An Overview of the Most Important Reference Architectures for Cloud Computing

Răzvan ZOTA, Ionuț Alexandru PETRE
The Bucharest University of Economic Studies
zota@ase.ro, ionut_petre33@yahoo.com

In this paper we have presented the main characteristics of the most important reference architectures designed for the cloud computing environment. Specifically, we have introduced the proposed architectures of the worldwide cloud computing companies like Cisco, IBM and VMware and we also had a look at the National Institute of Standards and Technology (NIST) reference architecture which is the starting point for all proposed architectures in the field. As one would expect, the provider dependent reference architectures are written is such a way to suit the services and products of the company, while NIST's architecture is a more general model with more comprehensive architectural details that we highlighted in this article. In the end of the article we draw out some conclusions regarding the existing reference architectures for cloud computing.

Keywords: *Reference Architecture, Cloud Computing, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).*

1 Introduction

Cloud computing is the new term used for utility computing, with emphasis on offering IT resources over the Internet, in exchange of storing and operating resources locally. In the existing literature there are a plethora of different reference architectures, models and frameworks for cloud computing. Usually, a reference framework for cloud computing tries to offer the baseline that stands on designing some interoperable cloud services and also their integration in the existing infrastructures of the Internet and private corporations. On a regular basis, a reference framework should offer a draft or an architectural template that could be used by others that wish to adopt similar solutions. A reference model consists in explaining the concepts and relationships which sustain reference architecture, while the term reference framework refers to both (architecture + model of reference) [1]. A cloud computing architecture of a cloud like solution represents the structure of such a system. The term also refers to conceiving proper documentation of the architectural system of a cloud computing solution, facilitating the communication between the investors, taking initial decisions and it also allows the reuse of the design components and templates for other similar projects [2].

A reference model of cloud architecture represents the abstracting of the cloud computing concepts and relationships, which can be used to train organizations and to create standards and guidelines in the purpose of aiding these application concepts. Groups of organizations like DMTF (Distributed Management Task Force) – are the initiators of a wiki page www.cloud-standards.org [3]. Cloud Security Alliance or Open Security Architecture develops reference models for cloud which can be used by different companies in the purpose of adopting new cloud technologies. Also, companies being active in the field (Cisco, IBM, VMware and others), also other federal agencies (GSA and others) are working on some reference models of their own which have specific characteristics. Next we will present four of the most important reference architectures in the field:

- Reference architecture CISCO - Cisco Cloud Reference Architecture Framework [4]
- Reference architecture IBM – IBM CCRA [5]
- Reference architecture National Institute of Standards and Technology (NIST) [6]
- Reference architecture VMware - Architecting vCloud [7]

DOI: 10.12948/issn14531305/18.4.2014.03

2 CISCO reference architecture

The CISCO reference architecture is based on the cloud definition provided by NIST, in which is stated, shortly, that a cloud represents IT services offered using a network. More precisely, the cloud is a model in which the IT resources and services are abstracted from the infrastructure and are provided "on demand" and "at scale" in an environment for multiple "tenants". "On demand" stands for resources which can be supplied and billed for only when they are used. "At scale" refers to the fact that the provided services offer an "infinite" pool of available resources which can provide for various demands. An environment with "multi-tenants" assumes that the resources are available for use for multiple consumers (for example, business units) in one implementation.

As a reference framework Cisco follows the NIST model for the cloud, with different services (IaaS, PaaS and SaaS) and the four deployment models in the cloud: private, public, hybrid and community could. Cisco talks about some of the benefits of a cloud based solution, which include mainly an increased efficiency and agility in IT. It mentions some of the basic elements of developing in the cloud which include the general steps of *virtualization*, *integration*, *automation* and finally *cloud service offerings.* After presenting these general steps Cisco shows the Cisco cloud strategy for Enterprises which contain 3 essential points:

- It offers products, services and solutions for enterprises to build a secure cloud;
- It allows enterprises to supply secure cloud solutions and services to internal clients;
- It contributes to the cloud marketplace by promoting innovative technologies, open source standards and ecosystems development.

