Implementation of Cloud Computing into VoIP

Floriana GEREA
Economic Informatics Department, Academy of Economic Studies, Bucharest, Romania
floriana.gerea@gmail.com

This article defines Cloud Computing and highlights key concepts, the benefits of using virtualization, its weaknesses and ways of combining it with classical VoIP technologies applied to large scale businesses.
The analysis takes into consideration management strategies and resources for better customer orientation and risk management all for sustaining the Service Level Agreement (SLA). An important issue in cloud computing can be security and for this reason there are several security solution presented.
***Keywords**: Cloud computing, VoIP, Data virtualization, DoS*

1 Introduction

Present article focuses on the importance of virtualization in VoIP technologies and how the virtualization can improve the VoIP communication technologies extending this article's conclusions.
Progress of research efforts in a new technology is contingent on having a rigorous organization of its knowledge domain and a comprehensive understanding of all the relevant components of this technology and their relationships.
The National Institute of Standards and Technology (NIST) defines cloud computing as a model for convenient, on-demand network access to computing resources such as networks, servers, storage, applications, and services that can be quickly deployed and released with very little management by the cloud-provider [4].
Cloud computing is an emerging technology from which many different industries and individuals can greatly benefit. Cloud computing services certainly have the potential to benefit both providers and users. However, in order for cloud computing to be practical and reliable, many existing issues must be resolved.
The use of cloud computing is particularly appreciated to users because it is rather inexpensive and it is very convenient. Users can access data or use applications with only a personal computer and internet access.
Over the years virtualization had an important role in developing IT projects. However which are the virtualization concepts, when can we use it and are there any risks that can appear in such implementation? These questions will be answered in the following paragraphs.
Also challenges in architectural design and security represent the main task that should be analyzed in implementing Cloud architecture for VoIP.

2. Architectural Cloud Computing

Cloud computing is quickly becoming one of the most popular new idea that will supposedly reshape the information technology (IT) services landscape. According to The Economist in a 2008 article, it will have huge impacts on the information technology industry, and also profoundly change the way people use computers [2]. What exactly is cloud computing then, and how will it have such a big impact on people and the companies they work for? In order to define cloud computing, it is first necessary to explain what is referenced by the phrase "The Cloud".
Cloud computing is in many ways a conglomerate of several different computing technologies and concepts like grid computing, virtualization, Service oriented

Architecture (SOA) [3], peer-to-peer (P2P) computing [2].

To begin understanding cloud computing, it is necessary to examine it in abstraction layers.

Figure 2 illustrates the five layers that constitute cloud computing [4]. A particular layer is classified above another if that layer's services can be composed of services provided by the layer beneath it.

The bottom layer is the physical hardware, namely the cloud-provider owned servers and switches that serve as the cloud's backbone. The next layer consists of the cloud's software kernel. This layer acts as a bridge between the data processing performed in the cloud's hardware layer and the software infrastructure layer which operates the hardware.

The abstraction layer above the software kernel is called software infrastructure. This layer renders basic network resources to the two layers above it in order to facilitate new cloud software environments and applications that can be delivered to end-users in the form of IT services.

The services offered in the software infrastructure layer can be separated into three different subcategories: computational resources, data storage, and communication. [5]

Several current examples of clouds that offer flexible amounts of computational resources to its customers include the Amazon Elastic Compute Cloud (EC2) [9], Enomaly's Elastic Computing Platform (ECP) [10], and RESERVOIR architecture [6]. Computational resources, also called Infrastructure as a Service (IaaS), are available to cloud customers in the form of virtual machines (VMs). Voice over Internet Protocol (VoIP) telephones, instant messaging, and audio and video conferencing are all possible services which could be offered by CaaS in the future.

All of three software infrastructure subcomponents, cloud-customers can rent virtual server time (and thus their storage space and processing power) to host web and online gaming servers, to store data, or to provide any other service that the customer desires.

