Insider Threat Mitigation in Cloud Computing

Rajashree Sahoo, Manoranjan Pradhan

Abstract— Insider threat is one in all the foremost crucial security threats for any trade, even it's the foremost eldest strategy to fall associate degree empire down, quite common in diplomacy per the human history. Within the cloud computing scheme there are many issues that's tougher than the conventional (not could) eventualities. If the corporate executive threats are the foremost dangerous threat even within the non-cloud platform then it should has multi-dimensional attack vectors in cloud computing Cloud Computing, that once provided domestically, has seen a technical and cultural shift of computing service provision to being provided remotely, and as a group, by third-party service suppliers. The info has currently been placed underneath the protection of the service supplier that was once placed underneath the protection domain of the service user. Cloud computing is associate degree raising technology paradigm, sanctioning and facilitating the dynamic and versatile provision of process resources and Services. Albeit the benefits offered by cloud computing are many there still exist second thoughts on the protection and privacy of the cloud services. Use of cloud services affects the protection posture of organizations and demanding infrastructures, thus it's necessary that new threats and risks introduced by this new paradigm are clearly understood and mitigated. During this paper we have a tendency to concentrate on the corporate executive threat in cloud computing. The target of this paper is to indicate that however a malicious corporate executive will steal confidential knowledge of the cloud user.

Index Terms— Cloud Computing, Security, Malicious Insider, Insider Threat, Counter Measure, Iaas, Saas, Paas.

1 Introduction

Organizations still embrace the benefits of flexibility, measurability, and management provided by cloud computing platforms and services, and infrequently considers security one among their high considerations in cloud environments. Basic nature of business executive threats can stay unchanged in very cloud surroundings. In cyber security analysis business executive threat could be a devious downside therefore in cloud computing. Though in cloud system users/customers don't concern concerning the situation and management of their information rather they a lot of concern concerning the safety (Confidentiality, Integrity and Authenticity) of the information unbroken within the cloud. The foregone conclusion business executive Threat Center defines a malicious business executive as a ″current or former worker, contractor, or different business partner World Health Organization has or had approved access to Associate in Nursing organizations network, system or information and on purpose exceeded or exploited that accessing a way that negatively affected the confidentiality, integrity, or handiness of the organizations info or info systems.″ [1]. In 2010, the Cloud Security Alliance (CSA) discharged high Threats to Cloud Computing, describing seven threat areas thought of most significant to organizations victimization cloud services, as well as malicious insiders [2]. The first Nineties, referring in the main to massive ATM networks Cloud computing began in earnest at the start of this century, simply many years past with the arrival of Amazon's web-based services. Next generation networks and repair infrastructures ought to overcome the measurability, flexibility, resilience and security bottlenecks of current network and repair architectures, so as to supply an outsized form of services and opportunities, adoptable by business models capable of dynamic and seamless utilization of IT resources supported user-demand across a multiplicity of devices, networks, providers, service domains and social and business processes. Cloud computing [3],[4] could be a new infrastructure readying surroundings that delivers on the promise of supporting on-demand services like computation, computer code and information access in a very versatile manner by programming information measure, storage and work out resources. in step with the office definition [5].

Service Models In Cloud Computing:

Cloud computing may be a delivery of computing wherever massively scalable IT-related capabilities are provided —as a service across the web to various external shoppers [6]. This term effectively reflects totally different the various aspects of the Cloud Computing paradigm which may be found at different infrastructure levels. Cloud Computing is normally classified into 3 services: —″IaaS", "PaaS" and "SaaS" [7].

IaaS (Infrastructure as a service) model:

The bottom layer is that the system layer, which has procedure resources like infrastructure of servers, network devices, memory, and storage. It's referred to as Infrastructure-as-a-service (IaaS). The procedure resources area unit created offered for users as on-demand services. With the employment of virtualization technology, IaaS provides virtual machines that enable shoppers to create advanced network infrastructures. This approach not solely reduces the value in shopping for physical instrumentality for businesses; it conjointly eases the load of network administration as a result of IT professionals isn't needed to unendingly monitor the health of physical networks. Example of a cloud computing service supplier of IaaS is Amazon's EC2.

