UNIVERSITATEA POLITEHNICA TIMISOARA

CLOUD COMPUTING CONCERNS AND SOLUTIONS

HABILITATION THESIS

DANIELA ELENA POPESCU
2017

Acknowledgements

To:

- Prof.dr.eng.Mircea Vlăduţiu
- The *Academic Computer School* from "POLITEHNICA" University of Timisoara
- My collegues from Computer Science and Information Technology Department
- My family

Table of Contents

REZUMAT

Teza mea de abilitare prezintă principalele realizări din activitatea științifică, didactică și profesională, realizate după dec. 1998, când am obținut titlul științific de doctor în domeniul „Știința Calculatoarelor”, la Universitatea ”POLITEHNICA” din Timișoara, Facultatea de Automatică și Calculatoare. Teza de doctorat a fost realizată sub îndrumarea D-lui Prof.dr.ing. Mircea Vlăduţiu.

Dupǎ obținerea titlului științific de doctor, am promovat pe plan didactic, pe bază de concurs, la poziția de conferențiar (în 1999), și pe urmă la poziția de profesor universitar (în 2003). În această perioadă am participat la o serie de proiecte de cercetare, dintre care la 3 am fost director de proiect. Am realizat, in calitate de autor sau co-autor, 8 cărți cu caracter didactic și **3** îndrumătoare de laborator, la care se adaugă și 2 capitole de carte la edituri internaționale și un suport media adițional pentru activități practice cu studenții pe care l-am pus la dispoziția studenților prin platforma de lucru Office 365.

Am fost autor sau co-autor la 25 articole indexate în baza de date ISI – Web of Science, dintre care 11 sunt în reviste cotate cu factor de impact, precum și la peste 20 articole indexate în baze de date internaționale. În perioada anilor 2010-2013 am fost implicată în Proiectul Erasmus de tip LLP-IP Intensive Programme (Long Life Learning – Intensive Programme): “Mobile and Web Development Technologies”, în care, în calitate de profesor, am predat module de curs cu tema *Mobile Cloud Computing* la Universitatea Politehnica Valencia-Campus Alcoi (Spania), La universitatea din Lahti (Finlanda) și la Universitatea din Oradea

De asemenea, în această perioadă, am fost recenzor la mai multe reviste și conferințe de prestigiu din domeniu (ca de exemplu International Journal of Advanced Intelligence Paradigms ISSN online: 1755-0394, Information Processing Letters 2014, Future Technologies Conference (FTC) 2016), expert CNCSIS (2004-2005), expert ARACIS (2015) și în 2017 expert la Comisia Europeana la programul HORIZONT 2020, apelul: H2020-SESAR-2016 call.

Teza de abilitare este structurată pe 7 capitole, împărţite în 3 părţi principale: prima parte, care conține 5 capitole, este dedicată realizărilor științifice; ce-a de-a doua parte este dedicată realizărilor profesionale și academice și prezintă planul de evoluție și dezvoltare a carierei, avut in vedere după obținerea abilitării de a conduce lucrări de doctorat; partea finală reprezintǎ o listă cu referințe bibliografice, în care sunt incluse și realizările științifice proprii.

În capitolul 2, “Securitatea Cloud Computing” am prezentat problemele generale ale securității cloud computing. Am pornit de la definirea modelului cloud computing, a problemelor de securitate asociate acestuia şi am prezentat modul în care trebuie gestionată securitatea cloud. Vulnerabilitățile, amenințările și riscurile asociate cloud computingului sunt şi ele prezentate în acest capitol.

Capitolul 3 este capitolul cel mai amplu şi consistent al primei părţi şi prezintă câteva soluții ce se impun pentru a asigura cele 3 elemente de securitate cloud: securitatea identității, securitatea informației şi securitatea infrastructurii. Cu referire la securitatea identității, am abordat problema *Identity Access Management* (IAM), şi am făcut o prezentare sumară a protocoalelor implicate, a standardelor existente pentru

federalizare şi a soluțiilor existente pentru (IAM). Acestea au fost publicate sub forma unui capitol de carte în Springer. Pentru autentificare este prezentată o soluție originală de autentificare hibridă, bazată pe utilizare text/imagine. O soluție pentru asigurarea securității informației este data de steganografie, care oferă posibilitatea de asigurare a confidențialității datelor în cloud (prin ascundere). Combinarea criptării cu steganografia se prefigurează ca fiind de perspectivă pentru asigurarea securității în domeniu. Pornind de la acest aspect, în ultima perioada am fost preocupată de performanța soluțiilor ce pot fi obținute prin utilizarea steganografiei şi am avut câteva contribuții științifice în acest sens, pe care le prezint în cadrul acestui capitol.

În cadrul secțiunii: *Arhitecturi de Securitate cloud*, pornind de la o soluție arhitecturală de securitate bazată pe 4 straturi de securitate, este dezvoltată o soluție arhitecturală cu 5 straturi de securitate, care asigură confidențialitatea, prin ascundere, a datelor memorate în cloud şi are ca şi scop creșterea gradului de încredere al clienților cu privire la asigurarea confidențialității datelor din cloud. Acest al 5lea nivel (adițional) are la bază utilizarea tehnicilor steganografice, cu suport de acoperire imagine.

Tot în cadrul capitolului 3, prezint o soluție ce permite detectarea atacurilor DDoS în mediu cloud bazată pe utilizarea sistemului de detecție al intruziunilor (*Intrusion Detection System*) şi a teoriei Dempster Schefer. Soluția prezentată a fost publicată, şi a fost şi implementată fizic, iar rezultatele experimentale i-au dovedit eficiența.

Capitolul 4 este un capitol în care abordez problemele de optimizare a alocării resurselor în cloud, în scopul asigurării unei disponibilități cât mai ridicate a datelor în mediul cloud. Prezint o soluție de alocare bazată pe un model ce identifică resursele implicate pentru realizarea serviciilor, o soluție de optimizare, a disponibilității fișierelor într-o reţea de tip P2P, bazată pe utilizarea algoritmilor genetici.

Problema delicată a migrării datelor în cloud pentru IMM-uri este abordată în capitolul 5. Se prezintă întreg procesul pe care trebuie sa îl considere o întreprindere pentru a realiza cu succes, şi eficient, o astfel de migrare într-un mediu cloud hybrid. Ca şi soluție de implementare a cloud-ului privat este prezentată platforma open-source Eucalyaptus, pe care am folosit-o, iar pentru managementul platformei se folosesc interfețele pentru management asociate ei, pentru care se face o trecere în revista şi o evaluare a avantajelor şi dezavantajelor oferite de fiecare în parte. Elementele de bază ale managementului securității cloud sunt şi ele prezentate în capitolul 5. În finalul capitolului este prezentată şi o soluție, publicată într-un articol ISI, pentru un sistem de management al serviciilor cloud pentru clustere inovative.

În capitolul 6 sunt prezentate realizările profesionale şi academice, precum şi planul de evoluție şi dezvoltare a carierei avut în vedere după obținerea dreptului de a conduce lucrări de doctorat, iar în capitolul 7 este prezentată o listă cu referințe bibliografice, în care sunt incluse şi realizările științifice proprii.

ABSTRACT

My habilitation thesis presents my main achievements in the scientific, didactic and professional activity, realized after dec. 1998, when I obtained my PhD in Computer Science, at the "POLITEHNICA" University of Timisoara, Faculty of Automation and Computer Science. The doctoral thesis was conducted under the guidance of Prof.dr.ing. Mircea Vlăduţiu, and the thesis was defended at "POLITEHNICA" University of Timisoara.

After obtaining my PhD, I was promoted on a competitive basis to the position of associate professor (in 1999) and then to the position of university professor (in 2003). During this periode I participated in a series of research grants, at three of them I was a director. In this periode I was author or co-author of 8 books and 3 practical guides, 2 book chapters at an international publishing house and some additional media supports for practical activities, available on my personal website and on the website of the University of Oradea. I also was author or co-author of 25 papers indexed in the ISI-Web of Science database, 11 of them being articles in journals, with impact factor, as well as more than 20 papers indexed in international databases.

During the years 2010-2013 I was involved in the Erasmus LLP-IP (Long Life Learning – Intensive Programme), "Mobile and Web Development Technologies", in which, as a teacher, I taught course modules on “Mobile Cloud Computing” at Universitat Politechnica de Valencia (Alcoi Campus- Spain), Lahti University (Finland) and University of Oradea (Romania).

In this period I also was reviewer at several prestigious journals and conferences (as International Journal of Advanced Intelligence Paradigms ISSN online: 1755-0394, Future Technologies Conference (FTC) 2016). I was also expert CNCSIS (2004-2005), expert ARACIS (2015) and in 2016-2017 Expert to the European Commission on the H2020-SESAR-2016 call.

The habilitation thesis is structured on 7 chapters, divided in 3 main parts namely: the first part has 6 chapters and is dedicated to scientific achievements; the second part is dedicated to professional and academic achievements and plans of carrier evolution and development, after the habilitation attainment; the final part represents a references list, including the personal scientific achievements.

In Chapter 2, "Cloud Computing Security", I have presented the general problems of cloud computing security. I started from defining the cloud computing model, the security issues associated with it, and I presented how cloud security should be managed. The vulnerabilities, threats and risks associated with cloud computing are also presented in this chapter.

Chapter 3 is the most comprehensive and consistent chapter of the first part and shows some solutions that are required to provide the three cloud security factors: identity security, information security, and infrastructure security.

Regarding identity security, I approached Identity Access Management (IAM), and made a brief presentation of the involved protocols, existing federation standards, and existing IAM solutions. These were published as a Springer book chapter. For Authentication, an original Hybrid Authentication solution based on text / image usage is presented. For ensuring information security one of the solutions is steganography, which provides the ability to secure confidentiality of data in cloud (by hiding). The combination of cryptography and steganography is Is prefigured as perspective for ensuring security in the field. Starting from this point of view, lately I was concerned

about the performance of the solutions that can be obtained by using steganography and I have had some scientific contributions in this regard that I present in this chapter.

In the section: Cloud Security Architectures, starting with an architectural security solution based on 4 layers of security, an architectural 5-layer security solution is developed. This ensures confidentiality by hiding data stored in the cloud, and aims to increase the confidence of customers in securing confidentiality of cloud data. This 5th level (additional) is based on the use of steganography techniques with image coverage support.

Also in Chapter 3, I present a solution for detecting DDoS attacks in a cloud environment based on the Intrusion Detection System and Dempster Schefer theory. The solution presented was published, and it was physically implemented, and the experimental results proved the effectiveness of the solution.

Chapter 4 is a chapter on how to optimize resource allocation in the cloud to ensure a higher availability of cloud data. I present an allocation solution based on a model that identifies the resources involved in delivering services, and an optimization solution for the availability of files in a P2P network based on the use of genetic algorithms.

The delicate issue of cloud data migration for SMEs is addressed in Chapter 5. It presents the entire process that a business must consider to successfully and efficiently achieve such migration in a hybrid cloud environment. As an implementation solution for the private cloud, the Eucalyptus open-source platform is used, and platform management is based on the associated management interfaces that are presented together with an evaluation of the benefits and disadvantages offered by each one. The basic elements of cloud security management are also presented in Chapter 5. At the end of the chapter is presented a solution for a cloud management cluster innovation system that was published in an ISI article

Chapter 6 presents the professional and academic achievements as well as the career development and career development plan envisaged after obtaining the right to conduct doctoral work

Chapter 7 presents a list of bibliographical references, including my scientific achievements.

PART I SCIENCIFIC ACHIEVEMENTS

1 INTRODUCTION

Over the last past 18 years, my research concerns have evolved and tracked the dynamics of the field.

In the first period, I was concerned about issues related with reliability, testability, especially in the field of computer architectures, after which my concerns were focused on physical security. The latter were directly related with the activity to my company (ACTUAL SRL) focused on design, execution and consultancy in the field of physical security, which I was forced to lead in the period 2006-2010.

With the emergence of the cloud computing paradigm, my concerns have been addressed in this area. The globalization of IT infrastructures has raised a new issue, which has become of major importance: it is the issue of information security particularly the confidentiality of data. There is also an European regulation that have to be implemented in Romania by May 2018 (GDPR). In view of these issues, a great effort of current research in the field of computing engineering is being phased in this direction. But the dynamic is huge! For example, for the Identity Access Management – one of the major security issues today, Gartner has predicted for 2020 a lot of changes. One of them is related with the IoT technologies and Gartner says that: “the Internet of Things will redefine the concept of Identity Management to include what people own, share, and use”. Gartner also predicts that: “By 2020, over 80% of enterprises will allow unrestricted access to non-critical assets reducing spending on IAM by 25%” and “70% of businesses will use attribute-based access control (ABAC) to protect critical assets” [R 72].

On the other hand, we already assist to the development of new IoT technologies, and new ideas for new computing paradigms such as P2P cloud storage, etc., which are starting to populate our world.

New technologies have emerged and are developing, as: AI & Advanced Machine Learning, Intelligent Apps, Intelligent, even adaptive security architecture, etc… All of them represents new challenges for the research community in the field. These new trends are leading companies in the Fourth Industrial Revolution universe, a vibrating universe in the rhythm of the eight billion connected devices existing on the planet today (by 2031 forecasts will increase to more than 200 billion devices); it is a combination of cyber-physical systems, the Internet of Things and the Internet of Systems.

Therefore, in the habilitation thesis, I focused on formulating a material that gathered under the umbrella of cloud computing paradigm concerns as much as possible from the results of my research effort in recent years. This is the moment when, Gartner say: “cloud should move away from experimentation and towards enterprise-wide implementation” [R 195]

The research period that should be covered in this thesis is great. 18 years in our field means a lot. 18 years already outlines more "historical" moments of evolution in the field. Therefore, the dynamics of the field has forced me to report the thesis to the results of my research from the last, at most, 10 years.

2 Cloud Computing Concerns

Cloud computing as actually one of the most popular themes of information computing is still at the wish list of many organizations [R 10] and one of the most important current research topics [R 28].

Cloud Computing is a technology which aims to provide on-demand scalable services over the Internet via Cloud vendors to multi-tenant organizations. Enterprises are interested to move their on-premises infrastructure into cloud computing. However, they are still concerned about the security risks implied by the act of embedding their resources within the cloud computing environment.

Cloud computing, can be seen as a service-oriented architecture (SOA) exploring almost every computing component including, but not limited to distributed computing, grid computing, utility computing, on-demand, open source, Peer-to-Peer and Web 2.0 [R 208]. It represents the natural next step from the grid model to a supply and demand utility model.

A trusted Identity and Access Management architecture for cloud services assumes establishing the list of the security requirements and using the suitable standards. The paper also relates an evaluation of the existing Identity Access Management solutions.

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” [R 138].

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 enterprises. 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) [R 21].

Enterprises are still concerned about the security risks implied by the act of embedding their resources within the cloud computing environment [R 177]. The cloud security research done till now reveals the necessity for improving the security in the Cloud Computing field [R 177], [R 35], [R 31] [R 104], [R 81], [R 96], [R 110], [R 1], [R 82], [R 170], [R 220], [R 105].

Identities, infrastructure and information are the principal elements for securing the cloud [R 180] (Figure 1).

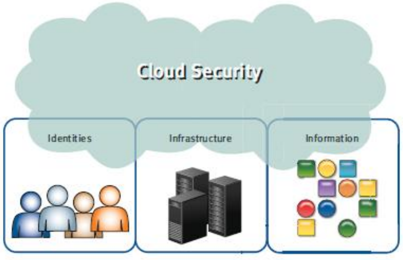


Figure 1 Cloud Security elements **[R 180]**

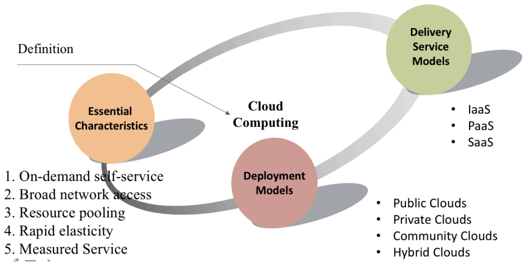


Figure 2 Cloud Computing according NIST

2.1 Cloud Computing definitions

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 [R 70] Three fundamental delivery models are for the cloud architecture: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

I. *Infrastructure-as-a-Service (IaaS)* is a cloud model that gives the infrastructure to the customers, who rent them from the cloud providers [R 177]. This infrastructure is deployed and used remotely by the clients [R 69]. The host infrastructure is complex [R 177]: computer hardware, computer network (routers, firewalls, load balancing etc.), Internet connectivity, platform virtualization environment, service-level agreements and utility computing billing.

II. *Platform-as-a-Service (PaaS)* is a Cloud model that makes available for the customers the Cloud infrastructure. PaaS provides the developers with the appropriate flavors of operating systems, databases, middleware, software tools and managed services, usually in a multitenant environment, where they should deploy the applications using the programming languages and the tools supported by the provider. The consumers had to look over the deployed applications [R 35] and not over the infrastructure.

III. *Software-as-a-Service (SaaS)* is a Cloud model which delivers the usage of software through Internet to the clients, who must pay for the applications [R 177]; they don't have to take care on the installation and maintenance of the software and with the management and the control of the Cloud infrastructure [R 35].

There are four deployment models for Cloud services [4]:

I. *Public Cloud* – can 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* **-** are owned and used by a single organization, which decrease the security exposures and eliminate the constraints of legal requirements and network restrictions [R 25]. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. del provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

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 to get better results in their businesses.

IV. *Hybrid Cloud* **–** put together two or more clouds (private, public or community) to mix the features of each delivery model and to increase the reliability and the complexity. It allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model can provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

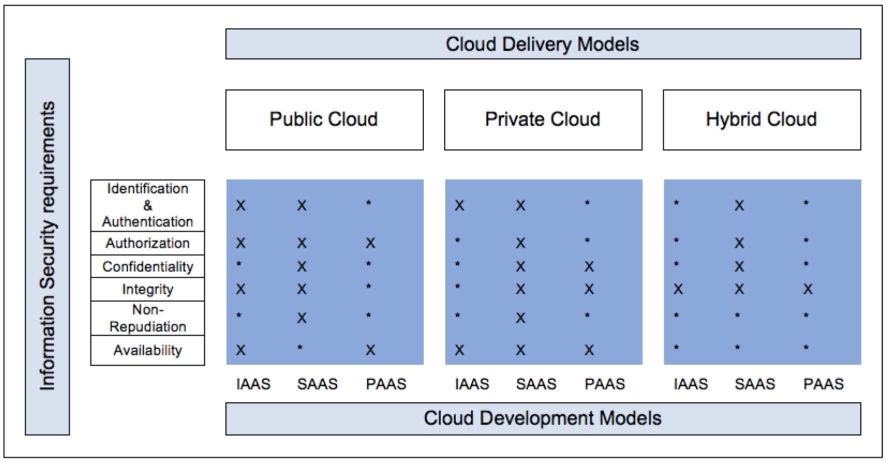
In Table 1 are summarized the various features of these cloud deployment models.

Deployment Model	Managed By	Infrastructure Owned By	Infrastructure Located At	Accessible and Consumed By
Public	Third party provider	Third party provider	Off-premise	Untrusted
Private	Organization (on-premise private clouds)	Organization	On-premise Off-premise	Trusted
	Third party provider (externally hosted private clouds)	Third party provider	On-premise Off-premise	
Community	Third party provider Organization	Third party provider Organization	Off-premise On-premise	Untrusted or Trusted
Hybrid	Both organization and third party provider	Both organization and third party provider	Both On-premise and Off-premise	Trusted or Untrusted

Table 1 Summary of the various features of cloud models

2.2 *Information security requirements*

Cloud computing security should be guided by the ISO 7498-2 standard [R 99], produced by *The International Standards Organisation* (ISO), in order to become an effective and secure technology solution. Figure 3, has been adapted from Eloff et al [R 170], and is illustrating the information security requirements coupled with the Cloud computing deployment model and delivery models. It should be viewed in context as a guideline in assessing the security level. These security requirements in context of Cloud computing are explained in [R 66] and Table 2.



	Public Cloud			Private Cloud			Hybrid Cloud		
	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS
Identification & Authentication	X	X	*	X	X	*	*	X	*
Authorization	X	X	X	*	X	*	*	X	*
Confidentiality	*	X	*	*	X	X	*	X	*
Integrity	X	X	*	*	X	X	X	X	X
Non-Repudiation	*	X	*	*	X	*	*	*	*
Availability	X	*	X	X	X	X	*	*	*

Figure 3 Cloud Computing Security Requirements (X = manadatory requirements, * = optional requirement), taken from [R 170]

	Information Security requirements	Description
1.	Identification & authentication	This process aims at verifying and validating individual cloud users by using user names and passwords in their cloud profiles. First, the specified users (depending on the type of cloud and the delivery model) are set, and additional priorities and permissions can be granted accordingly.
2.	Authorization	The authorization ensures the maintenance of referential integrity. It results in the control and privileges of process streams within Cloud computing and is maintained by the system administrator in a private cloud.
3.	Confidentiality	Privacy is a must when using a public cloud due to the public nature of cloud accessibility. It plays a major role in maintaining distributed data management across multiple distributed databases.
4.	Integrity	For preserving the data integrity in cloud computing, the ACID (atomicity, consistency, isolation, and durability) properties of the cloud's data must be imposed across all Cloud computing delivery models. The data integrity requirement is related to background checks in the cloud, especially when we access the data.
5.	Non-repudiation	Non-repudiation in Cloud computing is accomplished by applying traditional e-commerce security protocols and supplying tokens for data transmission in cloud applications such as digital signatures, timestamps, and confirmation receipts services.
6.	Availability	Availability is one of the most important security requirements for Cloud Computing information. It's actually a key factor in making decisions about the cloud type, cloud service providers, and delivery models. The Service Level Agreement is the most important document that highlights the availability of cloud and resource services between the cloud provider and the client.

Table 2 information security requirements

Therefore, by exploring the information security requirements at each of the various cloud deployment and delivery models set out by the ISO, vendors and organizations can become confident in promoting a highly protected safe and solid cloud framework.

2.3 Cloud Computing Threats, Vulnerabilities and Risks

The words *Vulnerability*, *Threat*, *Risk*, and *Exposure* often are used to represent the same thing even though they have different meanings and relationships to each other. A *Threat* is any potential danger to information or systems. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. Threats exploit existing vulnerabilities to cause damage or destruct a resource.

Vulnerability refers to a software, hardware, or procedural weakness that may provide an attacker the open door to enter a computer or network and have unauthorized access to resources within the environment. Vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software, or an unsecured physical entrance [R 106].

A *Risk* is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. The potential risks are mitigated using *controls.* A control may be a policy, procedure, a software configuration, or a hardware device that eliminates vulnerability or reduces the likelihood that a threat agent will be able to exploit vulnerability. In any enterprise, information security risks must be identified, evaluated, analyzed, treated and properly reported.

2.3.1 Security Threats in Cloud Computing

Service Oriented Architecture (SOA) and virtualization techniques are at the base of Cloud Computing, even they rise some security issues. Potential internal attackers are employees of third-party cloud service providers, clients, or third-party organization with direct access to privileged roles. All of them can exploit their privileged role in attacking services [R 31]. They are also external attackers who can compromise cloud services. They can cause several problems, which can be classified as follows: web applications security issues and virtualization security issues [R 129].

2.3.1.1 Web Applications Security Issues

SOA is an architecture based on a collection of services (e.g. web services), which provides the interaction between the distributed systems [R 191], [R 73]. A *Web Service* is a software system which provides interoperability between heterogeneous and distributed systems [R 146]. 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)* [R 181]. Unlike the browser-based interaction, in Web services is realized an application-to-application interaction [R 50]. While *XML* is used to tag the data, *SOAP* is used to exchange the XML messages [R 207]. To describe the available services is used the *WSDL* standard and for listing these services is used *UDDI* standard [R 181] [R 129].

By embracing Internet standards using XML-based Web Services (WS), the SOA approach offers a great IT flexibility and agility. It enables organizations to "publish" their services for the multitudes of potential internal and external service consumers [R 12] [R 129].

Both Web applications and SOA/WS-based applications can be deployed on an intranet (for company use), an extranet (for business partners), or even the public Internet (for consumers). But 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 [R 12] [R 129].

Attackers could affect the clouds services security attributes: availability, integrity and confidentiality. Table 3 presents the 2 types of security concerns in Cloud applications: wrapping attacks and browser security issues (e.g. account Hijacking, spoofing attacks), together with the mitigation techniques for each threat type [R 129].

	Threats		Mitigation techniques
Web Applications Security Issues	Wrapping attacks		• XML schema validation and Secure policy validation
	Browser security issues	Account Hijacking	• Multi-factor authentication • Monitoring solutions • Anomaly detection
		Spoofing Attacks 1. Cloud malware injection attack 2. Metadata spoofing attacks	• Hash service integration check • the use of a third-party detector tool

Table 3 Web applications threats and mitigation techniques [R 129]

Wrapping attack

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* [R 213]. *XML Signature* is used in Cloud platforms for signing digitally the XML fragments [R 104] - providing integrity and authentication. But, McIntosh and Austel discovered, that the SOAP message protected by XML Signature could be modified without invalidating the signature [R 82]. This attack could affect the cloud, and it was named *XML Signature Element wrapping attack* (*wrapping attack)*, or *XML rewriting attack* [R 129]. The solutions identified for this attack are [R 129]:

- *The inline approach* solution, which creates another element, the *SOAP Account*, that assures the detection of a possible attack, by keeping on it the following SOAP properties [R 81]: 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. 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. This solution can be broken and the SOAP Account element is not standardized. An alternate solution is the use of *verification* component *as a filter*.
- *XML Schema Validation* and *Security Policy Validation,* proposed by Gruschka and Iacono (2009), will not allow such a vulnerability to happen. It confirms if the incoming message is syntactically correct and it came for the unique ID and it helps to discover earlier the Denial-of-Service attack. Security Policy Validation should be done to verify if all assertions are fulfilled [R 81] [R 129].

Browser security issues

Browser security issues are related to the existent vulnerabilities on the cloud authentication procedure [R 129].

The threats called ***Account Hijacking*** (pharming, phishing and email-based attacks), open doors into the cloud accounts [R 211], by redirecting the victims to a fake web page to find their username and password. The web browser constitutes the Input/Output (I/O) into the cloud service for the cloud customers (Figure 4) [R 104] [R 129].

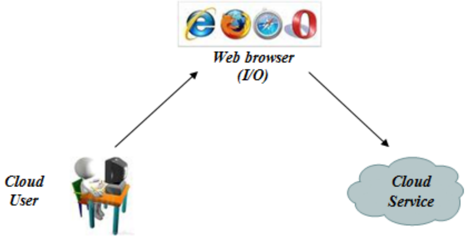


Figure 4. Web browser relationships [R 129].

As a solution, in [R 104] is suggested the use of *SAML* (*Security Assertion Markup Language*) for providing strong authentication and the increase of API (*Application Programming Interface*) security for addressing the browser enhancements [R 129].

Proposed solutions for mitigate the account hijacking threat are: using a multi-factor authentication mechanism instead of a one-factor authentication; the interdiction of the transmission of the account credentials between the providers and the clients and the use of monitoring solutions for detecting illegitimate users [R 36]. So, the anomaly detection of the user login into the cloud management interface is an alert signalizing that the user credentials could be compromised [R 54]. As a solution for the apparition of new threats into the cloud system after the Account Hijacking attack was realize, in [R 211] is given the *Unisys Secure Cloud* architecture solution, which embraces a "*defence in depth*" method, based on strong cryptographic authentication and on a detection system of unauthorized access [R 129].

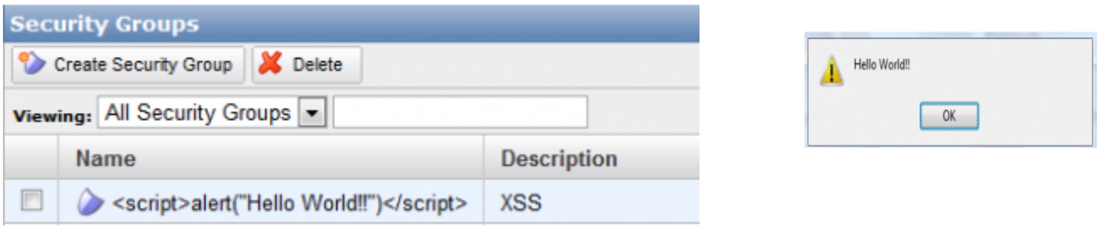
Spoofing attacks

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. Thus, malware injection attacks such as viruses or Trojan horses could be added by intruders into the Cloud systems [R 103]. Such an attack is done by an enemy, who inserts its malicious instance into the cloud and then the end-users will be redirected to use that malicious service implementation [R 104]. The injection attacks attempt to use the cloud services and applications vulnerabilities by using erroneous input by the attacker to inject the cloud environment with undesirable consequence for programmers. There are the following types of injection attacks [R 80] [R 129]:

- *SQL injection* – attacker introduces a malicious SQL code into the input field, to realize unwanted actions into the database
- *Cross-site scripting (XSS) injection* - an example (Figure 5) is introducing a script instead of a security group name in the Amazon EC2 API [R 51]

-



Security Groups

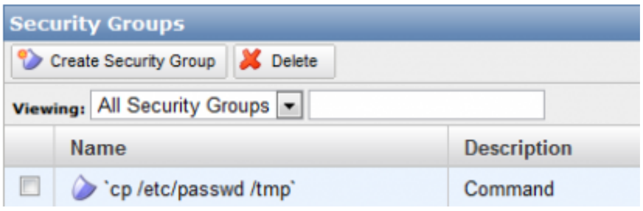
Viewing: All Security Groups

	Name	Description
□	<script>alert("Hello World!!")</script>	XSS

Hello World!!

Figure 5 XSS Attack into the Amazon EC2 API [R 129]

- *Command injection* – attacker introduces malicious command into the input field, which will cause 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 [R 51] (Figure 6).



Security Groups

Viewing: All Security Groups

	Name	Description
□	`cp /etc/passwd /tmp`	Command

Figure 6 Command injection attack into Amazon EC2 API [].

The best measure to protect against Injection attack 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 [R 104].

Another solution for combating these injection attacks is the use of a third-party detector tool like *Elastic Detector* [R 51] [R 129].

2. Metadata spoofing attacks

By changing the metadata WSDL description, this type of attack could pose troubles for the Cloud services. By modifying a service's WSDL, the attacker will achieve confidential information.

If the attacker changes syntactically the operation of a service to do something else, that could be a serious drawback for the Cloud (e.g change the deleteUser operation to do what the setAdminRights should do). The solution to detect these types of attacks is the use of a *hash-based integrity verification* of the metadata description should be done [R 104] [R 129].

2.3.1.2 Virtualization Security Issues

Virtualization does not provide full control over data availability. It allows services to be provided on demand in the Cloud environment, but at the same time allows the requesting of a Cloud service from an illegitimate user [R 104]. The intruder user may rent virtual resources and computing assets. Using virtual machines, a potential attacker will try to generate a powerful attack on the Cloud, trying to make Cloud services unavailable by compromising the data and modified them, or even losing that data [R 129].

Table 4 summarizes virtualization threats and mitigation strategies.

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

Table 4 Virtualization threats and mitigation techniques [R 129]

Flooding attacks

The maintenance of the availability of cloud services is an important security issue of cloud, that can be serious be affected by the overload of cloud network traffic realized by the *flooding attacks* (*Denial of Service attack*); this could make the cloud services unavailable [R 104]. A real damage for the Cloud could be the flooding attacks (Denial of Service attack), by overloading the cloud network traffic. This makes the Cloud services unavailable [R 104].

There are two types of Denial-of-Service attack: direct and indirect [R 129].

The Direct denial-of-service attack appears When a service from Cloud system is overloaded with nonsense requests; this type of attack will conduit at unavailability of that service.

The *indirect denial-of-service attack* or a *target denial-of-service attack* [R 31] [R 104] appears when a denial-of-service attack over a service to affect other services that are located in the same server. In this case, the downtime of those services is produced by the deficiency of the hypervisor and virtual machines to respond to the fakes requests [R 31].

As solutions responding to the flooding attacks were proposed: the increasing the bills for Cloud usage and the use of a virtual Demilitarized Zone (DMZ) area in the Cloud infrastructure [R 23] – which is a better solution [R 129].

Virtual-machine template images

When the template images are cloned, these Virtual-machine (VM) template images could produce the spreading of vulnerabilities [R 80]. This 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). This vulnerability can cause *data leakage*, as cloning a VM template image in another host means makes certain elements of an operating system public that should be private to a single host [R 129].

The solution for combating a possible attack is to use a firewall and an intrusion detection and prevention system [R 200].

Side channel attack

As shows in [R 176] the cloud-computing environment cloud is affected by side channel attack. The case study presented in [R 176] was done using Amazon's EC2 cloud provider, but it could be also applied for Microsoft's Azure or Rackspace's Mosso. This type of attack obtains information from the VM victim by placing the VM attacker in the same physical space with the victim, and then, the attacker will extract confidential information [R 43]. Consequently, the isolation between virtual machines provided by the hypervisor could be broken by the adversary. Thus, there are recommended the following mitigation techniques [R 129]:

1. resource monitoring and a strong authentication and authorization [R 37].
2. implement private VLAN clouds for each cloud customer to avoid the problem attacks if one of the cloud customers is compromised [R 23].

