Cloud Server Weather Station using Raspberry Pi

PROJECT REPORT

submitted for the course

Microprocessor and Interfacing (CSE2006)

by

Nikita Negi	16BCE2038
Pankita Shrivastava	16BCE2016
Akshaya B	16BCB0116

Winter Semester 2017 - 2018

Slot: B2

Name of Faculty: Prof. Jimmy Mathew

SCOPE

Curriculum for Applied Learning

Index

1. Abstract

This project aimed to create a proto type system which employs the services of a Raspberry Pi for observing the weather changes. This proto type discusses a monitoring system which gives information about environmental conditions on a more local level and briefly touches the technological advancements in monitoring the environment and bringing out the new scope in monitoring the current environment problems. The system could monitor surrounding weather conditions including humidity and temperature. This prototype and comparative analysis of the environment system was applied in different weather conditions. This prototype system was found to be comfortable for day to day use for effectively monitoring the climatic conditions anywhere at any time, which results cost reduction, asset saving, and productive management in for anyone interested in knowing the weather conditions at any given time, be it the common public or meteorologists. The prototype system is developed using open source hardware Raspberry PI and WIFI which proves cost effective and having low power consumption. Weather forecasting has to be reliable and accurate, regardless of its application. Also, it has to provide simple access to all the measured parameters. The quality of sensors and precision of measurements may vary, and the location of weather forecasting station can determine the accuracy and reliability of the weather data collection. The sensors gather the data of various environmental parameters and provide it to Raspberry PI which acts as a base station. The Raspberry PI then transmits the data using WIFI and the processed data will be displayed on laptop or any remote server having VNC viewer environment through accessing the server that is on the receiver side.

The current method of sharing files in a group involves a separate hardware (pen drive, hard disk etc.) or a working Internet connection to use cloud storage such as Google Drive, Dropbox etc. Such methods involve large investments in setting up a server in the form of a supercomputer, and the efficiency drops. Moreover, they are limited by the speed of the network. The purpose of our project is to create a Raspberry Pi server which allows you to share files on the same network without the use of any supporting hardware or a working Internet connection, hence saving time and increasing efficiency. Moreover, data can be easily accessed and a number of people can access the same data at any given time. The proposed system involves setting up a server using a Raspberry Pi. Files can be uploaded on the Pi server and it will create a hotspot, such that other laptops can connect to it and access the shared files. This enables file sharing and collaboration on projects etc. without the use of an external storage device or a working Internet connection. It also creates an additional layer of security by enabling the user to access the server only using a valid IPv4 address.

We used the features of the weather station and combined them with the hosting facilities of a cloud to create a dynamic weather station cloud server that can be accessed by users to get new and accurate details about temperature and humidity.

2. List of components

1. Raspberry Pi:

The model that we used required Wi-Fi compatibility, so we used the Raspberry Pi 3 model B+. It has a Broadcom BCM2837 processor quad core A53 (ARM v8), gigabyte Ethernet, USN connector for 5.1V D.C. Its cost was around Rs. 2,500.

2. SD Card:

We used a Strontium Nitro 433X 16GB micro SD card. It contains all the necessary softwares and libraries such as python, MySQL, Apache, PHP, Raspbian OS etc. Its cost was around Rs. 400.

3. Wires:

We have used some standard jumper wires with a pack costing around Rs.300.

4. Resistor:

We employed a 10 ohms resistor in between the 5volt power supply and the ground. It cost around Rs. 70.

5. DTH11:

To sense weather conditions, we used a DTH11 sensor. It measures temperature in degree Celsius and humidity in percentage. It runs on 5V DC and has a measurement range of 20-95% humidity and 0-50 degree Celsius. Its cost was around Rs. 225.

6. Breadboard:

To make stable connections, we used a standard solder less breadboard with 840 tie points. Its cost was around Rs. 100.

7. Data cable:

We used the USB data cable to provide power to the Raspberry Pi. Its cost was around Rs. 70.

8. Remote server:

This can be any device having Raspbian OS or VNC server installed. We used our personal mobile phones so the cost for this was zero.

Total cost of the project: Rs. 3665

3. Circuit diagram

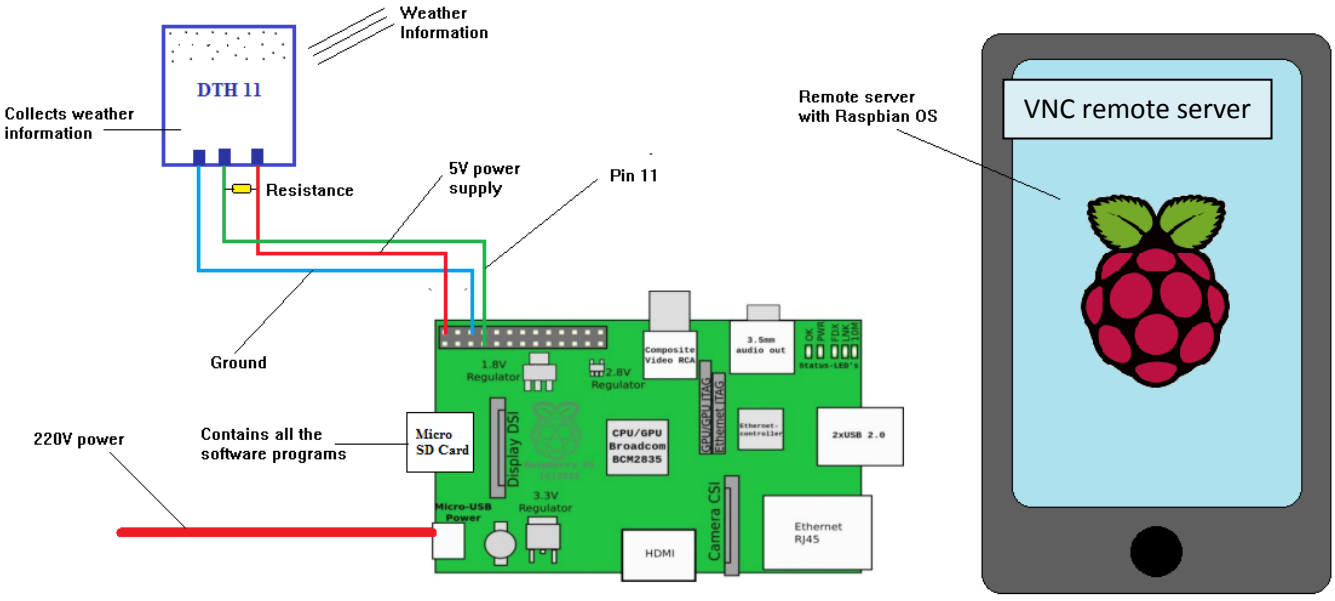

Fig 1. Circuit Diagram

The above diagram shows the various hardware components that are employed for the proper functioning of the system. The above diagram depicts how the various components are physically connected and how they interact with each other.

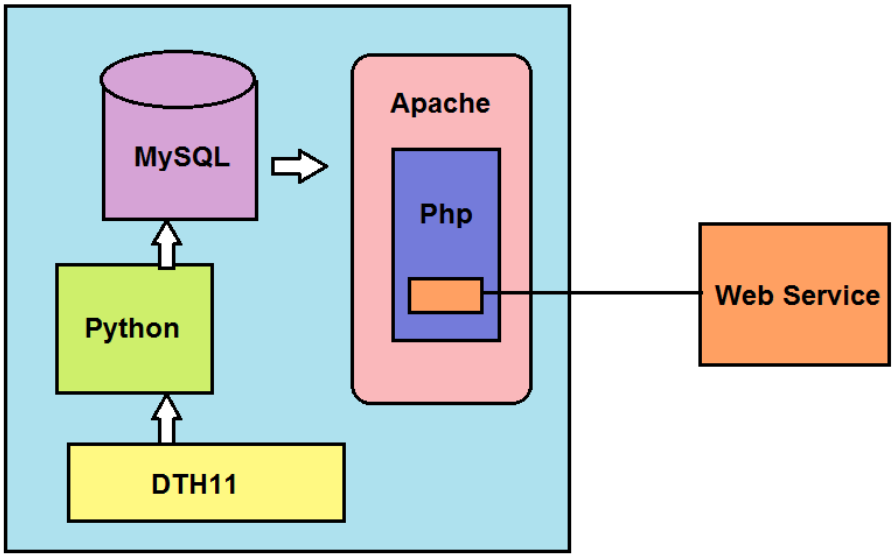

Fig 2. Project Environment

The DTH11 is responsible for collecting temperature and humidity readings from the environment. It is prompted by the python module to get refreshed readings every second. These readings are passed on to MySQL which acts as a database. To transfer these readings to the cloud server, Apache employs the services of PHP that deploys these readings on the cloud to be read by a remote server using a VNC viewer platform, having appropriate access.

