and applications to be exchanged.

4. ***Community cloud.*** Organized to provide a common function or purpose. This must share common objectives (mission, politics, security). This may be administered either by its constituent organizations or by third parties. This is the model defined by NIST, although most organizations, suppliers and cloud users only accept the three deployment models: public, private and hybrid

4. THE CLOUD BUSINESS MODEL

This is fully focused on the key characteristics of cloud computing so as to foster the concepts involved (technology and revenue models). These business models can be applied equally to cloud suppliers and consumers. The supplier's business model is based on developing and facilitating cloud technology and solutions. This includes the following solutions[7]:

- *Cloud services* provide their computing and network infrastructure through platforms and solutions. Cloud service and solution providers are similar, making it possible for cloud services and solutions to be developed from the consumer's perspective. Cloud service providers include organizations that have their own data centres and those supported by virtualization services. Suppliers are varied and well established, taking advantage of their data centres and experience in data and application hosting.
- *Cloud service suppliers.* These provide cloud-based platforms hosted in specific system and infrastructure environments so that developers can access the platform, develop a new business application and host it on the cloud-based platform.
- *Technology providers.* These develop the tools and technologies to enable the cloud to become established, providing consumers with resources from the cloud. They offer a wide range of tools, technologies and operating systems to foster the deployment of public, private, hybrid and community clouds.

7 Eric A. Marks, Bob Lozano. Executive's Guide to Cloud Computing. New Jersey: Wiley, 2010. (pp.82-83).

- *Solution providers.* These develop full applications or *suites* to build a large market of cloud consumers (other telephony and internet operators)
- *Business models for consumers. These* companies apply cloud concepts to their business strategies.

They offer business management solutions.

5. THE MOBILE CLOUD: PRESENT AND FUTURE

Mobile cloud computing (or the mobile cloud) is a cloud processing model. Data is stored in the cloud and accessed using a mobile device for presentation or as a screen. Although many mobile devices can be used, this usually refers to smartphones. The ease of transporting tablets and their size has made these two terminals the most likely to be used with the mobile cloud.

The mobile cloud requires a reliable connection at the highest possible speed with excellent bandwidth, a mobile device with Internet access (at least 3G telephones using HSDPA, HSUPA or HSPA+ protocols, or 4G LTE devices) and a suitable browser for the device. Mobile cloud services have mushroomed over recent years.

There are obviously some major short-term challenges and opportunities. The capacity of 3G and the imminent 4G networks is not infinite. In addition to saturation, telephone operators and content providers are faced with an increasing need for specialization and the generation of new business lines due to the unavoidable need to implement efficient and profitable technological innovations.

A key issue for the mobile cloud at the moment is synchronization[8], enabling users to send messages, make calls and access every type of content using multiple devices and systems. Streaming music services and cloud storage*already* involves synchronization tasks. This applies not just to devices, but also to social networks.

Apple's *iCloud* synchronization service revolutionized this service and brought it to the general public. This allows the user to upload any data they want from their device to the cloud. The cloud automatically synchronizes this data and makes it available to all Apple devices, which was not previously possible in open models. Other examples include the popular instant messaging services for mobile phones, that can send text, photos, videos, audio, etc, working with any mobile operating system or device.

In summary, the mobile cloud integrates cloud computing with mobile computing. The intelligence of computers, applications and data is now in the cloud, whereas previously it had been stored on a PC hard disk.

Much of the business of the future will travel through the mobile cloud.

8 There are many signs that synchronization is one of the decisive factors in favour of the cloud. For example, in August 2011, HTC, one of the major manufacturers of mobile phones and tablets, bought Dashwire, a company known for its Dashworks synchronization system in order to exploit its synchronization services.