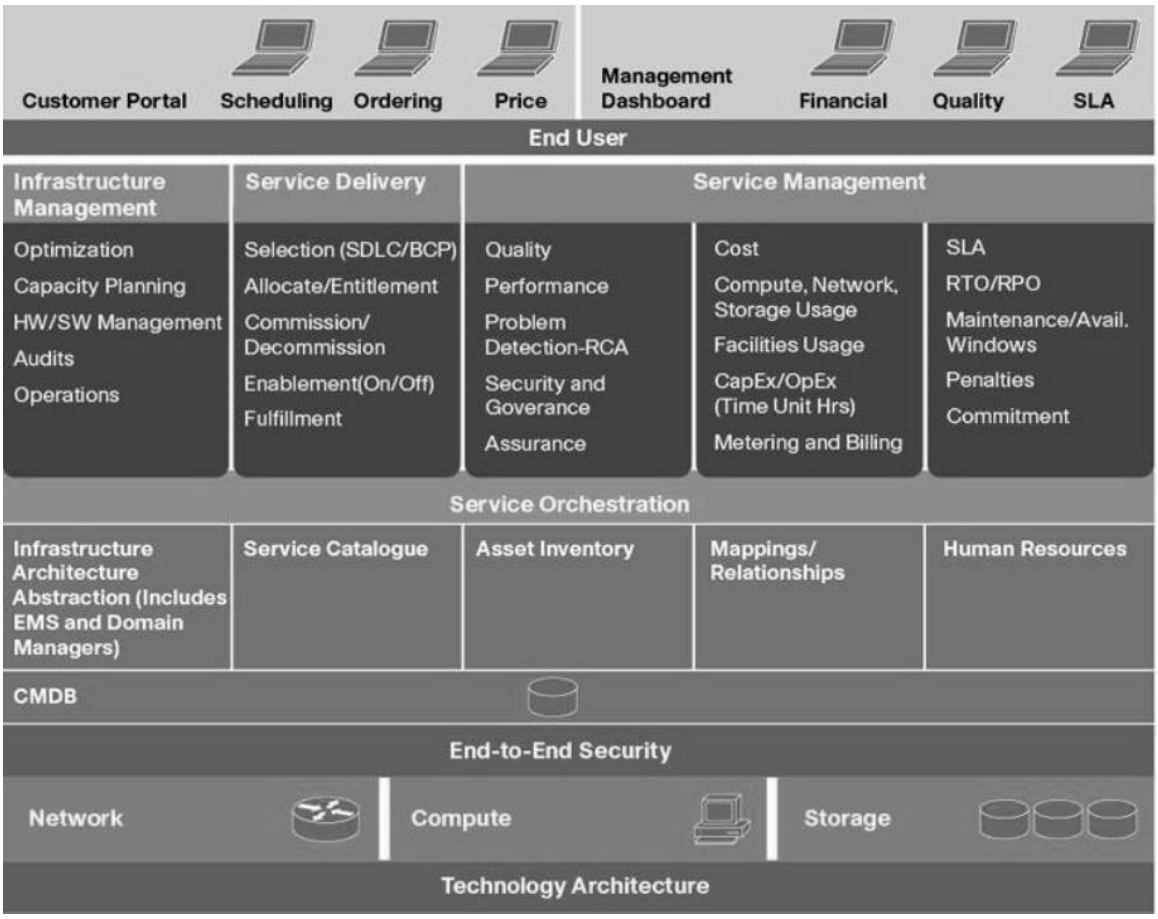

Fig. 1 Cisco's cloud computing reference architecture (Source: [4])

DOI: 10.12948/issn14531305/18.4.2014.03

Cisco Virtualized Multi-Tenant Data Center (VDMC) presents architecture and an end-to-end design for a complete solution for a private cloud with IaaS. VDMC consists of multiple design components for the cloud beginning IT infrastructure and ending with management and configuration components. The base construction blocks relies on stacks of integrated infrastructure parts, which can be combined and scaled; in this direction there is mentioned *Vblock™ Infrastructure Packages* from VCE coalition (VMware, Cisco, EMC) and also Secure Multi-Tenancy stack (SMT) which is being developed in partnership with NetApp and VMware.

The solution is built on top of a framework for providing services which can be used for hosting services outside IaaS on the basis of the same infrastructure: for example, virtual desktop infrastructure – VDI. The VDI solution from Cisco provides a complete infrastructure for an enterprise leading to an increase of control and security over data. Also it offers an easy migration to other new desktop operating systems and it assures control over operational expenses and capital. Cisco's solutions for building a private cloud can be used also by service providers to build cloud infrastructures so they can provide public, private and hybrid solutions for their clients. In communication with service providers and companies Cisco is developing an ecosystem for cloud providers, developers and consumers. This ecosystem has the advantage of using common approaches to cloud technology, administration, interconnection and operation in the cloud.

3 IBM reference architecture

The proposed reference architecture from IBM is called IBM CCRA (Cloud Computing Reference Architecture). It was defined in 2009 and it is continuously being improved. This solution is based on clients experience in implementing cloud hosted solutions by IBM along the years, offering guidelines for building IaaS, PaaS, and SaaS for using IBM's products. IBM CCRA is reflected in the design of IBM's cloud, developing for clients, hosting services and in IBM's products with a focus for reducing costs and obtaining a high rate of security, reliability, scalability and control.

IBM CCRA [5] consists of multiple documents, which presents the current state of knowledge in the field at the moment and it provides ideas for architecture and design for implementing cloud based solutions. Like Cisco's reference architecture white paper, IBM's presentation also starts with a brief summary of the benefits brought to the clients by using their cloud solutions. IBM CCRA saves time and money for clients by providing detailed documentation about the steps and the necessary components for building a cloud implementation for any type (public, private and hybrid). Clients can use IBM's experience with building public, private and hybrid cloud systems which are based on a common architecture with reusable entities and product recommendations.

Clients benefit with a faster start for building a cloud system which contains predefined cases and documentation that refers to architectural requirements or decisions that need to be made for security, service management, performance, scalability and virtualization. The increased flexibility of the business is another advantage of using common reference architecture for known models (public, private, and hybrid).

The last version, IBM CCRA 3.0, offers a series of new benefits, these are:

- Prescriptive guidance for designing IaaS, PaaS, SaaS solutions by using IBM's products.
- Consists of various architectural products which represent the best options in IT industry in regard of designing, implementing and administration roles and permissions in the cloud for consumers, service providers and builders of cloud services.
- Represents a modular framework which allows focusing on the most important field for cloud development (IaaS, PaaS, SaaS, and CSP).
- It offers a comparative sketch with the scope of realizing an analysis of the clients of the cloud with the goal of identifying integration points.