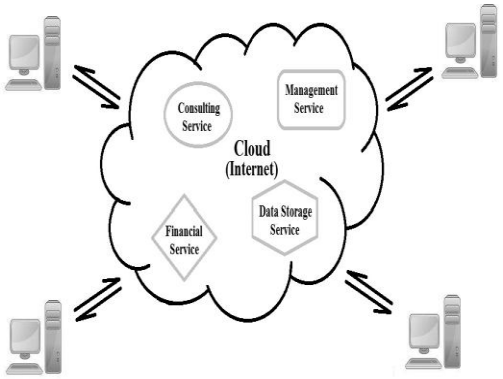

Fig. 1. Cloud computing [5]

When developers design their cloud software for a specific cloud environment, their applications are able to utilize dynamic scaling and load balancing as well as easily have access to other services provided by the cloud software environment provider like authentication and email. This makes designing a cloud application a much easier, faster, and more manageable task. There are several Virtual Infrastructure Managements in IaaS, such as CLEVER [25], Open-QRM [8], OpenNebula [6], and Nimbus [9].

Cloud management provides remote and secure interfaces for creating, controlling, and monitoring virtualized sources on an infrastructure-as-a-service cloud. VI management provides primitives to schedule and manage VMs across multiple physical hosts. VM managers provide simple primitives (start, stop, suspend) to manage VMs on a single host.

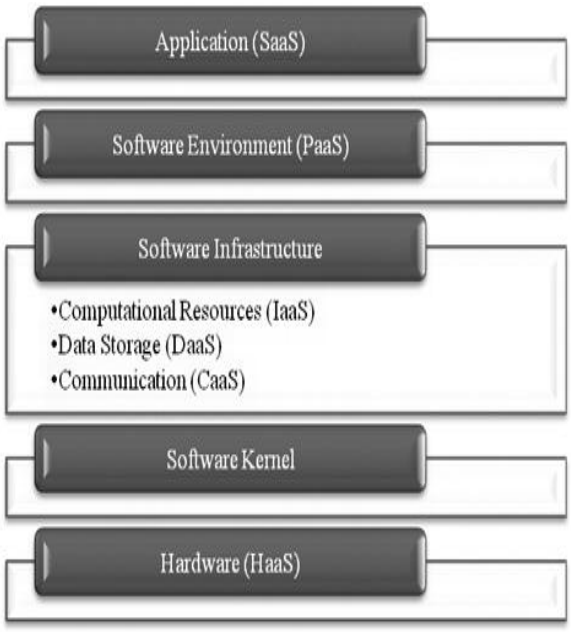

Fig. 2. The five abstraction layers of cloud computing [5]

3 Benefits from Cloud Computing

- *Access to Services that are otherwise unavailable.* In some circumstances, a service-provider may offer a new or exclusive capability - although this is likely to be the case only during a limited period of time, since most such services are, at least in principle, compatible. A more common situation is that some organizational users, and especially many individual users, may be technically or financially incapable of establishing and running a particular service for themselves
- *Access to Services from multiple desktop devices.* Each user, whether within an organization or acting as an individual, is likely to use multiple desktop devices, in various locations, including at home, at work, at clients' sites, in airport lounges, in Internet cafes, etc. By using authoritative data running on a remote device, the user reduces device-dependence in exchange for increased network-access dependence. In many circumstances, the trade-off may be advantageous
- Access to Services from scaled-down devices. A service may perform the vast majority of the function server-side, enabling the client to be run on a device with very limited capacity. This opens up scope for long-promised but little-used 'thin clients', but the primary devices used are more likely to be various forms of handheld computers, and mobile phones. This depends, however, on the service being designed with this aim in mind
- Access to Services from multiple device-types. Each user, whether within an organization or acting as an individual, is likely to use multiple kinds of devices, including desktop PCs, portable PCs, various forms of handheld computers, and mobile phones. A suitably-designed service may be able to support convenient access to data and applications on any and each of these device-types, through a variety of user-interfaces

Other Technical Benefits

- Professionalized backup and recovery. A service may be designed to provide assured backup of data and software, and assured, simple, efficient recovery. This is because these are core capabilities of a service provider, and that organization is likely to be more professional, attentive and disciplined than many user organizations and particularly individual users. Backup and recovery services can be provided whether the primary operational service is run on the user's own network, outsourced, or delegated to the cloud.
- *Scalability.* Where the transaction and/or data-volumes vary significantly over time, a service may offer assured server-capacity, storage-capacity, and access to the requisite application software. This may apply in a long-term growth curve (or indeed a tailing-off, as occurs with many legacy systems), and in contexts that involve highly-peaked demand, associated with daily, weekly, monthly, annual or even longer cycles, and with events