6. SECURITY: A WEAKNESS IN THE CLOUD?

Our first impression might be that taking hardware out of the picture makes the cloud feel less secure than traditional computing models. And in some cloud models, security control over these services is lost. However, if the supplier's security policies are well defined, and the user applies them faithfully, working in the cloud actually increases security

Unlike traditional computing, the user does not know exactly where the information is stored. Moving all information means *"relying on the security of others, which could be a cause for* concern. We can therefore pose a number of questions about safety strategy in the cloud:

- Where is the data used?
- How is it protected?
- Who is responsible for it?

The major cloud providers have a clear answer to this final question: the client is responsible for the data. IBM calls this type of security "*Secure by design*". This concept is that the environment should result from interaction between the service provider and the recipient.

Security must come from the client. When a company wants to put its data on the cloud, it must specify its preferences. Once these are known, the supplier can design a specific service for the company.

One of the most serious criticisms of the Cloud relates to data security and control. Organizations would seem to have greater control over data stored on their own infrastructure than data stored in the cloud. However, we must also consider legal requirements. The cloud can actually be safer than a traditional data centre, although methods for reinforcing information safety are radically different.

Cloud computing has a number of specific characteristics requiring risk assessment, such as data integrity, recovery and privacy, and legal issues relating to regulation and auditing information security systems.

Cloud risk assessment and security reviews must first consider the cloud implementation options (public, private and hybrid) and the service-delivery model (SaaS, PaaS, IaaS). Processes related to storage and virtualization in data centres are closely related to these models. As with the General Information Security Plan, no list of security controls could cover every eventuality; however, a risk-based approach can be adopted in moving or migrating to the cloud and selecting security options. There are two major categories of cloud implementation assets: data and applications.

7. CLOUD INFORMATION SECURITY OBJECTIVES

Developing secure software involves applying secure software design principles, which are the basic principles underpinning the software. This software underpinning is defined[9] as: "the foundations that enable us to have justified confidence that the software will have all the properties required to ensure that, when run, it will perform reliably, even with intentional failures. This means that it must be able to resist as many attacks as possible, containing the damage and recovering to a normal operating level.

The principles of cloud-based information system security are similar to those for Information Technology in general, but with cloud characteristics. These include **confidentiality, integrity** and **availability** (the security triangle; the main complements of which are authentication, authorization, audit, accountability and privacy.

7.1. Confidentiality

Preventing unauthorized material being revealed, whether intentionally or accidentally.

Confidentiality can be lost in many ways. Some of the telecommunications elements involved in achieving this include:

- Network security protocols
- Password verification
- Data encryption

In the cloud, confidentiality involves protection of data during transfer. The confidentiality policy defines the requirements for ensuring data remains confidential, preventing unauthorized releases of information. The information or data that can be exchanged must be defined. Some of the issues related to confidentiality include intellectual property rights, access control, encryption, interference, anonymity and coverage channels and traffic analysis.

7.2. Integrity

This ensures that the message sent is received and not altered. Data integrity must be ensured during storage and transfer. Data recovery measures must also be specified to correct any errors detected (deletion, additions and changes). This includes access control policies, who can transmit and receive data, and the information that can be exchanged.

Ensuring data integrity is of the utmost importance. Confidentiality does not in itself imply integrity: data may be encrypted for confidentiality purposes, but the user

9 Software Security Assurance Report.

may not have a mechanism to verify its integrity. Encryption is only sufficient for confidentiality. Data integrity also involves the use of authentication message codes.

Data integrity is particularly important in IaaS storage applications.

There are also costs involved in moving data to and from the cloud, and in network usage; these mainly relate to bandwidth. The client will want to check that the data is still on the web without having to download and then re-upload it.

7.3. Availability

In addition to confidentiality and integrity, we must also ensure that the data is available. *Availability* ensures reliable and timely access for appropriate people. It also ensures that systems are working appropriately.

Availability therefore involves elements that ensure reliability and stability in networks and systems. It ensures that connectivity is accessible when needed, permitting authorized users to access network and systems.

Threats to availability include malicious attempts to control, destroy or damage computing resources and to deny legitimate access to the system.