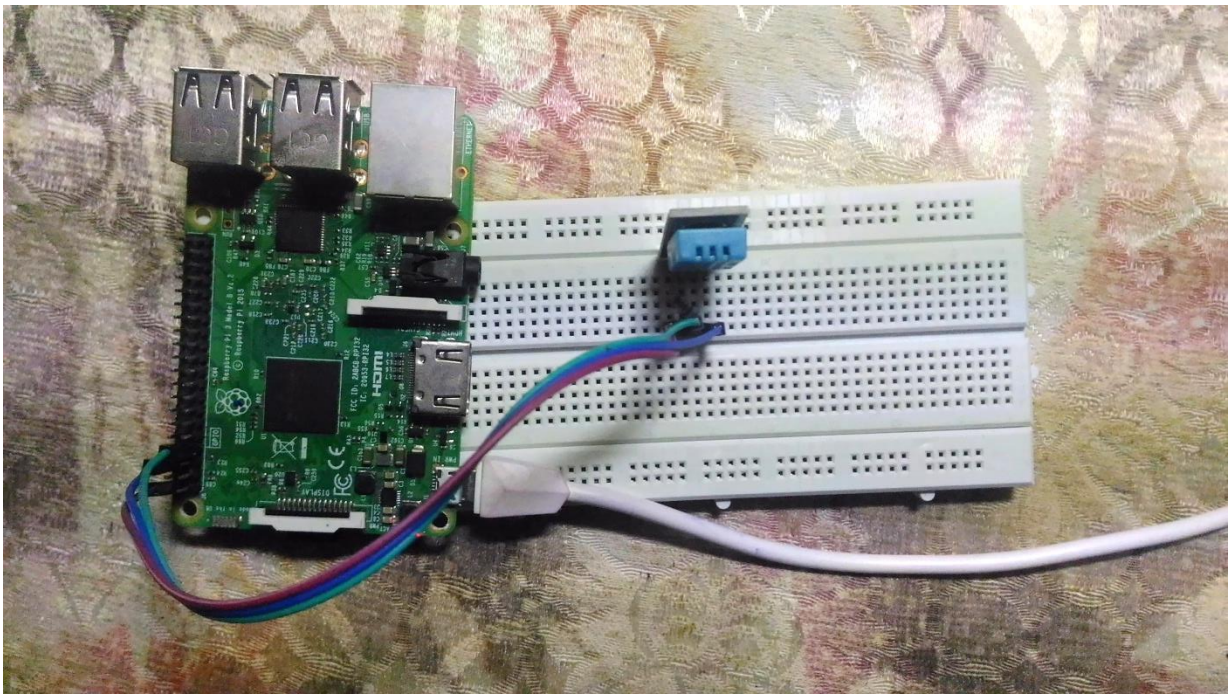

Image 1. Project Setup

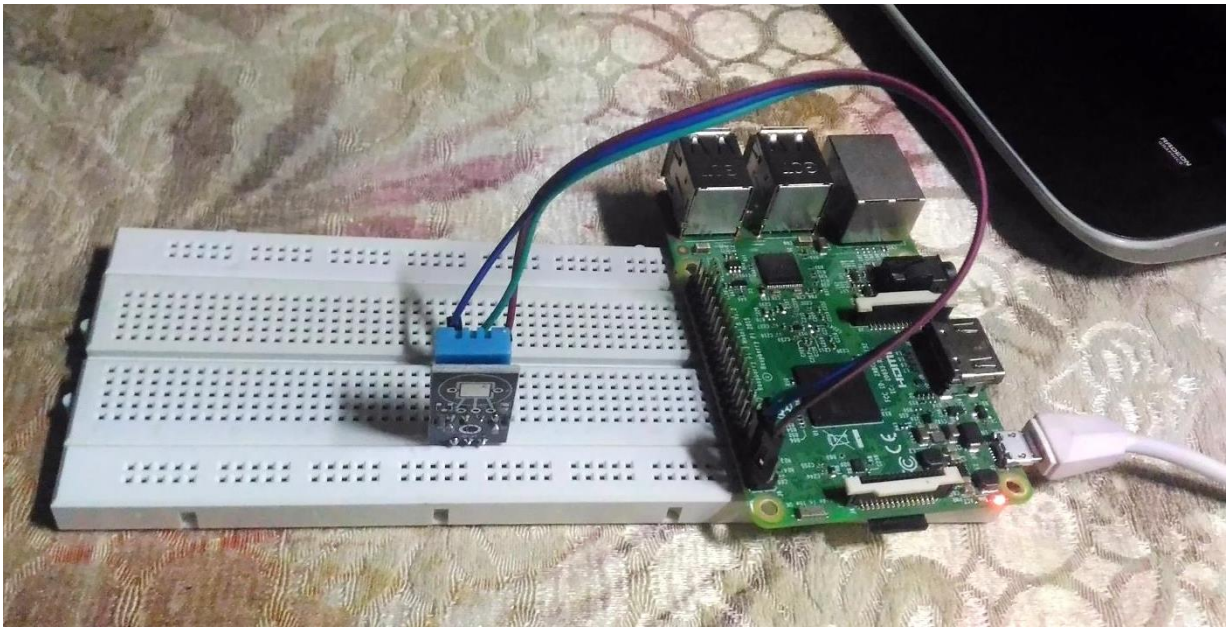

Image 2. Project setup

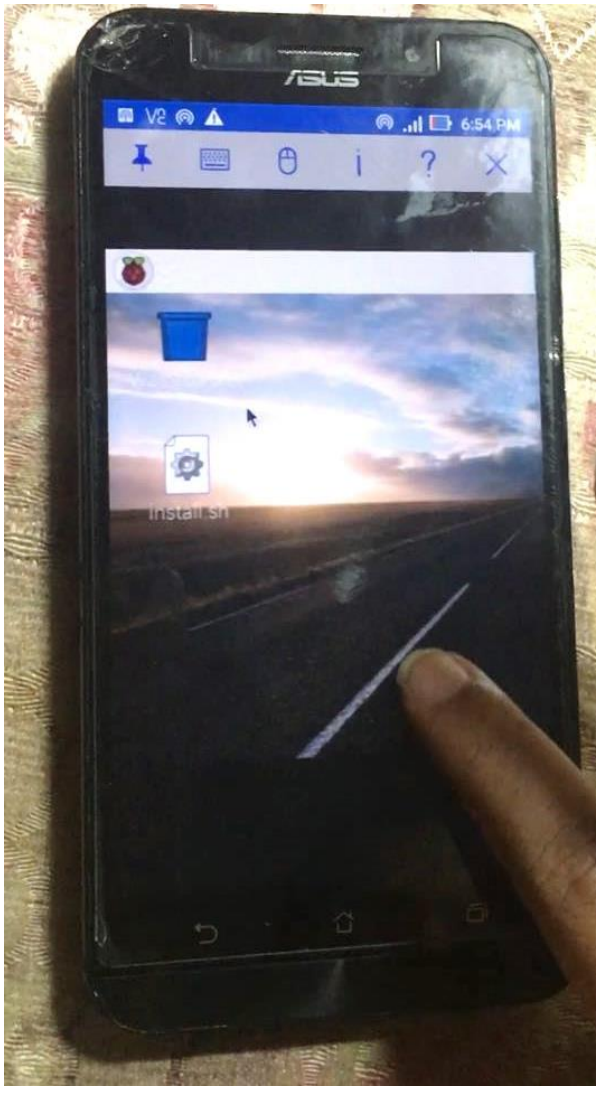

Image 3. VNC remote server

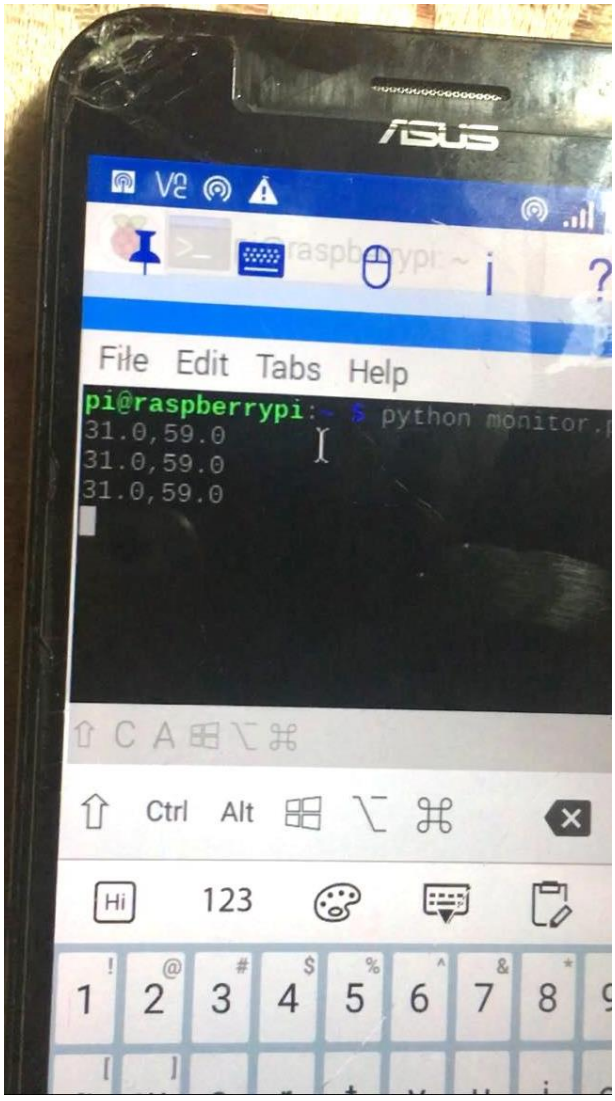

Image 4. Server readings

4. Modules

1. Analysis of threats: Akshaya
Studied the base paper carefully and listed the important treats related to our project

2. Coding of the raspberry pi: Nikita
Coded raspberry pi successfully including all the softwares and libraries.

3. Implementing on VNC viewer: Nikita
Converted our phone to remote server and opened Raspbian OS. Typed the necessary commands in python and output could be seen

4. Ensuring the smooth transfer of data over the cloud in a secure channel: Nikita
Making sure that the data is updated on cloud without any problems.

5. Installing important software and transferring it in SD card : Pankita
Installed all important software like rasbian-stretch-lite.zip, Win32diskimager-1.0.0, Putty, Xming-6-9-0-31, Ipscan-3.5.2

6. Compiling of the final research paper: Pankita
Collecting all the essential information and required subtopics and arranging them in form of research paper.

5. Self-assessment

Out paper was a theoretical study about different threats while sending data in cloud using raspberry pi .we have successfully uploaded the weather conditions on cloud and listed the treats which may affect our project

Threats we found in our project as compared to the base paper are –

1] Threat to the cloud applications :
The performance of CC depends heavily on networking and, therefore, any limitations or failures of the networking infra-structure (e.g. inside and between data center domains) can seriously impair the support of data-intensive and/or high-performance cloud applications. Threats of malware infections and data theft are lurking online. And since the Pi is just hardware where data is saved and loaded, the next logical step is to secure it.

2] Networking challenges in cloud:
The deployment of CC solutions in distributed data centers, concurrently with the universal users' access to the Internet, is challenging the research and standardization communities to modify existing network functionalities.

3] Maintenance and utility threat:
The virtualization of computing resources can offer significant advances in the following aspects: security, reliability, compatibility, utilization, maintenance, load balancing, and problem recovery.

4] Saas : limited access to the application:
In fact, the cloud subscriber only has a limited access to personalize any required application. Other limitations imposed to the cloud subscribers by the SaaS provider include the fact that only the SaaS provider can monitor the application-delivery performance.

5] Virtual Networking : Packet Sniffing and Spoofing threats:
This default behavior (behavior of VS where all frames with an unknown destination MAC is forwarded over the uplink to the physical external switch) can potentially create some security threats such as packet sniffing and spoofing. As an example, a VS access control list for security reasons can disallow two VMs located on the same physical host to have a direct communication between them. Sometimes it is not convenient to work directly on the Raspberry Pi. Maybe you would like to work on it from another device by remote control. VNC is a graphical desktop sharing system that allows you to remotely control the desktop interface of one computer (running VNC Server) from another computer or mobile device (running VNC Viewer). VNC Viewer transmits the keyboard and either mouse or touch events to VNC Server, and receives updates to the screen in return. You will see the desktop of the Raspberry Pi inside a window on your computer or mobile device. You'll be able to control it as though you were working on the Raspberry Pi itself.

6] Interoperability : Redundancy and incompatibility threats:
There is active standardization work in the CC area on inter-operability. Some coordination efforts have been established to minimize the problems of redundancy and incompatibility among specifications.

7] Security risks depend upon the cloud service model:
Saas interface (SaaS is short for software as a service). It is one of the more innovative new tools that has been developed for businesses. It is designed to help businesses integrate the applications they use into a format that they can use throughout their offices. One of the main things to consider is how the new software will work with your existing software, as well as with future software applications you may need to purchase.

- The SaaS interface can be maliciously hacked through application loopholes.
- The attacker can inject masked code into a SaaS system that can break isolation barriers.
- The lack of data integrity in the messages such that it can be changed during their transmission through the network in favor of a particular malicious intent of a man-in-the-middle attacker.

8] Open issues:
The first key issue is the dynamic management of cloud resources in resource-constrained scenarios or federated environments with service migration.
This resource management needs to be balanced against other aspects like notable fault tolerance, energy consumption, network utilization, load balancing, data congestion, data availability, harmonizing different security solutions within the cloud systems while maintaining performance, addressing multi tenancy security issues, namely to ensure the privacy during computations and security against insider threats

We feel that we have achieved a lot in this project. Not only have we covered all the bases as far as the paper is concerned, but we have also setup the practical examples of the review paper. We did a comparative study to see which threats are applied to our project, but we have also actually setup a remote server to dynamically display the weather station values of temperature and humidity on the server.

6. Summary

As per the objective of our project which was to create a Raspberry Pi server which allows us to share files on the same network, saving time and increasing efficiency, the project plan was carried out, to get an output of the readings of temperature and humidity through the VNC Viewer, which in turn accessed our raspberry pi through its IP address. We have also practically tried out our claim that, the server can host multiple clients from different platforms connecting to it at the same time and also the user needs to enter the valid IP address and port number to connect to the server. Thus, we can conclude that the Raspberry Pi efficiently does the work of weather station because of it's a compact yet very powerful device. In this project we have used sensors with digital input but with suitable A-D convertor we can easily use sensors with analog input. Data available on cloud server will be vanished automatically after several interval of time if we want. Comparison shown below satisfies how the discussed system is preferable in terms of cost and memory capacity.

The milestones of this project were:

- Selecting the base paper.
- Collecting hardware and software resources.
- Setting up the connections.
- Setting up the weather server.

The future of this system is very wide. Internet of Things is just opening its arms, Same system can be applicable to the variety of applications like Data monitoring ,sending and controlling of data at remote location.

7. Base paper

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Review and analysis of networking challenges in cloud computing

Jose Moura [a,n], David Hutchison [b]

[a] Instituto Universitário de Lisboa (ISCTE-IUL), Instituto de Telecomunicações, Portugal

[b] Lancaster University, InfoLab21, UK

article info

Article history:
Received 27 July 2015
Received in revised form 22 October 2015
Accepted 19 November 2015 Available online 11 December 2015

Keywords:
Cloud architecture Cloud solutions Security challenges Cloud DDoS Performance challenges

Management of cloud services in future networks

abstract

Cloud Computing offers virtualized computing, storage, and networking resources, over the Internet, to organizations and individual users in a completely dynamic way. These cloud resources are cheaper, easier to manage, and more elastic than sets of local, physical, ones. This encourages customers to outsource their applications and services to the cloud. The migration of both data and applications outside the administrative domain of customers into a shared environment imposes transversal, functional problems across distinct platforms and technologies. This article provides a contemporary discussion of the most relevant functional problems associated with the current evolution of Cloud Computing, mainly from the network perspective. The paper also gives a concise description of Cloud Computing concepts and technologies. It starts with a brief history about cloud computing, tracing its roots. Then, architectural models of cloud services are described, and the most relevant products for Cloud Computing are briefly discussed along with a com-prehensive literature review. The paper highlights and analyzes the most pertinent and practical network issues of relevance to the provision of high-assurance cloud services through the Internet, including security. Finally, trends and future research directions are also presented.

Contents

1. Introduction

The Cloud Computing (CC) market has been increasing very significantly. A recent study predicts that "from 2013 through 2016, $677 billion will be spent on cloud services worldwide" (Gartner, 2013). The CC paradigm involves moving both data sto-rage and applications into the network, offering to the users a ubiquitous access (Panagiotakis et al., 2015; Fernando et al., 2013). These resources are available via the cloud in the same way as they would have been previously using local computers. Nevertheless, CC resources are made available via distributed virtual servers. Such virtual servers can be moved among distinct physical servers and dynamically adjusted in terms of their memory, CPU, or sto-rage capacity, elastically following the users' load demand and satisfying their traffic requirements. CC is broadly accepted across the globe: diverse mobile operators (AT&T, 2012; BT, 2014; PT, 2014; DT, 2014; ND, 2014; MT, 2014) and technological enterprises (Salesforce, 2014; Google_a, 2014; Microsoft_a, 2014; Amazon, 2013; Dropbox, 2014; Microsoft_b, 2014; Google_b, 2014) are providing cloud services based on their network and computing infrastructures. In addition, four standardization organizations (one American: ANSI, which shares its CC vision with National Institute of Standards and Technology (NIST); and three European: CEN, CENELEC and ETSI) recently started a common initiative (ETSI, 2013) in several relevant areas, namely electric vehicles, smart grids, machine-to-machine (M2M) communication, smart cities, and more pertinently to this paper, CC. Furthermore, recent literature describes cloud systems and comprehensively discusses the most relevant decision aspects to make the move to CC (Badger et al., 2012; Jamshidi et al., 2013).

The performance of CC depends heavily on networking and, therefore, any limitations or failures of the networking infra-structure (e.g. inside and between data center domains) can ser-iously impair the support of data-intensive and/or high-performance cloud applications. Consequently, the deployment of CC solutions in distributed data centers, concurrently with the universal users' access to the Internet, is challenging the research and standardization communities to modify existing network functionalities. The need for these network changes is fueled by emerging CC usage scenarios with dynamic load, data mobility, addressing/routing based on data alternatively to IP destination, heterogeneous resources, federation, and energy-efficiency. The article we present here aims to add to the literature a compre-hensive and contemporary CC survey from the networking per-spective. Various and extensive work on CC can be found in the literature, as shown in Table 1.

The novelty of the work we present here, in relation to other surveys, is to discuss how the network architecture, protocols and algorithms should evolve to support cloud services more capably in highly dynamic and resource-constrained environments. In this way, we discuss aspects related to the future evolution of cloud systems, namely: reliable and efficient allocation of networking resources including virtualization and emergent security aspects. Another value of the current paper is to provide a single source of

Table 1
Cloud computing surveyed contributions.

Number	Reference	Main contribution
1	Vogels (2008)	Seminal work presenting important CC aspects from a hardware point of view: (i) illusion of infinite computing resources available on-demand; (ii) elasticity on resource usage according the demand; (iii) pay per use of com-puting resources on a short-term basis
2	Mei et al. (2008)	Presents a qualitative comparison between cloud, service and pervasive computing paradigms; this comparison was based on the classic model of computer architecture: I/O, storage, and computation
3	Buyya et al. (2009)	CC is envisioned as a paradigm that could deliver computing as the 5th utility (after water, electricity, gas, and telephony)
4	Armbrust et al. (2009, 2010)	Discussions about top 10 obstacles to and opportunities for growth of CC
5	Oracle (2010)	This paper presents an introduction to CC (i.e. essential characteristics; service and deployment models); it also discusses some cloud benefits and challenges
6	Zhang et al. (2010)	Extensive state-of-the-art implementation of CC; comparison of representative commercial products; discussion around research challenges
7	Duan et al. (2012)	A comprehensive discussion on Service-Oriented Architectures towards the convergence of Networking and CC
8	Alamri et al. (2013)	Focused on Sensor-Clouds
9	Dinh et al. (2013), Fernando et al. (2013)	Discussions on mobile cloud computing
10	Fernandes et al. (2014), Subashini and Kavitha (2011)	Stresses the distinct security requirements imposed by distinct cloud service models
11	Ali et al. (2015)	Discusses security vulnerabilities in mobile cloud computing

information compiling all the relevant CC studies, and providing readers with a concise update of this area.

The paper is also well aligned with the emergent networking proposals from both academia and standardization bodies to meet new cloud requirements. The authors have made an effort to assemble cloud resources and references and to present them at two levels; first, for those readers who are seeking to build knowledge on this topic; and second, for those seeking to progress their research. Finally, we identify current open issues that may form a barrier to the successful deployment and management of cloud services in future networks.

1.1. Organization of the paper

The main aim of this article is to review and analyze the major network functionalities that need to be modified or tuned to support the emergent properties of CC, using the present Internet infrastructure as a foundation. This contribution is organized as follows. Section 2 presents the main CC fundamentals and con-cepts, as well as tools and technologies to build clouds; this can help a non-specialized CC reader throughout the paper. Then, in Section 3, we narrow our discussion with a comprehensive review of recent literature discussing challenges imposed by CC in the current networking infrastructures. To structure our discussion a list of relevant networking aspects is suggested. Section 4 outlines research directions for future networks in support of CC applica-tions or services; this discussion is driven by representative sce-narios, namely the Internet of Things (IoT) and Network Functions Virtualization (NFV). In Section 5, we discuss current and future security challenges for cloud systems. Section 6 summarizes selected research challenges that could be addressed as future work. Finally, Section 7 concludes the article.

The next section offers background information, mainly dedi-cated to readers who are building their knowledge in CC. Readers already specialized in CC could jump to Section 3.