- *Collaboration convenience.* Collaborative content (including documents and other data which are co-owned and co-maintained) is inherently accessible and amendable by multiple authors. There are advantages in hosting a service such as a Wiki remotely from each of the participants. There may be advantages in the remote host being flexible rather than fixed
- *Copyright convenience.* The service-provider can assume responsibility for all aspects of acquisition, maintenance and licensing of software and of data

Few of the potential benefits arise solely from the incremental difference between cloud computing and its predecessors, and hence rational users need to consider whether cloud computing or some more conventional form of outsourcing, or indeed insourcing, is appropriate to their needs. Moreover, none of the benefits arise automatically, but rather are contingent on correspondence between the user's needs, on the one hand, and the service-provider's capabilities, terms of service and pricing, on the other.

Despite the technical benefits, it appears that service-providers perceive the primary driver for adoption as being cost-savings. A secondary driver may be convenience to business divisions arising from the ability to by-pass internal IT departments and contract directly for services. If this transpires to be the case, then the cautious risk assessment conventionally undertaken by IT departments will also be by-passed. It is therefore particularly important for senior executives to appreciate the downsides of cloud computing that are analyzed in the following sections. Technical factors are identified first, then business risks.

Despite all the benefits, there some security issues that are going to be discussed in the following part.

4 VoIP Cloud Computing vs. Traditional VoIP

In the traditional VoIP technology because the information is on a single server several problems can appear regarding data availability and integrity, security and in order to resolve these, money is spend on hosting software, applications and people with the requisite expertise. On the other hand Cloud Computing is less expensive because of its financial benefits.

Assuming that the hardware equipments can encounter several malfunctions, in a time when the services' quality is extremely important, the information needs to be available in real time. The traditional approach is to invest in a large number of equipments in order to avoid the loss of call and provide a correct functionality of the telephony service. However, these long term investments may be justified but at a closer analysis we can find that those equipments are not using all their resources. There has been statistically proven that most of the servers' hardware will never be fully used and as time passes they will be replaced due to moral and physical degrading.

Cloud computing can solve all these aspects. Organizations can avoid large investments in equipments and software by using a much smaller number of resources for one solution.

In this way investments can be made in fewer equipments with larger resources that are wiser employed, by creating a large number of virtual nods on one physical machine. By monitoring and controlling performance, organizations can easily decide which resources can be allocated on different services.

The reduction of operational costs

In cloud computing the organizations or the individual user are able to pay for only the services they need, avoiding the excess of employed resources that is involved in the traditional method.

Economy can be made, provided the service provider has an well-organized plan. In this way cloud computing has significant economical advantages comparing to the traditional method.

We also must mention the personnel costs that in the traditional method implies, because it requires a large number of people to mange resources, allocated in different geographical areas. Also, every new installation needs to be fully made, and this translates in large installation time for every new server. In cloud computing these aspects can be solved in a reduced amount of time, the installation of services taking very little. It is done by cloning other virtual nodes, so all the software and application installation is done only once and then all the new software is installed by cloning. In this way a large number of identical servers can be created within minutes, without the need to separately install each necessary application.

Cloud computing reduces human error to a minimum, due to the fact that there is no need to process the same information every time. It is enough to have only one correct virtual machine, that has been tested, all the other being replicas of the first.

- *Migrating services from one geographical area to another, from one machine to another, transferring from one solution to another*

The classical method required for each modification to restart all the installation procedures, which involved time spent and large costs. Cloud computing has the extraordinary benefit of easily moving information from one machine to another and between servers, without taking into account the geographical distance. It is possible for a virtual machine to have a node in Bucharest and to move that service within minutes on another server in Brasov, without damages or problems. Within minutes servers can be moved from one location to another, from one country to another, while keeping the service functional even while migrating.

This option did not exist in the traditional method. Using this method implied that the service would not be functional for at least several days, and that the physical movement of the server from one location to another was needed as well as a list of modifications that are necessary for any physical movement.

