ISCG 8046 – Cloud Computing

Lecturer: Sam Kolahi

Assignment 1

Deadline: 07/05/2014

Family Name	*First Name*	*Student ID*

Research Report
Cloud Computing

Author:

Unitec Institute of

Technology 07/05/2014

Abstract

This study provides an overview of Cloud Computing concept, historical development, architecture, applications, impacts and perspectives.

To produce this report, an extensive literature review was conducted, gathering views and concepts from relevant books, journals and publications as well as relevant institutions directly or indirectly related to the cloud computing scenario.

The study reviews the definitions of cloud computing, and outlines the subjacent technology that converged to compose the clout as we know today.

Cloud architecture is explained and most prominent platforms, vendors and their corresponding offerings are also outlined in this report, which covers relevant developments in terms of security, standards and interoperability in cloud computing.

The impact of cloud computing in technology, business, economy, social life and Politics is considered, as well as the challenges to be faced until cloud computing reaches its mature stage.

A session on paper discussions summarises the findings of the following papers:

I. A Comparative Study of High-Performance Computing on the Cloud;
II. A Survey on Cloud Interoperability: Taxonomies, Standards, and Practice;
III. Pragmatic assessment of research intensive areas in cloud: A systematic review;
IV. A review on cloud security;
V. A scalable blackbox-oriented e-learning system based on desktop grid over private cloud.

CONTENTS

1. Introduction

In recent years, cloud computing has become a hot topic in information technology industry.

Not limited to the technical circles, the subject has been increasingly attracting the interest from business leaders, virtually across every industry around the globe. Additionally, marketing departments of technology vendors have embraced a massive “rebranding” in an effort to associate their products to cloud “trending topic”.

As it can be noticed in Figure 1, Google Trends’ search interest index for cloud computing was equal to zero until late 2007, before climbing up in clear contrast to other related search terms.

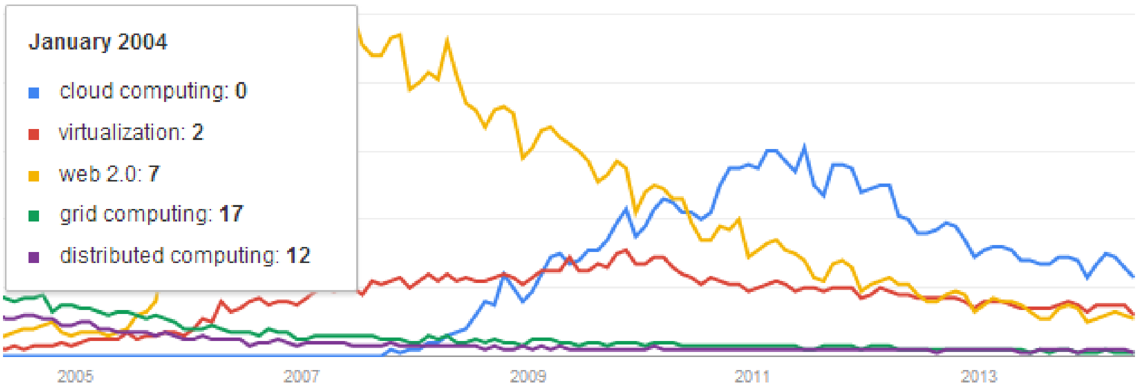

Figure 1-Google Trends: Interest in cloud computing over time since 2004

According to the Gartner Hype Report (Gartner, 2012), cloud computing is moving towards the through of disillusionment, when interest retrocedes before achieving more stable plateau.

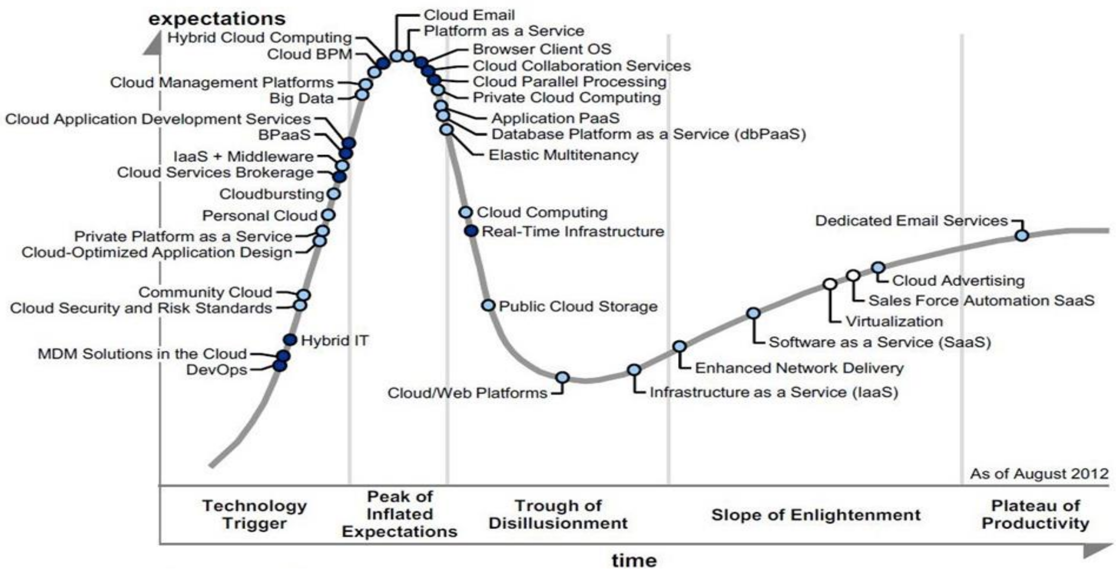

Figure 2-Cloud Computing Hype Cycle. Source (Gartner, 2012)

With countless number of definitions, different authors and sources often present diverging perceptions in relation to the nature of the cloud computing phenomenon, which is sometimes considered a "*computing model*", a *"technology"* (CSA - Cloud Security Alliance, 2011), a "style of computing" (Gartner, 2013), a "*category of . . . services"* (Buyya, Broberg, & Goscinski, 2011), a "*computing paradigm*" (Zhang, Wu, & Cheung, 2013) and so many others.

Rhoton (2010) makes an interesting observation, considering that, "although the definitions are not identical, or in some cases even very similar, they are still not contradictory. They simply emphasize different aspects of a complex and multi-faceted notion", typically along the lines of resources that are "available on-demand from an optimized, and highly scalable, service provider".

A widely adopted definition of cloud computing is provided by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction..." (NIST, 2011)*

The NIST definition also specifies five essential characteristics of cloud computing as being: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. (NIST, 2011)

> **On-demand self-service:** *A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.*
>
> **Broad network access:** *Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).*
>
> **Resource pooling:** *The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.*

> **Rapid Elasticity:** *Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.*
>
> **Measured service:** *Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. (NIST, 2011)*

In addition to these five essential characteristics, several other attributes such as Service-Level Agreement (SLA) Management, Economy of Scale, ease of utilisation, pay-per-use billing and others.

When combined, these attributes enable what is known as *"Utility Computing"* or, the provision of compute services in which resources and infrastructure are packaged and offered on a pay-as-you-go basis, resembling the methods in use for utilities like water, power and telephone connection. (Rosenberg & Mateo, 2011, p. 189)

The dream of computing as a utility dates back to the beginning of the ICT industry as it can be observed in the visionary speech of the American scientist John McCarthy for the Massachusetts Institute of Technology (MIT) centennial in 1961:

> *If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility, just as the telephone system is a public utility . . . The computer utility could become the basis of a new and important industry. (Buyya, Vecchiola, & Selvi, 2013, p. 21)*

2. History of cloud

Even though technologies such as virtualisation, multi-tenancy (timesharing), distributed computing have been in place for decades, it was necessary the convergence of several gradual advances to unleash the advent of cloud computing. Distributed systems, virtualization, Web 2.0, service orientation (Buyya, Vecchiola, & Selvi, 2013) and autonomic computing (Buyya, Broberg, & Goscinski, 2011) can be considered the most important technology pillars, whose historical developments are summarised based on the Historical Developments as described in (Buyya, Vecchiola, & Selvi, 2013).

