# SECURITY SOLUTIONS FOR CLOUD COMPUTING

Teză destinată obţinerii
titlului ştiinţific de doctor inginer
la
Universitatea "Politehnica" din Timişoara
în domeniul INGINERIA SISTEMELOR
de către

**Ing. Alina Mădălina LONEA**

| | |
|---|---|
| Conducători ştiinţifici: | prof.univ.dr.ing. Octavian PROŞTEAN |
| | prof. Huaglory TIANFIELD, PhD |
| Referenţi ştiinţifici: | prof.univ.dr.ing. Mihail ABRUDEAN |
| | prof.univ.dr. Dana PETCU |
| | prof.univ.dr.ing. Vladimir Ioan CREŢU |

Ziua susţinerii tezei: 22 Octombrie 2012

Seriile Teze de doctorat ale UPT sunt:

1. Automatică
2. Chimie
3. Energetică
4. Ingineria Chimică
5. Inginerie Civilă
6. Inginerie Electrică
7. Inginerie Electronică şi Telecomunicaţii
8. Inginerie Industrială
9. Inginerie Mecanică
10. Ştiinţa Calculatoarelor
11. Ştiinţa şi Ingineria Materialelor

Universitatea „Politehnica” din Timişoara a iniţiat seriile de mai sus în scopul diseminării expertizei, cunoştinţelor şi rezultatelor cercetărilor întreprinse în cadrul şcolii doctorale a universităţii. Seriile conţin, potrivit H.B.Ex.S Nr. 14 / 14.07.2006, tezele de doctorat susţinute în universitate începând cu 1 octombrie 2006.



România, 300159 Timişoara, Bd. Republicii 9,
tel. 0256 403823, fax. 0256 403221
e-mail: editura@edipol.upt.ro

# Acknowledgement

This PhD thesis is the result of my scientific work in the Department of Automation and Applied Informatics, Faculty of Automation and Computers at "Politehnica" University of Timisoara.

I would like take this opportunity to show my gratitude to those who made this thesis possible.

I would like to express my gratitude to my supervisor Prof.dr.eng.Octavian Proştean for all his support, guidance, patience and good advice, throughout my PhD.

I also thank to Professor Huaglory Tianfield, who accepted to supervise me during my research stage at Glasgow Caledonian University and who had continued to be my supervisor after my mobility there. I am truly grateful to him for his invaluable assistance, support and guidance.

I would also like to thank to Professor Tom Buggy from Glasgow Caledonian University, who accepted me as a visiting PhD student at Glasgow Caledonian University.

I would also like to thank my family for their endless support and encouragement.

Finally, I would like to acknowledge the strategic grant POSDRU/88/1.5/S/50783.

Timişoara, October 2012 Alina Mădălina Lonea

To my family

Lonea, Alina Mădălina

**Security Solutions for Cloud Computing**

Teze de doctorat ale UPT, Seria 12, Nr. 5, Editura Politehnica, 2012, 120 pagini, 40 figuri, 18 tabele.

ISSN: 2068-7990

ISBN: 978-606-554-548-9

Cuvinte cheie: Cloud Computing, private cloud, security, Identity Access Management, Authentication, Text-image based authentication, recall based, DDoS attacks, Eucalyptus, Dempster-Shafer Theory (DST), Intrusion Detection Systems (IDSs), Fault-tree analysis, Snort.

Rezumat,
Teza de doctorat prezintă noi soluţii de securitate aplicate în sistemele distribuite de tip Cloud Computing. Rezultatele de cercetare se referă la îmbunătăţirea securizării identităţii utilizatorilor, a informaţiei şi a infrastructurii, evidenţiindu-se trei contribuţii principale:

- proiectarea unei soluţii arhitecturale de securitate pentru cloud computing, propunându-se o structură bazată pe o descompunere multi-nivel (nivel 1-4);
- definirea, proiectarea şi analiza unei soluţii noi de autentificare pentru cloud computing, care combină tehnica propusă de autentificare hibridă text-imagine cu soluţia existentă de autentificare;
- proiectarea, implementarea, testarea şi validarea unei topologii cloud de sisteme de detectare a intruziunilor (IDS Cloud Topology), având ca şi obiectiv detectarea şi analiza atacurilor Distributed Denial of Service (DDoS) în sistemele cloud computing.

# TABLE OF CONTENTS

TABLE OF CONTENTS ..... 11
ACRONYMS ..... 13
LIST OF FIGURES ..... 15
LIST OF TABLES ..... 16
ABSTRACT ..... 17
1. INTRODUCTION ..... 18
1.1. Cloud Computing: Background ..... 18
1.1.1. Cloud Computing Characteristics ..... 14
1.1.2. Cloud Services ..... 15
1.1.3. Deployment Models ..... 15
1.1.4. Enterprises Migration to Cloud Services ..... 16
1.2. Motivation ..... 23
1.3. Thesis Goals ..... 25
1.4. Thesis Outline ..... 26
2. CLOUD COMPUTING SECURITY ..... 28
2.1. Security Management in Cloud Computing ..... 28
2.2. Security Issues In Cloud Computing ..... 29
2.2.1. Applications Security Issues ..... 29
2.2.2. Virtualization Security Issues ..... 33
2.3. Cloud security solutions ..... 35
2.3.1. Identity Security ..... 35
2.3.2. Information Security ..... 37
2.3.3. Infrastructure Security ..... 38
2.4. Conclusions ..... 39
3. ARCHITECTURAL SOLUTION OF SECURITY FOR CLOUD COMPUTING ..... 41
3.1. Identity and Access Management Requirements for Cloud Computing ..... 41
3.2. Current Cloud IAM solutions ..... 42
3.3. Design of the Architectural Solution of Security for Cloud Computing ..... 43
3.4. Cloud IAM Protocols ..... 47
*3.4.1.* Standards for Provisioning/De-provisioning identities ..... 47
*3.4.2.* Overview of Identity federation standards ..... 48
*3.4.3.* Solutions for authentication requirement ..... 51
*3.4.4.* Standards for authorization requirement ..... 51

3.5. Related work ..... 53
3.6. Conclusions ..... 55
4. AN HYBRID TEXT-IMAGE BASED AUTHENTICATION FOR CLOUD SERVICES ..... 56
4.1. Knowledge-based authentication techniques ..... 56
4.2. Authentication Solution ..... 58
4.3. Advantage of the authentication solution ..... 61
4.3.1. Solutions for possible attacks ..... 61
4.3.2. Time to register and login ..... 63
4.3.3. System's usability ..... 63
4.4. Conclusions ..... 64
5. PRIVATE CLOUD SET UP USING EUCALYPTUS ..... 65
5.1. Eucalyptus Architecture ..... 65
5.2. Eucalyptus Private Cloud Deployment ..... 66
5.3. Eucalyptus Management Tools ..... 68
5.4. Euca2ools Operations ..... 73
5.5. Problems and Solutions in the Private Cloud Setup ..... 74
5.6. Conclusions ..... 76
6. EXPERIMENTAL RESULTS AND EVALUATION ON DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS IN EUCALYPTUS PRIVATE CLOUD ..... 77
6.1. Dempster-Shafer Theory (DST) ..... 78
6.2. Proposed Solution ..... 79
6.3. Related Work ..... 82
6.3.1. Intrusion Detection Systems (IDS) in Cloud Computing ..... 82
6.3.2. IDS using Dempster-Shafer Theory ..... 84
6.4. Implementation of the Proposed Solution ..... 85
6.5. Generating DDoS Attacks ..... 87
6.6. Results and Evaluation ..... 87
6.7. Conclusions ..... 92
7. CONCLUSIONS ..... 93
7.1. Thesis contributions ..... 95
7.2. Future work ..... 98
BIBLIOGRAPHY ..... 99
LIST OF PUBLICATIONS ..... 116

# ACRONYMS

| | |
|---|---|
| ACID | Analysis Control for Intrusion Detection |
| API | Application Programming Interface |
| AWS | Amazon Web Services |
| BASE | Basic Analysis and Security Engine |
| BCP | Business Continuity Planning |
| bpa | Basic probability assignment |
| BSM | Business Service Management |
| BSP | Business Service Process |
| BSS | Business Suport Services |
| CAA | Cloud Application Architecture |
| CC | Cluster Controller |
| CCMA | Common Cloud Management Interface |
| CFU | Cloud Fusion Unit |
| CLC | Cloud Controller |
| CLI | Command Line Interface |
| CPA | Cloud Platform Architecture |
| CPU | Central Processing Unit |
| CRM | Customer Relationship Management |
| CSA | Cloud Security Alliance |
| CSP | Cloud Service Provider |
| DMZ | Demilitarized Zone |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| DR | Detection Rate |
| DRP | Disaster Recovery Planning |
| DST | Dempster-Shafer Theory |
| EBS | Elastic Block Storage |
| ECC | Eucalyptus Community Cloud |
| EC2 | Elastic Cloud Computing |
| ENISA | European Network and Information Security Agency |
| ERP | Enterprise Resource Planning |
| EUCALYPTUS | Elastic Utility Computing Architecture Linking Your Programs To Useful Systems |
| FN | False Negative |
| FP | False Positive |
| FTA | Fault-Tree Analysis |
| GUI | Graphical User Interface |
| HR | Human Resources |
| HTTP | Hypertext Transfer Protocol |
| IaaS | Infrastructure–as-a-Service |
| IAM | Identity and Access Management |
| IAMaaS | Identity and Access Management-as-a-Service |
| ICMP | Internet Control Message Protocol |
| ICT | Information and Communication Technology |
| IDaaS | Identity as a Service |
| IDC | International Data Corporation |
| IdM | Identity Management |
| IDMEF | Intrusion Detection Message Exchange |
| IdP | Identity Provider |

| | |
|---|---|
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IT | Information Technology |
| JSON | JavaScript Object Notation |
| KMS | Key Management Service |
| KVM | Kernel Virtual Machine |
| LDAP | Lightweight Directory Access Protocol |
| NC | Node Controller |
| NIDS | Network based Intrusion Detection System |
| NIST | National Institute of Standards and Technology |
| OASIS | Advancing Open Standards for the Information Security |
| OS | Operating System |
| OSS | Operational Support Services |
| PaaS | Platform-as-a-Service |
| PAE | Physical Address Extension |
| PAP | Policy Administration Point |
| PDP | Policy Decision Point |
| PEP | Policy Enforcement Point |
| PIP | Policy Information Point |
| PSTC | Provisioning Services Technical Committee |
| PSP | Provisioning Service Point |
| PST | Provisioning Service Target |
| RA | Requesting Authority |
| REST | Representational State Transfer |
| SaaS | Software-as-a-Service |
| SAML | Security Assertions Markup Language |
| SC | Storage Controller |
| SCIM | Simple Cloud Identity Management |
| SLA | Service Level Agreement |
| SME | Small and Medium sized Enterprise |
| SOA | Service Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| SP | Service Provider |
| SPML | Service Provisioning Markup Language |
| SSL | Secure Socket Layer |
| SSO | Single Sign-On |
| SSTC | Security Services Technical Commitee |
| S3 | Simple Storage Service |
| TCP | Transfer Control Protocol |
| TCP SYN | Transfer Control Protocol Synchronize |
| TFN | Tribe Flood Network |
| TN | True Negative |
| TP | True Positive |
| UDDI | Universal Discovery, Description, Integration |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VM | Virtual Machine |
| VMM | Virtual Machine Monitor |
| VMs-based IDS | Virtual Machines based Intrusion Detection System |
| VPN | Virtual Private Network |
| WSDL | Web Services description Languages |
| WS-Security | Web Services Security |
| XACML | Extensible Access Control Markup Language |
| XCP | Xen Cloud Platform |
| XML | Extensible Markup Language |

# LIST OF FIGURES

Fig. 1.1. NIST Cloud Computing Definition ..... 14
Fig. 1.2. The management process of enterprise's migration to IaaS [Lon+12a] ..... 17
Fig. 1.3. Choosing the Cloud Service Provider [Lon+12a] ..... 20
Fig. 1.4. Typical Service Level Agreement content [Lon+12a] ..... 22
Fig. 1.5. Results of IDC survey ranking security challenges ..... 24
Fig. 1.6. Principal Elements for Securing the Cloud [RSA09] ..... 25
Fig. 2.1. Web browser relationships [Lon+13] ..... 31
Fig. 2.2. XSS Attack into the Amazon EC2 API [Ela11], [Lon+13] ..... 32
Fig. 2.3. Command injection attack into Amazon EC2 API [Ela11], [Lon+13] ..... 33
Fig. 2.4. Identity Security Stack ..... 36
Fig. 2.5. Information Security Stack ..... 38
Fig. 2.6. Infrastructure Security Stack ..... 39
Fig. 3.1. Layer 1 of the Architectural Security Solution in Cloud Computing [Lon+11] ..... 44
Fig. 3.2. A detailed view of Layer 1 ..... 44
Fig. 3.3. Layer 2 of the Architectural Security Solution in Cloud Computing ..... 45
Fig. 3.4. Layer 3 of the Architectural Security Solution in Cloud Computing [Lon+11] ..... 46
Fig. 3.5. Layer 4 of the Architectural Security Solution in Cloud Computing [Lon+11] ..... 46
Fig. 3.6. SPML System Elements adapted from [OAS03a], [Lon+13] ..... 48
Fig. 3.7. Single Sign-On [OAS05a], [Lon+13] ..... 50
Fig. 3.8. OAuth token exchange [Lon+13] ..... 52
Fig. 3.9. The content of a XACML policy [Lon+13] ..... 53
Fig. 3.10. The architectural/usage model of XACML [Nor09], [Lon+13] ..... 53
Fig. 4.1. The Current Cloud Computing Authentication Solution [Pop+12] ..... 58
Fig. 4.2. Proposed Cloud Computing Authentication Solution [Pop+12] ..... 59
Fig. 4.3. Image Space ..... 59
Fig. 4.4. Individual image set and Password image set ..... 60
Fig. 4.5. Random locations of the individual image set [Pop+12] ..... 60
Fig. 4.6. Authentication form ..... 60
Fig. 5.1. Eucalyptus Architecture [Euc12a] ..... 66
Fig. 5.2. Private Cloud Configuration [Lon12] ..... 67
Fig. 5.3. Xen hypervisor configuration [Lon12], [Lon11a] ..... 68
Fig. 5.4. Right Scale Web Interface [Lon11b] ..... 73
Fig. 5.5. Right Scale – Cloud Volumes Attached [Lon11b] ..... 73
Fig. 5.6. Cloud Instances [Lon11b] ..... 73
Fig. 6.1. IDS Cloud Topology [Lon+12c] ..... 80
Fig. 6.2. Bpa's calculation [Lon+12c] ..... 82
Fig. 6.3. VM-based IDS Deployment [Lon+12d] ..... 86
Fig. 6.4. Relationships of the centralization components in Cloud Fusion Unit [Lon+12d] ..... 86
Fig. 6.5. Creating the views of join queries [Lon+12d] ..... 88
Fig. 6.6. Mass Assignments in DST [Lon+12d] ..... 90

# LIST OF TABLES

Table 2.1. Applications threats and mitigation techniques [Lon+13] ..... 30
Table 2.2. Virtualization threats and mitigation techniques [Lon+13] ..... 34
Table 3.1. Comparison between the Identity Federation standards [Lon+13] ..... 48
Table 5.1. Details of Eucalyptus private cloud [Lon12] ..... 66
Table 5.2. Cloud Systems Configuration [Lon12] ..... 67
Table 5.3. Euca2ools evaluation [Lon+12b] ..... 70
Table 5.4. Typica evaluation [Lon+12b] ..... 70
Table 5.5. Firefox Plugins evaluation [Lon+12b] ..... 71
Table 5.6. Cloud42 Evaluation [Lon+12b] ..... 71
Table 5.7. tAWS Tanacasino Evaluation [Lon+12b] ..... 72
Table 5.8. EC2 Dream Evaluation [Lon+12b] ..... 72
Table 5.9. The lifecycle of a euca2ools image [Lon12] ..... 74
Table 6.1. Boolean truth table for the OR gate ..... 78
Table 6.2. $m_{S1,S2}$ calculation [Lon+12c] ..... 82
Table 6.3. Snort Default Classifications [Sou11] ..... 89
Table 6.4. Bpa's calculation [Lon+12d] ..... 91
Table 6.5. Results of Dempster's combination rule [Lon+12d] ..... 91
Table 6.6. Evaluation metrics [Lon+12d] ..... 92

# ABSTRACT

The evolution of Cloud Computing marks the improvement of Information Technology (IT), because cloud services become a computing utility that facilitates our daily life.

The main purpose of this thesis is to contribute at the security improvement of cloud computing services. At the same time, the thesis presents a complex study that reveals the migration of enterprises resources to the cloud based services. The migration process was designed in order to analyze all the involved challenges, among which for the security issues the thesis will provide innovative solutions. Another motivation for this work was also presented in terms of the security review for cloud computing, which reveals that cloud computing is a technology with emerged challenges in terms of securing the identity, securing the information and securing the infrastructure.

Furthermore, the thesis introduces an architectural solution of security for cloud computing which is based on the security components of cloud computing. The main objective of the architectural solution of security is to secure the user's identities of cloud services. In this sense, an important element of the architectural security solution is the cloud Identity and Access Management (IAM) gateway.

Providing confidential information through Internet to Cloud Service Providers becomes ubiquitous and in the same time is becoming uncertain regarding the integrity, confidentiality and availability of the data. The solution for delivering confidentiality of data is to assure a proper authentication technique for cloud services. Whereas the current authentication system for cloud services relies on password based authentication the proposed solution focuses on improving the knowledge-based authentication in cloud environment. Therefore, the novel authentication system for cloud computing, that combines the proposed hybrid text-image authentication technique with the existing cloud authentication solution is presented. The proposed improvement addresses a hybrid text-image solution, which is an extension of the two level security approach of the current authentication solution in cloud computing. The performance of the proposed solution is expressed in terms of security and usability.

Moreover, this thesis is focused on detecting and analyzing the Distributed Denial of Service (DDoS) attacks in cloud computing environments. This type of attacks is often the source of cloud services disruptions. The proposed solution is to combine the evidences obtained from Intrusion Detection Systems (IDSs) deployed in the virtual machines (VMs) of the cloud systems with a data fusion methodology in the front-end. Specifically, when the attacks appear, the VM-based IDS will yield alerts, which will be stored into the Mysql database placed within the Cloud Fusion Unit (CFU) of the front-end server. In this context, a solution for quantitatively analyzing the alerts generated by the IDSs is proposed, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for the mentioned flooding attacks. At the last step the solution uses the Dempster's combination rule to fuse evidence from multiple independent sources. The thesis aims to evaluate the experimental results of the proposed solution. The experiments are performed in a private cloud model deployed using Eucalyptus open-source. After a set of DDoS attacks are launched against the VMs-based IDS, all the alerts collected from the VMs-based IDS are analyzed.

# 1. INTRODUCTION

## 1.1. Cloud Computing: Background

The evolution of Cloud Computing technology marks the improvement of Information Technology (IT), because Cloud services become a computing utility facilitating our daily life.

Cloud Computing is a technology that aims to provide on-demand scalable services over the Internet via Cloud vendors to multi-tenant organizations. Cloud Computing is defined by the National Institute of Standards and Technology (NIST) as *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [Mel+09].

Cloud Computing appears at the end of 2007 and it involves several computing paradigms like: virtualization, Grid Computing, cluster, Service Oriented Architecture (SOA) and web services, utility computing [Wan+08], [Gon+10]. A study including the comparison between Cloud Computing and these related technologies is presented in [Lon12].

Virtualization is considered the basis in cloud computing environment in order to efficiently utilize its physical resources (i.e. memory, CPU, I/O and Operating Systems - OSs) [Wan+08], [Xen12]. This capability provided by the virtualization layer allows multiple operating systems to action as guest operating systems within a host operating system. One of the following software can be utilized in order to make possible this capability: an installed application into the host OS (e.g. VMware Player, Oracle VirtualBox, ACE) or a software called hypervisor or Virtual Machine Monitor (VMM), which has to be installed directly to the hardware resources (e.g. Xen, KVM – Kernel Virtual Machine) [Wan+08], [Xen12]. Even if virtualization is an important element of cloud computing, there are several differences between cloud computing and virtualization. First, the fact that the workload is statically allocated differentiate virtualization from cloud computing which is based on dynamic allocation the workload using an Application Programming Interface (API) call [Pem10]. The dynamic allocation of workload is possible because of the elasticity characteristic of cloud computing, compared with the resource limits of virtualization [Wil11]. Furthermore, location is a distinctive element between cloud computing and virtualization [Wil11]. While, location of cloud computing can be seen as either on-premise if it is the case of private cloud, but in most of the cases is off-premise (hosted by a 3$^{rd}$ party), virtualization offers on-premise location [Wil11]. Also, cloud computing provides the advantage of location independence that virtualization technology does not [Wil11], [Lon12].

A different technology considered the basis in cloud computing is *Grid Computing*. At first sight, Grid Computing and Cloud Computing are similar, because both of them guiding us at reducing the cost of computing, increasing reliability and flexibility by providing resources on-demand [Fos+08], [Rin+09]. But it does not have to overlook that Grid computing is the backbone of cloud computing, with its support infrastructure. Cloud Computing followed the example of Grid computing,

which provides storage and compute resources. As a next step in technology, cloud computing comes with economy aspects in delivering more abstract resources and services [Fos+08],[Rin+09]. The business model of cloud refers to delivering the services over the Internet via a pay-as-you-go formula. As compared to the cloud-based business model, the business model of grid computing is project-oriented [Gon+10], [Buy+09], where organizations which adopt it are sharing the resources in a collaborative manner with other companies which are in the grid model. Grid is a virtual organization with advanced services, where distributed individuals and/or institutions share files and the most important thing: they have direct access to computers, software, data and other resources. This access is possible using condition sharing strategies that realize an organizational process, for users and providers of the resources [Mag+09], [Fos02]. Another feature that makes difference between Grid and Cloud is that the access for a resource in Grid could be delayed, because it means that the resource was allocated to other user and the requesting user should wait until the resource will be available again. This delayed allocation does not happen in the cloud environment, users receiving the resources on-demand. Wang and von Laszewski (2008) [Wan+08] highlight another difference between cloud computing and grid computing, related with the user-centric interfaces of cloud computing, that ensure for its users an easy to work environment compared with the Grid resources and services, which are accessed with difficulty by grid users because they are forced to learn new Grid commands and APIs [Lon12].

Besides the characteristics of Grid, cloud computing holds also the characteristics of *cluster computing*, that provides for its users the resources within a single administrative domain [Gon+10]. This is justified by the fact that cloud computing environment is composed from high-end computers (e.g. clusters, servers) as Grid is [Gon+10], [Lon12]. However, cloud computing is different than cluster computing. Cluster computing is mainly used for load balancing and providing high availability, while cloud computing is used for providing services. Moreover, cloud computing is distributed located while cluster computing has the same physical location. Also, the components of cluster computing are tightly coupled, while the layers of cloud computing are loosely coupled [Ben+10].

Furthermore, *Service Oriented Architecture (SOA) and Web Services* are utilized in cloud computing, because these services computing contribute at the automation of business processes using IT services [Buy+09], [Lon12]. SOA is a collection of services, which provides the interaction between distributed systems by communicating and exchanging the data [Buy+09], [Sha+08], [Rit+10], [Ger10], [Lon12]. Unlike SOA which delivers services from applications to other programs, Cloud Computing is focused on delivering cloud services to customers. The cloud end-users access the virtual resources and computing assets, using a framework provided by SOA [Rit+10], [Lon12]. Nevertheless, SOA and cloud computing are sharing the loosing coupling feature, but in different context: in SOA the loose coupling is between applications and in cloud computing is between applications and hardware [Ben+10].

In addition with the above comparison, a complete definition is presented in Fig. 1.1. This is the definition provided by NIST [Fur10]. Furthermore, each component of the definition is thoroughly described.

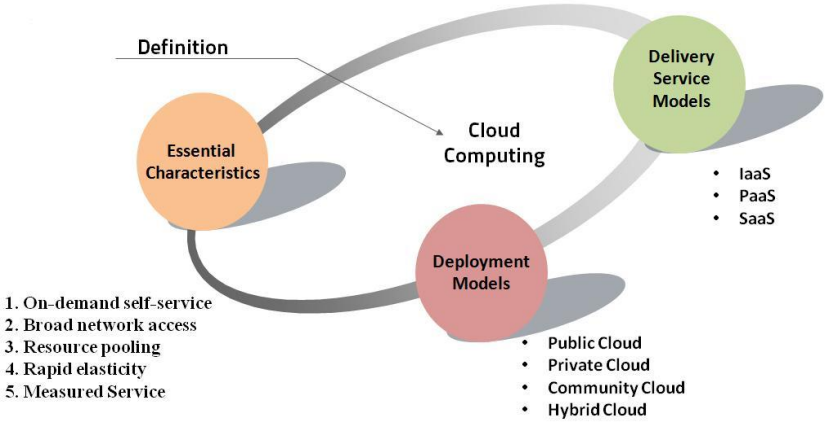


Fig. 1.1. NIST Cloud Computing Definition

The components of the cloud definition was also discussed in our paper [Lon+13] and in the PhD reports [Lon11a], [Lon11b].

### 1.1.1. Cloud Computing Characteristics

According to National Institute of Standards and Technology (NIST), the Cloud concept is defined by five main characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [Fur10], [Lon+13]:

I. *On-demand self-service:* The customers can obtain the desired services from Cloud providers without any interaction with the employees of the Cloud provider, because those services are requested online by them.

II. *Broad network access:* The client devices that consumers use for access the Cloud vary (e.g. mobile phones, laptops and PDAs).

III. *Resource pooling:* The customers in Cloud platform are multi-tenant. Even if the location of the resources is not actually known, the idea is that each of them requires over the Internet the exactly wanted resources (i.e. storage, processing, memory, network, etc), by specifying location at a higher level of abstraction (e.g. country, state or data centre). All together, this directs the reduction of capability's expenses, which is a real benefit for customers.

IV. *Rapid elasticity:* Any quantity of the capabilities could be purchased and released any time, which gives the elasticity feature in Cloud and it makes the clients to feel flexible in their options.

V. *Measured Service* is realized in cloud computing by monitoring, controlling and reporting the usability of the resources. The customers are informed what they have to pay for consuming those resources.

### 1.1.2. Cloud Services

The fundamental delivery models in the cloud architecture are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [Lon+13].

*I.* *Infrastructure-as-a-Service (IaaS)* is an outsourced service, which gives the infrastructure (represented by servers, data centre, network infrastructure) to the customers, who rent them from the cloud providers [Rit+10]. This infrastructure is deployed and used remotely by the clients [Fos+08]. The host infrastructure is complex because of the ranges of components that it owns [Rit+10]: computer hardware (for accomplish the scalability requirement typically is used the grid), computer network (routers, firewalls, load balancing etc.), Internet connectivity, platform virtualization environment, service-level agreements and utility computing billing. Examples of IaaS services are: Amazon Elastic Cloud Computing (Amazon's EC2), Rackspace, Nimbus, Savvis VMware vCloud [VMw+09].

*II.* *Platform-as-a-Service (PaaS)* is a Cloud model that makes available for the customers the Cloud infrastructure, where they should deploy the applications using the programming languages and the tools supported by the provider. The consumers do not need to take control over the infrastructure, but they had to look over the deployed applications [CSA09]. Examples of PaaS services are: Google App Engine, Microsoft Azure and Heroku [Jae+10].

III. *Software-as-a-Service (SaaS)* is a Cloud model which delivers the usage of software through Internet to the clients, who have to pay for the applications [Rit+10], but they do not have to take care of the troubles that came with the installation and maintenance of the software and with the management and with the control of the Cloud infrastructure [CSA09]. According to Jon Williams, the Chief Technology Officer of Kaplan Test Prep and Admissions, SaaS is another advantage that is adopted by many customers because of its purpose: *"I love the fact that I don't need to deal with servers, staging, version maintenance, security, and performance"*. Examples of SaaS services are: Salesforce.com, Google Apps, IBM Lotus Live, NetSuite [CPN10].

### 1.1.3. Deployment Models

There are four deployment models for Cloud services [CSA09], [Lon+13]:

*I.* *Public Cloud* – could be accessed by multiple organizations, because of the multi-tenant characteristic of Cloud. The services are delivered by the Cloud provider through Internet.

*II.* *Private Cloud* **-** unlike public clouds, the private models are owned and used by a single organization, which decrease the security exposures [Clo10]. There are two types of private cloud: *on-premises* (the private cloud being self-hosted) and *off-premises* (the private cloud being hosted by a third-party organization). Additionally, the management process of the private cloud can be on-premises and off-premises and those cloud services can be called private cloud self-managed, respectively private cloud off-managed [CSA09].

*III.* *Community Cloud* **-** it is formed by customers, who have the same field of activity and who are interested to share their infrastructure and services in order to get better results in their businesses. Thus, the cloud infrastructure is common for several organizations.

*IV.* *Hybrid Cloud* **–** put together two or more clouds (private, public or community) in order to mix the features of each delivery model and to obtain a model more reliable and complex.

### 1.1.4. Enterprises Migration to Cloud Services

This subchapter describes the proposed overall process taken by enterprises to manage the migration to Infrastructure as a Service (IaaS), which was published in [Lon+12a].

Information Systems (IS) has a great impact for the business growth of Small and Medium sized Enterprises (SMEs) and it started with personal computers in order to manage the day-to-day operations of the enterprises using the basic applications (i.e. word processing and accounting systems), complex applications (i.e. decisional support systems) and the services produced in the Internet age (i.e. email, web sites, transaction processing systems) [Lev+04]. Today, enterprises adhere to cloud computing technology, which is subject to a continuous development and it is considered the future and the improvement of Information and Communication Technology (ICT). While in 2000 the tendency of Small and Medium sized Enterprises (SMEs) was to migrate to the Enterprise Resource Planning (ERP) solutions [Ada+00], today ICT assists to a trend of SMEs to migrate from the traditional SMEs to the SMEs based cloud. The migration of enterprises to cloud is because of the advantages offered by this technology, defined by Joe Weinmann (2011) [Wei11] as an acronym: *C*ommon, *L*ocation-Independent *O*nline *U*tility on-*D*emand service, on the Axiomatic Cloud Theory. However, simultaneously with the increased number of enterprises that adopt cloud computing, the challenges of enterprises to exploit cloud for their business objectives are growing as well. Thus, companies go through a holistic process in order to manage the implemented cloud services [Lon+12a].

SMEs represent the target group of this study concerned with the outsourcing process to Cloud Service Provider (CSP) considering the fact that the number of SMEs is greater than the number of large organizations, making SMEs the heart of economies worldwide [Sha+10], [Van+11]. SME is a collective term for all micro, small or medium enterprises, which is qualified based on the following characteristics defined by the European Commission Recommendation (2003/361/EC): maximum number of staff (i.e. less than 250), annual turnover (e.g. ≤ 50 million Euros) or an annual balance sheet (e.g. total ≤ 43 million Euros) [Beg+12]. However, these characteristics do not influence the amount and nature of organisational data for SMEs. Despite the fact that SMEs are not sufficiently oriented toward the ICT solutions like the large organizations [Dai09], [Lev+04], SMEs started to explore the movement benefits to cloud services [Beg+12] for both business models (i.e. companies with existing IT infrastructure and start-up companies). Moreover, Devos, Van Landeghem and Deschoolmeester (2012) [Dev+12] state that SME presents insufficient internal IT expertise and needs external IT expertise. Nevertheless, Misra and Mondal (2011) [Mis+11] observed that the start-up SMEs area presents a stronger interest for adopting cloud based services. Van Hoecke, et al. (2011) [Van+11] present their awareness regarding the migration of SMEs with existing IT infrastructure to hybrid cloud and the outsourcing of resources to public clouds for the start-up SMEs [Lon+12a].

Companies can choose from a wide range of cloud services (i.e. Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service), which can be deployed in four deployment models (i.e. private cloud, public cloud, hybrid cloud and community cloud). The selection of the cloud deployment model depends on the size of the organization and its Information Technology (IT) maturity level. While SMEs would rather prefer to outsource their applications within an external cloud provider, the large organizations first take into consideration the solution of having a private cloud and after that, they can decide to migrate their non-critical information (i.e. test and development) to public deployments [CSC11]. Additionally, depending on the IT maturity level of the enterprise, the SMEs will move from the traditional SMEs to the SMEs based cloud in order to gain access to a wide range of advanced IT applications like: Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Human Resources (HR) and Collaboration tools [KPM11]. Sharma, et al. [Sha+10] demonstrates the benefits of using Enterprise Resource Planning (ERP) based cloud services instead of traditional ERP system by SMEs [Lon+12a].

Nonetheless, the aim of the proposed research represents a qualitative analysis of the overall process taken by SMEs to manage the migration of their applications to Infrastructure-as-a-Service (IaaS). We conducted a literature analysis using papers released both by academic and practitioner bodies, in order to respond to the following two research questions: What are the steps involved in the migration process of the SMEs to cloud services? What are the stages required by each step of the outsourcing process? In this sense we produced a theoretical process, which includes a collection of the following interrelated activities: data analysis step, decision making step, migration step and management step. In an IaaS cloud service, the CSP supports the hardware related issues, whilst the software related issues should be identified by enterprises that want to migrate to cloud [Lon+12a].