PaaS (Platform as a service) model:

The middle layer is that the platform layer and is understood as Platform-as-a-Service (PaaS). It's designed to produce a development platform for users to style their specific applications. Services provided by this cloud model embody tools and libraries for application development, permitting users to own management over the applying readying and configuration settings. With PaaS, developers aren't needed to shop for computer code development tools, thus reducing the price. GoogleApps is associate degree example of PaaS; it's a collection of Google tools that has Gmail, Google teams, Google Calendar, Google Docs, Google speak, and Google Sites. It permits users to customize these tools on their own domain names. Windows Azure is another PaaS supplier. It allows users to create applications victimization varied languages, tools or frameworks.

SaaS (Software as a service) model:

The top layer is that the application layer, also renowned as Software-as-a-Service (SaaS). This layer allows users to rent applications running on clouds instead of paying to get these applications. Because of its ability to cut back prices, SaaS is popular among corporations that deploy their businesses. With the use of the web support solutions provided by Groupon, Zen desk processes its thousands of daily customer tickets a lot of expeditiously, thus providing a higher client service. Marathon Data Systems is another example that offers SaaS. It provides solutions for field services such as pest management, lawn and landscaping, heating, air conditioning, plumbing, janitorial, maid, and carpet cleaning services.

A severe threat, that modern data systems and crucial infrastructures got to address, is the insider threat. In general, the insider threat is outlined as a person United Nations agency has the suitable access rights to associate data system and misuses his privileges [8] [9]. A worker United Nations agency has been decides to attack his former leader for revenge. Although her access rights (should) have been revoked, and she isn't considered legitimate user any longer, if she still has access to the infrastructure considered associate corporate executive threat. Mitigation of this problem is typically sophisticated, as a corporate executive will focus on a range of target systems and orchestrates his attack actuated by variety of reasons [10], from personal profit to narcissism. To make things worse, the insider sometimes has the privilege of time, so as to study the knowledge system and deploy a heavy attack, which is terribly tough to predict and sight in due time.

In this paper we specialize in the insider threat in cloud computing, the ways it manifests, and the challenges in addressing the matter. Then, we recommend acceptable countermeasures in associate effort to mitigate the matter. We present the insider threat in 2 scenarios: a) the insider is from the side of the cloud provider; b) the insider works for an organization .The rest of the paper is organized in as follows: Section 2 describes related work on the insider threat. In Section 3, we define the problem and analyze possible attack scenarios. We conclude and present ideas for future work in Section 4.

2 RELATED WORKS

The research community has targeted on several aspects of cloud computing security, such as authentication and authorization, digital forensics; secure data storage, as well as legal challenges. However, the problem of the insider threat within the cloud has not nonetheless received visible analysis focus. The traditional corporate executive threat is being consistently studied for quite a decade [11]. It is considered a posh issue, and there are numerous approaches in order to mitigate it. Psychology and social science are helpful tools in the battle against the insider threat. They offer precious data regarding the motives and therefore the method of a possible within attack [12] [13]. Detection of malicious insiders is hard to assistant. Some systems have been proposed to sight corporate executive threat [14]. A useful tool within the method of corporate executive detection is intrusion detection systems (IDS) [15] [16], as they can sight abnormal actions, packets with illegal content and deviations from traditional user behavior. Another useful technique, used to mitigate the insider threat, is system call analysis [17], command sequences and windows usage events [18]. The techniques based on the usage habits of the users, namely the system calls analysis, belong to a larger family of techniques called “host-based user profiling”, while intrusion detection systems belong to the “network-based sensors” family [18] [19]. Insider threat prediction makes an attempt have used each user and usage identification, in order to end in a possible differentiation in user’s behavior. There are additionally approaches that take psychological, sociological and instructional parameters into consideration, along with technological ones [20] [21] [22].

3 INSIDER THREAT MITIGATION IN CLOUD ENVIRONMENTS

There are the technical and operational countermeasures deployed in an infrastructure, defending against accidental or malicious human actions are arduous to do. The insider threat affects just about each infrastructure and remains an open analysis issue for decades. As mentioned in section 2, there has been some research focusing on this drawback, with respect to traditional IT infrastructure, though the manifestation of corporate executive threat in cloud computing has not been adequately researched upon. Given the functional context of cloud computing, a malicious insider with access to cloud resources will cause considerably additional injury to the organization. Furthermore, as the attack can have an effect on an oversized range of cloud users, the impact of such attack will be important. In order to review the matter, we suggest that it should be studied in two distinct ways: (a) Insider threat in the cloud provider and (b) Insider threat in the cloud outsourcer.