DOI: 10.12948/issn14531305/18.4.2014.03

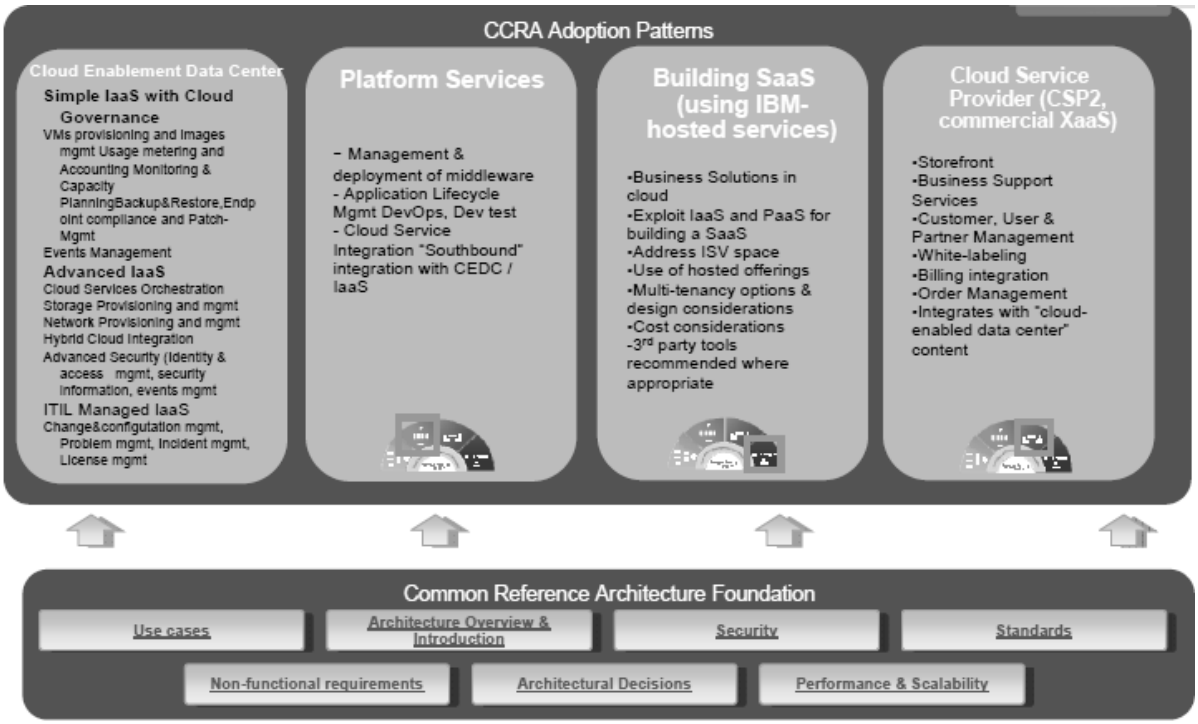

Fig. 2 A model for adopting IBM CCRA (Source: [5])

In Figure 2 we can see the proposed model for adopting IBM CCRA 3.0, based on four models which contain:

- Business drivers
- Actors and user stories
- Non-functional requirements
- System context
- Architectural decisions
- Overview of the architecture
- Components model
- Operation model
- Steps to follow

Also within this IBM architecture there are also documents for:

- General description of the architecture
- Roles and user stories
- Non-functional requirements
- Architectural decisions
- Security
- Performance and scalability
- Hybrid cloud
- Used standards

4 NIST reference architecture

4.1 Introduction

National Institute of Standards and Technology (NIST) - The national institute of standards and technology of the department of commerce in USA provided a document called "NIST cloud computing standards roadmap" [6], which contains: NIST's vision over the notion of cloud computing, a reference architecture for the cloud, some case studies, cloud computing standards and mapping them in contexts regarding security, interoperability and portability, as well as an analysis of the case studies for identifying gaps in standards elaboration.

NIST's definition for the cloud is unanimously accepted and it provides a clear understanding about cloud technologies and services. The reference architecture which is given by NIST comes as a normal follow up of NIST's cloud computing definition. NIST's reference architecture is a high-level conceptual generic model that represents a powerful tool when it comes to talking about requirements, structures and operation in cloud computing. The model does not fold to characteristics or requirements of producers or developers of the cloud and it does not define a prescriptive solution that inhibits innovation. This model defines a lot of actors, activities and functions which can be used in the process

DOI: 10.12948/issn14531305/18.4.2014.03

of development in the cloud computing relating with a taxonomy of the cloud computing. It contains a series of opinions and descriptions which are the base of a talk regarding characteristics, usages and standards in the cloud computing field.

The NIST reference architecture focuses on the needs that the cloud services offer and not on a design that defines a solution and an implementation. This helps with understanding operational complications that can occur in the cloud computing. NIST reference architecture does not represent system architecture of a system specific to cloud computing, it is rather a tool for describing, analyzing and development of a specific architecture using a common reference framework.

The design of the NIST reference architecture serves the following objectives:

- Understanding and illustration of various services of the cloud in the context of a generalized conceptual model for cloud computing.
- Providing technical references to governmental agencies and to other consumers for understanding, analyzing, categorizing and comparing cloud services.
- Security communication and analysis, possible standards for interoperability and portability and reference implementations.

4.2 General overview

In the document that NIST published there are five involved main actors which are involved in the development of a new taxonomy development regarding cloud computing. In this direction NIST defines the actors as being: cloud consumer, cloud provider, cloud auditor, cloud broker and cloud carrier. See Figure 3**.**