From consumer perspectives, the overall process taken by enterprises to manage the IaaS cloud services includes a collection of the following interrelated activities: data analysis step, decision making step, migration step and management step. Thus, Fig. 1.2 encompasses the proposed overall process and then each step is discussed separately [Lon+12a].

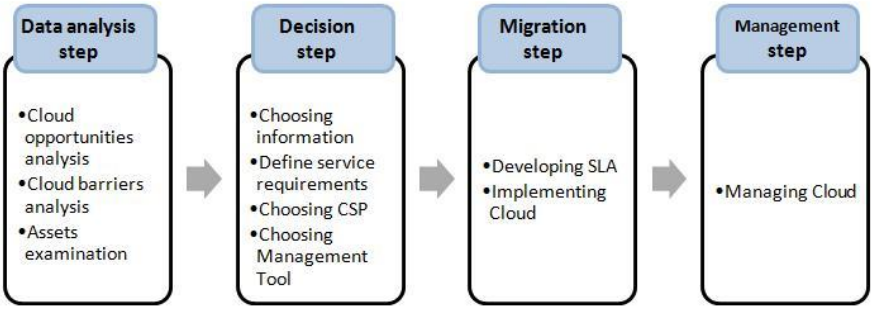


Fig. 1.2. The management process of enterprise's migration to IaaS [Lon+12a]

### 1.1.4.1. Data analysis step

Data analysis constitutes the initial step of the overall process taken by organizations to manage the migration to IaaS and it comprises: the analysis of cloud migration opportunities, the study of cloud adoption barriers and the examination of current infrastructure used by the organization. In this process, enterprises have to consider both the assessment of risks and rewards even if an analysis of costs produced by implementing cloud services should be realized [Lon+12a].

#### 1. Cloud rewards analysis

The rewards of enterprises to migrate to cloud services are based on three major categories: technical benefits, financial benefit and organizational growth.

The *technical benefits* are represented by the five cloud computing characteristics described in section 1.1.1 of this chapter. These five features of cloud computing give more flexibility to companies, which will obtain and release rapidly on-demand the desired cloud services using a broad types of devices from a pool of cloud resources via a pay-as-you-go formula. It was shown in [Mar+11] and [Van+11], that the usage of cloud services by enterprises depends on the amount of the workload which is not the same every time and it is closely related with the months of the year and the time of the day [Lon+12a].

Another cloud opportunity that enterprises should identify is the *financial benefit* [Kha+11], [KPM11]. The reduction of capability's expenses is directed by the resource pooling cloud characteristic, in collaboration with the elasticity capability of cloud providers, which optimize the cost usages. In addition, the cost efficiency of cloud utilization is proved also by a case study realized by Khajeh-Hosseini, Greenwood and Sommerville (2010) [Kha+10a], which calculates the system infrastructure costs involved over five year period for a company that maintain and provides IT solutions for the Oil & Gas industry. In this case study it was demonstrated that the costs of utilizing Amazon EC2 cloud service are smaller than the costs of utilizing the traditional IT system and the company has the advantage of rapid elasticity feature of cloud and the enterprise's in-house hosting costs are minimizing as well (e.g. electricity, cooling, off-site tape archiving). Thus, cloud computing records also a huge *energy savings* together with the cost benefit [Mar+11], [Van+11]. The IT investment for SMEs using cloud services is also reduced by the manageability of IT infrastructure of cloud providers which replace the work of IT support team provided by the in-house SMEs [KPM11]. SME based cloud achieves also financial growth by changing the responsibility for the upgrades and compliance of the applications, which will be the task of the cloud providers [KPM11], [Lon+12a].

Furthermore, another cloud opportunity should be reflected on. This is the *organizational growth* of the enterprises, which will be realized by facilitating the sales and marketing department to create new products/services [Kha+10a], [Lon+12a].

#### 2. Cloud risks analysis

Companies that want to migrate to cloud services have also to identify the cloud adoption risks and to consider how to manage the cloud adoption barriers. The major concerns of enterprises are the *security risks* implied by the act of embedding their resources within the cloud computing environment [Rit+10]. Hence, *migration*

*and integration* phases of existing enterprise application within the IaaS cloud services, should be deployed following a *business migration plan*, respectively a *business disruption plan* for the case that the migration process is causing the disruption of the business flow. All business managers, IT managers and IT vendors should cooperate in order to implement the business migration, respectively the business disruption plans [Sau10]. Disaster recovery solves handling the detection and prevention of possible incidents and provides a Business Continuity Planning (BCP) which enhances the future growth of enterprises [CSA09], [CSC11]. Although business migration plan, respectively business disruption plan cover a major area of security measures, *encryption and key management* usage in cloud computing is recognized as a core mechanism to protect resources (i.e. data in transit over networks, data at rest and data on backup media) [CSA09]. Even though the data is encrypted and a BCP exists, the measures inspected for securing the enterprise's data are not sufficient for securing the cloud services and *Identity and Access Management (IAM)* branch has to be considered, which secures the user identity of cloud computing services [RSA09], [CSA09], [Lon+12a].

Beside security, *data governance* for moving to cloud should comply with the specific enterprise's regulatory requirements (e.g. physical location of data, data breach, personal data privacy, data destruction, intellectual property, information ownership, law enforcement access, service availability) [CSC11]. Hence, the health and financial sectors are distinguished with many regulatory restriction of moving their data to cloud [Kha+10b]. Cloud Security Alliance (CSA) (2009) [CSA09] recommends the ISO/IEC 27001/ 27002 certifications for certifying the information security management systems of providers, respectively the SAS 70 Type II for providing a reference for auditors. However, the applicability of data governance for SMEs sector should be increased, at the moment being poorly served [Beg+12], [Lon+12a].

Additionally, at the stage when the company think to adopt cloud services, its employees are not prepared to deal with the cloud services. Thus, *organizational issues* are other challenges that should be perceived by enterprises [Hei+10], which will have to settle on the type of training activity: *internal* (i.e. by training their personal to use the cloud services) or *external* (i.e. by receiving temporarily or permanent external services) [CSC11]. In this context, specific training should be realized in this area and in this way the employees will be aware about the changes produced by cloud transition and it will reduce their fake understanding of losing their jobs [Sau10]. Just the IT departments concerned only with the hardware and network support will suffer scaling down the number of jobs inside of those IT departments [Kha+10a]. Thus, this is another solution to manage the challenges that comes with the changes produced by cloud on the IT business department [Sau10]. Consequently with this organizational change produced by the cloud migration, the job satisfaction of support engineers, sales & marketing staff and customer care staff is shrinking, because the technical role of support engineers is switching to reporting issues and the satisfaction of sales and marketing roles, respectively the satisfaction of customer care depend upon the cloud based services [Kha+10a], [Lon+12a].

**3. Assets examination**

Further, the examination of current infrastructure used by the organization is useful because enterprises should know what type of bit architecture (i.e. 32 or 64 bit) have their hardware infrastructure and their operating systems (OSs), where are deployed their application. Additionally, the business applications should be

investigated. This step of identifying these assets is required in order to prepare the migration process to an IaaS service compatible with the current infrastructure of the enterprise [Cis10], [Uni12], [Lon+12a].

#### 1.1.4.2. Decision making step

Decision making step implies the following decisions: what information should be moved into cloud and who will access the information, what Cloud Service Provider (CSP) the organization will choose and how the organization will manage the cloud services. We assumed that the cloud service type was chosen (i.e. IaaS) and the cloud deployment model was selected as well (i.e. public cloud).

**1. Choosing information**

Enterprises should decide what information should be moved into cloud. This decision should be realized based on the cooperation between the following departments: IT department and compliance department. The enterprise's preoccupation will establish a selection criteria of data and application preferred to migrate to cloud services, in order to assure confidentiality, integrity and availability requirements for the assets, based on the infrastructure examination and the cloud risks analysis [CSA09], [CSC11], [Lon+12a].

**2. Define service requirements**

In this sense being aware of the current infrastructure and applications used on the company and being aware about what information should be moved into cloud, the enterprise can define service requirements for IaaS [Uni12], [Lon+12a].

**3. Choosing CSP**

Choosing the right Cloud Service Provider (CSP) for enterprise will depend by the following criteria: cost efficiency, product strengths and market credibility. These three decisive factors were listed by Craig (2012) in the Enterprise Management Application Report in order to emphasize the criteria of evaluating the Application Performance Management of known solutions from the cloud marketplace, with the difference that instead of the market credibility it was used vendor strengths capability which includes a larger area of features. This paper suggests applying these determinants also for choosing the CSP, which will be discussed and evaluated for CSP (Fig. 1.3) [Lon+12a]:

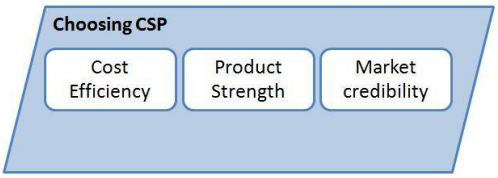


Fig. 1.3. Choosing the Cloud Service Provider [Lon+12a]

- *Cost efficiency* is one of the decisive factors for choosing the CSP. This factor is composed by the following two sub-factors: *cost advantage* and

*deployment & administration*. In terms of *cost advantage*, the modelling tool (from www.shopforcloud.com) described by Khajeh-Hosseini, et al. [Kha+11] could help the costumers to deploy a cloud model by choosing the deployment elements (i.e. server, storage and databases) from a variety list of cloud providers (i.e. Amazon Web Services, Microsoft Azure, Rackspace). After defining the system requirements (i.e. the second stage of the decision making step), enterprises may use this modelling tool in order to deploy the specified requirements. Hence, the tool produces a cost report based on selection of its computational resource usage patterns. This modelling tool is a free web interface, helpful for comparing the pricing schemes around cloud providers. Nevertheless, the cost reports calculates only the costs involved in deployment of a system based infrastructure, where it can be added additional costs (e.g. 3rd party plug-in to monitor costs – Cloudability.com, 3rd party platform to manage cloud resources – Right Scale cloud Management). Additional costs may include license costs, training/consulting services costs, expenditure of time consuming for employees who migrate to cloud services etc [Uni12], [Kha+11], [Lon+12a].
However, besides cost advantage another decisive factor which proves the cost efficiency is the *deployment and administration* analysis (i.e. ease of deployment, support and services, ease of administration) [Lon+12a].

- *Product strength* analysis provides information about the architecture and integration features, respectively about the functionality of CSP [Lon+12a].
- *Market credibility* strengthens the enterprise's decision about choosing the CSP, by analyzing the reputation of CSP on the market [Lon+12a].

**4. Choosing management tools**

Cloud management is a subject approached by researchers in the community and this can be observed by the big number of third party cloud management providers (i.e. Right Scale, enStratus, IMOD Kaavo, CloudWatch, Scalr, Tapin, Cloudkick). These third party cloud management tools are commercial versions, used in special by organizations which want to manage their cloud infrastructure. Thus, enterprises should select one of these commercial versions. In the Enterprise Management Application Report, Craig (2012) [Cra12] emphasizes the criteria of evaluating the Application Performance Management of known solutions from the cloud marketplace. According with Craig (2012) [Cra12] three criteria of selections is considered in their survey: *cost efficiency, product strengths and vendor strengths*. The results of the survey which define the vendor strengths include several categories, namely: vision, strategy, financial strength, research development and market credibility of vendors. For choosing the management tools, this paper proposes the first two criteria of selection: cost efficiency and product strengths from the report provided by Craig (2012) [Cra12] and instead of all vendor strengths elements, only the *market credibility feature* of the vendor will be evaluated [Lon+12a].

- The appraisal of *cost efficiency* should include the following objectives: cost advantage and deployment & administration analysis. Whilst the *cost advantage* is determined by price, licensing and maintenance costs of the management tool, the *deployment and administration* analysis is made to demonstrate the ease of deployment (i.e. time to deploy, packaging requirements, staff training, disruption minimization), a high vendor's customer support and the ease of administration (i.e. ongoing administration, update process, testing/migration) [Lon+12a].

- The investigation of *product strengths* is another selection's criterion of management tools and it should reveal an analysis of architecture and integration categories, respectively the analysis of their functionality [Lon+12a].
- The vendor's *market credibility* feature will review the reputation of the vendors on the cloud marketplace, with the purpose of enhancing the decision, after evaluating the cost efficiency and the product strengths [Lon+12a].

#### 1.1.4.3. Migration step

Migration step is the effective moving stage of enterprise's assets into cloud services. This step includes two activities: developing the Service Level Agreement (SLA) and implementing cloud.

**1. Developing SLA**

The Service Level Agreement (SLA) is a document that should be compulsory done between the cloud provider and the customer, in order to obtain and to maintain a clear aspect over the rights and the responsibilities of each party. This document is relevant for avoiding conflict that could occur during the contract, because it should specify a wide range of issues and the remedies and warranties of them [Kan+09], [Lon+12a].

The content of a typical service level agreement [Kan+09] is representing in Fig. 1.4.


Fig. 1.4. Typical Service Level Agreement content [Lon+12a]

*Definition of Services* is part of the SLA document, where the services are defined and described using detailed information, for create a good understanding over exactly what is being delivered. After the services are defined in SLA, then another section of it (*Performance Management)* should contain aspects of monitoring and measuring the service performance. Including benchmarks, targets and metrics in the requirements of SLA, the both parties of the agreement will be involved in monitoring the performance of the services. A reliable management

arises with the agreement, because relating and discussing the management problems will also be a part of the contract. *Problem Management* embraces the methods for preventing and combating the incidents [Kan+09], [Lon+12a].

The *customer duties and responsibilities* relate the obligations of the cloud's customers, because in the agreement document each party plays its role and have its own responsibility. While the customers have responsibilities also the provider of cloud should have *warranties and remedies* [Kan+09], [Lon+12a].

The SLA also should provide *security* features, creating control access to the information established by the customers and including the client's security policies and procedures that must be performed by suppliers. Beside the security features, both parties should include in the agreement document a *disaster recovery and business continuity* feature, because if an unplanned disaster happen, the customer should have the guaranty of safeguarding the data and the cloud provider should thing to keep its clients, by assuring the disaster recovery plan [Kan+09], [CSC11], [Lon+12a].

The final chapter in a typical service level agreement is the termination section, which should have the following topics: termination at end of initial term; termination for convenience; termination for cause and payments on termination [Kan+09], [Lon+12a].

2. **Implementing Cloud** constitutes the effective migration of the enterprise's information to the cloud service. This step will deploy the system using the CSP capabilities and the system requirements previously defined (i.e. phase 2 of decision making step), by migrating the information (i.e. phase 1 of decision making step) to the cloud service [Lon+12a].

#### 1.1.4.4. Management step

After migrating to cloud services, enterprises will manage the deployed cloud, using two management functions: *business* and *operational*. *Business management function*, also called *administrative group* by DMTF [DMT10b] guarantees the following business supports: customer management, contract management, inventory management, accounting and billing, pricing and ratings, metering and SLA management [DMT10a], [Hog+11], [Lon+12a].

The second management function called *operational management function* or *resource management group* by DMTF (2010b), is handling the provisioning/configuration operations and portability/interoperability operations [Hog+11], [DMT10a], [Lon+12a].

## 1.2. Motivation

One of the main advantages of Cloud Computing is that it offers the possibility to pay only for the services that you use, an idea that was envisaged by John McCarthy in 1961 *"computing may someday be organized as a public utility"*. From this feature of Cloud Computing it results another one: the ability of utilizing the services without having any concerns regarding the installation and maintenance problems. Cloud Computing is extending and in the same time it rises new challenges

regarding securing the data of the customers. Today, there are many providers that deliver cloud services for customers: Amazon Web Services, Microsoft Azure, Google Apps, IBM etc. Also for developers, researchers and testers there are open-source software like: Eucalyptus, OpenNebula, Nimbus and Xen Cloud Platform (XCP) [Che+10], [Lon+13].

Therefore, besides the current utility services (i.e. water, gas, electricity and telephony) [Buy+09], the computing utility services are developed. The main purpose of this thesis is to contribute at the security improvement of cloud computing utility service. At the same time, the thesis starts with a complex study that reveals the management of the enterprise's migration to the cloud based services in order to analyze all the involved challenges, among which for the security issues the thesis will provide innovative solutions.

The cloud security research done till now reveals the necessity for improving the security in the Cloud Computing field [Rit+10], [CSA09], [CPN10], [Jen+09], [Gru+09], [IBM09a], [Kan+09], [And09], [Gru+10], [Ram+10], [Zho+10], [JinJia-Jun10]. Thus, even if the advantages offered by this technology urge the companies to move their data into cloud services, enterprises are concerned about the security risks involved by the outsourcing process into cloud environment [Rit+10]. A survey conducted by International Data Corporation (IDC) in August 2008 confirms that security is the major barrier for the cloud users (Fig. 1.5). In this context, real security incidents were reported in the Cloud Computing systems (e.g. in 2008, there were outages in Amazon Web Services, AppEngine and Gmail) [Arm+09]. The access interruptions of users to the cloud services registers high costs for entire organizations [Per11].


Fig. 1.5. Results of IDC survey ranking security challenges

In [RSA09] the principal elements for securing the cloud are stated (i.e. identities, infrastructure and information) (Fig. 1.6).

These three elements from Fig. 1.6 (i.e. securing the user identity of Cloud Computing services, securing the infrastructure and securing the information) are the objectives of this research. The motivation for this work was also presented in terms of the security overview for cloud computing, that is presented in chapter 2 of this thesis.

In the first part, the thesis focuses on the Identity and Access Management (IAM) security category in the Cloud Computing field, giving the fact that the traditional IAM solutions can not be applied for the cloud computing services. This is because the companies do not have enough control on the cloud service provider's IAM [Jun09] and because the enterprises need to create a compatible identity

infrastructure that must be integrated within many cloud services using a secure linkage [Old11].

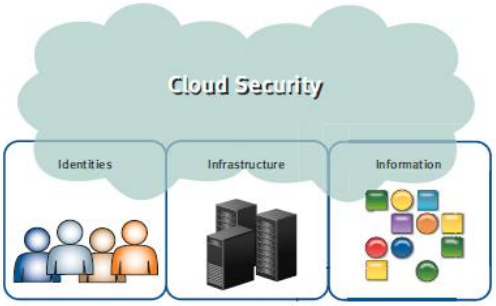


Fig. 1.6. Principal Elements for Securing the Cloud [RSA09]

Furthermore, the current authentication solutions in cloud computing services consists from user text-based authentication (i.e. username and password) and X.509 credentials. The problems with text-based authentication are the recall problems of remembering secure strings for passwords, along with the limitation of being vulnerable to a increased numbers of attacks (i.e. brute force attacks and packet sniffing). Thus, a new solution for authentication in cloud services must increase security, solve the recall problem and meet the usability requirement.

Moreover, the indispensability of securing the information in cloud computing services is proved by the disruptions produced through Denial of Service (DoS) and Distributed Denial of Services (DDoS) attacks in Cloud Service Providers (CSPs), whose service's availability was compromised for hours [Bha+11]. The countermeasures for protecting the cloud services against DoS and DDoS are the Intrusion Detection Systems (IDSs) [Ros+09], but unfortunately IDSs have the disadvantages that they generate massive amount of alerts and produce high false positive rates and high false negative rates [Yu+04], being a burden to analyze the log files generated by IDS sensors.

Thus, the need for assuring the trustworthiness in the Cloud Computing environment motivates the thesis goals.

## 1.3. Thesis Goals

The main goals of this thesis are to bring improvements in the context of securing the user identities, securing the information and securing the infrastructure in cloud computing services.

The first goal is to realize a qualitative analysis of the overall process taken by Small and Medium sized Enterprises (SMEs) to manage the migration of their applications to Infrastructure-as-a-Service (IaaS). This study is necessary in order to identify the involved activities of enterprises to outsource their data within cloud services, along with the engaged security issues.

The second goal is to perform relevant literature survey in the context of cloud computing security, for diagnosing the security management in cloud computing, for realizing an analysis of the cloud attacks with their corresponding

countermeasures and for investigating the challenges in context of identity, infrastructure and information security in cloud computing.

The third goal is to propose an architectural solution of security for cloud computing, considering the case of integrating the IAM of the on-premise private cloud enterprises to the externally cloud services. This architectural security solution is proposing to solve the encountered security challenges. Therefore, it is necessary to analyze the existing Identity and Access Management solutions applied for the Cloud Computing field. Another goal is to create a list of the security requirements within the Identity and Access Management security category of Cloud Computing. The next aim of the thesis includes the evaluation part of the IAM security protocols. Also, the thesis is proposing to evaluate the proposed architectural security solution by comparing it with the related work in the literature.

Furthermore, another objective of the thesis is to enhance the security for authentication requirement of IAM. This objective together with the third objective fulfills one of the main goals of the thesis: to secure the user identities of cloud computing services.

Finally, the next goal is to deploy a private cloud set up with the purpose of realizing experiments for detecting and analyzing Distributed Denial of Service (DDoS) attacks in cloud computing environments. The objective is to propose a solution in order to analyze the alerts generated by the Intrusion Detection Systems (IDSs) of the cloud systems, with the reason of securing the user identities, securing the information and securing the infrastructure in cloud computing.

## 1.4. Thesis Outline

The thesis structure is organised as follows. **Chapter 1** represents the introductory chapter of this thesis and it includes the theoretical background of cloud computing, together with the motivation, goals and the outline of the thesis. The background of cloud computing presented in this chapter provides besides the elements that characterize cloud computing (i.e. delivery service models, deployment models and characteristics), a theoretical overall process taken by enterprises to manage the migration of their applications to the Infrastructure-as-a-Service (IaaS).

Further, **chapter 2** presents the security management, the security issues and the security solutions in Cloud Computing. The security issues are classified from two perspectives: applications security issues and virtualization security issues, which include the threats implied with their mitigation techniques. Moreover, chapter two provides an overview with the security elements: identity, infrastructure and information.

Moreover, **chapter 3** emphasizes the architectural solution of security for cloud computing, which is reffering to the security components of cloud. Also, chapter 3 comprises the analysis of the current Identity and Access Management solutions and the IAM security requirements, in order to introduce the main element of the architectural security solution which is focused on exploring the Identity Access Management as a Service (IAMaaS), also called Cloud IAM Gateway. Additionally, the chapter reports the protocols that should be used in the IAMaaS component and the comparison of the proposed architectural security solution with the related work.

Furthermore, **chapter 4** exhibits a proposed hybrid text-image based authentication for cloud services. This solution covers the authentication requirement of the cloud Identity Access Management (IAM) gateway.

In **chapter 5**, a private cloud set up using Eucalyptus open source is presented. This chapter includes the description of Eucalyptus architecture, the private cloud deployment, the evaluation of the management tools that can be used, the euca2ools operations and the problems and solutions that were met on the private cloud set up.

In addition, the private cloud set up was used for realizing the experiments on detecting Distributed Denial of Service (DDoS) attacks in Eucalyptus private cloud. These experiments are presented in **chapter 6** where a proposed solution that analyze the alerts received from Intrusion Detection Systems (IDSs) is exposed. The solution combines the evidences obtained from Intrusion Detection Systems (IDSs) deployed in the virtual machines (VMs) of the cloud systems with a data fusion methodology in the front-end. This chapter presents the methodologies used in our solution (i.e. Dempster-Shafer theory in 3-valued logic, the fault-tree analysis, the Dempster's combination rule and the IDS in cloud computing), the proposed solution, the implementation of the proposed solution, the generating of DDoS attacks and the results and evaluation.

Finally, **chapter 7** draws the concluding remarks of the thesis, including the thesis contributions and the proposed future work.

# 2. CLOUD COMPUTING SECURITY

This chapter provides an overview of security for cloud computing. The challenges that are analyzed consists of: security management, security issues and security solutions of cloud computing. The identification of the existing issues in terms of security for cloud environment gives the starting points in the development process of this research work.

## 2.1. Security Management in Cloud Computing

Security Management in Cloud Computing is addressed by discussing the problems regarding compliance and audit, the business continuity and disaster recovery plans and the electronic investigations and protective monitoring.

**Compliance and audit**

A critical element of information security is compliance [Sue+09]. The data from cloud computing should comply with applicable local and international regulations, in order to protect the data based on external auditing, regulatory compliance and internal policy compliance by monitoring, establishing and demonstrating the set of controls in several control areas [Red+11]. The policies imposed by regulations depend on the type of data stored. Thus, for storing sensitive information there are specific regulatory requirements like: Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI-DSS), HIPPA (Health Insurance Portability and Accountability Act), Control Objectives for Information and Related Technologies (COBIT) [RSA09], [CSA12a], [Tak+10]. Another regulations imposed are referred to US government (i.e. FISMA- Federal Information Security Management Act, NIST - National Institute of Standards and Technology, FIPS - Federal Information Processing Standard). Also, other regulations from several member states of European Union (EU) are forbidden the migration of its citizen's data outside their borders [IBM09b].

Moreover, a risk that can happen in a cloud service is due to the location's ignorance where data is stored in the cloud. This lack of visibility must determine the clients of the cloud to ask the cloud provider about the specific jurisdictions of the country where data is hosted, because the laws of the countries require storing the data on a physical space inside of the country where the organization activates. Therefore, it is necessary keeping data at required specific laws [Clo10]. It is recommended to achieve compliance with the ISO 27001/27002 standards, which provides security management and controls within the cloud environment [Sha10], [CSA09], [Sue+09]. Another problem that can come with the location of data is that the decryption key and data in some cases must be seen by a third party audit or validation [Kan+09] and the asset management should accomplish access to the virtual and physical assets (hardware, network, software) in case of audit and compliance[Clo10].

**Business Continuity and Disaster recovery plans**

Business Continuity Planning (BCP) is a strategy adopted by organizations for recovering after a non-IT or IT-related disaster [Rit+10]. BCP is approached in the traditional physical security and it remains also relevant to Cloud Computing [CSA09]. In terms of IT-related disaster, the process that deals with the recovering procedures is called Disaster Recovering Planning (DRP) [Rit+10]. Disaster Recovering Planning should be approached by Cloud Service Providers for guaranteeing the information security of customers. Customers should be informed about the measures that cloud service providers plan to realize within the Disaster Recovering Planning, in this sense being accomplished transparency, being minimized the costs and being maximized the benefits [CSA11a]. Thus, customers will be sure that the measures specified in the Disaster Recovering Planning will increase the resilience against any service interruptions, caused by natural or man-made disasters or disruptions [CSA11a].

**Electronic investigations and protective monitoring** means placing the security between the cloud service and cloud user [Lon+13] and it continues to be a security risk for cloud customers who have to trust the monitoring systems deployed by cloud service providers [Kan+09].

## 2.2. Security Issues In Cloud Computing

John Chambers [McM09], Cisco Systems' Chairman and CEO had named security the "nightmare" of Cloud Computing. Security is a serious concern in Cloud with many threats and vulnerabilities. Cloud Computing provides on-demand services to their customers using the Service Oriented Architecture (SOA) model and the virtualization technique. But these came with security issues. The problems caused by the *external attackers* within the cloud computing landscape could be classified as follows: applications security issues and virtualization security issues. The *internal enemies* are employees of the cloud service providers, customers or third party organization of cloud services that have direct access to the services based on a privilege role and exploit their privileged role in order to attack the cloud services [CPN10], [Lon+13].

### 2.2.1. Applications Security Issues

Despite the fact that SOA increases the security concerns in cloud, it is deployed into the cloud because of the collection of services that it posses [Sha+08], [Ger10]. A *Web Service* is a software system which provides interoperability between heterogeneous and distributed systems [Nor09]. Web Services integrate web-based applications using the following standards over the Internet protocol: *XML (Extensible Markup Language)*, *SOAP (Simple Object Access Protocol)*, *WSDL (Web Services Description Languages)* and UDDI *(Universal Discovery, Description, Integration)* [Sac+10]. Unlike the browser-based interaction, in Web services is realized an application-to-application interaction [Dou+07]. While

*XML* is used to tag the data, *SOAP* is used to exchange the XML messages [W3C04]. The standard that describes the available services is *WSDL* and for listing those services is used *UDDI* standard [Sac+10], [Lon+13].

Typically embracing Internet standards through the use of XML-based Web Services (WS), the SOA approach holds the promise of greater IT flexibility and agility by enabling organizations to "publish" their services for the multitudes of potential internal and external service consumers [CA07], [Lon+13].

There are many parallels between Web applications and SOA/WS-based applications, including the fact that both can be deployed on an intranet (for company use), an extranet (for business partners), or even the public Internet (for consumers). The main difference is that the "user" in a SOA world can be another machine talking the language of XML, WSDL and SOAP, as opposed to a person seeing a web page rendered in a browser [CA07], [Lon+13].

The security attributes (i.e. availability, integrity and confidentiality) of cloud services could be affected by attackers. Furthermore, there are two types of security concerns in Cloud applications: wrapping attacks and browser security issues (e.g. account Hijacking, spoofing attacks). These are presented further together with the mitigation techniques for each threat type. So, Table 2.1 summarizes the way we see the web applications threats and mitigation techniques [Lon+13].

Table 2.1. Applications threats and mitigation techniques [Lon+13]

<table>
<tr><th></th><th colspan="2">Threats</th><th>Mitigation techniques</th></tr>
<tr><td rowspan="3">Applications Security Issues</td><td colspan="2">Wrapping attacks</td><td>• XML schema validation and Secure policy validation</td></tr>
<tr><td rowspan="2">Browser security issues</td><td>Account Hijacking</td><td>• Multi-factor authentication<br>• Monitoring solutions<br>• Anomaly detection</td></tr>
<tr><td>Spoofing Attacks</td><td>• Hash service integration check<br>• Filtering techniques<br>• Does not allow dynamic SQL generation</td></tr>
</table>

**Wrapping attack**

In terms of message security, Web Services introduces the WS-Security that came with two elements that are used for SOAP messages in Cloud Computing: *XML Signature* and *XML Encryption* [Wyn10]. *XML Signature* is used in cloud platforms for providing integrity and authentication by signing digitally the XML fragments [Jen+09]. But, XML Signature opens the door to hackers because as McIntosh and Austel discovered, the SOAP message protected by XML Signature could be modified without invalidating the signature [Gru+10]. This is a *XML Signature Element wrapping attack* (*wrapping attack)*, also called *XML rewriting attack*, which could

affect the cloud. Actually, in 2008 Amazon Elastic Cloud Computing (EC2) was vulnerable to the wrapping attacks, which allows access of the intrusion attack in cloud system [Lon+13].

For the wrapping attacks it was discovered the *inline approach* solution, which creates another element called *SOAP Account* in order to keep on it the following SOAP properties [Gru+09]: number of child elements, number of header elements inside the SOAP header, the number of references in each signature and the successor and predecessor of each signed object. The purpose of a new element is to assure the detection of a possible attack, because if a wrapping attack happens then one of these numbers from SOAP element will not be the same with the ones from the SOAP Account element [Lon+13].

Beside the inline approach it was discovered another solution in terms of wrapping attacks, because this one can be broken and the SOAP Account element is not standardized. This alternate solution was the use of *verification* component *as a filter*. But because all these ideas weren't technically matures Gruschka and Iacono [Gru+09] proposed the following: *XML Schema Validation* and *Security Policy Validation*. XML Schema Validation is the right approach that confirms if the incoming message is syntactically correct and came for the unique ID. It also helps to discover earlier the Denial-of-Service attack. Schema will not allow such a vulnerability to happen. In the same time with XML Schema Validation, Security Policy Validation should be done in order to verify if all assertions are fulfilled [Gru+09], [Lon+13].

**Browser security issues**

Browser security issues are related to the existent vulnerabilities on the cloud authentication procedure. The web browser constitutes the Input/Output (I/O) into the cloud service for the cloud customers (Fig. 2.1) [Jen+09], [Lon+13].

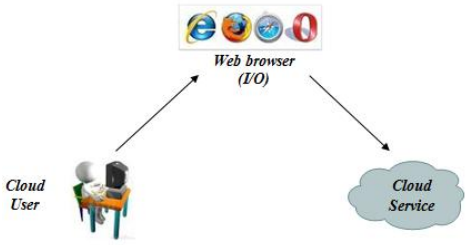


Fig. 2.1. Web browser relationships [Lon+13]

There were attacks into the cloud accounts, threats that are called *Account Hijacking* (pharming, phishing and email-based attacks) [Wre+10]. The corresponding threat is that of redirecting the victims to a fake web page in order to find their username and password [Lon+13].

Therefore in [Jen+09], it is suggested utilizing *SAML* (Security Assertion Markup Language) for providing strong authentication and there were suggested the security of API (Application Programming Interface) for addressing the browser enhancements [Lon+13].

In [CSA10] the recommendations regarding this threat sustain its amplified impact into the cloud environment, by presenting the eavesdropping problems that could compromise the user account and its service instances. Thus, for mitigate the

account hijacking threat there are proposed solutions like: a multi-factor authentication mechanism instead of one-factor authentication, the account credentials transmission between the providers and the clients should be disallowed and detecting illegitimate users using monitoring solutions [CSA10]. The anomaly detection (e.g. analysis of failed and successful logins, unusual time of day and multiple logins) of the user login into the cloud management interface is an alert that the user credentials could be compromised [ENI09]. The apparition of new threats into the cloud system after the Account Hijacking attack was realize, it's also pointed out in [Wre+10], where the Unisys Secure Cloud architecture embraces a "defense in depth" method, based on strong cryptographic authentication and on a detection system of unauthorized access [Lon+13].

