INT J COMPUT COMMUN, ISSN 1841-9836
8(1):70-78, February, 2013.

Detecting DDoS Attacks in Cloud Computing Environment

A.M. Lonea, D.E. Popescu, H. Tianfield

Alina Madalina Lonea
"Politehnica" University of Timisoara,
Faculty of Automation and Computers
B-dul Vasile Parvan, nr. 2, 300223, Timisoara, Romania
E-mail: madalina _ lonea@yahoo.com

Daniela Elena Popescu
University of Oradea, Faculty of Electrical Eng. and Information Tech.
Universitatii street, nr. 1, 410087, Oradea, Romania
E-mail: depopescu@uoradea.ro

Huaglory Tianfield
School of Engineering and Built Environment,
Glasgow Caledonian University
Cowcaddens Road, Glasgow G4 0BA, United Kingdom
E-mail: h.tianfield@gcu.ac.uk

Abstract:
This paper is focused on detecting and analyzing the Distributed Denial of Service (DDoS) attacks in cloud computing environments. This type of attacks is often the source of cloud services disruptions. Our solution is to combine the evidences obtained from Intrusion Detection Systems (IDSs) deployed in the virtual machines (VMs) of the cloud systems with a data fusion methodology in the front-end. Specifically, when the attacks appear, the VM-based IDS will yield alerts, which will be stored into the Mysql database placed within the Cloud Fusion Unit (CFU) of the front-end server. We propose a quantitative solution for analyzing alerts generated by the IDSs, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for the mentioned flooding attacks. At the last step, our solution uses the Dempsters combination rule to fuse evidence from multiple independent sources.
Keywords: cloud computing, cloud security, Distributed Denial of Service (DDoS) attacks, Intrusion Detection Systems, data fusion, Dempster-Shafer theory.

1 Introduction

Cloud computing technology is in continuous development and with numerous challenges regarding security. In this context, one of the main concerns for cloud computing is represented by the trustworthiness of cloud services. This problem requires prompt resolution because otherwise organizations adopting cloud services would be exposed to increased expenditures while at a greater risk. A survey conducted by International Data Corporation (IDC) in August 2008 confirms that security is the major barrier for the cloud users.

There are two things that cloud service providers should guarantee all the time: connectivity and availability, and if there are not met, the entire organizations will suffer high costs [1].

This paper is focused on detecting and analyzing Distributed Denial of Service (DDoS) attacks in cloud computing environment. This type of attacks is often the source of cloud services disruptions. One of the efficient methods for detecting DDoS is to use the Intrusion Detection Systems (IDS), in order to assure usable cloud computing services [2]. However, IDS sensors have the limitations that they yield massive amount of alerts and produce high false positive rates and false negative rates [3].

INT J COMPUT COMMUN, ISSN 1841-9836
8(2):263-274, April, 2013.

An Hybrid Text-Image Based Authentication for Cloud Services

D.E. Popescu, A.M. Lonea

Daniela Elena Popescu, Alina Madalina Lonea
Faculty of Electrical Engineering and Information Technology, University of Oradea
Romania, 410087 Oradea, 1, Armatei Romane Str.
E-mail: depopescu@uoradea.ro, madalina_lonea@yahoo.com

Abstract:
The problem of securing access to the online information is acute today when access to bank accounts, health records, intellectual property and business or politically sensitive information are made by only a few clicks, regardless of geographic location. At the same time, more and more of these accesses are made from handsets. Cloud Computing is eminently suitable for addressing problems related to limited client resources, as it offloads computation from clients and offers dynamic provisioning of compute resources. Authentication of the companys users to the cloud service is mandatory because in this way it is eliminated the attacks risks to enter into the Cloud services. A suitable authentication is required for organizations that want to access the Cloud services. Our solution regards increasing security at the Security Access Point level of Cloud Computing 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. A two factor password image based authentication method is proposed in this paper for cloud services. This authentication approach is used without additional hardware involved and presents the advantages of utilization in terms of security and usability. Every time when the user will be asked to provide his/her identity, a form for each image included in the photo will be listed. The user will have to remember the secret code for each image and to carefully introduce them in the forms. The global cloud access solution will be based on our hybrid proposed text-image based solution, and will be completed by the X.509 certificates.
Keywords: authentication, multi factor password authentification, strong authentification, image based, cloud services, IaaS, PaaS, SaaS.