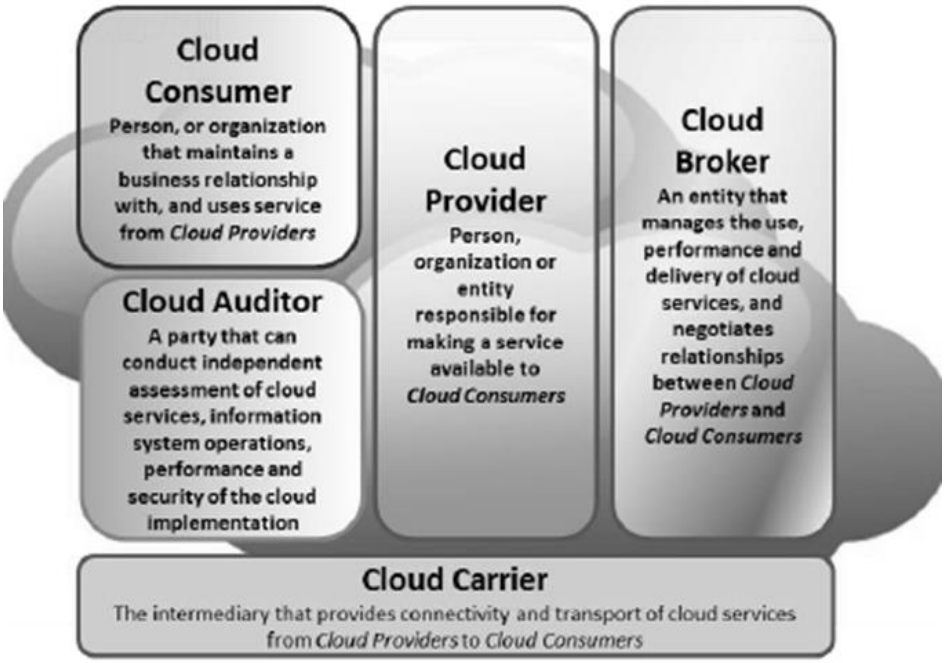

Fig. 3 Actors involved in NIST reference architecture (Source: [6])

These actors have key roles in the cloud computing process, each actor being an entity (person or enterprise) that assists in a transaction or process and executes a certain task. For example, a cloud consumer is an individual or an organization which purchases products and cloud services, while the person that offers these products and services is the cloud provider. Due to the diversity of the available products/services categories (Software, Platform or Infrastructure) there will be an alteration to the level of responsibilities for certain aspects regarding control, security and configuration. The cloud broker acts as a middle man

DOI: 10.12948/issn14531305/18.4.2014.03

between the consumer and the provider, negotiating their relationship, and it helps the consumers overcome the level of complexity of the cloud service, thus generating cloud services with added value. The cloud auditor offers a valuable function for the government by coordinating performance and monitoring cloud services security.
The cloud carrier represents the organization which has the responsibility of carrying data in a similar way as a power distributor for the electric grid.

4.3 Cloud consumer

The cloud consumer is the last one to which the cloud service offers support. A consumer represents a person or an organization which has a business relationship with a cloud provider. Basically the cloud consumer choses some service from a catalog belonging to the cloud provider, it sets some contract conditions for those chosen services and starts using them. The cloud consumer can pay for the provisioned services and it can plan his payments depending on the asked services. There are several scenarios and activities depending on the service that a consumer choses, these are listed in Table 1.
In Figure 4 there are a couple of examples of services that can be provided to cloud consumers.
SaaS applications are implemented, usually, as hosted services which can be accessed through a network that connects the consumers with SaaS providers. SaaS consumers can be enterprises which offer its members access to software applications, they are the end users of the applications, or they can be administrators of software applications that configure the applications for final end users. SaaS consumers can access and use applications on demand and they can pay based on the number of consumers or based on the consumed services (these can be measured as: *time usage, network bandwidth, amount of stored data or duration of stored data*).

Table 1. The cloud consumer and the cloud provider

Service Models	**Cloud consumer activities**	**Cloud provider activities**
SaaS	It uses an application/service for operations regarding business processes.	It installs, manages and assures maintenance and support for software applications from the cloud infrastructure.
PaaS	It develops tests, applies and manages hosted applications in a cloud system.	It provisions and manages the cloud infrastructure and the middleware for the consumers of the platform. It offers development, application and management tools for consumers.
IaaS	Creates/installs, manages and monitors services for the operations with the IT infrastructure.	It provisions and manages physical processing, data storage, network connection, hosting environment and cloud infrastructure for IaaS consumers.

DOI: 10.12948/issn14531305/18.4.2014.03

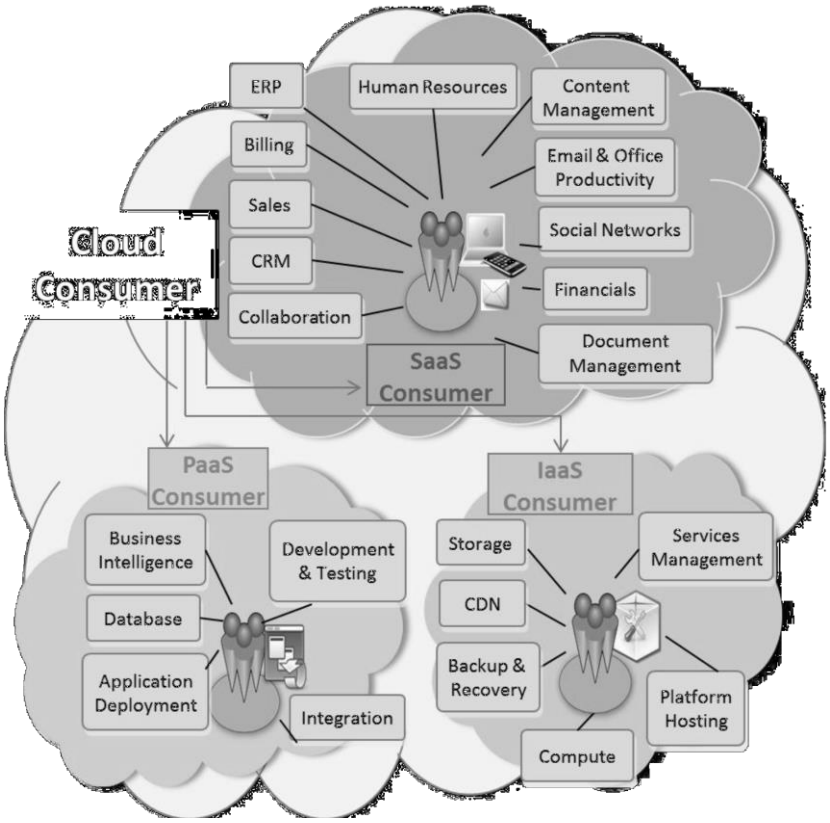

Fig. 4 Example of services for cloud consumers (Source: [6])

In the case of PaaS cloud consumers they use execution tools and resources offered by cloud providers for developing, testing, implementing and managing applications hosted in the cloud environment. PaaS cloud consumers can be application developers that design and implement applications, software testers that run and rest applications in different cloud environments, application developers that publish their applications in a cloud environment or application administrators that configure and monitor applications on a cloud platform. These types of cloud consumers can pay a tax based on the number of users, the type of consumed resources or duration of platform usage.