***Spoofing attacks***:

**1. Cloud malware injection attack**

The malware injection attack compromises the cloud services by attempting to inject them with malicious service implementation or malicious virtual machine instance. In order to realize such an attack, the enemy will insert its malicious instance into the cloud and then the end-users will be redirected to use that malicious service implementation [Jen+09]. In this way malware injection attacks such as viruses or Trojan horses could be added by intruders into the cloud systems [Jam+11], [Lon+13].

According with Grobauer, Walloschek and Stocka (2011) [Gro+11], the injection attacks attempts to use the cloud services and applications vulnerabilities by using erroneous input by the attacker in order to inject the cloud environment with undesirable consequence for programmers. There are the following types of injection attacks [Gro+11], [Lon+13]:

- *SQL injection* – attacker introduces a malicious SQL code into the input field, in order to realize unwanted actions into the database
- *Cross-site scripting (XSS) injection* - an example of XSS attack (Fig. 2.2) is introducing a script instead of a security group name in the Amazon EC2 API [Ela11]

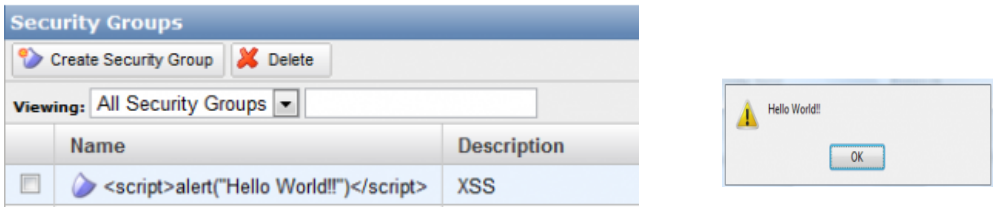


Fig. 2.2. XSS Attack into the Amazon EC2 API [Ela11], [Lon+13]

- *Command injection* – attacker introduces malicious command into the input field, which will cause at unwanted actions into the operating system; for instance, in the Amazon EC2 API the intruder could introduce a malicious command instead of a security group name (Fig. 2.3) [Ela11].

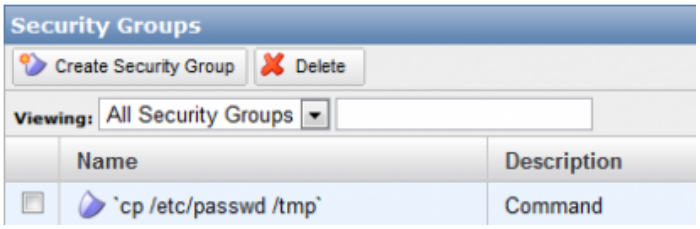


Fig. 2.3. Command injection attack into Amazon EC2 API [Ela11], [Lon+13]

Injection attack is an effective concern in cloud security and the best measure to protect against it is to use *a hash service integrity check*, which will compare the hash value of the original service instance's image with the hash values of the new service instance image [Jen+09]. In [Ela11] is presented their solution for combating these injection attacks: using a third-party detector tool like Elastic Detector [Lon+13]. In addition, Bhadauria, et al. (2011) [Bha+11] suggested two techniques for avoiding the SQL injection attacks: the code should be deployed for not allowing the dynamically generation of SQL and the user input should be controlled using filtering techniques. Moreover, the IBM Tokyo Research Laboratory is working on creating Active Content Filtering technology to protect systems against XSS attacks [IBM,n.d].

**2. Metadata spoofing attacks**

This type of attack could pose troubles for the cloud services by changing the metadata WSDL description. In this way the attacker will obtain confidential information because its consequence will be to achieve data by modifying a service's WSDL. If the attacker changes syntactically the operation of a service to do something else that can be a drawback for the cloud (e.g. change the deleteUser operation to do what the setAdminRights should do). In order to detect these types of attacks a *hash-based integrity verification* of the metadata description should be done [Jen+09], [Lon+13].

### 2.2.2. Virtualization Security Issues

Virtualization is a useful technique for cloud systems, but it does not offer full control of the data availability. In a Cloud environment, the customers can obtain on-demand the service, which is a great advantage for them, but in the same time an illegitimate user can request the cloud service [Jen+09]. The intruder user can rent virtual resources and computing assets. Utilizing virtual machines the possible attacker will try to generate tremendous attack over the cloud system by attempting to make the Cloud services unavailable or by compromising the data and modified it or even loose that data. In Table 2.2 the virtualization threats and their mitigation strategies were summarized [Lon+13].

Table 2.2. Virtualization threats and mitigation techniques [Lon+13]

| | ***Threats*** | ***Mitigation techniques*** |
|---|---|---|
| **Virtualization security issues** | Flooding attacks | • Virtual DMZ (Demilitarized zone)<br>• Intrusion Detection System<br>• Increase bills |
| | Virtual machine template image | • Firewall<br>• Intrusion detection and prevention system |
| | Side channel attack | • Resource monitoring<br>• Strong authentication and access control<br>• Private VLAN clouds |

**Flooding attacks**

Another security issue of the Cloud is to maintain the availability of the services. A real damage for cloud computing could be the flooding attacks (Denial of Service attack), by overloading the cloud network traffic. This makes the cloud services unavailable [Jen+09]. Real cases of flooding attacks were happening in 2008, where the attacks produced outages in Amazon Web Services, AppEngine and Gmail [Arm+09], [Lon+13].

There are two types of Denial-of-Service attack: direct and indirect. When a service from Cloud system is overloaded with nonsense requests, this is called *direct denial-of-service* attack, and in the final this type of attack will conduit at unavailability of that service. Beside this type of attack it is possible that a denial-of-service attack over a service to affect other services that are located in the same server. This is called *indirect denial-of-service attack* or a *target denial-of-service attack* [CPN10], [Jen+09]. The downtime of those services was produced by deficiency of the hypervisor and virtual machines to respond to the fakes requests [CPN10], [Lon+13].

Increasing the bills for Cloud usage was a proposed idea for responding to the flooding attacks. But a better solution for defending against flooding attacks in a cloud platform is to utilize a virtual Demilitarized Zone (DMZ) area in the Cloud infrastructure [Cis+09]. Moreover, Intrusion Detection Systems (IDSs) can be another solution in terms of flooding attacks [Ros+09], [Maz+10], [Lo+10], [Dha+11], [Lee+11], [Lon+13].

**Virtual-machine template images** could produce the spreading of vulnerabilities when the template images are cloned [Gro+11]. Problems can happen when the virtual image is taken from an unreliable source. That image may be as well entrusted, because it could be set to allow attackers (e.g., backdoor access for an attacker). The vulnerability of virtual machines replication produces *data leakage*. Cloning a virtual-machine template image in another host denotes making public certain elements of an operating systems that was meant to be private for a single host. A method to combat a possible attack is to use a firewall and an intrusion detection and prevention system [Tre09], [Lon+13].

**Side channel attack** is a type of attack that obtains information from the VM victim by placing the VM attacker in the same physical space with the victim. After that, the attacker will extract confidential information [Dis,n.d]. As shows in [Ris+09] the cloud-computing environment cloud is affected by side channel attack. Their case study was done using Amazon's EC2 cloud provider, but it could be also applied for Microsoft's Azure or Rackspace's Mosso. The isolation between virtual machines provided by the hypervisor could be broke by the adversary. Thus, there are recommended the following mitigation techniques: resource monitoring and a strong authentication and authorization [CSA10b]. Another countermeasure is to implement private VLAN clouds for each cloud customer in order to avoid the problem attacks if one of the cloud customers is compromised [Cis+09], [Lon+13].

## 2.3. Cloud security solutions

As we can seen from Section 1.3 of Chapter 1, the cloud security realm is consisted of the following three components: identity security, information security and infrastructure security. These three components are in close relationship with the CIA (Confidentiality Integrity and Availability) elements.

With respect to cloud security, Cloud Security Alliance (CSA) and European Network and Information Security Agency (ENISA) provided several guidance and recommendations. Thus, CSA [CSA09] offered a security guidance with 13 domains by structuring them in two major categories: governing in the cloud and operating in the cloud. Another guide provided by CSA in 2010 is about the Identity and Access Management. Further in 2011, CSA [CSA11a] presented a document guide about security as a service in cloud environment describing security for ten categories. Furthermore, an updated version of the security guidance of CSA appeared in 2009 [CSA09] is the version from 2011 [CSA11b]. Moreover, European Network and Information Security Agency (ENISA) [ENI09] suggested a security risk assessment, together with information assurance framework and information assurance requirements.

This section deals with the analysis of the three components of cloud security and it aims to emphasize the tight relation between them.

### 2.3.1. Identity Security

Identity security aims allowing only the authorized users to access the cloud services, in this way being provided the confidentiality and integrity of customer's data and applications in the ecosystem of cloud. The security control of users and infrastructure is correlated with the identity security [CSA09], [RSA09]. The major concerns related with identity security are the achieving of the following identity security requirements: strong authentication, identity provisioning, identity federation and granular authorization [CSA09] (Fig. 2.4).

*Privileged user access* means the data that will be stored in the cloud could be accessed only by authorized users, which are specified by the provider. If the

access to the cloud services is not controlled, then the privileged user access is a security risk. Cloud providers should have established a secure access and technical solutions [CPN10]. The enterprises should encrypt the data before introducing the data into cloud. In the encryption process, knowing the decryption key only by an authorized party from the cloud environment requires keeping the keys on segregated systems in house or with a second provider. The concern of security in cloud is not only the decryption key. The plain text that is transmitted to the cloud provider could be modified by an attacker [CPN10]. The encryption algorithm will vary depending on the clients, who will specify the requirements: what are the data they will want to be encrypted and who will see the data? Depending on their options regarding these two questions, the clients will apply the adequate encryption algorithm [IBM09a], [Lon+13].

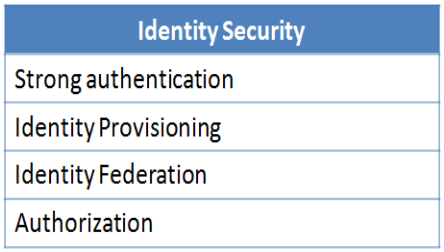


Fig. 2.4. Identity Security Stack

Thus, the objective of handling the identity security can be accomplished by creating an end-to-end identity management between cloud customers and cloud service providers, with the purpose of answering at the following security's challenges [CSA09]:

1. How the identity security control can be realized in order to be adapted for each type of cloud customers (e.g. their own behalf and a member of an organization), for each cloud deployment model and for each delivery service model?
2. How to realize in a secure and timely manner the provisioning and de-provisioning of users within cloud services?
3. Which type of Identity and Access Management (IAM) should be used (e.g. enterprise's on-premise IAM, third-party cloud based IAM and hosted IAM by cloud service provider)?
4. Which authentication mechanism should be used?
5. The same authentication credentials can be used to access multiple cloud systems?
6. Which users will have access to the cloud services? How the access rules will be built?

These are some of the security issues that rise when we think about identity security in cloud. A secure identity system for cloud computing is created by answering the questions above and finding reliable solutions for them.

In this sense, CSA [CSA09] provides guidance for creating stronger authentication and it also introduces the notion of Identity as a Service (IDaaS), which appears to become an IT Service as mobile phones are and as DNS providers deliver reliable and available naming services for customers [Old11].

The requirement of authentication needs a stronger mechanism than the traditional authentication based on an identifier (ID)/ password format [CSA09],

[Oku+10] in order to eliminate the identity theft which threats the current cloud systems [CSA11a]. From the cloud provider perspective, Okuhara, Shiozaki and Suzuki [Oku+10] present the Fujitsu's plans to fortify the standard authentication system of their cloud by using one-time password technique.

Moreover, for using the same authentication credentials in order to access multiple cloud systems is necessary to have a common identity management system for multiple cloud services, based on ID management framework (i.e. SAML – Security Assertions Markup Language, WS-Federation) [CSA09], [Oku+10]. Cloud Security Alliance [CSA09] recommends addressing the identity federation mechanism with respect to identity lifecycle management, authentication methods, token formats and non-repudiation.

### 2.3.2. Information Security

In cloud computing, information security requires protecting the confidentiality and integrity of data in storage, data in transmissions and data in use and safeguarding the data availability. Protecting data in use and data stored in cloud computing means isolating the data (i.e. information and applications), creating business continuity and disaster recovery plans, enabling proper incident handling and forensics and realizing permanent and appropriate auditing and compliance regulations, as well encrypting the data. Furthermore, for protecting the data of customers in transmissions while migrating to cloud services a proper encryption and key management should be identified and the problems regarding interoperability should be solved in order to make possible portability of customer's data among cloud service providers [CSA09] (Fig. 2.5).

In addition, the data security in cloud environment must address the data location, the data segregation and the data disposal. *Data location* can be a security risk. This lack of visibility must determine the clients of the cloud to ask the cloud provider about the specific jurisdictions of the country where data is hosted, because may be they should pay some taxes. Another problem that can come with the location of data is that the decryption key and data in some cases must be seen by a third party audit or validation [Kan+09]. This uncertainly of data location could produce other security risks. The environmental risk is one of them. Considering the region where that is stored, disasters like earthquakes, flooding, and extreme weather, could damage the security of customer data. Also, data location involves macro-economic risks [CPN10], [Lon+13].

*Data segregation* remains a security risk because Cloud Computing is defined by the multi-tenant concept. This means that multiple customers store their data into cloud. Data segregation between Cloud users is required because if the data is not separated, then when an attack happens to a customer from cloud, than all other customers will be affected [Kan+09]. Utilizing virtualization technology, Cloud Computing is exposed to attackers, who will try to downtime the hypervisor of the cloud [CPN10], [Lon+13].

*Moreover, the data Disposal* remains a securiy risk in Cloud Computing. Cloud Computing save the data of the customers for backups, data stores and physical media. Once a customer decides to delete his/her data from the cloud, cloud-based storage could not manage with this because of the multiple copies of the data [CPN10].

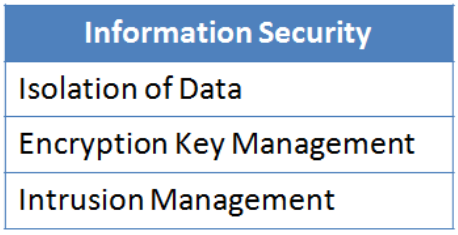


Fig. 2.5. Information Security Stack

**Isolation of data** is necessary because Cloud Computing is defined by the multi-tenant concept, which means that multiple customers store their data into cloud. Data segregation between Cloud users is required because if the data is not separated, then when an attack happens to a cloud customer, than all others customers will be affected [Kan+09]. Isolation of data is realized by securing the virtualization layer of cloud model.

**Encryption key management**

Protecting data in transit, protecting the data at rest and protecting the data in use in the service provider's data centre is achieved with proper encryption techniques which are aligned to suitable key management mechanisms [CSA12b], [IBM09a], [Red+11]. The key lifecycle management of the cryptographic security controls should provide access of customer to data according with policy rules and to revoke the access in case that the user no longer needs access [CSA12b]. Thus, the key management mechanism should also consider the case when the data of a customer is destroyed from cloud storage and to have procedures to destroy that cryptographic key [CSA12b]. Furthermore, the type of the Key Management Service (KMS) depends on the location where the cryptographic key is hosted: on the provider side (i.e. cloud key management Service), on the remote side (i.e. remote key management service) or on the client side (i.e. client side key management) [CSA12b].

**Intrusion Management**

The information in cloud computing can be altered or it can be denied the access of the authorized users. These issues can arise because of the intrusions which attack the cloud system. Thus, the cloud-based intrusions solutions include the analysis of the logging information (i.e. audit logs, error logs, security-specific logs, performance logs etc) and the detection and the protection against malicious activities. Even if security-specific logs (i.e. Intrusion Detection Systems (IDSs)) are investigated or the audit logs are performed, the purpose is to monitor, analyze and notify the logs and the events by Security Information and Event Management (SIEM), in order to remediate an incident if it is notified [CSA11a], [CSA11b].

### 2.3.3. Infrastructure Security

Securing the information in cloud computing is related with securing the physical and virtual infrastructure. The cloud service provider is responsible to

address the security control of physical infrastructure, environmental security control, network security control and virtualization security control, regardless of what delivery service model is used [CSA09], [CSA11b], [Gon+11] (Fig. 2.6).

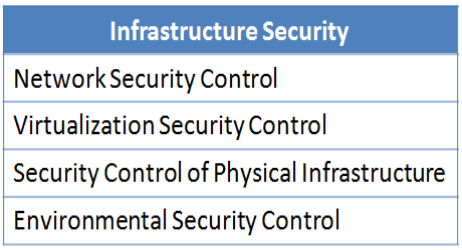


Fig. 2.6. Infrastructure Security Stack

The *security control of physical infrastructure* refers to the existence of host-based firewalls, Host Intrusion Detection Systems (HIDS)/ Host Intrusion Prevention Systems (HIPS), integrity and file/log management, encryption [CSA09].

The *environmental security control* maintains the physical infrastructure in proper conditions with facilities like: power, temperature and humidity controls (Heating, Ventilating and Air Conditioning), space, smoke detectors, fire suppression systems, motion-sensing alarms, secure entry points. Also, the environment is protected against environment hazards (i.e. flood, earthquake, etc) [CSA11b], [ENI09].

Concerning the *virtualization security control*, there should be implemented private Virtual Local Area Network (VLAN) for each cloud customer in order to avoid the problem attacks if one of the cloud customers is compromised. This will isolate the virtual machines which reside on the same physical device. In order to separate the organizational domains of each enterprise, there should be used Access Control List (ACL) for each private VLAN. ACL should also be implemented into the public cloud deployment model. Also a *virtual Demilitarized Zone* (*DMZ)* should be realized for each cloud customer environment, with the intention to create an external virtual place for each customer where the customers could store information that should be available for the others. The internal virtualization of Cloud customer, the private cloud customer, is the place dedicated for sensitive data that must be protected [Cis+09].

As regards *network security control, it* is achieved by firewalls and intrusion detection and prevention systems. These network security devices are the measures to protect against internal and Internet-based Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks. If the cloud infrastructure incurs the damage, then the cloud service providers appeal to the Disaster Recovering Planning [Sub+11], [Kra09], [Red+11].

## 2.4. Conclusions

A literature analysis of security management, security issues and security solutions of Cloud Computing have been presented. This chapter started with a

briefly outline about the security management represented by compliance and audit, business continuity and disaster recovery plans and e-investigations and protective monitoring.

Furthermore, an evaluation of the security issues of cloud computing has been described. The evaluation of the security threats was realized based on the identification of those attacks that compromised several cloud systems, together with the suggested mitigation techniques for each type of the possible attacks. The types of the security threats analyzed in this chapter were grouped according to the following two categories: the application security issues and the virtualization security issues. From the mitigation techniques suggested in this chapter to be used for protecting the cloud systems against security threats, we can observe that the following strategies lead to the establishment of effective secure measures: strong authentication, filtering techniques, Intrusion Detection Systems, isolation of data and monitoring solutions.

Additionally, this chapter provides an overview of the security solutions for cloud computing environment: identity security, information security and infrastructure security. These security solutions must remove the security risks which can destabilize the cloud computing system. Likewise, the security issues are eliminated through the security solutions in terms of identity, information and infrastructure in the cloud computing realm.

The literature review presented in this chapter motivates the next chapters, which outline the advancement in context of identity security, information security and infrastructure security, through the proposed solutions based on Identity Access Management, authentication and intrusion detection.

# 3. ARCHITECTURAL SOLUTION OF SECURITY FOR CLOUD COMPUTING

This chapter introduces an architectural solution of security for cloud computing, which is based on the security components discussed in chapter 2, in which securing the identities of cloud services plays a significant attention.

Identity and Access Management (IAM) for Cloud Computing has a different approach comparing with the traditional IAM, which tended to be centralized. The development of the Cloud Identity-as-a-Service (IDaaS) architectures, which is recommended by Cloud Security Alliance [CSA10b] is producing.

First, this chapter provides a list with the IAM requirements for Cloud Computing. Further, in section 3.2 the background of current cloud IAM solutions is presented, as shown in [Lon+13]. Section 3.3 contains the design of the proposed architectural solution of security for cloud computing, which includes the security cloud IAM gateway (also called *IAMaaS = IAM as a Service),* the network security control and the virtualization security control. Because this chapter focuses on the identity component of cloud security, section 3.4 discusses the several protocols that can be used for deploying the functions that comprise the cloud IAM gateway, as presented in our paper [Lon+13]. Moreover, the chapter achieves an evaluation of the proposed architectural solution of security for cloud computing through the related work presented in section 3.5.

## 3.1. Identity and Access Management Requirements for Cloud Computing

Cloud providers should have established a secure access and technical solutions. The data that will be stored in the cloud could be accessed only by authorized users, which are specified by the provider [CPN10]. Thus the IAM requirements are the following [Lon+13]:

i) Identity provisioning/de-provisioning
ii) Authentication
iii) Identity Federation
iv) Authorization

*Identity provisioning/de-provisioning Requirement*

Identity provisioning means the registration of users accounts to a cloud service, in a secure manner and on a specified time. In the same time, that user account could be de-provisioned by cancel it if it's necessary. Furthermore, the enterprises should have the capability to extend their identity management solutions to the cloud service. Currently, most Cloud providers don't offer a proper provisioning/de-provisioning for companies. Provisioning/de-provisioning is a relevant advantage in many situations. One of them is when a company hires an employee.

Her/his access on the applications will have to be denied and new accounts should be done for the new employee [CSA10].

*Authentication Requirement*

After provisioning the accounts users to the Cloud services, the company's users could authenticate to the Cloud service, by confirming that access credentials which were obtained in the provisioning process. Authentication is mandatory because in this way it is eliminated the attack's risks to enter into the Cloud services [CSA10].

*Identity Federation Requirement*

Identity Federation should be realized in order to deliver for cloud customers the opportunity to use the same entity's identity in others cloud services, without having to provide again the details of the identity, because they will be identified [Jun09].

*Authorization Requirement*

Authorization is the requirement that establish who has access to particular resources. This access is specified in the security policies, which different content depending on the user profile information.

## 3.2. Current Cloud IAM solutions

Identity and Access Management (IAM) must address an end-to-end secure identity between the client and the cloud service [Rit+10]. Identity Management (IdM) is the capability of identifying the users into the cloud services. The IAM could be realized in three methods: IAM inside the Cloud, IAM up to the Cloud and IAM down from the cloud [Gou+10]. Today there are numerous researches driven on all these methods. These three methods of implementing the IAM systems in cloud computing were also approached by the Open Group [Ope11], who referred them in accordance with three situations based on a buyer-seller scenario: seller controls, buyer controls and both parties controls. The terminology used by Open Group in their paper [Ope11] for these three situations is the following: seller's rules, buyer's rules and cooperative.

The *IAM inside the Cloud* is the simplest IAM method, based on creating the authentication procedure on each cloud service provider, which brings the limitation of remembering the different credentials for each cloud application [Sub+11]. Examples of IAM inside the Cloud were developed in: [VMw+09], [Fis09a], [Fis09b]. Even if it is an easier method, the independent stack does not look the appropriate approach for identification into the cloud services. This method does not address the integration with enterprise directory [Sub+11], [Lon+13], which does not conform with the complete Single Sign-On (SSO) for the services of cloud consumers because of the master repository location within the domain of cloud provider [Ope11].

The second methodology *IAM up to the Cloud* was adopted by: Juniper Networks, Inc. [Jun09]; Goulding, Broberg and Gardiner [Gou+10] and IBM Corporation [IBM10]. Using this methodology, the on-premise enterprises have their own IAM, which will want to extend it in the public Cloud service. This approach introduces new challenges which make it difficult to implement because of the

impediment of accessing the auditing and reporting features in the cloud service provider [Gou+10], [Lon+13]. Thus, if the enterprises adopt this IAM methodology, then a lot of complexity will be found, because the repository information should be customized in order to have the same format as the one delivered by cloud provider for extending the identity capabilities to the cloud service provider [Ope11].

The third IAM solution, *IAM down from the cloud*, seems more suitable for every size of the companies. It is called down from the cloud [Gou+10], because this IAM methodology is built as cloud based IAM services and the IAM services are delivered by a third party cloud provider. In addition, the IAM down from the cloud is called IAM-as-a-Service, terminology which is adapted from the terminology used by Cloud Security Alliance [CSA10b], who documented guidance for Identity-as-a-Service (IDaaS) in cloud. Thus, the cloud based IAM services are behaving in a cooperative manner between customers and cloud services and this is the reason why Open Group had designated as cooperative this type of IAM services in their paper [Ope11]. Even if some of the existing on-premise IAM solutions could be used for IAM down from the cloud, not all of them could be suitable [Gou+10]. An example of using a current on-premise IAM is *IBM Tivoli Identity management* solution, which was used by *Juniper Corporation* for its IAM down from the cloud solution [Jun09]. However, others testing in the area were not done to prove the suitability of others existing IAM for the IAM SaaS solution. This IAM technique also brings challenges in terms of efficiency, which are based on the obstacles imposed by the integration process of the on-premise IAM [Gou+10]. Other IAM down from the cloud architecture was deployed by Novell Company, which developed the *Novell Cloud Security Services*, which is an external Identity Access Management system that could be chosen by the cloud providers in order to enhance security of their customers. Using Novell Cloud Security Services the enterprises will have the ability to synchronize their IAM functions through the cloud service, because the credentials are securely transmitted via a Secure Bridge component to the Cloud Security Broker, which maintain the connection with the cloud service provider using custom connectors [Nov11], [Nov10]. Nevertheless, the cloud-based IAM services requires partnerships [Gou+10] with Cloud Service Providers (CSPs) for realizing the IAM services to be appropriate with the standards used by CSPs and for enhancing trust between customers and CSPs.

## 3.3. Design of the Architectural Solution of Security for Cloud Computing

The developed architectural model is proposing to apply security control to cloud computing for the following three elements: identities, information and infrastructure. The design of the architectural solution of security was realized using a multi-level decomposition structure (e.g. Layer 1-4).

Layer 1 of the architectural solution (Fig. 3.1) introduces the first element explored (i.e. securing the identities) and it outlines the relation between the entities that survives in the suggested architectural model. These elements are the following: customer, cloud Identity and Access Management (IAM) gateway and the cloud service, where the customer will get access to the cloud service using the cloud IAM gateway. The cloud IAM gateway which externalizes the IAM services to a 3rd party provider is called IAM as a Service (IAMaaS), idea advocated by Cloud Security

Alliance [CSA10b] who introduced the Identity as a Service (IDaaS) term. In addition, Cloud Security Alliance produced a recommendation guidance for IDaaS in terms of the types of the cloud service (i.e. SaaS, PaaS, IaaS) and in terms of the involved customers (i.e. internal to an organization, external to an organization or a consumer of a service) [CSA10b].

Thus, layer 1 introduces the Identity Access Management functions. This layer will be realized by creating web services security applications, which will integrate all these features: provisioning/de-provisioning, authentication, federation and authorization. The security services were realized in the literature for cloud environment. These security functions are suggested to be approached using the external security solution. The web services security applications of the cloud IAM gateway will be used like an *external security approach*, idea that was used in [Opi+07] for creating a Service Oriented Security. This security approach brings many benefits (e.g. scalability, portability, higher degree of reusability) comparing with the others security implementation approaches (e.g. embedded in the application, embedded in the middleware), even if it has the limitation regarding the performance.

Section 3.4 of this chapter will describe the evaluation of the standards that are considered reliable solutions for implementing the cloud based IAM services of the cloud IAM gateway.

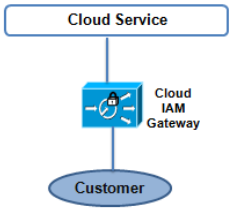


Fig. 3.1. Layer 1 of the Architectural Security Solution in Cloud Computing [Lon+11]

We consider that the customer from Layer 1 belongs to a private cloud of an enterprise, which wants to outsource their services to a Cloud Service Provider, which is a public cloud. Also, the cloud IAM gateway belongs to a third party cloud provider. Along with these considerations, Fig. 3.2 has been created in order to emphasize a clear view of the concerned entities from Layer 1 of the architectural security solution.

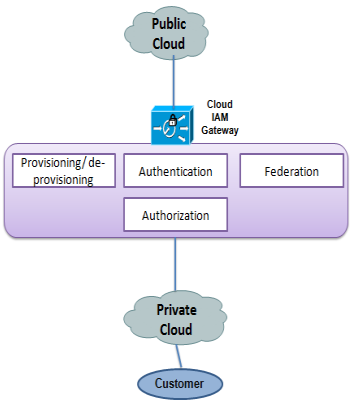


Fig. 3.2. A detailed view of Layer 1

Fig. 3.3 introduces the Layer 2 of the architectural security solution, which emphasizes the network security control, by using the firewall [Har09], in order to allow "ports" and "IP-level" access. Using the firewall rules will be avoided the XML threats. This security layer protects the pysical infrastructure of both service consumers and of cloud service providers [Lon+11].

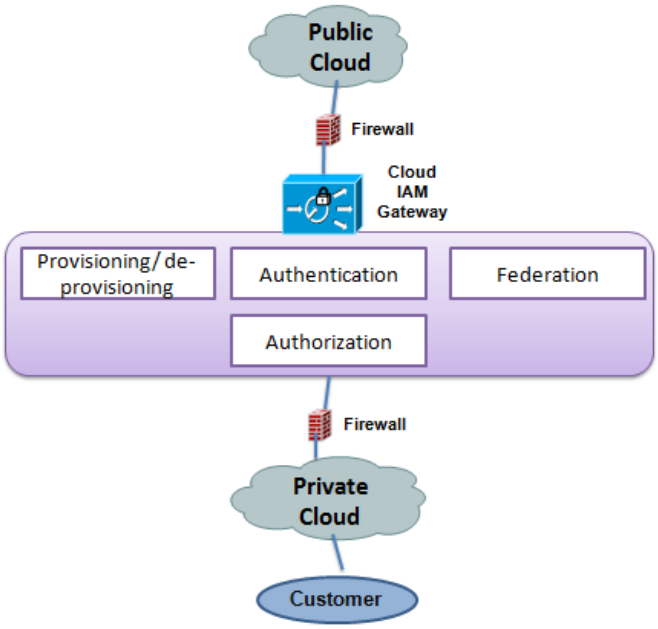


Fig. 3.3. Layer 2 of the Architectural Security Solution in Cloud Computing

Fig. 3.4 describes the new step of the architectural security solution in cloud computing, which improves the isolation of data customers, by splitting their data into private Virtual Local Area Network (VLAN) for each enterprise. The cloud that includes the data for all the implied customers is the public cloud. Segregation of organization's data is realized by developing private VLANs, which have to be configured based on the access restrictions for each virtual machine of customers in concordance with applied Access Control Lists (ACLs) [Cis+09]. Thus, data isolation of customers is increased by the utilization of the private VLANs for the information of customers and in the same time the virtualization layer of the Cloud Service Provider infrastructure is secured [Lon+11], [Lon12a].

Furthermore, creating virtual demilitarized zone (DMZ) for each cloud customer environment will create a virtual place that could be accessed by other customers and on the other hand will restrict the access to the information that resides on the private VLAN [Cis+09] (Fig. 3.5). In addition, a service provider cloud virtual DMZ is suggested to be used in order to be accessed by all customers. In the virtual DMZ of the cloud service provider, the cloud service providers can store data that concerns all customers, without compromising the customer's data. Also, Fig. 3.5 introduces a virtual DMZ place for each private cloud.

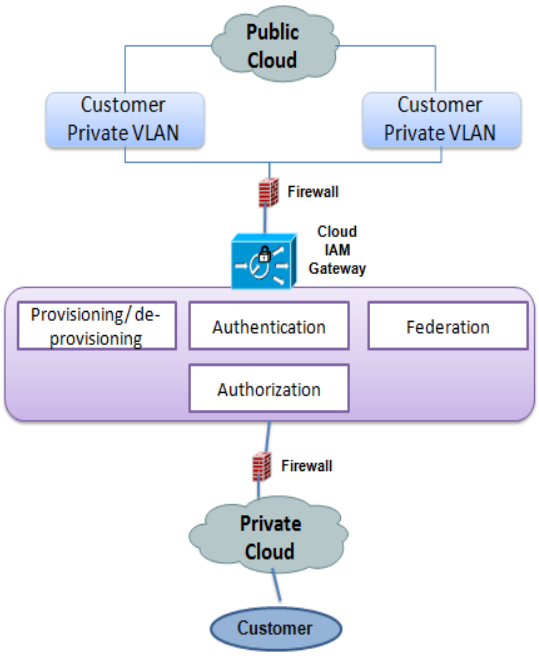


Fig. 3.4. Layer 3 of the Architectural Security Solution in Cloud Computing [Lon+11]

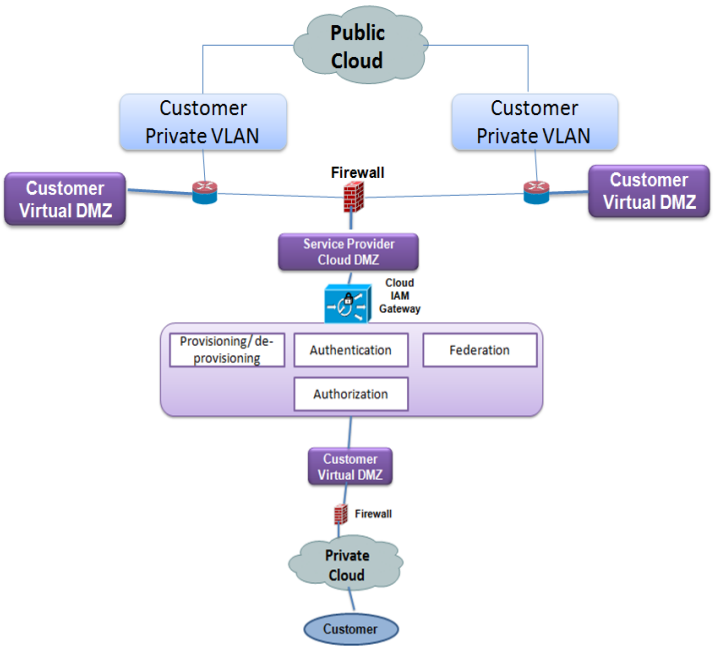


Fig. 3.5. Layer 4 of the Architectural Security Solution in Cloud Computing [Lon+11]

## 3.4. Cloud IAM Protocols

A trusted Identity and Access Management solution is creating using the suitable standards. Further, section 3.4.1 includes an evaluation of the standards for provisioning/de-provisioning identities (i.e. Services Provisioning Markup Language and Simple Cloud Identity Management). Subsequently, section 3.4.2 consists of a comparison between the identity federation standards (i.e. Security Assertion Markup Language, Liberty Alliance, WS-Federation, Shibboleth). Section 3.4.3 presents the solutions for authentication requirement. Afterwards section 3.4.4 describes two authorization models: user-centric and enterprise-centric.