2. Background of cloud computing

This section introduces the main fundamentals and concepts that may be needed to follow the paper. We briefly present the historical evolution of CC; then we discuss the foundational technologies of CC, and compare the different CC service models.

2.1. History and emergence of cloud computing

This section presents the most relevant aspects related to the history of CC. We start, however, with the origin of "cloud"; this word means an abstraction of the underlying infrastructure (computers, networks, data storage) that enables the normal operation of any CC system. It is also why network infrastructures have for many years been represented by an iconized "cloud", hiding its complex details from non-specialized individuals. The additional words presented together with "cloud" identify the scope of that "cloud", and it could be for example any of the following: computing, networking, mobile computing, and sensor networks. In addition, CC glossaries are available in CCGa (2014) and CCGb (2014). Furthermore, some CC taxonomies are in Rimal et al. (2009) and Beloglazov et al. (2011).

Table 2 briefly shows the historical evolution of CC since the 1960s until 2011.

More recently, in 2013, an international congress (Services, 2013) gave special attention to Big Data Research and its major impact on social development (Obama, 2012). Big Data is a recent trend (Ward and Barker, 2013; Diebold, 2012; Press, 2013) which aims to extract pertinent knowledge from large-scale, complex, and unstructured data. This work is being carried out by numerous organizations including NSF, DoD, and DARPA. Some DARPA Big Data projects related to CC are described in (DARPA_a, 2013; DARPA_b, 2013). Big Data implementation strongly depends on the existence of Internet cloud solutions to support big data storage, to scale up the distributed/parallel processing power, to enhance collaborative work, and to support the efficient, secure, and private access of mobile terminals to heterogeneous data and services (Moura and Serrão, 2015).

Clearly, CC evolution is currently related to the increasing popularity of Big Data. In fact, CC provides the necessary compu-tation, storage, applications, and networking, which support Big Data applications. These applications empowered by CC solutions can extract very useful information to guide better decisions in many usage areas like business, finance, politics, education, mili-tary, industry, transportation, research, and even healthcare (Griebel et al., 2015).

There are also important research areas for Future Networks with a strong relation to CC. These include Internet of Services, Grids, Service Oriented Architectures, Internet of Things (IoT), and Network Functions Virtualization (NFV). These two last areas (i.e. IoT and NFV) are discussed at the end of the paper in terms of network challenges that should be addressed to satisfy their major requirements when they are implemented within the cloud.

In the next sections, the concepts and technologies of CC are discussed.

2.2. Definition of cloud computing

There is an analogy between electricity and CC. Electricity is, of course, a utility where we expect a certain set of qualities (e.g. always-available, "five nines" reliability) and we believe that CC should aspire to be a utility too (Voorsluys et al., 2011).

Table 2
Cloud computing historical evolution from 1960s until 2011.

Organization/project	CC related main achievement	Year(s)
IBM	Mainframe time-sharing technology	1960s
MicronPC (changed to Web.com)	Initial provider of websites and web services to small businesses and consumers	1995
Salesforce	Enterprise-level applications to which end users could have access via their Internet connections	1999
Amazon	Mechanical Turk was offered as an online marketplace for work	2002
Amazon	The first widely accessible CC infrastructure service (Elastic Compute Cloud - EC2).	2006
Academic Cloud Computing Initiative (ACCI) project	The ultimate goal of this project was to prepare students to explore the new potential cloud systems could offer at that time	2007
Google	Google Docs avoided the need for end-users to have locally licensed and always updated applications in their devices because the applications were stored in a remote and centralized location; collaborative working was in this way much easier to deploy	2007
Eucalyptus, OpenNebula	These were launched as the first open-source computing toolkits for managing clouds	2008
Microsoft	Windows Azure was launched a cloud solution	2010
IBM	The Smarter Computing framework was announced including CC as a relevant tool	2011

CC refers to computing services that are provided within a cloud infrastructure and accessed on demand by customers, so that the customers do not have to be concerned with the details of service provisioning.

Now, we present some definitions of CC. Buyya et al. (2009) have characterized it as follows: "Cloud is a parallel and dis-tributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provi-sioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers." The

National Institute of Standards and Technology (NIST; Mell and Grance, 2011) has defined CC as "… a model for enabling con-venient, on-demand network access to a shared pool of configur-able 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." Further definitions about CC are available in Voor- sluys et al. (2011).

In recent years, the rise of CC is due to several foundational technologies that are discussed in the next section.

2.3. Foundations of cloud computing

CC resulted from the convergence of several technologies belonging to four distinct fields: hardware (e.g. virtualization), distributed computing (e.g. grid computing), the Internet (notably service-oriented applications), and network management (Voor- sluys et al., 2011).

Cloud services are normally situated in data centers each deploying thousands of computers. These systems need to scale up to very high rates of service demand with an acceptable processing time, and also with low costs in terms of energy and hardware. To achieve these goals, a conceptual cloud model such as the one shown in Fig. 1 could be adopted.

In the model of Fig. 1, the virtualization of computing resources can offer significant advances in the following aspects: security, reliability, compatibility, utilization, maintenance, load balancing, and problem recovery. In this way, a virtualization platform nor-mally requires a Virtual Machine Monitor (Hypervisor), which could run directly above the hardware resources of a physical

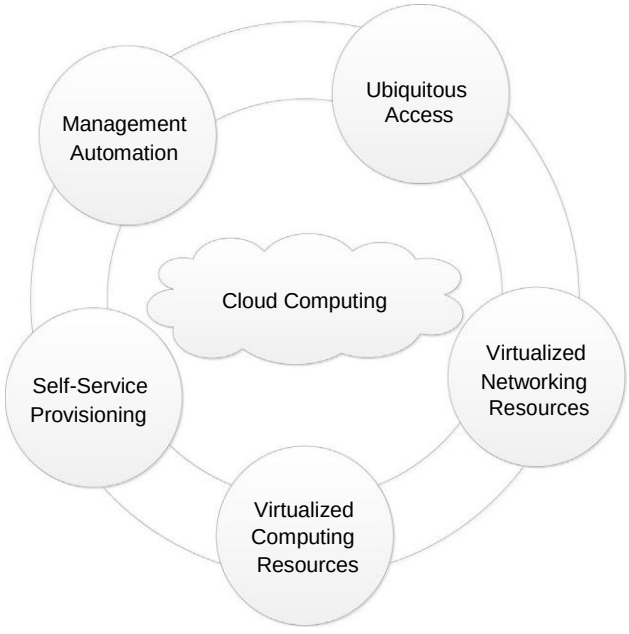

Fig. 1. A common view of architectural foundation elements of Cloud Computing.

computing machine (host) and immediately below the virtual machines (guests). There are many virtualization platforms underlying CC, as discussed in Voorsluys et al. (2011). There are three types of Hypervisor depending in what layer the Hypervisor entity is running. The first is designated as Type 1, and groups all the virtualization platforms with their Hypervisor running directly above the hardware of the host machine. The second, Type 2, represents all the virtualization platforms with their Hypervisor running directly above the operating system of the host. Finally, Type 3 is designated as hybrid and classifies all the virtualization platforms in which the Hypervisor runs at the same layer as the host operating system.

An example of a virtualized computing resource is that of grid computing, whose main goal is to distribute the processing of high complexity and/or time-consuming applications across a group of distinct machines to obtain the intended application results as fast as possible. Grid computing is very relevant in some specific use cases such as drug design, climate modeling, protein analysis, and physics research. GridGain (2014) is an open cloud platform to develop and run Java applications. It can split an initially complex task into multiple subtasks using the MapReduce programming model (Jin et al., 2011; Li et al., 2014). These subtasks are delivered to distinct machines and each one of these subtasks is executed in parallel. At the final stage, the processing results of all the subtasks are aggregated (i.e. reduced) back to one final result. An issue associated with some grid systems is the portability barrier imposed by the diverse operating systems, libraries, compilers and runtime environments available in the computing machines forming the grid processing environment. To overcome these issues, virtualization has been identified as a potential solution (Keahey et al., 2005).

Returning again to Fig. 1, alongside the architectural element of virtualized computing resources, a CC system also requires vir-tualized networking resources, ubiquitous (i.e. reliable/efficient/ secure) access, self-service provisioning, and management auto-mation. As these elements are self-explanatory, we refrain from discussing them in this section, with the exception of management automation. In fact, the high complexity associated with CC sys-tems has motivated the research on management automation. This aims to automatically optimize resources usage and adapt in real time to the customers' needs and operational system status (Murphy et al., 2010). As large data centers from CC providers have highly dynamic demands and workloads, these must be managed in an efficient way (Kim and Parashar, 2011). In the subsequent section, we discuss some important architectural aspects of CC

systems such as the diverse service models.

2.4. Cloud computing service models

We next discuss CC services, depending on the degree of awareness that cloud providers give to subscribers to control the supplied services. Each one of the following sections discusses a single CC service model. In the beginning of each section we highlight the differences between the associated model and other possible CC models concerning how the control scope is divided among the cloud provider and clients. Then, some real deploy-ments of that model are presented. Finally, the strong and weak functional aspects of each model are also discussed.

2.4.1. Software as a Service (SaaS)

A Software as a Service (SaaS) cloud system allows customers to have access to applications and settings that have been deployed by the provider. The clients can have access to these cloud applications using a simple browser. In SaaS, the software stack is controlled in its vast majority by the cloud provider and, significantly, the cloud subscriber is only authorized to control the

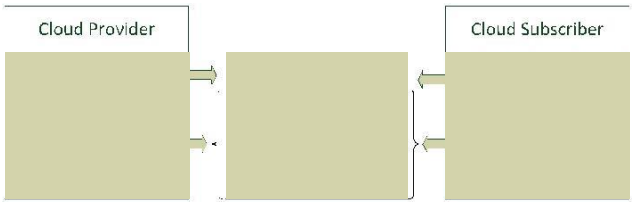

Fig. 2. SaaS provider/subscriber control responsibilities.

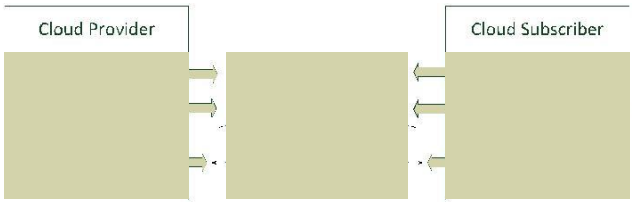

Fig. 3. PaaS provider/subscriber control responsibilities.

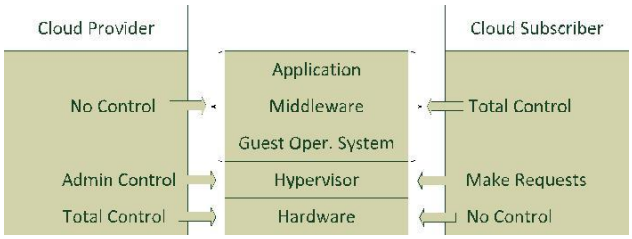

Fig. 4. PaaS provider/subscriber control responsibilities.

application level. For example, the subscriber cannot configure the middleware or even the operating system of each virtual machine. Fig. 2 illustrates how the cloud provider and subscribers share among them the control and management responsibilities through a vertical software stack comprising distinct layers.

A SaaS cloud has the potential to join and compose services from distinct providers. In this way, composed elements can pro-vide high-value solutions for use cases where a single element does not fulfill all the requirements. Many SaaS proposals are now offered. For example, the Salesforce platform offering diverse software components can build innovative, collaborative, com-munity, secure, personalized, mobile and real-time applications for customers (Salesforce, 2014). Similarly, the Programmable Web offers a diverse and numerous set of Application Programming Interfaces (APIs; ProgrammableWeb, 2014). The Programmable Web API lets a customer to find, retrieve and interconnect APIs, mashups, member profiles and other content from the Program-mable Web repository, producing a variety of interesting, novel, customized and on-the-fly services from finding specific product retailers to weather forecasts or geographical maps, although sometimes in a rather limited way.

The main advantage offered by SaaS cloud systems is that it almost eliminates the deployment and maintenance tasks for a customer, who can then rely on the SaaS provider to carry these out instead (Sridhar_a, 2009).

The SaaS products, in spite of their simplicity to offer pre-defined applications that can be settled together in innovative designs, have some drawbacks. As shown in Fig. 2, the cloud subscriber cannot add a new application to the portfolio of the SaaS provider. In fact, the cloud subscriber only has a limited access to personalize any required application. Other limitations imposed to the cloud subscribers by the SaaS provider include the fact that only the SaaS provider can monitor the application-delivery performance (i.e. configure the resources allocated to each client). In this way, cloud subscribers cannot in any way scale up or down the allocated resources according the storage needs or the data traffic changes overtime simply because they cannot configure the middleware (Fig. 2). To satisfy all these requirements that are not ensured by SaaS products, Platform as a Service (PaaS) solutions can be a good alternative option, as explained in the next section.

2.4.2. Platform as a Service (PaaS)

To allow customers full control of applications and configura-tions according to their particular requirements, a PaaS solution (see Fig. 3) can be used alternatively to SaaS solutions. In fact, comparing these two service models, shown in Figs. 2 and 3, a PaaS provider offers its customers an additional Application Pro-gramming Interface (API) for dynamically adjusting the compu-tational resources (e.g. memory, storage disk) according to custo-mers' requirements. Some very popular PaaS offerings are avail-able in (Google_a, 2014; Microsoft_a, 2014).

The platforms offered by PaaS vendors force their applications to be coded in a specific language, following their own API. This creates huge difficulties to move legacy applications to a new PaaS environment or to move applications between distinct cloud providers. This last scenario occurs if a customer takes the decision of changing its cloud provider. These problems could be avoided if the PaaS vendors agree on a standard API or if the customers decide to subscribe with an IaaS cloud provider (see next section).

2.4.3. Infrastructure as a Service (IaaS)

Where a cloud provider allows its subscribers to have total control of virtual machines (i.e. a customer can choose the oper-ating system for each dedicated virtual machine), we have an Infrastructure as a Service (IaaS) cloud model. Fig. 4 illustrates how the cloud provider and cloud subscribers share among them control and management responsibilities when an IaaS model is being used. An IaaS cloud system provides its customers with several fundamental technological resources such as processing, storage and networking. In this way, the customers can install and run distinct software and services of their own choice but without access to or management of the underlying physical system, as shown in Fig. 4, though possibly with a limited authorization to set up some networking elements (e.g. firewalls, NATs).

In the present case, the virtualization should be used to guar-antee to each cloud subscriber a machine with a full operating system that is completely independent from the remaining oper-ating systems associated with other subscribers, in spite of all these operating systems running over the same hardware. Fig. 4 illustrates, just above the hardware, the layer designated by the Virtual Machine Monitor (VMM), or commonly the 'hypervisor'. The hypervisor uses the same hardware and shares its computa-tional resources among diverse Virtual Machines (VMs). Each VM operates like a real machine but is completely isolated from the remaining VMs. In this case, the VM appears to the subscriber like a standalone machine that can be completely configured by that subscriber in various aspects, namely: (i) switch on/off the VM; (ii) install any supported guest operating system, (iii) install a full set of preferred applications/services; (iv) adjust computational resources such as memory, CPU cores, data storage or network interfaces. The previous VM configuration can be easily made through remote command messages sent to the provider's cloud.