4.4 Cloud providers

A cloud provider can be a person, enterprise or other entity responsible for making available a resource to a cloud consumer. A provider builds the infrastructure software/platform/services that manages the necessary technical infrastructure for providing these services, provisions services based on the service level agreements (SLA) and protects the security and private characteristic of these services. For the SaaS case the cloud provider implements, configures and updates the operating mode of the software applications on a cloud infrastructure in such a way that the provisioned services meet the corresponding level for the benefit of the consumer. The SaaS provider takes responsibility for managing and controlling applications as well as infrastructure, while cloud consumers have a limited administrative control over the applications.

For the PaaS case the provider manages cloud infrastructure for the platform and provisions execution tools and resources for the consumers of the platform for developing, testing, implementing and managing applications. The consumers control the behavior of the applications and also they control the settings of the hosting environment, but they cannot access the infrastructure on which the platform is hosted (network, servers, operating system, storage capacity).

For the IaaS case the provider provides capabilities of physical processing, storage, connection to the network and other fundamental

DOI: 10.12948/issn14531305/18.4.2014.03

calculation resources assuring and managing the hosting environment and the cloud infrastructure for the IaaS consumers. Cloud consumers implement and run applications, have a large control over the hosting environment of the cloud and the operating systems, but it does not manage or control the base infrastructure of the cloud (physical servers, network, storage capacity, hypervisors, etc.).

The cloud provider activities can be analyzed in detail from the perspective of the following five characteristics: *service implementation, service orchestration, service management, security and confidentiality.*

Service implementation refers to implementation models from the special paper called "NIST Special Publication 800-146, NIST *Cloud Computing Synopsis and Recommendations*", which defines public cloud models, private, community and hybrid. A public cloud is a cloud system in which the infrastructure and the compute resources are made public through a public network. A public cloud is owned by an enterprise which sells cloud services and serves various categories of clients.

In the private cloud case, the infrastructure is operated on entirely by a single enterprise which has access to computational resources and infrastructure in an exclusive way. The infrastructure can be managed by the enterprise (case which holds the name *on-site private cloud*) or it ban managed by a 3rd-party (case which has the name *outsourced private cloud*). A cloud community can be managed by several organizations or 3rd-parties and it can be implemented on the location of the client or outsourced. A cloud community serves several enterprises that have a common goal, which can be regarding security, confidentiality and conformity. A hybrid cloud is a combination of two or more models (private, community and public) created by unique entities that are connected by standardized technologies or property which assures data and applications of portability.

Service orchestration refers to a way of *organizing, coordinating and managing* of cloud infrastructure so as to offer the possibility of optimizing cloud services with the scope or reducing costs. Figure 5 shows an overview over the general requirements tied to each of the three service models.

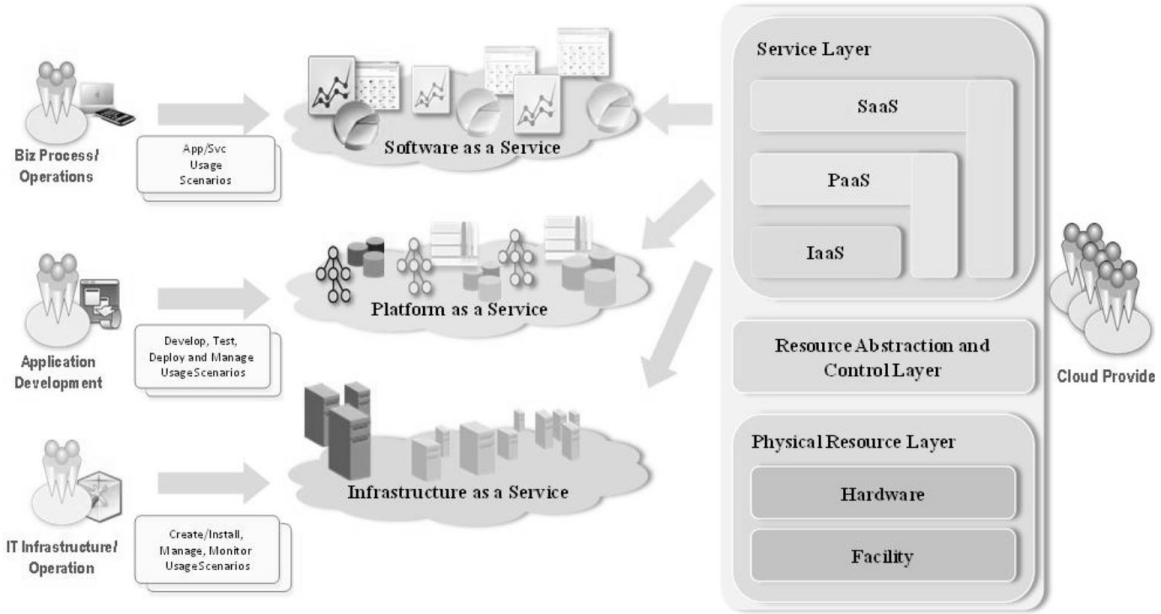

Fig. 5 Service orchestration for cloud providers (Source: [6])

Cloud service management contains all functions regarding necessary services for managing and operating offered services to cloud consumers. As it is shown in Figure 6, cloud service management can be described from the following perspectives: *business support,*

DOI: 10.12948/issn14531305/18.4.2014.03

provisioning and configuration, interoperability and portability requirements.