### *3.4.1.* Standards for Provisioning/De-provisioning identities

The *Service Provisioning Markup Language (SPML)* is used in terms of provisioning the users in the cloud services. Also, another standard has appeared from the initiative of Google, salesforce.com and Ping Identity. It is *Simple Cloud Identity Management (SCIM)*. Both provisioning standards are discussed below.

#### *1. Services Provisioning Markup Languages (SPML)*

SPML is an XML-based framework that was developed by OASIS (Advancing Open Standards for the Information Security) PSTC (Provisioning Services Technical Committee) and which is used for user's identities, resources and services provisioning. According with PSTC provisioning is "the automation of all the steps required to manage (setup, amend & revoke) user or system access entitlements or data relative to electronically published services". There are two SPML versions available: SPML Version 1.0 and SPML Version 2.0 [OAS03a], [Lon+13].

SPML contains three main components (Fig. 3.6): *Requesting Authority* (RA), *Provisioning Service Point* (PSP) and *Provisioning Service Target* (PST). RA is software that requests from PSP a SPML provisioning. Between RA and PSP exists a trust relationship, which is not created by SPML, but it is necessary to exist in order to realize the provisioning. Before provisioning between the RA and the PSP should exists a trust relationships that assure the authentication of the identities participating in the process. These steps are compulsory for eliminating the possibility of creating the attacks (like: denial of service, impersonation) between the SPML parties. The third element in a SPML model of Figure 5 is the PST, which is an end-point abstract element in the provisioning process. In the requesting made by PSP to the PST, PST is behaving like PSP and PSP is behaving like RA [OAS03a], [Lon+13].

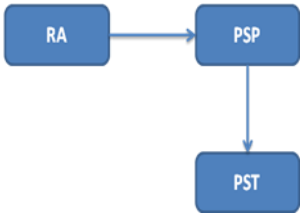


Fig. 3.6. SPML System Elements adapted from [OAS03a], [Lon+13]

### *2. Simple Cloud Identity Management (SCIM)*

Although SPML is a provisioning standard recognized in the cloud computing field, SCIM is an emerging protocol that was developed under the Open Web Foundation. SCIM appeared because SPML was considered too complicated to be implemented by cloud vendors. Thus, SCIM was created and it uses *REST* (Representational State Transfer) instead of SOAP (Simple Object Access Protocol) and *JSON* (JavaScript Object Notation) instead of XML [Har11], [Mor+11], [Lon+13].

SAML users change their options to JSON considering the difficulty of managing the features of SOAP [Lyn11], [Lon+13].

## *3.4.2.* Overview of Identity federation standards

In context of delivering the identity federation, Security Assertion Markup Language (SAML) seems to be preferred in production, considering the powerful features like: security, scalability and dependability [Pin10a], [Pin10b]. Table 3.1 presents our comparison between the identity federation standards and after that the identity federation standards (i.e. SAML, Liberty Alliance, WS-Federation, Shibboleth) are discussed.

Table 3.1. Comparison between the Identity Federation standards [Lon+13]

| ***Identity federation standards*** | ***Strengths*** | ***Weaknesses*** |
|---|---|---|
| ***SAML*** | • Dominant standard<br>• Distributed model (federation)<br>• Life cycle attributes of ID-FF<br>• Privacy attributes of Shibboleth<br>• Browser based identity federation | • Does not address identity requirements of web services |

| | | |
|---|---|---|
| ***Liberty Alliance*** | • Life cycle attribute<br>• Browser and Web Services based identity federation | • End of life |
| ***WS-Federation*** | • Web applications and web services identity federation<br>• Support for SAML 2.0 | • Domina nt in Microsoft Windows servers |
| ***Shibboleth*** | • Assures several privacy features | • Strictly used in academic world<br>• Strictly Open source implementation<br>• Centrali zed identity storage model |

***I. Security Assertion Markup Language (SAML)***

SAML is an XML-based framework, which was developed by OASIS Security Services Technical Committee (SSTC). The feature of SAML standard is to transfer the information about identity, authentication, attribute and authorization between organizations [OAS08]. It is recommended to use SAML together with the standards that implement authentication, provisioning and authorization in a cloud computing structure. Examples of cloud services providers which support the SAML standard are: Ping Identity, IBM Tivoli, CA Federation, Juniper Networks [Lon+13].

A SAML protocol could be used for guarantying the identity federation of the company's users. A remarkable advantage of SAML protocol is its ability to interoperate with other identity federation protocols (e.g. WS-* protocols) [Jun09]. The latest version of SAML (i.e. 2.0) includes the identity life cycle attributes of Liberty Identity Federation Framework (Liberty ID-FF) standard and as well the dominant privacy functionalities of Shibboleth 1.3 standard [BueAshRea08], [Lon+13].

A SAML entity consists of two parties: *SAML asserting party* and a *SAML relying party*. The SAML asserting party or SAML authority is characterized by the SAML assertions that it does. SAML relying party utilizes the accepted assertions. Two SAML entities could collaborate by sending and receiving a request. The entity that sends the request is called *SAML requester* and the one that receive it is called *SAML responder* [OAS08], [Lon+13].

A SAML entity could have different roles: identity provider (IdP), service provider (SP), attribute authority. The most important element in the SAML assertion is the *subject*. The subject involved in the SAML assertion is also called a *principal*, and it could be human, company or computer - an entity that can be authenticated [OAS08]. The subject of a cloud service is a user which wants to obtain a cloud service [Lon+13].

**Web Single Sign-on (SSO)** is one of the advantages provided by the SAML standard, because a user authenticated to one web site (Identity provider), can access directly another web site (Service Provider), as is related in Fig. 3.7. The authentication details of the user will be recognized by the service provider, who took them from the identity provider, with the specification that between the identity provider and the service provider exists a trust relationship. The user's information between the two web sites is transferred by the SAML standard [OAS05a]. The two web sites who established a trust relationship are partners and the process of sharing user's identity information between them creates a *federated identity* for that user [OAS08], [Lon+13].

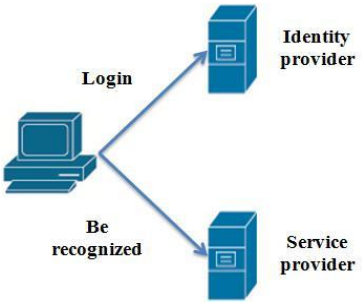


Fig. 3.7. Single Sign-On [OAS05a], [Lon+13]

### *II. Liberty Alliance Identity Frameworks*

The Liberty ID-FF end of life is caused by the fact that the identity life cycle attribute was integrated into the SAML 2.0 standard. Unlike SAML which is browser based identity federation, Liberty Alliance (Identity Federation and Identity Web Services Federation Frameworks) is browser and web services based identity federation [Pin10a]. Liberty (1.1, 1.2) is supported by IBM Tivoli Identity Federation [Bue+08], [Lon+13].

### *III. WS-Federation standard*

The WS-Federation standard is dominant in Microsoft Windows Servers, but it has the advantage to guarantee both web applications and web services based identity federation. And WS-Federation standard is interoperable with WS-Security standards. It is enhanced by Ping Identity cloud services provider, IBM Tivoli [Nov11], [BueAshRea08], [Lon+13].

### *IV. Shibboleth*

Even if Shibboleth adopts several privacy functionalities, it is strictly used in academic world and it enhances a centralized identity storage model [Maj+07], [Lon+13].

### *3.4.3.* Solutions for authentication requirement

A suitable authentication is required for organizations that want to access the Cloud services. Therefore, credential management, strong authentication, delegated authentication are leveraged across the cloud delivery models. Implementing authentication is very important, but organizations should be carefully at the attack implications. Attacks (like: impersonation, phishing, brute force dictionary based password) can occur on the credential details. Thus, authentication must be secured using the best techniques. Decreasing the risks in the cloud environment should be the priority for the Cloud providers and the organizations that adopt the cloud services. They also should select the appropriate solution in terms of cost [CSA10b], [Lon+13].

*SaaS* and *PaaS* cloud environment provide several authentication options for their customers. In the case of enterprises, the Identity provider (IdP) authenticate users and a trust relationship should be realized between the organizations and the cloud services by federation. Besides the enterprises could exist individual users that will want to authenticate at the cloud services. They could do it using the *user-centric authentication* (like: Google, Yahoo ID, OpenID, Live ID etc.). Hence, those individual users will access multiple sites using a single set of credentials [CSA10b], [Lon+13].

*IaaS* cloud environment disposes by two categories of users: the enterprise IT personnel and the application users. The enterprise IT personnel are the ones that develop and manage applications in the IaaS cloud model. For this type of users the solution that is recommended is to use a *dedicated VPN (Virtual Private Network)* with the IaaS environment, in order to apply the existing enterprise authentication systems (e.g. Single Sign-On solution or LDAP (Lightweight Directory Access Protocol) -based authentication) into the Cloud environment. If the VPN tunnel is not realized for feasibility reason, then authentication assertions (e.g. *SAML, WS-Federation*) are applied together with standard web encryption (i.e. *SSL*), which will determine the expanding of the enterprise's SSO capabilities to the Cloud service. Another solution that could be implemented in order to obtain the credentials authentication of users is to use the *OpenID* outside of the enterprise and to control the access of the users by specifying the appropriate privileges. Furthermore, also the *OATH-compliant solution (Open Authentication)* could be implemented in the Cloud systems for authenticating the users. These compliant solutions used strong authentication [CSA10b], [Lon+13].

### *3.4.4.* Standards for authorization requirement

#### *I. User-centric authorization model*

***OAuth (Open Authorization)*** is a user-centric authorization standard which provides for consumers (third-party) a limited access to the user's web resources and it doesn't require an authentication procedure. Unlike OpenID protocol which is used for authenticate the user in a cloud service, OAuth is used for allow third-party to access the user's web resources. The latest version of OAuth (i.e. OAuth 2.0) gives access to a large category of clients (i.e. web browsers, desktop applications and smart phones) [OAu,n.d], [Lon+13].

Even if OAuth 2.0 appears last year, it is having a fast expansion. The open source OAuth 2.0 libraries and the OAuth2.0 compatible cloud sites (e.g. Facebook, Twitter, SalesForce) prove its development [Wu+11], [Lon+13].

In the cloud computing landscape the parties involved by OAuth protocol are: the user, the OAuth Cloud service provider and the OAuth consumer (Fig. 3.9). First, the consumer wants to obtain a request token from Cloud service provider. The authorization is made by user and then the exchanging of the request token is realized between the consumer and the cloud service provider. This reveals the major capability of OAuth: to allow the users to control the access of their resources by delegating the access [Fis09b], [Wu+11], [Lon+13].

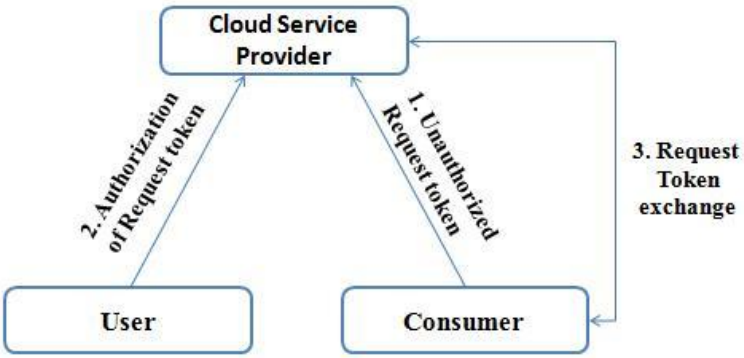


Fig. 3.8. OAuth token exchange [Lon+13]

### *II. Enterprise-centric authorization model*

**eXtensible Access Control Markup Languages (XACML)**

Extensible Access Control Markup Language (XACML) is an access control standard used for communicating policies by organisations, in order to access the online information [Dou+07]. Besides the policy language, XACML includes an access control decision request/response [Sun04], [Lon+13].

The XACML policy is composed by rules that have one of the following two actions: permit or deny. Each rule could have a target and/or a condition. The target (Fig. 3.10) contains the following attributes: Subjects, Resources, Actions and Environment. If the condition is part of the XACML rule that means the applicability of the rule is restricted [Nor09], [Lon+13].

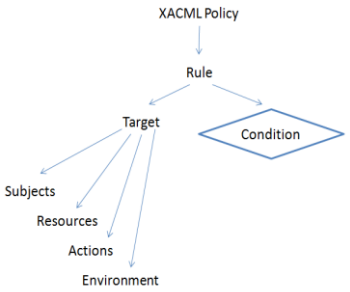


Fig. 3.9. The content of a XACML policy [Lon+13]

A PolicySet can include multiple policies and in the same time a policy can includes multiple distributed and decentralized rules, which are correlated by a rule-combining algorithm (i.e. deny-overrides, permit-overrides, first-aplicable) [Nor09], [Ber+10], [Lon+13].

In XACML (Fig. 3.11), a Policy Enforcement Point (PEP) limits access to various resources. The PEP will interact with a Policy Decision Point (PDP) using XACML messages to make a decision. PDP will in turn interact with a Policy Administration Point (PAP), which stores the policies [BerMarPac+10], [Lon+13].

XACML is used with SAML standard, because it achieves full functionality [Nor09], [Ber+10]. XACML's SAML profile defines how to protect, transport and exchange XACML messages. Using the XACML's SAML profile in WS-Security, Web Service providers can implement authorization by leveraging an XACML compliant PEP [Lak10], [Lon+13].

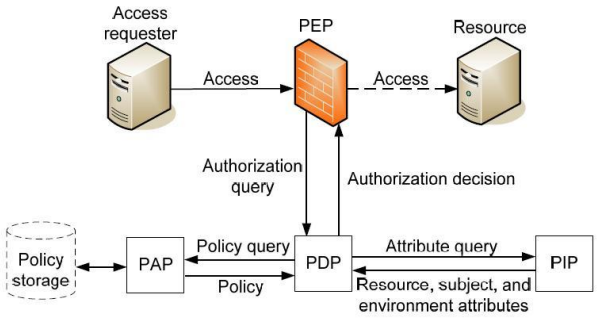


Fig. 3.10. The architectural/usage model of XACML [Nor09], [Lon+13]

## 3.5. Related work

This section encompasses the related work in the context of identity access management in Cloud Computing and the existing methods that were used for isolate the data in cloud environment. The view of the architectural solution of security for cloud computing includes the strengths of the existing cloud security solutions [VMw+09], [VMw07], [OAu,n.d], [Sav09] and aims to improve their limitations. The

architectural security solution is based on the guidance from [CSA10a], [CSA10b] and on the security architecture provided by VMware and Savvis (2009) [VMw+09], together with the specifications regarding the virtual demilitarized zone (DMZ) discussed in [Cis+09]. In this sense, Cloud Security Alliance provides recommendations for identity access management that were followed in this research work, in order to deliver a safe cloud platform.

The main component from the architectural solution of security is the cloud Identity and Access Management (IAM) gateway *(IAMaaS = IAM as a Service),* which will integrate all IAM security applications for all customers. More specifically, the IAM applications will be delivered down from the Cloud, which is one of the three strategies specified by Goulding, Broberg and Gardiner (2010) [Gou+10]. The idea of creating the IAM down from the cloud was adopted by Juniper Networks, Inc. (2009) [Jun09] and Novell (2010) [Nov10]. Juniper Networks, Inc. (2009) [Jun09] used the IBM Tivoli Identity Management for realize it. The creation of a IAMaaS seems more reliable compared with the others two IAM methodologies because it increases the security of customers. However, its implementation requires time consumption which is amplified by collaborations that should be maintained with Cloud Service Providers.

Further, in this chapter *standardized identity connectors* build on Service Provisioning Markup Language (SPML) or Simple Cloud Identity Management (SCIM) schema are suggested to be deployed within the architectural security solution instead of custom identity connectors (e.g. the ones developed by Novell [OAu,n.d], [Wu+11], which are linked with Java Servlets applications, applications that runs on Apache or applications such as SalesForce.

The proposed architectural security solution approached the *identity federation* described in [Jun09], in order to establish a trust domain between the SAML identity provider and the SAML service provider. Moreover, similar with the CA's strategies [Pin10b] the architectural solution of security will cover the following federation capabilities: Single Sign-On (SSO) and Single Logout (SLO). The SSO function is presented for both situations: *enterprise-centric* (using SAML protocol) and *user-centric* (using OpenID protocol),

The *authorization* is aimed to have similar paradigms of policies like Savvis [Sav09] who developed the Savvis security architecture (e.g., network policies, audit policies and system policies). The policy management approached in [Sav09] is an *Identity and Access Management* security requirement, which uses the *role-based access control* (RBAC) in order to identify each virtual machine with their corresponding user, role and privilege access and in the same time, the service consists of delivering the VM audit reports. This feature of separation of user's roles is also meet in the *enStratus Security Architecture* [enS10], which provides also an intrusion detection analysis capability in order to report a possible attack.

Moreover, the proposed architectural solution of security aspires to isolate the organization's data by creating private Virtual Local Area Networks (VLANs) and virtual demilitarized zone (DMZ) for each customer.

VMware and Savvis (2009) [VMw+09] have created the Cloud Security Reference Architecture. But, comparing with their architecture, the proposed architectural security solution is different because of the way the security architecture is approached. The Cloud Security Reference Architecture provided by VMware and Savvis [VMw+09] is a hosted architecture and all the security concerns are concentrated around the security features of the cloud service provider, where the IAM is concerning the cloud service provider. Also, a different scenario that regards the Cloud Security Reference Architecture provided by VMware and Savvis

[VMw+09] can be observed, in which is considered the case of the enterprises that deployed a private cloud using the Vmware product and that want to migrate with their vApp to the public cloud. Comparing with the case illustrated in [VMw+09], our architectural security model had considered the case of the enterprise that want to migrate to a public cloud, without having necessarily a private cloud developed with the same tehnology used by the cloud service provider. Thus, in this chapter interoperability was considered to be approached by the usage of federation capacity.

Furthermore, we created private Virtual Local Area Networks (VLANs) for each customer ideea adopted as well by VMware and Savvis (2009) [VMw+09], who suggested to utilize port groups for each customer in order to isolate their resources. The adoption of virtual Local Area Networks (VLANs) was also discussed in [Cis+09]. Additionally, our architectural solution of security included the virtual demilitarized zone (DMZ) for each customer private VLAN like it was described in [Cis+09]. VMware and Savvis (2009) [VMw+09] also used the DMZ zone but for the vApp of each customer in order to validate the patch level and the security level before moving it to the public cloud. Thus, the proposed architectural security solution brings a protection level for each customer's data by creating a virtual DMZ.

In this study it was also considered the goal of having a virtual DMZ for the Cloud Service Provider like VMware and Savvis [VMw+09] and additionally the proposed architectural security solution included a virtual DMZ area for each private cloud created by each enterprise.

## 3.6. Conclusions

This chapter has introduced an architectural solution of security for cloud computing in order to enhance the security for the following three elements: identities, information and infrastructure. The design of the architectural solution of security was realized using a multi-level decomposition structure (i.e. Layer 1-4). The first level of the architectural security solution has included the main security element: a cloud Identity Access Management (IAM) gateway, also called IAM-as-a-Service (IAMaaS). The cloud IAM gateway represents one of the current IAM solutions, namely the IAM down from the cloud, which was selected to be used in the architectural solution of security. The selection was made based on the evaluation of the current IAM solutions, in which we concluded that even if IAMaaS is harder to realize compared with the others two solutions, its advantages of increasing the security of customers and providing cooperative capabilities of customers with Cloud Service Providers (CSPs), are the reason of selecting it.

Further, the next three levels of the architectural security solution have reffered to securing the infrastructure and the information of cloud environment, by applying the network security control and by isolating the data of customers.

# 4. AN HYBRID TEXT-IMAGE BASED AUTHENTICATION FOR CLOUD SERVICES

Cloud computing environment is the future and evolution of Information Technology as we can see from Chapter 1, in which the advantages offered by cloud services for companies are described. However, the broad problem that worries the majority of cloud users is security. Providing confidential information (like: bank accounts, health records, intellectual property etc.) through Internet to Cloud Service Providers becomes ubiquitous and in the same time is becoming uncertain regarding the integrity, confidentiality and availability of our data. The solution for delivering confidentiality of data is to assure a proper authentication technique for cloud services. The current authentication solutions for cloud services are based on username and password credentials, together with the X.509 certificates [Pop+12].

Currently, the authentication systems are predominately using the knowledge based authentication, although another two authentication techniques exist (i.e. token-based and authentication based on biometrics) [Dha+00], [New+05]. Whereas the current authentication system for cloud services relies on password based authentication, the proposed solution focuses on improving the knowledge-based authentication in cloud environment.

Thus, before introducing the proposed authentication solution, a background of knowledge-based authentication techniques is presented. Further, this chapter presents the proposed hybrid authentication solution for cloud services based on text and images, which was published in our paper [Pop+12]. Finally, the chapter illustrates the analysis of the proposed solution, which represents the analysis of the following elements: the solutions for the possible attacks, the time for registration and login and the system's usability.

## 4.1. Knowledge-based authentication techniques

The knowledge-based authentication technique is something that the user knows. Three types of knowledge-based authentication techniques exist: password-based authentication, image-based technique and text-image based technique.

**Password-based authentication**

The username and password based authentication is a *knowledge-based authentication technique*, which requires to remember the password by recalling the memory of users. One of the problems with password based authentication is that most of the times, passwords-based authentication offer low security level, because users prefer to choose weak passwords in order to remember them or in order to enter them easily in their mobile phones. Another issue related to password based authentication is the habit of individuals to write down their complex passwords or to use the same password on different authentication systems [Dha+00]. These

issues show the existence of incompatibilities between security and usability requirements, due to the password-based authentication technique which relies on recall-based authentication. Furthermore, security and usability requirements are the main challenges for authentication's developers.

**Image-based Technique**

Image-based technique replaces the recall-based method of a knowledge-based authentication with the recognition-based method, minimizing the user recall load and providing a pleasant user experience [Dha+00].

Dhamija and Perrig in 2000 proposed a prototype of Déjà Vu relied on image-based authentication which strengthens the competence of this user-friendly technique because of their user study's results in which a greater percent of respondents succeeded using Déjà vu authentication (i.e. 90%), compared with the percent of respondents who had succeeded with the authentication based on passwords or PINs (i.e. 70%) [Dha+00]. A similar study based on image-based technique was performed by Newman, et al. [New+05], in which the password is created with images that previously were selected by users at the enrolment process.

Another work in terms of image-based technique was realized by Confident Technologies. They provide image-based authentication enterprises, websites, web and mobile applications and mobile devices [Con12].

Furthermore, the solution of using facial pictures is included in the same category for authentication (e.g. Passfaces). This approach uses facial pictures due to the innate ability of people to remember faces. However, it can have the disadvantage of choosing the faces to be related to that person such that the chosen image resembles with the use, facilitating impersonation [Dha+00].

There are several works concerning the image-based techniques. All of them demonstrate the recall advantage, but a series of drawbacks are noticeable. One of them is the existence of a trade-off between security and usability, because if the password chosen by users contains more images, this will increase security, but in the same time will reduce the possibility of positive recall [Jac06]. Another important vulnerability of this technique is its exposure to brute force attacks, because the attacker can download the image set in order to try all possible combinations [New+05].

**Text-image based Technique**

Text-image based technique comes with the user-friendly improvement for authentication procedure. This was demonstrated by the user study conducted at University of California at Berkeley [New+05].

One of the text-image based techniques is the story-based technique [Jac06]. This method was evaluated by Jackson [Jac06] in comparison with the picture-based and the facial-based techniques. It is a different solution that allows users to create their own story image by using a series of drop-down selection boxes.

Text-image based technique was also studied in the context of increasing the security and recalling capabilities for recovering the user's password [Mic+11], [Ren+10].

Renauld and Just [Ren+10] developed a challenge protocol for replacing the textual questions with pictures associated with text. The images used by Renauld

and Just [Ren+10] in their protocol are representing three pictorial cues (i.e. 'animals', 'places' and 'events'), which are correlated with indirect questions for eliminating the observation attacks. This idea of using pictorial cues is also presented in our proposed authentication solution in order to create an additional recall aid for users [Ren+10].

Another approach regarding the text-image based technique is also presented by Micallef and Just [Mic+11], where a novel method using avatars for improving the recovering password procedure is described. This method is a substitute for the traditional challenge questions, which most of the time are vulnerable to observation attacks. The solution provided by Micallef and Just [Mic+11] presents another way to realize the secondary authentication stage: to alternate text with images, by creating an authentication avatar, which consists of basic identifying information and personality information of the avatar. The avatar's information is selected by user from drop-down lists and an image is associated with each type of information. Our proposed authentication technique uses the same idea of associating images with text like Micallef and Just [Mic+11] created the avatar's secondary authentication, but in different context, for an authentication solution and in different way. Also this recovering solution proposed by Micallef and Just [Mic+11] resembles with the story-based interface but there are used with different purposes and of course the solution of Micallef and Just provides the originality of using false information for authentication by creating the avatar profile. The similarity between these solutions is that Micallef and Just [Mic+11] builds the story about the avatar as the story-based interface creates a story related to an individual image by drop down selection boxes [Jac06].

## 4.2. Authentication Solution

The proposed authentication solution was designed in order to increase the security at the Security Access Point (SAP) of cloud computing environment, which at the moment is built only with password-based authentication and X.509 credentials for accessing the cloud services (Fig. 4.1). Another factor that was considered for the proposed authentication solution is the human factor.

Security Access Point (SAP) of cloud computing is the server that provides front-end security services and is responsible with the authentication of users [Set11], [Pop+12].

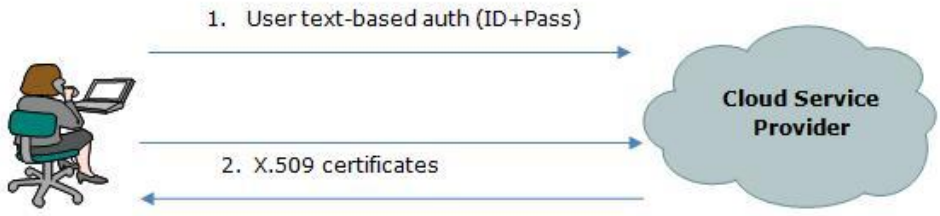


Fig. 4.1. The Current Cloud Computing Authentication Solution [Pop+12]

In the proposed authentication solution, the Security Access Point consists of three level security approaches (Fig.4.2):

Level 1: Text-based password

Level 2: Hybrid Text-Image based authentication

Level 3: X.509 certificates

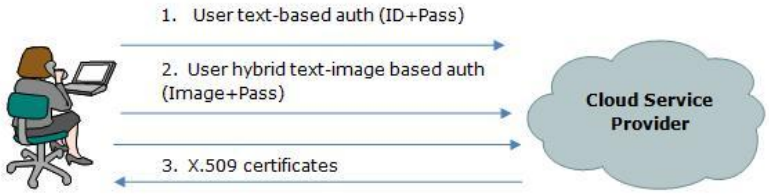


Fig. 4.2. Proposed Cloud Computing Authentication Solution [Pop+12]

In order to complete Level 2 from the authentication scheme of Fig. 4.2, individuals should first complete a registration process, which requires choosing one image from the three sets of image's grid (Fig. 4.3) and assigning passwords for all three images (Fig. 4.4). These individual's identity information are stored into a database with images that will be available into the image space of the front-end server of the cloud provider.

Thus, level 2 of the proposed authentication solution is a hybrid text-image based authentication in which the image-based authentication solution is combined with text-based authentication.

The following notations were used in order to define the proposed hybrid text-image based authentication solution: image space, individual image set, individual password set and presentation set. Some notations (i.e. image space, individual image set, presentation set) were taken from [New+05], but with different definitions and those differences are described bellow and in section 4.3 of this chapter. Also an additional notation (i.e. individual password set) was added.

Therefore, three image sets exists (Fig. 4.3) on the image space and each image set contains nine distinct images (i.e. in hue and color) and are also distinct in structure, but pertaining to a single category: 'flowers', 'animals' and 'fruits'. The images are easily to be described, because the security level is realized by the utilization of the *individual image set* that is combined with the corresponding *individual password set*.


Fig. 4.3. Image Space

*The individual image set* contains the picked three images by individual from each image set of the cloud image space. Individuals should have the possibility to re-selecting again the same images for confirming that the individual image set was correctly created [Nit+08]. Thus the enrolment procedure will have this confirmation capability. Additionally, for each image of the individual image set (i.e. Case A from Fig. 4.4) the user is requested to choose a password based on text (i.e. Case B from Fig. 4.4) in order to compose its own *individual password set*.

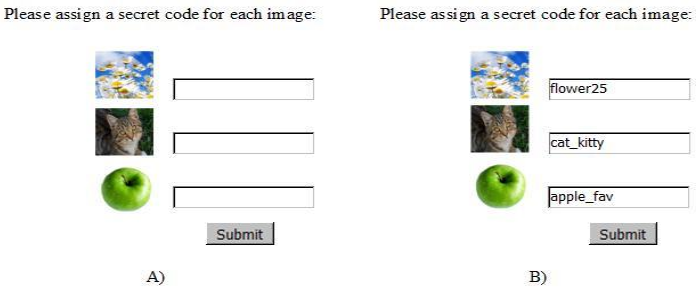


Fig. 4.4. Individual image set and Password image set

Fig. 4.5. Random locations of the individual image set [Pop+12]

*The presentation set* contains the individual image set selected by users, but those three images of the individual image set will be presented each time in different order for each authentication attempt, because the images are generated using a permutation algorithm (Fig. 4.5 and Fig. 4.6 ) [Pop+12]. As we can see from Fig. 4.6 the presentation set contains only the individual image set, also called portfolio images [Dha+00]. The proposed authentication solution does not have decoy images like the authentication Déjà vu prototype [Dha+00].

An illustrative example of the proposed solution is Fig.4.6, which requires the individual to assign a secret code for each of the three images. It can be observed the order of images which is distinct compared with the order of images presented in Fig. 4.4 in which the individual completed the registration process.

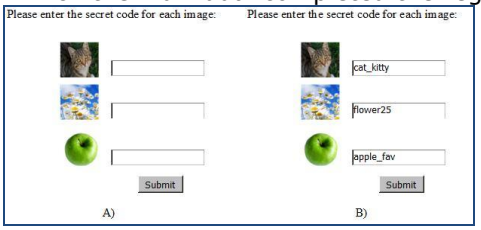


Fig. 4.6. Authentication form

## 4.3. Advantage of the authentication solution

This section includes the analysis of the following elements: solutions for the possible attacks, the time for registration and login and the system's usability, by comparing the proposed solution with others relevant solutions.

The proposed authentication solution for cloud services is focused on improving the security level for the knowledge-based authentication technique, which currently is used only with text-based passwords for authenticating users into cloud services.

In this sense, the proposed solution adds a new level security approach which is based on hybrid text-image authentication, which combines text with images. This solution started from the idea of creating an authentication solution to be user-friendly and secure for cloud users, so that the two authentication requirements do not affecting each other and to eliminate the trade-off between them.

Therefore, the hybrid solution from level 2 of the proposed authentication method combines the Image-based authentication (IBA) solution with text-based passwords. The image-based authentication seems to be addressed and supported by researchers [Dha+00], [New+05] due to the fact that recalling images is preferable than recalling text for users.

### 4.3.1. Solutions for possible attacks

Compared with the solution approached by Newman, et al. in 2005 [New+05], who use an image space with a single set of images different in hue, colour and structure, not easily to be described, the proposed solution uses an image space which contains three different image sets. An image set from the proposed solution includes different images in hue and colour, easily to be described and different in structure but belonging to a single category (i.e. first image set belong to 'flowers' category, second image set belongs to 'animals' category, third image set belongs to 'fruits' category). Thus, in the proposed solution the individual image set contains only three selected images by individuals to authenticate himself, while in solution proposed by Newman, et al. (2005) [New+05] the individual image set contains the images that a user chooses to authenticate himself which are not restricted to a image number.