2.3.2 Security Vulnerabilities in Cloud Computing

The most important vulnerabilities related to Cloud security, were identified by CSA who conducted a survey among industry experts. Based on this study, the final report for 2013 [R 26] was drawn up, a report in which the following critical security issues were identified in the order of their severity:

Vulnerability name	Description	Consequences	Measure to address the vulnerability
Data breaches	A virtual machine can access the data from another virtual machine on the same physical host – the problem is more prevalent when the tenants of the two virtual machines are different customers.	- The side-channel attacks. Occurs when a virtual machine can use a shared component to access the data of another virtual machine running on the same physical host [R 219].	Mitigation is complicated and the measures may affect data loss - encrypt all the client data and the clients need to have backup copies to be protected against Data Loss if the encryption key is lost
Data Loss	Permanent loss of customer data (unless there are copies of data)	- can have **catastrophic consequences** to the business - could **jeopardize the organization's compliance** (if these documents are in cloud)	- a **proper data backup off-line** or **on-line (**for services with zero-tolerance for data loss) **-** this task regards both the provider and the customer
Account / service Hijacking	The attacker after getting access to the clients credentials, can track their activities and transactions, manipulate their data, respond with false information, redirect their customers to illegal sites.	- can compromise the confidentiality, availability and integrity for cloud services - can be a starting point for launching further attacks.	- increase the awernass - **prohibit** the exchange of credentials between users and services, - use **strong authentication techniques** where possible.
Unsafe APIs	API's are used for provisioning, management, orchestration and monitoring. Their availability and security affects the availability and security of cloud services.	- can compromise the confidentiality and integrity of the cloud services ~~customers~~.	- Cloud service Providers must **provide secure API** - APIs must assure strong authentication and access control, encryption and monitoring. - the vendors must work to **guarantee service security** - users must **understand the security implications** of using APIs.

Vulnerability name	Description	Consequences	Measure to address the vulnerability
Denial of Service (DoS) & Distributed Denial of Service (DDoS)	An attacker can issue a denial of service attack against the cloud service to render it inaccessible, therefore disrupting the service. This can be done by using all its CPU, RAM, disk space or network bandwidth.	Can bring down the hole cloud - service interruptions for consumers - The possibility to use so much processing time to become too expensive for the customer, who must stop to use the services	- **strong authentication** - the **network monitoring traffic** behavior to distinguish between legitimate users and attack traffic, that must be blocked - A hybrid cloud DDoS protection solution - the use of security appliances like: firewalls, intrusion-detection, intrusion prevention systems
Malicious Insiders	Cloud service provides often don't follow the best security guidelines and don't implement a security policy, so, employees can gather confidential information from arbitrary customers without being detected.	The result may be: - data leakage - severe corruption of the affected systems and data. - business impact for the provider (even significant)	- Cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data
Insufficient due diligence	Without a good understanding of applications or services in the Cloud, and operational responsibilities organizations reach unknown levels of risk.	- operational and architectural problems.	- Organizations should not migrate to use Cloud services unless they are fully aware of their capabilities and certain that they have the human and IT resources needed
Issues with distributed technologies	Cloud computing services relies on many backend technologies Whose vulnerabilities can lea to exploitation in all clients. All layers of shared technology can be attacked to gain unauthorized access to data, like: CPU, RAM, hypervisors, applications, etc.	- it can affect a whole Cloud system (when an integral part is compromised it exposes the entire environment)	- Keeping systems updated and giving high attention to configuration can reduce the risk - A well-established **defense strategy** is recommended, which should be deployed at each cloud level
Unknown Risk Profile	There might be multiple attacks that haven't even been discovered yet, but they might prove to be highly threatening in the years to come.	- unpredictable	- all **security implications** must be considered when moving to the cloud, including constant software security updates, monitoring networks with IDS/IPS systems, log monitoring, integrating SIEM into the network, etc.
User Awareness	There are multiple social engineering attack vectors that an attacker might use to lure the victim into visiting a malicious web site, after which he can get access to the user's computer.	- unpredictable	- The users of the cloud services should be educated regarding different attacks, because the weakest link is often the user itself.

Table 5 Vulnerabilities in Cloud Computing

2.3.3 Security Risks in Cloud Computing

There are five security issues that should be considered and included in the typical Service Level Agreement (SLA) content. These are the following: privileged user access, data location, data segregation, data disposal and e-investigations and protective monitoring [R 110].

1. *Privileged user access* means - the data stored in cloud could be accessed only by authorized users, which are specified by the provider. Securing access and technical solutions are the tasks of the cloud provider [R 31].
2. *Data location* - The lack of visibility of the storage location requires cloud customers to ask the cloud provider for information about the jurisdiction of the country where the data is hosted (tax may be needed). Another aspect related to the location is that the decryption key and data in some cases must be seen by an audit or validation by a third party [R 109]. This data location uncertainty could generate other security risks such as macroeconomic risks [R 31], or environmental risk (Depending on the storage region there are disaster exposures such as earthquakes, floods and extreme weather conditions that could damage the security of customer data).
3. *Segregation of data - One of the key features of the cloud is that it is a multi-tenant; multiple customer' data are stored in the clouds. Segregation between user data is therefore required to protect other cloud customer in an attack situation, when an attack occurs on a particular user* [R 110]. On the other hand, *by the use of virtualization technology, Cloud Computing is exposed to attackers who will try to break down the cloud hypervisor* [R 31].
4. *Data Disposal* remains a securiy risk in Cloud Computing. Cloud Computing save the data of the customers for backups, data stores and physical media. When a client decides to delete cloud data, Cloud Storage can not resolve the situation due to multiple copies of data.(de exemplu pentru backup) [R 31].
5. *Investigations and protective monitoring* **-** means to place the security between the cloud service and cloud user.

All these five security risks require further development in the security context. Today's companies were developed specific methods to assure for their cloud customers secure environment.

3 Cloud security solutions

3.1 Identity Security Solution

Cloud service providers need to establish secure access and technical solutions to ensure they have the right people to access the right services. In this way, the data that will be stored in the cloud can only be accessed by authorized users, which are specified by the vendor. The best solution is to integrate access to data and services in the *Identity and Access Management Infrastructure* (IAM).

User security control is correlated with identity security that needs to find the best solution to meet all the 5 necessary identity security requirements: strong authentication, identity provisioning, identity federation, and granular authorization [R 35] [R 129] (Figure 7).

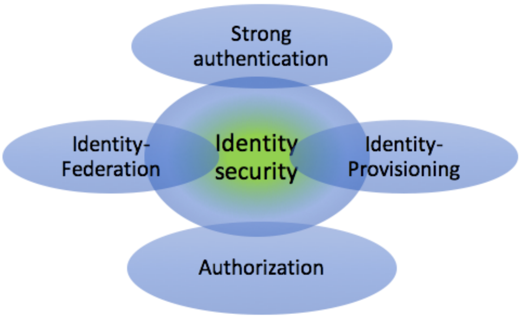


Figure 7 Identity Security Requirements

CSA provides in [R 35] a guidance for creating strong authentication and it introduce also the notion Identity as a Service (IDaaS). IDaaS appears to become an IT service as mobile phones are and as DNS provider deliver reliable and available naming services for customers [R 157].

3.1.1 Identity and Access Management (IAM) for Cloud Computing

An organization's identity services into the cloud is a prerequisite for strategic use of on-demand computing services [R 37].

Identity and access management (IAM) is the discipline for managing access to enterprise resources. It is a foundational element of any information security program and one of the security areas that users interact with the most [R 56] [R 129].

The traditional IAM solutions cannot be applied for the cloud computing services. This is because the companies don't have enough control on the cloud service provider's IAM [R 106] and because the enterprises need to create a compatible identity infrastructure that must be integrated within many cloud services using a secure linkage [R 157].

Identity and Access Management (IAM) for Cloud Computing has a different approach comparing with the traditional IAM, which tended to be centralized. It is producing the development of the Cloud Identity as a Service (IDaaS) architectures, which is recommended by Cloud Security Alliance [R 37].

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 [R 31]. The following four major IAM functions are essential for successful and effective management of identities in the cloud:

1. Identity provisioning/de-provisioning
2. Authentication & Federation
3. Access Control & user profile management
4. Support for compliance

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. One of the major challenges for organizations adopting cloud computing services is the secure and timely management of provisioning and de-provisioning of users in the cloud. 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 [R 36].

Authentication Requirement

After provisioning the accounts users to the Cloud services, the company's users could authenticate to the Cloud service, by confirming the access credentials which were obtained in the provisioning process. Authenticating users in a trustworthy and manageable manner is a vital requirement for the organizations using cloud services.

Therefore, organizations must address authentication-related issues such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services [R 36].

Identity Federation Requirement
Identity Federation should be realized 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 [R 106].
Federated Identity Management, in a cloud computing environment, enable organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP). A requirement for this context is the securely exchange of identity attributes between the service provider (SP) and the IdP.
Therefore, these organizations should understand the various possible solutions for addressing the challenges related with the identity lifecycle management, available authentication methods to protect confidentiality, and integrity, while supporting non-repudiation [R 36].

Access Control & User Profile Management:

- Access Control is the requirement that establish who has access to each resource. This access is specified in the security policies, with different content depending on the user profile information - depending on whether the user is acting on their own, or as a member of an organization. These are used to control access within the cloud service and should permit to be auditable [R 36].

Compliance:

- The understanding of how Identity Management can enable compliance with internal or regulatory requirements is important for cloud customers.
- A proper identity management ensure that account information, access grants and segregation of duty to cloud service providers can be considered together to meet the enterprise's audit and reporting requirements [R 36].

3.1.1.1 Necessary protocols for Identity and Access Management architecture

A trusted Identity and Access Management solution is creating using the suitable standards.

Standards for Provisioning/De-provisioning identities

There are two standards that are used for provisioning the users in the cloud services [R 129]:

- Services Provisioning Markup Language (SPML)
- *System for Cross-domain Identity Management* (SCIM) - currently appears from the initiative of Google, salesforce.com and Ping Identity

Services Provisioning Markup Languages (SPML)

SPML is an XML-based framework, developed by OASIS (*Advancing Open Standards for the Information Security*), PSTC (*Provisioning Services Technical Committee*) and that is used for provisioning users' identities, resources and services. 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 [R 152] [R 129].
SPML contains three main components (Figure 8): *Requesting Authority* (RA), *Provisioning Service Point* (PSP) and *Provisioning Service Target* (PST). RA is a 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 to realize the provisioning. This relationship must be established before provisioning; it assure the authentication of the identities participating in the process. These steps are compulsory for eliminating the possibility of creating attacks (like: DoS, impersonation) between the SPML parties. The third element in a SPML model of Figure 8 is the PST, which is an abstract end-point element in the provisioning process. In the requesting made by PSP to the PST, PST is behaving like PSP and PSP is behaving like [R 152] [R 129].

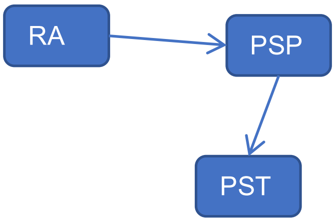


Figure 8 SPML System Elements adapted from **[R 129]**

System for Cross-domain Identity Management (SCIM)

The standard was initially called *Simple Cloud Identity Management*, but the name was officially changed to System for Cross-domain Identity Management (SCIM) when the IETF adopted it.

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 implement 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 [R 85]. SAML users change their options to JSON considering the difficulty of managing the features of SOAP [R 132] [R 129].

3.1.1.2 Standards for Identity federation

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 [R 160], [R 161]. Table 3 presents our comparison between the identity federation standards and after the identity federation standards (i.e. SAML, *Liberty Alliance, WS-Federation, Shibboleth*) are discussed [R 129].

Identity federation standards	Strengths	Weaknesses
SAML	• Dominant standard • Distributed model(federation) • Life cycle attributes of ID-FF • Privacy attributes of Shibboleth • Browser based identity federation	• Doesn't address identity requirements of web services
Liberty Alliance	• Life cycle attribute • Browser and Web Services based identity federation	• End of life
WS-Federation	• Web applications and web services identity federation • Support for SAML 2.0	• Dominant in Microsoft Windows servers
Shibboleth	• Assures several privacy features	• Strictly used in academic world • Strictly Open source implementation

Identity federation standards	Strengths	Weaknesses
		• Centralized identity storage model

Table 6 Comparison between the Identity Federation standards [R 129]

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 [R 154]. 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 that support the SAML standard are: *Ping Identity, IBM Tivoli, CA Federation, Juniper Networks* [R 129].

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) [R 106]. 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 [R 129].

A SAML entity consists of two parties:

1. SAML asserting party and
2. 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* [R 154]. 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 [R 154]. The subject of a cloud service is a user which wants to obtain a cloud service [R 129].

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 Figure 9. The authentication details of the user will be recognized by the service provider, who have them from the identity provider, with the specification that between the identity provider and the service provider exist a trust relationship. The user's information between the two web sites is transferred by the SAML standard [R 153]. 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 [R 154] [R 129].

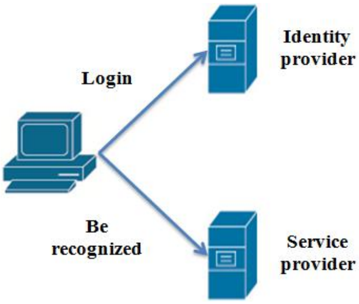


Figure 9 Single Sign-On [R 153]

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 [R 160]. Liberty (1.1, 1.2) is supported by IBM Tivoli Identity Federation [R 9] [R 129].

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 [R 161], [R 9] [R 129].

Shibboleth

Even if *Shibboleth* adopts several privacy functionalities, it is strictly used in academic or public world and it enhances a centralized identity storage model [R 134].

3.1.1.3 Solutions for authentication requirement

Authentication is the process of validating or confirming that access credentials provided by a user (for instance, a user ID and password) are valid. A user in this case could be a person, another application, or a service; all should be required to authenticate. A suitable authentication is vital for authorization (the process of granting access to requested resources). Authenticating users in a trustworthy and manageable manner becomes an additional challenge for organizations that begin to utilize applications in the cloud. [R 37].

Therefore, credential management, strong authentication, delegated authentication are leveraged across the cloud delivery models. Implementing authentication is very important, and organizations should also be carefully at the attack implications.

Authentication must be secured using the best techniques, because attacks (like: impersonation, phishing, brute force dictionary based password) could occur on the credential details. Decreasing the risks in the cloud environment should be a priority for Cloud providers and organizations that embrace cloud services. The solution must also be optimized in terms of cost [R 37].

Related with the 3 delivery models identified by NIST, it is important to point out that [R 129]:

- *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 [R 37].

- IaaS cloud environment disposes of 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, establishing a dedicated VPN, with the IaaS environment, is generally a better option, as they can leverage existing systems and processes. Thus, it can be applied the existing enterprise authentication systems such as Single Sign-On solution, or LDAP - based authentication service (Lightweight Directory Access Protocol) that provides an authoritative source of identity data.

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 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 (these must be limited). 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. With an OATH-compliant solution, companies can avoid becoming locked into one vendor's authentication credentials. OATH-compliant systems can support any similarly compliant form factor, including tokens, cell phones, and PDAs [R 37] [R 129].

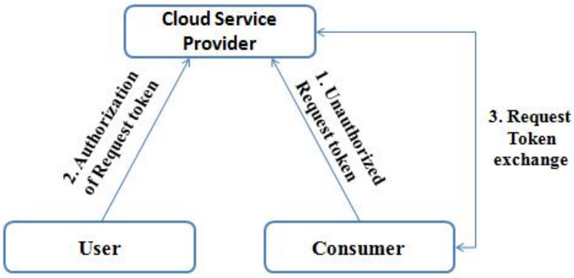
Standards for authorization requirement

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 authenticating the user in a cloud service, OAuth is used for allowing 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) [R 155] [R 129].

OAuth 2.0 appears in 2010, and had 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 [R 212] [R 129].

In the cloud computing landscape the parties involved by OAuth protocol are: the user, the OAuth Cloud service provider and the OAuth consumer (Figure 10). 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 [R 132], [R 212] [R 129].



Cloud Service Provider
2. Authorization of Request token
1. Unauthorized Request token
3. Request Token exchange
User
Consumer

Figure 10 OAuth token exchange [R 129]

Enterprise-centric authorization model

eXtensible Access Control Markup Languages (XACML) is an access control standard used for communicating policies by organizations, in order to access the online information[R 50]. Besides the policy language, XACML includes an access control decision request/response [R 197] [R 129].

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 (Figure 11) 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 [R 146] [R 129].

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-applicable) [R 146], [R 8] [R 129].

In XACML (Figure 1), 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 [R 8] [R 129].

XACML is used with SAML standard, because it achieves full functionality [R 146], [R 8]. 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 [R 119] [R 129].

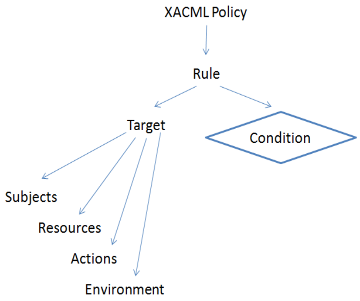


Figure 11 The content of a XACML policy [R 129]

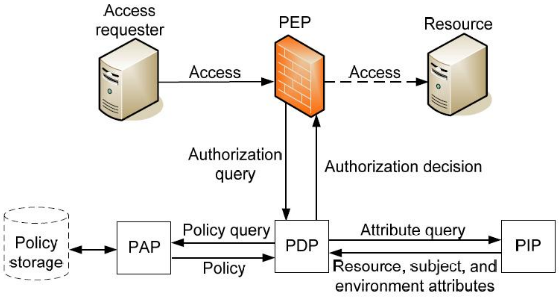


Figure 12 The architectural/usage model of XACML [R 146]

3.1.1.4 Current Cloud IAM solutions

Identity and Access Management (IAM) must address an end-to-end secure identity between the client and the cloud service [R 177]. 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 [R 79] Today there are numerous researches driven on all these methods [R 129].

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 [R 196]. Examples of IAM inside the Cloud were developed in: [R 206], [R 67], [R 68]. Even if it is an easier method, the independent stack doesn't look the appropriate approach for identification into the cloud services. This method doesn't address the integration with enterprise directory [R 196] [R 129].

The second methodology *IAM up to the Cloud* was adopted by: Juniper Networks, Inc. (2009); Goulding, Broberg and Gardiner (2010) and IBM Corporation (2010). 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 [R 79] [R 129].

The third IAM solution, *IAM down from the cloud*, seems more suitable for every size of the companies. 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 [R 79]. 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 [R 106]. However, others testing in the area weren't 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 [R 79]. 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 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 [R 148], [R 147] [R 129].

3.1.2 An Hybrid Text-Image Authentication for Cloud Services

One security solution regards increasing security at the Security Access Point level of CC and it is in fact a strong hybrid user authentication solution based on using image combined with text in order to avoid the weakness of simple user and password solution for authentication [R 164].

3.1.2.1 Related work concerning the authentication

There are three main techniques for user authentication: Knowledge based techniques, token-based techniques and techniques based on biometrics. The problem with the biometrics systems is the difficult trade-off between impostor pass rate and false alarm rate and the fact that they often require specialized devices. Recall problems are eliminated, and so are security problems concerning users writing down or choosing simple passwords. This eliminates nearly all the problems with security [R 113] [R 164].

3.1.2.2 Knowledge-based authentication techniques

Knowledge-based systems are the most frequently used for user authentication in our days. Most token-based authentication systems are also using knowledge based

authentication to prevent impersonation through theft or loss of the token. The fundamental weakness of knowledge-based authentication schemes based on recall-based authentication, is the human limitation to remember secure text passwords.
There are three types of knowledge-based authentication techniques: text-based authentication, image-base authentication and text-image based authentication [R 164].

Text-based Authentication Technique (TBA)

They need to use a user name and a password for the authentication process. But, these TBA techniques are vulnerable to more complex attacks, such as Brute force attacks and packet sniffing. Although a random, nonsensical password offers good security, the human brain finds them almost impossible to remember. The passwords have evolved from a simple dictionary or personal piece of text, to a nonsense mixture of different types of characters. This new approach of text based passwords conflicts with the human brains ability to remember strings – all studies made on human memory patterns show that the brain is more adept at remembering images.
Issues related with TBA techniques are:

- Users prefer to choose weak passwords, so most of the times, offer low security level
- The habit of of users to write down their passwords, to use the same password on different authentication systems

Therefore, security and usability requirements are the main challenge for text authentication developers [R 164].

Image-based Authentication Technique (IBA)

The recognition-based systems [R 198] are an alternative for these text-based authentication systems. IBA techniques replaces the recall-based method with the recognition-based method [R 169].
Rachna Dhamija et al, examined in 2000, the requirements of a recognition-based authentication system and they proposed the Déjà Vu solution, which authenticates a user through his ability to recognize previously seen images. This proposed authentication system is more reliable and easier if it is compared with the other one, and it has the advantage that it prevents users from choosing weak passwords and makes difficult to write down and share passwords with others [R 164].
The Déjà Vu prototype was compared with traditional password and PIN authentication. The results were successful: 90% of all participants succeeded in the authentication tests using Déjà vu, and only 70% succeeded using passwords and PINs.
Issues related with IBA techniques are the brute force attacks and the shoulder surfing
Other works related with IBA are[R 164]:

- Newman et al. (2005), in [R 144], were proposed a technique that creates passwords with images that were selected previous by users at the enrollment process.
- Confident Technologies provides image-based, multifactor authentication solutions for enterprise companies, websites, web and mobile applications, and mobile devices [R 29] (Confident Technologies, Inc., 2011). Their solution is based on encryping one-time authentication codes within an image-based challenge, being easy to use and highly secure. Users simply identify which pictures match their previously-chosen, secret categories to authenticate.

Confident technology can be used as a standalone multifactor authentication solution, or as an additional layer of authentication.
Image-based authentication solves the traditional trade-off between security and usability by providing strong authentication that is easy for people to use. As users simply tap a few pictures to authenticate, it is ideally suited for use on mobile devices.

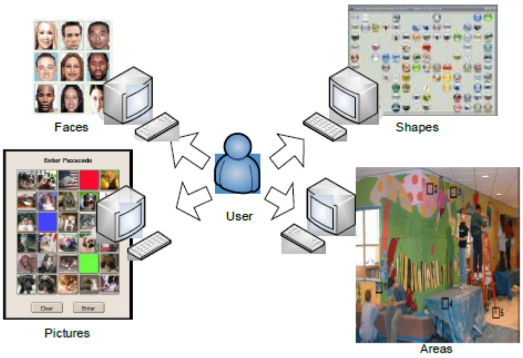


Figure 13 Different image-based interfaces on security systems [R 101]

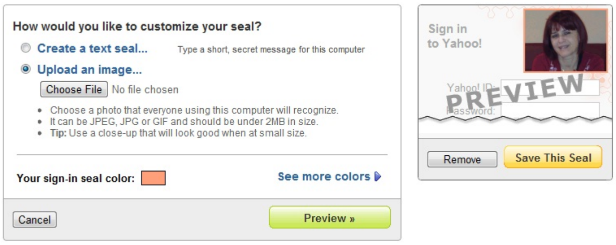
Therefore, IBA techniques are superior to text-based authentication, but there are also some noticeable drawbacks [R 164]:

- the existence of a trade-off between security and usability; if the passwords chosen by users contain more images, the security will be increased, but will also reduce the possibility of positive recall
- IBA techniques is exposed to the brute force attack, because there is the possibility that the attackers download the image set in order and to try all the combinations. In [R 101], Lee Jackson (2006**),** concluded that it is important to identify the right number of combinations available that does not compromise the system to this type of attack, and does not overload the user with images),
- the shoulder surfing - A solution is the grid based image authentication systems that randomize the position of different images each session (in situations where the intruder was not able to get a clear view of the image clicked, only an area view).

Text-Image-based authentication technique (TIBA)

TIBA technique makes more user-friendly the authentication procedure. There are several works concerning TIBA techniques All of them demonstrates their advantage
Jackson [R 101] realized a prototype that was used to evaluate the possibility of image-based authentication (IBA) method to be the main security method. He concluded that images, faces and text mixed with images seemed to offer good results concerning human memory. Five experiments were made for testing security, usability, recall, methodology undertaken and whether user could remember passwords based on multiple image-based interfaces [R 164].
The results experiments have been encouraging for IBA method; they showed that users were quite able to remember passwords contained on different image-based interfaces, and the human brain is able to hold successfully passwords on three completely different interfaces. Furthermore, they demonstrated that the method of combining text with images is the most effective – which is the basis for our approach.
Nitin et al. (2008**)**, in [R 145] described the new facility for authentication added to JUIT-IBA system which is running within the Jaypee University and Information Technology (JUIT). Being an IBA system, it is user-friendly and it uses Kerberos protocol to strengthen the security during authentication process. A new advanced security

feature was introduced to this system to make it more secure: the ***Sign in Seal***, which is a secret between the computer that is setting up and IBA. It is saved and associated with the personal computer. If multiple computers are connected to each connected computer, a single sign in must be created. The seal can be customized by creating a text seal or by uploading an image [R 164].



How would you like to customize your seal?

○ Create a text seal... Type a short, secret message for this computer

● Upload an image...

Choose File No file chosen

- Choose a photo that everyone using this computer will recognize.
- It can be JPEG, JPG or GIF and should be under 2MB in size.
- **Tip:** Use a close-up that will look good when at small size.

Your sign-in seal color: 🟧

Figure 14 Sign in seal at yahoo

From the security point of view, it is important that even if the hacker knows or guesses the ID on your personal information, he cannot use it to discover your sign in seal.
Even Yahoo has implemented the sign in seal method, with a seal that can be a text or an uploaded image (Figure 14) and it can be used in combination with our proposed method to increase the security [R 164].
In [R 173] (Renaud and Just 2010) developed a challenge protocol for replacing the textual questions associated with text that are commonly used as a backup when users forgot their “main” authentication secret.
They used a set of pictorial elements to prompt answers. The prompts solicit associative memories and serve as a stronger cue to aid the recall. All the pictures serve as an additional recall aid, which are correlated with indirect questions helping to reduce the exposure of the user to targeted observation attacks [R 108]. This proposed approach, maintains the same level of security as traditional questions as long as multiple questions are used in serial order [R 164].
Another approach for authentication uses an Authentication Avatar which represents the identity, including personality, of a fictional person that is generated almost randomly from a minimal user input [R 140].
So, an Avatar Profile (AP) contains information about the avatar, and a subset of the AP information is used by the user to respond to challenge questions regarding the avatar. The avatar information is not as easily determined by an attacker; therefore the security is improved [R 164].
The approach uses techniques to improve the memory association (such as repeated exposure to graphical imagery-related to the avatar at every login in order). Such images can be associated with the avatar itself, and with elements of the AP (a picture of the Avatar’s pet). This recovering solution resembles with the story-based interface (this one builds the story about the avatar and the story-based interface creates a story related to an individual image by drop down selection boxes), but the originality of this one is based on creating the avatar, that permits to use false information [R 164].
Therefore, this is an efficient solution that can be integrated into the global authentication process.
Our proposed authentication solution share with them the idea of combining text with images, the idea of using a randomize process in the authentication procedure, and the idea of using pictorial cues to create an additional recall aid for users [R 164].

3.1.2.3 The TIBA solution

The proposed TIBA solution was designed to increase the security at the Security Access Point (SAP) of cloud computing environment, which is built only with password-based authentication and X.509 credentials for accessing the cloud services (Figure 15). The solution takes also into account the human factor. So, the system from Figure 19 consists of an authentication service server (AS), and an authentication user agent (AUA) and it requires that the user have assigned a subset of images (as passwords) from a larger set. The set of all images used by the IBA system, named image set, contains images that are distinctive to the human eye, they are not easily describable and they differ in structure. The AS has access to the authentication database of images and associations of users with their individual image sets [R 164].

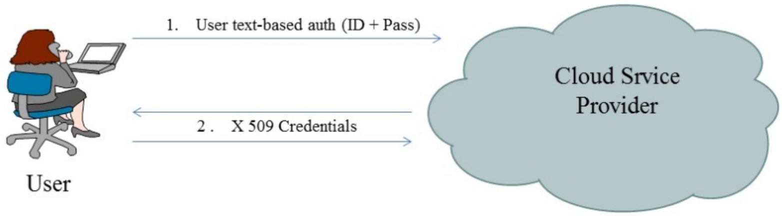


Figure 15 The current CC SAP authentification Solution [R 164].

The current solution for authenticating in CC is given in Figure 15.
To perform stronger authentication for accessing the cloud services, we propose to use an authentication scheme (Figure 16) that perform the following three steps [R 164]:

1) **Step 1** – TBA: the user ID and the text password assure access to the cloud services
2) **Step 2** – Hybrid TIBA: it uses our own proposed solution for authentication. The images are combined with text being a good solution for avoiding the brute force attacks and to ensure a strong authentication scheme
3) **Step 3** –X.509 cerificates: it uses this standard for obtaining the user credentials

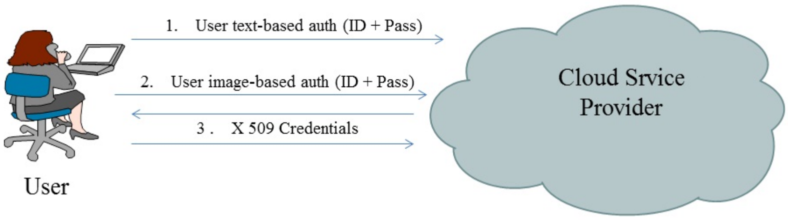

1. User text-based auth (ID + Pass)
2. User image-based auth (ID + Pass)
3 . X 509 Credentials
Cloud Srvice Provider
User

Figure 16 Our CC SAP authentification Solution [R 164].

3.1.2.4 The proposed hybrid TBA solution

To complete step 2 from the authentication scheme of Figure 16, users should first complete a registration process. It requires choosing one image from the 3 sets of grids of images and to assign passwords to all these three images. This identity information regarding the users should be stored in a database with images – available into an-image space of the front-end server of the cloud provider. Thus, step 2 of the proposed authentication solution is a hybrid TIBA in which IBA is combined with TBA [R 164].

When the user will register into the cloud service, will receive a randomly grid of images. Each grid of images will contain 3 images and each image will have a corresponding number (e.g. 1, 2, 3) (Figure 17) [R 164].

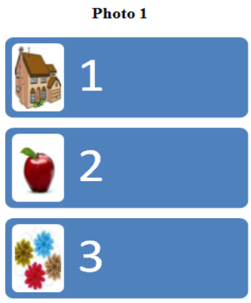
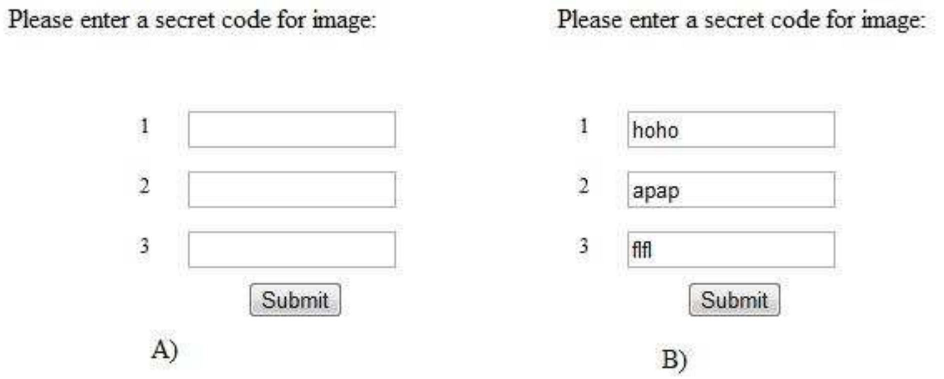


Figure 17 Grid of images

The user will have to provide a secret code for each image. In this sense, the user will receive a registration form, where it is asking to introduce secret characters for each corresponding number (Figure 18). The description of the proposed solution uses the following notations: image space, individual image set, individual password set and presentation set. Therefore, on the image space exist three image sets and each image sets contains 9 distinct images; they are distinct in structure, but they belong to a single category (animals, fruits, flowers). The security for this step will be realized by the individual image set that is combined with the corresponding individual password set. Consequently, the images must be easily to describe [R 164].

Let's suppose that there were introduced the following codes like it is emphasized in Figure 18.B.

After the user introduced their specific secret code for each corresponding image, the registration will be realized. The user should remember which code had provided for each type of image (e.g. in the above example the user choose for the house image the hoho code, for the apple image the apap code and for the flower image the flfl code), because the proposed authentication method requires entering these codes, but each time the images will be associated with different numbers (from 1 to 3), because the numbers are generated using a permutation algorithm. Therefore, for authentication procedure there will be the same images each time, but with another corresponding numbers (Figure 19) [R 164].



Please enter a secret code for image:

1
2
3
Submit

A)

Please enter a secret code for image:

1 hoho
2 apap
3 flfl
Submit

B)

Figure 18 The registration Form [R 164].

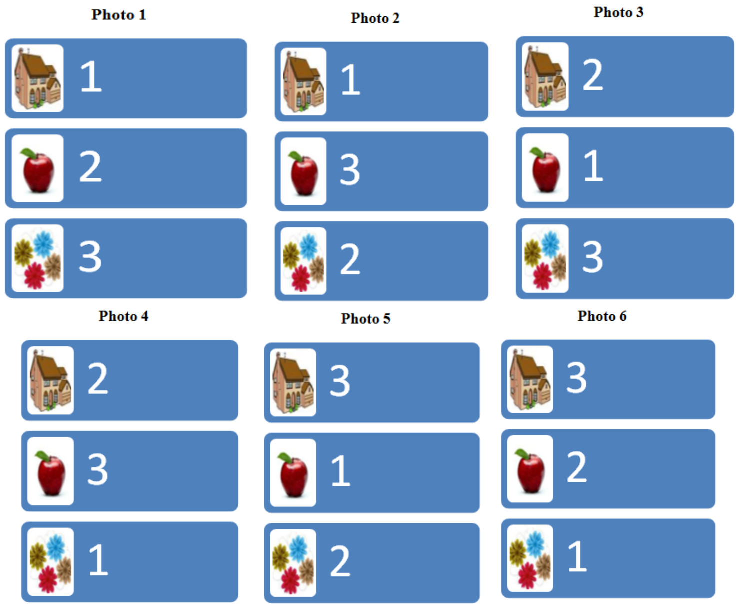


Figure 19 Relationship between the randomly grid of images and the secret code provided by user.