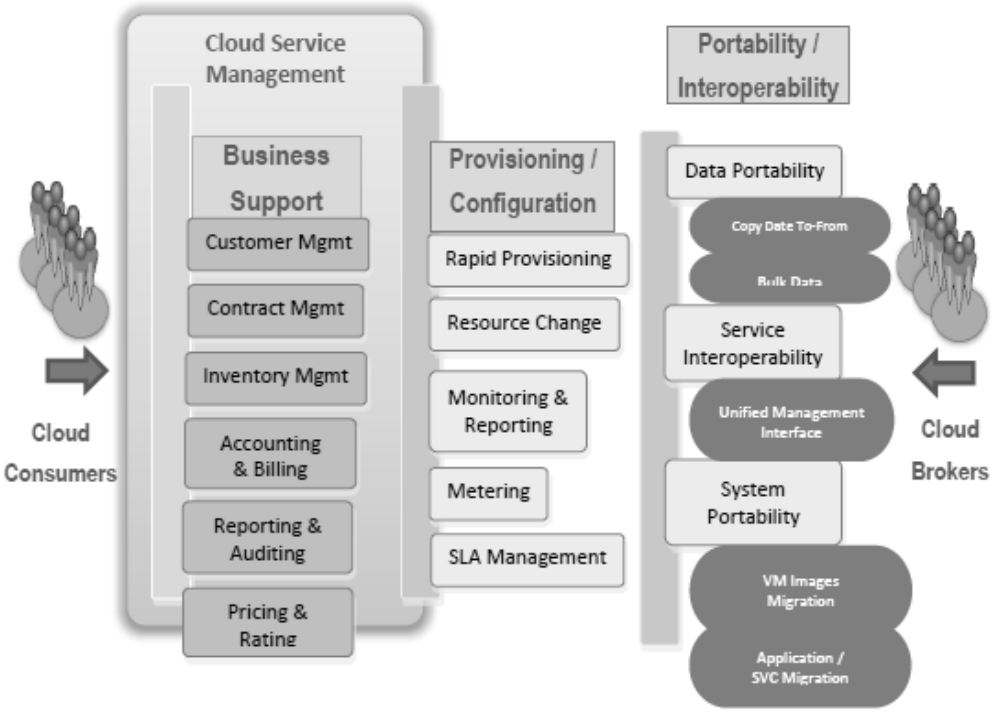

Fig. 6 Cloud service management (Source: [6])

Security is a vital function within all level of reference architectures (See Figure 7). At the Department of Defense of USA it was elaborated in July 2012 a Cloud Computing Strategy which foresees taking specific actions regarding "cyber-security, operation continuity, information insurance and resilience".

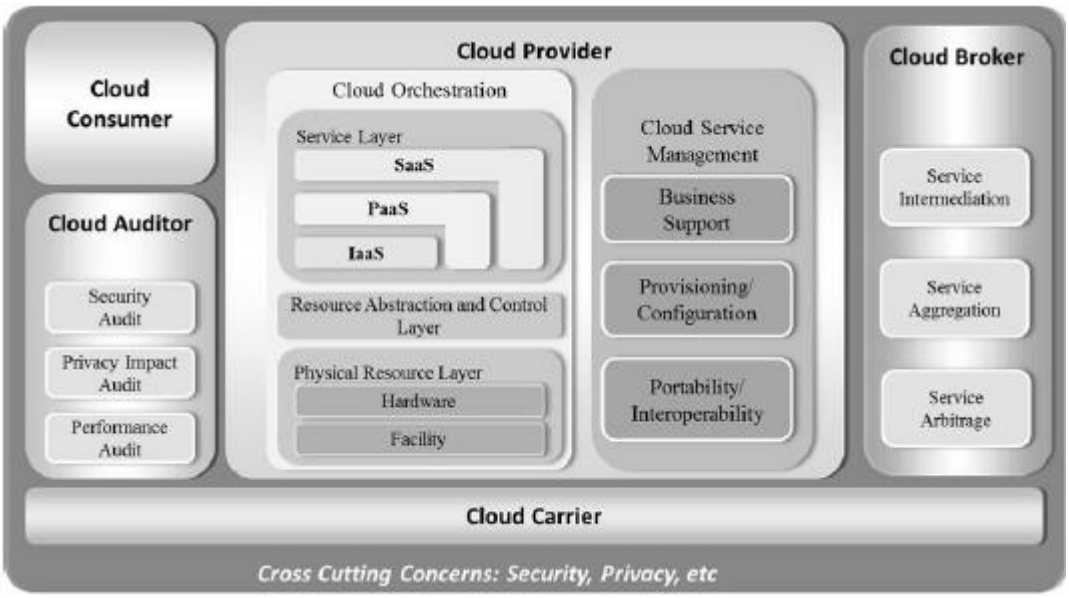

Fig. 7 Characteristics regarding security and confidentiality from the whole cloud architecture view (Source: [6])

Also in November 2012, NIST published a

DOI: 10.12948/issn14531305/18.4.2014.03

White Paper called "*Challenging Security Requirements for U.S. Government Cloud Computing Adoption*" which defines an overview over priority problems regarding governmental organizational security as obstacles in adopting cloud computing solutions.
In these documents there is an emphasis on the fact that security, compatibility and security policies requirements represent functions regarding jurisdiction characteristics of the country in which the cloud services are being offered, these vary from country to country. Due to this aspect and independent auditor will check compatibility with the security policies regulations.
Confidentiality and personal data protection is one of the key imperatives in the cloud field. Taking into consideration that cloud computing solutions offer a flexible way of accessing shared resources, software and information it raises an issue regarding confidentiality. For example, the Federal Council in USA has written a document "*Recommendations for Standardized Implementation of Digital Privacy Controls*" which takes in consideration three basic ways for confidentiality control: Personal information inventory, Confidentiality impact evaluation and Privacy Notice. The recommendations are that the governmental institutions can identify and take into consideration all personal information that can be collected or exposed through digital technology, analyze confidentiality risks through personal data updates and offer notifications to individuals in regard to the way of collecting, storing, and processing and publishing personal information.