2.1. Distributed systems

A distributed system is essentially a collection of independent computers that appear to its users as a single coherent system (Buyya, Vecchiola, & Selvi, 2013, p. 16).

To support cloud computing as we know today, distributed systems have evolved through three major milestones:

Mainframes: The first examples of large powerful and reliable computational structures leveraging multiple processing units. Even though mainframes cannot be considered distributed systems, they offered large computational power by using multiple processors, which were presented as a single entity to users.

Clusters: Cluster computing started as a low cost alternative to mainframes. Cheap commodity machines could be connected by a high-bandwidth network and controlled by specific software tools that manage them as a single system. Starting in 1980, clusters become the standard technology for parallel and high-performance computing.

Grids: Appeared in early 1990s as an evolution of cluster computing in an analogy to the power grid. Grids could aggregate geographically dispersed clusters by means of Internet connections, allowing different organisations connect and share computational power, “consuming” resources in the same way they used utilities such as power and water.

Cloud computing inherits characteristics of all these three technologies. It is characterized by having virtually infinite capacity, being tolerant to failures, and being always on, like mainframes. Cloud infrastructure is usually composed of nodes of commodity machines as in the case of clusters. The services made available by a cloud vendor are consumed on a pay-per-use basis, in line with the utility concept that characterized grid computing.

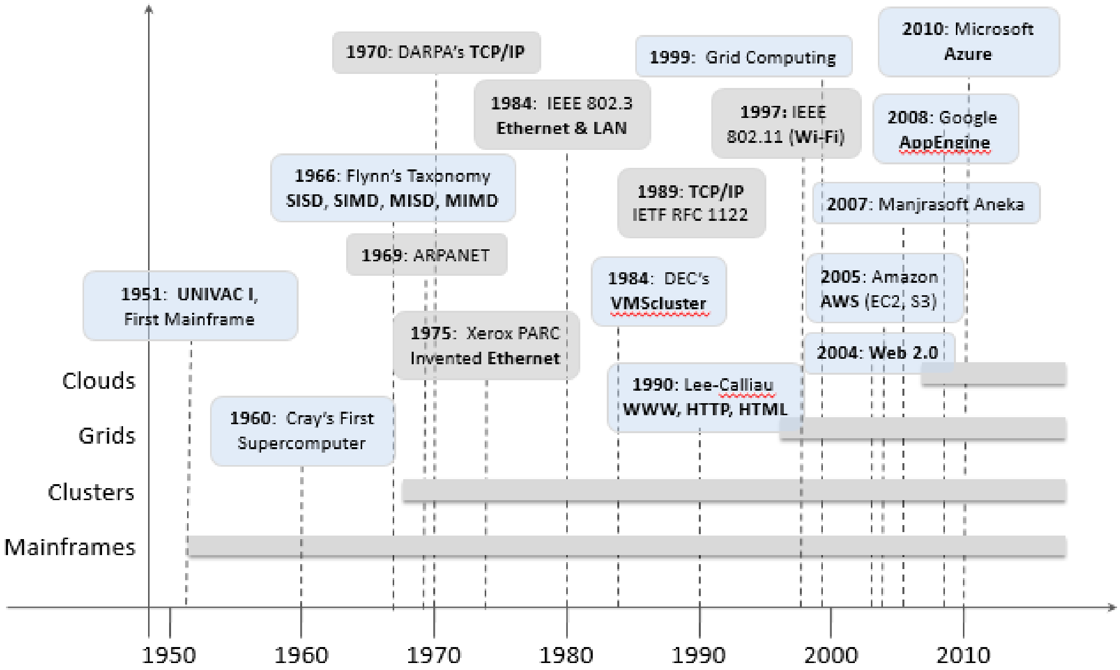

Figure 3-The evolution of distributed computing technologies, 1950s - 2010s.
Source: (Buyya, Vecchiola, & Selvi, Mastering Cloud Computer, 2013)

2.2. Virtualisation

Virtualisation involves a range of solutions enabling the abstraction of some of the fundamental elements for computing, such as hardware, runtime environments, storage and networking, creating "virtual" or "logical" computing environments that simulate the interface that is expected by a guest.

The most common type of virtualization is hardware virtualization, involving the use of virtual machines and hypervisors. Being mostly "software based", the creation of virtual environment is incomparably faster than an equivalent physical infrastructure. Additionally, several APIs enable the automation of several virtualisation tasks such as deployment and release of resources on demand and nearly in real time.

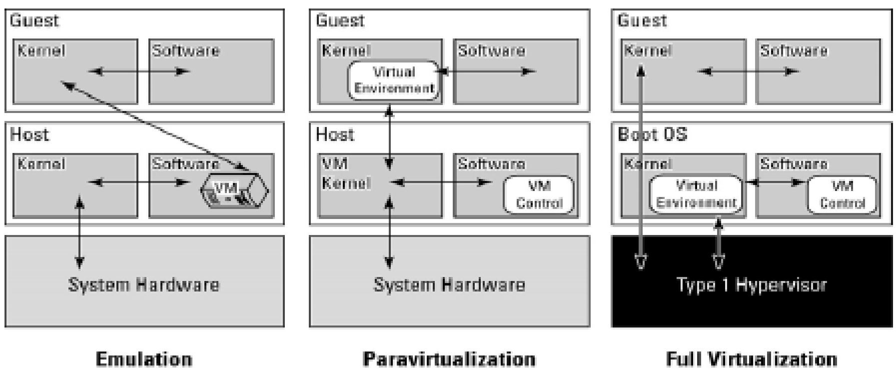

Figure 4-Virtualisation and Paravirtualisation examples (Sosinsky, 2011)

Different hardware virtualization approaches such as full virtualisation or paravirtualisation are supported by multiple vendors.

VMWare ESXi, Xen, KVM and Microsoft Hyper-V are the most widely used hypervisors.

Virtualizations are also employed to replicate runtime environments as is the case with Java Virtual Machine or .NET CLR).

An interesting feature of virtualisation is the offering of “Virtual Appliances” which are pre-built virtual machines with complete software stack pre-installed and ready for use.

Although virtualization has been around for more than 40 years, several technology limitations prevented its efficient use. Today those limitations were substantially overcome.

2.3. Web 2.0

2.4. Service Orientation

Service orientation is the core reference model for cloud computing systems. This approach adopts the concept of services as the main building blocks of application and system development. A service is supposed to be loosely coupled, reusable, programming language independent, and location transparent.

The service-oriented architecture (SOA), is a logical way of organising software systems to provide end users or other entities with services through published and discoverable interfaces.

Web services standards are built on top of ubiquitous technologies like HTTP, XML and may be programmatically aggregated in compositions called service mashups, accessible through the use of standard protocols such as SOAP and REST.

2.5. Data Centre Automation (Autonomic Computing)

Autonomic computing aims to improve systems by decreasing human interaction to manage those systems. The systems should manage themselves as much as possible. Large data centre of cloud computing providers must be managed in an efficient way and automation can perform tasks such as management of SLAs, capacity management, disaster recovery and automation of Virtual Machine provisioning (Buyya, Broberg, & Goscinski, 2011).

2.6. The “Cloud” metaphor

The first known reference to cloud computing was made in a 1996 MIT paper (http://ccs.mit.edu/papers/CCSWP197/CCSWP197.html) from Gillet and Kapor. However the term only gained popularity after Amazon repurposed its latent e-commerce resources, making it available as a cloud service (Rosenberg & Mateo, 2011).

The use of a cloud as a symbol was a common practice to represent the Internet in network diagrams, in which the cloud icon represents “the bunch of things” that makes the network actually work beyond your firewall, typically representing elements that are “someone else’s concern” (Velte, Velte, & Elsenpeter, 2010).

The similarity between cloud computing and some of the internet attributes are often a source of confusion. However, although the cloud computing should be considered in light of the essential characteristics mentioned in section 1.