Amazon EC2 is an IaaS cloud model that enables developers to build applications that are resilient against failure situations (Amazon, 2013). This is a major advantage over the PaaS cloud model discussed in the previous section. Amazon EC2 offers a very flexible virtual computing environment. In fact, this model allows its customers, using a simple web browser interface, to configure, not only, the diverse VM operational aspects referred in the pre-vious paragraph but also specifying the correct number of VMs to

properly satisfy the customer demand or requisites. We next dis-cuss some relevant Amazon EC2 features, such as: (i) Elastic Block Store (EBS), (ii) cloudwatch, (iii) auto scaling, (iv) elastic load balancing, (v) High Performance Computing (HPC), and (vi) VM import/export.

First, the Amazon EBS feature provides storage network volumes that can be attached in a reliable and elastic way to already running Amazon EC2 instances. Second, the cloudwatch feature monitors Amazon Web Services (AWS) resources and performance parameters generated by customers' applications, enabling the automatic tuning of virtual resources according to the customers' needs. The third Amazon feature designated by auto scaling tunes automatically the Amazon EC2 capacity according to the processing load. With auto scaling, it is possible to adjust the number of Amazon EC2 instances being used, according the demand and minimizing the cost. Fourth, using the elastic load balancing feature, it is possible to automatically distribute incoming application traffic among several Amazon EC2 instances. It also enables a system with high reliability, detecting unhealthy EC2 instances and automatically rerouting the data traffic destined for these to alternative healthy EC2 instances. Using the fifth Amazon feature designated by High Performance Computing (HPC), the AWS customers are able to solve complex scientific and/ or engineering problems exploring the potentialities of distributed applications that assist their research/work in physics, chemistry, biology, engineering, or computer science. The last EC2 feature, i.e. the VM import/export, enables a customer to easily import pre-viously configured Amazon EC2 instances as ready-to-use machines and afterwards export these back to the customer vir-tualization infrastructure. It allows the customer to deploy work-loads across his IT infrastructure with a controlled cost and always satisfying customer requirements including security, configuration management, and compliance.

Another current IaaS solution is available (Eucalyptus, 2014). In addition, there are some well identified and challenging issues to be solved in IaaS cloud services, such as virtual networking, cloud extension, and cloud federation (Azodolmolky et al., 2013). In addition, the programmability through a simplified API has been proposed very recently as a new concept to manage an IaaS cloud infrastructure. In fact, through a simplified API, the applications in an on-demand way can control distinct cloud system aspects, such as resource allocation (Wickboldt et al., 2014) and creation and management of overlay networks (Strijkers et al., 2014). As a proof of concept, it has been shown how to create an IPv6 network over a number of cloud locations around the world (Boutaba et al., 2014; Strijkers et al., 2014).

The reader should note that the previous cloud service tax-onomy formed by only three options (i.e. SaaS, PaaS, and IaaS) is rapidly extending to "X as a Service", where X namely includes Backend, Business Process, Database, Information, Infrastructure, Storage, Platform, Security, Software, Network, and more gener-ically Everything.

Although the functionality of cloud technologies has been comprehensively investigated, less attention has been devoted to relevant aspects of networking that can significantly impair the performance of cloud systems. This novel perspective is studied in the next section.

3. Network architecture in cloud computing

This section provides a comprehensive and structured review of recent literature, including relevant standardization contribu-tions. The structure of this section (and Section 4) is strongly related with Fig. 1 (i.e. CC Architectural Elements), as Table 3 shows.

Table 3
CC architectural element from Fig. 1 vs. discussion topics covered by the current survey.

CC architectural element from Fig. 1	Discussion topics covered by the current survey
Ubiquitous access	Reliable, efficient, and secure communications
Virtualized computing resources	Not covered
Virtualized networking resources	Virtual networking
Management automation	Other aspects (elasticity, federation, interoperability, cooperation, MCC, NFV, inter-cloud architectures, IoT)

In the following sections we discuss the most significant research/standardization efforts inside the networking area mainly for supporting, with enhanced performance, some CC emerging applications. These applications are setting new system requirements such as elastic load, dynamic allocation of network resources, and secure services distributed between private and public infrastructures. Table 4 shows more details about the organization of our subsequent discussion through Section 3 on short-term networking challenges.

3.1. Reliable communications

Full communications reliability should be supported to deliver data messages to the intended recipient(s) within a cloud infra-structure in a correct and timely way. Currently, standardization bodies are working towards several solutions to enhance com-munications through the available and forthcoming networking infrastructures. In the following text, we discuss the more relevant enhancements proposed within both IEEE and IETF that can be applied into cloud networking environments. The first enhance-ment implies a reliable link protocol, i.e. Fiber Channel over Ethernet – FCoE (ANSI/INCITS, 2009), which is an encapsulation mechanism. It can be used to simplify and enhance the inter-connection between a classical Ethernet network and a distributed storage area network (SAN). This encapsulation requires some changes in the Ethernet operation namely, the usage of an addi-tional mapping between Fiber Channel N_port IDs (i.e. FCIDs) and Ethernet MAC addresses.

To avoid losing frames, a second enhancement is appropriate, IEEE 802.1Qbb (IEEE, 2011), which uses a priority-flow control mechanism to selectively counteract losses due to the receiver's buffer overflow. This mechanism uses a pause control message that is sent by a receiver to the sender after the former predicts the potential for buffer overflow. Upon receiving a PAUSE frame, the sender responds by stopping transmission of any new frames through the link interconnecting both of them until the receiver is ready to accept frames again. The novelty of this solution is that it can control the transmission of flows in different ways depending on the diverse flow types.

The third enhancement proposal, IEEE 802.1Qau (IEEE, 2010), also avoids transmission losses as in the previous proposal but now avoiding losses that can occur during frame transmission, for example due to switch buffer overflow. This proposal supports congestion management of long-lived data flows within network domains of limited bandwidth-delay product. This is achieved by enabling switches to signal congestion to end stations capable of transmission rate limiting to avoid frame loss. There is also a major difference between the current controlling mechanism and the second mechanism, 802.1Qbb. The latter is a hop-by-hop mechanism, whereas the former, 802.1Qau, operates end-to-end.

The fourth proposal, IEEE 802.1Qaz (IEEE_c, 2011), defines enhancements to transmission selection to support allocation of

Table 4
High-level structured list of networking research activities in relation to cloud computing.

Main Area	Goal
Reliable communications (Section 3.1)	Support protocol heterogeneity; control of flow rate to avoid either receiver's buffer overflow or congestion; simplify the synchronization between transmitter and receiver; error detection
Efficient communications (Section 3.2)	Balance the load among alternative paths; higher data rates; provision for larger frame sizes; multiple virtual channels operating in parallel over a single physical channel; some extensions to Open Shortest Path First (OSPF); some BGP enhancements
Virtual networking (Section 3.3)	Virtual switch management; VLANs management with VM migration; SDN
Other important areas (Section 3.4)	Elastic allocation of cloud resources according the load variation; cloud federation; interoperability

bandwidth amongst traffic classes, plus a protocol for controlling the application of Data Center Bridging features.

The last proposal is associated with the IETF ConEx working group that is chartered to work on a congestion exposure mechanism for IPv6 networks. This mechanism allows data sour-ces to notify the network about the congestion suffered by pre-vious packets of the same data flow. A very recent contribution to this working group (Briscoe and Sridharan, 2014) shows how to police congestion at data center ingress nodes and thereby how traffic shaping can be applied to provide suitable per-flow per-formance. This functionality based on a feedback congestion mechanism to the ingress nodes avoids the configuration of any of the internal data center network switches with flow related con-figuration (Briscoe and Sridharan, 2014). Another way of solving the congestion problem in clouds is based on OpenFlow (McKeown et al., 2008), which uses a centralized design with controllers and some flow configuration in the switches estab-lishing the data path.

3.2. Efficient communications

Some ongoing work is investigating efficient communications, which is obviously very important in a cloud scenario. The reader may note some overlap between what will be discussed now and what was already discussed in the last section. The initial case we discuss here is Shortest Path Bridging (SPB), specified in the IEEE 802.1aq standard (IEEE_d, 2012). It is a computer networking technology intended to simplify the creation and configuration of networks, while enabling multipath frame forwarding. SPB is the replacement for the legacy spanning tree protocol (STP) (IEEE_f, 2004). Applying legacy STP into the typical flat (non-hierarchical) topology of current data centers is not recommended because it would force the existence of a root bridge and a hierarchical tree of switches without loops, which potentially create non-optimum switching paths inside the local network of the data center, and consequently cause the following problems: non-balanced load among the local links, some links become highly congested, and a significant delay growth of frame transmission among servers, which can negatively impact the overall datacenter performance. Alternatively, SPB allows all paths to be active with multiple (and eventually equal) cost paths, and provides much larger layer 2 topologies (i.e. up to 16 million virtual local area networks (VLANs) compared to the traditional limit of 4096). It also supports faster convergence times, and improves the efficiency of the mesh topologies through increased bandwidth and redundancy, allow-ing traffic to be balanced within a mesh across all possible paths. Additional related standardization work is being carried out by IETF in Transparent Interconnect of Lots of Links – TRILL (Eastlake et al., 2011; Perlman and Eastlake, 2011). The main goal of TRILL is to encapsulate each Ethernet frame within another envelope (i.e. using the outer TRILL header), which acts like a layer 3 envelope, and then this encapsulated frame can be routed using all the Layer 3 routing techniques that have evolved over the years, including shortest paths and multipath techniques (Perlman and Eastlake, 2011). It allows a fairly large Layer 2 cloud to be created, with a flat address space, so that nodes can move within the cloud without changing their IP addresses. The cost is a small overhead induced by the outer header added to each frame traversing the cloud infrastructure. At the time of writing, there is intensive activity at IETF on this topic. However, with the exception of (Amamou et al., 2014), we could not find any recent other work in this field. Therefore, it seems clear that further research would be valuable.

Another interesting enhancement aspect involves the Gigabit Ethernet, from 1 to 100Gbps and beyond, which is very well covered in (Stallings, 2015). This describes some enhancements to the MAC layer, such as provision for larger frame sizes; the usage of 2 control bits beyond the data bits to enable both easier transmitter/receiver synchronization and error-detection; and finally a multi-lane distribution allowing a single physical link to work as multiple parallel channels.

The design of networking systems that enable communications among data centers can involve the utilization of enhanced ver-sions of high-layered routing protocols such as OSPF (Retana and White, 2013). In this case, OSPF is used internally in each data center to support the routing of packets based on their final IP destination address through a path with the lowest cost. Following this track, (Retana and White, 2013) discusses three extensions to the Open Shortest Path First (OSPF) protocol that have direct applicability to efficient and scalable network operation in highly meshed environments, typically the ones present in the data centers. Specifically, the application extensions to OSPF to reduce flooding in Mobile Ad Hoc Networks (MANET), demand circuits designed to support on-demand links in wide-area networks, and OSPF stub router advertisements designed to support large-scale hub and spoke networks are considered in a typical data center network design; these sorts of protocol improvements could affect the scaling of data center environments. On the other hand, the Border Gateway Protocol (BGP) can be used in the core commu-nications among data centers. In this case, BGP is responsible for setting up Multiprotocol Label Switching (MPLS) that forwards traffic through the core network based on short path vector labels rather than long network prefixes. Nevertheless, BGP needs to be enhanced to support QoS/QoE per flow. To achieve this, SDN (Astuto et al., 2014) can potentially be very useful (Gupta et al., 2014). Another way in which BGP can be enhanced is the avail-ability of multiple routes to a given destination, where each of the routes has a different "exit point" from the local Autonomous System (AS) (Mohapatra et al., 2013). If this enhancement will be deployed in a communications scenario among data centers, due to the presence of multiple paths, the following benefits can be attained: reduce the restoration time after a failure, enable load balancing of traffic, help contain the failure to the local AS where the failure occurs, and allow one to bring down a router for maintenance without causing significant traffic loss among the data centers due to the availability of alternate exit points from the AS to a given destination.

3.3. Virtual networking

A typical physical host of a (cloud) data center has a hypervisor that enables diverse Virtual Machines (VMs, or guests) to run over the same host hardware. In order to offer a stronger interworking and interoperability between system and network elements, the virtualization of networking resources within a cloud infra-structure is becoming a very important requirement. In this way, the hypervisor is also associated with a virtual switch (VS). This device switches Layer 2 traffic among the VMs running in the same physical server. The VS learns about MAC addresses in a different way from a traditional switch because the former assumes by default that all frames with an unknown destination MAC should be forwarded over the uplink to the physical external switch. This default behavior can potentially create some security threats such as packet sniffing and spoofing (Wu et al., 2010). In addition, the VS can switch traffic among the intra-machine VMs according to pre-defined policies, which can control broadcast and Virtual LAN (VLAN) traffic. As an example, a VS access control list for security reasons can disallow two VMs located on the same physical host to have a direct communication between them. In this way, the VS is like a software routine that controls the traffic features of aggregation and access control associated to its virtual ports within a physical server containing diverse VMs (Sridhar_b, 2009; Chowdhury et al., 2010).

VSs also have some disadvantages (Sridhar_b, 2009). They can potentially create serious practical problems with traditional net-work architectures (Layland, 2010). One problem is related to the configuration of VLANs: each time a VM moves to other physical server, it is necessary to reconfigure the VLAN through distinct switches. This coordination among the switches could be complex, with a large latency, and sometimes impossible due to the fact these switches are from distinct vendors, each one with its own proprietary firmware and incompatible with the others. A poten-tial solution to these problems is separating the control functions from the network switch and placing them in accessible control servers. This separation can be supported by a Software Defined Networking (SDN) architecture Nunes et al., 2014) and using the OpenFlow protocol (Stallings, 2013). Some disadvantages of these new proposals include: the LAN overhead due to extra signaling/ control traffic; the lack of robustness against the failure of a con-trol server (i.e. the typical problem of a centralized solution); and the VLAN reconfiguration in aggregation and core switches. Some possible solutions to these disadvantages are, respectively: opti-mizing the OpenFlow protocol to reduce its header size and reduce the number of signaling/control messages; the deployment of redundant SDN controllers with horizontal/vertical communica-tion among them; and the deployment of hairpin switching, which is a new approach to allow the visibility of intra-VM traffic to external network switches. Hairpin switching is being actively discussed inside the IEEE (IEEE_e, 2012). The IEEE proposes a tagging approach in the header frame to perform hairpin switching.

SDN can be used to enhance some important aspects of clouds such as network virtualization and security, as illustrated in Table 5.

Table 5
SDN proposals to support network virtualization and security in cloud systems.

Topics	Network Virtualization	Security
SDN	Jain and Paul (2013), Corradi et al. (2014), Vestin et al. (2013), Banikazemi et al. (2013), Benson et al. (2011), Chowdhury et al. (2010)	Shin and Gu (2012)

3.3.1. Network virtualization

A SDN solution that dynamically manages networking tunnels is discussed in Jain and Paul (2013). This follows a proactive model to install the overlay tunnels. The overlay tunnels usually termi-nate inside virtual switches within hypervisors or in physical switches, acting as gateways to the existing network. This hybrid approach is very popular in recent data center network virtuali-zation, and it can use a huge variety of tunneling technologies (Jain and Paul, 2013).