5 The levels that can attack a VoIP infrastructure

Denial-of-Service or VoIP Service Disruption. Denial-of-service (DoS) attacks can affect any IP-based network service. The impact of a DoS attack can range from mild service degradation to complete loss of service. There are several classes of DoS attacks. One type of attack in which packets can simply be flooded into or at the target network from multiple external sources is called a distributed denial-of-service (DDoS) attack.[3] DoS attacks are difficult to defend against, and because VoIP is just another IP network service, it is just as susceptible to DoS attack as any other IP network services. Additionally, DoS attacks are particularly effective against services such as VoIP and other real-time services, because these services are most sensitive to adverse network status. Viruses and worms are included in this category as they often cause DoS or DDoS due to the increased network traffic that they generate as part of their efforts to replicate and propagate.[9]

ARP Spoofing

ARP is a fundamental Ethernet protocol [3]. Perhaps for this reason, manipulation of ARP packets is a potent and frequent attack mechanism on VoIP networks. Most network administrators assume that deploying a fully switched network to the desktop prevents the ability of network users to sniff network traffic and potentially capture sensitive information traversing the network. Unfortunately, several techniques and tools exist that allow any user to sniff traffic on a switched network because ARP has no provision for authenticating queries or query replies [4].

Additionally, because ARP is a stateless protocol, most operating systems (Solaris is an exception) update their cache when receiving ARP reply, regardless of whether they have sent out an actual request.

H.323-Specific Attacks

The only existing vulnerabilities that we are aware of at this time take advantage of ASN.1 parsing defects in the first phase of H.225 data exchange. More vulnerability can be expected for several reasons: the large number of differing vendor implementations, the complex nature of this collection of protocols, problems with the various implementations of ASN.1/PER encoding/decoding, and the fact that these protocols —alone and in concert — have not endured the same level of scrutiny that other, more common protocols have been subjected to. For example, we have unpublished data that shows that flooding a gateway or media server with GRQ request packets (RAS registration request packets) results in a DoS against certain vendor gateway implementations—basically the phones deregister [9].

SIP-Specific Attacks

Multiple vendors have confirmed vulnerabilities in their respective SIP (Session Initiation Protocol) implementations [3].The vulnerabilities have been identified in the INVITE message used by two SIP endpoints during the initial call setup. The impact of successful exploitation of the vulnerabilities has not been disclosed but potentially could result in a compromise of a vulnerable device. In addition, many recent examples of SIP Denial of Service attacks have been reported.

Recent issues that affect Cisco SIP Proxy Server (SPS) demonstrate the problems SIP implementers may experience due to the highly modular architecture or this protocol. The SSL implementation in SPS (used to secure SIP sessions) is vulnerable to an ASN.1 BER decoding error similar to the one described for H.323 and other protocols. This example illustrates a general concern with SIP: As the SIP protocol links existing protocols and services together, all the classic vulnerabilities in services such as SSL, HTTP, and SMTP may resurface in the VOIP environment.

Policies and Processes

Encryption

All VoIP systems should use a form of Media (RTP channel) Encryption in order to avoid the sniffing of VoIP data. All communications between network elements should be encrypted. Complete end-to-end IP voice encryption is recommended to mitigate the threat of eavesdropping attempts. Additionally, all administrative access to critical server and network components must use encrypted protocols such as SSL and/or SSH [5]. All access to remote administrative functions should be restricted to connections to the switch itself or to a designated management PC [9].

Physical Security

Physical security is an essential part of any security plan [6]. Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, intrusion, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Safeguards can be broken down into two categories: human and environmental.

Human safeguard recommendations are:

- Console access should be restricted or eliminated.
- Logon, boot loader, and other passwords must be a minimum of eight characters including at least one each of alpha, numeric, and ctl characters.
- VoIP components must be located in a secure location that is locked and restricted to authorized personnel only.
- Access to these components, wiring, displays, and networks must be controlled by rules of least privilege.
- System configurations (i.e., hardware, wiring, displays, networks) must be documented. Installations and changes to those physical configurations must be