One of the major threats is network attacks, such as denial-of-service; another threat is service provider availability. No supplier can guarantee full availability.

Availability requirements must ensure that computing resources are available to authorized users when they are needed.

The opposites of confidentiality, integrity and availability are revelation, alteration and destruction.

One difficulty in assessing availability is ensuring that cloud storage suppliers will still be in the sector in the future; this is difficult to measure, and we must therefore rely on robust suppliers.

Practical considerations

Service Level Agreement (SLA) must include these three principles. SLAs have developed from weak positions. However, we consider that major suppliers will ensure compliance with each SLA.

8. SECURITY AS A SERVICE (SecaaS)

In 2011, the Cloud Security Alliance (CSA) published a report setting up the "Security as a Service Council" working group. This also defined the security categories considered to be services. Its objective was to identify the definitions of Security as a

Service and the resources involved, to classify the various types of security as services and to guide organizations in implementing best practices.

The CSA classifies security as services into the following categories:

- Identity and access management
- Prevention of data loss
- Web security
- Email security
- Security assessment
- Intrusion management
- Information security and event management
- Encryption
- Business continuity and disaster recovery
- Security network

9. DATA PROTECTION IN THE CLOUD

European Union Directive 1995/46/EC[10], on ***data protection***, https://www.privacyinternational.org/article/privacidad-y-proteccion-de-datos-en-la-union-europea-_ftn12, defines the basis of personal data protection that EU Member States must incorporate into their legislation. The Directive's provisions may be invoked in national courts against the data protection provisions of Member States, repealing any regulations that do not comply with the Directive. In Spain, personal data and privacy are protected by the Agencia Española de Protección de Datos (Spanish Data Protection Agency) and the Institute INTECO.

According to Inteco's guide for companies[11]: "*The lifecycle of data processed in the cloud is:*

- ***Data is prepared for the cloud by changing*** *its format or creating a file with all the information required.*

10 European Union legislation website: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm.

11 Observatorio de la Seguridad de la Información, *Guía para empresas: seguridad y privacidad del cloud computing"*. Leon (Spain): INTECO. 2011. (observatorio.inteco.es; www.inteco.es). INTECO is the Leon-based Instituto Español de las Tecnologías de las Comunicaciones (Spanish Institute of Communications Technology). Its main task is to monitor and help companies -mainly SMEs- with their security and implementation policies.

- ***The data "travels" to the cloud over an Internet connection****, using email, a specific application or transferring a backup copy to the cloud.*

- ***Data is processed in the cloud****, from storage to complex mathematical operations. Backup copies can be stored on the cloud for future access.*

- ***The resulting data "travels" back to the user.*** *When processing is complete, the data should be returned to the user with the added value of the information generated in the cloud. Data may represent a risk to privacy when leaving the organization: A person with malicious intentions could intercept data during transfer. However, the data is stored and processed in an IT infrastructure that is outside the user's control".*

The mechanisms for minimizing these privacy risks are very simple. Before we migrate data to the cloud, we should ask: "Do we need to transfer all of the organization's data to the cloud?" The Inteco Guide uses the example of a company involved in managing salary payments that decides to use cloud services. This company's database contains the personal information of thousands of workers. Inteco recommends that sensitive data should not be transferred to the cloud, recommending keys that correspond to the files stored on the company's servers.

Data protection and privacy are key to operating in the cloud. National and international laws should take precedence over any other considerations in agreements with suppliers. As practically all Western legislation includes data protection, we will focus on privacy problems in using the cloud and the need for this to be regulated. We will also examine the prevailing policies.

10. PRIVACY AND IMPACT IN THE CLOUD

Privacy is particularly affected by cloud computing. Many legislators, and distributors of cloud solutions, provide guidelines for privacy protection. Theft of a company's identity could result not just in loss of its privacy, but also serious damage to its image and reputation. In the short term, this might affect business results, but in the longer-term if might cause a loss of credibility or confidence and negative publicity.