OpenStack controls large pools of compute, storage, and net-working resources belonging to private/public clouds. This soft-ware enables the system management through a dashboard or via the OpenStack API. OpenStack works with popular enterprise and open source technologies, making it ideal for heterogeneous infrastructures (Corradi et al., 2014).

The current distributed control plane of wireless networks is suboptimal for managing the limited spectrum, allocating radio resources, implementing handover mechanisms, managing inter-ference, and performing efficient load-balancing between cells. SDN-based approaches represent an opportunity for making it easier to deploy and manage different types of wireless networks, such as WLANs and cellular networks, eventually supporting traffic offloading. Traditionally hard-to-implement but desired features are indeed becoming a reality with the SDN-based wire-less networks. These include seamless mobility through creation of on-demand virtual access points (VAPs), downlink scheduling (e.g., an OpenFlow switch can do a rate shaping or time division), dynamic spectrum usage, and enhanced intercell interference coordination (Vestin et al., 2013). Other centralized SDN con-trollers such as Meridian (Banikazemi et al., 2013) can be used to manage target specific environments such as data centers, cloud infrastructures, and carrier grade networks.

SDN can also potentially offer networking primitives for cloud applications, solutions to predict network transfers of applications, mechanisms for fast reaction to operation problems, network-aware VM placement, QoS support, real-time network monitoring and problem detection, security policy enforcement services and mechanisms, and enable programmatic adaptation of transport protocols (Benson et al., 2011). SDN can help infrastructure pro-viders to expose more networking primitives to their customers, by allowing virtual network isolation, custom addressing, and the placement of middleboxes and virtual desktop cloud applications. Further information about network virtualization is available in Chowdhury et al. (2010).

3.3.2. Security

An already diverse set of security and dependability proposals is emerging in the context of SDNs. As an example, Shin and Gu (2012) discuss a proposal to monitor cloud infrastructures for fine-grained security inspections. It automatically analyzes and detours suspected traffic to be further inspected by specialized network security appliances, such as deep packet inspection systems.

3.4. Elastic allocation, federation, and interoperability

This section deals with additional networking research activ-ities in CC, which are summarized in Table 6.

3.4.1. Elastic allocation of cloud resources according the load variation

The authors of Hu et al. (2012) discuss solutions for addressing as well as routing and forwarding using layered network topolo-gies. Also, according to Seibold et al. (2012), running large data-bases requires the use of virtualization in order to cope efficiently with peak demands. They propose a cooperative approach, in which the database management systems communicate their

Table 6
Summary of other networking-based research activities in cloud computing.

Main topic within the area of cloud computing	Reference
Elastic allocation of cloud resources according the load variation	Hu et al. (2012), Seibold et al. (2012), Birke et al. (2012)
Cloud federation	Sridhar_b (2009), DMTF_a (2014), Sen and Soumya et al. (2013), Sakamoto et al. (2012)
Interoperability	DMTF_a (2014), OASIS (2014), SNIA (2014)

request for resources (typically then deployed by virtual machines) and adjust their resource usage. Additionally, a large-scale survey about workloads for data centers (Birke et al., 2012) may be a great help for a reliable future planning. Finally, the authors of Metri et al. (2012) have conducted extensive sets of experiments on data centers' energy efficiency and have identified the need for accurate load prediction and how to set up the necessary virtual machines to fulfill that load in a completely dynamic way.

3.4.2. Cloud federation

Another relevant area is cloud federation. Sridhar_b (2009) has defined cloud federation as follows: "Cloud federation manages consistency and access controls when two or more independent geographically distributed clouds share either authentication, files, computing resources, command and control, or access to storage resources."

Some of the most important features in cloud federation are, as discussed in Sridhar_b (2009):

A customer who considers multiple cloud services (e.g. SaaS) should instead use a single sign-on (SSO) scheme to authenti-cate that customer only once, irrespective of the cloud service providers involved. This requires a third-party authentication server that operates in a distributed way among customers and service providers. This authentication server initially receives the customer credentials and authenticates that customer. After this, the authentication server provides the credentials of the already authenticated customer to the selected cloud service provider. Kerberos (2014) is a security/trust framework that can support previous functionality.

All the computing and storage resources of a VM are normally saved in files. To support VM migration (Medina and Manuel Garcia, 2014) transparently and reliably among distinct cloud technologies, it is necessary to use a portable format to save and share the complete status information among different tech-nologies without any compatibility problems. In this way, the Desktop Management Task Force (DMTF) has produced a specification designated by Open Virtualization Format (OVF) to completely describe the VM in a neutral and universal format for use across many vendor platforms (DMTF_a, 2014).

Cloud federation is a very recent aspect in the cloud arena, fueled by the user's need for pervasive access to the applica-tion's portfolio and data. Also, the application could be from a provider, and the data being used by that application can be stored in another provider. Assuming this type of emergent scenario, the providers will be much better off in terms of business if they cooperate. Therefore, the providers are likely to establish peering agreements, producing compatible APIs to offer easy access to their clouds. In fact, this could occur even before the standardization organizations produce any standards in this area. If this occurs, the provider and vendor innovation could significantly impact the successful implementation of cloud federation.

The success of cloud federation implementation also depends on the coordination level between management and billing systems as well as the adoption of new business models (Sen et al., 2013) for this new environment. In this way, the customers are expected to be billed according to the amount of resources/data they use from each provider's cloud. In addition, cloud service providers can adopt some mobile opera-tor business models already being used to support peering/ roaming agreements among them.

A recent piece of work proposes a way of sending requests about energy prices to (federated) data centers to help optimize the savings in electrical energy (Sakamoto et al., 2012). They have developed a management policy to help target the requests to where electricity is cheaper. Their results suggest that reductions on electricity costs of 15% are possible.

3.4.3. Interoperability

There is active standardization work in the CC area on inter-operability. Some coordination efforts have been established to minimize the problems of redundancy and incompatibility among specifications.

The Desktop Management Task Force (DMTF) has specified OVF (Open Virtualization Format) by means of which the VM full configuration and status can be written into files, and eventually migrated among physical machines, using distinct hypervisors (DMTF_a 2014). Also, the DMTF's Open Cloud Standards Incubator is interested in studying the following aspects: cloud portability (working with multiple providers), federation of cloud providers, and service adaption to varying requirements.

There is also the Organization for the Advancement of Struc-tured Information Standards (OASIS) which views Service-Oriented Architectures (SOAs) as a basis of CC; SOAs are of course very popular in IT environments (OASIS 2014). More par-ticularly, they are investigating CC as follows:

Moving on-premise applications to private or public clouds.
Enhancing the interoperability of cloud applications and services.
Managing, in real-time, authorizations enriched by data that informs where users are, what they are doing, and which devices they are using.
Simplifying the querying and sharing of data across disparate applications, clouds, and mobile devices.
Developing a set of functional elements and measurable criteria or qualities that should be present in clouds deployed by public administrations.

The Cloud Storage Initiative (CSI) within the Networking Industries Association (SNIA) works on cloud-storage-related issues (SNIA, 2014). CSI is proposing personalized cloud storage. They have developed a new interface designated as the Cloud Data Management Interface (CDMI); this allows cloud customers to associate to their data some metadata that informs the cloud provider about relevant data services (e.g. data special requisites, backup, archive, encryption, authentication, and authorization).

4. Future network trends for cloud computing

The discussion on the networking issues presented in the previous section underlines that the cloud deployment through the Internet obliges investigators to revisit traditional network-ing concerns, such as reliable and efficient communications,

Table 7
High-level structured list on future network trends for cloud computing.

Main area	Goal
Reliable communications (Section 4.1)	Solve the tradeoff between resource allocation and fault tolerance in resource-constrained systems; enhancement of Gigabit Ethernet
Efficient communications (Section 4.2)	Cloud resources among tenants are urged to be shared in a safe and efficient ways within a cloud federated system; investigate and standardize relevant metrics to assess performance and energy efficiency of cloud systems
Virtual networking (Section 4.3)	SDN could help to study fully collaborative, peer-to-peer and pervasive web scenarios, where the client-server paradigm could become obsolete
Other important areas (Section 4.4)	Cooperation in Cloud Computing; Mobile Cloud Computing and Network Functions Virtualization; inter-Cloud Computing architectures; Internet of Things

virtualization, security, resource allocation, and interoperability, due to the use of multi tenancy over a pool of shared virtual resources, notably computing, storage, and networking.

Moreover, future trends in computer communications have often been debated. In particular, the following vision has been presented (Huston, 2012): "It is also evident that the pendulum of distribution and centralization of computing capability is swinging back, and the rise of the heavily hyped Cloud with its attendant collection of data centers and content distribution networks, and the simultaneous shrinking of the end device back to a terminal that allows the user to interact with views into a larger centrally managed data store held in this cloud, appears to be back in vogue once more". In the following sections we discuss relevant open issues in networking that could more effectively support CC. If correctly addressed, they could support the above vision about the evolution of computer communications and either attenuate or mitigate the networking issues that confront CC.

Table 7 shows more details about the organization of our subsequent discussion through Section 4 on future network trends for CC.

4.1. Reliable communications

A recent contribution (Bodik et al., 2012) optimizes the tradeoff between resource allocation (Chowdhury et al., 2010; Shieh et al., 2011; Ballani et al., 2011; Duffield et al., 1999; Ricci et al., 2003) and fault tolerance (i.e. availability) (Agarwal et al., 2010; Amiri, et al. 2000; Bansal et al., 2008; Yu et al., 2006) in future resource-constrained systems. Meanwhile, the current growth in demand is accelerating the investigation into enhancements of Gigabit Ethernet to produce a 400 Gbps Ethernet standard. Looking beyond this milestone, there is a widespread consensus that a 1 Tbps will eventually be produced (Stallings, 2015).

4.2. Efficient communications

Sharing computational, storage, and networking resources among cloud systems has been suggested in Popa et al. (2012). In addition, IETF work on Congestion Exposure (ConEx) proposes a method for achieving congestion proportionality. However, this approach is still an open issue (Popa et al., 2012). Sharing cloud resources in a conservative way, meaning that the unused cloud resources are shared in a safe and efficient ways among tenants within a high-complexity cloud federation scenario, seems a very challenging task.

A recent piece of work proposes a framework of new metrics able to assess performance and energy efficiency of cloud com-puting communication systems, processes and protocols (Fiandri et al., 2015). However, the authors do not explain how they have obtained their results. This is very difficult for others to replicate and make progress on top of their results. Further work is neces-sary to standardize the set of metrics that were investigated, and to perform evaluations in operational data centers.

4.3. Virtual networking

The authors of Panagiotakis et al. (2015) discuss a potential evolution for the future of mobile multimedia. They predict a networking environment serving a diverse set of pervasive and personalized cloud-based Web applications, where the client-server paradigm will become obsolete. In particular, it is believed that in the future Web, cloud-based Web applications will be able to communicate, stream and transfer adaptive events and content to their clients, creating a fully collaborative, peer-to-peer and pervasive Web environment. In parallel with these novel requirements, other relevant aspects will also evolve such as the convergence between networking and telecommunications infra-structures, cloud networking, cloud offloading, and the network function virtualization. The new heterogeneous virtualized eco-system that will be formulated creates new needs and challenges for its management and administration. For this, SDN seems a promising solution (Koumaras et al., 2015).

A very interesting research direction is the one pointed by (Mastorakis et al., 2015); this is about the intelligent and efficient management of networking resources on mobile cloud computing (Fernando et al., 2013). This will be further discussed in the fol-lowing section.

4.4. Cooperation, mobile cloud computing, network functions vir-tualization (NFV), inter-cloud computing architectures, and internet of things (IoT)

4.4.1. Cooperation in cloud computing

An obvious method for efficiently using the available cloud resources is to persuade cloud participants to cooperate among themselves. This cooperation can be enforced in several ways: through a common goal (Huerta-Canepa and Lee, 2010), using monetary incentives (Charilas et al., 2011), social incentives (Tanase and Cristea, 2011) or reputation incentives (Hwang et al., 2008; Charilas et al., 2011). The major problem associated with the common goal method (Huerta-Canepa and Lee, 2010) is that it does not work in the absence of a common activity among the potential collaborating entities. In the case of monetary incentive (Charilas et al., 2011), several issues need to be addressed to identify the most suitable cloud business model to be used (Sen and Soumya et al., 2013), and investigate more specific problems such as the credit representation; the security requirements to guarantee a safe monetary transaction; what price to use for each cloud resource; and what type of tariff should be selected (e.g. static, dynamic). Using social incentives such as those suggested in Tanase and Cristea (2011) also raises some problems such as pre-venting free riding. The main issues related with reputation mechanisms are the potential lack of fairness and trust associa-ted with the reputation values. This aspect requires further investigation.

4.4.2. Mobile cloud computing and network functions virtualization

Mobile Cloud Computing (MCC) has become an important research area due to the rapid growth of mobile applications and the emergence of cloud computing (Wang et al., 2015). MCC refers to the integration of cloud computing into a mobile environment. The final goal of MCC is to deliver to users a set of mobile services with enhanced QoE. To reach this objective, the mobile operators are deploying an initial strategy that offloads traffic from cellular networks to other available wireless access technologies (e.g. Wifi, WAVE). Other techniques to enhance QoE are service migration and data caching. In this way, and starting with service migration, it can be implemented among federated clouds for offering users a set of services (eventually from distinct cloud providers) with the highest QoE to each user; this offer could be dependent on several requisites namely, the user location, the user profile, and the user terminal characteristics. In addition, the data caching should be deployed to diminish the Round Trip Time (RTT) and its variability (i.e. jitter); consequently, the data should be stored at devices (e.g. MiddleBoxes/Proxies, Access Points, Base Stations, Terminals) very near the user terminals that are expected to consume that data.

To orchestrate all the technologies, strategies and techniques discussed in the last paragraph, making MCC a powerful solution, it is fundamental to program the network and service resources in an intelligent and efficient way. An interesting approach to deliver all this is using Network Functions Virtualization (NFV). The NFV is an emerging network architecture concept that uses virtualization technologies to abstract from the hardware entire classes of net-work node functions into building blocks that may connect, or chain together, to create intelligent and efficient communication services. As an example, a programmable NFV may consist of one or more virtual machines running, in a coordinated way, different software and processes, on top of standard high-volume servers, switches and storage, or even CC infrastructure, instead of having custom and proprietary hardware appliances for each network function. This new NFV architecture is potentially very flexible; it can deploy virtualized load balancers, firewalls, intrusion detec-tion devices, WAN accelerators, mobile devices power control (Mavromoustakis et al., 2015), and new MCC business models (Katzis, 2015).

The migration of NFV to the cloud environment seems a very challenging task for researchers and engineers due to the myriad of challenges that need to be managed in a harmonized way in order to deliver optimum seamless services to mobile users (Grover and Kheterpal, 2015). Many fundamental problems of mobile networks such as bandwidth availability and reliability, resource scarceness and finite battery energy need to be addressed before rolling out these types of services. To solve those problems, various types of resource management techniques should be deployed at mobile clouds such as resource offloading, cloud infrastructure, mobile devices power control (Mavromoustakis et al., 2015), control theory, data mining, machine learning, radio spectrum management and MCC business models (Katzis, 2015).