1 Introduction

As Cloud Computing (CC) model seems to be the best solution for solving the online access to services that became ubiquitous, authentication is becoming a focal point for security professionals [1]. The problem of securing access to the online information is acute today when access to bank accounts, health records, intellectual property and business or politically sensitive information are made by only a few clicks, regardless of geographic location. At the same time, more and more of these accesses are made from handsets. This introduces security vulnerabilities and complications, because handsets have computational, and power limitations compared with traditional computers and they are constrained in terms of text input being more prone to theft than traditional computers. It is also important to point out that mobile devices input constraints make difficult for users to input complex passwords. Cloud Computing is eminently suitable for addressing problems related to limited client resources, as it offloads computation from clients and offers dynamic provisioning of compute resources. So, CC emerges as a new computing paradigm 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.

Identity Management for Cloud Computing

Alina Mădălina Lonea[*], Huaglory Tianfield[**], Daniela Elena Popescu[***]

[*]Automation and Applied Informatics Department, "Politehnica" University of Timisoara, Faculty of Automation and Computers, B-dul Vasile Parvan, nr. 2, 300223, Timisoara, Romania

E-mail: madalina_lonea@yahoo.com

[**]School of Engineering and Built Environment, Glasgow Caledonian University, Cowcaddens Road, Glasgow G4 0BA, United Kingdom

E-mail: h.tianfield@gcu.ac.uk

[***]Computer Engineering Department, University of Oradea, Faculty of Electrical Engineering and Information Technology, Universitatii street, nr. 1, 410087, Oradea, Romania

E-mail: depopescu@uoradea.ro

A Survey of Management Interfaces for Eucalyptus Cloud

A.M. Lonea*, D.E. Popescu** and O. Prostean*
* "Politehnica" University of Timisoara / Automation and Applied Informatics Department, Timisoara, Romania
** University of Oradea / Computer Engineering Department, Oradea, Romania
madalina_lonea@yahoo.com, depopescu@uoradea.ro,
octavian.prostean@aut.upt.ro

Abstract— Cloud Computing is a technology which is susceptible to a continuous development, because of its strong advantages of accessing data from any place in the world over the Internet without concerning about the infrastructure used and the problems involved by the installation and maintenance processes. The purpose of this article is to provide an overview of several management interfaces for Eucalyptus cloud by addressing the taxonomy and evaluation of the cloud management interfaces. The taxonomy proposed in this paper results from the work accomplished by experimenting the Eucalyptus community cloud.

First, an evaluation of the Eucalyptus architecture is presented, in order to emphasize the Eucalyptus platform involved in cloud management process, which facilitates the deployment, management and execution of Infrastructure-as-a-Service (IaaS).

The cloud management tools are described from two perspectives. The first perspective analyzes the cloud portals from the user roles, while the second perspective addresses them with respect to the type of the tools employed. The taxonomy presented in this paper is related with the 5 elements of the *Common Cloud Management Architecture (CCMA)*, which was provided by Behrendt, et al. (2011) as one of the components of IBM Cloud Computing Reference Architecture. Thus, 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).

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).

This article is motivated by the fact that cloud management is a fundamental support for all users of cloud services from the cloud marketplace.

Keywords: cloud management, Eucalyptus Community Cloud, euca2ools, Graphical User Interfaces, Cloud API, third party cloud management tools, instances management, volumes management, user/groups management, key management

I. Introduction

Cloud Computing is a technology which is susceptible to a continuous development, because of its strong advantages of accessing data from any place in the world over the Internet without concerning about the infrastructure used and the problems involved by the installation and maintenance processes. Cloud Computing is defined by the US 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"*[2]. 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"*. The widely accepted Cloud Computing definition provided by NIST is expressed by Joe Weinmann (2011) as an acronym: a **C**ommon, **L**ocation-Independent **O**nline **U**tility on-**D**emand service, on the Axiomatic Cloud Theory.

Today, there are many providers that deliver cloud services for customers: Amazon Web Services, Microsoft Azure, Google Apps, IBM etc. These cloud services are delivered by commercial cloud platforms. A cloud platform corresponds to the cloud service provider, who has data centers where it runs applications and store data [4]. There are two types of cloud platforms: commercial and open-source. The cloud platforms deliver three types of cloud services: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

A previous research regarding the open source toolkits (i.e. Eucalyptus, Xen Cloud Platform, Open Nebula, Nimbus etc) was realized [5; 6; 7; 8].