The IT department often has responsibility for privacy control. However, business units should ensure that this is protected. Processes for cloud-computing and failure to respect the privacy of the organization and its employees should be standardized.

The concept of privacy-intimacy varies in different countries, cultures and jurisdictions.

Privacy[12] is defined as Personally Identifiable Information (PII), relating to the collection, use, storage and destruction of personal data. This is related to compliance with legal regulations and transparency in personal data usage. However, there is no consensus about what constitutes personal data. Let's look at the definitions given by major international bodies.

The Organization for Economic Cooperation and Development (OECD) defines privacy as: Any data relating to an identified or identifiable person; an identifiable person is one who could be directly or indirectly identified, particularly through reference to an identity number or one or more factors specific to their physical, psychological, mental, economic, cultural or social identity"[13].

There are a range or opinions on who is responsible for privacy and security. This is usually assigned to providers of cloud services through contractual agreements, such as Service Level Agreements (SLAs); however, the company responsible for the data cannot transfer its responsibility. In legal terms, the organization managing or owning the data is responsible for security failures. This is the case even when the user does not have the technical capabilities to ensure the contractual requirements with the cloud-service provider.

Experience shows that security and privacy issues have a cascade effect[14]. When an organization loses control over personal user information, the users are (directly and indirectly) responsible for subsequent damage. There can be a number of effects, such as identity theft, invasion of privacy and undesired soliciting.

New and novel threats are continuously arising. Protecting privacy in the cloud is therefore very complex and poses major challenges, although the privacy of data and applications in the cloud can be ensured to the same or even a higher degree.

11. THE EUROPEAN UNION'S PRIVACY PRINCIPLES

The European Union is one of the international organizations most concerned with protecting privacy on the Internet. It has set out some of the most advanced privacy protection principles in the world. Information transfers from the EU to other countries are annulled, if it is found that the receiving country does not have an equivalent degree of privacy protection. The EU's main privacy principles include[15]:

12 Spain's Royal Academy defines privacy as: "An aspect of private life that has a right to be protected from any intrusion" (www.rae.es).

13 www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.

14 *Ibid,* p. 150.

15 Current data protection and privacy policies can be consulted on the official European Union website at http://europa.eu/index_es.htm. For legal information, we recommend the EUR-Lex search tool at http://eur-lex.europa.eu/RECH_menu.do?ihmlang=en.

- Data can be compiled or collected in accordance with the law
- Information collected on a person cannot be divulged to other persons or organizations unless authorized by law or expressly agreed to by the individual.
- Personal data records must be accurate and up-to-date
- People have a right to correct errors in their personal data
- Data may only be used for the purposes for which it was collected, and must be used within a reasonable time period.
- Individuals have a right to receive a report on the information held on them.
- Transfer of personal data to third countries that do not ensure an equivalent level of protection EU must be prohibited.

These privacy policies are set out in full in EU Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Directive). One of the key propositions in this Directive is the restriction on transfers of personal data outside the European Union (or those countries regarded by the European Union as having similar data protection standards). The regulator's objective is to prevent organizations contravening privacy rules from transferring data to places where it is not legally protected. For this reason, organizations must assess cloud computing solutions very carefully, undertaking to find out whether the countries in which their data will reside are accepted by the European Union as having similar laws.

Updates to the EU Directive are published in the European Digital Agenda. The Directive contains a number of principles for permitting data transfer, including:

- The data subject unambiguously gives consent
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for the conclusion or performance of a contract, according to the needs of the data subject, between the controller and a third party.
- Processing is necessary or legally required in the public interest, or to establish, exercise or defend legal actions.
- Processing is necessary in order to protect the vital interests of the data subject.