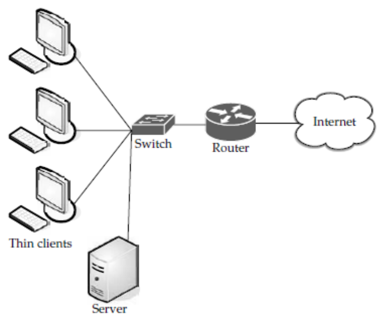

Figure 5-Cloud used to depict internet (Velte, Velte, & Elsenpeter, 2010, p. 20).

3. Cloud Architecture

In addition to the core definition and the five essential characteristics of the cloud, NIST definition (NIST, 2011) determines that the cloud computing is composed of three service models and four deployment models, often referred to as the “cloud layers” or “cloud stack”.

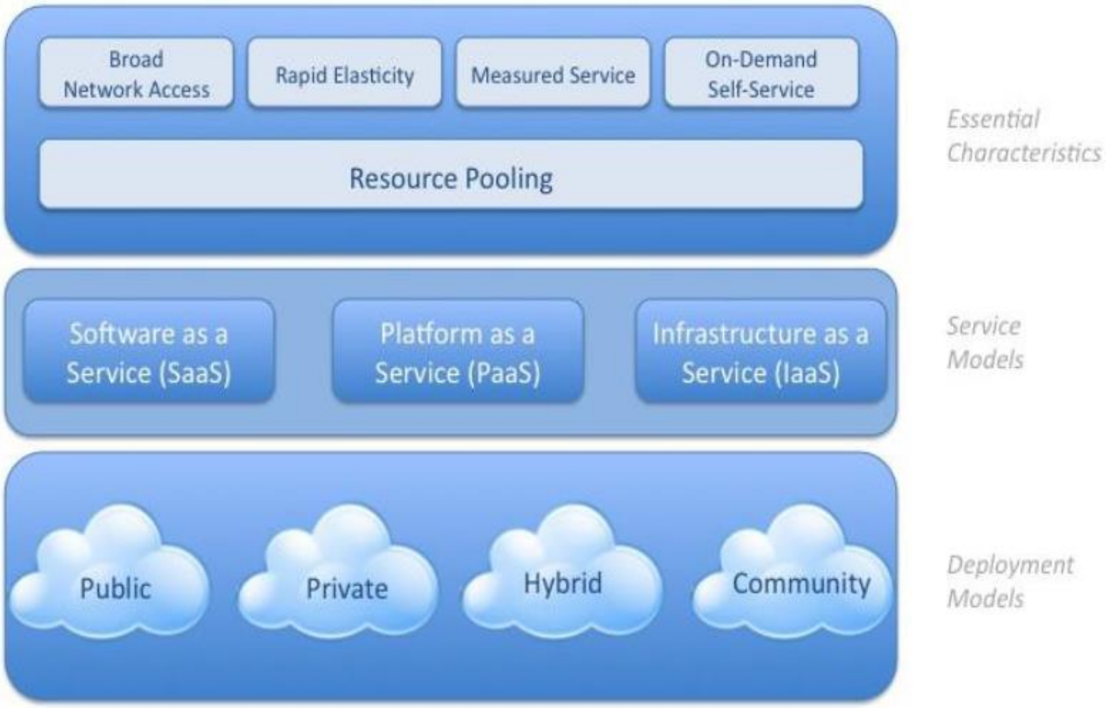

Figure 6 - NIST Visual Model of Cloud Computing Definition (CSA - Cloud Security Alliance, 2011)

3.1. Service Models (Cloud Layers)

The three NIST service models are summarised below.

Infrastructure-as-a-Service (IaaS): At the base of the stack, infrastructure-as-a-Service is a lower level service, delivering infrastructure in form of virtual hardware, storage, and networking. Virtual hardware is extensively used to provide compute resources that can be directly managed by users which are usually given tools and interfaces manage the software stack. The pricing model is generally based on dollars per hour rates. Virtual storage is delivered in the form of raw disk space or object storage. Virtual networking are logical emulation of networking connectivity between virtual and physical machine instances, both on private networks or over internet.

Platform-as-a-Serivce (PaaS): The next layer, is an intermediate level, built on top of the cloud infrastructure. Provides highly elastic and scalable execution environments, usually comprised of very specific technologies, frameworks or platforms on top of which the user can develop, deploy and execute its own applications through the extensive use of Application Programming Interfaces (APIs) made available by the PaaS provider. While is the responsibility of the provider to maintain the executable environment, scalability, fault tolerance and infrastructure security, the consumer is responsible for maintaining its application and, in many cases, in several cases, even its data backups. Applications built on top of specific vendor platforms are not usually portable to other vendor's platforms, implying in rigid ties with the vendor once a platform is chosen.

Software-as-a-Serivce (SaaS): Is a high-level service layer, built on top of very specific cloud execution environments and underlying infrastructure. Provides typical end-user applications as those traditionally offered on desktop computers such as word processing, spreadsheets, consumer relationship management (CRM), time management, project management, photo editing, e-mail, calendar, and many others. However, applications are accessed through web browsers and usually do not require installation of software components on the client side, as the application is typically run on the cloud, and only the presentation layer is made available to the user via web (although there are some few exceptions where some processing is done on the client side and can even require the installation of small pieces of software that interact with the SaaS platform).

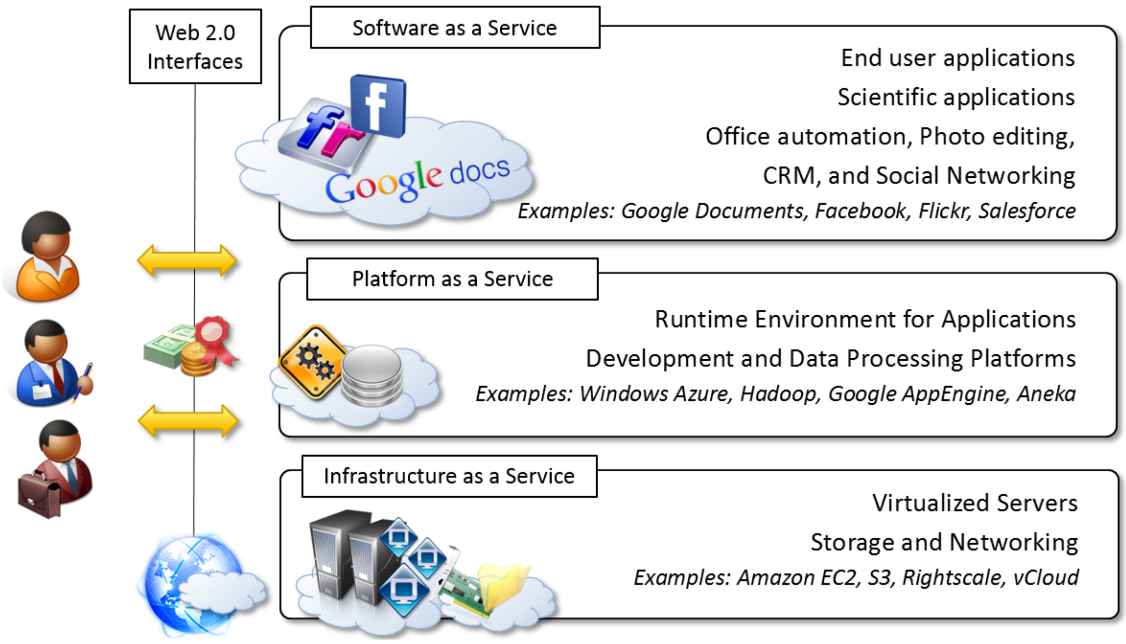

Figure 7-Cloud computing service models (Buyya, Vecchiola, & Selvi, 2013, p. 12)

3.2. Deployment Models (NIST, 2011)

The three NIST deployment models are summarised below.

Private Clouds: The cloud infrastructure is available to a single organisation, on or off premises, regardless of whether the infrastructure is owned, managed and operated by the organisation itself or a third party, or even a combination of the two.