The abstract images were not chosen as Dhamija and Perrig (2000) [Dha+00] used, because the proposed solution authenticates users through requesting a text-based password for each selected image. In this regard the security is increased, the remembering capabilities of the user brain are facilitated and the authentication system is protected against *shoulder surfing attacks* because of displaying for login the images of our individual image set in random positions [Jac06].

Dhamija and Perrig (2000) [Dha+00] show the meaning of using the Random Art instead of photographs which reduces the predictability of attackers to guess the portfolio images (i.e. individual image set) chosen by the victim to authenticate. However, using abstract images is a reliable solution for the case when the image space consists from a single image set and the password key

consists from the selected images. In the proposed solution the abstract images are replaced with describable images because a different solution was created compared with the prototype proposed by Dhamija and Perrig (2000) [Dha+00] and Newman, et al. (2005) [New+05]: three image sets within the image space were used, requesting the user to create an individual image set with three images and to allocate text passwords for each image. The idea of using the pictorial cues (i.e. the individual image set) was suggested by Renauld and Just (2010) in their paper [Ren+10], in which three pictorial cues (i.e. "animals", "places" and "events") are associated with indirect questions with the purpose of creating a secured and usable recovering procedure.

Furthermore, the proposed solution increases security because the keys to authenticate are hybrid, combining the individual image set with individual password set, compared with the solution from [New+05], [Dha+00], in which the password key contains only the images selected to represent the password, more exactly the individual image set.

If the user text-based authentication solution (i.e. Level 1) from the proposed cloud computing authentication solution (Fig. 4.2) is compromised, the hybrid text-based authentication (i.e. Level 2) cannot be compromised since the user is putting as passwords the secret codes from the individual password set corresponding to each image from the individual image set. This hypothesis was considered also by Ray (2012) [Ray12], who proposed the Ray's Scheme. Ray's Scheme is a graphical password based hybrid authentication system for smart hand held devices that uses the standard text-based authentication as a first step and then creates a combination of techniques: recognition-based (i.e. images ) and pure recall based techniques (i.e. specific digits are to selected and associated with images). Comparing with the scheme provided by Ray (2012) [Ray12], the proposed solution uses (at Level2) text-based passwords instead of digits for associating with images. This capability makes the proposed system more secure and protected against *brute force attacks* because the individual password set is composed from passwords that are larger in choices instead of the digits used by Ray (2012) [Ray12]. In this case the attacker will not have to download the image sets in order to try the possible combinations like is in the case presented by Newman, et al. (2005) [New+05], because each time the individual image set will be automatically displayed. But, the authentication solution can be attacked by attempts to find the passwords for each image from the presentation set, which are difficult to guess because there are three different passwords. Moreover, for the brute force attack problem, it should be considered to adjust an adequate time for attempt to authenticate and also to adjust the number of unsuccessful login attempts, in order to stop a potential attack [Dha+00], [New+05], [Jac06].

The *keystroke logging issue* is eliminated with the fact that the three images from individual image set will be displayed each time at random locations like a basic image based authentication (IBA) is built [New+05].

Moreover, the image space does not contain the "faces" category like Passfaces in order to avoid *impersonation attacks*. Dhamija and Perrig (2000) [Dha+00] noticed in their Déjà vu study the preference of respondents to choose images that closely resembled the users.

### 4.3.2. Time to register and login

Dhamija and Perrig (2000) [Dha+00] concluded in Déjà vu study that utilizing photographic images instead of abstract images reduces the time of users to login, thus the time to login into the proposed authentication system will be decreased because of the ability of peoples to recognize photo images easier than abstract images. In addition, the proposed solution includes text-based passwords besides the images key. Dhamija and Perrig (2000) [Dha+00] showed the capacity of respondents to realize the registration process quickest with the passwords and PINs instead of creating the image portfolios, but the users will need longer time to login. Because the proposed solution associates the text-based password with images we envisaged a shorter time to login compared with the time of attempting to login using the standard text-based password. This estimation is also supported by the following aspects: requesting only 3 images for creating the individual image set is reducing the time of user to enroll and automatically displaying at the authentication point the individual image set is reducing the time of individuals to login [Jac06]. In addition, the user study performed by Jackson in 2006 [Jac06] on three interfaces (i.e. basic picture based interface, facial picture based interface and story based interface) reveals that the story based interface was the most successful. The presented story based interface is a combination of images with text, which seems in a way with our proposed solution, but it is different because the user builds up a story using a drop down selection boxes [Jac06].

### 4.3.3. System's usability

The proposed authentication solution requires the user to correlate the passwords from the individual password set with the random images from the individual image set. Regarding the images displayed on the presentation set of the proposed solution, we do not using decoy images like Dhamija and Perrig (2000) [Dha+00] and Newman, et al. (2005) [New+05]. The presentation set from the proposed solution includes only the random images from the individual image set because in this way the individuals will not be confused by those decoy images. Dhamija and Perrig [Dha+00] discuss in their user study, the possibility of users to learn the decoy images and to be disoriented and to use them as the real individual image set.

Additionally, the presentation set displayed for users to authenticate will be listed with all required components in a single page (case A of Fig. 4.6).

Moreover, the fact that the proposed solution requires individuals to select a single image from each image set of the image space do not lead to confusion because users know exactly what they have to do. Also, when the individuals will have to login, the requirements are very clear: a form with the three selected images will be randomly displayed in order to associate for each of them the corresponding passwords. This capability of the proposed solution is useful for promoting good recall and good security [Jac06].

In this sense, there are two directions which demonstrate the good recall. First, the individual image set displayed in front of the users at the authentication procedure were designed in order to serve as a clue for user's memory like Micallef and Just (2011) [Mic+11] used images in order to increase the recall of users to remember the information about their avatar. Secondly, the results of the study conducted by Jackson (2006) [Jac06] show that in a picture based interface the

users are more comfortable if they have a specific number of images to select in order to complete the enrolment process.

## 4.4. Conclusions

This chapter is focused on the knowledge-based authentication techniques because the proposed authentication solution is based on hybrid text-image solution for authentication in cloud computing field. Thus, firstly a briefly outline of the knowledge-based authentication techniques was given (i.e. password-based, image-based and text-image based techniques). These three authentication techniques were individually discussed, emphasizing the limitations and the strengths that characterizing them. From the conducted analysis, the text-image based technique fits more in the authentication scheme to increase the capabilities of security and recall, compared to the other two authentication techniques. These advantages were also highlighted in relation to the recovering user's password.

In addition, the proposed authentication solution for cloud computing has been introduced, which consists of three level security approaches, compared with the current cloud computing authentication solution, which is represented by two level security approaches. Hence, the proposed authentication solution increases the security by providing an additional security level between the password-based authentication and X.509 credentials for accessing the cloud services of the current cloud solution. The proposed security level is based on hybrid text-image authentication and it was designed to reduce the trade-off between security and usability requirements, which was proved by analyzing the proposed solution in terms of possible attacks, with respect to the time spent by users for recording and authenticating, as well as in relation to the system's usability. These examinations were exposed by the analysis discussed at the end of the chapter, which demonstrated the capacity of the proposed solution to protect the system against shoulder surfing attacks and keystroke logging by displaying the individual images set in random positions, against brute force attacks by using the hybrid keys and against impersonation attacks by avoiding the "faces" category for defining the image sets. In terms of usability, a shorter time to register and login is combined with a good recall capability.

# 5. PRIVATE CLOUD SET UP USING EUCALYPTUS

This chapter presents the Eucalyptus open-source software, which was used for creating a private cloud deployment model, respectively the Infrastructure-as-a-Service (IaaS). Eucalyptus is the acronym for *Elastic Utility Computing Architecture Linking Your Programs To Useful Systems*. It is an open-source cloud platform, which was developed by University of California for creating private and hybrid clouds. Now, it is supported by Eucalyptus Systems, a Canonical Partner. Eucalyptus Systems also provides for its customers a commercial version, called Eucalyptus Enterprise Edition [Euc09].

The reason for selection of Eucalyptus cloud platform is because it is open-source and it provides interfaces compatible with Amazon Web Services (AWS) [Joh+10], [Kar+11] (e.g. Amazon Elastic Compute Cloud (EC2), Amazon Elastic Block Storage (EBS), Amazon S3 (Simple Storage Services) ). Furthermore, Eucalyptus cloud can be managed using the RightScale 3rd party management tool [Rig12] . Another opportunity provided by Eucalyptus team is Eucalyptus Community Cloud (ECC) [Euc12], which was tested before the development of the Eucalyptus private cloud.

## 5.1. Eucalyptus Architecture

According with administrator's guide provided by [Euc10], [Euc12a], the Eucalyptus architecture includes five components (Fig. 5.1): Cloud Controller (CLC), Walrus, Cluster Controller (CC), Storage Controller (SC) and Node Controller (NC).

The *Node Controller (NC)* is responsible for handling the hosting of virtual machines instances on every node and for the management of the virtual network endpoint. The NC inspects the VM's maturity from execution process to termination process [Euc10], [Lon+12b], [Lon11a], [Lon11b].

On the next level of the architecture are the Cluster Controller (CC) and the Storage Controller (SC), for each cluster that is formed by a collection of NCs sharing a LAN segment [Euc12a]. The *Cluster Controller* is the element that collects information about VMs and it deals with the VMs scheduling on particular NCs. A condition that CC must meet is that it must contain NCs which are in the same broadcast domain (Ethernet) [Euc10]. Cluster Controller decides where to place the request received from the Cloud Controller, by evaluating which Node Controller has sufficient free resources [Cor+10]. Each cluster also has a *Storage Controller (SC)*, which was developed to have the same capabilities like Amazon Elastic Block Storage (EBS) and to be able to communicate with others storage systems (NFS, iSCSI etc) [Euc10], [Lon+12b], [Lon11a], [Lon11b].

The module from Eucalyptus architecture that treats the incoming requests and provides high level resource scheduling is *Cloud Controller (CLC)*. CLC realizes the scheduling component by collaborating with the Cluster Controllers [Euc09]. Therefore, CLC decides where to place the request received from a Client, by evaluating which Cluster Controller has sufficient free resources [Cor+10],

[Nur+08], [Nur+09a], [Nur+09b]. In addition, Cloud Controller can be accessed through a command line interface (euca2ools) which has interfaces compatible Amazon Elastic Compute Cloud (EC2) and through a Web-based user interface. Situated at the same level in the architecture like Cloud Controller, *Walrus* module is used for storing data. It has compatible interface with Amazon S3 [Euc09], [Lon+12b], [Lon11a], [Lon11b].

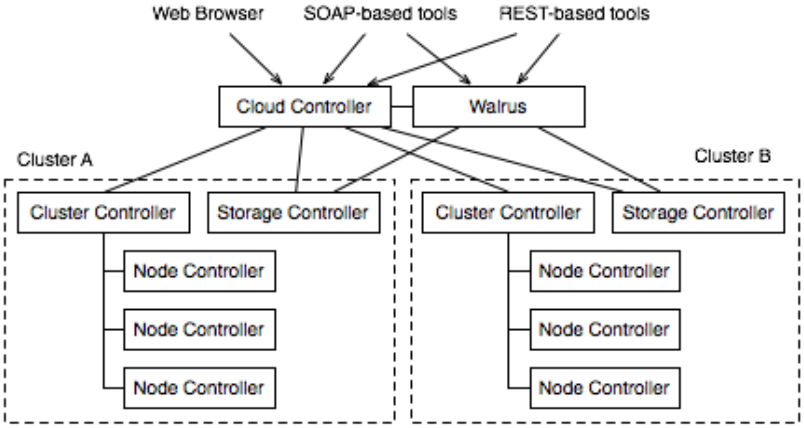


Fig. 5.1. Eucalyptus Architecture [Euc12a]

## 5.2. Eucalyptus Private Cloud Deployment

The private cloud was deployed using the binary packages of Eucalyptus 2.0.3 open source for CentOS operating system, as presented in [Lon12]. The details of the Eucalyptus private cloud setup are presented in Table 5.1 and Fig. 5.2. Table 5.2 illustrates the hardware components that constitute the physical infrastructure.

The Eucalyptus Administrator's Guide [Euc12a] constitutes the main source guide for deploying the private cloud. Additionall materials that were used in order to build it are: [Joh+10], [Sha,n.d], [Int11], [Sha10].

Table 5.1. Details of Eucalyptus private cloud [Lon12]

| | |
|---|---|
| ***Version*** | Eucalyptus 2.0.3 open source |
| ***Hypervisor*** | Xen |
| ***Topology*** | One front-end (cloud controller, walrus, cluster controller, storage controller) + 3 nodes |
| ***Networking mode*** | Managed |

Table 5.2. Cloud Systems Configuration [Lon12]

| | | ***Front-end*** | ***Node1*** | ***Node2*** | ***Node3*** |
|---|---|---|---|---|---|
| ***OS*** | | CentOS 5 on 64 bits architecture | CentOS 5 on 64 bits architecture | CentOS 5 on 64 bits architecture | CentOS 5 on 32 bits architecture |
| ***Hardware*** | ***Processor*** | AMD Sempron (tm) Processor | AMD Athlon (tm) 64 Processor | AMD Athlon (tm) 64 Processor | Intel (R) Pentium (R) |
| | ***Free Memory*** | 1024MB | 256MB | 256 MB | 128 MB |
| | ***Disk Space*** | 54GB | 51GB | 51GB | 162GB |
| ***NIC*** | | **eth0:** 192.168.1.50 **eth1:** 172.16.1.1 | **eth0:** 172.16.1.10 | **eth0:** 172.16.1.11 | **eth0:** 172.16.1.12 |
| ***Hostname*** | | front-end | node1 | node2 | node3 |

The cloud topology used is a front-end and three nodes (Fig. 5.2). The front-end is the server that runs the following Eucalyptus services: cloud controller, walrus, cluster controller and storage controller, while in nodes run the node controllers. Another important configuration in the Eucalyptus private cloud is the virtualization mode chosen, together with the networking mode [Lon12].

Fig. 5.2 describes that VMs were run in three physical machines and that each physical machines can run a single VM due to them hardware configuration.

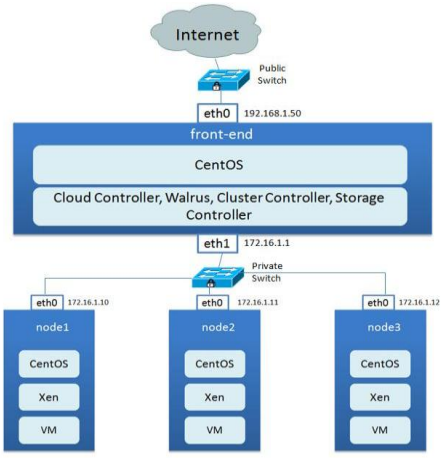


Fig. 5.2. Private Cloud Configuration [Lon12]

In terms of virtualization, the para-virtualization type was chosen, because the CPU (Central Processing Unit) of physical servers does not have virtualization support. In this sense, Xen hypervisor is utilized for realizing the virtualization of nodes, due to the fact that those nodes provide PAE (Physical Address Extension) support for CPU [Xen12], [Lon12].

Along with the virtualization technology, in the private cloud several virtual network elements were automatically created. Fig. 5.3 which was adapted from [Xen12] describes the relationships between physical (i.e. eth0) and logical cards (i.e. vif0.0, vif1.0, vif2.0, vif3.0). If for example, a node has one physical interface card (eth0) and three VMs can be created inside the node (the VMs have „eth0" for interface card), then inside the Domain 0 of the node the following virtual Ethernet interfaces will be generated: vif0.0, vif1.0, vif2.0, vif3.0. All vif's are connected to the Shared Bridge Connection (i.e. xenbr0), which behaves like a switch for all vif [Xen12]. The Shared Bridge (xenbr0) is also called Shared Physical Network Device [Kam11], [Lon12].

Xen uses the „libvirt" virtualization API for managing the VMs [Kam11], [Lon12].

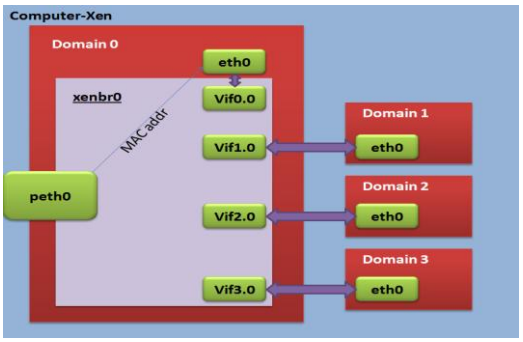


Fig. 5.3. Xen hypervisor configuration [Lon12], [Lon11a]

Moreover, the Eucalyptus private cloud makes use of the Managed networking mode because of the feature's granularity provided (e.g. connectivity, IP control, security groups, elastic IPs, metadata service and VM isolation) [Euc12a], [Lon12].

Beside the installation, configuration and registration of the Eucalyptus components, several firewall rules were created, while other rules are identified as being automatically deployed by Eucalyptus.

## 5.3. Eucalyptus Management Tools

This section describes the Eucalyptus management tools for the consumer role. A complete study regarding the analysis of cloud portals from the user roles was realized in our paper [Lon+12b].

An overview of the several Eucalyptus management tools is provided [Lon+12b], by addressing the taxonomy and our evaluation of the specified cloud management interfaces. The classification of the Eucalyptus management tools is

I. Web based management: Eucalyptus Admin Interface
II. Client tools:
   a. Command line tool: Euca2ools
   b. API Client: Typica
   c. Graphical User Interfaces (GUI) client: Firefox Plugins, Cloud42, tAWS Tanacasino, EC2 Dream
   d. Third party Management tools: Right Scale, enStratus, IMOD Kaavo, CloudWatch, Scarl, Tapin, Cloudkick

**I. Web based management**

The web based management interface of Eucalyptus private cloud is also called *administrator web interface*. This is because administrators have more management tasks to achieve using this interface, comparing with the tasks that can be performed by users, who have other management alternatives. In the same time, the tasks of administrator using the web based management interface are smaller than the tasks of administrator using other management options. But, this administrator web interface plays a significant role because it's the first interaction of users with Eucalyptus private cloud, who realizes the provisioning operation, which should be accepted by administrator. The management operations that are accessible by users are: user provisioning, catalog of available images, while administrators had the following management functionalities: Identity Management (adding users, user accounts Management), Configuration Management, Catalog of available images, Catalog of services [Euc12a], [Lon+12b].

The access of the users to the Eucalyptus administrative graphical interface is realized through the following URL: https://192.168.1.50:8443, where „192.168.1.50" is our front-end hostname [Euc12a], [Lon+12b].

II. **Client tools**

The client tools presented in this section encompasses the EC2 functionality of Eucalyptus cloud. Several management tools are discussed in order to provide an overview of these tools and to present the advantages and disadvantages of each client tools. First the command line based management (euca2ools) is discussed. Then an overview of a client Java library called Typica is presented as well. After that, several Graphical User Interfaces (GUIs) are discussed: Firefox Plugins, Cloud42, tAWS Tanacasino and EC2 Dream.

**a. Command line based management (euca2ools)**

**Euca2ools** is based on Web-services software packages (Axis2, Apache and Rampart) and it has capabilities identical with Amazon EC2 [Sem+n.d], [Nur+08]. The authentication procedure to the Euca2ool requires obtaining the needed keys via a zip file which must be downloaded by users [Sem+n.d]. WS-security mechanisms are the solution for authentication, especially the X.509 credentials [Euc09], [Ubu,n.d], [Lon+12b].

The end-user interacts with Eucalyptus using euca2ools client software, which provides the following management drivers: SSH key management, security group management, image management, instance management, storage

management and IP address management. These management functionalities (Table 5.3) of Euca2ools are well documented, which helps the Eucalyptus users. Table 5.3 also present a limitation of euca2ools: it is slower compared with GUI clients, because it is a command line tool, which marks the lack of convenience functions.

Table 5.3. Euca2ools evaluation [Lon+12b]

| Command line tool | Strenghts | Limitations |
|---|---|---|
| **Euca2ools** | - management drivers: SSH key management, security groups management, image management, instance management, storage management and IP address management<br>-it is well documented | -lack of convenience functions |

### a. API Client: Typica

**Typica** is a client Java library very useful for Java developers who work with the Amazon web services. Even if it has a poor documentation and it accesses the Amazon's API at a low level, Typica was used in several projects (e.g. enStratus, g-Eclipse, AWS Manger, Cloud Studio, Elastic Web etc). Table 5.4 emphasizes the advantages and disadvantages of Typica [Euc12b], [Goo11b], [Bit08], [Lon+12b].

Table 5.4. Typica evaluation [Lon+12b]

| | Strengths | Limitations |
|---|---|---|
| **Typica** | -reliable client Java library for a variety of Amazon web services<br>-convenient for Java developers | -poor documentation<br>-access the Amazon's API at a low level |

### a. Graphical User Interfaces (GUI)

**Firefox Plugins** are graphical user interface and were built as an extension of Mozilla Firefox. First, it appeared the Elasticfox plugin, which had the advantages of managing the Amazon EC2 accounts and it is an easy to use interface. But, because of the restriction limitation to EC2 environment, it was deployed the Hybridfox plugin, which provides compatibility between a public cloud (Amazon) and a private cloud (Eucalyptus) and in the same time it supports more features of Eucalyptus than Elasticfox, being an extended Elasticfox project. Now, Elasticfox also provides managing features for Eucalyptus accounts, but it is not working properly. Both Firefox Plugins have an easy to use interface, but they had the

disadvantage of being installed locally on the user device. An evaluation with strengths and limitations of Firefox Plugins is presented in Table 5.5 [Bit08], [Goo11a], [CSS09], [Lon+12b].

Table 5.5. Firefox Plugins evaluation [Lon+12b]

| Firefox Plugins | Strengths | Limitations |
|---|---|---|
| **Elasticfox** | -manages Amazon EC2 and Eucalyptus accounts<br>-easy to work with it, no need to separate documentation | -it is not web based<br>-restricted to EC2 environment<br>-do not have the ability to copy files between instances |
| **Hybridfox** | -provides compatibility between Amazon and Eucalyptus clouds<br>-supports more features of Eucalyptus than Elasticfox<br>-easy to work with it | -it is not web based |

**Cloud42** is an open-source management interface for every EC2 compatible services, which includes two types of interfaces: web-based GUI and web service interface. Table 5.6 summarizes this important advantage of Cloud42 together with others strengths and limitations. Cloud42 also provides basic and extended functionality (e.g. file transfer functionalities from an EMI instance into another EMI instance, controlling EC2 server instances remotely) [Euc12b], [Bit08], [jus11]. One of the limitations of Cloud42 is that it doesn't have the support for Elastic IP addresses [Bit08], feature that exists in Eucalyptus cloud [Lon+12b].

Table 5.6. Cloud42 Evaluation [Lon+12b]

| | Strengths | Limitations |
|---|---|---|
| **Cloud42** | - two interfaces types: web-based GUI and web service interface<br>- provides basic and extended functionality | -support for Elastic IP addresses is missing |

**tAWS Tanacasino** is another GUI management tool for Amazon EC2, which should be installed and provides the same functionality like the Firefox plugin Elasticfox. Thus it is an easy to use GUI, but it is used only locally on the user device (Table 5.7) [Euc12b], [Lon+12b].

Table 5.7. tAWS Tanacasino Evaluation [Lon+12b]

| | Strengths | Limitations |
|---|---|---|
| **tAWS Tanacasino** | -Eclipse GUI management tool for Amazon EC2<br>-easy to work with it<br>-provides basic functionality | -it is not web based |

**EC2 Dream** is a free desktop admin client which has the same functionalities like Amazon EC2 command line. It is a hybrid cloud admin which manages the Amazon EC2, RDS, Eucalyptus, OpenStack Compute and CloudStack. Table 5.8 shows also the EC2 limitations: the documentation of EC2 Dream is poor and it has the locally installed software limitation [Euc12b], [Lon+12b].

Table 5.8. EC2 Dream Evaluation [Lon+12b]

| | Strengths | Limitations |
|---|---|---|
| **EC2 Dream** | -free desktop admin client<br>-same functionalities like Amazon EC2 | -poor documentation<br>-it is not web based |

### *a. Third party cloud management tools*

The cloud management is a subject approached by researchers in the community and this can be observed by the big number of third party cloud management providers (i.e. Right Scale, enStratus, IMOD Kaavo, CloudWatch, Scarl, Tapin, Cloudkick). This third party cloud management tools are used in special by organization which want to manage their cloud infrastructure. All of these are commercial versions and provide free trials for a number of weeks (i.e. 1 or 2 weeks), with exception that Right Scale gives the opportunity to create free account in order to manage the Eucalyptus cloud [Lon+12b].

In this way, Right Scale 3rd party management was tested. It creates an optimized user experience by providing a Dashboard with the cloud resources pool, which are automated [Rig12].

It was created a Eucalyptus Community Cloud (ECC) account in order to realize experiments with the IaaS service provided by the Eucalyptus team. Then, it was added this ECC private cloud to a Right Scale account. Right Scale is a web management interface, for analyzing the features of this interface for the existing cloud infrastructure (Fig. 5.4).


Fig. 5.4. Right Scale Web Interface [Lon11b]

Like Eucalyptus, Right Scale has the capability to assign volumes to the instances (Fig. 5.5) and the newly attached block storage can be seen (Fig. 5.6).

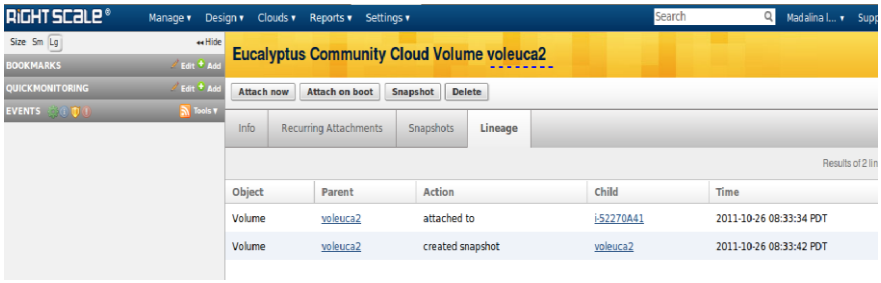


Fig. 5.5. Right Scale – Cloud Volumes Attached [Lon11b]

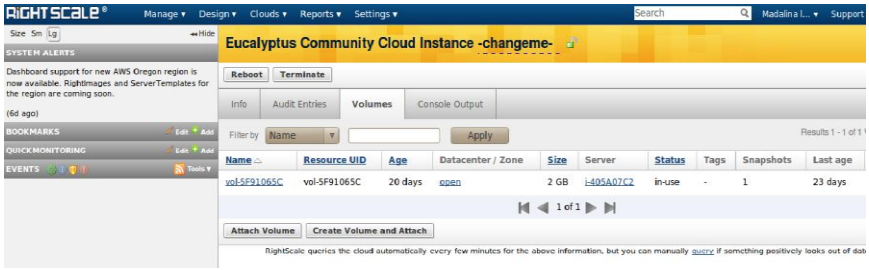


Fig. 5.6. Cloud Instances [Lon11b]

## 5.4. Euca2ools Operations

The first operations in Eucalyptus cloud environment is the registration of cloud controller, walrus, cluster controller, storage controller and nodes. After registering the nodes, they will be available into the eucalyptus.conf file and there are 2 situations to see them, even if go the "/etc/eucalyptus/eucalyptus.conf" file is checked or the "grep NODES /etc/eucalyptus/eucalyptus.conf" command is executed [Euc12c], [Lon12].

The private cloud is working properly because the „euca-describe-availability-zones verbose" command shows our available resources [Euc12c].Thus we can create three instances in total, from which two of them can be created using a 'medium' image type (i.e. 256 RAM + 1 CPU) and another one to be 'small' image type (i.e. 128 RAM + 1 CPU) or we can create three instances using the 'small' image type [Lon12].

The euca2ools operations are focused on working with instances and volumes. The possible operations with instances are emphasized in Table 5.9 and the lifecycle of the states can be observed (i.e. pending, running, shutting-down and terminated) [Joh+10], [Kar+11] together with the assignment of public IP address (192.168.1.55) and private IP address (172.16.10.66) for the created instance in this case. The range of the private IP addresses was stored into "/etc/dhcp.conf" file (i.e. 172.16.10.10 -> 172.16.10.250), while the range of the public IP addresses was written into "/etc/eucalyptus/eucalyptus.conf" file (i.e. 192.168.1.55 -> 192.168.1.60) [Euc12c], [Lon12].

The operations accessible with storage volumes are: creation, attachment / detachment to an instance and deletion. When the volume is attached to an instance, the state of the volume will be changed from „available" to „in-use" [Euc12c], [Lon12].

Table 5.9. The lifecycle of a euca2ools image [Lon12]

| *euca-run-instances emi-E7EC10AA -k mykey -t m1.small* | *euca-describe-instances* | *euca-describe-instances* | *euca-terminate-instances* | *euca-describe-instances* |
|---|---|---|---|---|
| i-375E0723 emi-E7EC10AA **0.0.0.0 0.0.0.0 pending** mykey | i-375E0723 emi-E7EC10AA **192.168.1.55 172.16.10.66 pending** mykey | i-375E0723 emi-E7EC10AA 192.168.1.55 172.16.10.66 **running** mykey | i-375E0723 emi-E7EC10AA 192.168.1.55 172.16.10.66 **shutting-down** mykey | i-375E0723 emi-E7EC10AA 192.168.1.55 172.16.10.66 **terminated** mykey |

## 5.5. Problems and Solutions in the Private Cloud Setup

This section comprises several important problems that were met on the private cloud setup. These issues and the corresponding solutions were identified during the cloud operation's manipulation. Some of the issues were found in the troubleshooting Eucalyptus section of Eucalyptus Administrator's Guide, while others were discovered as problems solved by the Eucalyptus community in the Engage question and answers section [Euc12d], [Lon12].

Availability of cloud resources is tested with „euca-describe-availability-zones verbose" command and it should not return „000/000". This concern was figured out adopting the troubleshooting Eucalyptus section of Eucalyptus Administrator's Guide [Euc12a]. The solution was to de-register and register again the cluster and nodes components [Lon12].

Another problem encountered in the private cloud is with the Internet access of the created instances. It was observed that at one moment the instances and the nodes did not have Internet access. The issue of Internet access registered in the instances was solved by adding the following rule into the "/etc/rc.d/rc.local" file of the front-end server [Lon12]:

*iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth0 -j SNAT --to-source 192.168.1.50*

The above rule allows the communication among the private addresses of the VMs (172.16.1.0/24) and the public addresses (192.168.1.50) [Euc12d], [Lon12].

Also, regarding the VMs usage, another problem encountered was that the installation procedure was not possible at a time. The approached solution was to modify the following file "/etc/apt/sources.list", by deleting the existing two lines and adding the following lines [Ser12], [Lon12]:

*deb http://archive.debian.org/debian/ lenny main contrib non-free*
*deb-src http://archive.debian.org/debian/ lenny main contrib non-free*
*deb http://archive.debian.org/debian-security lenny/updates main contrib non-free*
*deb-src http://archive.debian.org/debian-security lenny/updates main contrib non-free*
*deb http://archive.debian.org/debian-volatile lenny/volatile main contrib non-free*
*deb-src http://archive.debian.org/debian-volatile lenny/volatile main contrib non-free*

Besides the mentioned problems with VMs, the private cloud has presented problems with the storage volumes. Problems with volumes could appear if there are not correctly mounted, detached and un-mounted. For mounting and un-mounting the volumes, a script "start_ebs.sh" was created inside the volume that was attached to an instance. This script was taken from [Euc12c] (i.e. install a service into an EBS volume) and it contains the mounting and un-mounting services in order to facilitate the manipulation of these mandatory services every time when we enter and get out of the instance by starting and stopping the script. However, after restarting the Eucalyptus services, the old volumes could not be attached to a new instance, due to the fact that lvm2 (Logical Volume Management) was inactive. The sign of this issue underlined that the state of the volumes remains „available" instead of changing to „in-use". For solving this dilemma, three recovery steps discussed in [Can12] were followed. After processing them, the result of attaching the old volume to a new instance was obtained [Lon12].

## 5.6. Conclusions

This chapter presented the deploying of a private cloud using Eucalyptus open-source. First, the Eucalyptus architecture was described, in order to discuss the components of Eucalyptus architecture and to emphasize how the virtual machines scheduling is realized.

Further, the deployment of the private cloud was explained. Thus, the cloud topology used (i.e. a front-end and three nodes) together with their hardware configurations were illustrated. The private cloud deployment had showed that a single virtual machine (VM) can be created in each node, because of the hardware configurations of our system.

For managing the Eucalyptus private cloud, several tools can be used: the web based interface and the client tools (i.e. command line interface euca2ools, Application Programming Interface - API client, graphical user interface and the third party management tools). However euca2ools was mainly used and a delay time to create instances and storage volumes was remarked.

Additionally, the encountered problems during the installation and during the manipulations of the Eucalyptus platform, reveals that the robustness of Eucalyptus is related with the fact that Eucalyptus is under development being open-source software. However, the advantage of Eucalyptus of providing interfaces compatible with Amazon Web Services (AWS) constitutes the motivation of selecting it to create an experimental cloud platform.

# 6. EXPERIMENTAL RESULTS AND EVALUATION ON DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS IN EUCALYPTUS PRIVATE CLOUD

Cloud computing technology is in continuous development and with numerous challenges regarding security. In this context, one of the main concerns for cloud computing is represented by the trustworthiness of cloud services. This problem requires prompt resolution because otherwise organizations adopting cloud services would be exposed to increased expenditures while at a greater risk.