As a final interesting MCC scenario, the authors of (Batalla, 2015) elaborate on multimedia content delivery as one of the use cases of mobile cloud networks. These cloud networks are referred to as media clouds. Since mobile devices are becoming increas-ingly important receptors of multimedia content, mobile cloud computing is undertaking an important role for delivering audio-visual content from the cloud through the Internet towards the mobile users. On the other hand, high requirements of multimedia content streaming establish the necessity of cross layer mechan-isms for avoiding or decreasing the effects of, for example, mobile network congestion or cloud congestion. In this way, one should make use of novel models and algorithms for resource usage prediction that makes possible the optimal distribution of streaming data, and for prediction of the upcoming fluctuations of the network that provide the ability to make the proper decisions in achieving optimized QoS) and QoE for the end users (Kryftis et al., 2015).

4.4.3. Inter-cloud computing architectures

"Storage as a Service" (SaaS) for Internet content delivery, video encoding, and streaming services (e.g. Content Delivery Networks – CDNs) has come to the fore, potentially using a federation of cloud infrastructures. In this context, it is pertinent for providers to hide the different ways in which they operate. One way of performing this transparency is providing a suitable abstraction across the infrastructure heterogeneity. This abstraction can be ensured by a metadata system such as MetaCDN (2014) and Aka-mai (2014).

It is also important to be aware of legal issues related to data movement and storage among disparate geographic locations. Notably, the physical locations of both virtual machines and sto-rage arrays have a strong bearing on national laws in respect of security breaches or tampering with data, and in particular where data is moved between different locations (Voorsluys et al., 2011; SECCRIT, 2014). There are also important business issues that arise if or when a cloud provider changes owner or closes down, in respect of customer data and applications.

Also recently, research has been carried out in Service-Oriented Architectures (SOAs), especially from a convergence and network point of view (Duan et al., 2012). Some relevant aspects of this research will involve several areas, namely network virtualization (Chowdhury et al., 2010; Jain and Paul, 2013) over heterogeneous network infrastructures (e.g. wireless backhaul links, unidirec-tional optical links) (Tzanakaki et al., 2013), service discovery technologies (Rambold et al., 2009), QoS-aware web service composition (Strunk, 2010), and network applications based on SDN through a multi-cloud environment (Jain and Paul, 2013). SDN has been its main focus in the context of data centers and support of virtualized networks. Consequently, the application of the same approach to wide area networking is still yet to prove its viability. One such application is in supporting lambda path net-works, where the elements of the network are not packet switches but wavelength switches (Wei et al., 2014).

A very recent IETF discussion about inter-cloud computing architectures is available in (Aazam et al., 2015).

4.4.4. Internet of things

The ubiquitous network connectivity, affordable computing power combined with intelligent deployments make the Internet of Things (IoT) very valuable for the current Internet players. The convergence of network wireless access technologies, cloud, and APIs to analyze the data (Big Data) is creating an opportunity for independent software vendors, system integrators, and research-ers. Some new solutions are being developed. These solutions are based on new programming models and hardware devices. These can be deployed through very popular languages such as PHP, Python, Java, JavaScript, C#, and Ruby; microcontrollers and low-powered devices such as Arduino, Raspberry Pi, and other embedded devices. The usage scenarios of IoT are diverse and include e-Health, engineering, transportation, and social, to name just a few.

To migrate and operate the IoT devices in the cloud, some obstacles should be overcome; the first challenge is that to realize the true potential of IoT, the data generated by sensors has to be analyzed in real-time; a second challenge is to perform a very useful historical data analysis over structured or even unstruc-tured information previously collected from sensors.

5. Security aspects

The topic of security in particular is also discussed in our paper – this has been largely neglected in CC but is beginning to be recognized as a crucial element in the provision of CC services; customers increasingly wish to have assurance that their data and computations will be safe and secure. Trustworthiness is going to be a vital property of CC in the future, especially now that more customers are beginning to place critical services in the Cloud (SECCRIT, 2014). This functional perspective is very pertinent, and needs to be further investigated because the performance of dis-tributed clouds heavily depends on the underlying networks.

A related and important topic is that of resilience – the ability of a system to continue to provide a suitable quality of service even in the face of challenges, when for example security is compromised or a third party event such as a power outage occurs. This is a property that CC systems should strive to provide, espe-cially when supporting critical services (Sterbenz et al., 2010).

The subsequent discussion is aligned with the aspects identi-fied in Table 8.

5.1. Background

The relatively new and rapidly adopted model of cloud com-puting, aggregating in a distributed way so many distinct tech-nologies and solutions, is creating new system vulnerabilities and threats of new and damaging attacks. So, we now also discuss the security aspects of cloud systems.

5.1.1. Generic cloud security aspects

Initiating our discussion about security, as a generic (and obvious) but very important topic, one can argue that the security of cloud services should be no worse than that of the network services provided to customers through their local network infrastructures. To achieve this goal, a cloud provider should be conscious of the following aspects:

The cloud provider needs to apply the most recent security patches in its cloud infrastructure, such as firmware, operating systems and applications. Some problems could occur in the cloud operation due to incompatible patches. In this way, a rollback option should be available to change the infrastructure to the last stable configuration.

Data isolation must be supported among multiple VMs sharing the resources of the same physical host. Hypervisors also need their security patches to be up to date.

The cloud paradigm is changing the way the major manage-ment functions are deployed. Middleboxes such as load bal-ancers and firewalls are moving from the local infrastructure to the cloud (Sherry et al., 2012). As the cloud infrastructure could be a federation of clouds, then the previous middleboxes should be deployed in a distributed and coordinated way through distinct network domains. This also implies that these mid-dleboxes should be operating with the latest security patches.

Authentication and trust mechanisms are needed by the user and provider alike. In this scenario, SSO could be a good starting point. The spam e-mail problem can be also mitigated in the cloud (e.g. the spam could be verified and filtered in the VS associated with the hypervisor). Some useful techniques to mitigate spam in clouds could include the Sender Policy Frame-work (SPF) to authenticate the source of each e-mail, and the Apache SpamAssassin Project to classify, rank and filter any unwanted e-mail.

To enable communications among the diverse cloud resources/ hosts (sometimes from distinct providers) similar to that of a closed local network, the cloud provider's resources/hosts need to be reachable in a secure way through Virtual Private Network (VPN) tunnels. In one initiative, which addresses security and transparency simultaneously, CloudNet makes use of a Virtual Private Cloud (VPC), which brings CC and VPN technology together to give the user a private set of cloud resources (Wood et al., 2011).

Cloud services are often made public. Consequently, non-authorized access should be prevented (Patel et al., 2013; Modi et al., 2013). In addition, Distributed Denial of Service (DDoS) attacks carried out by compromised users' machines generate a large amount of bogus traffic. To avoid the negative impact on the system performance of this traffic, the cloud infrastructure can try to identify that traffic and then discard it from the network, redirecting it to a "black hole".

The Cloud Security Alliance (CSA) is working on the initial identification of top security threats in cloud systems as well as within mobile computing, and on the establishment of the more convenient actions/strategies to avoid those threats.

5.1.2. Security risks depend upon the cloud service model

According to Fernandes et al. (2014) and Subashini and Kavitha (2011) it is important that the diverse players using CC should be aware that PaaS, SaaS, and IaaS each have their own security issues. These distinct security aspects are summarized in Table 9, individualized per service model, and discussed in the following text.

The SaaS services are very similar to Web services over HTTP. In this way, the former inherits the classical security drawbacks of the latter, as follows:

The SaaS interface can be maliciously hacked through applica-tion loopholes (i.e. vulnerability in the system that enables an attacker to compromise that system) (Subashini and Kavitha, 2011).

The attacker can inject masked code into a SaaS system that can break isolation barriers (Subashini and Kavitha, 2011).

The lack of data integrity in the messages such that it can be changed during their transmission through the network in favor of a particular malicious intent of a man-in-the-middle attacker (Fernandes et al., 2014).

The PaaS systems are based on platforms such as, .NET and Java. The resources offered by these platforms are shared among mul-tiple customers (i.e. multitenancy aspect). Consequently, a proper isolation mechanism must ensure that one tenant cannot access to components of other tenants. For this, there is a clear tradeoff

Table 8
Main security aspects of cloud systems.

Main area	Goal
Background (Section 5.1) – Generic Cloud Security Aspects	Important security aspects a cloud provider/user should be aware of
Background (Section 5.1) – Security Risks Depend Upon the Cloud Service Model	Discussion in how the diverse cloud service models introduce heterogeneous security problems within a cloud system
Future Developments (Section 5.2)	Intrusion Detection/Prevention solutions; data privacy; technical and legal issues in CC systems; col-lusion avoidance mechanisms; secure query over encrypted data

Table 9
Main security aspects for the diverse cloud service models.

Service/topic	Main aspect	Reference
SaaS	The SaaS APIs inherit the classical security drawbacks of the Web services	Fernandes et al. (2014), Subashini and Kavitha (2011)
PaaS	There is a tradeoff between the level of isolation among tenants and the efficiency level in how the resources are used	Fernandes et al. (2014), Rodero-Merino et al. (2012)
IaaS	Common physical (computing, networking) resources are shared among the customers through virtualized instances	Fernandes et al. (2014), Perez-Botero et al. (2013), Vaquero et al. (2011), Pearce et al. (2013)

between resource consumption and the isolation level to be offered. Further discussion on this is in Rodero-Merino et al. (2012).

Common physical (computing, networking) resources are shared among the customers through virtualized instances, offer-ing IaaS solutions. Vaquero et al. (2011) discussed security from the networking, virtualization and physical sides of cloud IaaS networks. There are also management consoles, such as XenCenter for Xen VMs, which can be remotely accessed via the Web. Con-sequently, these management consoles are also vulnerable to a VM-to-VMM attack that consists in gaining access to the under-lying VMM (e.g. VmwarePlayer, VirtualBox) through a legitimately running VM managed by that VMM. This attack is normally designated by VM escape (Grobauer et al., 2011). If this attack is successful, the attacker can monitor other VMs, including shared resources and CPU utilization, and shutting down VMs. In respect to the networking aspect, the VMMs typically offer various basic types of networking to child VMs (Pearce et al., 2013): bridging virtual NICs to physical adapters (appears to be directly connected to the physical network), Network Address Translation (NAT) routing (sharing the IP address of the host), and internal and isolated networking (private network shared with the host). On public IaaS clouds, it is desirable to treat VMs as if they are stan-dard physical servers, thereby bridging VMs networking seeming as the better solution. A bridged adapter can capture traffic on the physical network, without any control from the physical host. This can be an issue in case of promiscuous mode where VMs can analyze all traffic including that not addressed to them (Pearce et al., 2013). To aggravate the scenario, VMMs are known not to yet be bug-free and, from time to time, a vulnerability comes along, as surveyed by Perez-Botero et al. (2013), who presented lists of vulnerabilities for Xen and KVM.

5.2. Future developments

There are also some available surveys concerning security issues in CC (Patel et al., 2013; Modi et al., 2013; Subashini and Kavitha. 2011), namely the ones that can impair integrity, avail-ability, and confidentiality. Using only firewall devices will not help solve these problems. Consequently, Patel et al. (2013) and Modi et al. (2013) examine proposals that incorporate the joint use of IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems). Finally, Samanthula et al. (2015) and Fernandes et al. (2014) discuss threats coming from the diversity of the SaaS, PaaS and IaaS approaches. They also discuss some solutions to target the security challenges in clouds. On one hand, the proposals based on signature detection offer the advantage of minimal response time and human intervention but have the disadvantage of not being able to detect previously unknown ('zero day') attacks. On the other hand, anomaly detection proposals have opposite functional characteristics in comparison with signature-based ones. Hybrid cloud IDPS schemes should be investigated for use in future systems.

Future cloud systems should be able to detect and prioritize simultaneous attacks in terms of their negative impact on the system performance. Then, these systems need to put into action prioritized corrective measures to limit the destructiveness of the more dangerous attacks. In addition, the security solutions should scale or adjust network node numbers, the node heterogeneity (e.g. a federated cloud system), and traffic load, to offer a satis-factory service. It is also worth noting that there is a trade-off between performance and the level of security adopted. Clearly, higher security levels will necessitate more checking, and conse-quently there will be fewer resources for regular customer use. It is therefore advisable to apply the minimally appropriate set of policies by means of self-managing and self-learning.

Cloud users would also need to feel confident that their data privacy is guaranteed when they upload the data to the cloud. To address this security requirement, as suggested in Satyanarayanan et al. (2009), would require trust establishment methods.

A significant piece of research is currently being carried out in the European FP7 project SECCRIT (Secure Cloud Computing for Critical Infrastructure IT), which addresses technical and legal issues in the context of cloud security. This (SECCRIT, 2014; Bless et al., 2013) "is a multidisciplinary research project with the mis-sion to analyze and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating secure, trustworthy, and high assurance cloud computing for cri-tical infrastructure IT." Also, the project is investigating relevant European legal frameworks with the aim of establishing guidelines for using cloud services in the critical infrastructure sector. Otherwise, the use of cloud in this sector, where stringent reg-ulatory and legal requirements exist, will continue to be severely limited. Furthermore, clear guidelines are needed on how to deal with liability issues following any service failures.

Very recently a new cloud service model is winning a con-siderable importance, the Data as a Service (DaaS), which we discuss in the following section.

5.2.1. Security risks of an emerging cloud service model: data as a service

A very recent piece of work (Samanthula et al., 2015) comple-ments previous work (Fernandes et al., 2014; Subashini and Kavitha, 2011), discussing the security risks involved with an emerging cloud service model: Data as a Service (DaaS). The typical usage scenario of this model is the one where the user data is outsourced to the cloud (e.g. Dropbox). However, the data owners lose control over their data because the cloud provider becomes a third party service provider. An initial solution to ensure the data privacy is to encrypt it before exporting it to the cloud. A legacy solution to this issue is based on symmetric key encryption but it is not secure when a revoked user rejoins the system. In this way, Samanthula et al. (2015) propose a homo-morphic encryption and proxy re-encryption scheme that pre-vents leakage of data privacy when a revoked user rejoins the system. This solution also prevents the collusion between a revoked user and the cloud provider. It also supports secure query processing over the encrypted data already stored in a federation of clouds. Further information on this is available in Samanthula et al. (2015).

6. Open issues

We now highlight some unresolved issues and point out future networking research directions in the area of CC (Table 10).

The first key issue is the dynamic management of cloud resources in resource-constrained scenarios (Bodik et al., 2012; Raiciu et al., 2011; Detal et al., 2013) or federated environments with service migration (Popa et al., 2012; MetaCDN, 2014; Akamai, 2014). This resource management needs to be balanced against other aspects, notably fault tolerance (Bodik et al., 2012), energy consumption (Voorsluys et al., 2011; Sakamoto et al., 2012), network utilization (Raiciu et al., 2011), load balancing (Detal et al., 2013), data congestion (Popa et al., 2012), and data availability (MetaCDN, 2014; Akamai, 2014). As an example, SDN may be used to limit the packet flow rate and to forward intelligently the data packets using convenient management policies, respectively, to mitigate congestion and optimize the data availability. In addition, another very interesting challenge needs to be addressed, namely the efficient delivery of diverse services, such as computation, storage, virtualization, applications, and networks (Buyya, 2014).