4.5 Cloud auditor

A cloud auditor is a 3rd-party which can do an independent evaluation over:

- Cloud services
- Performance and operation modalities of informational systems
- Cloud security implementations

The cloud auditor can evaluate provided services by a cloud provider in relation to various parameters, which are: security control, impact over confidentiality, performance and mapping to SLA characteristics. The audit action is extremely important to governmental institutions which need to assure security controls over the cloud providers including here actions over management, operation and technical solutions for confidentiality insurance, integrity and availability of the system and also of the data stored through it. For security audit, a cloud auditor can elaborate methods of controlling security verifications, including a checking phase of system compatibilities with the security policies of the benefiting enterprise.

4.6 Cloud broker

The cloud broker is an entity which manages usage, performance and provision of cloud services by negotiating the relationship between cloud providers and consumers. With the evolution of cloud computing systems, integration of cloud services can be a complex task which can be very difficult to manage for a cloud consumer. In both cases a cloud consumer asks for cloud services through a broker instead of contacting the cloud provider directly. Cloud brokers offer a single entry point for managing several cloud services. The key characteristic that separates a cloud broker from a cloud provider is the fact that it can offer a consistent interface for multiple providers indifferent if the interface is a technical or business one. In general there are three service categories for brokers:

- ***Service Intermediation:*** enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- ***Service Aggregation:*** combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
- ***Service Arbitrage: s***ervice arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker

DOI: 10.12948/issn14531305/18.4.2014.03

has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

4.7 Cloud carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication and other access devices. For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices. The distribution of the cloud services is done usually by network and telecommunication carriers or a transport agent where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives. Note that a cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers A document that gives details about establishing SLAs is "Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service"[8].

The NIST document [6] also presents some case studies from the cloud computing field regarding standards and interoperability, mapping cloud standards with existing ones (for example: security, portability, accessibility, performance and interoperability) and also identifying the difference between existent standardization and what needs to be done.

Cloud computing is the result of distributed systems evolution, also due to the advances in technology: better hardware, low price networks, virtualization technologies and mature interactive technologies. The majority of relevant standards from the cloud field belong to technologies from the pre-cloud era. In the same time, there are several challenges in the cloud computing zone which are being discovered by innovations brought by service and technology producers. The interaction of service models and the distributed nature of resource control and property in cloud computing has raised some standard differences; to the existing ones we add the pre-cloud computing era ones as well.

5 VMware reference architecture

VMware, a worldwide leader in virtualization field, brought also an important document that is the reference architecture specification for their products in the cloud computing field. This document is called "VMware vCloud[1] Architecting vCloud" [7] and it is an introduction that describes what a vCloud, constructors, resource, vCloud capabilities, management, sizing and vCloud implementation is. The general vCloud architecture is presented in the form of a puzzle in Figure 8 with these components:

- **vCloud Director –** user interface and coordinator; abstracts VMware resources.
- **vCloud API –** API interface used for interacting with vCloud.
- **VMware vSphere –** it's the base of virtualized resources being an element that consists of a series of products like vCenter Server and vCenter database, host ESXi and management assistant.
- **VMware vShield –** provides security services at network level.
- **VMware vCenter Chargeback –** an optional component that offers portability of resource usage measurement and eases provisioning.
- **VMware vCenter Orchestrator –** optional component that eases orchestration on vCloud API and vCloud vSphere levels.
- **VMware vCloud Request Manager –** optional component which overs provisioning demands and approving workloads, tracking software licenses and cloud policy partitioning.

[1] vCloud from VMware is the cloud version built on base VMware technologies and solutions.

DOI: 10.12948/issn14531305/18.4.2014.03

- **VMware vCloud Connector –** optional component what eases the transfer of an offline vApp application in OVF format from a local vCloud or vSphere to a remote vCloud.

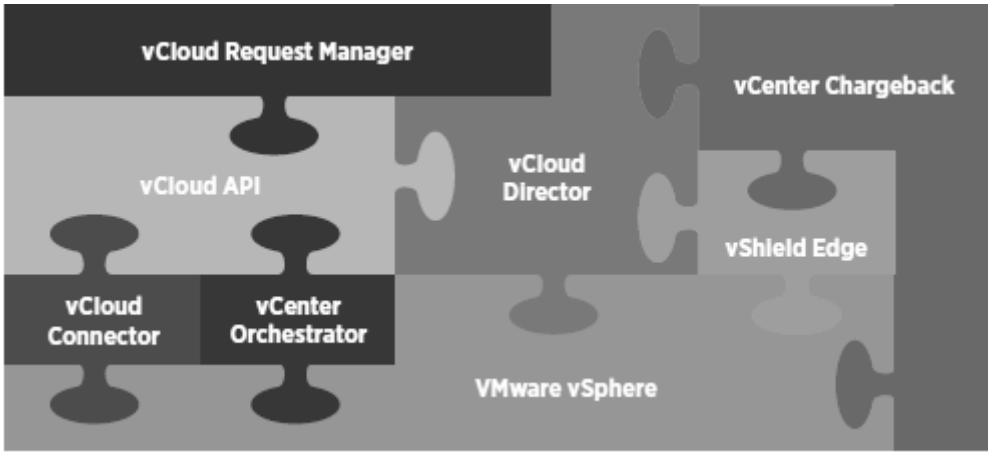

Fig. 8 vCloud architecture from VMware (Source: [7])