governed by a formal change management process.
- A system of monitoring and auditing physical access to VoIP components, wiring, displays, and networks must be implemented (e.g., badges, cameras, access logs). From the point at which an employee enters the building, it is recommended that there be a digital record of their presence.
- The server room should be arranged in a way that people outside the room cannot see the keyboard (thus seeing users/admin passwords).
- Any unused modems must be disabled/removed.
- No password evidence (notes, sticky notes, etc.) is allowed around the system.
- The CPU case should be locked and the key must be accounted for and protected. A backup key should be made and kept securely offsite (e.g., in a safety deposit box).
- USB, CD-ROM, monitor port, and floppy disks drives should be removed, disabled, or glued shut.
- Adequate temperature and humidity controls must be implemented to avoid equipment damage.
- Adequate surge protectors and UPS must be implemented, maintained, and tested.
- Cleaning and maintenance people should be prohibited from the area surrounding
any electronics.
- Food, drink, or smoking is prohibited in the same areas.

IP-PBX equipment must be located in a locked room with limited access. This type of access must be provided as a user authentication system with either a key-card or biometric device. The use of a keypad alone to gain access is not permitted. All methods of gaining entry into the room must provide for a list of users that have accessed the room along with a date/time-stamp [6].

6 Security for the VoIP Infrastructure

One example of how to configure a secure an system cloud for VoIP is the creation of a network demilitarized zone (DMZ) on a single host.

In this example, three virtual machines are configured to create a virtual DMZ on Standard Switch 1: Virtual Machine 1, 2,3 and 4 run Web server and are connected to virtual adapters through standard switches.

These virtual machines are multi homed. The Machine 5 and 6 runs an Asterisk server. The conduit between these elements is Standard Switch 2, which connects the firewalls with the servers. This switch has no direct connection with any elements outside. From an operational viewpoint, external traffic from the Internet enters Virtual Machine 1 through Hardware Network Adapter 1 (routed by Standard Switch 1) and is verified by the firewall installed on this machine. If the firewall authorizes the traffic, it is routed to the standard switch in the DMZ, Standard Switch 2. Because the Web server and application server are also connected to this switch, they can serve external requests. Standard Switch 2 is also connected to Virtual Machine 4 and Virtual Machine 5. This virtual machine provides a firewall between the DMZ and the internal corporate network.

This firewall filters packets from the Web server and application server. If a packet is verified, it is routed to Hardware Network Adapter 2 through Standard Switch 3. Hardware Network Adapter 2 is connected to the internal corporate network. This network could be used for virus propagation or targeted for other types of attacks. The security of the virtual machines in the DMZ is equivalent to separate physical machines connected to the same network.

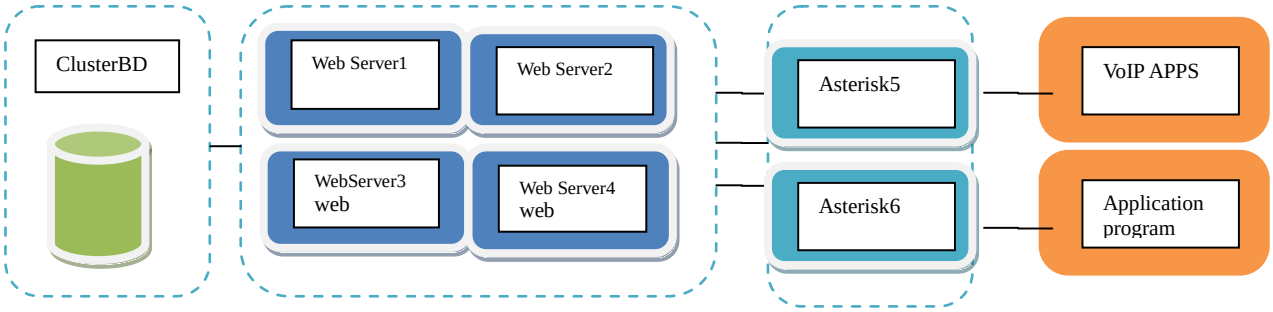

Fig. 3. Architecture VoIP

VoIP is a highly critical data application and as such, is subject to all the policies detailed in other data security policy sections (this assumes that the VoIP Security Policy module is part of a larger set of security policy modules).

Because in the cloud-based computing environment, the employees can easily access, falsify and divulge the data. Sometime such behaviour is a disaster for a big and famous company.