Our hybrid text-image solution can be applied not only for accessing the cloud, but also as a authentication method at cloud client level (especially for mobile clients) and also at the application level [R 164].
This Hybrid TIBA solution for cloud services is focused on improving the security level for the knowledge-based authentication technique, that is used in present only with text based passwords. The Hybrid TIBA solution adds a new level security approach which is based on hybrid text-image authentication (combines text with images). It realizes a user-friendly and secure authentication for cloud users. The two authentication requirements do not affect each other and eliminate trade-off between them [R 164].

3.2 Information Security Solutions

Information security in the cloud context requires protection of confidentiality and integrity for stored data, data in transmissions and data in use, as well as to preserve the data availability.
In addition, data security in the cloud environment should address the following three security risks: data location, data segregation and data disposal (which are discussed in the Section Security Risks in Cloud Computing).

Essential to be assured for information security, are the following [R 123].

- *Data Storage Security* – need to consider: Isolation of Data, Data storage zoning, Data tagging, Data retention policies, Data permanence/deletion, Data classification, Locality requirements, etc. [R 123]
- *Data Privacy Security* – need to consider: Backup, Archiving, Multi-tenancy issues (data isolation), Recovery, Privacy/privacy controls, prevention, Malicious data aggregation, Encryption (at-rest, in-transit, key management, key lifecycle management, Intrusion Management, Federal information processing standards, Digital signing / integrity, attestation, Data leak prevention etc. [R 123]

Governence is also essential for ensuring of data security. Therefor, in order to ensure information security should be considered the Audit and Legal Compliances activities, like: Fraud detection, Forensics, Auditing, SLAs, Monitoring, Accreditation, Compliance, Legal issues, Regulations, Public communication plans, Locality requirements, Discovery, Logging etc [R 123].

3.2.1 Steganography Approach to Ensure Data Storage Security in Cloud Computing

Although cloud computing is very useful in today's life, the general consciousness is that data is not secure. People do not trust that service providers do not take advantage of client data that is stored on an unknown server. Another problem concerns data exposure when loaded on the server. Now days, tools and video resources are available that can teach how to hack data packets, etc.
Therefore, it is a crucial job to manage data-at-rest in cloud computing. The main problem with data-at-rest in cloud is the loss of control; an unauthorized user can access data when data is stored in a shared environment. Although today storage devices use encryption techniques that restrict unauthorized access to data, encryption methods fail to provide authorized access if encryption and decryption keys are available to malicious users.
In [R 5] [R 182] [R 112] are proposed stenographic approaches that hide data in images. The architecture solution for such an approach, together with the security unit

to respond to these concerns and the security analysis for the proposed solution is given in [R 112].

Steganography is the technique that provides forward and backward compatibility for hiding the information in cover images performing the hiding operation in the spatial domain and frequency domain. It protects the secret message from an un-authorized person.

In fact, steganography is cryptography, and it is encryption. It turns a plaintext into a ciphertext, with the additional requirement that the ciphertext be indistinguishable from the plaintext – information is hidden being kept confidential (if the hiding is successful). But, if the adversary can break the system and get the contents, then he will see the content and thus the system is broken.

In Table 7 is given a brief comparison between Steganography and Cryptography.

Steganography	Cryptography
Hide the message	Try to hide the meaning of message (by transforming the message)
The practice of concealing a file, message, image or video within another file, message, image or video	Keyed transforming of a file, message, image or video (to hide information)
Requires a carrier. Therefore, the steganography payload size is much higher than the Obfuscated information	Sizes are same for Encrypted Data (payload) and Data that has been encrypted.
In steganography, no other the sender and receiver know the secret message	Cryptographc algorithm is recommended when there is no problem to know that there is a secret message
Data security depends on the hiding technique	Data security depends on selection of the keys
Useful for data hiding	Cryptography has further applications than securing data – for digital signature, authentication, etc

Table 7 comparison between Steganography and Cryptography

Anybody who suspects usage of steganography, from the network behavior, can develop and apply staganalytical techniques to extract the data. Should be combined with cryptographic techniques to prevent the retrieving of original data if the cover file is suspected to include hidden data – realizes two line of defense and a stronger privacy
Needs carrier of size at least ten times that of the size of text – it reduces the channel efficiency

3.2.2 Confident System Architecture

Chatterjee et al. (2015) identified different network entities for their proposed confident architecture [R 17], which is given in Figure 20.

These entities are:

- **The User:** Customers who want to use cloud infrastructure.
- **Cloud Service Provider-1 (CSP-1):** Cloud Infrastructure where the data will be stored in the form images.
- **Cloud Service Provider-2 (CSP-2):** For storing the encryption and decryption techniques - mechanism for hiding data into images and retrieving data from images.
- **Cloud Service Provider 3 (CSP-3):** Interact with CSP-1 and CSP-2 - all calculations for the user are done here

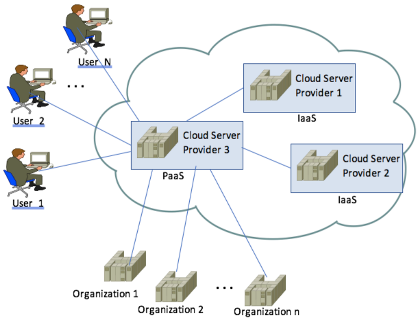


Figure 20 The architecture of our proposed model [R 17]

3.2.2.1 Security Model

Instead of storing data into a file, the data are hidden and stored into images. This is done by a steganography process [R 183]. This is the new paradigm of security through obscurity.

Therefore, steganography is the new paradigm of security through Obscurity. As example, in [R 17], an entire file is divided into multiple parts, and each part is stored into a corresponding image. The number of divisions in which the file is divided depends on file size and image size.

The proposed security model for storing data is in Figure 21 and the proposed model for retrieving data is given in Figure 22. In CSP-3 are done the computations for users.

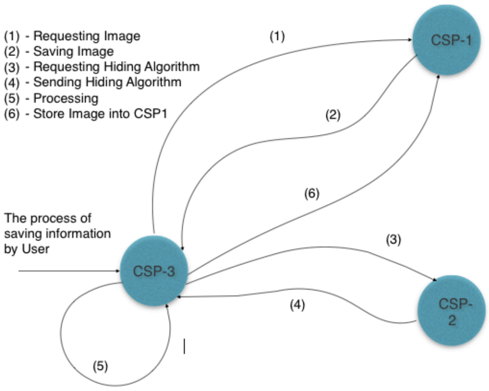

(1) - Requesting Image
(2) - Saving Image
(3) - Requesting Hiding Algorithm
(4) - Sending Hiding Algorithm
(5) - Processing
(6) - Store Image into CSP1
The process of saving information by User
CSP-1
CSP-3
CSP-2
(1)
(2)
(3)
(4)
(5)
(6)

Figure 21 Computational model for storing data [R 17]

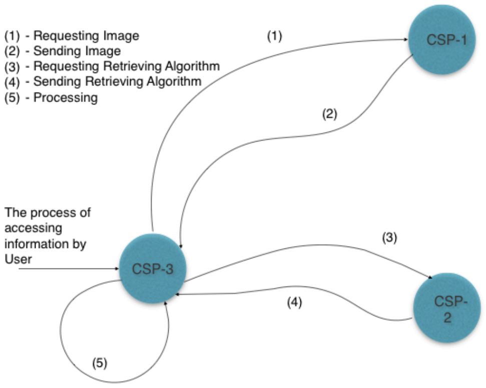

(1) - Requesting Image
(2) - Sending Image
(3) - Requesting Retrieving Algorithm
(4) - Sending Retrieving Algorithm
(5) - Processing
The process of accessing information by User
CSP-1
CSP-3
CSP-2
(1)
(2)
(3)
(4)
(5)

Figure 22 Computational model for Retrieving Data [R 17]

All temporary file must be deleted when the user log out from the system. The processes of storing data and retrieving data are dealing with:

- The Image Database - contains a set of images of different sizes stored in CSP-1. A set of images will be sent to CSP-3 when a user wants to store data into cloud.
- The File Database - is a file and this file holds the address of images where we will store our data; does not contain the actual information
- Embedding Data into Images process– this process generates files which are to be stored in cloud data storage. It counts the total no of character presented in the file and find the frequency of the occurrences of each character and codifies the original characters by Huffman codes. After that steganography is applied to both frequency of characters and the codified data.

3.2.2.2 Analysis of Wavelet, Ridgelet, Curvelet and Bandelet transforms for QR code based Image Steganography

In [R 87] we propose a data hiding based image steganography method that uses to perform image steganography four transforms from frequency domain. The experimental results demonstrate that the proposed method provides better stego-image quality and increases the embedding capacity. It maintains for the stego-image quality the PSNR value of above 47 dB without affecting the retrieved secret message. In the spatial domain, the information is hidden directly into the least significant bit (LSB) of the cover image without any modification. In [R 41] [R 11] [R 215] are presented methods and security problems related with the hiding operation in the spatial domain and in [R 133] is proposed an iterative method of palette based image steganography using spatial domain. For increasing security which is the major issue in the spatial domain, some channel selection criterion has been proposed [R 215]. In the frequency domain, the information is hidden in the transform coefficients. It transforms the spatial domain cover images into frequency domain cover images using Discrete fourier transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), ridgelet, curvelet and bandelet transform [R 87].

Reversible data hiding is also a research area for sensitive applications like medical, military and wireless; it retrieves the secret message and original cover image from the stego image with the same secret key on both the transmitter and receiver side. In the spatial domain, in [R 11] is proposed a reversible data hiding in the digital content using difference expansion and in [R 214] is proposed a high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding strategy. In the frequency domain, a lossless and reversible data hiding scheme in DCT-based compressed images have been proposed. The information is embedded in DCT coefficients of JPEG images [R 14] [R 87].

To achieve the high embedding capacity and good quality of stego image in [R 15] is proposed to use Haar DWT based on reversible data hiding. [R 120] propose the use of the curvelet transform for data hiding based on amplitude. The bandelet transform for data hiding have been proposed in [R 188]. The data hiding process changes the statistical properties of the image, which leads to steganalyst attempts to detect the statistical traces called statistical steganalysis. To resist the statistical steganalysis, reversible histogram transformation function based on LSB steganography technique has been proposed in [R 131] [R 87].

Image steganography using frequency domain method is found to be more efficient than the spatial method due to its high data security [R 87].

So, in [R 87] we briefly presented the five frequency domain techniques: (1) QR code (2) Integer discrete wavelet transformation (3) Ridgelet transformation (4) Curvelet transformation (5) Bandelet transformation, which are used for our study.

The QR code is used by our proposed method as a secret message to increase the security and embedding capacity of the steganography [R 87].

Integer Discrete Wavelet Transform (IDWT) is an important technique for transforming a cover image from spatial domain into frequency domain. The operation is performed through cohen-daubechies-feauveau wavelets in the three lifting steps for forward transform (splitting, prediction, update, and three lifting steps for inverse transform (inverse update, inverse prediction and merging). IDWT decomposes the cover image into approximation co-efficient (LL) which is low frequency band and detail co-efficient (LH, HL, HH) which is high frequency band. The high frequency band (LH, HL, HH) of IDWT hides the QR coded secret message [R 87].

The Finite Ridgelet Transform (FRIT) was proposed based on the Finite Radon Transform (FRAT) [R 87].

The curvelet transform was proposed by Candes and Donoho, to overcome the shortcomings of wavelet transform. It is a multiscale directional transform that represents the object with edges and it requires only fewer amounts of coefficients to represent the edges. There are two transformations related to the Fast Discrete Curvelet Transform (FDCTs) [R 87]:

1. Using Unequally-Spaced Fast Fourier Transform (USFFT)

2. The wrapping of specially selected fourier samples is the basis for the second one.

Our proposed method uses the FDCTs via USFFT [R 87].

Bandelet transform is mainly used to represent efficiently the edges and texture of the image. It takes the sharp transitions in the image as an advantage. The bandelet transform overcomes the wavelets' high dimension problem[R 87].

Proposed Methodology

To perform image steganography using frequency domain, we have selected: Integer Discrete Wavelet Transform (IDWT), Finite Ridgelet Transform (FRIT), curvelet transform and Bandelet transform.

Our embedding technique is based on the bit-plane compression method. adaptive histogram modification is carried out as a pre-processing of images in order to prevent overruns occur during the embedded process. The changes in the selected bit-plane of high frequency band are indicated by the overflow that happens when the grayscale value of the QR pixel code exceeds one of the two boundaries: the lower bound (0) or the upper bound (255). The QR coded secret message is embedded into the cover image by the embedding phase. The embedding algorithm is common for all the four transforms [R 87].

The concept of the proposed method is that, QR code can be embedded in the one or more bit-planes of transform's high frequency sub-bands. The space to hide the QR code is generated by compressing the bits in a bit-plane [R 87].

For instance, let us see the eight-bit binary data 01101101, from the left, the bit binary data 1 represents LSB and the binary data 0 at the eighth bit plane represents MSB. Let the bit-plane be represented by the notation k. QR code can be embedded in any of the selected bits-plane going from first bit-plane to the eighth bit-plane [R 87]:

In the frequency domain, the transform (IDWT, FRIT, FDCT via USFFT and bandelet transform) decomposes the cover image into low and high frequency sub-bands and the QR code can then be embedded in the transform's high frequency sub-bands. QR code can be embedded in any of the selected bit-plane with the secret key. The secret key is used to enhance the information security. The secret key is x-or-ed with the QR code. The bits in the selected bit-plane can be compressed using arithmetic coding to leave a space to hide the QR code. The extraction phase is an inverse process of the embedding phase. The extraction phase extracts the cover image and the QR code with the same secret key. The image quality varies depending on the nature of the transform [R 87].

The algorithm for the embedding phase is given below [R 87]:

1. Step 1: Adaptive histogram modification is used as a preprocessing.
2. Step 2: Decompose the cover image by IDWT, FRIT, FDCT via USFFT and Bandelet transform separately.
3. Step 3: Select the bit-plane (k =1, 2, 3, 4, 5, 6 and 7) of transform's high frequency sub-bands.

4. Step 4: Compress the data in selected k using arithmetic encoding to leave a space to hide QR code.
5. Step 6: Convert the secret data into a QR code and the secret key is embedded into a QR code for information security.
6. Step 7: Embed the QR code in the space left.
7. Step 8: Compute Inverse wavelet, ridgelet, curvelet and bandelet to get the stego image.

In our work, the five pre-processed cover images are tested for k =1, 2, 3, 4, 5, 6 & 7 to find the k value which has the best stego image quality. Arithmetic coding is used to compress the bit-plane to leave a space for hiding the QR code. It replaces an input symbol with some specific code [R 87].

Experimental Results and Discussions

The evaluating the performance of the proposed method many simulations experiments were done. Three commonly used gray-level images: “Baboon”, “Barbara”, “Lena” and two medical gray-level images: “Eye”, “Skull” (totally five gray level images) were used. For better result, the cover image was pre-processed by adaptive histogram equalization. The pixels of each pre-processed gray-level images are 512*512 which is used as a cover images are shown in Figure 23.
MATLAB R.2010 software was used.
Peak Signal-to-Noise Ratio (PSNR) and embedding capacity were the performance measures before an extraction, and after extraction, the performance measures used were: Tamper Assessment Factor (TAF) and Normalized Absolute Error (NAE). TAF is used to determine the credibility of image authentication, which is measured between the QR code and retrieved QR code. NAE is measured between the cover image and the restored cover image [R 87].
The relations for these performance measures are using the following notations: C(i,j) is the cover image, S(i,j) is the stego image, Q(i,j) is the QR coded secret message, Q’(i,j) is the retrieved QR coded secret message and C’(i,j) is the restored cover image, then:

$$MSE = \frac{1}{m \cdot n} \sum_{i=1}^{m} \sum_{j=1}^{n} [C(i,j) - S(i,j)]^2 \qquad (3.1)$$

$$PSNR = 10 log_{10} \left(\frac{255^2}{MSE} \right) \qquad (3.2)$$

$$TAF = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [Q(i,j) \oplus Q'(i,j)] \qquad (3.3)$$

$$NAE = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} |C(i,j) - C'(i,j)|}{\sum_{i=1}^{m} \sum_{j=1}^{n} |C(i,j)|} \qquad (3.4)$$

For all our experiments The QR code is hidden in the third, fourth, fifth, sixth and seventh bit-plane (k = 3, 4, 5, 6 and 7) of the high frequency sub-bands coefficients of IDWT (LH, HL and HH) of “Lena” image. By testing the “Lena” image for all the k values, the best stego-image quality is obtained for k =7. Hence, for all experiments, the selected bit-plane taken is for k =7 and applied to all the pre-processed cover images [R 87].

Results of IDWT

The proposed algorithm is applied to the IDWT based steganography. The resultant stego-images corresponding to the cover images are shown in Figure 23. Table 8, lists the PSNRs and the embedding capacity of the stego-images for all the k values [R 87].

From Table 8, it is evident that, in the commonly used images, the PSNR value is high for “Barbara” stego-image, but the embedding capacity is high for “Baboon” stego-image. In the medical images both PSNR value and embedding capacity is high for “Skull” stego-image when k= 7. Hence, the result varies according to the nature of the images, when performed in IDWT [R 87].

Results Of FRIT

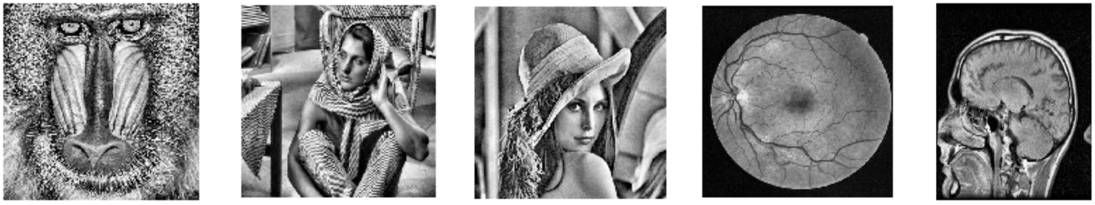
The proposed algorithm is applied to the FRIT based steganography. The resultant stego-images corresponding to the cover images are shown in Figure 24   Table 9, lists the PSNRs and embedding capacity of five stego images when k =1, 2, 3,4, 5, 6 and 7 [R 87].

From Table 9, it is evident that, in the commonly used images, the PSNR value is high for “Lena” stego-image, but the embedding capacity is high for “Baboon” stego-image. In medical images, the PSNR value is high for “Skull” stego-image. Hence, the result also varies according to the nature of the images, when performed in FRIT [R 87].

Results Of FDCT Via USFFT

In the third experiment, the proposed algorithm is applied to the FDCT via USFFT based steganography image. The resultant stego-images corresponding to the cover images are shown in Figure 25. Table 10, lists the PSNRs and embedding capacity of stego images for all the k values. FDCT provides a better result compared to the other transforms [R 87].

From Table 10, it is found that, in the commonly used images, the PSNR value is high for “Barbara” stego-image, but the embedding capacity is high for “Baboon” stego-image. In medical images, the PSNR value is high for “Eye” stego-image. Hence, a result also varies according to the nature of images, when performed in FDCT [R 87].

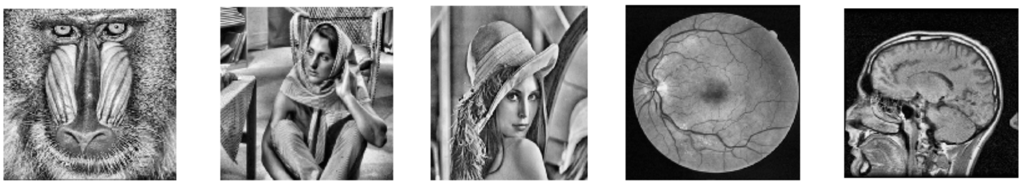


(a) k =7, 50.02 dB (b) k =7, 50.5 dB (c) k =7, 50.3 dB (d) k =7, 49.1 dB (e) k =7, 50.7 dB

Figure 23 Stego image using IDWT (a) Baboon, (b) Barbara, (c) Lena, (d) Eye and (e) Skull [R 87]

k	3 (PSNR & EC)		4 (PSNR & EC)		5 (PSNR & EC)		6 (PSNR & EC)		7 (PSNR & EC)	
Baboon	24.6	220839	29.7	260523	35.3	277980	40.9	284616	46.0	286613
Barbara	24.7	164844	29.5	202127	35.3	234438	40.8	260242	46.1	282077
Lena	24.9	138000	29.6	187032	35.2	257531	40.9	281449	46.1	286276
Eye	22.8	159067	27.6	169092	33.4	164131	39.3	245276	44.6	282148
Skull	24.8	149067	30.9	149048	35.1	142012	40.7	220305	46.2	279085

Table 8 PSNR value (dB) & embedding capacity for stego image of IDWT when k =3, 4, 5, 6, 7 [R 87]

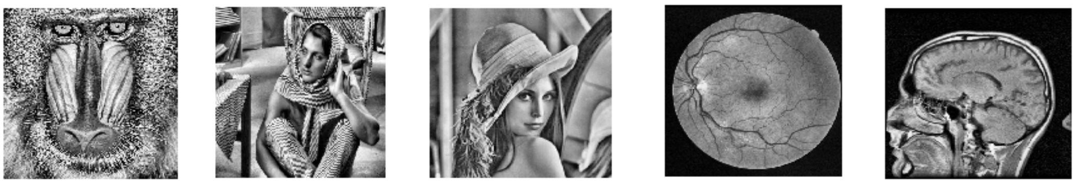


(a) k =7, 50.4 dB (b) k =7, 50.4 dB (c) k =7, 50.6 dB (d) k =7, 48.7 dB (e) k =7, 50.4 dB

Figure 24 Stego image using FRIT of (a) Baboon, (b) Barbara, (c) Lena, (d) Eye and (e) Skull [R 87]

k	3		4		5		6		7	
	(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)	
Baboon	24.3	149220	29.5	155985	34.9	157439	40.6	157690	45.8	157752
Barbara	24.2	138012	29.3	153533	34.8	156801	40.5	157527	45.9	157728
Lena	24.1	135682	29.1	151383	34.9	156421	40.9	157456	46.1	157697
Eye	22.6	105691	26.8	133529	33.2	151229	39.1	156448	44.4	157453
Skull	24.1	133919	29.2	149830	34.7	156071	40.6	157410	45.9	157683

Table 9 PSNR value (dB) & embedding capacity (bits) for stego image of FRIT when k =3, 4, 5, 6, 7 [R 87]

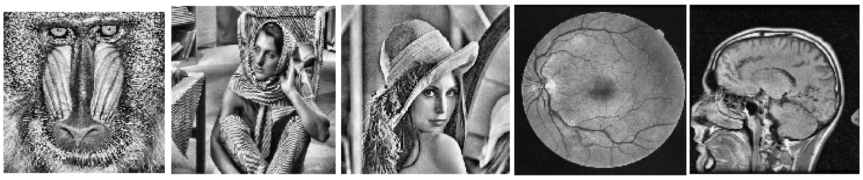


(a) k =7, 82.8 dB (b) k =7, 86.7 dB (c) k =7, 85.4 dB (d) k =7, 93.7 dB (e) k =7, 90.6 dB

Figure 25 Stego image using FDCT of (a) Baboon, (b) Barbara, (c) Lena, (d) Eye and (e) Skull [R 87]

k	3		4		5		6		7		
	(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		
Baboon	82.8	82.8	91203	82.8	91209	82.8	91208	82.8	91209	82.8	91209
Barbara	86.7	86.7	91208	86.7	91206	86.7	91207	86.7	91206	86.7	91208
Lena	85.4	85.4	91204	85.4	91206	85.4	91206	85.4	91209	85.4	91209
Eye	93.7	93.7	91208	93.7	91203	93.7	91207	93.7	91207	93.7	91209
Skull	90.6	90.6	91192	90.6	91205	90.6	91209	90.6	91208	90.6	91207

Table 10 PSNR value (dB) & embedding capacity (bits) for stego image of FDCT when k=3, 4, 5, 6 & 7 [R 87]



(a) k =7, 47.8 dB (b) k =7, 48.1 dB (c) k =7, 47.9 dB (d) k =7, 47.4 dB (e) k =7, 48.8 dB

Figure 26 Stego image using bandelet transform of (a) Baboon, (b) Barbara, (c) Lena, (d) Eye and (e) Skull [R 87]

k	3		4		5		6		7	
	(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)		(PSNR & EC)	
Baboon	21.8	310082	26.5	339076	31.9	347613	37.4	350860	42.9	351102
Barbara	21.8	255146	26.6	291495	31.9	318083	37.5	337516	43.0	346424
Lena	21.8	214182	26.4	271040	31.8	321103	37.4	344101	42.9	348321
Eye	22.2	198313	26.5	211691	31.1	270798	36.6	316730	42.6	338329
Skull	22.8	204271	27.6	241055	32.7	294760	38.4	328546	43.9	343150

Table 11 PSNR value (dB) & embedding capacity (bits) for stego image of bendlet when k=3, 4, 5, 6 & 7 [R 87]

Results Of Bandelet Transform

In the fourth experiment, the proposed algorithm is applied to the bandelet transform based steganography. The resultant stego-images corresponding to the cover images are shown in Figure 26 Table 3, list the PSNRs and embedding capacity of the stego-images for all the k values.

From Table 3, it is found that, PSNR value is high for “Barbara” stego-image, but the embedding capacity is high for “Baboon” stego-image. Hence, the result also varies according to the nature of images, when performed in bandelet transform [R 87].

Comparative Analysis For The Proposed Approaches

In Figure 27 and Figure 28 is given the comparative analysis performed for the proposed method are given.The PSNR value is high for FDCT, low for bandelet transform (Figure 27) and embedding capacity is high for bandelet transform and low for FDCT (Figure 28.). For medical applications, the steganography is used to hide the patient medical report with his/her scanned image and can be send to clinicians residing in any corner of the globe for diagnosis.

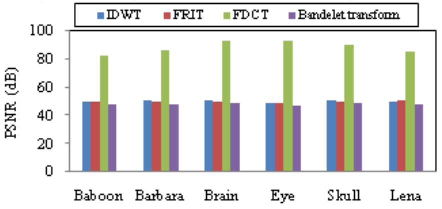


Figure 27 Comparison of PSNR value of the four transforms [R 87]

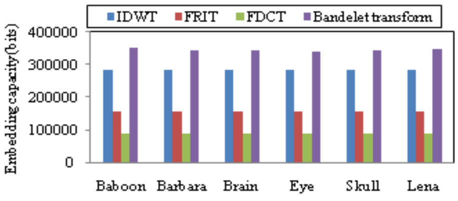


Figure 28 Comparison of embedding capacity of the four transforms [R 87]

When the patient medical report capacity is low, FRIT based steganography is preferable as it gives better quality of stego image when the embedding capacity is low. For secured communication applications like military domain, FDCT based steganography is preferable because it gives good quality of stego image. For academic applications like transforming more data within the local network or within the campus, bandelet transform based steganography is preferable as the time consumption is low and acceptable PSNRs value is provided. To embed the high amount of information and to attain quality of stego image IDWT based steganography is preferable, it also provides better results and is less time consuming to embed the information [R 87].

The comparison of the proposed technique with other works shows that the stego-image quality of the proposed method is significantly higher than those of the other works mentioned in literature survey. The embedding capacity is also increased in our proposed method compared with the other work [R 87].

3.2.2.3 Application of Genetic Algorithm and Particle Swarm Optimization techniques for Improved image steganography systems

Though the frequency domain techniques are preferred for image steganography applications, there still are significant drawbacks associated with these techniques. Thus, in transform based approaches, the transform coefficients that embed in random manner the secret data may not be optimal in terms of the stego image quality and embedding capacity.

So, in [R 89] is explored, in the context of determining the optimal coefficients in these transforms, the application of Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). The proposed methodology increases the fidelity of the stego image and embedding capacity and also provides more security, by combining frequency domain transforms such as Bandelet Transform (BT) and Finite Ridgelet Transform (FRIT) combination with GA and PSO. BT and FRIT were chosen to yield the high embedding capacity and GA and PSO were used to find the most significant coefficients for better information hiding. It is a novel attempt to enhance the efficiency of the steganography system.

The experimental results of the proposed approaches has been compared with recent works [R 89].

Particle Swarm Optimization(PSO)

Particle Swarm Optimization (PSO) is a population based optimization techniques, which has been developed by Kennedy and Eberhats in 1995. The potential solution is represented by each individual. Each particle's position is altered according to its neighbors and with its own practical experience. In each iteration, the predetermined particles correspondingly produce fitness value from the fitness function and also have velocity to direct the movement of the particle. Each particle in a population keeps track of its best solution (fitness) in the search space which has achieved so far by that particle. This fitness value is called pbest (personal best). PSO keep track of another best solution that is obtained so far by any particle in the neighbor- hood of that particle. This is known as gbest (global best) [R 89].
A detailed algorithm is given in [R 4].

The Proposed Methodology

The proposed methodology is based on two phases: the embedding phase and the extraction phase. In Figure 29 is depicted by the block diagram of embedding phase [R 89].

Embedding Phase

The first step of embedding phase is to read the cover image $A(x, y)$. The cover image is decomposed using specific transforms (BT & FRIT). Then, the most significant coefficients are selected using GA and PSO. Embedding the secret data in the most significant coefficients, that will increase the fidelity for the stego image.
Next step is to read the secret data B'(x,y). The secret data B'(x,y) is hidden in the most significant coefficients [R 89].

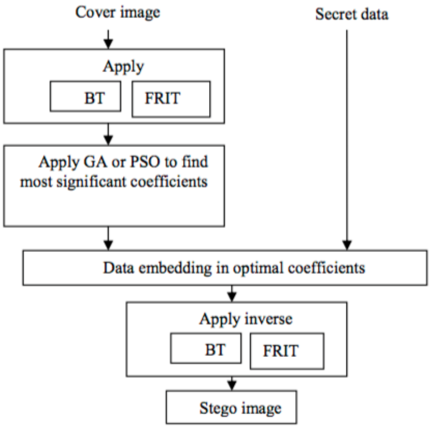

Cover image
Secret data
Apply
BT
FRIT
Apply GA or PSO to find most significant coefficients
Data embedding in optimal coefficients
Apply inverse
BT
FRIT
Stego image

Figure 29 Block diagram of Data embedding [R 89]

Extraction Phase

The extraction phase extracts the embedded secret data and cover image separately. Decompose the stego image using specific transform (BT and FRIT). Then use the positions of most significant coefficients to determine the extraction key. The extraction key posses the position of most significant coefficients [R 89].

GA base data embedding

The procedure of GA for finding the most significant coefficients in BT and FRIT is given below [R 89].
Step 1. Parameter Representation; these are given in [R 89].

Step2. Fitness Function
To enhance the quality of stego image, Peak Signal-to-Noise ratio (PSNR) equation is taken as a fitness function. GA and PSO search for the chromosomes with highest fitness value from the fitness function. PSNR is measured between cover image and stego image. If PSNR value is high, the fidelity of stego image is also high [R 89].

$$\mathrm{MSE} = \frac{1}{\mathrm{m \cdot n}} \sum_{\mathrm{i=1}}^{\mathrm{m}} \sum_{\mathrm{j=1}}^{\mathrm{n}} [\mathrm{A(x, y)} - \mathrm{Stego(x, y)}]^2 \qquad (3.5)$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \quad (3.6)$$

Step3. Selection Process:
According to the rank selection method, the 1st rank will be allotted to the highest fitness value and 2nd rank will be allotted to the next highest fitness value. The procedure is adopted for all 1024 chromosomes for each individual. The 15 individuals are reordered according to the rank allotted. The first top two fitness individuals (P_{good}) undergo crossover and mutation. The last two weak fitness individuals (P_{bad}) are discarded and leave a space for 2 new offspring for the next iteration [R 89].
Step 4. Reproduction operators: Crossover and mutation are the two reproduction operators.
Two individuals are chosen from (P_{good}) to produce new offspring. Two-point crossover is used for generating new chromosomes. The mutation process is also used for offspring formation. In this method, bits are swapped to form the new chromosomes. After crossover and mutation, the discarded offsprings are replaced with new offsprings [R 89].
Step5. Test for convergence:
Repeat the above-mentioned procedure for specific number of iteration. The resulting most significant coefficients selected by GA are considered as the optimal solution which will give a better stego image quality [R 89].

PSO based data embedding

PSO is used to give the most significant coefficients in BT and FRIT to embed the secret data. The most significant coefficients are obtained by following steps [R 89] [R 75].

Step 1. Parameter Representation is given in [R 89].

Step 2. Fitness function: The fitness function for PSO is same as used in GA.

Step 3. Initialization: In the 1st iteration, PSO randomly select the position and velocity. Then, for each particle the fitness value is calculated from the fitness function which is measured between cover and stego image.