The purpose of this article is to provide an overview of several management interfaces for Eucalyptus cloud by addressing the taxonomy and evaluation of the cloud management interfaces. The taxonomy proposed in this paper results from the work accomplished by experimenting the Eucalyptus community cloud.

Thus, the cloud management tools are described from two perspectives. The first perspective analyzes the cloud portals from the user roles, while the second perspective addresses them with respect to the type of the tools employed. These interaction styles emphasize the

978-1-4673-1014-7/12/$31.00 ©2012 IEEE

In: V. E. Balas et al. (Eds.), Soft Computing Applications,
"Advances in Intelligent Systems and Computing" Series, Volume AISC 195, Springer-Verlag, 2013, pp. 367-379

Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud

Alina Mădălina Lonea[1], Daniela Elena Popescu[2],
Octavian Prostean[1], and Huaglory Tianfield[3]

[1] Automation and Applied Informatics Department,
"Politehnica" University of Timisoara, Faculty of Automation and Computers,
B-dul Vasile Parvan, nr. 2, 300223, Timisoara, Romania
madalina_lonea@yahoo.com, octavian.prostean@aut.upt.ro
[2] Computer Engineering Department, University of Oradea,
Faculty of Electrical Engineering and Information Technology,
Universitatii Street, nr. 1, 410087, Oradea, Romania
depopescu@uoradea.ro
[3] School of Engineering and Built Environment,
Glasgow Caledonian University,
Cowcaddens Road, Glasgow G4 0BA, United Kingdom
h.tianfield@gcu.ac.uk

Abstract. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks appear to be main threats for cloud computing. The protection of cloud services against DoS and DDoS attacks is realized using Intrusion Detection Systems (IDSs).This paper aims to evaluate the experimental results of our proposed quantitative solution. The experiments are performed in a private cloud model deployed using Eucalyptus open-source, with virtual machines based IDS (VMs-based IDS) being created in three nodes and the Mysql database together with the graphical interfaces for monitoring the alerts being installed and configured in the front-end server. After a set of DDoS attacks are launched against the VMs-based IDS, we analyze all the alerts collected from the VMs-based IDS.

Keywords: attacks, cloud computing, data fusion, DDoS attacks, Dempster-Shafer Theory (DST), Eucalyptus, Intrusion Detection Systems (IDSs), Fault-Tree Analysis, Snort.

1 Introduction

Trustworthiness of cloud services become today a concern for cloud customers and providers. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks appear to be their main threats. In the recent times, Cloud Service Providers (CSPs) had suffered security breaches and the service's availability was compromised for hours [2].

The Overall Process Taken by Enterprises to Manage the IaaS Cloud Services

Alina Mădălina Lonea[1], Daniela Elena Popescu[2] and Octavian Proştean[1]
[1]Automation and Applied Informatics Department, Faculty of Automation and Computers, "Politehnica" University of Timisoara, Timisoara, Romania
[2]Computer Engineering Department, Faculty of Electrical Engineering and Information Technology, University of Oradea, Oradea, Romania
madalina_lonea@yahoo.com
depopescu@uoradea.ro
octavian.prostean@aut.upt.ro

Abstract: Small and medium-sized enterprises (SMEs) were the initial focus for cloud services and they are susceptible to a continuous adoption of cloud computing services, because of its strong advantages of accessing data from any place in the world over the Internet without concerning about the infrastructure used and the problems involved by the installation and maintenance processes. However, organizations need to consider simultaneously both risks and rewards within the decision making process, in order to assure an efficient expertise. SMEs represent the target group of this study concerned with the outsourcing process to Cloud Service Provider (CSP) considering the fact that the number of SMEs is greater than the number of large organizations, making SMEs the heart of economies worldwide (Sharma, et al., 2010; Van Hoecke, et al., 2011). The aim of the proposed research represents a qualitative analysis of the overall process taken by SMEs to manage the migration of their applications to Infrastructure-as-a-Service (IaaS). We conducted a literature analysis using papers released both by academic and practitioner bodies, in order to respond to the following two research questions: What are the steps involved in the migration process of the SMEs to cloud services? What are the stages required by each step of the outsourcing process? In this sense we produced a theoretical process, which includes a collection of the following interrelated activities: data analysis step, decision making step, migration step and management step. In an IaaS cloud service, the CSP supports the hardware related issues, whilst the software related issues should be identified by enterprises that want to migrate to cloud. Thus, this paper is first proposing to address an overview of the data analysis step. This 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. Further, another objective of this paper is to address the decision making step, which implies the following decisions: what information should be moved into cloud and who will access the information, what 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 the cloud service type was chosen (i.e. IaaS) and the cloud deployment model was selected as well (i.e. public cloud). Furthermore, the effective moving stage of enterprise's assets into cloud services is the migration step, which includes two activities: developing the Service Level Agreement (SLA) and implementing cloud. In addition, the last step of the overall process is the management step, which is realized using two management functions: business and operational.