Some service providers develop some technical method aimed to avoid the security treats from the interior. For instance, some providers limit the authority to access and manage the hardware, monitor the procedures, and minimize the number of staff who has privilege to access the vital parts of the infrastructure. However, at the provider backend, the administrator can also access the customer's VM-machine.

Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This, however, is becoming increasingly challenging because as security developments are made, there always seems to be someone to figure out a way to disable the security and take advantage of user information.

Traditional telephony, based on dedicated transmission lines, used over the last decades, has found through VoIP an important competitor, mainly because of the technology differences between them. In traditional telephony, through the switch-circuit system (circuit commuting), a communication channel between the two correspondents is assured. This channel (physic electric circuit obtained by cables and electronic circuits) must be assured before the communication starts. During the conversation the channel must be used only by the same initial correspondents, being a channel dedicated to communication. At the end of the conversation, this channel must be cancelled. This system was later improved by multiplexing of more channels on the same physic conductor, but each of these channels is dedicated only to one call at a certain time. In telecommunication, circuit commuting represents o routing method of the transmission between two correspondents, through one or more commuting centres. Between these two correspondents a continuous electronic connection is established, which will have the audio signal. The total of these telephonic central systems and of the connections that forms between them is called public network of commuting telephony (PSTN: Public Switched Telephone Network).

Improved functionality: another important advantage is that of a improved functionality as compared to classic telephony. Some of the functionalities offered by VoIP are difficult or even impossible to accomplish in the classic telephony. Among these, there is the possibility to use an IP telephone wherever there is a connexion to Internet. This creates the possibility that the "fix" telephone be taken in travelling, having the call number everywhere. The most important beneficiaries of this facility are the Call Centre agencies, that use VoIP

telephony in foreign countries due to the reduced costs with cheaper work force.

7 Conclusion

By innovation and a perfectible degree of security, VoIP industry is consolidating is market place, frightening to be able soon to take the place of conventional solutions (expensive, insecure and inflexible).

Cloud computing allows to create inexpensive systems, with little upfront costs and to be scaled to massive sizes, when needed. In many cases the best VOIP solution is to use cloud computing and replace the classical solution. The advantages can be defined both by the providers, which are motivated by the future profits that can arise due to the lower costs that the classical technology, as well as the users who have the possibility of reducing or eliminating the telephony service costs.

References

[1] G. Gruman, E. Knorr, What cloud computing really means. *InfoWorld*, (2009, May). [Online]. Available: http://www.infoworld.com/d/cloudcomputing/what-cloud-computing-reallymeans-031

[2] L. Siegele, Let it rise: A survey of corporate IT. *The Economist*, (Oct., 2008).

[3] P. Watson, P. Lord, F. Gibson, Panayiotis Periorellis, and Georgios Pitsilis. *Cloud computing for e-science with carmen*, (2008), pp. 1–5.

[4] R. M. Savola, A. Juhola, I. Uusitalo, Towards wider cloud service applicability by security, privacy and trust measurements. *International Conference on Application of Information and Communication Technologies (AICT)*, (Oct., 2010), pp. 1–6.

[5] M.-E. Begin, An egee comparative study: Grids and clouds – evolution or revolution. *EGEE III project Report*, vol. 30 (2008).

[6] B. Rochwerger, D. Breitgand, E. Levy, A. Galis, K. Nagin, I. M. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres, M.Benyehuda, W. Emmerich, F. Galan, The Reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*, vol. 53, no. 4 (July, 2009), pp. 1–11.

[8]"Implementing QoS Solutions for H.323 Videoconferencing over IP", *Cisco Systems Technical Whitepaper Document Id: 21662*, 2007.

[9] P. Calyam, M. Haffner, E. Ekici, C.-G. Lee, "Measuring Interaction QoE in Internet Videoconferencing", *Proc. of IFIP/IEEE MMNS*, 2007.

[10] S. Winkler, "Digital Video Quality: Vision Models and Metrics", *John Wiley and Sons Publication*, 2005.

Floriana GEREA is Security Analyst at Raiffeisen Bank. She has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2007. Currently, she is a PhD student in the field of Economic Informatics at the Academy of Economic Studies. She is co-author of one book ("Telecomunicatii si Tehnologia bazelor de date"), 6

published articles, and 2 scientific papers. Her fields of interest include: Linux, Clusters, VoIP and Cloud Computing.