SDN can be also useful for enhancing the available security in cloud environments, e.g. data centers, by deploying new features such as IDPS (Patel et al., 2013; Modi et al., 2013). It is also important to combine research on legal aspects alongside those of security and resilience if CC and services are to be successfully deployed in critical infrastructure IT (SECCRIT, 2014; Sterbenz et al., 2010). There are a few open issues that need to be addressed for providing a secure CC environment (Ali et al., 2015), such as:

- Harmonizing different security solutions within the cloud sys-tems to offer the desired security level.
- Addressing multi tenancy security issues, namely to ensure the privacy during computations within virtualized, shared and distributed processing environments.
- Security against insider threats; these insider attacks can be avoided to an extent by having definitive criteria for judging between normal and malicious (or compromised) user behavior.
- Finding solutions that create a proper balance between the security requirements and cloud performance.

As suggested in Sherry et al. (2012), it will be necessary to investigate the outsourcing of middleboxes (e.g. NATs, firewalls, load balancers) to the cloud. This outsourcing is justified by the fact the current middleboxes being deployed within the networks of customers impose a considerable cost, management complexity and network overhead. In addition, network hypervisors (i.e. hypervisors coupled with vSwitches controlled by SDN) can bring to future networks the benefits of machine virtualization in terms of flexibility, scale, performance, and assurance, by creating a vir-tualized network infrastructure (Vmware, 2014). This is provisioned as an overlay solution that offers to the application level a full set of reliable networking services with complete indepen-dence of both the underlying network layers (router/switch hardware, physical network topology) and operator domains. Silva et al. (2013) also proposed, at the network edge, a solution that controls the admission of mobile flows in a resource-constrained scenario. Additionally, the accepted flows are managed according to their Classes of Service. The output of this last work could be particularly interesting to be adopted in MCC scenarios.

A new networking paradigm is showing up, namely intelligent embedded systems sensing of local information and reporting it to the Internet for further analysis. Researchers are using the term Internet of Things (IoT) to designate this emerging area. This model should be very relevant everywhere, e.g. in smart cities, houses, office buildings, vehicles, shopping malls, and industrial applications (Comer, 2014). The exponential proliferation of these small devices, each one requiring an IP address for communication with specialized CC systems, should at long last help accelerate the adoption of IPv6.

Companies across the globe clearly also see the cloud's new-business potential (Sen et al., 2013) for promoting sustainable competitive advantage against their market competitors.

In summary, the providers, developers, and end-users of CC must consider several issues in order to take best advantage of CC; these including security, privacy, trust, and resilience; interoper-ability among distinct CC infrastructures; availability, fault-toler-ance, and disaster recovery; and resource management. Another very important CC challenge to be addressed is the 'green' aspect of power efficiency in cloud systems (Sharkh et al., 2013). If these diverse cloud challenges and risks are correctly addressed by industry and academia, possibly working in tandem, the long-term success of CC will hopefully be guaranteed (Voorsluys et al., 2011).

Table 10
Summary of open networking-based issues to deploy cloud computing in future networks.

Open issue	Reference
Dynamic management of cloud resources	Bodik et al. (2012), Raiciu et al. (2011), Detal et al. (2013)
Cloud federation environments	Popa et al. (2011), MetaCDN (2014), Akamai (2014)
Fault tolerance	Bodik et al. (2012)
Energy consumption	Voorsluys et al. (2011), Sakamoto et al. (2012)
Network utilization	Raiciu et al. (2011)
Load balancing	Detal et al. (2013)
Data congestion	Popa et al. (2012)
Data availability	MetaCDN (2014), Akamai (2014)
Intrusion detection and prevention systems	Patel et al. (2013), Modi et al. (2013)
Legal aspects alongside security and resilience	SECCRIT (2014)
Harmonize a large number of diverse security solutions; address multi tenancy security issues; mitigate insider attacks; ensure the right balance between security efficiency and cloud performance	Ali et al. (2015)
Outsourcing of middleboxes (e.g. NATs, firewalls, load balancers) to the cloud; optimizing mobile networks through the management of flows	Sherry et al. (2012), Silva et al. (2013)
Network hypervisors (i.e. hypervisors coupled with virtual switches controlled by SDN)	Vmware (2014)
CC and Internet of Things	Comer (2014)
The new-business potential of clouds	Sen et al. (2013), Sharkh et al. (2013)

7. Conclusion

Despite the many advantages offered by CC, there are also net-working concerns that hamper its fast adoption. This article has reviewed and analyzed the networking-related issues that arise due to resource outsourcing, the virtualized, shared, and public nature of CC, the emerging challenges from security breaches, and the increasing need to provide a resilient CC infrastructure and services.

The major goal of this article was to examine comprehensively the role of networking in CC, and the issues arising. We looked at the origins of CC and discussed the various developments that brought it to the present day. Foundation technologies and architectural models were discussed, as well as some of the more relevant CC offerings. The most pertinent network aspects were presented and discussed in detail, focusing on the crucial support that the networking infrastructure provides for CC. This discussion also presented and examined relevant contributions from indus-try, academia and standardization arenas. Finally, the article also highlighted relevant CC areas requiring further research.

Acknowledgment

The research presented in this article was partly funded by the European Union Seventh Framework Programme (FP7/2007-13), Grant agreement no. 312758: the SECCRIT project.

References

Agarwal Sharad, John Dunagan, Navendu Jain, Stefan Saroiu, Alec Wolman, and Harbinder Bhogan. Volley: automated data placement for geo-distributed cloud services. Proceedings of the 7th USENIX conference on networked systems design and implementation. Berkeley (CA, USA): USENIX Association; 2010. 16 p.

Akamai. (https://www.akamai.com/); 2014 [retrieved 02.03.14].

Alamri Atif, Ansari Wasai Shadab, Hassan Mohammad Mehedi, Shamim Hossain M, Abdulhameed Alelaiwi, Anwar Hossain M. A survey on sensor-cloud: archi- tecture, applications, and approaches. Int J Distrib Sensor Netw 2013 18 p.

Ali M, Khan S, Vasilakos A. Security in cloud computing: Opportunities and chal- lenges. Inf Sci 2015;305(1):357–83.

Amamou Ahmed, Haddadou Kamel, Pujolle Guy. A TRILL-based multitenant data center network. Comput Netw 2014;68:35–53.

Amazon. Elastic compute cloud. ⟨ https://aws.amazon.com/pt/ec2/⟩; 2013 [retrieved 02.03.14].

ANSI/INCITS. Fibre channel backbone-5 Rev 2.0. ANSI. 04/06/2009. ⟨ http://www.t11.org/ftp/t11/pub/fc/bb-5/09-056v5.pdf⟩; 2014. [retrieved 03.03.14].

Armbrust Michael et al. Above the clouds: a berkeley view of cloud computing. Technical report no. UCB/EECS-2009-28; 2009 23 p.

Armbrust Michael, et al. A view of cloud computing. Communun ACM 2010; 53(4):50–8.

AT&T. AT&T cloud architect. ⟨ http://cloudarchitect.att.com/Home/⟩; 2012. [retrieved 02.03.14].

Aazam M, Huh E-N, Kim S. Inter-cloud computing architecture, IETF Informational document, draft-aazam-cdni-inter-cloud-architecture-02 (Expires in 17/09/ 2015); 2015. 22 p.

Azodolmolky S, Wieder P, Yahyapour R. Cloud computing networking: challenges and opportunities for innovations. IEEE Commun Mag 2013;51(7 (July 2013)):54–62.

Badger Lee, Tim Grance, Robert Patt-Comer, Jeff Voas. Cloud computing synopsis and recommendations, NIST Special Publication 800-146. NIST. May of 2012. http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf ⟨ http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf⟩; 2012 [retrieved 03.03.14].

Ballani Hitesh, Paolo Costa, Thomas Karagiannis, Ant rowstron. Towards predictable datacenter networks. In: Proceedings of the ACM SIGCOMM 2011 conference. New York (NY, USA): ACM; 2011. p. 242–253.

Banikazemi M, Olshefski D, Shaikh A, Tracey J, Wang G. Meridian: an SDN platform for cloud network services. IEEE Commun Mag 2013;51(2):120–7.

Bansal N, Bhagwan R, Jain N, Park Yoonho, Turaga D, Venkatramani C. Towards optimal resource allocation in partial-fault tolerant applications. In: INFOCOM 2008. The 27th conference on IEEE computer communications; 2008. 10 p.

Batalla JM. Adaptation of cloud resources and media streaming in mobile cloud networks for media delivery. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud computing networks and environments. Hershey (PA): Information Science Reference; 2015. p. 175–202 doi:10.4018/978-1-4666-8225-2.ch007.

Beloglazov Anton, Buyya Rajkumar, Choon Lee Young, Zomaya Albert Y. A tax- onomy and survey of energy-efficient data centers and cloud computing sys- tems. Adv Comput 2011;82(2011):47–111.

Benson T, Akella A, Shaikh A, Sahu S. Cloudnaas: a cloud networking platform for enterprise applications. In: Proceedings of the 2nd ACM symposium on cloud computing, ser. SOCC'11; 2011. p. 8:1–13.

Birke R, LY Chen, Smirni E.; 2012. Data centers in the cloud: a large scale perfor-mance study. In: IEEE 5th international conference on cloud computing (CLOUD); 2012. p. 336–43.

Bless Roland, Hutchison David, Schöller Marcus, Smith Paul, Tauber Markus. SECCRIT: secure cloud computing for high assurance services. ERCIM News 2013;95.

Bodik Peter, Menache Ishai, Chowdhury Mosharaf, Mani Pradeepkumar, Maltz David A, Stoica Ion. Surviving failures in bandwidth-constrained datacenters. In: Proceedings of the ACM SIGCOMM 2012 conference on applications, tech-nologies, architectures, and protocols for computer communication. New York (NY, USA): ACM; 2012. p. 431–42.

Boutaba Raouf, Limam Noura, Stefano Secci, Taleb Tarik. Cloud networking and communications. Comput Netw 2014;68:1–4.

Briscoe Bob, Sridharan M. IETF – internet draft. IETF. 14/02/2014. http://tools.ietf.org/html/draft-briscoe-conex-data-centre-02; 2014 [retrieved 03.03.14].

Buyya Rajkumar, Yeo Chee Shin, Venugopal Srikumar, Broberg James, Brandic Ivona. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. future generation computer systems. . Elsevier Science Publishers B.V.; 599–616.

Buyya Rajkumar. Introduction to the IEEE transactions on cloud computing. IEEE Trans Cloud Comput 2014;1(1):3–9.

CCGa. Cloud computing glossary (1). ⟨ http://cloudtimes.org/glossary/⟩; 2014 [retrieved 02.03.14].

CCGb. Cloud computing glossary (2). ⟨ http://cloudglossary.com/⟩ 2014 [retrieved 02.03.14].

Chowdhury NM, Kabir Mosharaf, Boutaba Raouf. A survey of network virtualization. Comput Netw 2010;54(5 (April 2010)):862–76.

Charilas D, Vassaki Stavroula, Panagopoulos Athanasios, Constantinou Philipp. Cooperation incentives in 4G networks. In: Zhang Y, Guizani M, editors. Game theory for wireless communications and networking. CRC Press; 2011. p. 295–314 [chapter 13].

Comer Douglas. The ZigBee IP protocol stack. Internet Protocol J 2014;17(2):19–38. Corradi A, Fanelli M, Foschini L. VM consolidation: a real case based on openstack cloud. Future Gen Comput Syst 2014;32(0):118–27.

DARPA_a. Proceed Darpa Project. DARPA. ⟨ http://www.darpa.mil/Our_Work/I2O/Programs/PROgramming_Computation_on_EncryptEd_Data_(PROCEED).aspx⟩; 2013 [retrieved 02.03.14].

DARPA_b. DARPA. Mission-oriented Resilient Clouds (MRC). ⟨ http://www.darpa.mil/Our_Work/I2O/Programs/Mission-oriented_Resilient_Clouds_(MRC).aspx⟩; 2013 [retrieved 02.03.14].

Detal Gregory, Paasch Christoph, Van Der Linden Simon, Merindol Pascal, Avoine Gildas, Bonaventure Olivier. Revisiting flow-based load balancing: stateless path selection in data center networks. Comput Netw 2013;57(5 (April 2013)):1204–16.

Diebold Francis. On the origin(s) and development of the term 'Big Data'. PIER Working paper no. 12-037. 21/09/2012. ⟨ http://papers.ssrn.com/sol3/papers. cfm?abstract_id¾ 2152421⟩; 2014 [retrieved 02.03.14].

Dinh Hoang T, Lee Chonho, Niyato Dusit, Wang Ping. A survey of mobile cloud computing: architecture, applications, and approaches. Wirel Commun Mobile Comput 2013;13(18):1587–611.

Dropbox. Dropbox.⟨ https://www.dropbox.com/⟩; 2014 [retrieved 02.03.14].

Duan Qiang, Yuhong Yan, Vasilakos AV. A survey on service-oriented network vir- tualization toward convergence of networking and cloud computing. IEEE Trans Netw Serv Manag 2012;9(4 (December 2012)):373–92.

Duffield NG, Goyal Pawan, Greenberg Albert, Mishra Partho, Ramakrishnan KK, van der Merive Jacobus E. A flexible model for resource management in virtual private networks. In: Proceedings of the conference on applications, technol-ogies, architectures, and protocols for computer communication. New York (NY, USA): ACM; 1999. p. 95–108.

ETSI. American and European Standards Organizations agree to collaborate on aligning standards to facilitate trade between EU and US. ETSI. 14/02/2013. ⟨ http://www.etsi.org/news-events/news/649-2013-02-ansi-eso-collaboration- at-jpg?highlight ¼ YTozOntpOjA7czo1OiJjbG91ZCI7aToxO3M6OToiY29;tcHV0aW5nIjtpOjI7czoxNToiY2xvdWQgY29tcHV0aW5nIjt9); 2014 [retrieved 02.03.14].

Eucalyptus. Eucalyptus. Eucalyptus. ⟨https://www.eucalyptus.com/why-euca lyptus⟩; 2014 [retrieved 02.03.14].

Fernandes D, et al. Security issues in cloud environments: a survey. Int J Inform Sec 2014;13(2):113–70.

Fernando Niroshinie, Loke Seng W, Rahayu Wenny. Mobile cloud computing: a survey. Future generation computer systems. . Elsevier Science Publishers B. V.; 84–106. Elsevier Science Publishers B. V.; 84–106 n.° 1 (# jan# .

Fiandri C, Kliazovich D, Bouvry P, Zomaya A. Performance and energy efficiency metrics for communication systems of cloud computing data centers. IEEE Trans Cloud Comput 2015;99 14 p..

Gartner. Gartner says worldwide public cloud services market to total $131 billion. 28/02/2013. ⟨ http://www.gartner.com/newsroom/id/2352816⟩; 2014 [retrieved 02.03.14].

Google_a. Google App engine: platform as a service. 07/02/2014. ⟨ https://developers.google.com/appengine/⟩; 2014 [retrieved 02.03.14].

Google_b. Google drive. ⟨ http://learn.googleapps.com/drive⟩; 2014 [retrieved 02.03.14].