Step 4. Calculate pbest and gbest: After the fitness function evaluation, estimate pbest as gbest. Considering the maximization problem, the global best position is calculated as,

$$\mathrm{gbest} = \begin{cases} \mathrm{P_x(t+1)} & \text{if } (\mathrm{P_x(t+1)} \geq \mathrm{P(pbest)}) \\ \mathrm{pbest} & \text{if } (\mathrm{P_x(t+1)} < \mathrm{P(pbest)}) \end{cases} \quad (3.7)$$

where, P is the fitness function which measures the closest optimum solution

Step5. Update particle position and velocity: Let Px(t) be the current position of particle x in the search space at time t . The current position (Px(t)) is updated to new position (Px(t+1)) according to the velocity V_x(t+1) is given by,

$$\mathrm{P_x(t+1) = P_x(t) + V_x(t+1)} \quad (3.8)$$

In every iteration, each particle is updated according to the pbest and gbest value. The velocity of particle x is updated:

$$\mathrm{V_x(t+1) = w \cdot V_x(t) + c_1 r_1(t)[pbest - P_x(t)] + c_2 r_2(t)[gbest - P_x(t)]} \quad (3.9)$$

where, $V_x(t)$ is the current velocity of particle x at time t, w is the inertia weight factor, $P_x(t)$ is the current position of particle x at time t, c1 & c2 are cognitive and social acceleration constants, r1(t) & r2(t) are the random values in the range between [0,1].

Step6. Test Convergence: Repeat the above procedure till there is no change in particle positions.
The resulting best coefficients selected by PSO are considered as the optimal solution (give a better stego image quality). The best positions selected by PSO in the data embedding are taken as key and will be later used in the data extraction for the extraction of secret data.

Experimental Results and Discussions

The software used for implementation is MATLAB. Four gray-level images such as “Sailboat”, “Barbara” “Girl” and “Tiffany” are used in this work. The cover gray-level images are shown in Figure 30 [R 89].
he performance measures used in this paper are Peak signal-to-noise ratio (PSNR) and embedding capacity (bits). The PSNR performance measure is used to measure the quality of stego image. The PSNR is defined through the mean square error (MSE). Embedding capacity (bits) gives the amount of data that can be hidden in the cover image. A high embedding capacity is always required for all steganography system. Tamper Assessment Factor (TAF) measures the quality of retrieved secret data. The value of TAF should be between 0-1. The Normalized absolute error (NAE) measures the quality of reconstructed cover image.

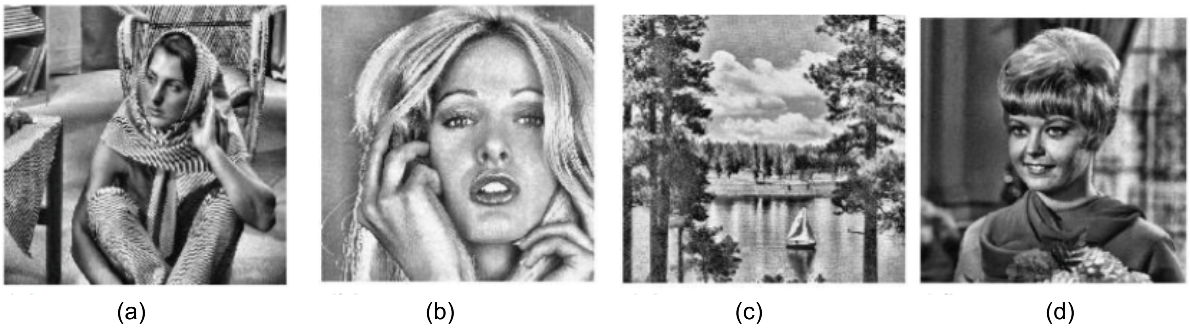


Figure 30 Sample cover images: (a) Babara, (b) Tiffany (c) Sail boat, (d) Girl. [R 89].

The Normalized absolute error (NAE) measures the quality of reconstructed cover image. Let $A(x,y)$ be the cover image, $B(x,y)$ be the secret message, $B'(x,y)$ be the retrieved secret image and $C'(x,y)$ be the restored cover image, x and y denote the row and column. TAF and NAE are defined as [R 89]:

$$\mathrm{TAF} = \frac{1}{m\cdot n}\sum_{i=1}^{m}\sum_{j=1}^{n}[B(x,y)\oplus B'(x,y)] \qquad (3.10)$$

$$\mathrm{NAE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}|A(x,y)-A'(x,y)|}{\sum_{i=1}^{m}\sum_{j=1}^{n}|A(x,y)|} \qquad (3.11)$$

4.5 Comparative analysis

The comparative analysis of the proposed methodologies is shown in Table 12 [R 89].

Images	PSNR(dB)			
	BT	FRIT	BT	FRIT
	GA	GA	PSO	PSO
Barbara	37.36	40.45	43.89	25.87
Tiffany	37.50	40.81	43.83	46.28

Sail Boat	38.23	40.61	43.83	45.95
Girl	37.56	40.63	43.55	45.06
Average	37.36	40.45	43.89	45.87

Table 12 Comparison of optimization techniques based Bandelet transform and FRIT- PSNR values [R 89]

The obtained results prove that PSO gives better result than GA for both BT and FRIT, because GA is random in nature. An approximate of 3–6 dB is received with FRIT based optimization techniques over the BT based optimization techniques [R 89].

Images	PSNR(dB)			
	BT	FRIT	BT	FRIT
	GA	GA	PSO	PSO
Barbara	350860	157527	350191	157728
Tiffany	337516	157421	341297	157707
Sail Boat	321304	157172	341297	157641
Girl	339662	157418	345744	157700
Average	350860	157527	350191	157728

Table 13 Comparison of optimization techniques based Bandelet transform and FRIT- Embedding capacity (bits) [R 89]

From Table 13, also results that PSNR values and embedding capacity are higher for PSO based techniques than those for GA based techniques [R 89].

On the other hand, the average embedding capacity of 902136 bits is obtained with FRIT with GA and PSO. Thus, the optimization techniques have significantly increased the efficiency of the steganography system [R 89].

In conclusion, GA and PSO are used to give the most significant coefficients to embed more amounts of secret data. The proposed methodology maintains the fidelity of stego image with an average PSNR value of 37.56 dB for BT combined with GA, average value of 43.55 dB for BT combined with PSO, average value of 40.63 dB for FRIT combined with GA and average of 46.06 dB FRT combined with PSO. The proposed method performance has been also compared with the other related works [R 89]; it permits to obtain better fidelity of stego image and high embedding capacity. The proposed algorithm can be used for secure communication, respectively for hiding digital information.

3.3 Infrastructure Security Solution

Information security in cloud also involves securing physical and virtual infrastructure. Infrastructure can be defined as services that make clouds and cloud services availability to customers as well as the different transport mechanisms from customer to cloud, and between the various components within the cloud.

	Infrastructure Security	Security means
1.	Network security control	- firewalls and Intrusion Detection and Prevention Systems; useful for for protecting against DoS and DDoS attacks [R 35]
2.	Security control of Physical Infrastructure	- host-based firewalls; - Host Intrusion Detection/ Prevention Systems (HIDS) / (HIPS); - Integrity and file/log management; - Encryption [R 35]
3.	Virtualization security control	- Virtual Local Area Network (VLAN) (implemented private for each cloud customer) - isolate the virtual machines which reside on the same physical device. - Access Control Lists (ACL) - separate the organizational domains for each enterprise (must be used for each private LAN) - ACL - implemented in the public cloud deployment model. - Virtual Demilitarized Zone (DMZ) - for each customer environment

		- private cloud costumer, dedicated for sensitive data that must be protected [R 23]
4.	Environmental Security Control	- Maintains physical infrastructure in proper conditions (power, temperature and humidity controls, space smoke detectors) [R 38]

Table 14 Infrastructure Security [R 89]

Regardless of the delivery model, the cloud provider delivers physical infrastructure security, environmental security control, network security control, and virtualization to control physical infrastructure security, environmental security control, network security control, and virtualization [R 123].

Infrastructure security will be given by the following elements: Physical Security, Network Infrastructure Security, Firewalls, Access Control Lists (ACLs), Availability (Performance and anti-DoS), Security Policies (Including facilities/services available to customers), Remote access, Mobile access and platforms, Virtualization issues, Environmental controls, Disaster recovery, Identity / authentication / federation, Staffing / employee background etc [R 123].

In (Table 14) are detailed the means for infrastructure security control.

These kinds of controls can be written into the service level agreement (SLA).

In [R 123] is given a comparison of six cloud service providing companies regarding the infrastructure. security.

3.4 Cloud Security Architectures

The General Cloud Computing Architecture is composed by a massive network of “cloud servers” [R 139] that uses virtualization to maximize the utilization of the computing power available/per server (Figure 31). Clouds users’ interfaces with the cloud by the Cloud Portal, which allows the user to select a service from a service catalogue and system management will find the correct resources that will be allocated in the cloud by the provisioning service. The optional Monitoring and metering tracks the usage of the cloud, so the resources used can be attributed to a certain user.

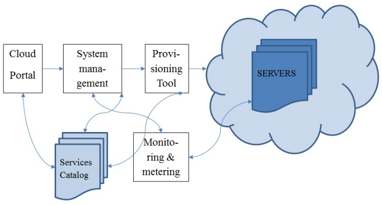


Figure 31 Cloud Computing Architecture

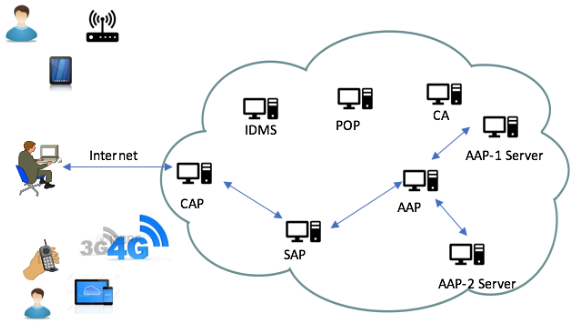


Figure 32 Security Components and Architecture for Cloud Computing Environments [R 164]

CC offer a lot of advantages such as: it is an efficient way to store and maintain databases, being a helpful tool for business, the services offered by CC are in cloud as SaaS, cloud computing solutions are in general less expensive than their software counterparts (pricing being offered on a per-user basis), an efficient use of CC reduce energy consumption significantly, the costumers are freed of problems related to the technological issues of installing and maintaining the IT.

In CC the servers are not accessed direct through network connections, they are accessed by the services they provide, ensuring a high degree of transparency to the cloud. Users in fact access certain cloud components (request brokers) and those

cloud components distribute requests to individual servers, as appropriate. This important cloud functioning aspect, was use as a basis for the security components and architecture solution for CC Environments given in [R 189].
To preserve the transparency character for CC, Security components and services must be transparent and also generic - adjustable to individual users, requirements, applications, and required services (Figure 32).

- The Application Access Point (AAP) Server is the service that distributes - based on types of requests, or other parameters - cloud service requests to individual application servers. It is related and use the Services Publishing and Dispatching (SPD) Server. The SPD server is based on the UDDI standard for discovering application services available in the cloud and it is used for publishing and discovering of cloud applications services.
- The Communication Access Point (CAP) is in fact the communication services provider, which can accept requests coming through different communications protocols.
- The Security Access Point (SAP) is the cloud server that provides front-end security services and is responsible with the authentication of users. It must be based on open standards and applicable in an open environment.
- Certification Authority (CA) server provides certification services in the cloud by issuing certificate to the client and to the SAP.
- The Identity Management System (IDMS) X.500 compliant directory, is another server that provides registration and identification services in the cloud.

To ensure the CC security, security techniques should be implemented at the Client level, at the SAP level and at the AAP level.

In [R 127] was proposed for the customers that belongs to a private cloud and want to outsource their services to a Cloud Service Provider (CSP), a 4 layer Architectural Security Solution in Cloud Computing (Figure 33)

3.4.1 The 5 Layer Cloud Security Architecture

A 4 Layer Cloud Security Architecture was proposed in [R 127] and is presented in Figure 33. This architectural solution covers the security for the all three above discussed elements: the identity, information and the infrastructure.

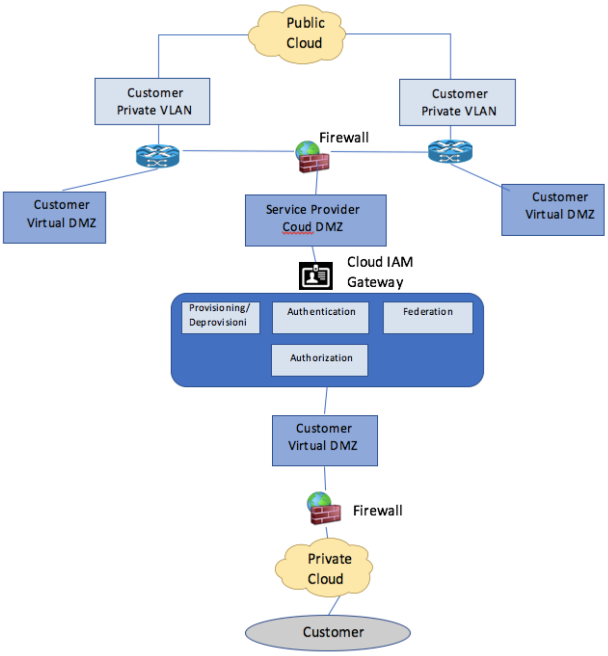


Figure 33 The 4 Layer CSA [R 127]

Layer 1, based on a Cloud IAM Gateway that belongs to a third-party cloud provider, introduces the Identity Access Management function. This will be realized by creating web security applications services which integrate the provisioning/deprovisioning, authentication, federation, authorization. These web security applications will be used like an external security approach.

Layer 2 of this architectural security solution introduce a firewall for enhancing the network security control (allow ports and IP access). This layer protects the physical infrastructure of both service customer and of cloud service providers [R 127].

Layer 3 by segregating the organizations' data, by using private VLAN, improve the isolation of data customer. VLAN are configured based on the access restrictions for each customers' virtual machine, based on Access Control Lists.

Layer 4 of security is assured by creating virtual demilitarized zone (DMZ) for each customer. This virtual zone could be accessed by other customers, and will restrict the access to the information that resides on private VLAN. Also, CSP will also have a DMZ zone to be accessed by all customers. In this zone will be stored data concerning all the customers – without affecting the customer's data.

This architecture will be completed with a 5th layer in Section 1.1.12. This 5th layer will be an additional layer introduced for enhancing the security for data-at-rest, by hiding the information in images.

Considering the steganography approach for securing at-rest data in public clouds, which is proposed in [R 17] and presented in Figure 20, I propose to complete the 4 layer CSA [R 127] with an extra Layer to hide data stored in the public cloud in images.

It results the following architecture given in Figure 34.

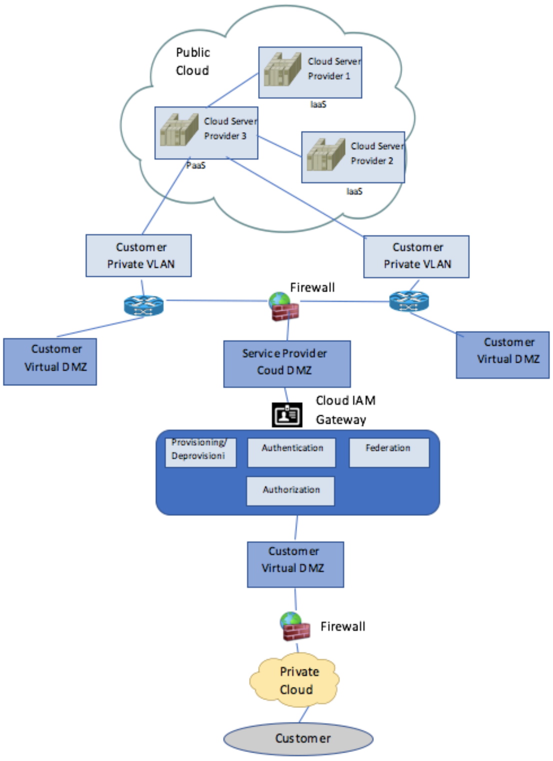


Figure 34 The 5 Layer CSA Architecture

The Security strength of the proposed approach

This 5 layer architecture combines the advantages given by the 4 layer architecture with the advantages offered by the combination of encrypting and data hiding technique proposed in [R 17] to prevent unauthorized data access in cloud data storage - based on using the Huffman Coding. Unauthorized users cannot rectify the original content of the data due to human visual system which has very low sensitivity. The authors made a detailed presentation of all processes needed to realize this security system (Embedding Data into Images, File Codifications, Hiding Data within Images Steganography, Searching of Valid Image, Mapping Data from a File to Image, Retrieving Data from Image, Construction of Huffman Tree, and a detailed security and performance analysis to prove that their approach offers high security of data-at-rest at any Cloud Service Provider (CSP) [R 17].

3.5 Detecting DDoS Attacks in Cloud Computing Environment

Distributed Denial of Service (DDoS) attacks in cloud computing environments are often the source of cloud services disruptions [R 159]. One of the efficient methods for detecting DDoS is to use the Intrusion Detection Systems (IDS), [R 179]. However, IDS sensors have the limitations that: they yield massive number of alerts and produce high false positive rates and false negative rates [R 216].

With regards to these IDS issues, our proposed solution aims to detect and analyse 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 (within the front-end), which takes the alerts from multiple heterogeneous sources and combines them using the Dempster's combination rule [R 126].

Therefore, our approach quantitatively represents the imprecision and efficiently utilizes it in IDS to reduce the false alarm rates, and it can be used for analysing the logs generated by sensors, which seems to be a big issue [R 121].

3.5.1 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 [[R 20].

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 [[R 20] [R 126].

According with DST method, for a given state space (Ω) the probability (called mass) is allocated for the set of all possible subsets of Ω, namely 2^{Ω} elements.

For quantitatively representing the imprecision, we applied the DST operations in 3-valued logic using the fault-tree analysis (FTA), adopted by [R 83] and also used [R 168] [R 126]. DST can also be utilized in IDS to reduce the false alarm rates by the representation of ignorance [R 57] [R 194] [R 193].

Thus, if a standard state space Ω is {True, False}, then 2^{Ω} 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 [R 193].

Since in DST the [sum of all masses] = 1 and m(Φ) = 0

$$\Rightarrow m(True) + m(False) + m(True, False) = 1 \qquad (3.12)$$

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 15 describes the Boolean truth table for the OR gate [R 193].

		b1	b2	b3
	v	T	F	(T,F)
a1	T	T	T	T
a2	F	T	F	(T,F)
a3	(T,F)	T	(T,F)	(T,F)

Table 15 Boolean truth table for the OR gate

From Table 15 we have [R 126]:

$$m\{A\} = \{a1, a2, a3\} = \{m(T), m(F), m(T,F)\} \qquad (3.13)$$

$$m\{B\} = \{b1, b2, b3\} = \{m(T), m(F), m(T,F)\} \qquad (3.14)$$

$$\Rightarrow m\{A \text{ v } B) = (a1b1 + a1b2 + a1b3 + a2b1 + a3b1; a2b2; a2b3 + a3b2 + a3b3) = (a1 + a2b1 + a3b1; a2b2; a2b3 + a3b2 + a3b3) \qquad (3.15)$$

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} [R 187] [R 126]:

$$m_{12}(A) = \frac{\sum_{B\cap C=A} m1(B)m2(C)}{1-K} \text{ when } A \neq \phi \qquad (3.16)$$

$$m_{12}(\phi)=0 \tag{3.17}$$

where K = $\sum_{B \cap C=\emptyset} m1(B)m2(C)$

The factor 1-K, called *normalization factor*, is constructive for entirely avoiding the conflict evidence.

3.5.2 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. A complete survey upon intrusion detection using DST is presented in [R 44] and other related work, together with the relationship of our work comparative to the other works are pointed out in [R 126].

Our study was to detect DDoS attacks in cloud computing environments. Dempster-Shafer Theory (DST) was used to analyze the results received from each sensor (i.e. VM-based IDS).

The data used in our solution were generated by ourselves, by performing DDoS attacks using specific tools against the VM-based IDS [R 126].

We used in our work the solution of data fusion of the evidences obtained from sensors and given in [R 193] [R 18]. It was realized using the Dempster-Shafer combination rule, which was demonstrated in [R 193] as being advantageous – 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 relieved, as the number of alerts will decrease [R 126].

3.5.3 The Proposed Solution

Our solution is presented in Figure 35. 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) [R 126].

The first step of our solution was the deployment stage of a private cloud using Eucalyptus open-source version 2.0.3. The topology of the implemented private cloud was: a front-end (with Cloud Controller, Walrus, Cluster Controller, Storage Controller) and a back-end (i.e. three nodes) [R 124]. The Managed networking mode was chosen because of the advanced features that it provides and Xen hypervisor was used for virtualization [R 126].

Then, the VM-based IDS were created, by installing and configuring Snort into each VM. The reason for choosing this IDS location is to avoid the overloading problems and to reduce the impact of possible attacks [R 136] [R 179] [R 126]. In [R 128] are detailed the 6 steps involved in the creation of the VMs-based IDS (Figure 36).

These IDSs yield alerts, which are stored into the Mysql database placed within the Cloud Fusion Unit (CFU) of the front-end server. A single database was used 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. There are similar solutions that use the idea of obtaining and controlling the alerts received from the IDS Sensor VMs using an IDS Management Unit [R 179] [R 42] but our solution adds the capacity to analyse the results using the Dempster-Shafer theory of evidence in 3-valued logic.

As showed in Figure 37, the Cloud Fusion Unit (CFU) comprises 3 components: Mysql database, bpa's calculation and attacks assessment [R 126].

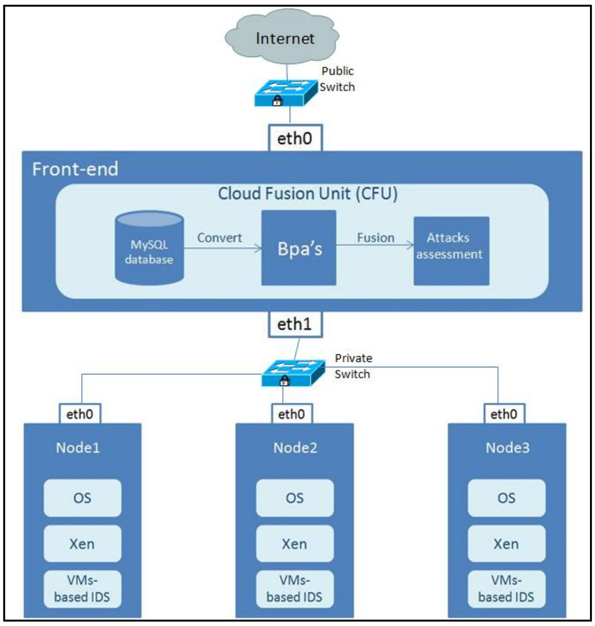


Figure 35 IDS Cloud Topology **[R 126]**

Step 1: Register Debian pre-packeged VMs into private cloud
Step 2: Deploy instances
Step 3: Create the Eucalyptus storage volume and attach it to the instance
Step 4: Install and configure Snort into the VMs
Step 5: Detach the Eucalyptus volume
Step 6: Deploy snapshot of the volume

Figure 36 VM-based IDS Deployment [R 128]

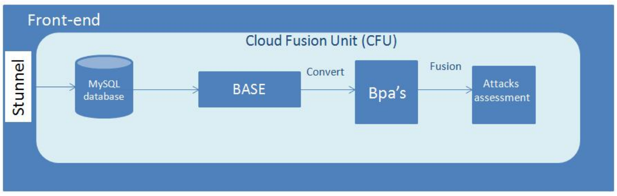


Figure 37 Relationships of the centralization components in CFU **[R 128]**

Figure 37 is an extended scheme of the CFU component from Figure 36. The BASE - Basic Analysis and Security Engine was introduced between Mysql the storing server) and the Bpa's component. BASE is the successor of ACID (Analysis Control for Intrusion Detection) [], and was chosen because is a web server analysis tool for monitoring the alerts received from the VM-based IDS sensors [R 172]. Additionally, its reporting strategy facilitates the procedure of obtaining the Basic probabilities assignment (Bpa's) [R 128].

The DDoS attacks against the VMs-based IDS were simulated using the Stacheldraht DDoS tool, which s based on the 'Client', 'Handler (s)/Master (s)', 'Agent(s)/Daemon(s)', 'Victim(s)' architecture. This 3 layers 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 2 additional features: an encrypted client to handler communication and the agents that are automated remotely updated [R 45] [R 33] [R 128].

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) [R 128].

3.5.3.1 Mysql database

The Mysql database was introduced for storing the alerts received from the VM-based IDS. These alerts are converted into Basic Probabilities Assignments (bpa's). In [R 128], a quantitative analysis of the TCP SYN flooding attacks, UDP flooding attacks and ICMP flooding attacks was realized, in order to reduce the large amounts of false alarms rates produced by the Intrusion Detection Systems. Our snort database is described in [R 128], together with the created Join Database Tables (Fig.4 from [R 128])

Therefore, first the mass assignments for all 3 states of each sensor illustrates [R 128]:

$$\begin{cases} m_x(T)\text{, the DDoS attack occurs} \\ m_x(F)\text{, the DDoS attack doesn't occur} \\ m_x(T, F)\text{, the "unknown" classification of the DDoS attacks.} \end{cases} \qquad (3.18)$$

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

Figure 38 presents the mass assignments calculated for two VM-based IDS, which were realized by implementing the pseudocode proposed in Figure 36.

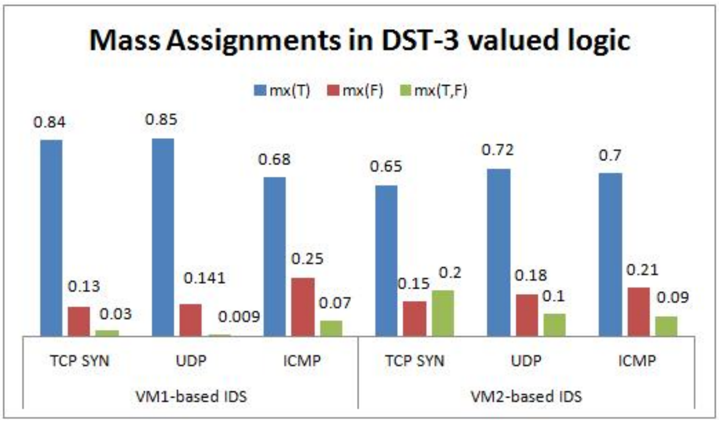


Figure 38 Mass Assignments in DST **[R 128]**.

First, the detection rate ($m_x(T)$) for each flooding attack against each VM-based IDS [R 128] was computed as defined in [R 217]:

$$\textit{Detection Rate (DR)} = \frac{\textit{number of true attacks reported}}{\textit{number of total observable attacks}} \qquad (3.19)$$

Then, the computation of the probabilities for (True, False) element [R 128] was realized based on [R 217]. $m_x(F)$ will be calculating by the help of DST, based on [sum of all masses] = 1:

$$m_x(F) = 1\text{-}m_x(T)\text{- } m_x(T, F) \qquad (3.20)$$

The results from Figure 4 reveal a high detection rate ($m_y(F) > 0.65$) 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.

3.5.3.2 Basic probabilities assignment (bpa's) calculation

For calculating the basic probabilities assignment, first we decide to the state space Ω. So, we have choosen to use DST operations in 3-valued logic {True, False, (True, False)} suggested by [R 214] for the following flooding attacks: TCP-flood, UDP-flood, ICMP-flood, for each VM-based IDS. Thus, the analyzed packets were: TCP, UDP and ICMP. Further, a pseudocode (Figure 39) for converting the alerts received from the VM-based IDS into bpa's was provided, to obtain the following probabilities of the alerts received from each VM-based IDS:

- (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))

```
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
```

Figure 39 Pseudocode for converting the alerts into bpa's [R 128

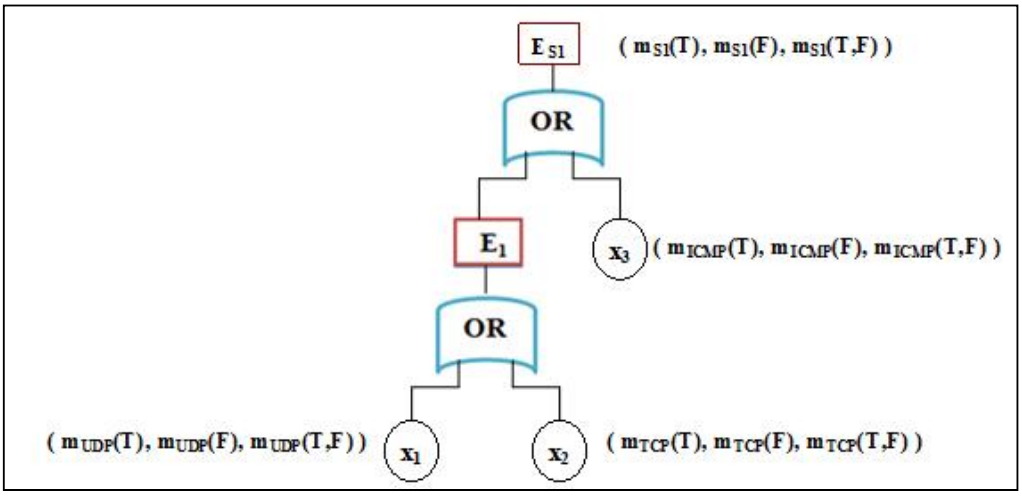

E S1
(mS1(T), mS1(F), mS1(T,F))
OR
E1
X3
(mICMP(T), mICMP(F), mICMP(T,F))
OR
(mUDP(T), mUDP(F), mUDP(T,F))
X1
X2
(mTCP(T), mTCP(F), mTCP(T,F))

Figure 40 Bpa's calculation **[R 126]**

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 Figure 40, that 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 [R 128]. The calculus will be done based on the results obtained in Figure 38 and is given in [R 128].

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

$$Bel(S1) = m_{S1}(T) \qquad (3.21)$$
$$Pl\ (S1) = m_{S1}(T) + m_{S1}(T, F) \qquad (3.22)$$

3.5.3.3 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 16 and equation (3.16).

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

Table 16 mS1,S2 calculation **[R 126]**

As a conclusion of our work, we affirm that by using DST our proposed solution has the following advantages: to accommodate the uncertain state, reduce the false negative rates, increase the detection rate, resolve the conflicts generated by the combination of information provided by multiple sensors and alleviate the work for cloud administrators.

4 Resource allocation

4.1 Resource allocation optimization for clouds

Fault tolerance is a major concern in the cloud environments to guarantee availability of critical services, application execution, and hardware. As the cloud computing systems continue to grow in their scale and complexity, it is of critical importance to ensure the stability, availability, and reliability in such systems.

Therefore, the cloud service providers must assure the fault tolerance/availability of the services they provide to the end users. The fault-tolerance validation of a service is of critical importance to ensure the SLAs are properly adhered. However, due to numerous stochastic factors involved, it is quite difficult to verify that a fault-tolerant machine will meet the reliability requirements.

A practical approach of implementing fault tolerance is through redundancy that involves duplication of hardware and software components, such that if a component or a process fails, the backup process or component is available to take place of primary.

We will present an approach that permit to optimizing the allocation of hardware resources at CSP level that will either maximize reliability at a cost or minimize costs for a required reliability. The optimization solution presented is based on the use of genetic algorithms [R 162] [R 163] [R 166] [R 205].

4.1.1 The Model Description

Let model the cloud computing computation as a system constructed from objects (instances) and resources. The objects that participate in a computation are related to each other via semantic links pointed to by the objects joints. We define a resource as an element that requires no other services, Objects may require services from resources or other objects [R 192].

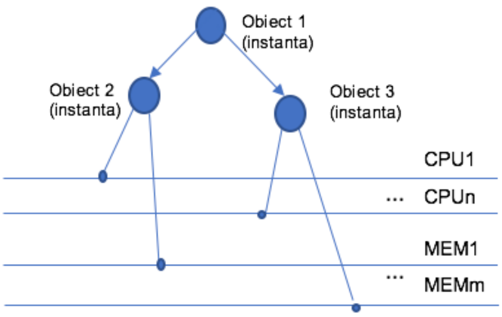


Figure 41 The Allocation model

The properties of the resources may allow us to model the system elements in terms of resource segments. For example, we may model one particular memory as a resource, if we know the probability of failure for it. On the other hand, if we don't have the probability of failure at this level, we may model the whole memory at a given locality as a resource. Therefore, this model is flexible in supporting a complete resolution of the system elements.

We allocate required resources to executing an "to be executed" objects. These resources are physically linked according to their geographic and hardware constraints. However, in addition to resources, objects may need services that are provided by other objects, which in turn may need other services and resources and so on. We represent this relationship with a graph, where objects and resources are nodes and the relations between them are direct arcs. The resources are always the leaf-nodes; they are not expected to need services from other resources.

This model can be utilized for identifying the number of resources that need to be allocate to ensure the availability/reliability of a service provided by a Cloud Provider.

The services provided by CSP each involve the running of a series of instances that we can associate with the objects of the proposed model. Successful completion of the service is conditional upon the successful completion of the instances, depending on their turn, by the proper functioning of the resources involved.

We assume that realization of a cloud service involves the use of several instances in the cloud (all of which must be functional), which in turn are conditioned by the proper functioning of several resources. The Service Reliability Model will be a series model that will include a number of n components (the resources involved in performing the service) serially connected from the reliability point of view is considered.