12. THE RISKS AND THREATS OF CLOUD COMPUTING

The NIST (*National Institute of Standards and Technologies*) publication "*Guidelines on Security and Privacy in Public Cloud Computing*" describes the current status of this new model for distributing services and applications, and sets out the need to spread best security practices. This is not the only document to reflect the increasing concerns about security in such platforms, and other influential bodies have also issued reports in this area.

The "*Riesgos y amenazas en el Cloud Computing*" report by INTECO[16] summarizes some of these documents to give an overview of the threats, risks and key aspects of security in the *cloud*. The report describes *cloud* infrastructure and services and analyses the various security concerns in the light of international criteria and standards. The concerns raised in these reports focus on **data management**, particularly with regard to ownership and how data is processed and handled. The analysis in the report gives an overview of the problems and draws conclusions that are common to all points of view.

One of the key aspects is **data ownership and security**. The reports pay particular attention to data ownership and processing, as the infrastructure could be managed in multiple countries, and this could give rise to conflicts in the legal framework to which they are subject. These environments also process huge quantities of data, and this could give rise to information leaks, whether intentional or accidental.

Regulatory compliance is also one of the keys to security in a *cloud environment.* This is due to the lack of transparency with this infrastructure; the subscriber should therefore inform themselves clearly about how the environment is managed.

A range of software from different providers is involved in creating a *cloud* service. This is a **complex environment, and** potential vulnerabilities must be monitored and patched as necessary. Another important aspect is **identity and access control**. In general, infrastructure is shared by multiple companies and users, and poor set up could lead to unauthorized access to confidential data. An appropriate identity and access control policy must be defined based on minimum privilege levels for *cloud* environments.

Finally, **service level agreements (SLA) are a common denominator**. All recommendations state that these must be reviewed and created specifically, detailing controls, regulations, protection measures and service recovery periods. ENISA, the European Union Security Agency, has recently published specific regulations for cloud contracts.

16 INTECO www.inteco.es. This INTECO report is based on the ENISA (European Network and Information Security Agency) report **Security and Resilience in Governmental Clouds.** ENISA: www.enisa.europa.eu/.

13. *CLOUD COMPUTING* IN THE WHITE HOUSE

The *ReadWriteWeb*[17] technology website has published a report on a *White House* initiative supporting *Cloud Computing*. In July 2010, Barak Obama's technology advisor Vivek Kundra presented *cloud computing* to Congress as an essential part of the Government's technological infrastructure.

Kundra focused on four points:

- Government IT is outdated and sometimes antiquated
- Federal data centres now number more than 1,000. The private market is cutting back in data centres through private *clouds,* hybrids and public services.
- Cloud-based, data driven services can drive policy. This requires platforms that provide a base for interaction between constituents and stakeholders in federal agencies. Interoperability between agencies across platforms requires cloud-driven services with core sets of standards.
- Transparency means the capability to get real-time access to public data.

Cloud computing makes it possible to interact with the Federal Government using data to generate ideas and transform debates about public policy issues. One example of this is the cloud-based **data.gov** service. **usaspeding.gov** is another major cloud-based service aiming to increase transparency.

13.1. The White House *Cloud Computing* Strategy

The White House launched its federal Cloud Computing strategy guide for incorporating this model into federal bodies in 2011. This document[18], which Kundra coordinated, defined the *cloud computing* concept and the impact it would have on savings and service levels in the federal government.

This was the result of policies implemented since 2010 to facilitate the migration of US government services to the cloud.

The US government requires federal agencies to use cloud-based services when there is a secure, appropriate and economically advantageous solution. The strategy states that all of its Agencies must adjust their budgets incorporating the cloud, reassessing all processes that are inefficient.

17 *ReadWriteWeb.com*, 05/07/2010.

18 The document is available at: www.cio.com/documents/Federal-Cloud-Computing-Strategy.pdf.

The strategy states that cloud computing provides intangible benefits to the public, such as viewing their electricity consumption *online, to help* private consumers regulate their usage; sharing of medical records in different locations and by different specialties etc.