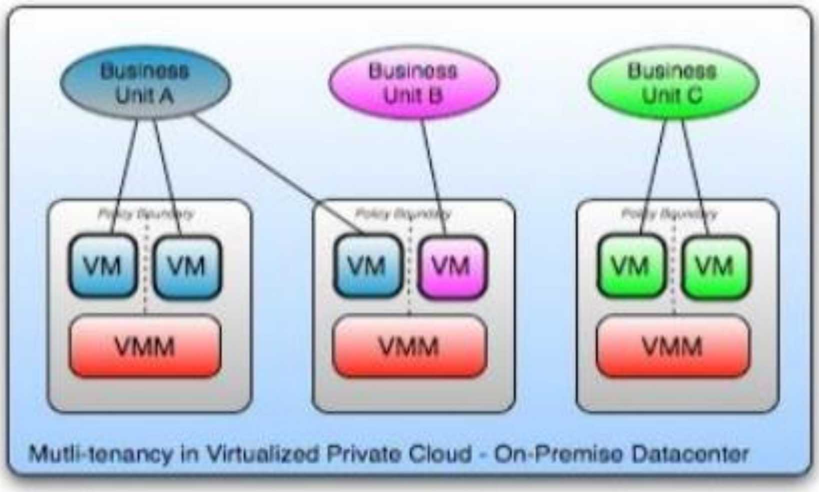

Figure 8-Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure (CSA - Cloud Security Alliance, 2011, p. 14)

Public Clouds: The cloud infrastructure is available to be used by the general public, commercially or for free, on the premises of the service providers, owned, managed and operated by a business, govern or academic organisation or a combination of them.

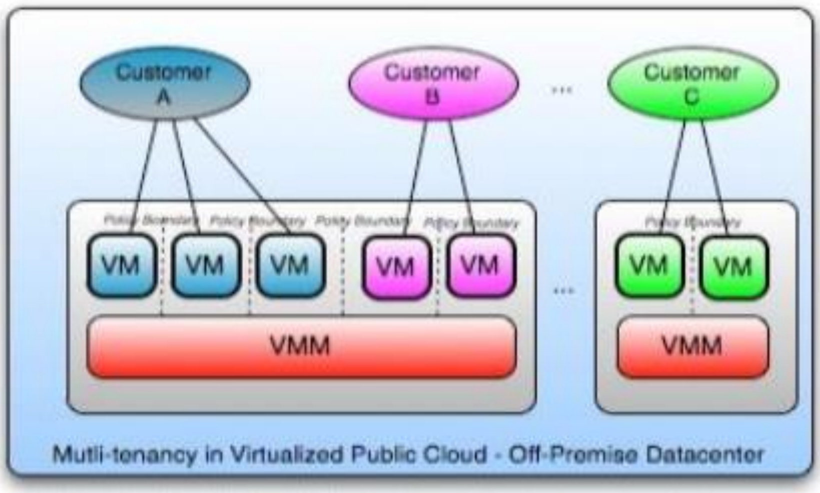

Figure 9 - Public Cloud Provider with 3 business customers, each with different security, SA, governance and billing policies on shared infrastructure (CSA - Cloud Security Alliance, 2011, p. 14)

Hybrid Clouds: The cloud infrastructure is comprised of two or more clouds of different deployment models that keep being separate clouds, however, tied together by shared interface that allows for data and application portability

Community Clouds: The cloud infrastructure made available to be exclusively used by a specific community of users from organisations willing to cooperate on shared concerns, such as those addressed by scientific of medical applications. Infrastructure can be on or off premises and owned, managed or operated by one or more organisations of the community or even a third party.

3.3. Topology

Over the last fifty years, typical computer topology have shifted from the mainframe in the 1960s to the client-server in the 1980s and the N-tier architectures, which separated the business logic both from the presentation and database layers in the 1990s.

Cloud computing is now stimulating and supporting the mesh connectivity, where every system on the network can communicate with the others and every device, including client devices, is considered part of the cloud computing topology.

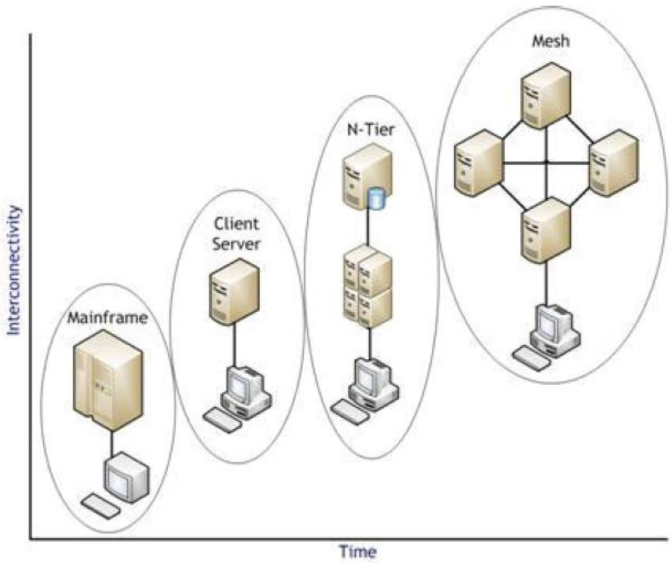

Figure 10-Topology Evolution (Rhoton, 2010)

4. Cloud Technologies, Vendors and Platforms

4.1. Cloud Infrastructure Management

One of the most challenging aspects when building a cloud infrastructure is how to orchestrate the so advertised elasticity, scalability, reliability and security in a fast, efficient way to provision resources dynamically with minimum human intervention.

The crucial element to handle this task is called virtual infrastructure manager (VIM), which are similar to traditional operating systems, however, aggregating resources from multiple computers that are presented as a uniform view to users and applications.

VIM tools overlap with another type of tools called “cloud toolkits” (Buyya, Vecchiola, & Selvi, 2013, p. 17), which expose interfaces for creating, controlling and monitoring virtualised resources, however with less sophisticated features than specialized VIM.

Typical features found in VIMs: (Buyya, Vecchiola, & Selvi, 2013, p. 18)

- Virtualisation support;
- Self-service, On-Demand Resource Provisioning;
- Multiple Backend Hypervisors;
- Storage Virtualisation;
- Interface to Public Clouds;
- Virtual Networking;
- Dynamic Resources Allocation;
- Virtual Clusters;
- Reservation and Negotiation Mechanism;
- High Availability and Data Recovery;

Most popular VI managers available:

- Apache VCL (Virtual Computing Lab);
- AppLogic;
- Citrix Essentials;
- Enomaly ECP;
- Eucalyptus;
- Nimbus3;
- OpenNebula;
- OpenPEX;
- oVirt;
- Platform ISF;
- VMWare vSphere and vCloud;

4.2. IaaS Providers

Infrastructure-as-a-Service providers can have considerably distinguished offerings depending on the availability of specific features included in the final service package.

The most influential characteristics are: (Buyya, Broberg, & Goscinski, 2011)

- Geographic presence;
- User interfaces and access o to servers;
- Advance Reservation of Capacity;
- Automatic Scaling and Load Balancing;
- Service –Level Agreement;
- Hypervisor and Operating System Choice;

Amazon Web Services (AWS)

Amazon have pioneered the introduction of IaaS clouds in 2006 and offers a comprehensive set of cloud services:

EC2	Virtual Servers
S3	Storage
Cloudfront	Content Delivery
Cloudfront Streaming	Video Streaming
SimpleDB	Structured Datastore
RDS	Relational Database
SQS	Reliable messaging
Elastic MapReduce	Data Processing

Figure 11 - IaaS services offered by Amazon

Flexiscale

A United Kingdom based provider offering services similar to Amazon, however with distinct features by default.

Web services (SOAP)
Web-based user interfaces
Access to virtual server mainly via SSH (Linux) and RDP (Windows)
100% availability SLA with automatic recovery ov VMs in case of hardware failure

Figure 12-IaaS services offered by Flexiscale

Joyent

Offers servers based on Solaris containers virtualisation technology, with a notable feature of automatic vertical scalability that allow a server make use of additional CPUs up to the number of available core in the physical machine.

Multiple geographic locations in US;
Web-based user interfaces
Access to virtual server via SSH and Web-based virtualisation tool;
100% availability SLA with OS-level virtualisation Solaris containers and automatic vertical scaling

Figure 13-IaaS services offered by Joyent

GoGrid

Offers a wide range of pre-built Windows and Linux images (appliances). Among the most notable features is the "hybrid hosting" facility, combining traditional hosts with auto-scaling cloud server infrastructure.