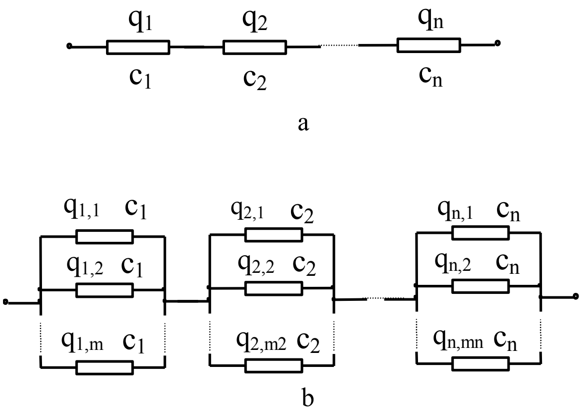


Figure 42 Reliability Model

Each element *i* (1 $\leq$ *i* $\leq$ *n*) is characterized by its failure probability, q_i, and by its cost, c_i, as depicted in Figure 42.a.

The reliability function P_p, respectively the cost function C_p for this system, are computed using the following expressions [R 163]:

$$P_p = \prod_{i=1}^{n}(1-q_i) \qquad (3.23) \qquad\qquad C_p = \sum_{i=1}^{n} c_i \qquad (3.24)$$

We consider for the entire system the Distributive Static Redundancy (DSR) by which each element *i (i=1…n)* is replaced with a group of m_i identical elements of the same type, connected in parallel from the reliability point of view (Figure 42.b). We admit the case that the elements in the same group have the same attributes of the safety running, which is stated by the following relation [R 163]:

$q_{i,1} = q_{i,2} = ... = q_{i,m_i} = q_i$, for *i* = 1, *n* (3.25)

In these conditions, for the redundant system, the function of reliability (P_D) and the expression for the cost (C_D) are given by the relations (3.26) and (3.27) [R 163].

$$P_D = \prod_{i=1}^{n}\left(1 - q_i^{m_i}\right) \qquad (3.26) \qquad\qquad C_D = \sum_{i=1}^{n} m_i \cdot c_i \qquad (3.27)$$

We will consider only the situation in which we have: $Q_D = 1 - P_D \ll 1$. This condition is fulfilled in the case that every group of elements has a high reliability, which is equivalent with relation (3.28) [R 163].

$q_i^{m_i} << 1$, for *i* = 1, *n* (3.28)

Considering this last relation, it results:

$$P_D \cong 1 - \sum_{i=1}^{n} q^{m_i} \qquad (3.29)$$

4.1.2 The allocation algorithm

The distributed DSR problem can be addressed in two ways. The first approach considers the maximum allowed value of the cost, C_{DM}, and finds the values of $m_1, m_2, ... m_i, ... m_n$ in such a way, that the reliability function of the redundant system, P_D, has the maximum (optimum) value. The second approach considers the minimum allowed value of the reliability function, P_{Dm} and searches for the values of $m_1, m_2, ... m_i, ... m_n$ so that the cost function of the redundant system, C_D, has the minimum (optimum) value. The un-faulty working probability, P_D, is a monotonous rising function dependent of *n* variables, $m_1, m_2, ... m_i, ... m_n$, which respect the relation [R 163]:

$$\sum_{i=1}^{n} m_i \cdot c_i = C_{DM} \qquad (3.31)$$

One of these variables (m_n, for instance) can be expressed depending on the others, as presented below [R 163]:

Expressing m_n from relation (3.31) and replacing it in relation (3.29), leads to the next relation.

$$P_D = 1 - \sum_{i=1}^{n} q_i^{m_i} - q_n^{\frac{C_{DM} - \sum_{i=1}^{n} m_i \cdot c_i}{c_n}} \qquad (3.32)$$

Next, looking for the maximum value of the function $P_D\left(m_1, m_2, ... m_i, ... m_n\right)$, we will use the partial differential annulment method.

$$\frac{\partial P_D}{\partial m_i} = -q_i^{m_i} \cdot \ln q_i + q_n^{m_n} \frac{c_i \cdot \ln q_n}{c_n} = 0 \quad \Rightarrow \quad \frac{q_i \cdot \ln q_i}{c_i} = \frac{q_n^{m_n} \cdot \ln q_n}{c_n} = \alpha \qquad (3.33)$$

It is important to note that α is a coefficient that is independent of ***i***.

Let: $\beta_i = \frac{c_i}{lnq_i}$ (3.34)

$\Rightarrow \quad \alpha = \frac{q_i^{m^i}}{\beta_i}$ (3.35)

Then: $m_i = \frac{ln(\alpha \cdot \beta_i)}{lnq_i} = \frac{\beta_i \cdot ln(\alpha \cdot \beta_i)}{c_i}$ (3.36)

Substituting this computed relation for m_i in relation (3.31) gives:

$C_{DM} = \sum_{i=1}^{n}[\beta_i \cdot ln(\alpha \cdot \beta_i)] = \sum_{i=1}^{n}\beta_i \cdot ln|\alpha| + \sum_{i=1}^{n}(\beta_i \cdot ln|\beta_i|)$ (3.37)

$\Rightarrow \quad ln|\alpha| = \frac{C_{DM} - \sum_{i=1}^{n}\beta_i \cdot ln|\beta_i|}{\sum_{i=1}^{n}\beta_i}$ (3.38)

Consequently, returning to (3.36), we obtain:

$m_i = \frac{ln|\alpha| + ln|\beta_i|}{lnq_i}$ (3.38)

So, for calculating the values of m_1, m_1, … m_i, … m_n, we have the following algorithm:

```
The Input data are: the cost c_i, and the failure rate q_i, of each component
For a serial reliability model
Begin
        For each elementar component from 1 to n calculate
        Begin
                $\beta_i = \frac{c_i}{lnq_i}$
                $S1 = S1 + \beta_i \cdot ln|\beta_i|$,
                $S3 = S3 + \beta_i$
        end
        Calculate: $ln|\alpha| = \frac{C_{DM} - S1}{S3}$
        For each elementar component from 1 to n calculate
        begin
                $m_i = \frac{ln|\alpha| + ln|\beta_i|}{lnq_i}$
        end
        Apply GA for obtaining integer solutions
End
```

Figure 43 Pseudocode for obtaining the integer values for m_i

Applying the above relations, one usually obtains fractional values for m_1, m_1, … m_i, … m_n. The cost of the obtained system is exactly the maximum imposed one, C_{DM}. But m_i should have positive integer values.

In order to obtain these integers values, we will initially consider for m_i the integer part of the value obtained using (19). Thus, the cost of the resulted system, C , is less than the imposed cost, C_{DM}. It remains to decide how we can use more efficiently the money resulted from the removal of the fractional parts of elements, in order to increase the system reliability [R 163].

For solving this, we use the genetic algorithm. The imposed cost is now [R 163]:

$C_{DM}' = C_{DM} - C$. (3.38)

The inferior limit for each type of element is 0, as it is possible not to add any element of that type. Thus, the superior limit for each type is computed like this:

$\max_i = \frac{C_{DM}'}{c_i}$ (3.39)

In [R 163] is investigated the effect of reducing the searching space of the genetic algorithm using a mathematical algorithm. It makes a comparison between two implementations of a reliability system optimizing problem using genetic algorithms and mathematical methods.

[R 163] attempts to show how mathematical methods can be used to improve the results of genetic algorithms, particularly GAlib, considering two approaches for solving the distributed static redundancy. GAlib is a C++ library of genetic algorithms, implemented by Matthew Wall form the Massachusets Institute of Technology.

4.1.3 Genetic Alghorityms

Genetic algorithms (GAs) are global random search methods widely employed in optimization problems, or in problems where the gradient of a given objective function is not available. The power of GAs consists in only needing objective function evaluations to carry out their search.

GAs consist in having a population of candidate solutions (individuals, chromosomes) to an optimization problem that evolves at each iteration t of the algorithm, called generation [R 27] [R 75] [R 92]. In each generation, relatively successful individuals are selected as parents for the next generation. A new generation of solutions evolves, using genetic operators like crossover and mutation. Each individual is evaluated relatively to the user defined fitness function. Individuals are then ordered by fitness and the process is repeated until a criterion of stop is reached. Fitness function is a scalar value that combines the optimization objectives and is obtained in the evaluation step, when a problem specific routine returns its value. The fittest individuals will survive generation after generation while also reproducing itself. At the same time the weakest individuals disappear from each generation [R 163].

Individuals must be encoded in some alphabet, like binary strings, real numbers, and vectors.

In a practical application of GAs, a population pool *P(t)* of chromosomes must be installed and they can be randomly set initially. In each cycle of genetic evolution, a subsequent generation is created from the chromosomes in the current population, shown in Figure 44 [R 163].

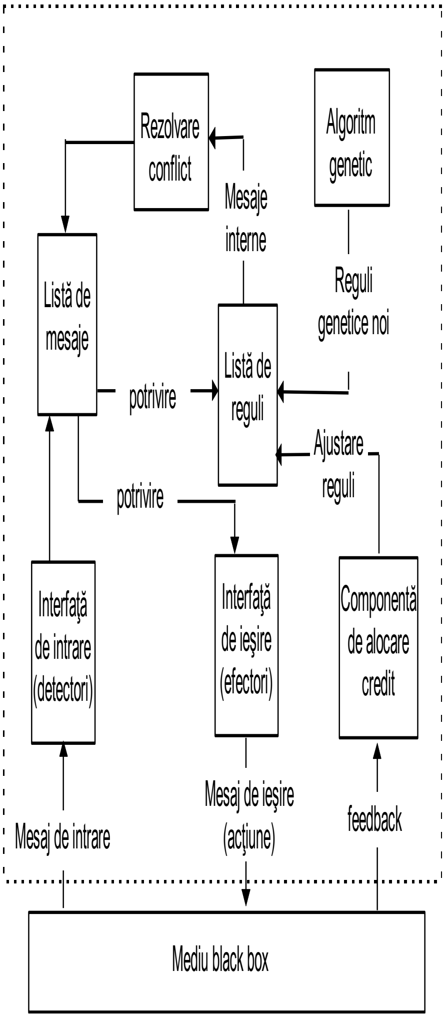


Figure 44 Creating the next generation in Gas [R 163]:

In the evaluation step, the Fitness value for each individual in the population is computed. During the selection stage, a temporary population denoted “Mating pool” is created in which the fittest individuals have a higher number of instances than those less fit. During the evolution, GAs employ *genetic operators* like crossover and mutation. The crossover is applied with the probability P_l. It randomly mates the individuals and creates offsprings D_1 and D_2 from two parents I_1 and I_2 by combining the parental genes and transferring them to the next generation. The mutation operator is applied with a low probability P_m. It creates new individuals D_3, which are inserted into the population, by randomly changing the parent I_3 [R 163].

The algorithm establishes the next generation P(t+1) and by this way, individuals of the original population are substituted by the new created individuals.

In essence, the procedure of a GA is given as follows:

Step 1. Generate randomly a population of chromosomes.
Step 2. Calculate the fitness for each chromosome in the population.
Step 3. Create offspring's by using genetic operators.
Step 4. Stop if the search goal is achieved. Otherwise continue with Step 2.

In usually optimization problems, besides the design variables there are constraints related to some physical or economical restrictions [R 76].

GAs can consider the constraints by using different methods. The most used approach is to reject the infeasible individuals. Another approach is to use penalty functions. In this case, violation of constraints takes the form of penalties. The basic idea of this approach is to "punish" the fitness value of an individual whenever the solution produced violates some of the constraints imposed by the problem [R 163].

4.1.4 System Modeling and Implementation of the Genetic Algorithm

The solution for the presented problem was implemented in Microsoft Visual C++ and uses the GAlib class library [R 71].

The genomes are objects of the class GA1DArrayAlleleGenome<int>. This class defines an integer array genome with alleles, which means that the domain of possible values of the elements can be specified. There can be specified one common domain for all the elements in the array – by defining a set of alleles. We used this type of genome to limit the searching space [R 163].

The genome creation

For the creation of the genome, the array of sets of alleles and the objective function are specified. The array is created as an integer array, having the size equal with the maximum number of elements that can be serially connected. The searching space for the genetic algorithm can be easily limited by limiting the size of the domains of the elements in the array genome. To encode the individuals, an array of sets of alleles is used. For each type of element, the corresponding set of alleles is appended. The program uses a configuration function that is called when another genetic algorithm is started or when the constant values of the problem change [R 163].

The configuration function performs the following actions:

- Creates the genome and the corresponding operators;
- Creates the genetic algorithm (the function gets as argument the created genome);
- Sets the parameters of the genetic algorithm;
- Calls the initialization function for the genetic algorithm.

Then, an initialize, a crossover and a mutation operator are established [R 76], [R 165], [R 210]. The initialize function initializes a genome like this: each element in the array is set to a randomly chosen value in the allele set. This value is then adjusted so that the initial genome respects the maximum imposed cost. This adjusting procedure, intended to obtain valid individuals, is also performed when mutation is applied.

The mutation operator performs two steps. First, the number of elements is computed proportionally with the mutation rate. If this number is less than 1, we cross twice the array in each sense, changing the value of each element with a value that is randomly chosen but so that the cost does not go beyond the imposed cost. If the calculated number of elements is greater than 1, this difference will be the number of elements that will be affected by mutation. These elements are randomly selected and the new value for each is randomly established. Then adjusting is performed in order not to surpass the imposed cost [R 163].

As crossover operator, we use the uniform crossover between parents of the same length, which generates each child by randomly taking bits from each parent. For each bit we flip a coin to see if that bit should come from the mother or the father.

Figure 2 depicts the uniform crossover operator for arrays of the same length.

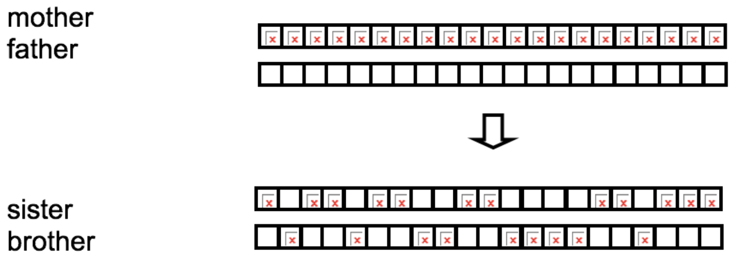


Figure 45 Uniform crossover [R 163]

The objective function for the genetic algorithm (the evaluator of the genome or fitness function) is implemented as a function that receives as argument the genome and returns the fitness value. If the cost correspondent to the genome surpasses the maximum imposed cost, the genome is penalized. This is performed returning a negative value. If the cost is allowable, the function returns the computed reliability of the system, computed using relation (3.26). Relation (3.29) could also have been used. The presented mathematical solution works for the case the failure probability of the elements in the system, q_i, is very small [R 163].

4.1.5 Program Facilities and Obtained Results

The implementation is available as two executable files, one for each implementation. The user can specify the maximum imposed cost. The user is also allowed to set how many groups of elements there are in the system (n) and, for every group, the failure probability (q_i) and the cost (c_i). It can be selected the type of the genetic algorithm to run: *Simple*, *Steady-State*, *Crowding*, *Incremental* and *Deme.*The evolution for the selected genetic algorithm can be controlled by the following commands: reset the evolution, evolve one generation, evolve many generations, continuously evolve, and stop the evolution. These commands are also available through the toolbar. There is also the possibility of specifying the genetic algorithm's parameters: mutation probability, crossover probability and population size.

The current generation is displayed during evolution. The best solution found until the current generation is displayed both textually and graphically [R 163].

Using the presented above mathematical method, the genetic algorithm searching space is not limited all the time with the same percent. The limitation performed by this method is dependent of the initial data [R 163].

- For limitations of the searching space to 30 % or 16 %, for instance, there are no differences between the two solutions.
- For a limitation to or 8.5 %, in 87 % of cases, there is no difference of performance between the two implementations, and in the rest of cases (13 %), the pure genetic algorithm needs mean 7 generations more.

- Not even for a limitation to 0.5 %, the difference is not sensible.

The graphic in Figure 46 presents the differences between the two implementations: pure genetic algorithm and mathematical method + genetic algorithm in the case of a limitation of the searching space to 0.26 %, from 12168 to 32 points. The vertical axis represents the number of generations necessary to find the optimum solution. We can notice that the second method (represented with blue) is more efficient [R 163].

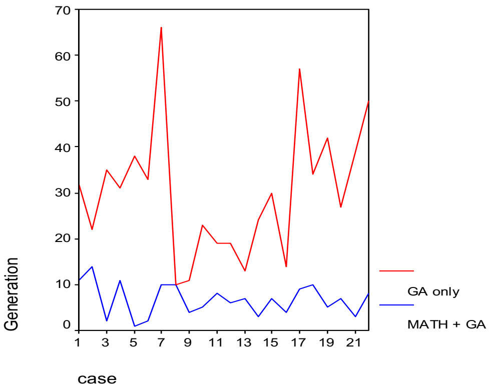


Figure 46 Differences between the two implementations [R 163]

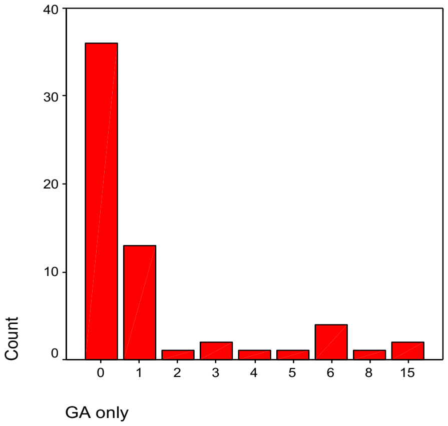


Figure 47 limitation of the searching space [R 163]

In Figure 47 we can observe the difference in the case of a limitation of the searching space to 0.0128 %, from 7776 to 1 point. After this limitation, the solution is found in the first generation. The graphic shows the situation before the limitation. We can see that in 59 % of cases, the solution is obtained in the first generation, in 21.3 % – after one generation and in the rest of 19.7 % cases – after approximating 6.5 generations. The mean number of generation after which the solution is found is 1.51. So, we can see that the effect is not considerable but for very big limitations [R 163].
The tests were made using the crowding genetic algorithm, having the following parameters [R 163]:

- population size = 500,
- mutation probability = 0.01,
- crossover probability = 0.9.

We conclude that genetic algorithms are powerful search techniques suitable to solve reliability problems, but an efficient modeling of the problem using mathematical methods can improve even more their performance. The main advantage of using genetic algorithms is that they require no gradient information about the problem and they are resistant to becoming trapped in local optima [R 163].

4.2 Optimizing File Availability in Peer-to-Peer Content Distribution Cloud Storage

The peer-to peer paradigm was invented for large networks. In this type of systems, copying a file by a peer not prevent another peer also to copy it, but the files that contribute to the common pool are costly. Analyzing models for P2P file sharing suggests that a fixed contribution to the number of files shared at a given time can be asymptotically optimal as the number of participants grows [R 22]. Thus, this problem

can be optimized, but optimization is difficult since it includes a high number of parameters and implies integer programming [R 6] [R 141].
Genetic algorithms (GAs) require little knowledge about the problem being solved, are easy to implement and robust. being suited to many optimization~~.~~ So, is presented a genetic algorithm approach for optimizing the File Availability in Peer-to-Peer (P2P) file sharing systems [R 165].

4.2.1 P2P SHARING SYSTEMS

Based on the notations and the assumptions presented in [R 6] let consider a P2P sharing system with the following characteristics: a nuber of I nodes with P_i, the up probability for node I and S_i, the shared storage for node i. Let consider J the number of distinct files, with b_j the size of the j th file, q_j the request probability of the j th file and x_{ij} - a zero-one variable which is equal to 1 if node i contains a replica of file and is zero otherwise. Also, n_j denote the number of replicas for file j and let consider the special case, where each node is up with the same probability p_i=p. The problem is to choose a number of non-negative integers n_i, … , n_J such that the relation (3.40) is maximized subject to constraints given by relation (3.41).
The hit probability is [R 6]:

$$P_{hit} = 1 - \sum_{j=1}^{J} q_j \prod_{i=1}^{I} \left(1 - p_i\right)^{xij} \tag{3.40}$$

The constraints that must be satisfy are:

$$\sum_{j=1}^{J} b_j x_{ij} \le S_i, \quad i = 1,...,I \tag{3.41}$$

In conclusion we have to maximize $1 - \sum_{j=1}^{J} q_j \left(1 - p\right)^{n_j}$ when $\sum_{j=1}^{J} b_j n_j \le S$, where $S = S_1 + ... + S_I$ is the total shared storage.
This optimization problem can be also solved efficiently by genetic programming [R 165].

4.2.2 The Genetic Algorithms

For considering the constraints we reject the infeasible individuals. The basic idea is to “punish” the fitness value of an individual whenever the solution produced violates some of the constraints imposed by the problem. A simple GA is applied, having the following main features [R 165]:

- Individuals are encoded like vectors of binary strings;
- The genetic operators are implemented according with the encoding scheme used;
- Randomly generates the initial population, but allows the use of an initial population specified by the user;
- Performs the GAs specific iteration;
- Includes the best performing individual of the parent generation in the new generation in order to prevent a good individual being lost by the probabilistic nature of reproduction;
- Allows the user to establish the GAs parameters: the size of the population, the type of selection scheme, crossover and mutation and the probability of applying the genetic operators.

The design variables of the problem are the positive integer numbers: n_1, … , n_J that maximize relation (3.40) related to the restrictions given by relation (3.41).
The coding scheme uses vectors of pozitive integer numbers, having the form of relation and presented in Figure 48 [R 165].

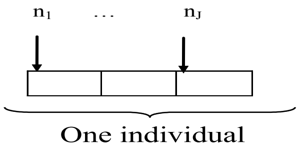


Figure 2

Figure 48 Individuals encoding scheme [R 165

It has to be noted that, in the evaluation step, the binary strings are decoded to the corresponding pozitive integers and are used to establish the Fitness function [R 165.

4.2.2.1 The crossover operator

The crossover operator acts at genotypic level, and so it is intended to work with binary strings. The crossover algorithm consists in following steps [R 165:
- Randomly choose two parents p_1 and p_2, with the crossover probability.
- Randomly choose $k_1 \in [1,2,..,l_1$-1], a number that becomes the crossover point, where l_1 is the length of the first parent. The chromosomes of the first parent are divided in 3 subchromosomes: a left subromosome placed on the left side of k_1-1, a right subromosome placed on the right side of k_1+1 and a central one, placed between k_1-1 and k_1+1.
- Randomly choose $k_2 \in [1,2,..,l_2$-1], a number that becomes the crossover point, where l_2 is the length of the first parent. The chromosomes of the first parent are divided in 3 subchromosomes: a left subchromosome placed on the left side of k_2-1, a right subchromosome placed on the right side of k_2+1 and a central one, placed between k_2-1 and k_2+1.
- By exchanging the central subchromosomes between the two parents, the crossover produces two offsprings.

Besides this basic approach, the crossover operator verifies if the obtained individuals fulfill the constraints of the problem. If not, it uses a repairing strategy, by repeatedly generating offsprings until the restrictions are fulfilled [R 165.

4.2.2.2 The mutation operator

Similar with the crossover operator, the mutation operator also acts at genotypic level, and so it is intended to work with binary strings. The one point mutation algorithm consists in following steps [R 165:
- Randomly choose a parent p with the mutation probability.
- Randomly choose $k \in [1,2,..,l]$, a number that becomes the mutation point, where l is the length of the parent. The selected element is replaced with a complementary value.

Similar with the crossover operator, the mutation operator verifies if the mutated individual fulfills the constraints of the problem. If not, it uses a repairing strategy, by repeatedly generating a new individual, until the restrictions are fulfilled.

4.2.2.3 Appling GAs in optimisation problems

The first step to start the optimization is to define the initial population. This is carried out, by generating individuals having the form depicted in Figure 44 with the randomly picked positive integer parameters in their domain. Also, the individuals are subject to the constraints given in relation (3.41).

By generating the initial population, the infeasible individuals are rejected and the random generation of individuals continues until the required number of individuals is established without violating the constraints [R 75].

Once the parent population is available, the individuals are to be evaluated related to their quality in the search space. The approached problem deals with the objective given by relation (3.43):

Fitness=$1-\sum_{j=1}^{J} q_j (1-p)^{n_j}$ (3.43)

The selection operator uses the Fitness value. In this approach, the roulette wheel selection is used, which is the traditional selection function. The probability of surviving is equal to the fitness of a given individual, divided by the sum of the fitness of all individuals. In the implementation of the algorithm, simple elitism was also applied. This technique guarantees survival of the best individual [R 165].

Through the recombination operator a new population is created. All the parameter values have been calculated based on *inherited* values from the parent population. Therefore, no *new* information has been inserted in the population but only *old* information has been recombined. In order to introduce new information into the population pool, the mutation operator is used [R 165].

The traditional crossover and mutation operators are modified in such a way to produce allowable offspings, that respect the restrictions [R 75] [R 165].

4.2.2.4 Study Cases

A P2P network with the following characteristics was considered [R 165]:

- Number of files: J= 250
- Number of nodes: I=10
- The shared storages S_i for each node are equal quantities.
- The size of the files are equals.

The request probability of the j th file: $q_j = \frac{1}{J}$. The up probability for i th node: $p_j = \frac{1}{I}$

The problem is to find the J positive integers nj that maximize the hit probability given by (3.46). The unknown parameters n_j belong to the interval [1, 50]. Was considered a GAs with a population of 100 individuals. An individual is a vector of 250 integers.The restriction are given by (3.43). Since all the sizes bj are equals and their value related to S is established in such a way that the constraint becomes:

$\sum_{j=1}^{J} \cdot n_j \leq 6200$ (3.44)

The Fitness value is equal with the objective function (3.47). The initialization routine continues to randomly generate vectors of integers until the restriction is fulfilled. The crossover operator and the mutation operators use a reparing strategy. These operators are applied repeatedly until the restriction criteria is fulfilled. Two different runs were considered [R 165].

Study case 1

GAs used a population of 50 individuals and evolved for 30 generations.

After the genetic run, the Fitness value for the solution gives a high hit probability:

$P_{hit} = 0.8164$ (3.45)

The obtained solution fufills the constraints since

$$\sum_{j=1}^{J} \cdot n_j = 6140 < 6200 \qquad (3.46)$$

Figure 49 plots the obtained solution, that is, the vector having 250 integer components. The evolution of the Fitness during GAs generations is presented in Figure 50, where the Fitness value is plotted related to the generation number [R 165].

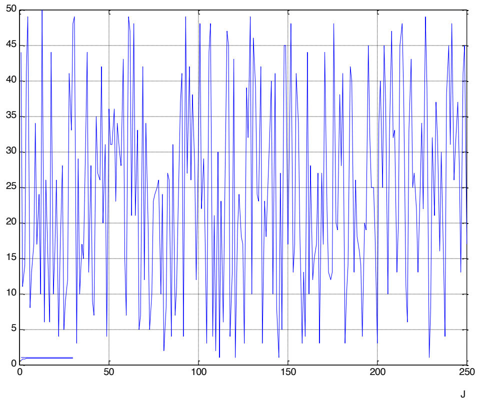


Figure 49 The solution for the study case 1 (a vector with 250 integer components)

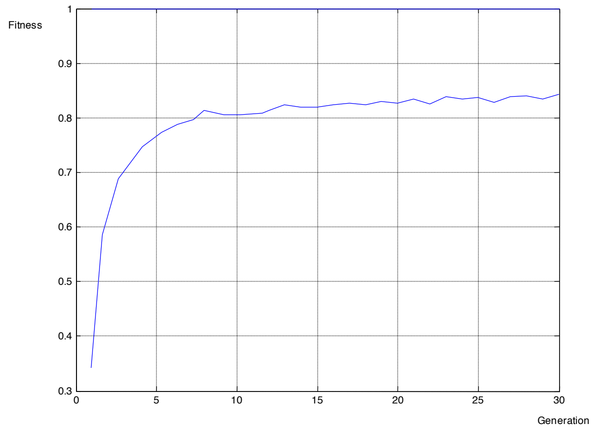


Figure 50 Fitness value related to the generation number in study case 1

Study case 2

GAs used a population of 100 individuals and evolved for 30 generations.

After the genetic run, the Fitness value for the solution gives a high hit probability:

$$P_{hit} = 0.9236 \qquad (3.47)$$

The obtained solution fufills the constraints since

$$\sum_{j=1}^{J} n_j = 6166 < 6200 \qquad (3.48)$$

Figure 51 plots the obtained solution, that is, the vector having 250 integer components. The evolution of the Fitness during GAs generations is presented in Figure 52, where the Fitness value is plotted related to the generation number [R 165].

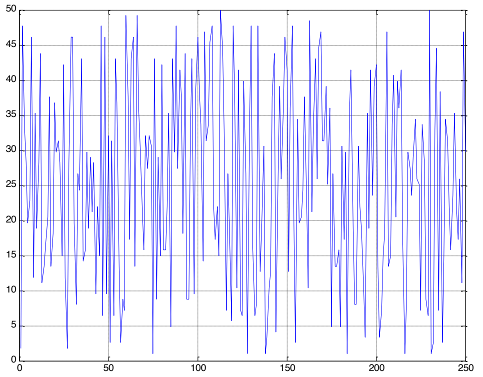


Figure 51 The solution for the study case 2 (a vector with 250 integer components)

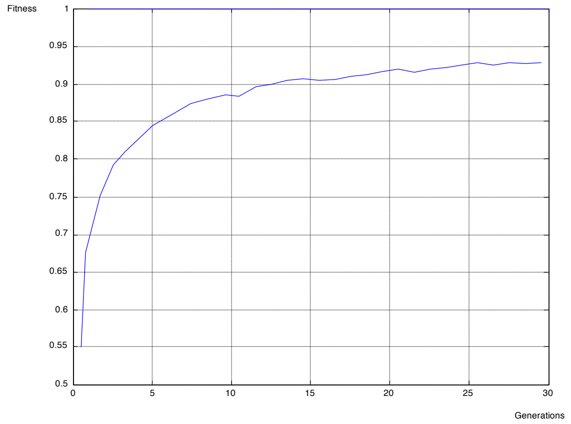


Figure 52 The solution for the study case 2 (a vector with 250 integer components)

By examining the Figure 50 and Figure 52, it can be seen that the Fitness function increases generation after generation. Also, a higher number of individuals leads to better solutions. The obtained results show that genetic algorithms seem to be suitable

for the approached task. The disadvantage that belong to the used method consists in the fact that, for large networks the design problem is time demanding. But, in recent years, the increasing computation power of computers makes this disadvantage lesser, so that it is possible to use stochastic algorithms effectively in many applications, such as this type of problems [R 165].
This approach can be continued by investigating other, more complex networks.

5 The Integration of cloud services into organizations

1.1 The overall process taken by enterprises to manage the IaaS cloud services

In [R 130] is presented qualitative analysis of the overall process taken by SMEs to manage the migration of their applications to Infrastructure-as-a-Service (IaaS), 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 Cloud Service Provider (CSP) supports the hardware related issues, whilst the software related issues should be identified by enterprises that want to migrate to cloud.
From consumer perspectives, the overall process taken by enterprises to manage the IaaS cloud services includes a collection of the following interrelated activities [R 130]:

1. The data analysis step constitutes the initial step of the overall process taken by organizations 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.
2. The decision-making step, starts by choosing the cloud service type (i.e. IaaS) and cloud deployment model (i.e. public cloud), and 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. The decisions will be made based on the analysis step. We assumed that IaaS is the cloud service type chosen public cloud is the cloud deployment model selected [R 130].
3. The migrating step is the effective moving stage of enterprise’s assets into cloud services, which includes two activities: developing the Service Level Agreement (SLA) and implementing cloud.
4. The management step, is realized using two management functions: business and operational.

Thus, Figure 53 encompasses the proposed overall process and then each step is discussed separately [R 130].

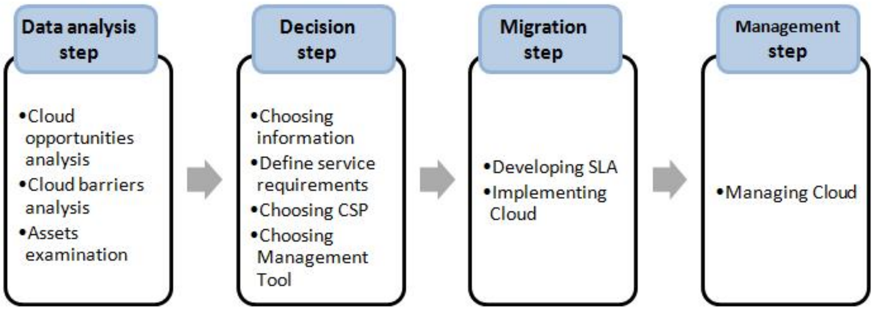


Figure 53 The Management Process of Enterprise’s Migration to IaaS **[R 130]**

In an IaaS cloud service, the Cloud Service Provider (CSP) supports the hardware related issues, whilst the software related issues should be identified by enterprises that want to migrate to cloud [R 130].

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. RightScale, enStratus, IMOD Kaavo, CloudWatch, Scarl, Tapin, Cloudkick). Our study was motivated by the fact that cloud management is a fundamental support for all users of cloud services from the cloud marketplace [R 130].

Companies can choose from the wide range of cloud delivery services (i.e. SaaS, PaaS and IaaS), which can be deployed in all four deployment models (i.e. private, public, hybrid and community cloud). The selection of the cloud deployment model depends on the size of the organization and its IT (Information Technology) maturity level [R 130].

While Small and Medium Enterprises (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 [R 142] [R 130].

5.1.1 Data analysis step

Represents the initial step of the overall process taken by organizations to manage the migration to IaaS and it includes [R 130]:

1. the analysis of cloud migration opportunities,
2. the study of cloud adoption barriers and
3. the examination of current infrastructure used by the organization.