There are two things that cloud service providers should guarantee all the time: connectivity and availability, and if there are not met, the entire organizations will suffer high costs [Per11].

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks appear to be the main threats of cloud services. While DoS attacks make the cloud service unavailable for authorized users by overloading the server that provides the cloud service with a large number of requests, DDoS attacks make the cloud service unavailable by overloading the victim server from distributed master locations utilizing the slave platforms [Bha+11].

This chapter is focused on detecting and analyzing Distributed Denial of Service (DDoS) attacks in cloud computing environment. One of the efficient methods for detecting DDoS is to use the Intrusion Detection Systems (IDS), in order to assure usable cloud computing services [Ros+09]. However, IDS sensors have the limitations that: they yield massive amount of alerts and produce high false positive rates and false negative rates [Yu+04].

With regards to these IDS issues, the proposed solution from [Lon+12c] aims to detect and analyze Distributed Denial of Service (DDoS) attacks in cloud computing environments, using Dempster-Shafer Theory (DST) operations in 3-valued logic and Fault-Tree Analysis (FTA) for each VM-based Intrusion Detection System (IDS). The basic idea is to obtain information from multiple sensors, which are deployed and configured in each virtual machine (VM). The obtained information is integrated in a data fusion unit, which takes the alerts from multiple heterogeneous sources and combines them using the Dempster's combination rule. Our approach represents the imprecision and efficiently utilizes it in IDS to reduce the false alarm rates.

Specifically, the proposed solution combines the evidences obtained from Intrusion Detection Systems (IDSs) deployed in the virtual machines (VMs) of the cloud system with a data fusion methodology within the front-end.

The proposed solution can also solve the problem of analysing the logs generated by sensors, which seems to be a big issue [Lee+11].

The experimental results of the proposed solution were evaluated in our paper [Lon+12d] and section 6.6 from this chapter presents the results and evaluation.

## 6.1. Dempster-Shafer Theory (DST)

Dempster-Shafer Theory is established by two persons: Arthur Dempster, who introduced it in the 1960's and Glenn Shafer, who developed it in the 1970's [Che+06], [Lon+12c].

As an extension of Bayesian inference, Dempster-Shafer Theory (DST) of Evidence is a powerful method in statistical inference, diagnostics, risk analysis and decision analysis. While in the Bayesian method probabilities are assigned only for single elements of the state space (Ω), in DST probabilities are assigned on mutually exclusive elements of the power sets of possible states [Sia+03], [Sia+05], [Lon+12c].

According with DST method, for a given state space (Ω) the probability (called mass) is allocated for the set of all possible subsets ofΩ, namely $2^{\Omega}$ elements. Consequently, the state space (Ω) is also called *frame of discernment,* whereas the assignment procedure of probabilities is called *basic probability assignment* (bpa) [Gut91], [Sia+03], [Sia+05], [Lon+12c].

We will apply the particular case of DST, i.e., the DST operations in 3-valued logic using the fault-tree analysis (FTA), adopted by Guth [Gut91]. Thus, if a standard state space Ω is {True, False}, then $2^{\Omega}$ should have 4 elements: {Φ, True, False, (True, False)}. The (True, False) element describes the imprecision component introduced by DST, which refers to the fact of being either true or false, but not both. DST is a useful method for fault-tree analysts in quantitatively representing the imprecision [Gut91]. Another advantage of DST is it can efficiently be utilized in IDS to reduce the false alarm rates by the representation of ignorance [Esm97], [Sia+03], [Sia+05], [Lon+12c].

Moreover, for the reason that in DST the [sum of all masses] = 1 and m(∅) = 0, we have the following relation:

$$m(True) + m(False) + m(True, False) = 1 \tag{6.1}$$

In order to analyze the results of each sensor we'll use the fault tree analysis, which can be realized by boolean OR gate. Table 6.1 describes the Boolean truth table for the OR gate [Lon+12c].

Table 6.1. Boolean truth table for the OR gate

| | | $b_1$ | $b_2$ | $b_3$ |
|---|---|---|---|---|
| | v | T | F | (T,F) |
| $a_1$ | T | T | T | T |
| $a_2$ | F | T | F | (T,F) |
| $a_3$ | (T,F) | T | (T,F) | (T,F) |

From Table 6.1 we have:

$$m\{A\} = \{a1, a2, a3\} = \{m(T), m(F), m(T, F)\} \tag{6.2}$$

$$m\{B\} = \{b1, b2, b3\} = \{m(T), m(F), m(T,F)\} \tag{6.3}$$

⇨

$$m\{AvB\} = (a1b1 + a1b2 + a1b3 + a2b1 + a3b1; a2b2; a2b3 + a3b2 + a3b3) = (a1 + a2b1 + a3b1; a2b2; a2b3 + a3b2 + a3b3) \tag{6.4}$$

At the last step, our solution applies the Dempster's combination rule, which allows fusing evidences from multiple independent sources using a conjunctive operation (AND) between two bpa's $m_1$ and $m_2$ , called the joint $m_{12}$ [Sen+02], [Lon+12c]:

$$m_{12}(A) = \frac{\sum_{B \cap C = A} m1(B)m2(C)}{1 - K} \text{ when } A \neq \emptyset \tag{6.5}$$

$m_{12}(\emptyset) = 0$

Where $K = \sum_{B \cap C = \varphi} m1(B)m2(C)$

The factor 1-K, called *normalization factor*, is constructive for entirely avoiding the conflict evidence [Lon+12c].

Data fusion is also applied in real world examples: robotics, manufacturing, remote sensing and medical diagnosis, as well in military threat assessment and weather forecast systems [Dis08], [Lon+12c].

Sentz and Ferson [Sen+02] demonstrated in their study that Dempster's combination rule is suitable for the case that the sources of evidences are reliable and a minimal conflict or irrelevant conflict is generated [Lon+12c].

## 6.2. Proposed Solution

In order to detect and analyze Distributed Denial of Service (DDoS) attacks in cloud computing environments, the solution presented in Fig. 6.1 was proposed. For illustration purpose, a private cloud with a front-end and three nodes is set up. Whilst the detection stage is executed within the nodes, more precisely inside the virtual machines (VMs), where the Intrusion Detection Systems (IDSs) are installed and configured; the attack's assessment phase is handled inside the front-end server, in the Cloud Fusion Unit (CFU) [Lon+12c].

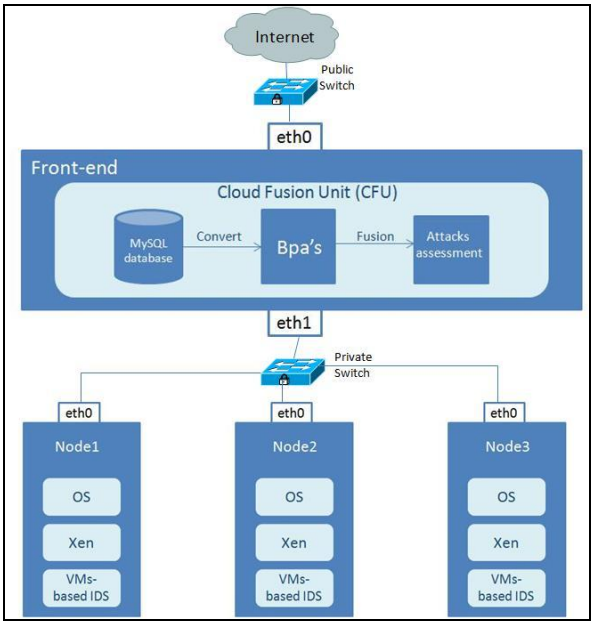


Fig. 6.1. IDS Cloud Topology [Lon+12c]

The first step in the proposed solution includes the deployment stage of a private cloud using Eucalyptus open-source version 2.0.3. The topology of the implemented private cloud is: a front-end (with Cloud Controller, Walrus, Cluster Controller, and Storage Controller) and a back-end (i.e. three nodes). The Managed networking mode is chosen because of the advanced features that it provides and Xen hypervisor is used for virtualization [Lon+12c].

Then, the VM-based IDS are created, by installing and configuring Snort into each VM. The reason of using this IDS location is because the overloading problems can be avoided and the impact of possible attacks can be reduced [Maz+10], [Ros+09], [Lon+12c].

These IDSs will yield alerts, which will be stored into the Mysql database placed within the Cloud Fusion Unit (CFU) of the front-end server. A single database is suggested to be used in order to reduce the risk of losing data, to maximize the resource usage inside the VMs and to simplify the work of cloud administrator, who will have all the alerts situated in the same place. A similar idea of obtaining and controlling the alerts received from the IDS Sensor VMs using an IDS Management Unit was presented by Roschke, et al. (2009) as a theoretical IDS architecture for cloud. A similar approach of using an IDS Management Unit is proposed in Dhage, et al. [Dha+11]. However, the proposed solution adds the capacity to analyze the results using the Dempster-Shafer theory of evidence in 3-valued logic [Lon+12c].

As showed in Fig. 6.1, the Cloud Fusion Unit (CFU) comprises three components: Mysql database, bpa's calculation and attacks assessment [Lon+12c].

I. **Mysql database**

The Mysql database is introduced with the purpose of storing the alerts received from the VM-based IDS. Furthermore, these alerts will be converted into Basic Probabilities Assignments (bpa's), which will be calculated using the pseudocode below.

**II. Basic probabilities assignment (bpa's) calculation**

For calculating the basic probabilities assignment, first we decide to the state space Ω. In this paper we use DST operations in 3-valued logic {True, False, (True, False)} suggested by Guth (1991) for the following flooding attacks: TCP-flood, UDP-flood, ICMP-flood, for each VM-based IDS. Thus, the analyzed packets will be: TCP, UDP and ICMP. Further, a pseudocode for converting the alerts received from the VM-based IDS into bpa's is provided. The purpose of this pseudocode is to obtain the following probabilities of the alerts received from each VM-based IDS [Lon+12c]:

*($m_{UDP}(T)$, $m_{UDP}(F)$, $m_{UDP}(T,F)$ )*
*( $m_{TCP}(T)$, $m_{TCP}(F)$, $m_{TCP}(T,F)$ )*
*( $m_{ICMP}(T)$, $m_{ICMP}(F)$, $m_{ICMP}(T,F)$ )*

- **Pseudocode for converting the alerts into bpa's** [Lon+12c]**:**

*For each node*
*Begin*
*For each X ∈ {UDP; TCP; ICMP}:*
*Begin*
*1: Query the alerts from the database when a X attack occurs for the specified hostname*
*2: Query the total number of possible X alerts for each hostname*
*3: Query the alerts from the database when X attack is unknown*
*4: Calculate the Belief (True) for X, by dividing the result obtained at step 1 with the result obtained at step 2*
*5: Calculate the Belief (True, False) for X, by dividing the result obtained at step 3 with the result obtained at step 2*
*6: Calculate Belief (False) for X: {1- Belief (True) – Belief (True, False)}*
*End*
*End*

Furthermore, after obtaining the probabilities for each attack packet (i.e. UDP, TCP, ICMP) for each VM-based IDS, the probabilities for each VM-based IDS should be calculated following the fault-tree as shows in Fig. 6.2 [Lon+12c].

Fig. 6.2 reveals only the calculation of the probabilities (i.e. $m_{S1}(T)$, $m_{S1}(F)$, $m_{S1}(T,F)$ ) for the first VM-based IDS [Lon+12c].

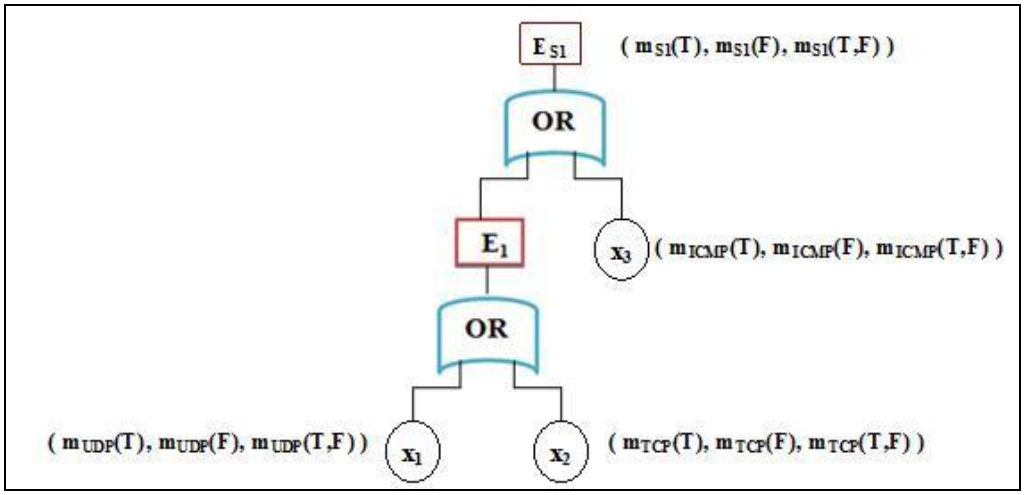


Fig. 6.2. Bpa's calculation [Lon+12c]

Thus, using the DST with fault-tree analysis we can calculate the belief (Bel) and plausibility (Pl) values for each VM-based IDS:

$$Bel(S1) = m_{S1}(T) \quad (6.6)$$

$$Pl\ (S1) = m_{S1}(T) + m_{S1}(T, F) \quad (6.7)$$

III. **Attacks assessment**

The attacks assessment consists of data fusion of the evidences obtained from sensors by using the Dempster's combination rule, with the purpose of maximizing the DDoS true positive rates and minimizing the false positive alarm rate. $m_{S1,S2}(T)$ can be calculated using Table 6.2 and equation (6.5).

Table 6.2. $m_{S1,S2}$ calculation [Lon+12c]

| | $m_{S1}(T)$ | $m_{S1}(F)$ | $m_{S1}(T, F)$ |
|---|---|---|---|
| $m_{S2}(T)$ | $m_{S1}(T) * m_{S2}(T)$ | $m_{S1}(F) * m_{S2}(T)$ | $m_{S1}(T, F) * m_{S2}(T)$ |
| $m_{S2}(F)$ | $m_{S1}(T) * m_{S2}(F)$ | $m_{S1}(F) * m_{S2}(F)$ | $m_{S1}(T, F) * m_{S2}(F)$ |
| $m_{S2}(T, F)$ | $m_{S1}(T) * m_{S2}(T, F)$ | $m_{S1}(F) * m_{S2}(T, F)$ | $m_{S1}(T, F) * m_{S2}(T, F)$ |

## 6.3. Related Work

### 6.3.1. Intrusion Detection Systems (IDS) in Cloud Computing

One of the IDS strategies proved reliable in cloud computing environments is its applicability to each virtual machine. This is the method we'll choose for our proposed solution. Mazzariello, et al. (2010) [Maz+10] presented and evaluated this method in comparison with another IDS deployment strategy, which uses single IDS

near the cluster controller. IDS applied to each virtual machine in cloud computing platform eliminate the overloading problem, because in a way the network traffic is split to all IDSs. Thus, applying IDS to each virtual machine gets rid of the issue of the IDS strategy near the cluster controller, which tends to be overloaded because of its necessity to monitor all the supposed traffic from the cloud computing infrastructure. Another advantage of this strategy as described by Roschke, et al. (2009) [Ros+09] is the benefit of reducing the impact of the possible attacks by the IDS Sensor VMs [Lon+12c].

However, the limitation of IDS strategy applied to each virtual machine is the missing of the correlation phase, which is suggested in the future work by Mazzariello, et al. (2010) [Maz+10], [Lon+12c].

The correlation phase will be included in the proposed solution, because beside the IDS for each virtual machine, the IDS cloud topology will include a Cloud Fusion Unit (CFU) on the front-end, with the purpose of obtaining and controlling the alerts received from the IDS sensor VMs as presented by Roschke, et al. (2009) [Ros+09] in their theoretical IDS architecture for cloud, which utilizing an IDS Management Unit [Lon+12c].

Compared to Roschke, et al. (2009) [Ros+09] who suggested the utilization of IDMEF (Intrusion Detection Message Exchange) standard, a useful component for storage and exchange of the alerts from the management unit, the alerts in the proposed solution will be stored into the Mysql database of Cloud Fusion Unit. The Cloud Fusion Unit will add the capacity to analyze the results using the Dempster-Shafer theory (DST) of evidence in 3-valued logic and the Fault-Tree Analysis for the IDS of each virtual machine and at the end the results of the sensors will be fused using Dempster's combination rule [Lon+12c].

A similar method of using a IDS Management Unit is proposed in Dhage, et al. (2011) [Dha+11], who presented a theoretical model of an IDS model in cloud computing, by using a single IDS controller, which creates a single mini IDS instance for each user. This IDS instance can be used in multiple Node controllers and a node controller can contain IDS instances of multiple users. The analysis phase of the mini IDS instance for each user takes place in the IDS controller. Compared with Roschke, et al. (2009) [Ros+09] where the emphasis is on how to realize the synchronization and integration of the IDS Sensor VMs, in Dhage, et al. (2011) [Dha+11] the focus is to provide a clear understanding of the cardinality used in the basic architecture of IDS in cloud infrastructure [Lon+12c].

Applying the IDS for each virtual machine is an idea suggested also by Lee, et al. (2011) [Lee+11], who increases the effectiveness of IDS by assigning a multi-level intrusion detection system and the log management analysis in cloud computing. In this sense the users will receive appropriate level of security, which will be emphasized on the degree of the IDS applied to the virtual machine, and as well on the prioritization stage of the log analysis documents. This multi-level security model solves the issue of using effective resources [Lon+12c].

Lo, et al. (2010) [Lo+10] proposed a cooperative IDS system for detecting the DoS attacks in Cloud Computing networks, which has the advantage of preventing the system from single point of failure attack, even if it is a slower IDS solution than a pure Snort based IDS. Thus, the framework proposed by Lo, et al. (2010) [Lo+10] is a distributed IDS system, where each IDS is composed of three additional modules: block, communication and cooperation, which are added into the Snort IDS system [Lon+12c].

### 6.3.2. IDS using Dempster-Shafer Theory

Dempster-Shafer Theory (DST) is an effective solution for assessing the likelihood of DDoS attacks, which was demonstrated by several research papers in the context of network intrusion detection systems. Dissanayake [Dis08] presented a survey upon intrusion detection using DST [Lon+12c].

This study is detecting DDoS attacks in cloud computing environments. Dempster-Shafer Theory (DST) is used to analyze the results received from each sensor (i.e. VM-based IDS) [Lon+12c].

Data used in experiments using DST vary: Yu and Frincke (2005) [Yu+05] used DARPA DDoS intrusion detection evaluation datasets, Chou et al. (2008) [Cho+08] used DARPA KDD99 intrusion detection evaluation dataset, Chen and Aickelin (2006) [Che+06] used the Wisconsin Breast cancer dataset and IRIS plant data, while others scientists generated their own data [Sia+05]. The data to be used in the proposed solution will be generated by ourselves, by performing DDoS attacks using specific tools against the VM-based IDS [Lon+12c].

Siaterlis, et al. (2003) [Sia+03] and Siaterlis and Maglaris (2005) [Sia+05] performed a similar study of detecting DDoS using data fusion and their field was an operational university campus network, while in this solution the DDoS attacks are proposed to be detected and analyzed in our private cloud computing environment [Lon+12c].

Additionally, the attacks generated against the TCP, UDP, ICMP packets, are consider to be analyzed, like Siaterlis, et al. (2003) [Sia+03] and Siaterlis and Maglaris (2005) [Sia+05]. However, instead of applying DST on the state space $\Omega$= {Normal, UDP-flood, SYN-flood, ICMP-flood}, our study uses DST operations in 3-valued logic as suggested by Guth (1991) [Gut91] for the same flooding attacks: TCP-flood, UDP-flood, ICMP-flood, for each VM-based IDS. Like Siaterlis and Maglaris (2005) [Sia+05], Chatzigiannakis, et al., (2007)[Cha+07] chosen the same frame of discernment, while Hu, et al. (2006) [Hu+06] used a state space: {Normal, TCP, UDP and ICMP} [Lon+12c].

Furthermore, compared with the study performed by Siaterlis, at al. (2003) and Siaterlis and Maglaris (2005) [Sia+05], who use a minimal neural network at the sensor level, the proposed solution will assign the probabilities using: DST in 3-valued logic, the pseudocode and the fault tree analysis [Lon+12c].

Whilst the computational complexity of DST is increasing exponentially with the number of elements in the frame of discernment [Dis08], the DST 3-valued logic proposed to be used in this research will not encounter this issue, which will meet the efficiency requirements in terms of both detection rate and computation time [Lo+10], [Lon+12c].

Finally, the data fusion of the evidences obtained from sensors studied by Siaterlis and Maglaris (2005) [Sia+05] will be used in this study. The data fusion will be realized using the Dempster-Shafer combination rule, which was demonstrated in Siaterlis and Maglaris (2005) [Sia+05] for its advantages, i.e., maximization of DDoS true positive rates and minimization of the false positive alarm rate, by combining the evidence received from sensors. Therefore, the work of cloud administrators will be alleviated, whereas the number of alerts will decrease [Lon+12c].

## 6.4. Implementation of the Proposed Solution

The proposed Intrusion Detection System (IDS) Cloud topology [Lon+12c] is shown in Fig. 6.1. It presents the Eucalyptus private architecture, the procedure of creating the virtual machines based IDS (VMs-based IDS) and the installation and configuration of Mysql database together with the graphical interfaces for monitoring the alerts in the Cloud Fusion Unit (CFU) of the front-end server from the Eucalyptus cloud architecture. The others two components (i.e. Basic probabilities assignment and Attacks Assessment) from the Cloud Fusion Unit (CFU) are discussed in section 6.6 of this chapter.

The IDS Cloud Topology was implemented in the Eucalyptus private cloud environment, that was described on chapter 5.

Furthermore, the VMs-based IDS were created and Debian-based euca2ools images were utilized. The experimental results were conducted for three Debian virtual machines: one image is Debian 32-bit architecture and the other two are Debian 64-bit architectures. The operations for creating the VM-based IDS are similar for all three images and only the type of software differs based on the bit architecture (e.g. 32 or 64). The creation of the VMs-based IDS consists of the following six operations (Fig. 6.3) [Lon+12d], using the Eucalyptus User's Guide [Euc12c], the Snort installation guides [Wei12], [Moo11], [Har07], the Snort Users Manual [Sou11] and [Reh03], [Bak+07]:

***Step 1.*** Debian (e.g. 32 and 64 bit architecture) pre-packaged virtual machines were downloaded from Eucalyptus website. Afterwards, the images were bundled, uploaded and registered into our private cloud. These initial steps at the creation of the images are recorded in the image management section of Eucalyptus User's Guide [Euc12c].

***Step 2.*** Furthermore, those images were utilized at the deployment of instances.

***Step 3.*** Then, a Eucalyptus storage volume of 5 GB was created in order to be attached to the created instance.

***Step 4.*** Moreover, the VMs-based IDS were deployed by installing and configuring Snort open-source Network based Intrusion Detection System (NIDS) into the VMs. The reason for selection of this NIDS is because of its characteristics: it has packet payload; its decoded output display is user friendly and its output analysis is high performed [Van+12]. Moreover, Snort was configured for defending against DDoS tools. In this sense the predefined DDoS rules were included in the snort configuration file. The attacks capturing procedure is made using the Barnyard tool, which stores in a binary unified file all the events with the purpose to send them to a centralized Mysql database in front-end, using a secure tunnel (i.e. stunnel) [Wei12], [Moo11], [Har07], [Sou11], [Reh03], [Bak+07], [Bre02], [Bor+10]. The VMs-based IDS were configured to send all the collected data to the Mysql database using Snort together with Barnyard. Thus, the "barnyard2.conf" file on each VM-based IDS includes the following output [Wei12], [Moo11], [Har07]:

*"output database: alert, mysql, user=snort password=xxxxxx dbname=snortdata host=192.168.1.50".*

After the installation and configuration of the VM-based IDS was completed, the volume was un-mounted.

***Step 5.*** In order to have a working storage volume, the Eucalyptus volume should be detached from the instance [Euc12c].

***Step 6.*** We created backup of the above volume by deploying snapshot element [Euc12c].

After the VMs-based IDS were deployed, we started Snort and Barnyard in all three VMs-based IDS and we conducted DDoS attacks against these three VMs-based IDS using Stacheldraht tool. Snort is started with the following command: "snort -c /etc/snort/snort.conf -i eth0", while barnyard is started with: "/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /etc/snort/barnyard.waldo -G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map -C /etc/snort/classification.config" [Lon+12d].

| |
|---|
| Step 1. Register Debian pre-packed VMs |
| Step 2. Deploy instances |
| Step 3. Create the Eucalyptus storage volume |
| Step 4. Install and configure Snort into the VMs |
| Step 5. Detach the Eucalyptus volume |
| Step 6. Deploy snapshot of the volume |

Fig. 6.3. VM-based IDS Deployment [Lon+12d]

The integration of IDS in Eucalyptus cloud was reported in the literature. Borisaniyia et al. (2010) [Bor+10] presents their experimental setup of the Snort network-based intrusion detection into the Cluster Controller components of Eucalyptus private cloud and the analysis of the capture attacks transmitted every minute by IDS to the Mysql server, which is located in the Cloud Controller component of Eucalyptus. The placement of IDS in our proposed solution is into the VMs (Fig. 6.1), which reveals a different approach comparing with the experimental setup revealed by Borisaniyia et al. [Bor+10]. However, the centralization of the distributed sensors is recorded in a single Mysql server as in the solutions given by Borisaniyia et al. (2010) [Bor+10], Brennan (2002) [Bre02], Skinner (2012) [Ski12], [Lon+12d].

Furthermore, the implementation of the proposed solution enhances the collaboration of the VMs-based IDS with the front-end component of the private cloud, by receiving the alerts transmitted by VMs-based IDS into Mysql server [Bre02], [Ski12]. The alert's transmission is secured because Stunnel is installed in the front-end (Fig. 6.4) [Lon+12d].

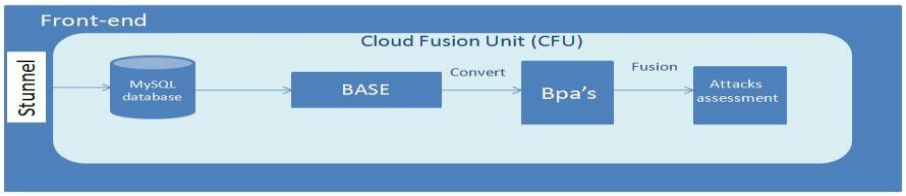


Fig. 6.4. Relationships of the centralization components in Cloud Fusion Unit [Lon+12d]

Fig. 6.4 is an extended scheme of the CFU component from Fig. 6.1. The data analysis tool (i.e. BASE - Basic Analysis and Security Engine) was introduced between the storing server (i.e. Mysql) and the Basic probabilities assignment (Bpa's) component. BASE is the successor of ACID (Analysis Control for Intrusion Detection) [Bak+07]. BASE was chosen because it is a web server analysis tool for monitoring the alerts received from the VM-based IDS sensors [Reh03]. Additionally, its reporting strategy facilitates the procedure of obtaining the Bpa's [Lon+12d].

## 6.5. Generating DDoS Attacks

DDoS attacks against the VMs-based IDS using the Stacheldraht DDoS tool were simulated. Stacheldraht tool is based on the 'Client', 'Handler (s)/Master (s)', 'Agent(s)/Daemon(s)', 'Victim(s)' architecture. This three layer architecture includes the collaboration of three distributed servers (i.e. client –telnetc, master- mserv, daemon - td). Stacheldraht combines the characteristics of both Trinoo and TFN (Tribe Flood Network) DDoS attack tools and provides two additional features: an encrypted client to handler communication and the agents are automatically remotely updated [Dit99], [Cri00], [Lon+12d].

The types of DDoS attacks involved in this experiment are: *bandwidth depletion attacks* (i.e. ICMP- Internet Control Message Protocol flood attacks, UDP- User Datagram Protocol flood attacks) and *resource depletion attacks* (i.e. TCP SYN – Transfer Control Protocol Synchronize attacks) [Spe+04], [Mir+04], [Lon+12d].

*ICMP flood attack* attempts to make the victim host unavailable by sending ICMP requests to the victim using spoofed source addresses. Thus, the consumption of resources to receive back those replies from the target to the attacker is eliminated and only the victim is responsible to handle large amounts of requests and replies [Cri00], [Nor+02], [Lon+12d].

*TCP SYN flood attacks* exhaust the victim by sending SYN packets to the target with invalid IP source addresses. The consequence of this action is seen in the absence of the ACK packets back to the victim, which makes the TCP connection unattainable [Cri00], [Nor+02]. In this sense, the TCP services of the target site become unavailable for authorized users [Cri00], [Lon+12d].

While TCP is a connection oriented protocol, UDP is connectionless. This difference between UDP and TCP makes UDP flood attack more difficult to be realized. The strategy adopted by UDP flood attack is based on sending UDP packets to dead ports from the target site. The life-threatening consequences of UDP flood attacks are produced not only against the target host and also against the hosts on the same segment [Cri00], [Nor+02] , [Lon+12d].

## 6.6. Results and Evaluation

The created Mysql database (i.e. snortdata) stores the alerts received from each VM-based IDS. Our snort database consists of the 15 tables taken from snort-mysql database and the 6 ACID (Analysis Control for Intrusion Detection) tables. We have used in our experiment 4 tables from Snort database (i.e. tcphdr, udphdr,

icmphdr, sig_class) and a table from ACID database (i.e. acid_event). The views from join queries (i.e. tcp_acid_class, udp_acid_class, icmp_acid_class) (Fig. 6.5) were created, with the purpose to investigate and prioritize the DDoS events based on the following three criteria: True (i.e. a DDoS attack occurs), False (i.e. a DDoS attack doesn't occur) and (True, False) case (i.e. if the type of the event is unknown) [Lon+12d].

For example, „tcp_acid_class" view was created by matching data from „tcphdr" table, "acid_event" table and "sig_class" table as follow [w3s12], [w3s12a], [Lon+12d]:

*CREATE VIEW tcp_acid_class AS*
*(SELECT tcphdr.sid, tcphdr.cid, tcphdr.tcp_sport, tcphdr.tcp_dport,*
*acid_event.signature, acid_event.sig_class_id, acid_event.sig_priority,*
*sig_class.sig_class_name*
*FROM tcphdr*
*INNER JOIN acid_event*
*ON tcphdr.sid=acid_event.sid and tcphdr.cid=acid_event.cid*
*INNER JOIN sig_class*
*ON acid_event.sig_class_id=sig_class.sig_class_id);*

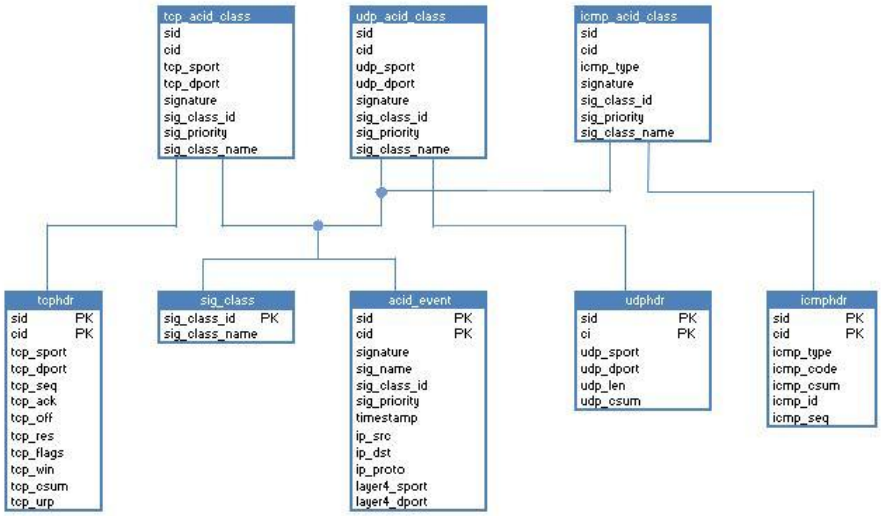


Fig. 6.5. Creating the views of join queries [Lon+12d]

In our paper [Lon+12d], we have made the assumptions that DDoS attacks are detected if the priority of the event is 1 (i.e. high) or 2 (i.e. medium) and if the priority is 3 (i.e. low) or 4 (i.e. very low) an alert will be generated.

When a DDoS attack is produced, the total number of each x $\in$ {TCP SYN, UDP, ICMP} flood attack is calculated by querying the above corresponding views based on the 'sid', 'sig_priority' and 'sig_class_name' fields. For this situation Snort reacts with one of the following actions [Sou11]: drop, sdrop or reject, protecting the virtual machines [Lon+12d].

In the case that Snort generates alerts, two possible cases: False and (True, False) were considered. The (True, False) state is recorded when the attempts to attack the VMs-based IDS are framed as "unknown" classtype. The attack classification of Snort rules is listed in Table 3.2 from the Snort Users Manual [Sou11] (see Table 6.3) and this list appears on the 'classification.config' file of Snort installation [Lon+12d].