13.2. Federal *Cloud-Computing Initiative*

The Federal Cloud Computing Initiative (FCCI) was published in May 2011. As a result, the Government held a *public* tender for cloud-service providers. This tender covered a range of services:

- **EaaS** (email as a service)
- Office automation (office software)
- Cloud storage services (virtual hard drives)
- Professional services

Based on the implementation of the cloud, the tender stated that services should be offered in three forms: the Government Community Cloud, private clouds and public clouds.

13.3. Practical considerations for fostering *cloud computing* in the USA

In 2011, Vivek Kundra stated[19] that migrating federal services would save billions of dollars in computing costs.

The US Federal Government is the largest IT purchaser in the world, spending over 80 billions dollars per year. It plans to close 40% of its data centres (800 out of 2000) over the coming four years to reduce its technology spend and modernize the way it uses computers to manage data and provide services to the public. Kundra has said that reducing the number of data centres is part of a wide-ranging strategic approach to computing in the Internet era; the Government is migrating to the cloud, where users use remote applications, such as email. External technology agencies or companies can provide these cloud services to the government. This will enable the Government to save 5 billions dollars per year by reducing hardware and software demands in government agencies. The cost saving on data centres is estimated at 3 billion dollars per year;

As a sign of this migration to the cloud, around 140,000 federal employees have moved to cloud-based email, saving around 42 million dollars per year.

19 Steve Lohr in an New York Times interview on 20 June 2011. http://www.nytimes.com/2011/07/20/technology/us-to-close-800-computer-data-centers.html [as of 20-07-2011].

14. THE EUROPEAN UNION *CLOUD COMPUTING* STRATEGY

The EU approved its European Digital Agenda in 2010[20]. *Cloud Computing* was one of the strategic trends covered.

The Granada Declaration recognizes *Cloud Computing* as a strategic sector where Europe has substantial market potential. Usage of *cloud computing is increasing.* The European Commission estimates that cloud services will generate around 35 billion euros of revenue in 2014.

Following a number of official announcements, a consultation was carried out in Brussels in 2011 to collect information for the development of a European *cloud computing strategy.* Commissioner Kroes' idea was to "engage major cloud users to look for opportunities for a coordinated move on standardization to support interoperability and portability of data".

Kroes has repeatedly stated that *cloud computing* is a major opportunity for the public sector.

Continuing work towards the launch of a European cloud strategy, on 2 April 2012 ENISA issued a press release announcing its Guide for monitoring cloud computing contracts to increase information about security criteria for service agreements.

15. CONSIDERATIONS FOR A SPANISH CLOUD COMPUTING STRATEGY

In line with the EU strategy, the Spanish Digital Agenda will set out objectives, areas for development and measures to promote the Information Society during the parliament. The Ministry of Industry has set up a Senior Steering Group for the Digital Agenda, which met for the first time in May 2012. This body is responsible for proposing and sponsoring measures to develop the Government's telecommunications and information society strategy, the Spanish Digital Agenda.

Spain has a number of general objectives, and will develop a number of lines of actions through specific measures to achieve each of these. The Ministry of Industry's recent pronouncements state that these priority areas will be *smart cities* and electronic commerce.

As with the EU, we propose that this should also include a Spanish cloud computing strategy, incorporating guidelines emanating from European strategy.

20 The European Digital Agenda was published as the conclusion of the Granada Declaration at the meeting of IT ministers held on 18 and 19 April 2010 in Granada. This Agenda was subsequently approved.

16. THE FUTURE IS IN THE CLOUDS

The three main global events (the CES Fair in Las Vegas, the World Mobile Congress in Barcelona and the CeBIT, IT fair in Hannover) set the trends followed by organizations and companies, predicting social and technological changes. 2012 was no exception. All three events focused on the cloud as the dominant technological architecture. This trend has been confirmed by a number of respected reports: *cloud computing* is taking over in business, industry, the media…

Moreover, the cloud will incorporate more and more services offered by large companies, and by SMEs, as it is their natural habitat.