In this process, businesses need to consider both risk and reward assessment, and involve an analysis of the costs of implementing cloud services [R 130].

5.1.1.1 Cloud rewards analysis

According to National Institute of Standards and Technology (NIST), the Cloud concept is defined by the five main characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [R 70] (Figure 2), which constitutes the *technical benefits* [R 130].

Another cloud opportunity that enterprises should identify is the *financial benefit* [R 117]. 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. [R 115] considers a case study 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 and demonstrates 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) [R 130].

5.1.1.2 Cloud risks analysis

For the migration process, an important step is to identity the cloud adoption risks and to consider how to manage the cloud adoption barriers. Thus, the major concerns of enterprises are the *security risks* implied by the act of embedding their resources within the cloud computing environment [R 135] [R 130].

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 [R 130].

Therefore, the implementing of the business migration involves the cooperation of all business managers, IT managers and IT vendors to implement the business migration, respectively the business disruption plans [R 130].

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 [R 35] But the core mechanism to protect resources is considered the ***encryption and key management*** usage in cloud computing (i.e. data in transit over networks, data at rest and data on backup media). All these measures are not sufficient for securing the cloud services and *Identity and* ***Access Management (IAM)*** must also be considered, which secures the user identity of cloud computing services [R 180] [R 130].

Also, besides security, *data governance* plays significant risk awareness for several enterprises sectors: financial services companies, energy and utilities, retail and wholesale industries and manufacturing. Data governance, for the migrating process, 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) [R 39]. Important to note that, for the health and financial sectors there are many regulatory restriction related with the moving of their data to cloud [R 116] [R 115]. [R 35] recommends the ISO/IEC 27001/ 27002 [R 97] [R 98] certifications for certifying the information security management systems of providers, respectively the SAS 70 Type II for providing a reference for auditors [R 130].

For a successful migration process, the employees should be prepared to deal with the cloud services. Thus, *organizational issues* are another challenge that businesses should face [R 86], Organizations will need to settle 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) [R 39]. Thus, 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 [R 184]. At the level of IT departments, only hardware and network support employees will be affected by job cuts [R 115] [R 203] Consequently, the technical role of support engineers is turning to reporting issues and the satisfaction of sales and marketing roles; the satisfaction of customer care depends on cloud-based services [R 117] [R 130].

5.1.1.3 Assets examination

This step is required to prepare the migration process to an IaaS service compatible with the current infrastructure of the enterprise [R 24] **[**R 202]; it supposes an examination of current infrastructure used by the organization, which is useful because enterprises should know what type of bit architecture (i.e. 32 or 64 bit) they have, their hardware infrastructure and their operating systems (OSs), where are deployed their application. The business applications should also be investigated in this step [R 130].

5.1.2 Decision making step

After the choose of the cloud delivery service type and the cloud deployment model, the 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 selection was made for: IaaS and the public cloud [R 130].

5.1.2.1 Choosing information

Based on the cooperation between the IT department and compliance department, enterprises should decide what information should be moved into cloud. They should 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 [R 35] [R 39] [R 130].

5.1.2.2 Define service requirements

The enterprise should define service requirements for IaaS, based on the current infrastructure, on the applications used by the company, and on the information that should be moved into cloud [R 202] [R 130].

5.1.2.3 Choosing CSP

For choosing CSP, we proposed to use the first two criteria of selection presented in the report: Enterprise Management Application Report, provided by [R 32]: cost efficiency and product strengths and instead of all vendor strengths elements (vision, strategy, financial strength, research development and market credibility of vendors), only the *market credibility feature* of the vendor to be evaluated.
Therefore, our suggestion is to apply our above-mentioned factors: cost efficiency, product strengths and market credibility, that will also be used for evaluating the CSP. (Figure 54) [R 130]:

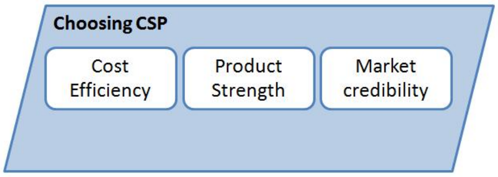


Figure 54 Choosing CSP [R 130]

1. *Cost efficiency* is a decisive factor for choosing the CSP. This factor has two elements: the *cost advantage* and the *deployment & administration*. In terms of *cost advantage*, the modelling tool (from www.shopforcloud.com) described by [R 117] 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). This modelling tool, a free web interface, can be used to deploy the specified requirements (already defined) and it produces a cost report based on selection of its computational resource usage patterns. It is helpful for comparing the pricing schemes around cloud providers. However, it calculates only the costs involved in the deployment of a system based infrastructure, where it can be added additional costs (e.g. 3rd party plugin to monitor costs – Cloudability.com, 3rd party platform to manage cloud resources – RightScale cloud Management). Furthermore, additional costs may also include license costs, training/consulting services costs, expenditure of time consuming for employees who migrate to cloud services etc [R 202]. However,

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) [R 130].

2. *Product strength* analysis provides information about the architecture and integration features, and about the functionality of CSP [R 130].
3. *Market credibility,* based on the analyse of the CSP reputation on the market, strengthens the enterprise's decision about choosing the CSP [R 130].

5.1.2.4 Choosing management tools

Cloud management is a hot subject approached by researchers in the cloud community, proved by the big number of third-party cloud management providers (i.e. RightScale, enStratus, IMOD Kaavo, CloudWatch, Scalr, Tapin, Cloudkick), who offer third-party cloud management tools, which are commercial versions, used in special by organizations that want to manage their cloud infrastructure. Enterprises should select one of these commercial versions [R 130]. For choosing the management tools, we proposed to use the first two criteria of selection presented in the report provided by [R 32]: cost efficiency and product strengths and instead of all vendor strengths elements only the *market credibility feature* of the vendor to be evaluated:

- The *cost efficiency* evaluation should include the following objectives: cost advantage and deployment & administration analysis. While the cost advantage is determined by the price, the licensing and maintenance costs of the management tool, the implementation and management analyses are made to demonstrate the ease of implementation (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) [R 130].
- The investigation of *product strengths* undertakes an analysis of the categories of architecture and integration, respectively an analysis of their functionality [R 130].
- The vendor's *market credibility* feature will review the reputation of the cloud market vendors in order to improve the decision after evaluating the cost effectiveness and product potential [R 130].

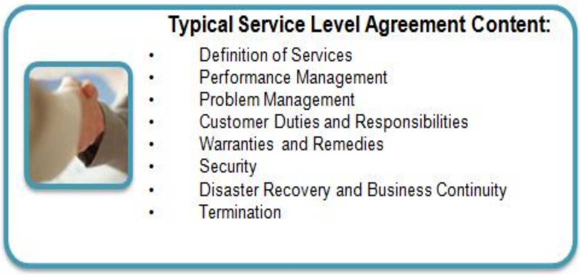
5.1.3 Migration step

Migration step is the effective moving stage of enterprise's assets into cloud services. This step includes 2 activities: developing the Service Level Agreement (SLA) and the Cloud Implementation [R 130].

5.1.3.1 Developing SLA

The Service Level Agreement (SLA) is a document that should be compulsory done between the cloud provider and the customer, to obtain and to maintain a clear aspect over the rights and the responsibilities of each party. It 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 [R 110] [R 130].

Figure 55 presents the content of a typical service level agreement proposed in [R 110].



Typical Service Level Agreement Content:

- Definition of Services
- Performance Management
- Problem Management
- Customer Duties and Responsibilities
- Warranties and Remedies
- Security
- Disaster Recovery and Business Continuity
- Termination

Figure 55 Typical Service Level Agreement CONTENT [R 130]

Definition of Services

Is the part of the SLA document, where the services are defined and described using detailed information, for creating a good understanding of exactly what is being delivered [R 130].

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 should be involved in monitoring the performance of the services. A well-done agreement is a guaranty of a reliable management [R 130].

Problem Management

Regards the methods for preventing and combating the incidents [R 110] [R 130].

The Customer Duties and Responsibilities

This part regards the obligations of the cloud's customers [R 130].

Warranties and Remedies

While the customers have responsibilities also the provider of cloud should have *warranties and remedies* [R 110]. In the SLA each party plays its role and have its own responsibility [R 130].

Security

SLA 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 [R 130].

Disaster Recovery and Business Continuity

Beside the security feature, both parties should include in the agreement document a disaster recovery and business continuity feature. If an unplanned disaster happens, 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 [R 110] [R 39] [R 130].

Termination

Is the final chapter of the SLA, and should have the following topics: termination at end of initial term; termination for convenience; termination for cause and payments on termination [R 110] [R 130].

5.1.3.2 Cloud Implementation

Consists in effectively realizing the effective migration of the enterprise's information to the cloud service. The system's deployment will be done 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 [R 130].

5.1.4 Management step

After migrating to cloud services, enterprises must manage the deployed cloud. It can be done by using two management functions: *business* and *operational*. The *Business management function*, also called administrative group by [R 47] guarantees business supports for: customer management, contract management, inventory management, accounting and billing, pricing and ratings, metering and SLA management [R 46] [R 91].
The *operational management function* or *resource management group* (in [R 47]), is handling the provisioning/configuration operations and portability/interoperability operations [R 91] [R 46] [R 130].
Other related works together with a comparative analyze related to our work, are detailed presented in [R 130].

This section may be used as a guide for improving the efficiency, quality and capacity management of enterprises to move their data and applications into cloud. Furthermore, a well-done migration process to cloud services decreases the enterprise's expenditure for decision making as regards transition into cloud.

The holistic migration process presented is only a qualitative research, which doesn't provide a case study for evaluating the described process. However, this will be part of our future work.

5.2 Management Interfaces for Eucalyptus Cloud

Cloud management, which is a fundamental support for all users of cloud services from the cloud marketplace, 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. RightScale, enStratus, IMOD Kaavo, CloudWatch, Scarl, Tapin, Cloudkick) [R 129].
In [R 129] is presented an overview of several management interfaces for Eucalyptus cloud by addressing the taxonomy and evaluation of the cloud management interfaces. The proposed taxonomy results from the work accomplished by experimenting the Eucalyptus community cloud.
The cloud management tools are described from two perspectives. The first perspective analyses the cloud portals from the user roles, while the second perspective addresses them with respect to the type of the tools employed [R 129].
On the other side, related with the Common Cloud Management Architecture (CCMA), one of the components of IBM Cloud Computing Reference Architecture [R 7], the first category of interfaces (i.e. the cloud portals from the user roles) encompasses the Service Consumer Portal, the Service Provider Portal and the Service Development Portal, while second category of interfaces includes the main components of CCMA: Operational Support Services (OSS) and Business Support Services (BSS) [R 129].
There are two types of cloud platforms: commercial and open-source.
Many providers deliver today cloud services for customers through commercial cloud platforms. These platforms (Amazon Web Services, Microsoft Azure, Google Apps, IBM etc.) corresponds to the cloud service provider, whose data centres run applications and store data [R 16] [R 129].

Related with the open-source platforms, in [R 30] [R 186] [R 156] were realized researches regarding the open source toolkits (i.e. Eucalyptus, Xen Cloud Platform, Open Nebula, Nimbus etc).

According with Tianfield (2011) the cloud architecture consists of Cloud Platform Architecture (CPA) and Cloud Application Architecture (CAA) [R 199]. The management process for these architecture starts with the operating systems, which manages the physical infrastructure; the management process is followed by the hypervisor, which has the job to dynamically provision and manage the virtual machines (VMs); it continues with Cloud APIs (Application Programming Interface), which include management and customer portals. At the CAA level, the granularity of cloud management is increased by cloud brokers, which work with the associated cloud ontologies and the Business Service Process (BSP) layer which performs Business Service Management (BSM), Service Level Agreement (SLA), service orchestrations and process management [R 199] [R 129].

5.2.1 Eucalyptus Community Cloud Interface Management

Eucalyptus is the acronym for *Elastic Utility Computing Architecture Linking Your Programs To Useful Systems*. It is an open-source cloud platform, developed by University of California for creating private and hybrid clouds and supported today by Eucalyptus Systems, a Canonical Partner; it also provides a commercial version, called *Eucalyptus Enterprise Edition* [R 61] [R 129].

According with administrator's guide provided by [R 62] the Eucalyptus architecture includes five components (Figure 56): *Cloud Controller* (CLC), *Walrus, Cluster Controller* (CC), *Storage Controller* (SC) and *Node Controller* (NC); these are detailed in [R 129].

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.

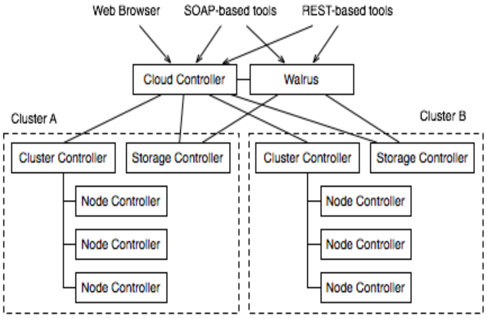


Figure 56 Eucalyptus Architecture [R 129]

Each *cluster* is formed by a collection of NCs sharing a LAN segment [R 62] and it has:

- A *Cluster Controller* is the element that collects information about VMs and deals with the VMs scheduling on particular NCs; CC must contain NCs which are in the same broadcast domain (Ethernet). Cluster Controller decides where to place the request received from the Cloud Controller, by evaluating which Node Controller has sufficient free resources [5].
- A *Storage Controller* (SC) – was developed to have the same capabilities as Amazon Elastic Block Storage (EBS) and to be able to communicate with others storage systems (NFS, iSCSI etc) [R 59].

Cloud Controller (CLC) treats the incoming requests and provides high level resource scheduling by collaborating with the Cluster Controllers [R 61].

Cloud Controller is the interface to the management platform, ability which is developed using the Amazon Elastic Cloud Computing (EC2) and a Web-based user interface.
Walrus module is used for storing data. It is situated at the same level in the architecture like Cloud Controller and has compatible interface with Amazon S3 [R 61].

5.2.2 Cloud Management Tools

5.2.2.1 Cloud User Interfaces

In terms of user roles the interface is the same for all 3 types of users (i.e. consumer, provider and developer), but with different rules, policies and constraints for each user role.
Because of the specific functionality of provider portal based on the user roles [R 49], the provider interface includes [R 129]:

1. The ***Service Development Portal -*** the interface used by cloud service developers to deploy new cloud services.
2. The ***Service Provider Portal*** - assures for its customers a service management of the following functionalities: operations, business and transition.
3. The ***Service Consumer Portal*** has the same management functions as the service provider portal with the difference that service consumer portal has involved different access rights with different capabilities: consumer service manager, consumer service administrator and service user [R 49].

The taxonomy of the management functions in the provider interface, was realized by extracting and analyzing each management service from the Cloud Service Management structure provided by NIST [R 90] and integrating them in the corresponding functions of the provider interface from [R 49] [R 129].

1. Business management functions (called administrative group in [R 48]) [R 129].

Guaranties the following business support:

- customer management contains the following sub-functions: subscription management, customer account management and entitlement management
- contract management
- inventory management contains the following sub-functions: service offering management, service request management and order management
- accounting and billing contains the following sub-functions: billing, clearing and settlement, accounts payable, accounts receivable
- pricing and rating contains the following sub-functions: pricing, billing and service offering catalog
- metering
- SLA management

2. Operational management function (called resource management group in [R 48]) [R 129].

Is related with the provisioning/configuration operations and portability/interoperability operations [R 90].

The provisioning/configuration operations include the following tasks:

- rapid provisioning
- monitoring and reporting
- reporting and auditing

According with [R 48] the portability/interoperability operations compose the transition management functions and it regards:

- resource change
- data portability
- service interoperability
- system portability

5.2.2.2 Eucalyptus Management Tools

This section regards Eucalyptus management tools for the consumer role. The service consumer portal has the following capabilities: consumer service manager, consumer service administrator and service user [R 49] [R 129].

Eucalyptus Management Tools are classified as:

1. Web based management: Eucalyptus Admin Interface
2. 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: RightScale, enStratus, IMOD Kaavo, CloudWatch, Scarl, Tapin, Cloudkick

1. Web based management

It is also called *administrator web interface* 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. It ensures the interaction with ECC IaaS cloud, by providing the provisioning operation, which should be accepted by administrator [R 129].

The management operations that are accessible by users are: user provisioning, catalog of available images [R 129].

The management operations that are accessible by administrators: Identity Management (adding users, user accounts Management), Configuration Management, Catalog of available images, Catalog of services [R 60] [R 129].

Note that ECC don't allow end-users the images management capability; ECC has its own catalog of images, created by administrator, and offered for use to the end-users [R 129].

The access of the users to the ECC administrative graphical interface is realized through the following URL: https://ecc.eucalyptus.com:8443 [R 129].

2. Client tools

The client tools presented covers the EC2 functionality of Eucalyptus cloud [R 129].

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 [R 186] [R 149]. The authentication procedure for users requires downloading the needed keys via a zip file [R 186]. The authentication solution are solution ES-security mechanisms (X.509 credentials) [R 61] [R 201].

euca2ools client software assures the user interaction with ECC. It provides the following management drivers: SSH key management, security group management, image management, instance management, storage management and IP address management. These management functionalities of Euca2ools are well documented, which helps the Eucalyptus users but it is slower compared with GUI clients, because it is a command line tool, which marks the lack of convenience functions [R 129].

a. API Client: Typica

Typica is a client Java library useful for Java developers who work with the Amazon web services. 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 17 covers the advantages and disadvantage of Typica [R 129].

a. Graphical User Interfaces (GUI)

Firefox Plugins are GUI and are built as an extension of Mozilla Firefox. First, appears the Elasticfox plugin, which had the advantages of managing the Amazon EC2 accounts and it is an easy to use interface. Hybridfox plugin 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.

Table 17 covers the advantages and disadvantages of this tool.

Command line tool	**Type**	**Strenghts**	**Limitations**
Euca2ools	Command line [R 186] [R 149] [R 61] [R 201]	• management drivers: SSH key management, security groups management, image management, instance management, storage management and IP address management • it is well documented	• lack of convenience functions
Typica	Client Java library [R 58] [R 77] [R 65]	• reliable client Java library for a variety of Amazon web services • convenient for Java developers	• poor documentation • access the Amazon's API at a low level
Elasticfox	GUI –Mozilla Firefox plugins [R 65] [R 78] [R 40]	• manages Amazon EC2 and Eucalyptus accounts • easy to work with it, no need to separate documentation	• it's not web based • restricted to EC2 environment • don't have the ability to copy files between instances
Hybridfox		• provides compatibility between Amazon and Eucalyptus clouds • supports more features of Eucalyptus than Elasticfox • -easy to work with it	• it's not web based
Cloud42	open-source management interface for every EC2 compatible services [R 58] [R 65] [R 107]	• 2 interfaces types: web-based GUI and web service interface • provides basic and extended functionality (file transfer functionalities from a EMI instance into another EMI instance, controlling EC2 server instances remotely)	• support for Elastic IP addresses is missing
tAWS Tanacasino	GUI management tool for Amazon EC2 [R 58]	• Eclipse GUI management tool for Amazon EC2 • easy to work with it • provides basic functionality	• it's not web based
EC2 Dream	desktop admin client [R 58]	• free desktop admin client • same functionalities like Amazon EC2	• poor documentation • it's not web based

Table 17 Euca2ools evaluation [R 129]

Cloud42 is an open-source management interface for every EC2 compatible services, which includes 2 types of interfaces: web-based GUI and web service interface. Table 17 covers the advantages and disadvantages of this tool.

tAWS Tanacasino is another GUI management tool for Amazon EC2 [R 58] should be installed and is similar with Firefox plugin Elasticfox. Table 17 covers the advantages and disadvantages of this tool.

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 17 covers the advantages and disadvantages of this tool.

b. Third party cloud management tools

This third-party cloud management tools are used by organization that want to manage their cloud infrastructure. These are commercial versions and provide free trials for several weeks (i.e. 1 or 2 weeks), except RightScale, which offer the opportunity to create free account for managing the Eucalyptus cloud.
The RightScale 3rd party management creates an optimized user experience by providing a Dashboard with the cloud resources pool, which are automated [R 175].

5.3 Security management in Cloud Computing

Virtualized physical resources, virtualized infrastructure (IaaS), as well as virtualized middleware platforms (PaaS) and business applications (SaaS) are provided and consumed as services in Cloud for businesses. It is important that all interfaces (both for customers and the cloud security providers) maintain the security [R 118].
A holistic illustration of the cloud surrounded by the devices and security features is given in Figure 57.
Managing security within the enterprise is one of the most important business issues that organizations need to address. Therefore, the biggest challenge in implementing successful the Cloud Computing technologies in an organization is managing the security. By focusing more on information security awareness, on privacy and by ensuring that appropriate policies and procedures are put in place, Cloud computing can become the most viable information technology solution [R 170].

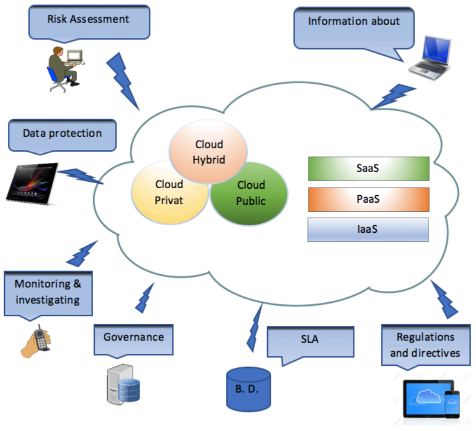


Figure 57 Cloud Computing Map [R 170]

Standards for the management of information security and collections of best practice measures were developed and established. Important standards for the development and operation of an Information Security Management System (ISMS) are the ISO 270xx [R 190].

Therefore, the Security management in Cloud Computing is related with data protection, compliance and audit, the business continuity and disaster recovery plans and the electronic investigations and protecting monitoring [R 135] [R 177].

5.3.1 Data Protection, Compliance and Audit

Personal data that is gathered, processed or used in the cloud, must have a guaranteed protection, in compliance with data protection laws.

The user transferring data to the cloud provider is an important feature of Cloud Computing.

In [R 66] is detailed a sensible aspect relating with the European General Data Protection Law. So, If the data is personal, "this transfer is a case of transmitting personal data or of processing personal data on behalf of others, which is not to be classified as transmission". The legal classification of the transfer is based on the legitimacy of the transfer in accordance with the data protection legislation and the contractual legal form. When cloud data is transferred to the cloud provider, the cloud user gives up all the legal responsibility to protect the data of the cloud provider. They also lose the option of exercising any influence on the manipulation of the data they have transmitted. It is important how the SLA is done, because at the level of civil law, that part of the liability can remain with the cloud user. Thus, the transmission requires a legal basis under data protection law.

The cloud service provider should also comply with the other legal requirements required by the cloud user. Compliance is therefore a critical element of information security in cloud. Cloud data must comply with local and international regulations. They must be able to undergo internal and external auditing for compliance checking. Controls should be provided to monitor and demonstrate their existence. [R 171]. Compliance with regulations and laws across different geographic regions may be a challenge for organizations. It is extremely important to ensure that the contract clearly stipulates the areas where the Cloud provider is responsible and accountable.

On the other hand, the policies imposed by regulations depend on the type of data stored.

Specific regulatory requirements are for storing sensitive information there are, like: Payment Card Industry Data Security Standard (PCI-DSS), HIPPA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley Act (SOX), Control Objectives for Information and Related Technologies (COBIT) [R 185].

There are also other regulations imposed by global regions.

Important to mention that there are also regulations from several member states of European Union (EU) are forbidden the migration of its citizen's data outside their borders. An important aspect that must be considered by cloud customers is to ask the cloud provider about specific jurisdictions of country where data is hosted, because the laws of the country require storing the data on a physical space inside of the country where the organization activates. Data must be kept at required specific laws. And, also related with this need of transparency related with data location, is the fact that the asset management should accomplish access to the virtual and physical assets (hardware, network, software) in case of audit and compliance. It is recommended to achieve compliance with the ISO 27001/27002 standards, which provides security management and controls within the cloud environment [R 190].

5.3.2 Business Continuity and Disaster Recovery Plans

Disaster recovery (DR) and business continuity refers to an organization's ability to recover from a disaster and/or unexpected event and resume operations, and it is also relevant for Cloud Computing,

Organizations often have a plan in place (usually referred to as a Disaster Recovery Plan or Business Continuity Plan) that outlines how a recovery will be accomplished. The key to successful disaster recovery is to have a plan (emergency plan, disaster recovery plan, continuity plan) well done before disaster appears.

Business Continuity Plan (BCP) is the process of creating systems of prevention and recovery to deal with potential threats to a company. A BCP outlines a range of disaster scenarios and the steps the business will take in any scenario to return to regular trade. The process that deals with the recovering procedures is called Disaster Recovering Planning (DRP). It is important to be implemented by Cloud Service Provider, as a guaranty of keeping the security infoemation for the customers. DRP specifies, in a documented written form, the procedures a company must follow in the event of a disaster. It is actually a statement that includes the consistent actions to be taken before, during and after a disaster [R 177]. Clients need to know the actions that CSP intends to implement in DRP as a guarantee of the specified measures.

5.3.3 Electronic investigations and protecting monitoring

It is related with Incident Response, Audit and Assessment. Is realized by placing the security between the cloud service and cloud user, to protect themselves against the security risk of trusting the monitoring systems deployed by cloud service providers.

Incident response in cloud environments requires a solid infrastructure management that should be connected with robust monitoring and alerting.

For organizations with internal clouds, they should have strong management capabilities and visibility into their systems. These will be realized using virtualization tools, that enable to run their infrastructures and setup their own monitoring. There are some virtualization tools that enable even the virtualization-specific log management, and intrusion detection, security event management, anti-malware and the use of quarantine capabilities (including Network Access Control, or NAC) [R 190].

In the case of public cloud, it is very important for customers to negotiate the service with public cloud providers, and specific service monitoring, alerting and response policies and trigger factors should be included in service contracts.

The service contract must also indicate when the service provider has to alert the client, on the basis of which events and what specific details / events has to be provided to the clients for the investigations.

This cloud-based operating policy will be like the already implemented internal policy; In addition, policies will need to take account of localization and mobility associated with cloud applications.[R 190].

5.4 A Cloud Service Management System Approach for Innovative Clusters

Given the advantages of cloud which allows the delivery of scalable resources on demand, we propose in [R 167] a Cloud Service Management System (CSMS) that provides IT services for the innovative clusters companies that can be customized for both enterprises with the associated clusters. In this sense, CSMS will be built within a private cloud with multiple clusters.

We are focused to deliver broad range of cloud services as the ones described by

David Linthicum in [R 122] due to their spread across industry. These are: Storage-as-a-service, Database-as-a-service, Information-as-a-service, Process-as-a-service, Application-as-a-service, Platform-as-a-service, Integration-as-a-service, Security-as-a-service, Management / Governance-as-a-service, Testing-as-a-service, Infrastructure-as-a-service. These services can be rent by customers depending on their needs and used as computing utilities. The advantage is the decrease of the initial investment and that billing changes accordingly with the computing requirements for an individual or an organization changes, without incurring any additional cost. Within such a system, actors begin to depend one on another and to take advantage of the local knowledge base, if this interdependence causes a continuous flow of product and process innovations, diffusion of knowledge and collective learning processes at local or regional level, public-private partnerships being the synergistic factors that lead to these innovative clusters [R 167].

From the security perspective of the proposed Cloud Service Management System, that besides the stages of a Service Level agreement (SLA) content [R 122] [R 130], our services provided within each cluster of the CSMS must enhance availability, confidentiality, data integrity, control and audit.

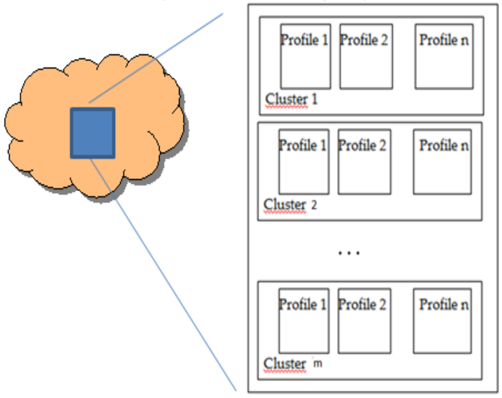
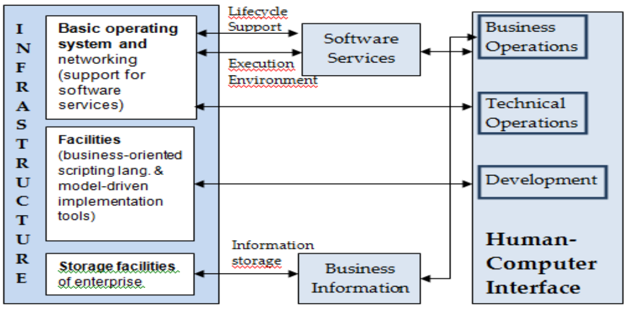


Figure 58 The CSMS [R 167]



INFRASTRUCTURE
Basic operating system and networking (support for software services)
Facilities (business-oriented scripting lang. & model-driven implementation tools)
Storage facilities of enterprise
Lifecycle Support
Execution Environment
Software Services
Information storage
Business Information
Business Operations
Technical Operations
Development
Human-Computer Interface

Figure 59 The Infrastructure [R 167]

Each cluster is designed to have a different profile (e.g. IT, tourism, health services, green energy etc.) which will integrate all the companies mapped with it, with the objective of keeping the profile of each company (Figure 58). The idea is that the existing companies, should migrate their services into the related cluster for integration within the CSMS. Thus, the CSMS will bring together all the involved services provided by the enterprise applications (Online shopping, billing and payment processing, Interactive product catalogue, Content management, Customer relationship management, Manufacturing and other business processes integration, IT services management, Enterprise resource management, Human resource management, Business intelligence management, Business collaboration and security, Form automation).

Moreover, to make the cloud computing approach to work as an efficient Cloud Service Management for the innovative clusters, and to deliver the business agility and IT flexibility promised by Web Services, it is required the creation of a Service Oriented Environment (SOE) [R 158]. Our approach is to deliver value to customers through the services provided using the SOE without implying any additional cost and risk from the customer perspective [R 167].

The CSMS services need to deliver to customers: simplicity, flexibility, reusability and independence from technology. Services may be published, discovered and used in a technology-neutral, web-based service protocols. Thus, through a common interface, separate business services are created and managed within each cluster to achieve the objectives of each company that has its own assets, employees, suppliers, partners (and information about them) or existing IT infrastructure [R 122] [R 55].

The huge increase in IT interoperability that SOA can bring not only at enterprise level but also at the level of the innovative cluster is based on the use of smaller modular services that have also interface descriptions and contracts that ensure business agility.

These services are identified, defined and described in the context of cluster business activities and are performed by the IT computing infrastructure and managed at CSMS level. For each service, it is clearly established what it does, and is stipulated in a contract [R 167].

The development of efficient and flexible solutions is ensured using SOA techniques such as service composition, discovery, message-based communication, and model-based implementation [R 158]. SOA represents not only the architecture of services, but also the policies, practices and frameworks, by which we ensure the appropriate services provided and consumed for the entire innovative cluster, in order to ensure the best business result [R 122]. The software services used by innovative cloud business operations are supported by a Cloud infrastructure that, along with IT services, improves the flow of information across companies and between companies in the innovative cluster, and all of them end the outside. The access to these services frequently involves a human-computer interface, often implemented as a web interface using portals, (Figure 59) [R 167].

Thus, our proposed CSMS approach considers and meet different quality of services (QoS) parameters of each individual enterprise and service which will be included in specific Service Level Agreements (SLAs), after the negotiation between the cloud service provider and the customers (companies). Realizing that technological progress is the heart of regional development and decision-makers could support the development of technology clusters towards transforming them into regional innovative clusters, the application of our proposal aims to overcome existing bottlenecks in terms of business strategies and regional development policies in a region of Romania (in particular the North-West) [R 167], in order to stimulate and optimize the organization and management of innovative clusters from value chain perspective and guide their planning activities towards a differentiation strategy in which cluster members cooperate with high value added niches (smart diversified specialization) and, consequently, to create regional growth and development. To achieve the ideal agile business collaborating environments the IT infrastructure needed to access the functionality of the service should be configured by the user without the need to become expert in the field. A well-suited solution could be the Cloud Computing Open Architecture (CCOA), proposed in [R 204] [R 167].

Therefore, our CSMS solution for the management of services of the innovative cluster is developed based on the Cloud Computing Open Architecture, which we should customize to ensure the services needed to migrate the companies' services into the related cluster for integration within the CSMS.

Thus, at the second level of the CCOA model [R 204], we propose to develop the innovative clusters using an HPC infrastructure. Level 3, structured as SOA, will be used to define the profiles and the services for each company included in each cluster. Level 4 will be specific to each cluster, namely profile. Level 5 provides the granular services, while level 6 will have custom profile services for each cluster (Figure 60) [R 167].

In this context, the classic concept of a network of companies, which designates a form of cooperation between legally independent companies geographically dispersed but with common interests in economic terms has evolved to the concept of collaborative networks of innovative technological systems which refers to coordinated cooperation (in terms of the configuration network) between different organizations pursuing a common goal: the development of a region; the concept of cluster technology has evolved in the innovative cluster, facilitated by the information technology facility to transform into a cumulative process and ”institutional density” cooperation and technological knowledge flow, leading to the accumulation of ”strong local base of knowledge” and the creation of a system like the “innovative milieu” [R 114] [R 63] [R 84] [R 64].