3.1 Insider threat in the cloud provider

This is the primary case scenario for each cloud suppliers and cloud purchasers, i.e. a malicious system administrator working for the cloud supplier. Because of her business role within the cloud supplier, the insider will use her approved user rights to access sensitive information. For example, an administrator accountable for acting regular backups of the systems wherever consumer resources square measure hosted (virtual machines, data stores), could exploit the reality that she has access to backup sensitive user information. Depending on the insider’s motives, the result of such an attack during a cloud infrastructure can vary from information run to severe corruption of the affected systems and information. Either way, the business impact for the provider can be vital. All common cloud types (IaaS, PaaS, SaaS) are equally affected by business executive attacks as long because the insiders access the datacenters or cloud management systems.

3.1.1. Countermeasures:

Effective mitigation of the insider threat requires a large number of countermeasures, implemented by both cloud providers and clients.

Client side

- Confidentiality:

Even in IaaS, where purchasers have the most access to the cloud infrastructure, cloud clients are unlikely to observe that somebody has gained unauthorized access to their knowledge victimization OS level security mechanisms like IDS/IPS. The reason is that an business executive operating for the cloud supplier (e.g. a malicious administrator) has access to the physical infrastructure which is not controlled by the consumer. Clients will create use of crypto logical techniques [23], in an effort to safeguard the confidentiality and integrity of their outsourced knowledge. Storing data in encrypted kind associated decrypting them every time they have to be accessed against a business executive, as the decryption key needs to be keep somewhere within the cloud too. A robust resolution to the current downside isn't storing the encoding keys within the cloud however perform knowledge manipulation directly on encrypted knowledge. A number of techniques are projected in an endeavor to deal with this downside [24] [25] [26].However, the performance overhead of such techniques is them currently impractical for real world applications.

- Availability:

In availability, the use of multiple datacenters, ideally in different regions, is the only economical answer, assuming that the cloud supplier cannot face a worldwide outage. Multiple providers supply such Associate in nursing choice to their shoppers, switching to the backup datacenter, in case an instance within the primary knowledge center fails. Such technique protects the client as long as the malicious business executive cannot interfere with multiple datacenters at an equivalent time

Provider Side:

- Separation of duties:

Separation of duties for the provider staff and system directors is one of the foremost effective mechanisms for limiting the potential harm of such attacks. The insider can solely have specific access rights to the infrastructure, thus she can solely be ready to attack the systems will access. Nevertheless, such actions will increase the risk of detection of the assailant

- Logging:

All user actions, and especially actions of power users, such as administrators, have to be extensively logged and audited. Apart from acting as a deterrent measure for potential attackers, it will additionally alter early detection of doubtless malicious actions.

- Legal binding:

Legal binding can act as a deterrent live against a potential assaulter, as it may end up to civil penalties. However, there are many open legal problems, due to the very fact that a cloud infrastructure is sometimes supported by multiple data centers in numerous countries. As the cloud provider's attack may well be a special country than the physical location of the attacker, each legal or physical entity is subject to completely different frameworks of law and, thus, administration of justice becomes a complex issue [27].

- Insider detection models:

Insider detection models are enforced in the provider's infrastructure in an attempt to detect malicious workers are often terribly useful tools for prediction and in-time detection of insider attacks [20]. The models are based mostly on predicting malevolent actions, in order to accentuate monitoring of suspicious users.

TABLE 1
COUNTERMEASURES

Countermeasures	Countermeasures
Cryptographic techniques	Client
Geo-redundant data centers	Client and Provider
Separation of duties	Provider
Logging	Provider
Legal binding	Provider
Insider detection models	Provider

Client: Client side countermeasures, Provider: Provider site countermeasures.

3.2 Insider Threat in the Cloud Outsourcer:

In the second scenario, the insider is an employee of an organization, In the whole IT infrastructure into the cloud. Initially, this could be considered as a traditional insider problem. To solve this problem the models are used.

- Detection models:

Providers can use insider detection models for detecting malicious employees. However, the use of such models by the cloud client(s), who have outsourced their IT infrastructure, is problematic. As a potential malicious user accessing the cloud infrastructure, a detection model will have to correlate data from both the cloud infrastructure and the user workstation. As long as these models have not been applied or studied within the context of cloud computing, we can only speculate about the results. The first case scenario is that the prediction system will conclude in so many false positives/ negatives, that the results cannot be trusted. Therefore, for the time being the existing detection and prediction models and techniques are unable to operate in cloud infrastructures.