Also provide hardware load balancing, auto-scaling capabilities, and persistent storage for free as part of its core IaaS offerings.

Rackspace

Provide a range of virtual appliances in the cloud, both Linux and Windows. Similar to GoGrid, Rackspace also offers hybrid approach allowing the combination of dedicated and cloud server infrastructures. It enables static IP addresses, persistent storage and load balancing for free in all offerings.

4.3. PaaS Providers

PaaS providers deliver execution environments and abstraction tools that enable developers create applications without worrying too much about the underlying cloud infrastructure. Abstractions such as MapReduce model, Web Services, Workflow models, high-performance distribution of computational tasks are made accessible for programming languages and platforms such as Python, Java, .NET and Ruby.

It is interesting to note that traditional relational database lack scalability to handle several petabytes of data stored in commodity computers across the cloud. Thus, distributed storage technologies have emerged, favouring schema-less, non-relational databases capable of robust and highly scalable performance.

Google App Engine

Enable Python and Java Web applications on the elastic google infrastructure. Applications scale dynamically according to traffic and data storage. Developers gain scalability by using native features of the platform API, in exchange, some flexibility is lost, such as the direct access to file system or creation of new threads.

Microsoft Azure

The comprehensive .Net stack plus Java & Ruby SDK services available on the cloud. Azure Fabric Controller provides auto-scaling, reliability and manages memory and load balancing. Also, .NET service bus acts as a messaging component between applications, which can be integrated to Windows LiveID and .NET Workflows.

Force.com

Force.com evolved as a complete platform that enables the development of complete and reliable and scalable software on the cloud, not limited to the Salesforce CRM application.

Developers can choose between Apex, a java-like programming language, or Visual force, a XML-like syntax for building user interfaces in HTML, AJAX or Flex.

Heroku

A platform focused on deployment of Ruby on Rails web applications. In this platform, the servers are never exposed to users, and applications are automatically handled by a powerful logic layer that automatically distributes applications across CPUs and handles failures.

Aneka

A flexible .NET-based service-oriented resource management and development platform. In Aneka, each server hosts a container providing the base infrastructure for persistence, security and communication. It supports both physical and virtual nodes, as well as instances rented from Amazon. Aneka also supports execution of legacy High-Performance Computing Models as well as MapReduce.

5. Reasons for cloud usage and success

The ability to consume computing as a utility has profound implications and can bring significant benefits to organisations and end users.

Change from CAPEX to OPEX: The change from capital to operational expenses, eliminates the need for upfront investments in technology and let consumers pay-as-they-go, changing (usually for the better) the cost structure of organisations. In addition to the elimination of upfront costs, the new model collaborates to reduce the incidence of tasks, as it reduces investment in assets and increase expenses. (Rosenberg & Mateo, 2011, p. 7)

Low barrier to entry: With dramatically reduced upfront capital expenditures, computing resources are accessible for small business.

Agility to provision infrastructure: Substantial savings are achieved by eliminating traditional effort in planning, purchasing, provisioning and configuring physical infrastructure (Rosenberg & Mateo, 2011, p. 8).

Ease of utilisation: Self-service and minimum human intervention are paramount in the cloud paradigm. Thus, cloud computing services usually offer great autonomy to consumers.

Focus on core business: Not having to deal with the demanding management of ICT infrastructure, organisations can intensify the focus on its core business.

Rightsizing: Infrastructure size can be scaled to match business seasonality, growth or shrinkage.

Risk: Organizations can deflect some of its risks by carefully negotiating SLA with service providers.

Security: Although cloud computing introduces new security risks, it can also strengthen organisation security in several domains due to rigid security policies, audits, redundancy, fault tolerance, authentication, intrusion detection and many other security best practices that, in specific situations, might overcome the security risks.

6. Relevant developments in cloud computing

6.1. Standards and Interoperability

Interoperability and security are probably the most important bottlenecks constraining growth and maturity of this market. That is why these two subjects have attracted a great deal of attention both from industry and academia.

The industry knows the problem very well and, despite of short term convenience of protecting their proprietary mechanisms while lock-in its customers, vendors are aware that the market will never achieve full maturity until consumers have the ability to port their cloud solutions from one vendor to others.

Although standardisation and interoperability may scare vendors, rising concerns that consumers become too cost-focused, several activities have been initiated on the standards front, indicating that vendors are motivated to work together to move the technology forward.

In 2009, the Open Cloud Manifesto defined a set of core principles considered of high priority by vendors. Since then, several standards workgroups gathered efforts towards the construction of interoperability standards for the cloud.

> ***The Distributed Management Task Force (DMTF)*** *has a focus on interoperable management of enterprise computing and cloud computing.*
>
> ***The Storage Networking Industry Association (SNIA)*** *has defined a Cloud Data Management Interface (CDMI) and hosts a working group that is examining container capabilities, lifecycle management and storage security.*
>
> ***The Object Management Group (OMG)*** *is modelling deployment of applications and services on clouds for portability, interoperability and reuse.*
>
> ***The Organization for the Advancement of Structured Information Standards (OASIS)*** *has taken responsibility for extending WS* standards, SAML, XACML and KMIP key management infrastructure to be cloud friendly.*
>
> ***The Open Group Cloud Work Group*** *is collaborating on standard models and frameworks aimed at eliminating vendor lock-in for enterprises.*
>
> ***The Open Cloud Consortium (OCC)*** *supports the development of standards for cloud computing and frameworks for interoperating between clouds. They develop benchmarks and support reference implementations for cloud computing. (Rhoton, 2010)*

6.2. Cloud Security

In a coordinated effort make cloud computing more secure, over the past four years, the Cloud Security Alliance gathered a broad set of stakeholders and around 120 corporate members to discuss, evaluate and define best practices and guidance to mitigate risks associated to cloud computing adoption.

Several publications have been released, including a comprehensive publication "Security Guidance for Critical Areas of Focus in Cloud Computing" which is now in its 3rd version, as well as the "The Notorious Nine Cloud Computing Threats", amongst several other publications reflecting industry best practices and knowledge from industry stakeholders from around the world. The nine notorious threats reported are Data Breaches, Data Loss, Account or Service Traffic Hijacking, Insecure Interfaces and APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence and Shared Technology Vulnerabilities.

The third version of the flagship "Security Guidance for Critical Areas of Focus in Cloud Computing" has defined 14 domains involved in governing or operating the cloud:

1. Cloud Computing Architectural Framework;
2. Governance and Enterprise Risk Management;
3. Legal: Contracts and Electronic Discovery;
4. Compliance and Audit Management;
5. Information Management and Data Security;
6. Interoperability and Portability;
7. Traditional Security, Business Continuity, and Disaster Recovery;
8. Data Centre Operations;
9. Incident Response;
10. Application Security;
11. Encryption and Key Management;
12. Identity, Entitlement, and Access Management
13. Virtualization;
14. Security as a Service;

In the words of the editors of the publication, in its 3rd edition "the guidance assumes a structural maturity in parallel with multinational cloud standards development in both structure and content" (CSA - Cloud Security Alliance, 2011).

7. Impact of cloud computing

7.1. Technology

Technology is certainly where the impact of cloud computing is most evident as new service delivery models have already changed the way end users and companies consume and pay technology services. Cloud computing also offers significant potential to offload batch processing, analytics and compute-intensive desktop applications. Mobile technologies may also benefit from the high availability and coverage of cloud providers and reduce risks associated to mobile computing as more sensitive data could be stored on the cloud instead of the device. Disjoint technologies are increasingly getting connected such as Cloud Print Services triggered from mobile devices. (Rhoton, 2010)

7.2. Business

Business are experiencing a huge impact with the advent of cloud computing. Again, cloud is changing not only the raw computing and connectivity, it is dramatically changing traditional processes, workflows and time scales. The move from CAPEX to OPEX, the agility to scale up and down, the outsource of IT infrastructure management allows for increased focus on core competencies. Companies become more flexible to adapt and respond to changes in market conditions. Moreover, the crescent level of standardisation entailed by cloud computing might blur traditional distinction between small, medium business and enterprises (Rhoton, 2010).