GridGain. Gridgain in-memory computing. ⟨ http://www.gridgain.com/⟩; 2014 [retrieved 02.03.14].
Griebel L, Prokosch H-U, Köpcke F, Toddenroth D, Christoph J, Leb I, Engel I, Sedl-mayr M. A scoping review of cloud computing in healthcare. BMC Med Inform Decis Mak 2015;15(17), . http://dx.doi.org/10.1186/s12911-015-0145-7 16 p..
Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulner- abilities. IEEE Secur Priv 2011;9(2):50–7.
Grover J, Kheterpal G. Mobile cloud computing: an introduction. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud computing networks and environments. Hershey (PA): Information Science Reference; 2015. p. 1–23. http://dx.doi.org/10.4018/978-1-4666-8225-2.ch001.
Gupta A, et al. SDX: a software defined internet exchange. SIGCOMM. Comput. Commun. Rev. 2014;44(4 (August 2014)):551–62.
Hu Yan, Zhu Ming, Xia Yong, Chen Kai, Luo Yanlin. 2012. GARDEN: generic addressing and routing for data center networks. In: IEEE 5th international conference on cloud computing (CLOUD); 2012. p. 107–14.
Huerta-Canepa Gonzalo, Lee Dongman. A virtual cloud computing provider for mobile devices. In: Proceedings of the 1st ACM workshop on mobile cloud computing services: social networks and beyond. New York (NY, USA): ACM; 2010. p. 6:1–5.
Huston Geoff A. Retrospective: twenty-five years ago. Internet Protocol J 2012; 15(1):24–35.
Hwang Junseok, Shin Andrei, Yoon Hyenyoung. Dynamic reputation-based incen-tive mechanism considering heterogeneous networks. In: Proceedings of the 3rd ACM workshop on performance monitoring and measurement of hetero-geneous wireless and wired networks. New York (NY, USA): ACM; 2008. p. 137–44.
IEEE. IEEE Standard for local and metropolitan area networks—virtual bridged local area networks amendment 13: congestion notification. IEEE Std 802.1Qau-2010 (Amendment to IEEE Std 802.1Q-2005); April 2010. p. c1-119.
IEEE. IEEE standard for local and metropolitan area networks—media access control (MAC) bridges and virtual bridged local area networks—Amendment 17: priority-based flow control. IEEE Std 802.1Qbb-2011 (Amendment to IEEE Std 802.1Q-2011 as amended by IEEE Std 802.1Qbe-2011 and IEEE Std 802.1Qbc-2011); Sept 2011. p. 1–40.
Jain R, Paul S. Network virtualization and software defined networking for cloud computing: a survey. IEEE Commun Mag 2013;51(11 (November 2013)):24–31.
Jamshidi Pooyan, Ahmad Aakash, Pahl Claus. Cloud migration research: a sys- tematic review. IEEE Trans Cloud Comput 2013;1(2):142–57.
Jin Hai, Ibrahim Shadi, Qi Li, Cao Haijun, Wu Song, Shi Xuanhua. The mapreduce programming model and implementations. In: Cloud Computing. John Wiley & Sons, Inc.; 373–90.
Katzis K. Mobile cloud resource management. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud computing networks and environments. Hershey (PA): Information Science Reference; 2015. p. 69–96. http://dx.doi.org/10.4018/978-1-4666-8225-2.ch004.
Keahey K, Foster I, Freeman T, Zhang X. Virtual workspaces: achieving quality of service and quality of life in the grid. . Scientific Programming (IOS Press); 265–275.
Kim Hyunjoo, Parashar Manish. CometCloud: an autonomic cloud engine. In: Cloud Computing, 2011. John Wiley & Sons, Inc.; 275–97.
Koumaras H, Damaskos C, Diakoumakos G, Kourtis M, Xilouris G, Gardikis G, Koumaras V, Siakoulis T. Virtualization evolution: from IT infrastructure abstraction of cloud computing to virtualization of network functions. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud computing networks and environments. Hershey (PA): Information Science Reference; 2015. p. 279–306. http://dx.doi.org/10.4018/978-1-4666-8225-2.ch010.
Kryftis Y, Mastorakis G, Mavromoustakis CX, Batalla JM, Bourdena A, Pallis E. A resource prediction engine for efficient multimedia services provision. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud com-puting networks and environments. Hershey (PA): Information Science Reference; 2015. p. 361–80. http://dx.doi.org/10.4018/978-1-4666-8225-2.ch012.
Li Feng, Ooi Beng Chin, Tamer Ozsu M, Wu Sai. Distributed data management using MapReduce. . ACM Computing Surveys (ACM); 31:1–42.
Mastorakis G, Mavromoustakis CX, Pallis E. Resource management of mobile cloud computing networks and environments. Hershey (PA): IGI Global; 1–432. http://dx.doi.org/10.4018/978-1-4666-8225-2.
Mavromoustakis CX, Mastorakis G, Bourdena A, Pallis E, Stratakis D, Perakakis E, Kopanakis I, Papadakis S, Zaharis ZD, Skeberis C, Xenos TD. A social-oriented mobile cloud scheme for optimal energy conservation. In: Mastorakis G, Mav-romoustakis C, Pallis E, editors. Resource management of mobile cloud com-puting networks and environments. Hershey (PA): Information Science Refer-ence; 2015. p. 97–121. http://dx.doi.org/10.4018/978-1-4666-8225-2.ch005.
McKeown Nick, et al. OpenFlow: enabling innovation in campus networks. SIG- COMM Comput Commun Rev (ACM) 2008;38(2 (# mar# 2008)):69–74.
Medina Violeta, Manuel Garcia Juan. A survey of migration mechanisms of virtual machines. ACM Comput Surv (ACM), 46; 30:1–33.
Mei Lijun, Chan WK, Tse TH. A tale of clouds: paradigm comparisons and some thoughts on research issues. In: Asia-Pacific services computing conference, 2008. APSCC'08. IEEE; 2008. p. 464–9.
Mell Peter, Grance Timothy. The NIST definition of cloud computing. Tech. rep. Gai-thersburg (MD): National Institute of Standards and Technology (NIST); 2011.
Metri G, Srinivasaraghavan S, Shi Weisong, Brockmeyer M. Experimental analysis of application specific energy efficiency of data centers with heterogeneous servers. In: IEEE 5th international conference on cloud computing (CLOUD); 2012. p. 786–93.
MetaCDN. (http://www.metacdn.com/); 2014 [retrieved 02.03.14].
Microsoft_a. Windows azure. ⟨ https://www.windowsazure.com/en-us/⟩; 2014 [retrieved 02.03.14].
Microsoft_b. OneDrive. ⟨ https://onedrive.live.com/about/en-us/⟩; 2014 [retrieved 02.03.14].
Modi Chirag, Patel Dhiren, Borisaniya Bhavesh, Patel Hiren, Patel Avi, Rajarajan Muttukrishnan. A survey of intrusion detection techniques in cloud. J Netw Comput Appl 2013;36(1 (# jun# 2013)):42–57.
Mohapatra, P, et al. Fast connectivity restoration using BGP add-path. IETF – Internet Draft. IETF. ⟨ https://tools.ietf.org/html/draft-pmohapat-idr-fast-conn- restore-03⟩; 2013 [retrieved 26.06.15].
Moura Jose, Serrão Carlos. Security and privacy issues of big data. In: Zaman N, Seliaman M, Hassan M, Marquez F, editors. Handbook of research on trends and future directions in big data and web intelligence. Hershey (PA): Information Science Reference; 2015. p. 20–52 doi:10.4018/978-1-4666-8505-5.ch002.
Murphy Michael A, Abraham Linton, Fenn Michael, Goasguen Sebastien. Autonomic clouds on the grid. J Grid Comput, 8; 1–18.
ND. Cloud solutions. http://www.nttdata.com/global/en/services/cloud/index.html; 2014 [retrieved 02.03.14].
Nunes B, Mendonca M, Nguyen X, Obraczka K, Turletti T. A survey of software- defined networking: past, present, and future of programmable networks. IEEE Commun Surv Tutorials PP 2014;2014(99):1–18(2014;2014:1–18.
Obama. Big data initiative: announces $200 million in new R&D investments. 29/ 03/2012. ⟨ http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf⟩; 2014 [retrieved 02.03.14].
Oracle. Cloud Computing. May of 2010. ⟨ http://www.oracle.com/us/technologies/cloud/oracle-cloud-computing-wp-076373.pdf⟩; 2014 [retrieved 02.03.14].
Panagiotakis S, Vakintis I, Andrioti H, Stamoulias A, Kapetanakis K, Malamos A. Towards ubiquitous and adaptive web-based multimedia communications via the cloud. In: Mastorakis G, Mavromoustakis C, Pallis E, editors. Resource management of mobile cloud computing networks and environments. Hershey (PA): Information Science Reference; 2015. p. 307–60 doi:10.4018/978-1-4666-8225-2.ch011.
Patel Ahmed, Taghavi Mona, Bakhtiyari Kaveh, Celestino Junior Joaquim. Review: an intrusion detection and prevention system in cloud computing: a systematic review. J Netw Compu Appl, 36; 25–41.
Pearce M, Zeadally S, Hunt R. Virtualization: issues, security threats, and solutions. ACM Comput Surv, 45; 17:1–39.
Perez-Botero D, Szefer J, Lee RB. Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the international workshop on security in cloud computing (SCC); 2013. p. 3–10.
Popa Lucian, Krishnamurthy Arvind, Ratnasamy Sylvia, Stoica Ion. FairCloud: sharing the network in cloud computing. SIGCOMM 2012. ACM; 2012. 12 p.
Press, Gil. A very short history of big data. Forbes. 21/12/2013. ⟨ http://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/⟩; 2014 [retrieved 02.03.14].
ProgrammableWeb. Programmable Web. 2014. ⟨ http://www.programmableweb. com/⟩ [retrieved 03.03.14].
PT. Cloud solutions. ⟨ https://cloud.ptempresas.pt/Pages/Catalog/ServiceDetail.aspx? s¼ 06IG3nFf0pSkKNHn-KBVCw&language¼ en-US⟩; 2014 [retrieved 02.03.14].
Raiciu Costin, Barre Sebastien, Pluntke Christopher, Greenhalgh Adam, Wischik Damon, Handley Mark. Improving datacenter performance and robustness with multipath TCP. In: Proceedings of the ACM SIGCOMM 2011 conference. New York (NY, USA): ACM; 2011. p. 266–77.
Rambold Michael, Kasinger Holger, Lautenbacher Florian, Bauer Bernhard. Towards autonomic service discovery a survey and comparison. In: Proceedings of the 2009 IEEE International Conference On Services Computing. Washington (DC, USA): IEEE Computer Society; 2009. p. 192–201.
Retana A, White R. Internet Protocol J 2013;16(2):23–9.
Ricci Robert, Alfeld Chris, Lepreau Jay. A solver for the network testbed mapping problem. SIGCOMM Comput Commun Rev (ACM), 33; 65–81.
Rimal Bhaskar Prasad, Choi Eunmi, Lumb Ian. A taxonomy and survey of cloud computing systems. In: Proceedings of the 2009 fifth international joint con-ference on INC, IMS and IDC. Washington (DC, USA): IEEE Computer Society; 2009. p. 44–51.
Rodero-Merino L, Vaquero LM, Caron E, Desprez F, Muresan A. Building Safe PaaS clouds: a survey on security in multitenant software platforms. Comput Secur 2012;31(1):96–108.
Sakamoto T, Yamada H, Horie H, Kono K. Energy-price-driven request dispatching for cloud data centers. In: IEEE 5th international conference on cloud com-puting (CLOUD); 2012. p. 974–6.
Salesforce. Salesforce1 platform. ⟨ http://www.salesforce.com/eu/platform/over view/⟩; 2014 [retrieved 02.03.14].
Samanthula Bharath, Elmehdwi Yousef, Howser Gerry, Madria Sanjay. A secure data sharing and query processing framework via federation of cloud computing. Inf Syst 2015;48:196–212.
Satyanarayanan Mahadev, Bahl P, Caceres R, Davies N. The case for VM-based cloudlets in mobile computing. IEEE Pervasive Comput 2009;8(4 (Oct 2009)):14–23.
SECCRIT project. ⟨ https://www.seccrit.eu/⟩; 2014 [retrieved 14.03.14].
Seibold M, Wolke A, Albutiu M, Bichler M, Kemper A, Setzer T. Efficient Deployment of Main-Memory DBMS in Virtualized Data Centers. IEEE 5th International Conference on Cloud Computing (CLOUD) 2012;2012:311–8.
Sen, Soumya Carlee, Joe-Wong Sangtae, Ha, Chiang Mung. A survey of smart data pricing: past proposals, current plans, and future trends. ACM Comput Surv (ACM), 46; 15:1–37.
Services. Services world congress 2013. ⟨ http://www.servicescongress.org/2013/⟩; 2013 [retrieved 02.03.14].

Sharkh MA, Jammal M, Shami A, Ouda A. Resource allocation in a network-based cloud computing environment: design challenges. IEEE Commun Mag 2013; 51(11 (November 2013)):46–52.

Sherry Justine, Hasan Shaddi, Scott Colin, Krishnamurthy Arvind, Ratnasamy Sylvia, Sekar Vyas. Making middleboxes someone else's problem: network processing as a cloud service. In: Proceedings of the ACM SIGCOMM 2012 conference on applications, technologies, architectures, and protocols for computer commu-nication. New York (NY, USA): ACM; 2012. p. 13–24.

Shieh, Alan, Kandula Srikanth, Greenberg Albert, Kim Changhoon, Saha Bikas. Sharing the data center network. In: Proceedings of the 8th USENIX conference on networked systems design and implementation. Berkeley (CA, USA): USENIX Association; 2011. p. 23.

Shin S, Gu G. CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?). In: Proceedings of the 2012 20th IEEE international conference on network protocols (ICNP), ser. ICNP'12; 2012. p. 1–6.

Silva Joao, Jose Moura, Rui Marinheiro, Joao Almeida. Optimizing 4G networks with flow management using an hybrid broker. In: Proceedings of the of interna-tional conference on advances in information technology and mobile com-munication. Elsevier; 2013. p. 290–8.

SNIA. Cloud storage initiative. SNIA. ⟨ http://www.snia.org/forums/csi⟩; 2014 [retrieved 03.03.14].

Sridhar_a T. Cloud computing – a primer, Part 1: models and technologies. Internet Protocol J 2009;12(3):2–19.

Sridhar_b T. Cloud computing – a primer, Part 2: infrastructure and implementa- tion topics. Internet Protocol J 2009;12(4):2–17.

Stallings W. Gigabit Ethernet: from 1 to 100 Gbps and beyond. Internet Protocol J 2015;18(1):20–32.

Sterbenz James, Hutchison David, Çetinkaya Egemen, Abdul Jabbar, Justin Rohrer, Schöller Marcus, Smith Paul. Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Comput Netw 2010;54(8):1245–65.

Strijkers Rudolf, Makkes Marc, Laat Cees de, Meijer Robert. Internet factories: creating application-specific networks on demand. Comput Netw 2014;68: 187–198.

Strunk A. QoS-aware service composition: a survey. In: 2010 IEEE 8th European conference on web services (ECOWS); 2010, 67–74.

Subashini S, Kavitha V. Review: a survey on security issues in service delivery models of cloud computing. J Netw Comput Appl, 34. (Academic Press Ltd.; 1–11.

Tanase Mihai, Cristea Valentin. Quality of service in large scale mobile distributed systems based on opportunistic networks. In: Proceedings of the 2011 IEEE workshops of international conference on advanced information networking and applications. Washington (DC, USA): IEEE Computer Society; 2011. p. 849–54.