The cloud of services and data will be used by organizations and companies and by private consumers to reduce infrastructure and maintenance costs, by transferring some hardware and software costs to the cloud. Physical storage will gradually cease to be in private units and will also move to the cloud.

Full migration will gradually come about as scalability (extension of the technological needs of companies with no loss of quality) improves, and as cloud services and mobile and social media applications gain in popularity.

The three most widely known cloud services -IaaS, PaaS and SaaS- will be offered by multiple providers, making decisions easier.

We should note the change in mentality that cloud storage will bring about; sites such as iCloud, Amazon Drive, Dropbox, SugarSync, SkyDrive, Box.com, Strato and the planned Google Drive will continue to offer solutions that make life easier for people, organizations and companies.

Cloud IT projects must however ensure ***security***, choice of suppliers, scalability, assessment (the chance to test the service prior to contracting), the implementation of flat-rate fees, service level agreements (SLA), ***and data protection and privacy.***

Cloud Computing has matured, and can now continue to grow constantly. News about the Cloud will be appearing non-stop in the press and on radio and television, further promoting the model and its main forms. In all likelihood, cloud computing will be the driver of the computing of the future

The dominant trends will be **mobility** and **ubiquity**. There will soon be two billion mobile phone users, and the devices will become more and more intelligent; the number of Internet users is expected to reach five billion in the decade. Most Internet users will connect to the cloud to download web programs and applications, any time, anywhere, and using any device: "ubiquity is a becoming an achievable dream through the Internet, the Web and, in particular, the Cloud".

In conclusion, it is not that the "***future is not what it was***", as my beloved Groucho Marx put it, but that the future has arrived. The future is here and it uses the cloud, which will become the focal point of the new digital universe.

BIBLIOGRAPHY

BANKINTER/ACCENTURE (2010). *Cloud computing. La tercera ola de las Tecnologías de la Información.* 2010. [Available at: www.fundacionbankinter.org].

CIERCO, David. (2011). *Cloud Computing. Retos y oportunidades.* FUNDACIÓN IDEAS, 2011. [available at: www.fundacionideas.org].

NIST. *Guidelines on Security and Privacy in Public Cloud Computing*. NIST, 2011.

ENISA (2011). *Seguridad y resistencia en las nubes de la Administración Electrónica.* Brussels: ENISA, January 2011. Translated from the English by INTECO under the direction of Daniele Catteddu. [Available at www.inteco.es].

INTECO-CERT , (2011). *Riesgos y amenazas en cloud computing*. March 2011. [Available at www.inteco.es].

JOYANES, Luis (2009*a*) "La Computación en Nube *(Cloud Computing)*: El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento" en *ICADE,* nº 77, January-March 2009, Madrid: Pontificia Comillas University.

JOYANES, Luis. (2009*c*). *Company 2.0 seminar: Integration of Web 2.0 and Cloud Computing into the company.* Madrid: Corenetworks [online: www.corenetworks.es].

KRUTZ, Ronald L. and DEAN VINES, Russell (2010). Cloud Security. A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley.

KUNDRA, Vivek, (2011). *Federal Cloud Computing Strategy.* Washington: The White House, February 2011.

MARKS, Eric A. and LOZANO, Bob. (2010). *Executive's Guide to Cloud Computing*. New Jersey, Wiley.

MATHER Tim *et al*. (2009). *Cloud Security and Privacy.* Sebastopol: O'Reilly.

NAHARI, Hadi y KRUTZ, Ronald L. (2011). Web Commerce Security. Design and Development. Indianapolis, Wiley.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* March 2011. INTECO-CERT**.** [Available at www.inteco.es].

VELTE, Anthony T. *et al* (2010). *Cloud Computing. A Practical Approach.* New York: McGraw-Hill.