Keywords: cloud management, outsourcing, IaaS, SME, cloud risks, cloud benefits, service level agreement

1. Introduction

Information Systems (IS) has a great impact for the business growth of Small and Medium sized Enterprises (SMEs) and it started with personal computers in order to manage the day-to-day operations of the enterprises using the basic applications (i.e. word processing and accounting systems), complex applications (i.e. decisional support systems) and the services produced in the Internet age (i.e. email, web sites, transaction processing systems) (Levy and Powell, 2004). Today, enterprises adhere to cloud computing technology, which is subject to a continuous development and it is considered the future and the improvement of Information and Communication Technology (ICT). While in 2000 the tendency of Small and Medium sized Enterprises (SMEs) was to migrate to the Enterprise Resource Planning (ERP) solutions (Adam and O'Doherty, 2000), today ICT assists to a trend of SMEs to migrate from the traditional SMEs to the SMEs based cloud. The migration of enterprises to cloud is because of the advantages offered by this technology, defined by Joe Weinmann (2011) as an acronym: *C*ommon, *L*ocation-Independent *O*nline *U*tility on-*D*emand service, on the Axiomatic Cloud Theory. However, simultaneously with the increased number of enterprises that adopt cloud computing, the challenges of enterprises to exploit cloud for their business objectives are growing as well. Thus, companies go through a holistic process in order to manage the implemented cloud services.

Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844
Vol. VI (2011), No. 1 (March), pp. 187-195

Using Fixed Priority Pre-emptive Scheduling in Real-Time Systems

D. Zmaranda, G. Gabor, D.E. Popescu, C. Vancea, F. Vancea

Doina Zmaranda, Gianina Gabor, Daniela Elena Popescu
Codruta Vancea, Florin Vancea
University of Oradea
Romania, 410087 Oradea, 1 Universitatii St.
E-mail: {zdoina,gianina,depopescu,cvancea,fvancea}@uoradea.ro

Abstract: For real-time applications, task scheduling is a problem of paramount importance. Several scheduling algorithms were proposed in the literature, starting from static scheduling or cyclic executives which provide very deterministic yet inflexible behaviour, to the so called best-effort scheduling, which facilitates maximum run-time flexibility but allows only probabilistic predictions of run-time performance presenting a non-predictable and non-deterministic solution. Between these two extremes lies fixed priority scheduling algorithms, such as Rate Monotonic, that is not so efficient for real-time purposes but exhibits a predictable approach because scheduling is doing offline and guarantees regarding process deadlines could be obtained using appropriate analysis methods. This paper investigates the use of Rate Monotonic algorithm by making adjustments in order to make it more suitable for real-time applications. The factors that motivate the interest for fixed priority scheduling algorithms such Rate Monotonic when doing with real-time systems lies in its associated analysis that could be oriented in two directions: schedulability analysis and analysis of process interactions. The analyzing process is carried out using a previously implemented framework that allows modelling, simulation and schedulability analysis for a set of real-time system tasks, and some of the results obtained are presented.
Keywords: real-time systems, fixed priority preemptive scheduling.

1 Introduction

Real-time systems are often safety critical and require a high quality design in order to obtain and guarantee the requested properties. The design process consists in building models on which the required system properties are assessed; based on this previously developed models an implementation that preserves these properties is further developed.

In order to develop a large-scale real-time system we must be able to manage both the logical complexity and timing complexity using a highly disciplined approach [10].The problem of dealing with logical complexity is addressed by the several existing software engineering general methodologies [11] while timing complexity represents an issue that is addressed by specific scheduling algorithms.

For real-time systems, two modelling approaches are known in the literature: first of it allows handling of traditional, periodically sampled control systems, and is represented by the so called timed-triggered approach; the second type of model deals with discrete event systems, and it is known as the event-triggered approach. If the main advantage of event-driven approach is flexibility and better resource utilization, the main advantage of time-driven approach is predictability.

Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844
Vol. V (2010), No. 4, pp. 558-566

Some Aspects about Vagueness & Imprecision in Computer Network Fault-Tree Analysis

D. E. Popescu, M. Lonea, D. Zmaranda, C. Vancea, C. Tiurbe

Daniela Elena Popescu, Doina Zmaranda, Codruta Vancea, Cristian Tiurbe
University of Oradea
Romania, 410087 Oradea, 1 Universitatii St.
E-mail: {depopescu,zdoina,cvancea,ctiurbe}@uoradea.ro

Madalina Lonea
"Politehnica" University of Timisoara
Romania, Timisoara, 2-4 V. Parvan Blvd.
E-mail: madalina_lonea@yahoo.com

Abstract: Based on the available information (eg.multiple functional faults or sensor errors give rise to similar alarm patterns or outcomes), some states in the behaviour of a network can not be distinguished from one another. So, the computer network's fault tree reliability analysis frequently relies on imprecise or vague input data. The paper will use a Dempster-Shafer Theory to accommodate this vagueness and it will show how imprecision can give rise to false-negative, and false-positive inferences; there will be assigned upper and lower bounds for the probability on elements of the state space. After illustrating the computational simplicity of incorporating the Dempster-Shafer Theory probability assignments, we will apply them for analyzing the reliability of the network of our department.
Keywords: reliability analysis, networks, Dempster-Shafer Theory, fault tree.

1 Introduction

The probabilities are no longer appropriate to represent vagueness in risk and reliability analyses; fuzzy set theory was proposed instead to quantify vagueness in this area [1]. Development in DST have shown how probability can be adapted to incomplete or vague information, especially information that is based on human judgment or human-machine interaction.

False positives and false-negatives are often the end products of vagueness or imprecision. They can arise from imprecision due to noise in monitored data, sensor device failure, or from the ambiguity about the logic rules in the fault tree.

So, when the researcher has only imprecise information, he must appeal to fuzzy-set theory techniques, either the common laws or logic his appreciation for the logic relations in fault trees. Fuzzy data can be incorporated through Dempster Shafer Theory (DST) [2] [3] [4] [5] in conventional fault-tree analysis yield meaningful results.

2 Dempster-Shafer Theory mass assignments

DST generalizes classical probability theory by assigning upper und lower bounds for probabilities, as opposed to point values, to both the elements and the subsets of the state space. For a given state space, Ω, mass (probability) is assigned over the set of all possible subsets of Ω. Because each element of Ω is also a subset of Ω (comprising 1 element) any classical probability assignment can be represented in DST. Just as the probabilities of a distribution sum to 1, so do the masses of a DST-distribution.

A PROPOSED CACHE LINE IMPLEMENTATION SOLUTION WITH ERROR/CORRECTING CAPABILITIES FOR MANAGING CACHE COHERENCY IN MULTIPROCESSOR SYSTEMS

Daniela Elena POPESCU
Department of Computers, Faculty of Electrical Engineering and Informatics Technology,
University of Oradea, no.1 University Str. 410087, Oradea, tel. 0040 723 268 428, e-mail: depopescu@uoradea.ro

ABSTRACT

The paper presents a solution for designing a cache coherency state machine for a multiprocessor system with error/correcting capabilities for the unidirectional errors and the used resources implied by a FPGA implementation of our solution. The cache coherency method used is based on the MESI protocol. The implementation is realized with FPGA by using the ALTERA Program.

Keywords: *cache memory, memory coherency, error detector*

1. CACHE COHERENCY

In contemporary multiprocessor systems, it is customary to have one or two levels of cache associated with each processor [1]. This organization is essential to achieve reasonable performance. It does, however, create a problem known as the *cache coherence* problem.

The essence of the problem is this: Multiple copies of the same data can exist in different caches simultaneously, and if processors are allowed to update their own copies freely, an inconsistent view of memory can result.

There are two common write policies:

Write back: Write operations are usually made only to the cache. Main memory is only updated when the corresponding cache line is flushed from the cache.

Write through: All write operations are made to main memory as well as to the cache, ensuring that main memory is always valid.

Hardware schemes differ in a number of particulars, including where the state information about data lines is held, how that information is organized, where coherence is enforced, and the enforcement mechanisms [2].