Within such a system, SMEs will depend on one another and take advantage of the local knowledge base and causes a continuous flow of product and process innovations, diffusion of knowledge and collective learning processes at local or regional level; public-private partnerships being the synergistic factors that lead to “innovative milieux”, toward learning regions [R 143], creative regions, knowledge based regions etc. [R 13] [R 3].

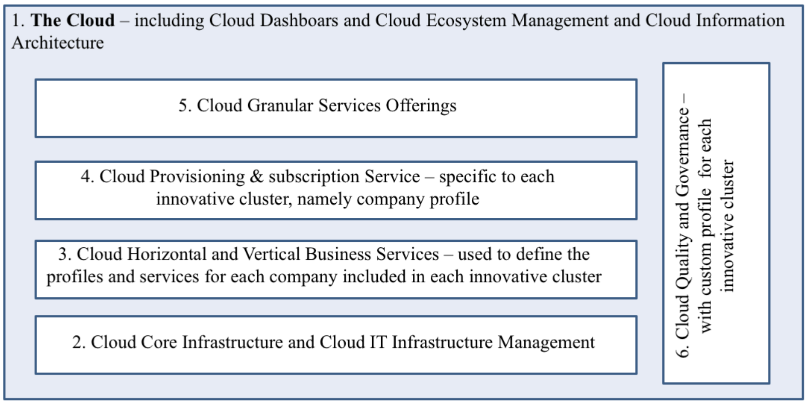

1. **The Cloud** – including Cloud Dashboars and Cloud Ecosystem Management and Cloud Information Architecture
5. Cloud Granular Services Offerings
4. Cloud Provisioning & subscription Service – specific to each innovative cluster, namely company profile
3. Cloud Horizontal and Vertical Business Services – used to define the profiles and services for each company included in each innovative cluster
2. Cloud Core Infrastructure and Cloud IT Infrastructure Management
6. Cloud Quality and Governance – with custom profile for each innovative cluster

Figure 60 The CSMC model [R 167].

Therefore, the proposed CSMC model aims to represent an important support for the development of existing clusters and to find solutions for the functionality and sustainability of new clusters in the North-West region for valuing high regional clustering potential. In this respect, can be identified a broad range of cloud services that can be rent by firms from same industry, aligning cluster members on value chain. Also, several services can be adapted to the cluster specificity, like: project planning, marketing planning, strategy, business plan, KPI’s system etc. Within such a system, actors begin to depend one on another and to take advantage of the local knowledge base, if this interdependence causes a continuous flow of product and process innovations, diffusion of knowledge and collective learning processes at local or regional level, public-private partnerships being the synergistic factors that lead to innovative clusters.

Part II. Professional and academic achievements. Evolution and career development plans

6 Professional and academic achievements. Evolution and career development plans

Beginning with 1985 I worked as a research engineer at Institute for Design in Automation, Bucharest, and then, after 1990 I worked at University of Oradea. In 1998

I have submitted my PhD these and I got the title of Doctor in Computer Science field.

Today I am a professor in the Department of Computer Science and Information Technologies and I coordinate Integrated IT Service Management at the University of Oradea. My areas of competence are: computer architecture, cloud computing, artificial intelligence, testing digital circuits, computing network security and information management.

In this chapter are synthesized the main professional and academic achievements after obtaining the PhD degree in Computer Science, in 1998.

6.1 Professional and academic achievements

After obtaining (in 1998) the PhD degree, in 1999 I was promoted as an associate professor and in 2003 I was awarded a professorship position, which I am currently occupying at the Department of Computers and Information Technology, from the Faculty of Electrical Engineering and Information Technology at the University of Oradea.

From 2000 to 2012 I was Head of the Computer Science Department of the Faculty of Electrical Engineering and Information Technology at the University of Oradea and since 2012 I am the Coordinator of the Integrated IT Management Center at the University of Oradea (I was ITIL certified in 2012).

At the beginning of my teaching career in higher education, in 1990, both my didactic and research activities focused mainly on the field of reliability and computer architectures.

The title of my PhD thesis was "Contributions to Computer Assisted Testing and Testable Synthesis of Computers with Increased Reliability", and the Scientific Coordinator was Prof. Dr. Mircea Vlăduţiu, from the Department of Computer Science from the "Politehnica" University of Timisoara.

Didactic field

After obtaining the doctorate title, my preoccupations in the field of computing architectures and reliability continued. My didactic activity in the following period was materialized by teaching courses and laboratory classes for Computer Systems Architecture, Digital Electronics and Digital Systems Testing with 2nd and 3rd year students from the Computer and Information Technology study programs. Considering the dynamics of computers' field, over time, I have taught and coordinated teaching activities for the courses of: Artificial Intelligence and Cloud Computing (for bachelor programs).

In my work, both before and after obtaining the PhD, I was concerned with improving my teaching skills with the aim of practicing student-centered education. To that end, I have created the resources necessary for teaching and learning in my disciplines. I have updated these resources constantly and made them available to students in electronic form through the means available at the University of Oradea (the Office 365 Platform).

Many of my research achievements have resulted in topics presented in the courses taught and in the practical activities related to them.

Also in this field, I contributed as head of department, together with the staff of the department (mostly graduates of the "Politehnica" University of Timisoara) and with the support of our professors from Computer Science Department of Timisoara, to the introduction at the University of Oradea of the in-depth studies program: "Security of Computing Systems". Since 2004 I have contributed to the introduction of the master study program "Management in Information Technology", which is currently in operation at the Faculty of Electrical Engineering and Information Technology in Oradea. At this program, I am the holder of the "Data Security Management" course.

On the other hand, in the field of Bachelor's degree programs, I have contributed to the launch of the "Information Technology" study program, which is still in operation. At present I am responsible for the study program "Management in Information Technology" at the Faculty of Electrical Engineering and Information Technology in Oradea.

In order to improve the teaching and research infrastructure, from the projects earned as a director or in which I was a member, I acquired specialized equipment, and software for the laboratory: “Computer Systems Architecture” of the Department of Computers and Information Technology.

I coordinated more than 20 dissertation papers and more than 40 diploma projects for undergraduate or master students at the Faculty of Electrical Engineering and Information Technology in Oradea.

Scientific field

In the scientific field, my work in the last 18 years after obtaining the PhD degree can be summarized as follows:

- Author or co-author of 26 articles indexed in ISI - Web of Science database, of which 11 in quoted magazines with impact factor;
- Author or co-author of 15 articles indexed in international databases;
- Co-author of 2 book chapters at international publishing house;
- Author or co-author of 8 books at a publishing house recognized by CNCSIS;
- Internships in the frame of Tempus Programs (other than Erasmus) at 2 research laboratories:
    - The Quality Research Laboratory from Paisley University (UK)
    - TIMA laboratory of the CNRS, Grenoble-INP and UGA (France)
- I had an international research grant, I was a director of 3 national research contracts (one in progress), and member in several international and national research projects;
- I was organizer of an international Scopus Conference (SOFA 2007) and a series of national / international annual conferences organized by our Computers and Information Technology Department in the period 2000-2012
- reviewer la 6 ISI journals, 5 journals indexed in internationally recognized databases in the field and numerous other non-indexed journals and conferences
- Journals indexed into internationally recognized databases and many other non-indexed journals and conferences (over 50 reviews);
- member SRAIT and IEEE;

Academic field

In the academic field, in the last 17 years I have been constantly involved in academic management at various levels. So:

- Between 2000-2012 I was Head of Department of Computer Science and Information Technology
- since 2012 I am the Coordinator of the Integrated IT Management Center at the

University of Oradea

- For the entire period, I was part of the Council Department of Computer and Information Technology;
- Between 1994-2016 I was part of the Council of Faculty of Electrical Engineering and Information Technology;
- Between 2004-2012 I was part of the Senate of the University of Oradea;

For the last 18 years, I have been involved in various expertise at both local, national and international level. So:

- I was an auditor of study programs and curricula at the University of Oradea;
- Member of the Quality Commission of the Faculty of Electrical Engineering and Information Technology of Oradea;
- Member of over 20 commissions for teaching positions at the University of Oradea, and other universities;
- Expert of the Romanian Agency for Quality Assurance in Higher Education (ARACIS) – 2015;
- Expert of the Scientific Research Council in Higher Education (CNCSIS) (2004-2005) Where I evaluated several projects
- Expert of the European Commission's European Research Agency (ERA), with 10 projects evaluated, including the HORIZON'2020 program, starting with the H2020-SESAR-2016 call

6.2 Career development and development plan

During my career development, I considered that the three main components, professional, didactic and scientific components, each with its specific characteristics, are interdependent and mutually supportive. I have always tried to integrate the evolution of the three personal components into the evolution of the collective, the institution and the system they are part of, with common benefits for all parties involved. That is why I have been actively involved in the life of the academic community where I am a member of (my achievements being a proof).

I intend that after obtaining the right to conduct doctoral studies I will remain active in academic life and move on to another level of sharing knowledge at doctoral level and training of independent researchers capable of carrying out a scientific activity - Individually, and integrated into collectives at local, national or international level.

During my professional career, I had models from which to learn; a special mention for Professor Mircea Vlăduţiu, from the Polytechnic University of Timisoara, as well as the whole team of teachers from the "School of Computers " from Timisoara.

At this moment, I consider that my experience and the modern means of learning and transmitting information will help to train my future PhD students in their completion in the academic and research fields. This will be accompanied by continuous personal training and openness to new themes and research tools that will surely appear in the coming years.

I have identified the following objectives, for which I will describe ways to put them into practice:

- In the didactic field:
    - proposing a master university education program: Information Security Management
    - developing and updating the disciplines I am or will be holder of;

    - the internationalization of didactic activity;
    - diversification of didactic activity;
- In the scientific field:
    - increasing the visibility of research activity;
    - diversification of research topics and extension of interdisciplinary applications in other fields;
    - diversification of current collaborations and initiation of collaboration with us and centers and institutions research in the country and abroad;
- traversal objectives:
    - inclusion of research results in didactic activity;
    - active involvement of students in research activity
- In the academic / professional field:
    - developing more concrete collaborations with companies in the field
    - developing more concrete collaborations with other higher education and research institutions in the country and abroad;
    - Continue to work in the advisory, decision-making and expertise structures, in which I am involved, and, if necessary, to take on new responsibilities.

Objectives for the Didactic field

In the didactic field, a main objective I propose is to initiate a Masters in *Information Security Management*. I intend to do this, because the Increasing growth of diffuse data and IT systems pose serious security challenges which can only be addressed by a holistic approach to security management protocols. Also, applications in the area of social networks or cloud computing and new technologies need to be increasingly taken into account when planning and implementing information and communications systems. In this sense, I should develop and update the disciplines I am or will be the holder of.

I should also introduce my teaching activity in an advanced degree program, specific to doctoral studies; this program will be one in the field of Information Security Management field.

In this sense, I intend to identify the practical needs and applications demanded by companies and institutions in our region in their day-to-day work and to design the program such that it will allow the training of specialists / researchers who can not only respond to and solve their needs and applications, but also come up with innovative solutions to put them into practice and thus to contribute to the advancement of the society in which they will operate.

The internationalizing of teaching activities by diversifying international mobility will be another important objective I for me. For this purpose, I intend to use the existing collaborations, and to develop future collaborations with laboratories in which I have been, or with whom my colleagues, from my department work, and even to try to identify the possibilities for the realization of some PhD theses in collaboration ("cotutela").

Such collaborations lead also to bilateral motilities for teachers. By including colleges from foreign universities in our local doctoral or master programs will bring added value and diversification, that are beneficial to students. For the PhD students, I will also consider the diversification of my teaching activity by organizing workshops and summer schools.

Objectives for the scientific field

In the scientific field, one of my main objectives will be to increase the visibility of research activity.

This is necessary because the classification of the research fields depends on the activity of the researchers in each field, and the visibility of the research has an increasing share.

In this context, I will consider the capitalization and dissemination of research results in a larger proportion, in journals from the main stream of publications (in the yellow area and the red area in the field) and in interdisciplinary journals, which are accessed by researchers from several research fields.

Also, in my doctoral work, I will initiate and encourage them to publish in this manner: after two papers at the conferences, they will make a synthesis to subscribe to a journal in the research field.

The publication of research results in interdisciplinary journals is favored by the multitude of possible IT applications, and I will consider the diversification of research topics and the extension of interdisciplinary applications in other fields as well.

This diversification will be achieved both by exploiting the diversity in my experience gained over time, as well as by identifying new applications requiring efficient and secure information management, data and information security, respectively optimizations for various objectives in which I can carry out research activity together with the PhD students. In addition, I will consider also the initiation of new research areas, which I have not approached yet, or which I have approached very little to date.

Over the past 18 years, my research concerns have evolved and tracked the dynamics of the field.

In the first period, I was concerned about issues of reliability, testability, especially in the field of computer architectures, after which my concerns were focused on physical security. The latter were directly related to my company (ACTUAL SRL) focused on design, execution and consultancy in the field of physical security, which I was forced to lead in 2006-2010.

With the emergence of the cloud computing paradigm, my concerns have been addressed in this area. The globalization of IT infrastructures has raised a new issue, which has become of great importance: it is the issue of information security and, in particular, the confidentiality of data. There is also a European regulation that must be implemented in Romania by May 2018 (GDPR). In view of these issues, a great effort of current research in the field of computing engineering is being phased in this direction. The maturity of cloud computing is shaping up and, with the development of new IoT technologies, new ideas for new computing paradigms such as p2p cloud storage, etc. are starting to populate.

Some of the research domains that I have addressed in recent years, together with my research intentions for the future, are enumerated below:

- Interfacing of the UniWeb Information System with the Unique Matricol Register portal (research carried out with FDI financing 2016). Since the two informatics systems are based on different classification tables, it was necessary to create a mechanism that would allow the integration of the local data management system for students enrolled at the University of Oradea - UniWeb, with the “Matricol Unic Register” system -RMU.

- Maintaining data security for the UNIWEB system and the data management in order to update the information on the “Matricol Unic Register” Portal (ongoing research with FDI funding 2016, project manager); We are in the stage of setting architectural solution
- Research on the high-speed interconnection of IT infrastructures of two university campuses (cross-border: University of Oradea with University of Debreten), carried out within a cross-border project in which I participated and the results materialized by implementating of the IT / voice IT infrastructure of our university
- Cloud computing research - carried out in collaboration with colleagues from my department and other departments and which have been materialized in published scientific papers, in course support (a book) and practical applications for students (on support media). Starting from this research we intend to advance a financing request for the development of a private cloud solution at the level of the regional development center that will allow the integration of the regional innovation clusters
- Smart Campus research - done in collaboration with colleagues from other faculties, and that have materialized in the establishment of development strategies, development projects at the university level and the publishing of scientific articles. In this field, future research is intended - I intend to address this field related with the new IoT technologies, which are in trend.
- researches in the field of optimizations based on the use of artificial intelligence techniques - realized within research projects within our geothermal research center, materialized by publishing of scientific articles.

Among the new areas of research that I have started to address lately, and I want to continue, I mention:

- Research in the steganography field, based on the use of images as a support for hiding information - done in collaboration with colleagues from other foreign universities, materialized in scientific publications in the field. I intend to continue the research in this field and to broaden it by identifying some elements for connecting the results of this research with the designing of new architectures, with increased information safety and confidentiality, for the new computing paradigms. I have already published 3 scientific papers in this field;
- Research in the artificial intelligence field and image processing field. In this sense, I have already realized a scientific paper that is in publishing process. It is an emerging field with high impact on the IT dynamic development of the last period;
- Research on the realization of a smart campus at the University of Oradea. In this sense, we intend to involve the Integrated IT Management Center of our University. We want to look for smart campus solutions that we should to implement and integrate into our IT structure. In this respect, we have already done researches for the identification of solutions for smart waste management in the university campus, as well as researches for energy efficiency improvement. Our results have materialized for the time being in the scientific papers that have been published or are to be published. I have already published 2 papers in this field;
- I also intend to develop a Laboratory for SMART Information Security Operations (SMART - OASI). Such a laboratory will deploy in fact an Information Security Operations Center (ISOC), a dedicated site where the organization's IT systems (websites, applications, databases, data centers and servers, Networks, desktops, and other objects) are monitored, evaluated, and defended.

Another objective in the scientific field is the diversification of the current collaborations and the initiation of collaboration with new centers and research institutions from the country and abroad. In this respect, following the collaboration and expertise activities carried out in recent years in various university centers in the country and abroad, I have started collaborations with colleagues from these centers, which can be put into practice more effectively, as a result of obtaining the ability to Conducts doctoral work.

The collaborations that I have maintained over time with universities / laboratories from France, UK, Spain, and Portugal, will be intensified as I will be able to extend these collaborations also in the field of PhD thesis. The closest collaborations I have are with: the TIMA - INP Grenoble Lab, University of Valencia - Alcoi Campus, University of Debrecen. In recent years, the elaboration of the theses in cotutela was one of the topics debated with collaborators from abroad, and obtaining the right to conduct doctoral work will be the necessary means to achieve this goal.

Transversal Objectives

Considering the diversification of my didactic and scientific activity, as a result of my habilitation to lead doctoral studies, I also propose several transversal objectives, combining the achievements of the didactic with the scientific ones.

One of my main concerns in recent years is the inclusion of research results in didactic activity, along with the active involvement of students in the research activity.

This is what I have practiced so far; I involved students in research activities and encouraged them to publish their work at the student scientific sessions organized by the Faculty of Electrical Engineering and Information Technology in Oradea. After obtaining the habilitation to conduct doctoral work, the achievement of these last two objectives will be facilitated by the way in which the didactic activity with doctoral students is achieved within their advanced university training program. I will also encourage and assist PhD students to get involved in teaching to share their research results and doctoral experience with undergraduate and master students.

I will support the pyramid activity: each doctoral student will collaborate and integrate the activity of some master students that I will have at the dissertation, and each master will coordinate and integrate the activity of some students I will have on the bachelor's project. By integrating their research work, the teaching materials will be improved; the teaching material will also contain research results, that permit a good understanding and the transmission of information to students, contributing to the attractiveness of the disciplines and subjects presented.

Objectives for the academic / professional field

In the academic / professional field, I intend to develop more concrete collaborations with other companies in the field, as well as with other higher education and research institutions in the country and abroad.

The diversification of the collaboration with the companies in the field will be corroborated with the diversification of the current collaborations and the initiation of the collaboration with new research centers and institutions from the country and abroad.

On the other hand, even at the university level I have collaborated with the students of the Computer and Information Technology study programs in the Integrated IT Management Center of University of Oradea, who volunteered to implement the Office 365 platform for all the users from our university. Along with them, I enroll students on the platform at the beginning of each academic year. I intend to maintain this collaboration, and even to develop it, because with the great diversity of technologies which are involved in building the infrastructure of the University of Oradea, it is very useful to students and can be used for the development of research in the field.

Another important academic / professional objective will be to continue working in the advisory, decision-making and expertise structures that I am involved in, and taking on new responsibilities when appropriate.

At national level, I will continue to work as an evaluation expert within the Romanian Agency for Quality Assurance in Higher Education (ARACIS), depending on how I will be required to evaluate some study programs in the field or in institutional evaluations. I will also get involved in the assessment of national projects through the (https://www.brainmap.ro/) of the Higher Education, Research, Development and Innovation Funding Unit (UEFSCDI).

At international level, I intend to continue to be involved in the evaluation of research projects within the European Research Agency (ERA).

Some of the above-mentioned objectives and the means described for their achievement are possible at present too, but I believe that obtaining my habilitation to conduct PhD works will be a means to facilitate the faster realization of these objectives and to contribute to achieving a functional research structure. In addition, my habilitation will also give me the chance to share knowledge and to form students and research at doctoral level

PART III BIBLIOGRAPHY

7 BIBLIOGRAPHY

7.1 References

[R 1] Andrei, T., 2009. “Cloud Computing Challenges and Related Security Issuess. A Survey Paper” [online] Available at: <http://www1.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html> [Accessed 21 May 2011], 2009.

[R 2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H, Konwinski, A., Lee, G., Petterson, D.A., Rabkin, A., Stoica, I. and Zaharia, M., 2009. “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.

[R 3] Armstrong, H. & Taylor, J. 2000. Regional Economics and Policy. Third Edition. Oxford: Blackwell: 298;

[R 4] Bajaj R., Bedi P., Pal S. K., Best hiding capacity scheme for variable length messages using particle swarm optimization, Proceedings of SEMCCO, LNCS., 2010, 6466, 237–244.

[R 5] Baker, A. R., Esler, J.: Snort Intrusion Detection and Prevention Toolkit. Syngress Publishing, Inc. (2007)

[R 6] Balakrishnan, H., Kaashoek, M., Karger, D., Morris, S., Stoica I. Looking up data in P2P systems. Communications of the ACM, 2003.

[R 7] Behrendt M., et al. “IBM Cloud Computing Reference Architecture v2.0”. IBM, 2011

[R 8] Bertino, E., Martino, L.D., Paci, E. and Squicciarini, A.C. , 2010. Security for Web Services and Service-Oriented Architecture. Berlin Heidelberg: Springer, ISBN 978-3-540-87741-7.

[R 9] Buecker, A., Ashley, P. and Readshaw, N., 2008. Federated Identity and Trust Management. International Bussiness Machines (IBM), Redpaper.

[R 10] Buyya, R.; C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009. View at Publisher · View at Google Scholar · View at Scopus

[R 11] C K Chan and L M Cheng, “Hiding data in images by simple LSB substitution”, Pattern Recognition Letters, vol.37, pp. 469-474, 2004.

[R 12] CA Software, 2007. “CA SOA Security Manager: Securing SOA / Web Services Based IT Architectures.” [online] CA. Available at: http://www.ca.com/files/technologybriefs/34499-ca-soa-sm-tech-brf_162833.pdf [Accessed 17 February 2011].

[R 13] Capello, R. & Nijkamp, P. (eds.) 2009. Handbook of Regional Growth and Development Theories. Edward Elgar Publishing: 6; Oxford University Press: 62;

[R 14] Chang C C et al., “Reversible hiding in DCT-based compressed images”, Information Sciences, vol. 177, pp. 2768-2786, 2007.

[R 15] Chang, C C et al., “A high payload frequency-based reversible image hiding method”, Information Sciences, vol. 180, pp. 2286–2298, 2010.

[R 16] Chappell, D., “The benefits and risks of Cloud Platforms”. [online] Microsoft Corporation. Available on http://www.davidchappell.com/writing/white_papers/Cloud_Platforms_for_Business_Leaders,_v1.0--Chappell.pdf, [Accessed on 27 February 2011], 2011

[R 17] Chatterjee, Trijit; Mrinal Kanti Sarkar, Dr. V S Dhaka, Steganographic Approach to Ensure Data Storage Security in Cloud Computing Using Huffman Coding (SAHC), JCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015 ISSN (Online): 2277-5420 www.IJCSN.org, [R 18] Chatzigiannakis, V., et al., 2007. Data fusion algorithms for network anomaly detection: classification and evaluation. Proceedings of the Third International Conference on Networking and Services (ICNS'07)

[R 19] Chen, Q. and Aickelin, U., 2006. Dempster-Shafer for Anomaly Detection. In Proceedings of the International Conference on Data Mining (DMIN 2006), Las Vegas, USA, pp. 232-238.

[R 20] Chen, Q. and Aickelin, U., 2006. Dempster-Shafer for Anomaly Detection. In Proceedings of the International Conference on Data Mining (DMIN 2006), Las Vegas, USA, pp. 232-238.

[R 21 Chen, X., Wills, G.B., Gilbert, L. and Bacigalupo, D., 2010 "Using Cloud for Research: A Technical Review," [online] JISC. Available at: http://tecires.ecs.soton.ac.uk/docs/TeciRes_Technical_Report.pdf [Accessed 10 November 2010]

[R 22] Chervenak, A., A framework for constructing scalable replica location services. Proceeding of the IEEE Supercomputing, 2002.

[R 23] Cisco and VMware, 2009 "DMZ Virtualization Using VMware vSphere 4 and the Cisco Nexus 1000V Virtual Switch" [online]. Available at: http://www.vmware.com/files/pdf/dmz-vsphere-nexus-wp.pdf [Accessed 20 October 2010].

[R 24] Cisco Systems, Inc. (2010)."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.

[R 25] Cloud Computing Use Case Discussion Group, 2010. "Cloud Computing Use Cases White Paper Version 4.0." [online] Cloud Computing Use Case Discussion Group. Available at: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf [Accessed 6 November 2010].

[R 26] Cloud Vulnerabilities Working Group Cloud Computing Vulnerability Incidents: A Statistical Overview, August 23, 2012; Revised March 13, 2013, https://www.cert.uy/wps/wcm/connect/certuy/abfd80ca-3142-4d28-b99c-e8f841568dde/Cloud_Computing_Vulnerability_Incidents.pdf?MOD=AJPERES

[R 27] Coello, C., An Empirical Study of Evolutionary Techniques for Multiobjective Optimisation in Engineering Design, PhD thesis, Department of Computer Science, Tulane University, New Orleans, LA, 1996

[R 28] Colomo-Palacios, R.; E. Fernandes, M. Sabbagh, and A. de Amescua Seco, "Human and intellectual capital management in the cloud: software vendor perspective," The Journal of Universal Computer Science, vol. 18, no. 11, pp. 1544–1557, 2012. View at Google Scholar

[R 29] Confident Technologies, Inc., 2011. Confident ImageShieldTM. [online] Available at: http://www.confidenttechnologies.com/products/confident-imageshield [Accessed 30 June 2011].

[R 30 Cordeiro, T. et al. Open Source Cloud Computing Platforms. Ninth International Conference on Grid and Cloud Computing, pp. 366-371, 2010

[R 31] CPNI, 2010. "Information Security Briefing Cloud Computing." [online] Centre for the Protection of National Infrastructure. Available at: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf [Accessed 2 October 2010].

[R 32] Craig, J. (2012). "Ema Radartm For Application Performance Management (Apm) For Cloud Services: Q1 2012". Enterprise Management Associates (Ema).

[R 33] Criscuolo, P.J.: 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, https://e-reports-ext.llnl.gov/pdf/237595.pdf (2000)

[R 34] CSA - CLOUD SECURITY ALLIANCE SecaaS Implementation Guidance, Category 8: Encryption [online] Cloud Security Alliance, 2012b, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf

[R 35] CSA, 2009. "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1." [online] Cloud Security Alliance. Available at: <https://www.cloudsecurityalliance.org/csaguide.pdf> [Accessed 14 October 2010].

[R 36] CSA, 2010. "Top Threats to Cloud Computing V1.0." [online] Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, [Accessed 27 July 2011].

[R 37] CSA, 2010b. "Domain 12: Guidance for Identity & Access Management V2.1." [online] Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide-dom12-v2.10.pdf [Accessed 3 November 2010].

[R 38] CSA, Security as a Service [online]. Cloud Security Alliance, https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf

[R 39] CSCC, (2011). "Practical Guide To Cloud Computing Version 1.2", [Online], Cloud Standards Customer Council, Http://Www.Isaca.Org/Groups/Professionalenglish/Cloudcomputing/Groupdocuments/Cscc_Pg2ccv1_2.Pdf

[R 40] CSS Corp Labs, 2009. Hybridfox: Cross of Elasticsfox and Imagination. [online] Available on http://cssinnovations.blogspot.com/2009/11/hybridfox-cross-of-elasticsfox-and.html, Accessed on 12 February 2011

[R 41] D C Wu and W H Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, vol.24, pp. 1613–1626, 2003.

[R 42] Dhage, S. N., et al., 2011. 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.

[R 43] Discretix Technologies Ltd., n.d. "Introduction to Side Channel Attacks." [online]. Available at: <http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf> [Accessed 25 October 2010].

[R 44] Dissanayake, A., 2008. Intrusion Detection Using the Dempster-Shafer Theory. 60-510 Literature Review and Survey, School of Computer Science, University of Windsor

[R 45] Dittrich, D.: The "stacheldraht" distributed denial of service attack tool. University of Washington, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt (1999)

[R 46] DMTF, (2010a). "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., Http://Www.Dmtf.Org/Sites/Default/Files/Standards/Documents/Dsp-Is0103_1.0.0.Pdf.

[R 47] DMTF, (2010b). "DMTF Architecture for managing clouds", [online], Distributed Management Task Force, Inc., http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf.

[R 48] DMTF. "DMTF Architecture for managing clouds". [online] Distributed Management Task Force, Inc. Available on http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf, Accessed on 11 February 2012, 2010.

[R 49] 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. Available on http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0103_1.0.0.pdf , Accessed on 11 February 2012, 2010.

[R 50] Douligeris, C. and Ninios, G. P., 2007. 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.

[R 51] Elastic Security, 2011. "Amazon EC2 'broad character' support and Security impact on third party tools such as Elastic Detector." [online]. Available at: http://elastic-security.com/2011/02/18/amazon-ec2-broad-character-support-and-security-impact-on-third-party-tools-such-as-elastic-detector/ [Accessed 30 July 2011].

[R 52] Elliot, D.; Swartz, E.; Herbane, B. (1999) Just waiting for the next big bang: business continuity planning in the UK finance sector. Journal of Applied Management Studies, Vol. 8, No, pp. 43–60. Here: p. 48.

[R 53] Endo, P.T., Gonçalves, G.E., J. Kelner, J. and D. Sadok. A Survey on a Cloud Computing Solutions. Workshop em Clouds, Grids e Aplicações, 2010.

[R 54] ENISA, 2009. "Cloud Computing Bnefits, Risks and Recommendations for Information Security." [online] European Network and Information Security Agency. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport [Accessed 27 July 2011].

[R 55] Entreprise Concept. [Online]. Available: http://enterprise-concept.com/ro/servicii/ service-oriented-architecture-soa/. [05.12.2013]

R 56] Ernst&Young, Identity and access management Beyond compliance, Insights on governance, risk and compliance 2013, http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf

[R 57] Esmaili, M., 1997. Dempster-Shafer Theory and Network Intrusion Detection Systems. Scientia Iranica, Vol. 3, No. 4, Sharif University of Technology.

[R 58] Eucalyptus System, Inc. "EC2-compatible tools". [online] Available on http://open.eucalyptus.com/wiki/ec2-compatible-tools, Accessed on 12 February 2012.

[R 59] Eucalyptus Systems, Inc. "Eucalyptus Cloud Computing Platform Administrator Guide Version 1.6." [online]. Available on http://open.eucalyptus.com/AdministratorGuide.v1.final.03.23.pdf, Accessed on 5 March 2011, 2010.

[R 60] Eucalyptus Systems, Inc. "Eucalyptus Community Cloud" [online] Available on http://open.eucalyptus.com/try/community-cloud, Accessed on 28 January 2011.

[R 61] Eucalyptus Systems, Inc. “Eucalyptus Open-Source Cloud Computing Infrastructure – An Overview” [online]. Available on http://www.eucalyptus.com/pdf/whitepapers/Eucalyptus_Overview.pdf, Accessed on 28 January 2011, 2009.

[R 62] Eucalyptus Systems, Inc.”Eucalyptus Administrator‟s Guide (2.0)”.[online] Available on http://open.eucalyptus.com/wiki/EucalyptusAdministratorGuide> Accessed on 5 March 2011, 2010.

[R 63] European Commission 2007. Innovation Clusters in Europe. A Statistical Analysis and Overview of Current Policy Support, Europe Innova / PRo Inno Europe paper n 5, DG Enterprise and Industry report.

[R 64] European Commission 2013. Innovation Union progress at country level 2013. [Online]. Available: http://ec.europa.eu/research/innovation-union/pdf/ state-of-the-union/2012/innovation_union_progress_at_country_level_2013. pdf#view=fit&pagemode=none [24.09.2013]

[R 65] F. Bitzer. “Management Framework for Amazon EC2”. Diploma Thesis, 2008.

[R 66] Federal Office for Information Security, Security Recommendations for Cloud Computing Providers (Minimum information security requirements), White Paper https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2

[R 67] Fischer International Identity, LLC., “Identity as a Service (IAAS) Technology”, White paper, 2009.

[R 68] Fischer International Identity, LLC., “Product Overview Introducing Fischer Identity”, White paper, 2009.

[R 69] Foster, I., Zhao, Y., Raicu, I. and Lu, S., 2008, “Cloud Computing and Grid Computing 360-Degree Compared”, Grid Computing Environments Workshop, GCE’08, pp. 1-10.

[R 70] Furlani, C.M. (2010). “Cloud Computing: Benefits And Risks Of Moving Federal It Into The Cloud”, [Online], National Institute Of Standards And Technology (Nist), Http://Www.Nist.Gov/Director/Ocla/Testimony/Upload/Cloud-Computing-Testimony-Final-With-Bio.Pdf

[R 71] GAlib documentation, http://lancet.mit.edu/galib-2.4/

[R 72] Gartner IAM 2020 Predictions, The Future Is Now, https://www.avatier.com/products/identity-management/resources/gartner-iam-2020-predictions/

[R 73] Geric, S., 2010. Security of Web Services based Service-oriented Architectures. MIPRO2010, Proceeding of the 33rd International Convention, Opatija, Croatia, pp. 1250-1255.

[R 74] German Federal Office for Information Security, BSI-Standard 100-1, Bonn, Germany, 2008.

R 75] Goldberg, D., Richardson, J., Genetic algorithms with sharing for multimodal function optimisation, Proceedings of the First International Conference on Genetic Algorithms and Their Applications, 1987

[R 76] Goldberg, David Edward, “Genetic Algorithms in Search and Optimization”, Addison-Wesley Pub. Co., 1989 ISBN 0-201-15767-5

[R 77] Google Project Hosting. “Typica”. [online] Available on http://code.google.com/p/typica/, Accessed on 15 February 2012, 2011.