7.3. Economy

The technology and business impact might influence the economy eliminating barriers for many industries, leading to enhanced startup speed and a larger number of smaller companies entering the market. Knowledge workers can become increasingly independent of large corporate infrastructure. Increasing amount of media and content might be found through "crowdsourcing" initiatives. There are also speculations on the possibility of the erosion of the middle class as a consequence to the increase in the availability of skills from volunteer work and the corresponding polarisation of income only on the very successful. The low entry barrier also fostered venture capital investments on small startups due to reduced risk. On the other hand, small firms are less reliant on external investors due to the ubiquity and affordability of high quality resources available on the cloud. (Rhoton, 2010).

High performance computing on the cloud have paved the way for the appearance of virtual money such as Bitcoin, which is already being traded on financial markets and requires intensive computing to "mine" new coins.

7.4. Social

A multitude of web 2.0 enabled SaaS such as e-mails, social networking, online and mobile image and video sharing have already changed the way people communicate or look for a job today. Possible increases in off-shoring can occur by virtue of the location independence. Privacy invasions, and the increasing tolerance to privacy invasions, might have profound impacts if they occur in large scale (Rhoton, 2010).

7.5. Political

Politicians have to address all the above mentioned impacts, reviewing, updating, creating new regulations, compliance, overseeing developments, ethical implications and assessing potential risks. On the other hand, social networking have played an important role enabling unprecedented protests that quickly jump from the virtual world to the physical world (Rhoton, 2010).

8. Discussions

Notwithstanding the compelling benefits associated to cloud computing, legitimate challenges, risks and issues are associated with the new paradigm and, as should be the case with the adoption of any new technology, a move towards cloud computing should be considered with precaution.

New problems and challenges associated with cloud computing are regularly being posed to the cloud community, including IT practitioners, managers, governments and regulators (Buyya, Vecchiola, & Selvi, 2013).

Besides the practical aspects related to configuration, networking and sizing, a new set of challenges concerning the dynamic provisioning of services and resources are yet to be tackled.

As an example, in an IaaS, how many resources need to be provisioned, and for how long, in order to get the maximum benefit? (Buyya, Vecchiola, & Selvi, 2013).

Amongst numerous developments taking place in the cloud computing arena, standards, interoperability and security developments are probably the most crucial. A huge leap was achieved in terms of computing, storage and networking scalability. However, the lack of standards acts as a huge bottleneck for the adoption on cloud computing. Additionally, solid guidelines and best practice security frameworks to support prevention, audits and security benchmarks are still in its initial steps of development.

Themes such as confidentiality, secrecy, compliance have still a long way before reaching its maturity.

Regulatory issues are particularly threatening due to the distributed and ubiquitous nature of the cloud, making it difficult to keep control of the physical location and ownership of the data.

On the other hand, cloud computing is already enabling innovative approaches in virtually every aspect of our lives, some of them are presented in the next session, in which five papers are reviewed and discussed.

9. Discussed Papers

9.1. Paper I - (Marathe, Harris, Lowenthal, & de Supinski, 2013)

A Comparative Study of High-Performance Computing on the Cloud

This paper evaluates the appropriateness of cloud computing as an alternative to dedicated high-performance clusters typically used in large compute centres such as those found in national laboratories where high-performance computing (HPC) is employed.

Several previous studies have discussed and compared the performance of dedicated high-performance clusters in relation to commercially available cloud computing services, like Amazon EC2 for example, using benchmarks such as NAS Parallel, ASC Sequoia and ASC Purple.

These studies have consistently demonstrated the superiority of HPC clusters in terms of raw performance and contributed to the prevailing notion that cloud computing services such as EC2 are useless for typical HPC applications.

Unlike the preceding studies, which took *raw computing performance* as the unique comparison factor, this study considered both *turnaround time* and *cost* to compare the two alternative computing solutions from the HPC user perspective.

This broader approach makes huge sense as different combinations in terms of average waiting queues, as well as project time or budget constraints will result in different "efficiency needs" from the HPC user standpoint. For a project tightly constrained in terms of budget, lower raw computing performance might be acceptable, provided that it allows for budget savings. In other situations, clusters with the highest raw performance might not provide the best turnaround time for the project due to long waiting queues before the application actually starts.

To perform their experiment, the researchers compared five different HPC clusters from the Lawrence Livermore National Laboratory (LLNL) to the "Cluster Compute Eight Extra Large", or simply "CC2", offered as part of Amazon's EC2 services.

Cluster Name	CPU speed (GHz)	Cache size (MB)	Memory size (GB)	Cores per Node	Interconnect Technology
Sierra	2.8	12	24	12	Infiniband QDR
Hera	2.3	0.5	32	16	Infiniband DDR
Cab	2.6	20	32	16	Infiniband QDR
Hyperion	2.4	6.0	12	8	Infiniband DDR
uDawn	0.85	0.02	2	4	3d Tours
Amazon EC2	2.59	20	23	16	10 GigE

Table 1 - System specification for the study

After comparing the total turnaround time for typical HPC benchmarks at different scales, the study used economic theory to develop an economic model to establish a cost baseline for the LLNL clusters in order to compare with Amazon EC2 price model.

Contrary to the prevailing perception, despite of having much higher latency and much lower bandwidth, EC2 execution and turnaround times outperformed LLNL clusters in jobs with lower task volume. With higher task count, LLNL clusters usually have faster execution, however in several occasions turnaround time is compromised by long queue wait times. EC2 offer better turnaround and costs in several benchmarks and it appropriateness, as well as the appropriateness of each of the five LLNL clusters, vary from application to application depending on how computing intensive, communication intensive is the application, as well as the number of tasks involved.

9.2. Paper II - (Zhang, Wu, & Cheung, 2013)

A Survey on Cloud Interoperability: Taxonomies, Standards, and Practice

In this paper, the authors present the state-of-the-art in terms of cloud computing standards definition and adoption.

Despite of the vertiginous advances of cloud computing in recent years, and the rapid proliferation of cloud service vendors such as Amazon, Google, Microsoft and SalesForce, each vendor promotes its own cloud infrastructure and incompatible standards and formats to access the cloud.

While the lack of interoperability among cloud providers might be temporarily interesting from the provider perspective, it is certainly not sustainable in the long run. For this reason, several standardisation initiatives have emerged involving academia and industry contributors.

Among other definitions, the study refers to the European Commission concept of interoperability which, applied to the cloud computing arena, could be translated as the "ability to understand each other's application formats, SLA templates, formats of authentication and authorisation token, attribute data and others, such that different clouds can cooperate or interoperate".

As Software as a Service (SaaS) interoperability is mostly related to data, the article focuses on interoperability among IaaS clouds, adopting the following taxonomy:

Access Mechanisms: How developers and users can access services through Application Programming Interface (API), Graphical User Interface (GUI) and Command-Line Interface (CLI);

Virtual Appliance: Standards for virtual machines (VM) containing complete software stack installed.

Storage: Standards for Management and organisation of storage and also, standards for backup, replication and snapshots.

Network: Standards for resource "Addressing" over network and "Application-level communication" using RESTful APIs in order to minimise coupling between client and server components.

Security: Standards for authentication, authorization, accounting and encryption.

Service-Level Agreement (SLA): Standards for SLA Architecture, template format, monitoring and SLA Objectives.

Amongst the various standardisation efforts, the study have considered prominent working groups, including those operating under the Open Grid Forum (OGF) umbrella, the Distributed Management Task Force (DMTF) consortium and the Storage Networking Industry Association (SNIA).

The authors discussed three major open standards which are widely adopted nowadays, namely Open Virtualization Format (OVF), The Cloud Data Management Interface (CDMI) and Open Cloud Computing Interface (OCCI).

OVF is a packaging standard for deployment of virtual appliances, currently supported by many platforms including IBM, Microsoft, Jump-Box, virtualBox, XenServer, ABiCloud, OpenNode Cloud, SUSE Studio, Morfeo Claudia and Openstack.