From an infrastructure point of view vCloud is build on a virtual infastructure that has its components splited into an administration cluster. In [7] there are presented the constructive details of the components from Figure 8 and also usage stories about those components. From those usage stories it stands out the importance of connection logs existence. As a result, tracking and monitoring is important in order to prevent future attacks. An audit of a log allows an organization to verify compatibilities, detect violations of security and initialize restore points if it is necessary. A rule of thumb is to regularly examine the logs for identifying any suspicios activity. The laws and external rules can also require access to special levels of monitoring and checking. Rules are needed for restricting access, while log parsing can give some hints about system configuration errors or failures and applying any SLA rules. Thus we have identified some scopes for logs:

- *compatibility requirements* – logs are needed for assisting audit control as well as checking security breaches, analysis and responses. For example, an authentication log can check if an resource has been accesed only by authorized users.
- *client demands* – end users (usally refered to as *tenants*) can obtain access to logs to correspond to their requirements.
- *operation integrity* – operation alerts can be defined for logs to trigger remediation notifications.

6 Conclusions

We have summarized here four important reference architectures for cloud computing, respectively Cisco – Cisco Cloud Reference Architecture Framework, IBM CCRA, National Institute of Standards and Technology (NIST) and finally, VMware's Architecting vCloud. Between all of them, the NIST's architecture is provider independent, while the other three architectures belong to worldwide leaders of the cloud computing like Cisco, IBM and VMware. There are also proposed other reference architectures for cloud computing from other vendors like Oracle, Microsoft, Amazon, Google or open source flavors like OpenStack.

After going through the four architectures we can conclude that the independent platform architecture from NIST is the most comprehensive, containing also architectural details and talking about concrete case studies of usage. The other three platform dependent architectures basically follow NIST's definition using their own technologies and solutions based on their own services or infrastructure elements.

All the four architectures for cloud computing considered here are containing common base elements and rely on the same definition of a cloud and are following the same service

DOI: 10.12948/issn14531305/18.4.2014.03

models described by NIST like: SaaS, PaaS and IaaS. Also, all the architectures are embracing the cloud consumers' and providers' interests with emphasis on the administration part, offered services and access to resources. Security of the data stored in the cloud environment is also a main concern of the cloud architectures [9].

As a final conclusion, no matter the reference architecture we discuss about, even it is independent (NIST) or company specific, it contains several common components and services. As an addition, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) have published in October 2014 under the auspices of ISO/IEC 17789:2014 specifies the cloud computing reference architecture (CCRA). The reference architecture "includes the *cloud computing roles, cloud computing activities,* and the *cloud computing functional components* and their relationships" [10], being available only by buying from *www.iso.org*. As for future research we will investigate this new ISO/IEC proposed standard which could become in the future the *de facto* standard for cloud computing reference architecture.

References

[1] L.Wilkes, "Cloud computing reference architectures, models and frameworks*"*, *Everware CBDI*, 2011, Available at http://everware-cbdi.com/ccrfam

[2] K. Gerald, "Cloud computing architecture", Siemens AG, 2010, Available at http://www.sei.cmu.edu/library/assets/presentations/Cloud%20computing%20architecture%20-%20Gerald%20Kaefer.pdf

[3] Cloud standards wiki, Available at http://cloud-standards.org/wiki/index.php?title=Main_Page

[4] Cisco White Paper, "Cloud: What an Enterprise Must Know", Available at http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/cloud-computing/white_paper_c11-617239.html, 2011.

[5] IBM, "IBM Cloud Computing Reference Architecture", Available at https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wf3cce8ff09b3_49d2_8ee7_4e49c1ef5d22/page/IBM%20Cloud%20Computing%20Reference%20Architecture%203.0

[6] NIST – US Department of Commerce, "NIST Cloud Computing Standards Roadmap", Available at http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[7] VMware, "VMware vCloud Architecting a vCloud, Technical White Paper", 2010, Available at http://www.vmware.com/files/pdf/VMware-Architecting-vCloud-WP.pdf

[8] CIO Council, "Creating Effective Cloud Computing Contracts for the Federal Government – Best Practices for Acquiring IT as a Service", Available at https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

[9] C. Gurkok, "Securing Cloud Computing Systems", in Network and System Security (Second Edition), edited by John R. Vacca, Syngress, Boston, 2014, Pages 83-126, Available at http://www.sciencedirect.com/science/article/pii/B9780124166899000046

[10] ISO/IEC 17789:2014 Standard, Available at https://www.iso.org/obp/ui/#iso:std:60545:en

DOI: 10.12948/issn14531305/18.4.2014.03

Răzvan Daniel ZOTA has graduated the Faculty of Mathematics Informatics at the University of Bucharest in 1992. He holds a Ph.D. in Economic Informatics from 2000 and now is professor at the Department of Economic Informatics and Cybernetics from the Bucharest University of Economic Studies. From 2010 he is Ph.D. supervisor in the field of Economic Informatics. His last published books in 2004 are "IT Basics" and "Computer Networks" in ASE Publishing House. His recent work focuses on business cloud computing, computer networks and applications.

Ionuț Alexandru PETRE has graduated the University of Bucharest, Department of Technology, Information Technology in 2011. He continued his studies getting a Master's degree from the Politehnica University of Bucharest, Faculty of Applied Sciences in the field of *Models for decision, risk and forecasting*. Ionuț is currently a Ph.D. candidate at Bucharest University of Economic Studies in the field of Economic Informatics. He is a software developer for an outsourcing IT company, working continuously since 2010.

DOI: 10.12948/issn14531305/18.4.2014.03