[R 78] Google. “Hybridfox”. [online] Available on http://code.google.com/p/hybridfox/, Accessed on 12 February 2011, 2011.

[R 79] Goulding, J.T., Broberg, J. and Gardiner, M., 2010. “Identity and access management for the cloud: CA’s strategy and vision.” [online] CA, Inc., White paper. Available at: http://www.ca.com/files/WhitePapers/iam_cloud_security_vision_wp_236732.pdf [Accessed 11 August 2011].

[R 80] Grobauer, B., Walloschek, T. and Stocker, E., 2011. Understanding Cloud-Computing Vulnerabilities. Security & Privacy, IEEE , vol.9, no.2, pp.50-57, March-April 2011.

[R 81] Gruschka, N. and Iacono, L.L., 2009.“Vulnerable Cloud: SOAP Message Security Validation Revisited”, IEEE International Conference on Web Services, ICWS 2009, Los Angeles, pp. 625-631.

[R 82] Gruschka, N. and Jensen, M., 2010. “Attack Surfaces: A taxonomy for Attacks on Cloud”, http://download.hakin9.org/en/Securing_the_Cloud_hakin9_07_2010.pdf, Vol.5, No. 7, Issue 7/2010 (32) [Accessed 20 October 2010].

[R 83] Guth, M.A.S., 1991. A Probabilistic Foundation for Vagueness & Imprecision in Fault-Tree Analysis. IEEE TRANSACTIONS ON RELIABILITY, 40(5), pp.563-569.

[R 84] Hamdouch, A. 2008. Conceptualizing Innovation Clusters and Networks, International Conference: Innovation Networks, Tacoma-Seattle, Washington, USA, May 14-16, 2008. [Online]. Available: http://rrien.univ-littoral.fr/wp-content/uploads/2008/04/ hamdouch-innovationclusters-tacoma-seattlemay2008-final.pdf. [22.07.2013]

[R 85] Harding, P., 2011. State of Cloud Identity. 2nd annual Cloud Identity Summit, San Francisco.

[R 86] Heinle, C. And Strebel, J. (2010). “Iaas Adoption Determinants In Enterprises”. Inproceedings 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.

[R 87] Hemanth Jude, Popescu D.E, et al., Analysis of Wavelet, Ridgelet, Curvelet and Bandelet transforms for QR code based Image Steganography, EMES 2017

[R 88] Hemanth Jude; Maheswari, Uma; Popescu D.E; Naaji, Antoanela ,The Boon of Bandelet Transform and Discrete Curvelet Transform: Application to Image Steganography , CITCEP 2015 Congress on Information Technology, Computational and Experimental Physics December 18-20, 2015 Cracow, Poland, http://www.fis.agh.edu.pl/Conf-ITCEP/wp-content/uploads/CITCEP-2015-program-detailed.pdf

R 89] Hemanth, Jude; Umamaheswari, S; Popescu, DE; Naaji, A Application of Genetic Algorithm and Particle Swarm Optimization techniques for improved image steganography systems, Hemanth, OPEN PHYSICS, Volume: 14 Issue: 1 Pages: 452-462, Published: JAN 2016, DOI: 10.1515/phys-2016-0052, Accession Number: WOS:000394270500008

[R 90] Hogan, M. Liu, F. et al. “NIST Cloud Computing Standards Roadmap – Version 1.0.” NIST Nationale Institute of Standards and Technologies, 2011.

[R 91] Hogan, M., Liu, F., Sokol, A. And Tong, J. (2011). “Nist Cloud Computing Standards Roadmap – Version 1.0”. Nist Nationale Institute Of Standards And Technologies.

[R 92] Holland, J, Genetic Algorithms, Scientific American Ed, pp 66-72, 1992

[R 93] Hu, W., Li, J. and Gao, Q. 2006. Intrusion Detection Engine Based on Dempster-Shafer’s Theory of Evidence. Communications, Circuits and Systems Proceedings, 2006 International Conference, 3, 1627-1631

[R 94] Hunt, Phil (February 27, 2014). "Standards Corner: SCIM and the Shifting Enterprise Identity Center of Gravity". Oracle Fusion Middleware (blog). Oracle. Retrieved May 17, 2015.

http://www.simplecloud.info/specs/draft-scim-core-schema-01.html> [Accessed 10 September 2011].

[R 95] IBM Corporation, 2010. “IBM Tivoli Access Management for Cloud and SOA environments”. [online] Available at: ftp://public.dhe.ibm.com/common/ssi/ecm/en/tis14053usen/TIS14053USEN_HR.PDF [Accessed 11 August 2011].

[R 96] IBM, 2009a, “IBM Point of View: Security and Cloud Computing.” [online] Available at: <ftp://public.dhe.ibm.com/common/ssi/ecm/en/tiw14045usen/TIW14045USEN_HR.PDF> [Accessed 2 October 2010].

[R 97] International Organization for Standardisation and International Electrotechnical Commission, ISO/IEC, 27001, Geneva, Switzerland, 2013.

[R 98] International Organization for Standardisation and International Electrotechnical Commission, ISO/IEC, 27002, Geneva, Switzerland, 2005.

[R 99] ISO.ISO7498-2:1989.Informationprocessingsystems-OpenSystems Interconnection. ISO 7498-2

[R 100] J Tian, “Reversible data embedding using a difference expansion”, IEEE Trans. on circuits and Systems for video technology, vol. 13, pp. 890-896, 2003.

[R 101] Jackson, Lee; 2006, Analysis of Image-Based Authentication and its Role in Security Systems of the Future, 2006, from http://www.soc.napier.ac.uk/~bill/lee2006.pdf

[R 102] Jaeger, T. and Schiffman, J., 2010. “Outlook: Cloudy with a chance of Security Challenges and Improvements”, IEEE Security & Privacy, vol.8, no. 1, pp.77-80.

[R 103] Jamil, D. and Zaki, H., 2011. Security Issues in Cloud Computing and Countermeasures. International Journal of Engineering Science and Technology (IJEST), Vol.3, No.4, ISSN: 0975-5462.

[R 104] Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L.L., 2009. “On technical Security Issues in Cloud Computing”, IEEE International Conference on Cloud Computing (Cloud ‘09), Bangalore, pp. 109-116.

[R 105] Jing, X. and Jian-Jun, Z., 2010. “A Brief Survey on the Security Model of Cloud Computing”, 2010 Ninth International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES), pp. 475-478.

[R 106] Juniper Networks, Inc., 2009. “Identity Federation in a Hybrid Cloud Computing Environment Solution Guide.” [online] Available at: http://www.juniper.net/us/en/local/pdf/implementation-guides/8010035-en.pdf [Accessed 20 February 2011].

[R 107] just works! Software. “Cloud 42”. [online] Available on http://cloud42.net/index.php, Accessed on 12 February 2012

[R 108] Just, M. and D. Aspinall. 2009, Personal choice and challenge questions: A security and usability assessment. In L. Cranor, editor, SOUPS, ACM International Conference Proceeding Series. ACM, 2009.

[R 109] Kamal Dahbur, Bassil Mohammad, Ahmed BisherTarakji, A Survey of risks, threats, and vulnerabilities in cloud computing, ACM 978-1-4503-0474-0/04/2011

[R 110] Kandukuri, B. R., Paturi, R.V. And Rakshit, A. (2009). “Cloud Security Issues”. In: Ieee International Conference On Services Computing. Bangalore, 21-25 September 2009, Pp. 517-520

R 111] Kangasharju, J. ; K. W. Ross ; D. A. Turner, Optimizing File Availability in Peer-to-Peer Content Distribution, published in: INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, Print ISBN: 1-4244-1047-9, INSPEC Accession Number: 9833371

R 112] Karun Handa et al, Data Security in Cloud Computing using Encryption and Steganography, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 786-791, ISSN 2320–088X, [online], http://www.ijcsmc.com/docs/papers/May2015/V4I5201599a50.pdf

[R 113] Kay, R., 2005, QuickStudy: Biometric authentication, retrieved April 20, 2005

[R 114] Ketels, Ch. & Slvell, . 2006. Innovation Clusters in the 10 New Member States of the European Union, European Communities. [Online]. Available: http://www.isc.hbs.edu/ pdf/Clusters_EU-10_2006.pdf. [22.07.2013]

[R 115] Khajeh-Hosseini A., Greenwood D. And Sommerville I. (2010). “Cloud Migration: A Case Study Of Migrating An Enterprise It System To Iaas”. Ieee 3rd International Conference On Cloud Computing (Cloud 2010). Miami, Usa.

[R 116] Khajeh-Hosseini A., Sommerville I. And Sriram I. (2010). “Research Challenges For Enterprises Cloud Computing”. Lscits Technical Report

[R 117] Khajeh-Hosseini A., Sommerville I., Bogaerts J., Teregowda P. (2011). “Decision Support Tools For Cloud Migration In The Enterprise”. Ieee 4th International Conference On Cloud Computing (Cloud 2011), Washington Dc, Usa.

[R 118] Klems, M; Lenk, A, Nimis, J, Sandholm T and Tai S 2009, ‘What’s Inside the Cloud? An Architectural Map of the Cloud Landscape’, IEEE Xplore, pp 23-31, viewed 21 June 2009.

[R 119] Lakshminarayanan, S., 2010. Interoperable Security Standards for Web Services. IEEE IT Professional, Vol.12, Issue 5, pp. 42-47.

[R 120] Lari M R A, Ghofrani S and McLernon D, “Using Curvelet transform for watermarking based on amplitude modulation”, Signal Image and Video Processing, vol. 8, pp. 687-697, 2014.

[R 121] Lee, J-H., Park, M-W., Eom, J-H. And Chung, T-M., 2011. 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.

[R 122] Linthicum, D. S. 2009. Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide. Addison-Wesley Information Technology Series.

[R 123] Lipi Akter, Prof. Dr. S M Monzurur Rahman, Md. Hasan, INFORMATION SECURITY IN CLOUD COMPUTING, International Journal of Information Technology Convergence and Services (IJITCS) Vol.3, No.4, August 2013, http://airccse.org/journal/ijitcs/papers/3413ijitcs02.pdf

[R 124] Lonea A.M., Popescu D.E. and Prostean O., 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)

[R 125 Lonea A.M., Popescu D.E., Security Issues for GRID Systems, 4th International Workshop on Soft Computing Applications, 2010, IEEE Xplore, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5565622, Page(s): 73 - 76
Digital Object Identifier: 10.1109/SOFA.2010.5565622 (IEEE)

[R 126] Lonea A.M., Popescu D.E., Tianfield H, Detecting Distributed Denial of Service (DDoS) Attacks in Cloud Computing EnvironmentInternational Journal of Computers, Communications & Control, IJCCC, ISSN: 1841-9836, eISSN: 1841-9844, Accession Number: WOS:000312043600008 (ISI Journal)

[R 127] Lonea A.M., Teza de doctorat, Security Solutions for Cloud Computings, Universitatea “Politehnica Timisoara”, seria 12, Ingineria sistemelor, nr.5, Editura Politehnica Timisoara, ISSN: 2068-7990, ISBN 978-606-548-9 2012

[R 128] Lonea AM, Popescu DE, Prostean O, Tianfield H, Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud, SOFT COMPUTING APPLICATIONS, Book Series: Advances in Intelligent Systems and Computing, Volume: 195 Pages: 367-379, Published: 2013, Conference: 5th International Workshop Soft Computing Applications (SOFA), Szeged, HUNGARY, AUG 22-24, 2012, Publisher SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN, GERMANY, ISBN:978-3-

642-33940-0; 978-3-642-33941-7, ISSN: 2194-5357, Accession Number: WOS:000314077300034 (ISI Proceeding)

[R 129] Lonea AM, Tianfield H, Popescu DE, Identity Management for Cloud Computing New Concepts and Applications in Soft Computing Volume 417, 2013, pp 175-199, ISSN: 1860949X, ISBN: 978-364228958-3, Source Type: Book series, DOI: 10.1007/978-3-642-28959-0-11 Document Type: Conference Paper, https://www-scopus-com.am.e-nformation.ro/record/display.uri?eid=2-s2.0-84867464838&origin=publicationMetricPage, SCOPUS (13 citari) (Springer)

[R 130] Lonea, AM, Popescu, DE, Octavian Prostean, The overall process taken by enterprises to manage the IaaS cloud services, Conference: 6th European Conference on Information Management and Evaluation (ECIME) Location: Univ Coll Cork, Cork, IRELAND Date: SEP 13-14, 2012
PROCEEDINGS OF THE 6TH EUROPEAN CONFERENCE ON INFORMATION MANAGEMENT AND EVALUATION Pages: 168-177, Published: 2012, Accession Number: WOS:000321564000021 (ISI Proceeding)

[R 131] Lou D C and Hu C H, “LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis”, Information Sciences, vol. 188, pp. 346–358, 2012.

[R 132] Lynch, L., 2011. Inside the Identity Management Game. IEEE Internet Computing, Vol. 15, Issue 5, pp. 78-82.

[R 133] M Y Wu, Y K Ho and J H Lee, “An iterative method of palette-based image steganography”, Pattern Recognition Letters, vol. 25, pp. 301–309, 2004.

[R 134] Majava, J., Biasiol, A. and Van der Maren, A., 2007. “Report on comparison and assessment of eID management solutions interoperability.” [online] European Communities. Available at: < http://ec.europa.eu/idabc/servlets/Doceb29.pdf?id=29620> [Accessed 10 February 2011].

[R 135] Martens, B. And Teuteberg, F. (2011). ”Risk And Compliance Management For Cloud Computing Services: Designing A Reference Model”. In Proceedings Of The Seventeenth Americas Conference Of Information Systems, Detroit, Michigan, August 4th-7th.

[R 136] Mazzariello, C., Bifulco, R. and Canonico, R., 2010. Integrating a Network IDS into an Open Source Cloud Computing Environment. In Sixth International Conference on Information Assurance and Security, pp. 265-270.

[R 137] McMillan, R., 2009. “Cisco CEO: Cloud Computing a ‘Security nightmare” [online]. Available at: < http://www.csoonline.com/article/490368/cisco-ceo-cloud-computing-a-security-nightmare-> [Accessed 20 October 2010].

[R 138] Mell, P. and Grance, T., 2009. “The NIST definition of Cloud Computing. “ [online] National Institute of Standards and Technology (NIST). Available at: < csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> [Accesssed 2 October 2010].

[R 139] Metri P. and Sarote G., 2011, “Privacy Issues and Challenges in Cloud computing,” International Journal of Advanced Engineering Sciences and Technologies, vol. 5, no. 1, pp. 5-6, 2011.

[R 140] Micallef, Nicholas; Mike Just, 2011, “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.

R 141] Milojicic, D., Kalogeraki, V., Lukose, R., Nagaraja K. et all, Peer-to-peer computing. Technical report, HP Laboratories, 2002.

[R 142] Molony, D. And Kirchheimer, E. (2011). “What Multinationals Want: Opportunities In Cloud Computing”, [Online], Ovum White Paper, Http://Www.Cw.Com/Assets/Content/Pdfs/Resource/Ovum-Cloud-Wp.Pdf.

[R 143] Morgan, K. 1997. The Learning Region: Institutions, Innovation and Regional Renewal, Regional Studies, Vol. 31.5, 491-503

[R 144] Newman, Richard E.;, Piyush Harsh, and Prashant Jayaraman, 2005, “Security Analysis of and Proposal for Image Based Authentication,” IEEE Carnahan, 2005

[R 145] Nitin, Vivek Kumar Sehgal, et al., 2008, 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

[R 146] Nordbotten, N.A., 2009. XML and Web Services Security Standards. IEEE Communications Surveys & Tutorials, Vol. 11, Issue 3, pp. 4-21.

[R 147] Novell, 2010. “Annexing the Cloud Novell Cloud Security Service” [online]. Novell. Available at: <http://www.asiacloudforum.com/system/files/WP_Novell_annexing_cloud_security.pdf> [Accessed 21 May 2011].

[R 148] Novell, 2011. “Novell Cloud Security Service 1.0 SP2” [online]. Novell. Available at:<http://www.novell.com/documentation/novellcloudsecurityservice/> [Accessed 21 May 2011].

[R 149] Nurmi, D. et al. “Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems”. University of California, Santa Barbara, 2008

[R 150] Nurmi, D. et al. “The Eucalyptus Open-source Cloudcomputing System”. 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009.

[R 151] Nurmi, D. et al. Eucalyptus: An open-source cloud computing infrastructure. SciDAC 2009, IOP Publishing, Journal of Physics: Conference Series 180, 2009.

[R 152] OASIS, 2003a. “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> [Accessed 4 November 2010].

[R 153] OASIS, 2005a. “SAML V2.0 Executive Overview.” [online] OASIS. Available at: < http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf > [Accessed 10 November 2010].

[R 154] OASIS, 2008. “Security Assertion Markup Language (SAML) V2.0 Technical Overview.” [online] OASIS. Available at: < http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf > [Accessed 10 November 2010].

[R 155] OAuth, n.d., “OAuth Community Site.” [online] Available at: <http://oauth.net/ > [Accessed 10 September 2011].

[R 156] Ogrizovic, D.;, B. Svilicic and E. Tijan. “Open Source Science Clouds”. MIPRO 2010, Opatija, Croatia, pp.1189-1192, 2010.

[R 157] Olden, E., 2011. "Architecting a Cloud-Scale Identity Fabric," Computer, vol.44, no.3, pp.52-59.

[R 158] Open Group, SOA and Enterprise Architecture. [Online]. Available:http://opengroup.org/ soa/source-book/soa/soa_ea.htm .[14.12.2013].

[R 159] Perry, G., 2011. Minimizing public cloud disruptions, TechTarget, [online]. Available at: <http://searchdatacenter.techtarget.com/tip/Minimizing-public-cloud-disruptions> [Accessed 08 February 2012].

[R 160] Ping Identity, 2010a. “The Primer: Nuts and Bolts of Federated Identity Management White Paper.” [online] Ping Identity Corporation. Available at: http://secprodonline.com/~/media/SEC/Security%20Products/Whitepapers/2008/06/Ping%20Identity_WP_PrimerFIM%20pdf.ashx [Accessed 10 February 2011]. Valid!

[R 161] Ping Identity, 2010b. “SAML 101 White paper.” [online] Ping Identity Corporation. Available at:< https://www.pingidentity.com/unprotected/upload/SAML-101.pdf> [Accesed 10 February 2011].

[R 162] Popescu C., Popescu D.E., “Digital Systems Reliability and Testability”, Bucharest, Matrix Rom, 2001

[R 163] Popescu D.E., Popescu C., Rusu C., The Analysis Of The Influence Of Searching Space Limitation Of Genetic Algorithms On Reliability Maximization Problem, SOFA 2005, IEEE Workshop on Soft Computing Applications, 27-30Aug.2005, Szeged-Hungary, & Arad –Romania, pp.362-267, 2005

[R 164] Popescu DE, Lonea AM, An Hybrid Text-Image Based Authentication for Cloud Services, INT J COMPUT COMMUN, ISSN 1841-9836, 8(2):263-274, April, 2013, International Journal of Computers, Communications & Control, IJCCC , ISSN: 1841-9836, eISSN: 1841-9844, , Accession Number: WOS:000314903200008 (ISI Journal)

[R 165] Popescu DE, Vladu E.

A Genetic Algorithm Approach For Optimizing The File Availability In Peer-To-Peer Content Distribution, Journal Of Computer Science And Control Systems, 2009 (DOAJ)

[R 166] Popescu, C.; Popescu, D.E., System Design Optimization By Genetic Algorithms, Optimum Q, Revista de specialitate, cultura si educaţie in domeniul calităţii si fiabilităţii, vol.XII, Nr. 1-2/2002, ISSN 1220-6598, pag.100-106, 2002

[R 167] Popescu, D.E.; Dodescu, A., Filip, P., Cloud Service Management System for Innovative Clusters. Application for North-West Region of Romania, International Journal of Computers Communications & Control, data publicarii 2014/6/15, Vol.9, nr.4, pag.453-462, ISSN: 1841-9836, eISSN: 1841-9844, Accession Number: WOS:000337771000007 (ISI Journal)

[R 168] Popescu, D.E.; Madalina Alina Lonea, D.Zmaranda C.Vancea, C.Tiurbe, Some Aspects about Vagueness & Imprecision in Computer Network Fault-Tre Analysis, INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL Volume: 5 Issue: 4 Pages: 558-566 Published: NOV 2010, ISSN: 1841-9836, Accession Number: WOS:000282600700015

[R 169] Rachna Dhamija et al, 2000, Déjà Vu: a user study using images for authentication, Proceeding SSYM'00 Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, USENIX Association Berkeley, CA, USA ©2000, http://sparrow.ece.cmu.edu/~adrian/projects/usenix2000/usenix.pdf

[R 170] Ramgovind, S., Eloff, M.M. and Smith, E., 2010. “The management of security in Cloud Computing”, Information Security for South Africa (ISSA), pp. 1-7, 2010, http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/27_Paper.pdf

[R 171] Reddy, V.K.; 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

[R 172] Rehman, R. UR.: Intrusion Detection with Snort: Advanced IDS Techniques using Snort, Apache, Mysql, PHP and ACID. Pearson Education Inc., Publishing as Prentice Hall PTR (2003)

[R 173] Renaud, Karen; Mike Just, 2010, “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.

[R 174] Richard Chow PARC, et al., 2011, Authentication in the Clouds: A Framework and its Application to Mobile Users, ACM Cloud Computing Security Workshop (CCSW); 2010 October 8; Chicago, IL.

[R 175] RightScale, Inc. “RightScale Cloud Management”. [online] Available on http://www.rightscale.com/, Accessed on 12 February 2012, 2012.

[R 176] Ristenpart, T., Tromer, E., Schacham, H. and Savage, S., 2009. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party compute Clouds. ACM Conference on Computer and Communications Security, Chicago.

[R 177] Rittinghouse, J. W. and Ransome, J.F, Cloud Computing Implementation, Management and Security. Boca Raton: CRC Press, 2010.

[R 178] Romanian North-West Regional Development Agency 2013. 2014-2020 Regional Devel- opment Plan (draft, September 2013). [Online]. Available: http://www.nord-vest.ro/ Document_Files/Planul-de-dezvoltare-regionala-2014-2020/00001513/tp9mg_PDR% 202014-2020%20DRAFT%20sept_2013.pdf. [18.02.2014].

[R 179] Roschke, S., Cheng, F. and Meinel, C., 2009. Intrusion Detection in the Cloud. In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729-734.

[R 180] RSA, (2009). “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

[R 181] Sachdeva, S., Machome, S. and Bhalla, S., 2010. Web Services Security Issues in Healthcare Applications. 9th IEEE/ACIS International Conference on Computer and Information Science (ICIS), Yamagata, pp. 91-96.

[R 182] Sandeep Sahu, Aditi Bhadoria, Survey on Cloud computing security using steganography, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 8, August 2015, [online] http://ijsetr.org/wp-content/uploads/2015/08/IJSETR-VOL-4-ISSUE-8-2975-2978.pdf

[R 183] Sarkar, M. K; and T. Chatterjee, “Enhancing Data Storage Security in Cloud Computing Through Steganography”, ACEEE International Journal on Network Security, ISSN: 2152-5064, Vol. 5, Issue. 1, pp: 13-19, Jan 2014.

[R 184] Saugatuck Technology Inc. (2010). “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.

[R 185] Security Guidance for Critical Ares of Focus in Cloud, Cloud Security Alliance, https://cloudsecurityalliance.org/research/grc-stack/#_overview

[R 186] Sempolinski P. and D. Thain. “A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus.” [online] University of Notre Dame. Available on http://www.cse.nd.edu/~ccl/research/papers/psempoli-cloudcom.pdf, Accessed on 13 February 2011

[R 187] Sentz, K. and Ferson, S., 2002. Combination of Evidence in Dempster-Shafer Theory. Sandia National Laboratories, Sandia Report

[R 188] Seo J S and Yoo C D, “Image watermarking based on invariant regions of scale-space representation”, IEEE Trans. on Signal Processing, vol. 54, pp. 1537–49, 2006.

[R 189] SETECS® Inc, 2011, Security Architecture, for Cloud Computing Environments, White Paper– February 1, 2011, http://security.setecs.com/Documents/5_SETECS_Cloud_Security_Architecture.pdf

[R 190] Shacklerford, Cloud Security and Compliance: A Primer - SANS Institute, A SANS Whitepaper – August 2010 [online]https://www.sans.org/reading-room/whitepapers/analyst/cloud-security-compliance-rimer-34910

[R 191] Shah, D. and Patel, D., 2008. Dynamic and Ubiquitous Security Architecture for Global SOA. The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Valencia, Spain, pp. 482-487.

[R 192] Shem-Tov Levi, Ashok K. Agrawala, Real-time system design, McGraw-Hill Pub. Co., 1990 - 299 pagini

[R 193] Siaterlis, C. And Maglaris, B., 2005. One step ahead to Multisensor Data Fusion for DDoS Detection. Journal of Computer Security, Vol. 13, Issue 5, September 2005, pp. 779-806.

[R 194] Siaterlis, C., Maglaris, B. and Roris, P., 2003. A novel approach for a Distributed Denial of Service Detection Engine. National Technical University of Athens. Athens, Greece.

[R 195 Smarter with Gartner, http://www.gartner.com/smarterwithgartner/category/it/cloud/

[R 196] Subashini, S. and Kavitha, V., 2011. “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, vol. 34, pp. 1-11.

[R 197] Sun Microsystems, Inc., 2004. “Sun’s XACML Implementation Programmer’s Guide for Version 1.2.” [online] Sun Microsystems. Available at: < http://sunxacml.sourceforge.net/guide.html > [Accessed 7 February 2011].

[R 198] Tari, F., Ant Ozok, A., Holdon, H.S, 2006, A Comparison of Percieved and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords, retrieved June 10 2006 from http://cups.cs.cmu.edu/soups/2006/proceedings/p56_tari.pdf

[R 199] Tianfield., H. “Cloud Computing Architectures”. Proceedings of 2011 IEEE International Conference on Systems, Man and Cybernetics (SMC’11), Anchorage, Alaska, USA, 2011.

[R 200] Trend Micro, 2009. “Cloud Computing Security” [online] A Trend Micro White Paper. Available at: <http://www.whitestratus.com/docs/making-vms-cloud-ready.pdf> [Accessed 20 October 2010].

[R 201] Ubuntu Documentation. “UEC Overview”. [online] Ubuntu. Available on https://help.ubuntu.com/10.04/serverguide/C/uec.html, Accessed on 16 February 2011.

[R 202] Universität Osnabrück, (2012). “Total Cost Of Ownership Calculator For Cloud Computing Services”, [Online], Http://Www.Cloudservicemarket.Info/Tools/Tco.Aspx

[R 203] Varia, J. (2010). “Migrating Your Existing Applications To The Aws Cloud”. Amazon Web Services.

[R 204] Vitek, A. J. & Morris, M.N, 2012, Service Oriented Cloud Computing Architectures, UMM CSci Senior Seminar Conference. [Online]. Available: https://wiki.umn.edu/pub/UmmCSciSeniorSeminar/.[07.11.2013]

[R 205] Vlăduţiu, M., 1989, Tehnologie de ramură şi fiabilitate, curs litografiat IPTVT, pp.95-110

[R 206] VMware and SAVVIS, 2009. “Securing the Cloud A Review of Cloud Computing, Security Implications and Best Practices” [online]. VMware. Available at:< http://www.savvis.net/en-US/Info_Center/Documents/Savvis_VMW_whitepaper_0809.pdf> [Accessed 15 October 2010].

[R 207] W3C, 2004. “Web Services Architecture, W3C Working Group Note.” [online] World Wide Web Consortium. Available at: < http://www.w3.org/TR/ws-arch/#id2260892> [Accessed 20 January 2011].

[R 208] Weinhardt C, Anandasivam A, Blau B, and Stosser J, ‘Business Models in the Service World’, IT Professional, vol. 11, pp. 28-33, 2009.

[R 209] Weinmann J. “Axiomatic Cloud Theory”. [online] Available on http://www.joeweinman.com/Resources/Joe_Weinman_Axiomatic_Cloud_Theory.pdf, Accessed on 5 June 2011, 2011.

[R 210] White Bill C., “Random Walk Population Sizing as a Model of decision Making in a Deceptive Schema Partition” – a thesis presented for the Master of Science Degree, The University of Tennessee, Knoxville, 1999

[R 211] Wrenn, G., CISSP, ISSEP, 2010. “Unisys Secure Cloud Addressing the Top Threats of Cloud Computing”. [online]. Available at: < http://www.unisys.com/unisys/unisys/inc/pdf/whitepapers/38507380-000.pdf>, White Paper [Accessed 17 October 2010].

[R 212] Wu, W., Zhang, H. and Li, Z., 2011. Open Social based Collaborative Science Gateways. 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 554-559.

[R 213] Wynn, R., 2010. Securing the Cloud: Is it a Paradigm Shift in Information Security. In: Hacking IT Security Magazine, Vol.5, No.7.

[R 214] X Gui, X Li and B Yang, “A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding”, Signal Processing, vol. 98, pp. 370–380, 2014.

[R 215] X Zhang and S Wang, “Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security”, Pattern Recognition Letters, vol. 25, pp. 331–339, 2004.

[R 216] Yu, D. and Frincke, D., 2004. 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.

[R 217] Yu, D. and Frincke, D., 2005. Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory. ACM-SE 43: Proceedings of the 43rd ACM Southeast Conference, pp. 142-147.

[R 218] Z Ni et al., “Reversible Data Hiding”, IEEE Trans. on circuits and Systems for video technology, vol.16, pp. 354-362, 2006.

[R 219] Zhang, Y, Juels, A., Reiter, M.K. Ristempart, T.; Cross-vm side channels and their use to extract private keys. Proceedings of the 2012 ACM conference on Computer and communications security, pp.305-316, ACM, 2012

[R 220] Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A., 2010. “Security and Privacy in Cloud Computing: A Survey”, 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG), pp. 105-112.

7.2 Representative works

1. AM Lonea, **DE Popescu,** H Tianfield
   Detecting Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environment, International Journal of Computers, Communications & Control, IJCCC, ISSN: 1841-9836, eISSN: 1841-9844
   Accession Number: WOS:000312043600008 (ISI Journal)
2. **DE Popescu**, AM Lonea
   An Hybrid Text-Image Based Authentication for Cloud Services, INT J COMPUT COMMUN, ISSN 1841-9836, 8(2):263-274, April, 2013, International Journal of Computers, Communications & Control, IJCCC , ISSN: 1841-9836, eISSN: 1841-9844,
   Accession Number: WOS:000314903200008 (ISI Journal)
3. AM Lonea, H Tianfield, **DE Popescu**
   Identity Management for Cloud Computing, New Concepts and Applications in Soft Computing Volume 417, 2013, pp 175-199, ISSN: 1860949X, ISBN: 978-364228958-3, Source Type: Book series, DOI: 10.1007/978-3-642-28959-0-11 Document Type: Conference Paper, https://www-scopus-com.am.e-nformation.ro/record/display.uri?eid=2-s2.0-84867464838&origin=publicationMetricPage, SCOPUS (13 citari) (**Springer**)
4. 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**)
5. AM Lonea, **DE Popescu,** O Prostean, H Tianfield
   Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud, SOFT COMPUTING APPLICATIONS Book Series: Advances in Intelligent Systems and Computing, Volume: 195 Pages: 367-379, Published: 2013, Conference: 5th International Workshop Soft Computing Applications (SOFA), Szeged, HUNGARY, AUG 22-24, 2012, Publisher SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN, GERMANY, ISBN:978-3-642-33940-0; 978-3-642-33941-7, ISSN: 2194-5357
   Accession Number: WOS:000314077300034 (ISI Proceeding)
6. AM Lonea, **DE Popescu**, O Prostean
   The overall process taken by enterprises to manage the IaaS cloud services, Conference: 6th European Conference on Information Management and Evaluation (ECIME) Location: Univ Coll Cork, Cork, IRELAND Date: SEP 13-14, 2012, Proceedings Of The 6th European Conference On Information Management And Evaluation, Pages: 168-177, Published: 2012
   Accession Number: WOS:000321564000021 (ISI Proceeding)
7. D.Zmaranda, Gianina Gabor, **D.E. Popescu**, C.Vancea, Fl. Vancea
   Using Fixed Priority Pre-emptive Scheduling in Real-Time Systems, INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, Volume: 6 Issue: 1 Pages: 187-195, Published: MAR, 2011, ISSN: 1841-9836
8. **D.E. Popescu**, AM Lonea, D.Zmaranda C.Vancea, C.Tiurbe
   Some Aspects about Vagueness & Imprecision in Computer Network Fault-Tree Analysis, International Journal of Computers Communications & Control

Volume: 5 Issue: 4 Pages: 558-566 Published: NOV 2010, ISSN: 1841-9836
Accession Number: WOS:000282600700015

9. **D.E. Popescu**
A Proposed Cache Line Implementation Solution with Error/Correcting Capabilities for Managing Cache Coherency in Multiprocessor Systems, , ACTA ELECTROTECHNICA ET INFORMATICA, pp.68-74, ISSN 1335-8243, 2009
http://www.aei.tuke.sk/papers/2009/3/2009-3.htm#POP

10. **D.E. Popescu,** A.Dodescu, P.Filip
Cloud Service Management System for Innovative Clusters. Application for North-West Region of Romania, International Journal of Computers Communications & Control, data publicarii 2014/6/15, Vol.9, nr.4, pag.453-462, ISSN: 1841-9836, eISSN: 1841-9844
Accession Number: WOS:000337771000007