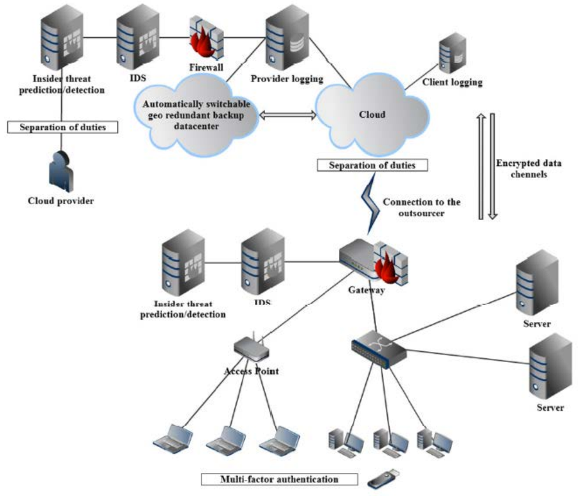
Insider threat prediction/detection
IDS
Firewall
Provider logging
Client logging
Automatically switchable geo redundant backup datacenter
Cloud
Separation of duties
Cloud provider
Separation of duties
Encrypted data chennels
Connection to the outsourcer
Insider threat prediction/detection
IDS
Gateway
Server
Access Point
Server
Multi-factor authentication

Fig. 1. Visualization of all security countermeasures versus insider threat.

In Fig. 1 we visualize number countermeasures of an early implementation model, in an effort to defend against malicious insiders. Risk analysis should be the first step before implementing such countermeasures, as depending on the risk profile of the organization, implementation of all countermeasures may be inappropriate and result in performance degradation.

•IDS:

Use of Intrusion Detection Systems (IDS), as a means of attack identification, is also problematic. Host based IDS can be used transparently in IaaS, as they usually require the installation of a software agent on the Operating System, which is under client's control. However, this is not an option in PaaS and SaaS, unless the cloud provider supports such mechanisms.

•Separation of duties:

In a traditional infrastructure there are well-defined user roles (system/network/database administrators, etc.) In the cloud, it is likely that the person who manages the cloud infrastructure is the same with the one that configures the firewall rules. This users can use Amazon Elastic Cloud (EC2), where configuration about every aspect of the virtual infrastructure is done using a simple web-based dashboard.

•Attack origin identification:

Traditionally, an authorized user wishing to access the data center of her organization needs to go physically on-site, sign in, and use specific access credentials.valid credentials for each system she wishes to access. This could be used to trace the origin of attack and act as evidence. VPN's may allow remote to the infrastructure remotely, but it is safe to assume that only a limited number of users will be granted remote access and strong authentication and monitoring will be in place. In comparison, gaining access to a virtual infrastructure on the cloud equals to getting access to the cloud console's access credentials used for managing the virtual infrastructure of the client. No physical evidence is available. The digital evidence will likely be the IP address, where the attacker logged in from.

•Single point of failure:

One important point is the criticality of the cloud management console. Access to such console gives the user complete control over the virtual infrastructure, enabling her to create new virtual systems, modify existing ones, clone systems and destroy virtual systems instantly. Termination equals to destruction of both the virtual machine instance (operating system) and any data stored in it. This action is catastrophic and could lead to vast money loss, as well as damages to the infrastructure [13].

•Data leakage:

Data leakage attacks are easier than to perform on a virtualized infrastructure. An attacker with access to the administrative console can exploit specific features of the virtual systems to her benefit, such as saving a snapshot of a particular system. Having acquired an image of the target system, she can modify it offline, circumvent the host's security mechanisms, and thus gain access to the data, while the original system will show no signs of intrusion.

3.2.1 Countermeasures:

Client Side

• Log Auditing:

Clients are used to need to the collected data and audit all log files from their cloud systems, including any SaaS Logs are invaluable in helping detect in time, an attack.

• Host based IDS:

Host based IDS should be installed on all sensitive systems hosted in the cloud (IaaS), as they enable clients to detect in time ongoing attacks and at the same time maintain a low false-positive rate. Until cloud aware insider detection models are developed, and it is most effective measure for mitigating the insider threat.

Provider Side

• Anomaly detection:

From the provider's side, anomaly detection mechanisms are used to identify abnormal behavior in client instances. The provider is then able to contact the client and inform her about the anomaly. The more data input the provider has, the better the chances are for detecting potential issues. For example, if a SaaS provider identifies that a user account of a client is used for querying a large number of records in the database, while the same account was regularly making only few queries per day, then she should escalate the issue to the client for investigation. This requires the implementation of anomaly detection systems by the Providers for monitoring client instances.