2. ERROR CORRECTION

A semiconductor memory is subject to errors. These can be categorized as hard failures and soft failures.

Both hard and soft errors are clearly undesirable, and most modern main memory systems include logic for both detecting and correcting errors [2] [3]. Fig. 1 illustrates in general terms how the process is carried out.

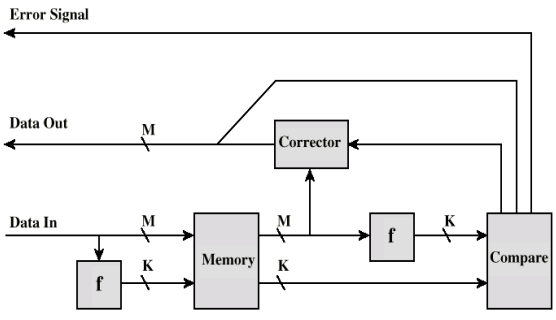

Fig. 1 Error-Correcting Code Function

When data are to be read from memory, a calculation is performed on the data to produce a code. Both the code and the data are stored. Thus, if an M-bit word of data is to be stored, and the code is of length K bits, then the actual size of the stored word is M+K bits. When the previously stored word is read out, the code is used to detect and possibly correct errors. A new set of K code bits is generated from the M data bits and compared with the fetched code bits. The comparison yields one of three results:

- No errors are detected. The sent data bits are sent out
- An error is detected, and it is possible to correct the error. The data bits plus error correction bits are fed into a corrector, which produces a corrected set of M bits to be sent out
- An error is detected, but it is not possible to correct it. This condition is reported

Codes that operate in this fashion are referred to as error-correcting codes [1] [4]. A code is characterized by the number of bit errors in a word that it can correct and detect.

To provide cache consistency on an SMP (Symmetric Multiprocessors), the data cache often supports a protocol known as MESI. For MESI, the data cache includes two status bits per tag, so that each line can be in one of four states:

- **Modified:** The line in the cache has been modified (different from main memory) and is available only in this cache.
- **Exclusive:** The line in the cache is the same as that in main memory and is not present in any other cache.
- **Shared:** The line in the cache is the same as that in main memory and may be present in another cache.
- **Invalid:** The line in the cache does not contain valid data.

Table 1 summarizes the meaning of the four states. Fig. 2 and Fig. 3 displays the state diagram for the MESI protocol. Each line of the cache has its own state bits and therefore its own realization of the state diagram. At any time a cache line is in a single state. If the next event is from the attached processor, then the transition is dictated

INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 9(4):453-462, August, 2014.

Cloud Service Management System for Innovative Clusters. Application for North-West Region of Romania

D. Popescu, A. Dodescu, P. Filip

Daniela Popescu, Anca Dodescu*
University of Oradea
Economy Department
Romania, 410610 Oradea, University Street, 1
depopescu@uoradea.ro
*Corresponding author: adodescu@uoradea.ro

Petru Filip
1. Dimitrie Cantemir Christian University,
Romania, 040042 Bucharest, Splaiul Unirii, 176
2. Agora University of Oradea,
Romania, 410526 Oradea, Piata Tineretului, 8
3. University of Oradea
Romania, 410610 Oradea, University Street, 1
pfilip@uoradea.ro

Abstract: 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, we propose a Cloud Service Management System (CSMS) that provides IT services for these innovative clusters companies that can be customized for both enterprises with the associated clusters.
Within such a system, actors begin to depend one on another and to take advantage of the local knowledge base. Each cluster is designed to have a different profile which will integrate all the companies mapped with it, with the objective of keeping the profile and data for each company. For the existing companies the idea is to migrate their services into the related cluster for integration within CSMS. Thus, our proposed CSMS will consider 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 CSMS. Realizing that technological progress is at 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 the North-West region of Romania.
Keywords: cloud computing, service oriented architecture, open cloud architecture, IT services, innovative clusters, supply chain management

1 Introduction

The paper proposes a *Cloud Service Management System (CSMS)* that provides IT services for the innovative clusters companies in order to develop collaborative mechanisms specific for innovative clusters aimed to solving the problems identified in the economic development of the North-West region of Romania.
Although in the past 20 years numerous studies have been conducted regarding the importance of innovative clusters for the regional economic development, the number of innovative clusters in Romania, in general, and in the North-West region, in particular, is surprisingly small, many of the existing clusters not being functional, due to lack of experience in organizing and managing