CDMI defines a functional interface that applications can use to create, retrieve, update and delete data elements from a cloud by abstracting storage containers which contain data objects, acting as a storage backbone in cloud interoperability.

OCCI acts as a service front-end to an IaaS provider's internal infrastructure management framework, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling and monitoring.

The study provides an overview of three state-of-the-art implementations of IaaS cloud management system:

OpenStack: Comprised of a compute controller, storage systems, virtual machine image service and networking service, is particularly effective for the network addressing issue over WAN (wide area network) and comes equipped with a software-defined network functionality.

Eucalyptus: Consisting of a Cloud Controller, Walrus Storage, Cluster Controller, Storage Controller and Node Controller, this system creates scalable private and hybrid clouds within one's existing IT infrastructure and features high-fidelity Amazon AWS (Amazon Web Services) API implementation providing easy interoperability with AWS clouds.

OpenNebula: An open-source data centre visualization technology offering feature-rich, flexible solutions for the comprehensive management of virtualised data centres to enable on premise infrastructure as a service clouds. The system offer four main different interaction perspectives: Cloud interface for Cloud Consumers, Administrator interfaces for Cloud Administrators, extensible low-level APIs for Cloud Integrators and marketplace for Appliance Builders. It also offers full Amazon EC2 Query interface, enabling seamless integration with Amazon EC2 clouds.

In addition the "Vendor-centric" standardisation, the study discusses the "user-centric" approach to standardisation as a means to overcome the dependency on the industry players adherence to standards, which can take too long to happen, if ever. The user-centric approach uses a Xen-Blanket hypervisor on top of another hypervisor (Xen or KVM), allowing for the migration of Virtual Machines between Amazon EC2 without any modification.

Finally the study discuss the availability of interoperability libraries such as LibCloud and δ-Cloud to support the development of interoperable applications. These libraries provide abstractions that help developers write applications without being tied to a specific cloud vendor or an intermediate layer such as OpenStack.

The authors conclude their study pointing out that many missing issues are still open and a lot of tasks remain to be addressed in areas such as, "network virtualization", "SLA Interoperability" and "Resource Pricing" which becomes particularly complex in case of nested virtualisations as is the case with the use of Xen-Blanket hypervisors in "user-centric" standardisation.

9.3. Paper III - (Hasteer, Murthy, & Bansal, 2013)

Pragmatic assessment of research intensive areas in cloud: A systematic review

This paper offers a systematic review of research intensive areas in the field of cloud computing in the period from 2009 to 2012.

After presenting a brief overview of cloud computing concepts, the study relates to the increasing popularity of the subject in the media, also mentioning the importance of cloud computing and future adoption projections as portrayed by renowned industry research reports such as IDC Cloud Report.

Given the crescent attention to the subject, and the rapid growth rate being experienced by cloud services, the study aimed to identify the nature and the extent of the work done in this field and point out important areas to realise its potential:

a) Assessing and categorizing the work accomplished so far;
b) Collecting evidence that suggests implications for practice;
c) Identifying areas and problems that need attention.

Although no previous systematic review has been performed on intensive research areas in cloud computing, relevant related reviews on specific fields were mentioned such as *Intrusion detection and prevention in Cloud Computing* (CIDPS), as well an empirical examination of switching behaviour from traditional IT to Cloud Services from the two factor theory perspective. A bibliometric analysis on search based software engineering and a study on the commoditisation of computing and its consequent delivery model as a utility were also cited.

The study followed the Kitchenham guidelines for systematic reviews order to answer the following questions:

1. What are the key areas of research in the cloud environment?
2. What is the nature of work that has been accomplished so far?
3. What are the vital benefits of the work to researchers and practitioners?
4. What are the gaps in the current state of research?

After defining a set of search keywords, its corresponding synonyms, and searching on ACM Digital Library, IEEE Xplore, Elsevier and Google Scholar databases, some exclusions were performed based on relevance or to eliminate redundancy, resulting in 36 relevant studies to be considered.

The studies were then categorised in four groups: I – Cloud Services, II – Cloud Migration, III – Cloud Deployment, IV – Cloud Security, with six, five, ten and sixteen papers respectively.

The results show that security is certainly the most researched topic, however the author points out that laws in cloud computing are yet to be formulated. The study also indicates the lack of research related to development models to cater to multi-tenancy architecture, as well as few studies related to variability of quality attributes in computing as a service.

In my opinion, the study have not addressed its research questions properly. Also, I is questionable whether the search keywords and categories used to group previous researches are really adequate for the intent of this work. A more efficient review should probably consider less specific keywords and define more specific categories based on the papers found.

9.4. Paper IV - (Duygu & Seref, 2013)

A review on cloud security

This paper provides a general review on security areas, standards and most relevant issues associated to cloud computing.

The authors introduce the concepts of cloud computing, highlighting benefits such as minimal maintenance efforts and costs, as well as high availability and dynamic scalability of computer resources charged based on usage. Cloud computing is described in light of the definitions provided by the National Institute of Standards and Technology (NIST) of the United States of America, consisting of five essential characteristics, three service models and four deployment models.

On the other hand, the study points out security concerns such as data prevention, web security, location, identity and access management, recovery, data loss prevention, web and e-mail security, security assessments, regulatory compliance, violation management, encryption, data segregation, business continuity and disaster recovery arising from increasing adoption of cloud computing services.

The study then discusses new security threats and precautions that deserve special attention in the cloud computing environments.

Availability: The author mentions the importance to a careful attention to Service Level Agreements (SLA), as it regulates the maximum time for which resources may be unavailable. The study suggests that backups are “ideal way to reduce unavailability of resources because of a breakdown”, which I completely disagree, as the mere fact that a backup had to be used, means that you didn´t have the original resource available, hence, unavailability was not reduced. Moreover, it would be advisable to implement redundant infrastructure where possible and feasible, in order to ensure high-availability for critical systems.

Integrity: Making sure that the content is not unintentionally or maliciously modified or destroyed.

Confidentiality: Ensuring that information is only accessible to authorised users.

Multi-tenancy: Distinct tenants should have their information isolated from each other.

Elasticity: While scaling up and down, might cause one resource previously assigned a consumer to expose information from that consumer when the same resource is reassigned to other consumers.

Privacy: Intimately connected to confidentiality, privacy protection such as encryption and other mechanisms should be embedded in all security solutions and instances.

Audit: Verification of logs, events and monitoring to be performed by a Third Party Auditor (TPA) to verify integrity of data in cloud on behalf of cloud client.

Trust: Heavily dependent on the deployment model. Should be handled in all levels, internally and externally to cloud providers. In some situations Trusted Third party (TTP) relationships can be established in the provision of confidentiality, authentication and authorization.

Nonrepudiation: To prevent the issue of denial, nonrepudiation enabled protocol or handshake should be implemented.

Data leakage: Data Leakage Prevention (DLP) applications should be used to protect sensitive data in association with strong encryption mechanisms.

Deployment models: Security level varies according to deployment models. Public clouds offer are the least secure as they offer less control to end user. Private cloud are the most secure, as they allow for full control of the cloud environment.

Service Models: Service models also offer different security levels, being the SaaS (Software as a Service) the level where users have less control over security and IaaS (Infrastructure as a service) where users have more security control.

Stakeholders: Weak security habits from the end users, malicious customers, hackers, and privilege management of internal workers are some of the threats arising from different stakeholders.

Attacks: A flaw in one client's application might open the door to the entire cloud exposing other tenants. Host Intrusion Prevention Systems (HIPS) should be implemented as hackers can now use an array of cloud servers to crack an encryption key in minutes.

The study also mention five Cloud Security Models:

I. International Telecommunications Union's (ITU) Networks and Open Communications Security architecture for Systems Providing End to End communications;
II. The Cloud Multiple Tenancy Model of NIST;
III. Cloud Cube Model;
IV. Sood's Combined Approach;
V. CCMDSM – Cloud Computing Multi-dimension Data Security Model.

Although the authors provide a brief comparison of the advantages and disadvantages of each model, It is not clear whether those factors are valid for all deployment of service models or.