Table 6.3. Snort Default Classifications [Sou11]

| Classtype | Description | Priority |
|---|---|---|
| attempted-admin | Attempted Administrator Privilege Gain | high |
| attempted-user | Attempted User Privilege Gain | high |
| inappropriate-content | Inappropriate Content was Detected | high |
| policy-violation | Potential Corporate Privacy Violation | high |
| shellcode-detect | Executable code was detected | high |
| successful-admin | Successful Administrator Privilege Gain | high |
| successful-user | Successful User Privilege Gain | high |
| trojan-activity | A Network Trojan was detected | high |
| unsuccessful-user | Unsuccessful User Privilege Gain | high |
| web-application-attack | Web Application Attack | high |
| attempted-dos | Attempted Denial of Service | medium |
| attempted-recon | Attempted Information Leak | medium |
| bad-unknown | Potentially Bad Traffic | medium |
| default-login-attempt | Attempt to login by a default username and password | medium |
| denial-of-service | Detection of a Denial of Service Attack | medium |
| misc-attack | Misc Attack | medium |
| non-standard-protocol | Detection of a non-standard protocol or event | medium |
| rpc-portmap-decode | Decode of an RPC Query | medium |
| successful-dos | Denial of Service | medium |
| successful-recon-largescale | Large Scale Information Leak | medium |
| successful-recon-limited | Information Leak | medium |
| suspicious-filename-detect | A suspicious filename was detected | medium |
| suspicious-login | An attempted login using a suspicious username was detected | medium |
| system-call-detect | A system call was detected | medium |
| unusual-client-port-connection | A client was using an unusual port | medium |
| web-application-activity | Access to a potentially vulnerable web application | medium |
| icmp-event | Generic ICMP event | low |
| misc-activity | Misc activity | low |
| network-scan | Detection of a Network Scan | low |
| not-suspicious | Not Suspicious Traffic | low |
| protocol-command-decode | Generic Protocol Command Decode | low |
| string-detect | A suspicious string was detected | low |
| unknown | Unknown Traffic | low |
| tcp-connection | A TCP connection was detected | very low |

The (True, False) element was introduced and modeled by Guth (1991) in the Dempter-Shafer Theory (DST) in 3-valued logic in relation with the fault-tree analysis (FTA). In this paper, a quantitative analysis of the TCP SYN flooding attacks, UDP flooding attacks and ICMP flooding attacks is carried out, in order to reduce the large amounts of false alarms rates produced by the Intrusion Detection Systems [Lon+12d].

The creation of the above three views of join queries, the total number of events when an x ∈ {TCP SYN, UDP, ICMP} flood attack occurs and the total number of events when the event is unknown, can be used to calculate the basic probability assignment for each sensor machine, according to Dempster-Shafer theory [Lon+12d].

Therefore, first the mass assignments for all three states of each sensor are defined as follows [Lon+12d]:

$$\begin{cases} m_x(T), \text{ the DDoS attack occurs} \\ m_x(F), \text{ the DDoS attack doesn't occur} \\ m_x(T, F), \text{ the "unknown" classification of the DDoS attacks.} \end{cases} \quad (6.8)$$

where x ∈ {TCP, UDP, ICMP} flood attack in the private cloud

Fig. 6.6 depicts the mass assignments calculated for two VM-based IDS, which were realized by implementing the pseudocode proposed in [Lon+12c]. Hence, first the detection rate ($m_x(T)$) for each flooding attack against each VM-based IDS was computed [Lon+12d]. The detection rate (i.e. $m_x(T)$) was defined the same as Yu and Frincke [Yu+05]:

$$Detection\ Rate\ (DR) = \frac{number\ of\ true\ attacks\ reported}{number\ of\ total\ observable\ attacks} \quad (6.9)$$

Then, the computation of the probabilities for (True, False) element was realized based on the above descriptions. $m_x(F)$ [Gut91], [Lon+12d] will be calculated by applying DST, which says that the [sum of all masses] = 1 :

$$m_x(F) = 1-m_x(T)- m_x(T, F) \quad (6.10)$$

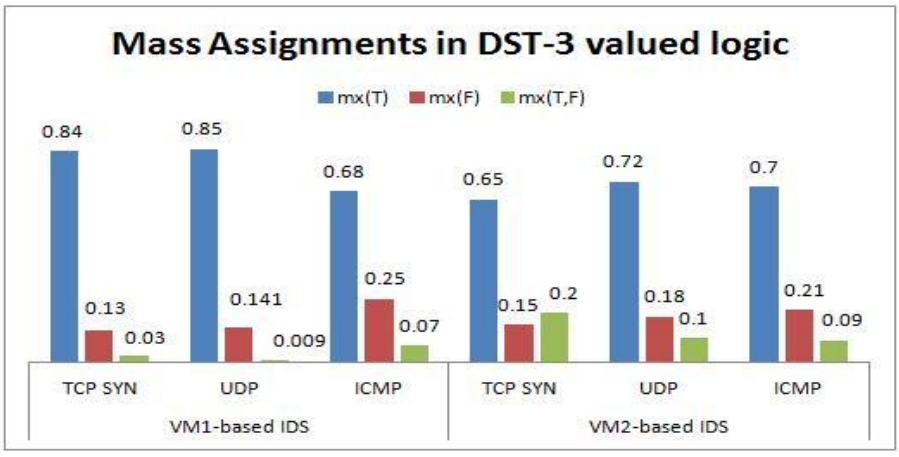


Fig. 6.6. Mass Assignments in DST [Lon+12d]

The results from Fig. 6.6 reveal a high detection rate ( $m_x(T) > 0.65$) and $m_x(F) \in [0.07, 0.25]$, obtained from the VM-based IDS, which were configured with proper rules and thresholds against the DDoS attackers [Lon+12d].

Moreover, we present in depth the analysis of the obtained results by using a Fault-Tree Analysis for each VM-based IDS and combining those Bpa's results into an attacks assessment at the end using the Dempster's combination rule [Lon+12d].

Therefore, the basic probabilities assignment will be calculated for each VM-based IDS using a Fault-Tree Analysis as described in Fig. 6.2 and using the results from Fig. 6.6.

The results obtained for each VM-based IDS are described in Table 6.4. A high detection rate and a low false rate can be seen for both VM-based IDS. Comparing the results from Fig. 6.6 with the results from Table 6.4, when a Fault-Tree Analysis is realized, we can see the decrease in the false alarm rates (i.e. $m_y(T,F)$), together with the decrease in the true negative rate (i.e. $m_y(F)$) and the increase in the detection rate (i.e. $m_y(T)$), where y denotes one of the VM-based IDS, also called sensors (i.e. S1, S2) [Lon+12d].

Table 6.4. Bpa's calculation [Lon+12d]

| ***y*** | ***$m_y(T)$*** | ***$m_y(F)$*** | ***$m_y(T,F)$*** |
|---|---|---|---|
| ***S1*** | 0.99232 | 0.004583 | 0.003098 |
| ***S2*** | 0.9706 | 0.00567 | 0.02373 |

Finally, the evidences obtained from both VM-based IDS are combined using Dempster's combination rule and the results are shown in Table 6.5 [Lon+12d].

Table 6.5. Results of Dempster's combination rule [Lon+12d]

| ***$m_{12}(T)$*** | ***$m_{12}(F)$*** | ***$m_{12}(T,F)$*** |
|---|---|---|
| 0.963146 | 0.010227 | 0.026628 |

It can be seen that the conflict generated from the two VM-based IDS (Table 6.4) is irrelevant and Table 6.5 highlights the maximization of the detection rate, together with the minimization of the false alarm rates [Lon+12d].

The results from Table 6.5 were interpreted using the evaluation metrics: overall accuracy and the error rates, as described in [Tho+08] and [Wit+05] (Table 6.6), where:

$$Overall\ Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{6.11}$$

$$Error\ Rate = \frac{FP+FN}{TP+TN+FP+FN} \tag{6.12}$$

Table 6.6. Evaluation metrics [Lon+12d]

| ***TP*** | ***TN*** | ***False rates (FN+FP)*** | ***Overall Accuracy*** | ***Error Rate*** |
|---|---|---|---|---|
| 0.963146 | 0.010227 | 0.026628 | 0.9733 | 0.0266 |

TP= true positive, TN= true negative, FP=false positive, FN= false negative

## 6.7. Conclusions

This chapter achieved the evaluation of the experiments on detecting Distributed Denial of Service (DDoS) attacks in Eucalyptus private cloud. An Intrusion Detection System (IDS) Cloud Topology was proposed, in which two virtual machines have been configured with Network IDS (NIDS) Snort to defend against DDoS attacks and the centralization, correlation and analysis of the evidences obtained from sensors has been handled in a Cloud Fusion Unit (CFU) inside the front-end machine of the private cloud. The virtual machines in which Snort was installed and configured, are called virtual machines based IDS (VM-based IDS) and the flooding attacks that were analyzed are the following: TCP SYN flooding attacks, UDP flooding attacks and ICMP flooding attacks.

The false alarm rates generated by IDSs were reduced because the proposed solution is based on the Dempster-Shafer theory in 3 valued logic, which represents the imprecision. Subsequently, the analysis conducted with the Fault-Tree Analysis (FTA) for each VM-based IDS has showed a high detection rate and a low false alarm rate.

Afterwards, because the conflict yielded by the two VM-based IDSs was irrelevant, Dempster's combination rule has produced the maximization of the detection rate and the minimization of the false alarm rate, results that were evaluated with the overall acurracy and the error rate metrics.

# 7. CONCLUSIONS

Identity security, information security and infrastructure security for cloud computing environment have been studied and enhanced in this thesis. Chapter 1 began with a theoretical background of cloud computing, which includes the comparison of cloud computing with several related technologies, the description of delivery service models, the description of deployment models and the essential characteristics of cloud computing, followed by the introduction of the proposed overall process taken by enterprises to manage the migration of their resources to the Infrastructure-as-a-Service (IaaS). Chapter 1 has also addressed the motivation, the goals and the outline of the thesis.

Furthermore, chapter 2 presented a literature review of security for cloud computing environment. Starting with the security management, chapter 2 emphasized the security issues of cloud computing from two perspectives: applications security issues and virtualization security issues. The application security issues have been referred to the wrapping attacks and to the browser security issues (i.e. account Hijaking and spoofing attacks), in accordance with their mitigation techniques that were identified. Likewise, the virtualization security issues have been evaluated together with their mitigation strategies and the discussed threats are: flooding attacks, virtual machine template image and side channel attack. From the suggested list of the mitigation techniques for each technical security threats of cloud computing, we noticed the following predominant solutions: strong authentication, filtering techniques, Intrusion Detection Systems, isolation of data and monitoring solutions, which are met as solutions for security components in cloud computing. Thus, in addition with the security management and issues that were presented, a special attention in chapter 2 was directed toward the security solutions of cloud computing: securing the identities, securing the information and securing the infrastructure, which represents the security solutions in cloud computing in terms of avoiding the security risks and eliminating the security threats. The aim of investigating the security solutions was to research the branches that require further improvement. The proposed improvements were presented in terms of securing the identities (see Chapter3 and Chapter 4) and in terms of securing the infrastructure and information (see Chapter 3 and Chapter 6).

Therefore, chapter 3 was focused on improving the security in cloud computing by proposing an architectural solution of security for cloud computing, in which securing the identities was the main objective. Other objectives of the cloud security solution have been to apply security control as well for information and infrastructure, by assigning the network security control and by isolating the data of customers. In terms of securing the identities, Identity Access Management (IAM) was explored by inquiring about current cloud IAM solutions and by creating a list with IAM requirements. The element from the proposed architectural solution of security that had introduced the IAM capability is the Cloud IAM gateway, also called IAM as a Service (IAMaaS). The Cloud IAM gateway appeared more suitable compared with the others two IAM techniques (i.e. IAM inside the private cloud of the enterprise and IAM inside the Cloud Service Provider platform). The prefference of the cloud IAM gateway was selected because it is a IAM solution which increases

the security of customers and strengthens the capability of enterprises to cooperate with Cloud Service Providers (CSPs). Nevertheless, the efficiency limitation is still a challenge because of the larger time needed to implement this IAM solution and to collaborate with CSPs and customers by establishing trust relationships. Moreover, several protocols were analyzed to fulfill the IAM security requirements. The purpose was to propose an architectural solution of security for cloud computing, which was compared with the existing related work.

In chapter 4 a proposed authentication solution for cloud computing has been provided. The proposed improvement addressed a hybrid text-image solution, which is an extension of the two level security approach of the current authentication solution in cloud computing (i.e. username and password, together with X.509 certificates for accessing the cloud services). The aim was to increase the security level of the existing authentication solution which is based on the password-based technique. This is because in the analysis conducted in the first part of the chapter 4, the password-based technique was identified as a low security level compared with the other two knowledge-based authentication techniques (i.e. image-based technique and text-image based technique). Therefore, text-image based technique was preferred because of its strengths: increasing security and increasing the recalling capabilities. Moreover, the proposed hybrid text-image based solution was designed to combine the three random images from individual image set with the individual password set, where the individual image set consists from three images that were chosen by user at the registration process from three image sets (i.e. „flowers", „animals" and „fruits" categories) and the individual password set consists from the passwords that the user had allocated at the enrolment process for each image of the individual image set. After presenting the proposed solution, the chapter introduced a complex analysis. The analysis of the proposed text-image security approach was achieved at the end of chapter 4 through the following factors: solutions for possible attacks, the time needed for registration and login and the system's usability. After the conducted analysis for inspecting our solution in terms of the possible attacks, there were highlighted several advantages. Thus, the proposed solution will protect the cloud system against shoulder surfing attacks and keystroke logging attacks, because the images from the individual image set are displayed in random positions each time at the login stage. Likewise, the system is as well protected against brute force attacks due to the hybrid keys used to authenticate users and two adjustments were suggested to strengthen the security level: the setting of an adequate time for attempt to authenticate and the setting of the number of unsuccessfull login attempts. Another attack that is avoided by using the proposed solution is the impersonation attack, due to the usage of the „flowers", „animals" and „fruits" image sets, instead of „faces" category. The reliability of the proposed technique was explored also in terms of usability requirement, which demonstrated a good recall in relation with a shorter time to register and login.

Moreover, chapter 5 presented the deployment of the Eucalyptus private cloud using the binary packages of Eucalyptus 2.0.3 open-source, which facilitates the deployment, management and executation of Infrastructure as a Service (IaaS). The purpose of this experimental part was to implement a private cloud platform, in order to use it for deploying the proposed Intrusion Detection System cloud topology from chapter 6. Chapter 5 also achieved a comparative analysis of the Eucalyptus management tools.

In chapter 6 we have proposed a solution using Dempster-Shafer Theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for each VM-

based Intrusion Detection System (IDS), in order to detect and analyze Distributed Denial of Service (DDoS) attacks in cloud computing environments. The proposed solution represents the imprecision and efficiently utilizes it in IDS to reduce the false alarm rates by the representation of the ignorance. The evaluation was conducted for two virtual machines, where Snort Network Intrusion and Detection System was installed and configured to defend against DDoS attacks. The centralization, correlation and analysis of the evidences obtained from the virtual machine based Intrusion Detection Systems (i.e. VM-based IDS) was realized in a front-end Cloud Fusion Unit. Whilst the computational complexity of DST is increasing exponentially with the number of elements in the frame of discernment, the DST 3-valued logic in the proposed solution does not have this issue, which meets the efficiency requirements in terms of both detection rate and computation time. At the same time, the usability requirement has been accomplished, because the work of cloud administrators will be alleviated by using the Dempster rule of evidence combination whereas the number of alerts will decrease and the conflict generated by the combination of information provided by multiple sensors is entirely eliminated. To sum up, by using DST the proposed solution has the following advantages: to accommodate the uncertain state, to reduce the false alarms rates, to increase the detection rate, to resolve the conflicts generated by the combination of information provided by multiple sensors and to alleviate the work for cloud administrators.

## 7.1. Thesis contributions

This thesis presents several contributions:

- The comparison study between Cloud computing and related technologies has been realized by emphasizing the differences and similarities. [Lon12] (Chapter 1)
- The overall process taken by Small and Medium-sized Enterprises to manage the migration of their applications to the Infrastructure-as-a-Service was composed. The proposed process was realized in a justified succession of interrelated activities. [Lon+12a] (Chapter 1)
- A study aiming to classify the security issues for cloud computing was conducted (i.e. application security problems and security issues of virtualization). For each type of security issue, an evaluation table was created with the corresponding threats and mitigation techniques. [Lon+13] (Chapter 2)
- The synthesis of an analysis of current Identity and Access Management (IAM) solutions for cloud computing was performed. [Lon+13] (Chapter 3)
- A design of an architectural solution of security for cloud computing has been proposed, which was realized using a multi-level decomposition structure (e.g. Layer 1-4). The first layer has included the security cloud IAM gateway (IAMaaS=IAM as a Service), in order to fulfill the specified list of IAM requirements, while the last 3 layers were focused to secure the infrastructure and the information of cloud environment, by applying the network security control and by isolating the data of customers. [Lon+11], [Lon11] (Chapter 3)

- The comparative analysis of several protocols for the cloud Identity Access Management (IAM) gateway was realized. [Lon+13] (Chapter 3)
- The definition, the design and the analysis of a novel authentication system for cloud computing, that combines the proposed hybrid text-image authentication technique with the existing cloud authentication solution have been realized. The proposed hybrid text-image authentication has been addressed in comparison with existing text-image authentication techniques and the analysis part demonstrates the performance of the improvement proposed to the initial authentication system in cloud computing, in context of security and usability. [Pop+12] (Chapter 4)
- The deployment of a private cloud using the Eucalyptus software and the completion of a comparative analysis for its management tools were performed. [Lon+12b] (Chapter 5)
- The design, the implementation, the testing and the validation of an Intrusion Detection Systems (IDS) Cloud Topology, for detecting and analyzing the Distributed Denial of Service (DoS) attacks in cloud computing have been achieved. Particular attention has been given to the efficiency requirements (i.e. detection rate and computation time) and to the usability requirement, which have been accomplished. [Lon+12c], [Lon+12d] (Chapter 6)

This thesis is supported by several research papers. The list of the publications was tagged according to the type of the publication: ISI Journal, ISI Conference Proceedings, Conference Proceedings and Springer Book Chapter. Thus, the list of the publications is the following:

- **A.M. Lonea**, D.E. Popescu and O. Prostean, *"The Overall Process Taken by Enterprises to Manage the IaaS Cloud Services"*. Proceedings of the 6th European Conference on Information Management and Evaluation (ECIME), Cork, Ireland, September 12-14, 2012, edited by Dr Tadgh Nagle, University College Cork, ISBN: 978-1-908272-65-2, pp.168, submitted to Thomson ISI for indexing **(ISI Conference Proceedings)**
- **A.M. Lonea,** D.E. Popescu, O. Prostean and H. Tianfield, *"Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud"*. Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary**,** in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 367-379, Springer-Verlag Heidelberg, 2013, *Agreement* SPIN: 86113511 GPU/PS: Science & Engineering/HS/89, ISSN: 1867-5662, (Accepted – Agreement SPIN: 86113511 GPU/PS: Science & Engineering/HS/89) **(ISI Conference Proceedings)**
- **A.M. Lonea,** *"Private Cloud Set Up Using Eucalyptus open source"*. Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary, in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 381-389, Springer-Verlag Heidelberg, 2013, *Agreement* SPIN: 86113511 GPU/PS: Science & Engineering/HS/89, ISSN: 1867-5662, (Accepted – Agreement SPIN:

86113511 GPU/PS: Science & Engineering/HS/89) **(ISI Conference Proceedings)**

- **A.M. Lonea**, D.E. Popescu and O. Prostean, *"A Survey of Management Interfaces for Eucalyptus Cloud"*. IEEE 7th International Symposium on Applied Computational Intelligence and Informatics, SACI 2012, Timisora, Romania, May 24-26, 2012, pp. 261-266, ISBN: 978-1-4673-1013-0 **(IEEE Conference Proceedings)**
- **A.M. Lonea**, D.E. Popescu and H. Tianfield, *"Detecting Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment*", presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836,vol. 7, , Issue 5, 2012 **(ISI Journal)**
- D.E. Popescu and **A.M. Lonea**, "*An Hybrid Text-Image based Authentication for Cloud Services*", presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836, vol. 7, Issue 5, 2012 **(ISI Journal)**
- **A.M. Lonea**, "*Cloud Computing Security*". Second Workshop: Interdisciplinary and Research Management, "Politehnica" University of Timisoara, Timisoara, Romania, 24-25 November 2011 (**Conference Proceedings**)
- **A.M. Lonea**, H. Tianfield and D.E. Popescu, "*Identity Management for Cloud Computing*", Book Chapter in "New Concepts and Applications in Soft Computing", Studies in Computational Intelligence, Springer-Verlag, pp. 175-199, Volume 417/2013, ISBN: 978-3-642-28958-3 **(Springer Book chapter)**
- **A.M. Lonea**, H. Tianfield, T. Buggy and O. Prostean, "*Cloud Security Architecture (CSA)*". Poster presented at Scottish Informatics and Computer Science Alliance (SICSA) PhD Conference, SICSA 2011 PhD Conference, Edinburgh, Scotland, 23-25 May 2011. **(Conference Proceedings)**
- **A.M. Lonea** and D.E. Popescu, "*Security Issues For GRID Systems*", 4th International Workshop on Soft Computing Applications, SOFA 2010, Arad, Romania, ISBN: 978-1-4244-7985-6, July, 2010, pp. 73-76 **(IEEE Conference Proceedings)**

The PhD reports that were presented are the following:

- **A.M. Lonea**, "Cloud Security Architecture", Ph.D. Report, Glasgow Caledonian University, School of Engineering and Computing, Glasgow, United Kingdom, May, 2011.
- **A.M. Lonea**, "Cloud Security Architecture", Ph.D. Report, "Politehnica" University of Timisoara, Timisoara, Romania, June, 2011.
- **A.M. Lonea**, „Identity Management for Cloud Computing", Ph.D. Report 1, "Politehnica" University of Timisoara, Timisoara, Romania, September, 2011.
- **A.M. Lonea,** „Authentication and Intrusion Detection Solutions in Cloud Computing", Ph.D. Report 2, „Politehnica" University of Timisoara, Timisoara, Romania, September, 2012.

This PhD programme was partially funded by the strategic grant POSDRU/88/1.5/S/50783.

## 7.2. Future work

Several extensions have been identified during this work in terms of cloud security and cloud administration.

Thus, as future work I plan to implement the proposed hybrid text-image based authentication presented in this thesis, in order to make a user study, to evaluate the results and to compare them with the theoretical analysis. Additionally, this proposed authentication solution can be applied as well at the application level in cloud computing. A future extension for this work would be to add a secondary authentication mechanism, in case that the user has forgotten their passwords.

In terms of identity security, the enforcement of the proposed architectural solution of security for cloud computing would be part of my further research plans, in which the cloud Identity Access Management (IAM) gateway appears to require enhancement in order to realize proper integration of enterprises to cloud services.

While the experimental results for detecting Distributed Denial of Service (DDoS) attacks were performed into a private cloud model deployed using Eucalyptus open-source, the Intrusion Detection System (IDS) cloud topology could be used as well for the others cloud deployment models. Moreover, another extension will be to realize the detection procedure of possible DDoS attacks using the following open source IDSs toolkits: Network Intrusion Prevention and Detection System (i.e. Snort) and Host-based Intrusion Detection System (i.e. OSSEC), in order to deliberate the attacks assesment of evidences by analyzing the conflict generated by both types of sensors. Therefore, another future direction is to utilize OSSEC besides Snort for defending the virtual machines against DDoS attacks and both IDSs will be deployed and configured separately, respective each IDS will correspond to a distinct virtual machine.

Another potential aspect that can be improved is to continue the work regarding the management process taken by enterprises to manage the outsourcing procedure of their data at the Infrastructure-as-a-Service (IaaS) by investigating the companies from Romania that had migrated from traditional Enterprise Resource Planning (ERP) towards ERP-based cloud.

Moreover, another potential avenue of future research would be to try the OpenStack software, which becomes to be used in the cloud field. OpenStack was not considered for this work because at the moment of starting the experimental part it was not available. The purpose is to realize an evaluation based on a comparison between OpenStack and Eucalyptus software.

# BIBLIOGRAPHY


[Ada+00] F. Adam and P. O'Doherty,Lessons from enterprise resource planning implementations in Ireland - towards smaller and shorter ERP projects, Journal of Information Technology (15:4), pp 305-316, 2000

[And09] T. Andrei, Cloud Computing Challenges and Related Security Issuess. A Survey Paper. [online]. http://www1.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html, 2009

[Arm+09] M. Armbrust, A. Fox, R. Griffith, A. Joseph, et al.: Above the Clouds: A Berkely View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, Berkely Electrical Engineering and Computing Science, University of California, Berkely, 2009

[Bak+07] A.R. Baker and J. Esler, Snort Intrusion Detection and Prevention Toolkit. Syngress Publishing, Inc., 2007

[Bak+10] A. Bakshi and B. Yogesh, Securing Cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine. In: Second International Conference on Communication Software and Networks, pp. 260-264. IEEE Computer Society Washington, DC, USA, 2010

[Beg+12] C. Begg and T. Caira, Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation, Volume 15, Issue 1, pp. 01-12, 2012

[Ben+10] A. Ben Letaifa, A. Haji, M. Jebalia, et al., State of the Art and Research Challenges of new services architecture technologies: Virtualization, SOA and Cloud Computing. International Journal of Grid and Distributed Computing, Vol. 3, No. 4, December, 2010

[Ber+10] E. Bertino, L.D. Martino, E.Paci and A.C. Squicciarini, *Security for Web Services and Service-Oriented Architecture.* Berlin Heidelberg: Springer, ISBN 978-3-540-87741-7, 2010

[Bha+11] R. Bhadauria, R. Chaki, N. Chaki, S. Sanyal, A Survey on Security Issues in Cloud Computing. CoRR. [online]. http://arxiv.org/ftp/arxiv/papers/1109/1109.5388.pdf, 2011

[Bit08] F. Bitzer. "Management Framework for Amazon EC2". Diploma Thesis, 2008

[Bor+10] B. Borisaniya, A. Patel, R. Patel, D. Patel, Network-based Intrusion Detection in Eucalyptus Private Cloud. In: 2010 International Conference on Advances in Communication, Network, and Computing, pp. 209-212. India, 2010

[Bre02] M.P. Brennan, Using Snort for a Distributed Intrusion Detection System. SANS Institute, Version 1.3, http://www.sans.org/reading_room/whitepapers/detection/snort-distributed-intrusion-detection-system_352, 2002

[Bue+08]] A. Buecker, P. Ashley and N. Readshaw, Federated Identity and Trust Management. International Bussiness Machines (IBM), Redpaper, 2008

[Buy+09] R. Buyya, et al.: Cloud Computing and emerging IT platforms: Vision, Hype and reality for delivering computing as the 5th utility. Future Generation Computer Systems, Vol. 25, Issue 6, pp.599-616, 2009

[CA07] CA Software, *CA SOA Security Manager: Securing SOA / Web Services Based IT Architectures.* [online]. http://www.ca.com/files/technologybriefs/34499-ca-soa-sm-tech-brf_162833.pdf, 2007

[Can12] Canonical Ltd., Attaching EBS volumes failed after rebooting SC host. [online]. https://bugs.launchpad.net/eucalyptus/+bug/733067, 2012

[Cha+07] V. Chatzigiannakis, G. Androulidakis, K. Pelechrinis, et al., Data fusion algorithms for network anomaly detection: classification and evaluation. Proceedings of the Third International Conference on Networking and Services (ICNS'07), 2007

[Che+06] Q. Chen and U. Aickelin, U., Dempster-Shafer for Anomaly Detection. *In Proceedings of the International Conference on Data Mining (DMIN 2006)*, Las Vegas, USA, pp. 232-238, 2006

[Che+10] X. Chen, G.B. Wills, L. Gilbert, D. Bacigalupo, Using Cloud for Research: A Technical Review. JISC. [online]. http://tecires.ecs.soton.ac.uk/docs/TeciRes_Technical_Report.pdf, 2010

[Cho+08] T. Chou, K.K. Yen, J. Luo, Network intrusion detection design using feature selection of soft computing paradigms. *International Journal of Computational Intelligence*, Volume 4, Issue 3, pp.102-105, 2008

[Cis+09] Cisco and VMware, DMZ Virtualization Using VMware vSphere 4 and the Cisco Nexus 1000V Virtual Switch. [online]. http://www.vmware.com/files/pdf/dmz-vsphere-nexus-wp.pdf, 2009

[Cis10] Cisco Systems, Inc.: Planning the Migration of Enterprise Applications to the Cloud. [online], Cisco White Paper, http://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf, 2010

[Clo10] Cloud Computing Use Case Discussion Group: Cloud Computing Use Cases White Paper Version 4.0. Cloud Computing Use Case Discussion Group, http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf, 2010

[Con12] Confident Technologies Inc., Confident ImageShieldTM. [online]. http://www.confidenttechnologies.com/products/confident-imageshield, 2012

[Cor+10] T. Cordeiro, D. Damalio, N. Pereira, et al., Open Source Cloud Computing Platforms, Ninth International Conference on Grid and Cloud Computing, pp. 366-371, 2010

[CPN10] CPNI: Information Security Briefing Cloud Computing. Centre for the Protection of National Infrastructure. [online]. http://www.cpni.gov.uk/Documents/Publications/2010/2010007ISB_cloud_computing.pdf, 2010

[Cra12] J. Craig, EMA Radar™ for Application Performance Management (APM) for Cloud Services: Q1 2012. Enterprise Management Associates (EMA), 2012

[Cri00] P.J. Criscuolo, Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000 and Stacheldraht. CIAC-2319, Department of Enery Computer Incident Advisory Capability, UCRL-ID-136939, Rev.1, Lawrence Livermore National Laboratory, [online]. https://e-reports-ext.llnl.gov/pdf/237595.pdf, 2000

[CSA09] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, [online]. http://www.cloudsecurityalliance.org/csaguide.pdf, 2009

[CSA10] CSA, *Top Threats to Cloud Computing V1.0.* [online] Cloud Security Alliance. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, 2010

[CSA10b] CSA, Domain 12: Guidance for Identity & Access Management V2.1. [online] Cloud Security Alliance. http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf, 2010b

[CSA11a] CSA, Security as a Service. [online]. Cloud Security Alliance. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf, 2011a

[CSA11b] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. [online]. Cloud Security Alliance. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011b

[CSA12a] CSA, GRC Stack. [online]. Cloud Security Alliance. https://cloudsecurityalliance.org/research/grc-stack/, 2012a

[CSA12b] CSA, SecaaS Category 8: Encryption Implementation Guidance. [online]. Cloud Security Alliance, 2012b

[CSC11] CSCC: Practical Guide to Cloud Computing Version 1.2, [online], Cloud Standards Customer Council, [online]. http://www.isaca.org/Groups/ProfessionalEnglish/cloudcomputing/GroupDocuments/CSCC_PG2CCv1_2.pdf, 2011

[CSS09] CSS Corp Labs, Hybridfox: Cross of Elasticsfox and Imagination. [online]. http://cssinnovations.blogspot.com/2009/11/hybridfox-cross-of-elasticsfox-and.html, 2009

[Dai09] W. Dai, The Impact of Emerging Technologies on Small and Medium Enterprises. Journal of Business Systems, Governance and Ethics, Vol. 4, No. 4, pp. 53-60, 2009

[Dev+12] J. Devos, H. Van Landeghem and D. Deschoolmeester, SMEs and IT: Evidence for a Market for "Lemons". The Electronic Journal Information Systems Evaluation, Volume 15, Issue 1, pp. 25-35, 2012

[Dha+11] S.N. Dhage, B.B. Meshram, R. Rawat, et al., *Intrusion Detection System in Cloud Computing Environment*. In International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India, pp. 235-239, 2011

[Dha+00] R. Dhamija, A. Perrig, Déjà vu: a user study using images for authentication, Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, USENIX Association Berkeley, CA, USA, 2000

[Dis,n.d] Discretix Technologies Ltd., Introduction to Side Channel Attacks. [online]. http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf, n.d.

[Dit99] D. Dittrich, The "stacheldraht" distributed denial of service attack tool. University of Washington. [online]. http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt, 1999

[Dis08] A. Dissanayake, *Intrusion Detection Using the Dempster-Shafer Theory*. 60-510 Literature Review and Survey, School of Computer Science, University of Windsor, 2008

[DMT10a] DMTF: Use Cases and Interaction for managing clouds. [online], White paper from the Open Cloud Standards Incubator, Version 1.0.0. Distributed Management Task Force Inc., [online]. http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0103_1.0.0.pdf, 2010a

[DMT10b] DMTF: DMTF Architecture for managing clouds, [online], Distributed Management Task Force, Inc. [online]. http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf, 2010b

[Dou+07] C. Douligeris and G. P. Ninios, *Security in Web Services*. In: C. Dougligeris and D. Serpanos, ed. 2007. Network Security: Current Status and Future Directions. Wiley IEEE Press Publisher, Chapter 11, pp. 179-204, 2007

[Ela11] Elastic Security, Amazon EC2 'broad character' support and Security impact on third party tools such as Elastic Detector. [online]. http://elastic-security.com/2011/02/18/amazon-ec2-broad-character-support-and-security-impact-on-third-party-tools-such-as-elastic-detector/, 2011

[ENI09] ENISA, *Cloud Computing Bnefits, Risks and Recommendations for Information Security*. [online] European Network and Information Security Agency. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport, 2009

[enS10] enStratus Networks LLC, enStratus Security Architecture, White Paper, 2010.