Finally the study presents the results of a review of forty relevant papers to determine the main research topics on cloud security, being the "Challenges" the most addressed topic, followed by security solutions, security metrics and security strategy, being models or architectures the least researched topic.

A comparative matrix displays the security issues most highlighted in the reviewed literature, featuring Privacy, Availability, Integrity, Confidentiality and attacks as the most prominent subjects in most recent years.

9.5. Paper V - (Chen , Lin, Li , Hsu , & Chen , 2014)

A scalable blackbox-oriented e-learning system based on desktop grid over private cloud

In this study, the authors developed an innovative approach by merging volunteer computing in and a private cloud computing to achieve scalability, enhance responsiveness and address typical security risks of a web-based e-learning system.

The application in context is a black-box “programming language e-learning system”, in which the student is assessed according to the outcomes of their programming work regardless of the internal code used solve a given problem. Such e-learning environment is characterized by unstable workloads and security risks brought by external executable objects incorporated to servers.

The authors have implemented a private cloud, complemented by a grid of virtual machines built on top of learner’s desktop, powered by BOINC, a volunteer computing platform successfully employed for large scientific research in fields as biology, astrophysics, engineering and climate. On top of these two technologies, a web server and the e-learning system itself use BOINC API (Application Programming Interface) to automate the deployment of standard virtual machines (VM) on top of the volunteer computers.

When connecting to the e-learning system, the users are not only consumers of computing resources, but also a volunteer computing resource providers when idle capacity is available. Due to the intermittent nature of the development work, the overall system performance and responsiveness scales in direct correlation to the number of simultaneous users.

To allow for better computing tasks distribution algorithms, the system differentiates virtual machines built on top of the volunteer desktop grid, defined as volunteer workers (VW) and the private cloud infrastructure servers, defined as official workers (OW) used to ensure minimum level of computational capacity when the simultaneous users are below a certain threshold.

As the number of simultaneous online users grow, the private cloud offloads work to the desktop grid using BOINC server, which breaks each task into small “wrokunits” and distributes to volunteer workers. Redundant computing is used to address issues such as malicious attacks, network latency and hardware malfunctions. This technique dispatch two or more replicas of the same job to different computers and consider the job complete only after receiving exact the same results from a certain number of volunteers.

The experiment tested three four different configurations for task distribution policies, one involving only volunteer workers (VC_conf) and standard scheduling algorithm, another which is the same as VC_conf, however adding two official workers (OC_conf), a third configuration which is the same as the previous, except for the use of the optimised workunit-based algorithm and, the last configuration, being traditional client-server (CS) setup for all tasks.

For up to ten simultaneous users, the CS setup outperformed the other configurations, as BOINC infrastructure posed an overhead which didn´t compensate for small loads. However, for higher number of simultaneous users, the VC_conf offered considerable improvement. OC_conf didn’t offer considerable improvement over VC_conf, as dozens of volunteers are capable of fetching the majority of the tasks. And the WU_conf have proven to be even more efficient.

The approach proven to be an efficient way to scale system resources. Also is interesting to note that a single idle volunteer can add considerable computing capacity to the overall system.

10. Conclusion

Cloud computing as a multi-faceted topic, whose ramifications spread across a myriad of other topics which, in many cases, are multi-faceted as well, ranging from very technical aspects to social, economic and political implications.

While there is relative consensus on the general notion of what cloud computing is all about, a precise and comprehensive definition of cloud computing is yet to be created, if ever.

This study managed to compile the views of several authors to provide an outline of the core ideas associated to cloud computing, its underlying technologies, historical development and drivers behind the evolution of this paradigm.

Despite of the great achievements obtained so far, it is clear that that computing is still in its infancy, and the real revolution is yet to come.

With ubiquitous high-performance computing and communication unleashing cooperation, problem solution and knowledge building at vertiginous speed, cloud computing is paving the way to profound and unparalleled social transformations to take place sooner than most of us would expect.

11. References

Brogi, A., Ibrahim, A., Soldani, J., Carrasco, J., Cubo, J., Pimentel, E., & D'Andria, F. (2014, 01). SeaClouds: A European Project on Seamless Management of Multi-cloud Applications. *SIGSOFT Softw. Eng. Notes*, pp. 1-4.

Buyya, R., Broberg, J., & Goscinski, A. (2011). *Cloud Computing Principles and Paradigms.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). *Mastering Cloud Computer.* Waltham,MA: ElsevierInc.

Chen , L.-P., Lin, J.-A., Li , K.-C., Hsu , C.-H., & Chen , Z.-X. (2014, 03 20). A scalable blackbox-oriented e-learning system based on desktop grid over private cloud. *Future Generation Computer Systems, 38*, pp. 1–10.

CSA - Cloud Security Alliance. (2011). Defined Categories of Service 2011. Retrieved from https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/

CSA - Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus in Cloud Computing. (v3.0). Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

CSA - Cloud Security Alliance. (2013, Feb). The Notorious Nine Cloud Computing Top Threats in 2013. (T. T. Group, Ed.) Retrieved from http://www.cloudsecurityalliance.org/topthreats

Duygu , S., & Seref, S. (2013). A Review on Cloud Security. *Proceedings of the 6th International Conference on Security of Information and Networks*(SIN '13), pp. 321--325.

Gartner. (2012). *Hype Cycle for Cloud Computing, 2012.* Gartner. Retrieved from https://www.gartner.com/doc/2102116/hype-cycle-cloud-computing-

Gartner. (2013, Oct 24). *Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016.* Retrieved from Gartner: http://www.gartner.com/newsroom/id/2613015

Hasteer, N., Murthy, B., & Bansal, A. (2013, 05 13). Pragmatic assessment of research intensive areas in cloud: a systematic review. *ACM SIGSOFT Software Engineering Notes, 38*(3), pp. 1-6. doi:10.1145/2464526.2464533

Josyula, V., Orr, M., & Page, G. (2012). *Cloud Computing: Automating the Virtualized Data Center.* Indianapolis: Cisco Press.

Li , Z., Mitra , K., Zhang , M., Ranjan , R., Georgakopoulos , D., Zomaya , A., . . . Sun , S. (2014, 16 01). Towards understanding the runtime configuration management of do-it-yourself content delivery network applications over public clouds. *Future Generation Computer Systems*.

Mahmood, Z., & Hill, R. (2011). *Cloud Computing for Enterprise Architecures.* Springer.

Marathe, A., Harris, R., Lowenthal, D., & de Supinski, B. (2013). A Comparative Study of High-performance Computing on the Cloud. *Proceedings of the 22Nd International*

Symposium on High-performance Parallel and Distributed Computing(HPDC '13), pp. 239-250.

NIST. (2011). *The NIST Definition of Cloud Computing.* Special Publication 800-145 , National Institute of Standards and Technology, Gaithersburg, MD.

Perez-Botero, D., Szefer, J., & Lee, R. (2013). Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. *Proceedings of the 2013 International Workshop on Security in Cloud Computing*(Cloud Computing '13), pp. 3-10.

Rhoton, J. (2010). *Cloud Computing Explained* (2nd ed.).

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud Computing: Implementation, Management and Security.* Boca Raton: CRC Press.

Rosenberg, J., & Mateo, A. (2011). *The Cloud at Your Service.* Greenwhich: Manning Publications Co.

Sosinsky, B. (2011). *Cloud Computing Bible.* Indianapolis,: Wiley Publishing, Inc.

Vaquero, L., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009, January). A Break in the Clouds: Towards a Cloud Definition. *SIGCOMM Comput. Commun. Rev., 39*(1), pp. 50-55.

Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach.* New York: McGraw Hill.

Winkler, V. (2011). *Securing the Cloud.* Waltham, MA: Elsevier Inc.

Yadav, N., Khatri, S., & Singh, V. (2014, January). Developing an Intelligent Cloud for Higher Education. *SIGSOFT Softw. Eng. Notes, 39*(1), pp. 1-5.

Zhang, Z., Wu, C., & Cheung, D. (2013, 04). A Survey on Cloud Interoperability: Taxonomies, Standards, and Practice. *SIGMETRICS Perform. Eval. Rev., 40*, pp. 13-22.