[Esm97] M. Esmaili, M. *Dempster-Shafer Theory and Network Intrusion Detection Systems*. Scientia Iranica, Vol. 3, No. 4, Sharif University of Technology, 1997

[Euc09] Eucalyptus Systems, Inc., Eucalyptus Open-Source Cloud Computing Infrastructure – An Overview. [online]. http://www.eucalyptus.com/pdf/whitepapers/Eucalyptus_Overview.pdf, 2009

[Euc12] Eucalyptus Systems, Inc., Eucalyptus Community Cloud. [online]. http://open.eucalyptus.com/try/community-cloud, 2012

[Euc10] Eucalyptus Systems, Inc., Eucalyptus Cloud Computing Platform Administrator Guide Version 1.6. [online]. http://open.eucalyptus.com/AdministratorGuide.v1.final.03.23.pdf, 2010

[Euc12a] Eucalyptus Systems, Inc., Eucalyptus Administrator's Guide (2.0). [online]. http://open.eucalyptus.com/wiki/EucalyptusAdministratorGuide, 2012a

[Euc12b] Eucalyptus System, Inc., EC2-compatible tools. [online]. http://open.eucalyptus.com/wiki/ec2-compatible-tools, 2012b

[Euc12c] Eucalyptus Systems, Inc., Eucalyptus User's Guide (2.0). [online]. http://open.eucalyptus.com/wiki/EucalyptusUserGuide_v2.0, 2012c

[Euc12d] Eucalyptus Systems, Inc., Engage where you connect your needs with Eucalyptus people and knowledge. [online]. https://engage.eucalyptus.com/, 2012d

[Fis09a] Fischer International Identity, LLC., Identity as a Service (IAAS) Technology, White paper, 2009.

[Fis09b] Fischer International Identity, LLC., Product Overview Introducing Fischer Identity, White paper, 2009.

[Fos02] I. Foster, What is the Grid? A Three Point Checklist. Argonne National Laboratory & University of Chicago, 2002

[Fos+08] I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud Computing and Grid Computing 360-Degree Compared. In: Grid Computing Environments Workshop, GCE '08, pp.1-10, 2008

[Fur10] C. M. Furlani, Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud. National Institute of Standards and Technology (NIST), http://www.nist.gov/director/ocla/testimony/upload/Cloud-Computing-testimony-FINAL-with-Bio.pdf (2010)

[Ger10] S. Geric, Security of Web Services based Service-oriented Architectures. In: MIPRO2010, Proceedings of the 33th International Convention, pp. 1250-1255, Opatija, Croatia, 2010

[Gon+10] C. Gong, J. Liu, Q. Zhang, et al., The Characteristics of Cloud Computing. In: 39th International Conference on Parallel Processing Workshops (ICPPW), pp. 275-279, 2010

[Gon+11] N.M. Gonzales, C.C. Miers, F.F. Redigolo, et al., A quantitative analysis of current security concerns and solutions for cloud computing. Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science, pp.231-238, 2011

[Goo11a] Google. *Hybridfox*. [online]. http://code.google.com/p/hybridfox/, 2011a

[Goo11b] Google Project Hosting, Typica. [online]. http://code.google.com/p/typica/, 2011b

[Gou+10] J.T. Goulding, J. Broberg and M. Gardiner, *Identity and access management for the cloud: CA's strategy and vision.* [online] CA, Inc., White paper.http://www.ca.com/files/WhitePapers/iam_cloud_security_vision_wp_236732.pdf, 2010

[Gro+11] B. Grobauer, T. Walloschek and E. Stocker, Understanding Cloud-Computing Vulnerabilities. *Security & Privacy, IEEE ,* vol.9, no.2, pp.50-57, March-April, 2011

[Gru+09] N. Gruschka and L.L. Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited. IEEE International Conference on Web Services, ICWS 2009, Los Angeles, pp. 625-631, 2009

[Gru+10] N. Gruschka and M. Jensen, Attack Surfaces: A taxonomy for Attacks on Cloud. [online]. http://download.hakin9.org/en/Securing_the_Cloud_hakin9_07_2010.pdf, Vol.5, No. 7, Issue 7/2010 (32), 2010

[Gut91] M.A.S. Guth, A Probabilistic Foundation for Vagueness & Imprecision in Fault-Tree Analysis. *IEEE TRANSACTIONS ON RELIABILITY*, 40(5), pp.563-569, 1991

[Har11] P. Harding, *State of Cloud Identity*. 2nd annual Cloud Identity Summit, San Francisco, 2011

[Har09] T. Harris, Migration and Security in SOA. [online]. University of Leeds, White Paper. http://www.thbs.com/pdfs/Migration_and_Security_in_SOA.pdf, 2009

[Har07] P. Harper, Snort Enterprise Install, [online]. http://www.internetsecurityguru.com/documents/Snort_Base_Barnyard_CentOS_5.pdf, 2007

[Hei+10] C. Heinle and J. Strebel, IaaS adoption determinants in enterprises. In Proceedings of the 7th international conference on Economics of grids, clouds, systems, and services (GECON'10), J. Altmann and Omer F. Rana (Eds.). Springer-Verlag, Berlin, Heidelberg, 93-104, 2010

[Hog+11] M. Hogan, F. Liu, A. Sokol and J. Tong, NIST Cloud Computing Standards Roadmap – Version 1.0. NIST Nationale Institute of Standards and Technologies, 2011

[Hu+06] W. Hu, J. Li and Q. Gao, *Intrusion Detection Engine Based on Dempster-Shafer's Theory of Evidence*. Communications, Circuits and Systems Proceedings, 2006 International Conference, 3, 1627-1631, 2006

[IBM09a] IBM: IBM Point of View: Security and Cloud Computing. ftp://public.dhe.ibm.com/common/ssi/ecm/en/tiw14045usen/TIW14045USEN_HR.PDF, 2009a

[IBM09b] IBM, Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security [online]. http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf, 2009b

[IBM10] IBM Corporation, *IBM Tivoli Access Management for Cloud and SOA environments*. [online] ftp://public.dhe.ibm.com/common/ssi/ecm/en/tis14053usen/TIS14053USEN_HR.PDF, 2010

[IBM,n.d] IBM, Web2.0/SaaS Security [online]. Tokyo Research Laboratory. http://www.research.ibm.com/trl/projects/web20sec/web20sec_e.htm, n.d.

[Int11] Intel, Intel Cloud Builder Guide to Cloud Design and Deployment on Intel Platforms Ubuntu Enterprise Cloud. White Paper, 2011

[Jam+11] D. Jamil and H. Zaki, Security Issues in Cloud Computing and Countermeasures. *International Journal of Engineering Science and Technology (IJEST)*, Vol.3, No.4, ISSN: 0975-5462, 2011

[Jac06] L. Jackson, Analysis of Image-Based Authentication and its Role in Security Systems of the Future. [online]. http://www.soc.napier.ac.uk/ bill/lee2006.pdf, 2006

[Jae+10] T. Jaeger and J. Schiffman, Outlook: Cloudy with a chance of Security Challenges and Improvements. IEEE Security & Privacy, vol.8, no. 1, pp.77-80, 2010

[Jen+09] M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, On technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing (Cloud '09), Bangalore, pp. 109-116, 2009

[Jin+10] X. Jing and Z. Jian-Jun, A Brief Survey on the Security Model of Cloud Computing. In: 2010 Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), pp. 475-478, 2010

[Joh+10] D. Johnson, M. Kiran, R. Murthy, et al., Eucalyptus Beginner's Guide – UEC Edition. v1.0. [online]. http://cssoss.files.wordpress.com/2010/06/book_eucalyptus_beginners_guide_uec_edition1.pdf , 2010

[Jun09] Juniper Networks, Inc., Identity Federation in a Hybrid Cloud Computing Environment Solution Guide. [online]. http://www.juniper.net/us/en/local/pdf/implementation-guides/8010035-en.pdf, 2009

[jus11] just works! Software. Cloud 42. [online]. http://cloud42.net/index.php, 2012

[Kam11] M. Kamran Azeem, "Xen, KVM, Libvirt and IPTables". [online]. http://cooker.techsnail.com/index.php/XEN,_KVM,_Libvirt_and_IPTables, 2011

[Kan+09] B.R. Kandukuri, R.V. Paturi, A. Rakshit, Cloud Security Issues. IEEE International Conference on Services Computing, Bangalore, pp. 517-520, 2009

[Kar+11] G.R. Karpagam and J. Parkavi. Setting up of an Open Source based Private Cloud. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, 2011

[Kha+10a] A. Khajeh-Hosseini, D. Greenwood and I. Sommerville, Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. IEEE 3rd International Conference on Cloud Computing (CLOUD 2010). Miami, USA, 2010

[Kha+11] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, P. Teregowda, Decision Support Tools for Cloud Migration in the Enterprise. IEEE 4th International Conference on Cloud Computing (CLOUD 2011), Washington DC, USA, 2011

[Kha+10b] A. Khajeh-Hosseini, I. Sommerville and I. Sriram, Research Challenges for Enterprises Cloud Computing. LSCITS Technical Report, 2010

[KPM11] KPMG, The Cloud Changing the Business Ecosystem. [online] http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The_Cloud_Changing_the_Business_Ecosystem.pdf, 2011

[Kra09] F.J. Krautheim, Private Virtual Infrastructure for Cloud Computing. Proceedings of the 2009 conference on Hot topics in cloud computing, Article No.5, Usenix Association Berkeley, CA, USA, 2009

[Lak10] S. Lakshminarayanan, Interoperable Security Standards for Web Services. *IEEE IT Professional*, Vol.12, Issue 5, pp. 42-47, 2010

[Lee+11] J-H. Lee, M-W. Park, J-H. Eom and T-M. Chung, T-M. *Multi-level Intrusion Detection System and Log Management in Cloud Computing*. In 13th International Conference on Advanced Communication Technology (ICACT) ICACT 2011, Seoul, 13- 16 February, pp.552- 555, 2011

[Lev+04] M. Levy and P. Powell, Strategies for Growth in SMEs: The Role of Information and Information Systems. Elsevier, Oxford, 2004

[Lo+10] C-C. Lo, C-C. Huang and J. Ku. *A Cooperative Intrusion Detection System Framework for Cloud Computing Networks*. In 39th International Conference on Parallel Processing Workshops, pp.280-284, 2010

**[Lon+10]** **A.M. Lonea**, D.E. Popescu, Security Issues For GRID Systems. In: 4th International Workshop on Soft Computing Applications, SOFA 2010, Arad, Romania, pp. 73-76, ISBN: 978-1-4244-7985-6, July, 2010.

**[Lon+11]** **A.M. Lonea**, H. Tianfield, T. Buggy and O. Prostean, "*Cloud Security Architecture (CSA)*". Poster presented at Scottish Informatics and Computer Science Alliance (SICSA) PhD Conference, SICSA 2011 PhD Conference, Edinburgh, Scotland, 23-25 May 2011.

**[Lon11a]** **A.M. Lonea**, "Cloud Security Architecture", Ph.D. Report "Politehnica" University of Timisoara, Timisoara, Romania, June, 2011a.

**[Lon11b]** **A.M. Lonea**, Identity Management for Cloud Computing, Ph.D. Report 1, "Politehnica" University of Timisoara, September, 2011b.

**[Lon12a]** **A.M. Lonea**, Cloud Computing Security. Second Workshop: Interdisciplinary and Research Management, "Politehnica" University of Timisoara, Timisoara, Romania, 24-25 November 2011.

**[Lon12]** **A.M. Lonea**, Private Cloud Set Up Using Eucalyptus open source. Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary, in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 381-389, Springer-Verlag Heidelberg, 2013 **(ISI Conference Proceedings)**

**[Lon+12a]** **A.M. Lonea,** D.E. Popescu and O. Prostean, The Overall Process Taken by Enterprises to Manage the IaaS Cloud Services. In: 6th European

Conference on Information Management and Evaluation, ECIME 2012, Cork, Ireland, 13-14 September, 2012a, edited by Dr Tadgh Nagle, University College Cork, ISBN: 978-1-908272-65-2, pp.168, submitted to Thomson ISI for indexing **(ISI Conference Proceedings)**

**[Lon+12b]** **A.M. Lonea,** D.E. Popescu and O. Prostean, A Survey of Management Interfaces for Eucalyptus Cloud. 7th IEEE International Symposium on Applied Computational Intelligence and Informatics, SACI 2012, Timisora, Romania, pp. 261-266, ISBN: 978-1-4673-1013-0, May 24-26, 2012b

**[Lon+13]** **A.M. Lonea,** H. Tianfield, D. E. Popescu, Identity Management for Cloud Computing. Book Chapter in "New Concepts and Applications in Soft Computing", Studies in Computational Intelligence, Springer-Verlag, pp. 175-199, Volume 417/2013, ISBN: 978-3-642-28958-3

**[Lon+12c]** **A.M. Lonea,** D.E. Popescu, D.E., Tianfield, H., Detecting Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment. presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836, vol. 7, Issue 5, 2012

**[Lon+12d]** **A.M. Lonea,** D.E. Popescu, O. Prostean and H. Tianfield, "Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud". Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary, in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 367-379, Springer-Verlag Heidelberg, 2013 **(ISI Conference Proceedings)**

**[Lon12b]** **A.M. Lonea,** „Authentication and Intrusion Detection Solutions in Cloud Computing", Ph.D. Report 2, „Politehnica" University of Timisoara, Timisoara, Romania, 2012

[Lyn11] L. Lynch, Inside the Identity Management Game. *IEEE Internet Computing*, Vol. 15, Issue 5, pp. 78-82, 2011

[Mag+09] F. Magoulès, J. Pan, K-A. Tan, et al., Introduction to Grid Computing. CRC Press Taylor & Francis Group, London, 2009

[Mar+11] S. Marston, Z. Li, S. Bandyopadhyay, et al., Cloud Computing – The business perspective. Decision Support Systems, 51, pp. 176-189, 2011

[Maj+07] J. Majava, A. Biasiol and A. Van der Maren, *Report on comparison and assessment of eID management solutions interoperability*. [online]. European Communities. http://ec.europa.eu/idabc/servlets/Doceb29.pdf?id=29620, 2007

[Maz+10] C. Mazzariello, R. Bifulco and R. Canonico, Integrating a Network IDS into an Open Source Cloud Computing Environment. In Sixth International Conference on Information Assurance and Security, pp. 265-270, 2010

[McM09] R. McMillan,Cisco CEO: Cloud Computing a 'Security nightmare'. [online]. http://www.csoonline.com/article/490368/cisco-ceo-cloud-computing-a-security-nightmare- , 2009

[Mel+09] P. Mell and T. Grance, The NIST definition of Cloud Computing. National Institute of Standards and Technology (NIST). [online] csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, 2009

[Mic+11] N. Micallef and M. Just, Using Avatars for Improved Authentication with Challenge Questions, in Proceedings of the The Fifth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2011), August, 2011

[Mir+04] J. Mirkovic, J. Martin, P. Reiher, A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, Volume 34, Issue 2, pp.39-53, 2004

[Mis+11] S.C. Misra and A. Mondal, Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. Mathematical and Computer Modelling, Volume 53, Issues 3-4, pp. 504-521, 2011

[Moo11] N. Moore, Snort 2.9.1 CentOS 5.6 Installation Guide. [online]. http://www.snort.org/assets/159/Snort_2.9.1_CentOS_5.pdf, 2011

[Mor+11] C. Mortimore, P. Harding, P. Madsen and J. Smarr, Simple Cloud Identity Management: Core Schema 1.0 –draft1 . [online]. http://www.simplecloud.info/specs/draft-scim-core-schema-01.html, 2011

[New+05] R.E. Newman, P. Harsh and P. Jayaraman, Security Analysis of and Proposal for Image Based Authentication, IEEE Carnahan, 2005

[Nit+08] Nitin, Vivek Kumar Sehgal, Durg Singh Chauhan, Munish Sood and Vikas Hastir, *Image Based Authentication System with Sign-In Seal*, Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA, 2008

[Nor09] N.A. Nordbotten, N.A., XML and Web Services Security Standards. *IEEE Communications Surveys & Tutorials*, Vol. 11, Issue 3, pp. 4-21, 2009

[Nor+02] S. Northcutt and J. Novak, Network Intrusion Detection. Third Edition, New Riders Publishing, ISBN: 0-73571-265-4, 2002

[Nov10] Novell, *Annexing the Cloud Novell Cloud Security Service*. [online]. Novell. http://www.asiacloudforum.com/system/files/WP_Novell_annexing_cloud_security.pdf, 2010

[Nov11] Novell, Novell Cloud Security Service 1.0 SP2. [online]. Novell. http://www.novell.com/documentation/novellcloudsecurityservice/, 2011

[Nur+08] D. Nurmi, R. Wolski, C. Grzegorczyk, et al., Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems. University of California, Santa Barbara, 2008

[Nur+09a] D. Nurmi, R. Wolski, C. Grzegorczyk, et al., The Eucalyptus Open-source Cloud computing System. 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009a

[Nur+09b] D. Nurmi, R. Wolski, C. Grzegorczyk, et al. „Eucalyptus: An open-source cloud computing infrastructure". *SciDAC 2009, IOP Publishing, Journal of Physics: Conference Series 180,* 2009b

[OAu,n.d] OAuth, n.d., "*OAuth Community Site*." [online]. http://oauth.net/ , n.d.

[OAS03a] OASIS, *Service Provisioning Markup Language (SPML) Version 1.0*. [online] OASIS. Available at: < http://www.oasis-open.org/committees/download.php/4137/os-pstc-spml-core-1.0.pdf, 2003a.

[OAS05a] OASIS, *SAML V2.0 Executive Overview*. [online] OASIS. http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf , 2005a

[OAS08] OASIS, Security Assertion Markup Language (SAML) V2.0 Technical Overview. [online] OASIS. http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf , 08

[Oku+10] M. Okuhara, T. Shiozaki and T. Suzuki, Security Architectures for Cloud Computing. FUJITSU Sci. Tech. J., Vol. 46, No. 4, pp. 397-402, October, 2010

[Old11] E. Olden, Architecting a Cloud-Scale Identity Fabric. Computer , vol.44, no.3, pp.52-59, 2011

[Ope11] Open Group, An Architectural View of Security for Cloud Examining Policy-Based Security Through Scenarios. The Open Group. White Paper, 2011

[Opi+07] C. Opincaru and G. Gheorghe, Service Oriented Security Architecture. Proceedings of the 2nd International Workshop on Enterprise Modelling and Information Systems Architectures (EMISA'07), pp. 61-67, 2007.

[Pem10] K. Pemmaraju, The Evolution of Clouds: Private and Hybrid Clouds. [online]. http://sandhill.com/article/the-evolution-of-clouds-private-and-hybrid-clouds/, 2010

[Per11] G. Perry, Minimizing public cloud disruptions, TechTarget. [online]. http://searchdatacenter.techtarget.com/tip/Minimizing-public-cloud-disruptions, 2011

[Pin10a] Ping Identity, *The Primer: Nuts and Bolts of Federated Identity Management White Paper*. [online] Ping Identity Corporation.

http://secprodonline.com/~/media/SEC/Security%20Products/Whitepapers/2008/06/Ping%20Identity_WP_PrimerFIM%20pdf.ashx, 2010a

[Pin10b] Ping Identity, 2010b. *SAML 101 White paper.* [online] Ping Identity Corporation.https://www.pingidentity.com/unprotected/upload/SAML-101.pdf, 2010b

**[Pop+12]** D.E. Popescu and **A.M. Lonea**, An Hybrid Text-Image based Authentication for Cloud Services, presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836, vol. 7, Issue 5, 2012

[Ram+10] S. Ramgovind, M.M. Eloff, E. Smith, The management of security in Cloud Computing. Information Security for South Africa (ISSA), pp. 1-7, 2010

[Ray12] P.R. Ray, Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices. Journal of Information Engineering and Applications, Vol. 2, No. 2, 2012

[Red+11] V.K. Reddy and L.S. Reddy, Security Architecture of Cloud Computing. International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 9, pp. 7149-7155, 2011

[Reh03] R.UR. Rehman, Intrusion Detection with Snort: Advanced IDS Techniques using Snort, Apache, Mysql, PHP and ACID. Pearson Education Inc., Publishing as Prentice Hall PTR, 2003

[Ren+10] K. Renaud K., Just M., Pictures or Questions? Examining User Responses to Association-Based Authentication, to appear in the ACM Proceedings of the British HCI Conference 2010, Dundee, Scotland, 6-10 September, 2010

[Rig12] RightScale, Inc., *RightScale Cloud Management*. [online]. http://www.rightscale.com/, 2012

[Rin+09] T. Rings, G. Caryer, J. Gallop, et al., Grid and Cloud Computing: Opportunities for Integration with the Next Generation Network. Journal of Grid Computing, Vol. 7, Number 3, pp. 375-393, 2009

[Ris+09] T. Ristenpart, E. Tromer, H. Schacham and S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party compute Clouds. *ACM Conference on Computer and Communications Security*, Chicago, 2009

[Rit+10] J.W. Rittinghouse and J.F. Ransome, Cloud Computing Implementation, Management and Security. CRC Press, Boca Raton, 2010

[Ros+09] S. Roschke, F. Cheng and C. Meinel, Intrusion Detection in the Cloud. In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729-734, 2009

[Ros+05] M. Rosenblum and T. Garfinkel, Virtual machine monitors: current technology and future trends. IEEE Computer, Vol. 38, Issue 5, pp. 39-47, 2005

[RSA09] RSA: The Role of Security in Trustworthy Cloud Computing, [online], White Paper, http://www.emc.com/collateral/about/investor-relations/9921_CLOUD_WP_0209_lowres.pdf, 2009

[Sac+10] S. Sachdeva, S. Machome and S. Bhalla, *Web Services Security Issues in Healthcare Applications*. 9th IEEE/ACIS International Conference on Computer and Information Science (ICIS), Yamagata, pp. 91-96, 2010

[Sau10] Saugatuck Technology Inc., Stepping Up to the Cloud: Managing Changes and Migration for Mid-Sized Business. [online]. http://fm.sap.com/data/UPLOAD/files/Saugatuck-Stepping_Up_to_the_Cloud-Managing_Changes_and_Migration_for_Mid-sized_Business.pdf, 2010

[Sav09] Savvis, Inc., Securing Virtual Compute Infrastructure in the Cloud. [online]. White paper. http://www.savvis.com/en-US/Info_Center/Documents/HOS-WhitePaper-SecuringVirutalComputeInfrastructureintheCloud.pdf, 2009.

[Sem+n.d] P. Sempolinski and D. Thain. A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus. [online] University of Notre Dame, http://www.cse.nd.edu/~ccl/research/papers/psempoli-cloudcom.pdf, n.d.

[Sen+02] K. Sentz and S. Ferson, Combination of Evidence in Dempster-Shafer Theory. Sandia National Laboratories, Sandia Report, 2002.

[Ser12] Server Fault, Apt-get update getting 404 on debian lenny. [online]. http://serverfault.com/questions/374651/apt-get-update-getting-404-on-debian-lenny, 2012

[Set11] SETECS Inc, Security Architecture, for Cloud Computing Environments, White Paper. [online]. http://security.setecs.com/Documents/5 SETECS Cloud Security Architecture.pdf, 2011

[Sha10] D. Shackleford, Cloud Security and Compliance: A Primer. [online]. SANS. http://www.sans.org/reading_room/analysts_program/mcafee_carbird_08_2010.pdf , 2010

[Sha10] J. Shafer, I/O Virtualization Bottlenecks in Cloud Computing Today. Second Workshop on I/O Virtualization (WIOV'10), Pittsburgh, USA, 2010

[Sha+08] D. Shah, D. Patel, Dynamic and Ubiquitous Security Architecture for Global SOA. In: The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp. 482-487, Valencia, Spain, 2008

[Sha,n.d] A. Sharma, Private cloud setup using eucalyptus and xen. [online]. http://www.akashsharma.me/private-cloud-setup-using-eucalyptus-and xen/#Cloud_(2D)_setup_private_cloud, n.d.

[Sha+10] M. Sharma, A. Mehra, H. Jola, et al., Scope of Cloud Computing for SMEs in India. Journal of Computing, Volume 2, Issue 5, ISSN: 2151-9617, 2010

[Sia+03] C. Siaterlis, B. Maglaris and P. Roris, *A novel approach for a Distributed Denial of Service Detection Engine.* National Technical University of Athens. Athens, Greece, 2003.

[Sia+05] C. Siaterlis and B. Maglaris, One step ahead to Multisensor Data Fusion for DDoS Detection. *Journal of Computer Security*, Vol. 13, Issue 5, September 2005, pp. 779-806, 2005

[Ski12] W.T. III. Skinner, Identity Management in a Public IaaS Cloud. James Madison University, Master Thesis. [online]. http://www.scribd.com/doc/90183632/3/Thesis-Statement, 2012

[Sou11] Sourcefire, Inc., Snort Users Manual 2.9.2. [online]. http://www.snort.org/assets/166/snort_manual.pdf, 2011

[Spe+04] S.M. Specht and R.B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. In: Proceedings of the 17th International Conference on Parallel and Distributed Systems, pp. 543-550, 2004

[Sub+11] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011

[Sue+09] J. Suess and K. Morooney, Identity Management & Trust services, Educause review, pp. 25-42, September/ October, 2009

[Sun04] Sun Microsystems, Inc., *Sun's XACML Implementation Programmer's Guide for Version 1.2*. [online] Sun Microsystems. http://sunxacml.sourceforge.net/guide.html, 2004

[Tak+10] H. Takabi, J.B.D. Joshi andG-J. Ahn, Security and Privacy Challenges in Cloud Computing Environments. IEEE Computer and Reliability Societies, pp. 24-31, 2010

[Tho+08] C. Thomas and N. Balakrishnan, Performance Enhancement of Intrusion Detection Systems using advances in sensor fusion. In: 11th International Conference on Information Fusion, pp. 1-7, 2008

[Tre09] Trend Micro, Cloud Computing Security [online] A Trend Micro White Paper. Available at: <http://www.whitestratus.com/docs/making-vms-cloud-ready.pdf, 2009

[Ubu,n.d] Ubuntu Documentation, UEC Overview. [online] Ubuntu, https://help.ubuntu.com/10.04/serverguide/C/uec.html, n.d.

[Uni12] Universität Osnabrück, Total Cost of Ownership Calculator for Cloud Computing Services. [online]. http://www.cloudservicemarket.info/tools/tco.aspx, 2012

[Van+11] S. Van Hoecke, T. Waterbley, J. Devos, et al., Efficient Management of Hybrid Clouds. Cloud Computing 2011: The Second International Conference on Cloud Computing, Grids and Virtualization, pp. 167-172, 2011

[Van+12] R. Vanathi and S. Gunasekaran, Comparison of Network Intrusion Detection Systems in Cloud Computing Environment. In: 2012 International Conference on Computer Communication and Informatics (ICCCI-2012). Coimbatore, India, 2012

[VMw07] VMware, Inc., Understanding Full Virtualization, Paravirtualization and Hardware Assist. [online]. VMware. http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf, 2007

[VMw+09] VMware and SAVVIS, Securing the Cloud A Review of Cloud Computing, Security Implications and Best Practices. Vmware. [online] http://www.savvis.com/en-us/info_center/documents/savvis_vmw_whitepaper_0809.pdf, 2009

[Wan+08] L. Wang and G. von Laszewski, Scientific Cloud Computing: Early Definition and Experience. In: 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08), pp. 825-830, 2008

[Wei11] J. Weinman, Axiomatic Cloud Theory. [online]. http://www.joeweinman.com/Resources/Joe_Weinman_Axiomatic_Cloud_Theory.pdf,2011

[Wei12] J. Weir, Building a Debian\Snort based IDS. [online]. http://www.snort.org/assets/167/IDS_deb_snort_howto.pdf, 2012

[Wil11] L. Wilkes, Making Sense of Cloud Computing. CBDI Journal, Everware-CBDI Inc, pp. 1-14, January, 2011

[Wit+05] I.H. Witten and E. Frank, Data Mining. Practical Machine Learning Tools and Techniques, Second Edition, Kaufmann Press, Elsevier Inc, San Francisco, 2005

[Wre+10] G. Wrenn, CISSP, ISSEP, *Unisys Secure Cloud Addressing the Top Threats of Cloud Computing*. White Paper [online]. http://www.unisys.com/unisys/unisys/inc/pdf/whitepapers/38507380-000.pdf, 2010

[Wu+11] W. Wu, H. Zhang and Z. Li, Open Social based Collaborative Science Gateways. 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 554-559, 2011

[Wyn10] R. Wynn, *Securing the Cloud: Is it a Paradigm Shift in Information Security*. In: Hacking IT Security Magazine, Vol.5, No.7, 2010

[W3C04] W3C, *Web Services Architecture, W3C Working Group Note.*[online]. World Wide Web Consortium. http://www.w3.org/TR/ws-arch/#id2260892, 2004

[w3s12] w3schools.com, SQL Joins. [online]. http://www.w3schools.com/sql/sql_join.asp, 2012

[w3s12a] w3schools.com, SQL Views. [online]. http://www.w3schools.com/sql/sql_view.asp, 2012

[Xen12] Xen.org: Get started with Xen, http://wiki.xen.org/wiki/Main_Page (2012)

[Yu+04] D. Yu and D. Frincke, A Novel Framework for Alert Correlation and Understanding. International Conference on Applied Cryptography and Network Security (ACNS) 2004, Springer's LNCS series, 3089, pp. 452-466, 2004

[Yu+05] D. Yu and D. Frincke, Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory. In: Proceedings of the 43rd ACM Southeast Conference, ACM-SE 43, pp. 142-147, 2005

[Zho+10] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Security and Privacy in Cloud Computing: A Survey. In: 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), pp. 105-112, 2010

# LIST OF PUBLICATIONS

**ISI Journals:**

1. **A.M. Lonea**, D.E. Popescu and H. Tianfield, *"Detecting Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment*", presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836, vol. 7, Issue 5, 2012

2. D.E. Popescu and **A.M. Lonea**, "*An Hybrid Text-Image based Authentication for Cloud Services*", presented at International Conference on Computers, Communications & Control (ICCCC 2012), Baile Felix, Romania, May 8-12, 2012, will be published in International Journal of Computers, Communications and Control (IJCCC), ISSN 1841-9836, vol. 7, Issue 5, 2012

**ISI Conference Proceedings:**

1. **A.M. Lonea**, D.E. Popescu and O. Prostean, *"The Overall Process Taken by Enterprises to Manage the IaaS Cloud Services"*. Proceedings of the 6th European Conference on Information Management and Evaluation (ECIME), Cork, Ireland, September 12-14, 2012, edited by Dr Tadgh Nagle, University College Cork, ISBN: 978-1-908272-65-2, pp.168, submitted to Thomson ISI for indexing

2. **A.M. Lonea**, D.E. Popescu, O. Prostean and H. Tianfield, *"Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud"*. Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary, in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 367-379, Springer-Verlag Heidelberg, 2013, *Agreement* SPIN: 86113511 GPU/PS: Science & Engineering/HS/89, ISSN: 1867-5662, (Accepted – Agreement SPIN: 86113511 GPU/PS: Science & Engineering/HS/89)

3. **A.M. Lonea**, *"Private Cloud Set Up Using Eucalyptus open source"*. Proceedings of the 5th International Workshop on Soft Computing Applications – SOFA 2012 August 22-24, 2012, Szeged, Hungary, in volume "Advances in Intelligent and Soft Computing", V.E. Balas et al. (Eds): Soft Computing Applications, AISC 195, pp. 381-389, Springer-Verlag Heidelberg, 2013, *Agreement* SPIN: 86113511 GPU/PS: Science & Engineering/HS/89, ISSN: 1867-5662, (Accepted – Agreement SPIN: 86113511 GPU/PS: Science & Engineering/HS/89)

**Book Chapter:**

- **A.M. Lonea**, H. Tianfield and D.E. Popescu, "*Identity Management for Cloud Computing*", Book Chapter in "New Concepts and Applications in Soft Computing", Studies in Computational Intelligence, Springer-Verlag, pp. 175-199, Volume 417/2013, ISBN: 978-3-642-28958-3

**Conference proceedings:**

1. **A.M. Lonea**, D.E. Popescu and O. Prostean, *"A Survey of Management Interfaces for Eucalyptus Cloud"*. IEEE 7th International Symposium on Applied Computational Intelligence and Informatics, SACI 2012, Timisora, Romania, May 24-26, 2012, pp. 261-266, ISBN: 978-1-4673-1013-0 **(IEEE)**

2. **A.M. Lonea**, "*Cloud Computing Security*". Second Workshop: Interdisciplinary and Research Management, "Politehnica" University of Timisoara, Timisoara, Romania, 24-25 November 2011.

3. **A.M. Lonea**, H. Tianfield, T. Buggy and O. Prostean, "*Cloud Security Architecture (CSA)*". Poster presented at Scottish Informatics and Computer Science Alliance (SICSA) PhD Conference, SICSA 2011 PhD Conference, Edinburgh, Scotland, 23-25 May 2011.

4. **A.M. Lonea** and D.E. Popescu, "*Security Issues For GRID Systems*", 4th International Workshop on Soft Computing Applications, SOFA 2010, Arad, Romania, ISBN: 978-1-4244-7985-6, July, 2010, pp. 73-76 **(IEEE)**