• Separation of duties:

Separation of duties is an effective mechanism for limiting the impact of an insider attack. Cloud providers should implement robust identity and access management mechanisms and enable the cloud clients to create multiple accounts and multiple access rights for their users. By supporting multiple accounts, the client can enforce separation of duties.

- Multi factor authentication:

Providers should support multi-factor authentication schemes in an effort to thwart phishing and password hijacking attacks against the cloud console management interface. Amazon EC2 is already supporting such mechanism, allowing clients to log in using certificates and OTP tokens.

TABLE 2
COUNTERMEASURES

Countermeasures	Countermeasures
Identity and Access management Client and Provider	Client and Provider
Multi factor authentication Client and Provider	Client and Provider
Log analysis and auditing Client	Client
IDS Client	Client
Insiderprediction/detection models	Client

Client: Client side countermeasures, Provider: Provider site countermeasures.

4 CONCLUSION AND FURTHER WORK

In this paper we discuss the insider threat in the cloud environment. The insider threat is a well-known open research problem for recent decades, and - whilst in traditional IT infrastructures a set of adequate countermeasures has been proposed - this is not the case with cloud environments. An insider attack in the cloud is easier to perform and has far greater impact than an attack in a traditional infrastructure. We identified two types of insider threat in cloud computing. The first is the one who works for the cloud provider. She could cause great deal of damage in both the Provider and its customers. The second is who works for the organization that decides to outsource. We described and documented the differences between the traditional insider and the insider in cloud. The paper has demonstrated the need for new insider prediction and detection models, to be used in the Cloud .We recommend a number of countermeasures, for both the cloud clients and providers, for each insider scenario. These should be implemented in-line with the needs of each organization.

Our future work will focus on the implementation and analysis of insider threat detection models for the cloud, analysis of users' habits in the cloud and behavioral analysis of cloud usage along with ways for the providers to offer security as a service within the cloud..

REFERENCES

[1] D. *Cappelli*, A. *Moore*, and R. *Trzeciak*, *The CERT Guideto Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*, ser. SEI Series in Software Engineering. Addison-Wesley Professional, 2012.

[2] C. S. *Alliance*, "*Top threats to cloud computing, version1.0*," Cloud Security Alliance, Tech. Rep., March 2010. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[3] "*Star-205 cloud security alliance - top threats to cloud computing v2.0.pdf*," in RSA Conference Europe, 2010. [Online]. Available: http://365.rsaconference.com/docs/DOC-2819

[4] C. *Braun*, M. *Kunze*, J. *Nimis*, and S. *Tai*. —"*Cloud Computing, Web-based Dynamic IT-Services*". Springer Verlag, Berlin, Heidelberg, 2010.

[5] Peter *Mell* and Tim *Grance*, —'*The NIST Definition of Cloud Computing*, NIST Report‖, July 2009.

[6] Thepparat T., *Harnprasarnkit* A., *Thippayawong* D., *Boonjing* V., *Chanvarasuth* P., —‖A Virtualization Approach to Auto-Scaling Problem‖, Eighth International Conference on Information Technology: New Generation (ITNG), 2011.

[7] Liang-Jie *Zhang*, Carl K. *Chang*, Ephraim *Feig*, Robert *Grossman*, —*Business Cloud: Bringing The Power of SOA and Cloud Computing*‖, *2008 IEEE International Conference on Services Computing* (SCC 2008), pp.xix, July 2008.

[8] Theoharidou M., *Kokolakis* S., *Karyda* M., *Kiountouzis* E., "*The insider threat to Information Systems and the effectiveness of ISO 17799*", Computers & Security, Vol. 24,No. 6, pp. 472-484, 2005.

[9] Bishop M., *Gates* C., "*Defining the Insider Threat*", in Proc. of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, Tennessee, Vol. 288, 2008..

[10] Shaw E., *Ruby* K., *Post* J., "*The insider threat to information systems: The psychology of the dangerous insider*", Security Awareness Bulletin, Vol. 2, pp. 1-10, 1988.

[11] *Anderson* J., "*Computer security threat monitoring and surveillance*", Technical Report, J. Anderson Company, Pennsylvania, 1980.

[12] *Theoharidou* M., *Kokolakis* S., *Karyda* M., *Kiountouzis* E., "*The insider threat to Information Systems and the effectiveness of ISO 17799*", Computers & Security, Vol. 24, No. 6, pp. 472-484, 2005.

[13] Shaw E., *Ruby* K., *Post* J., "*The insider threat to information systems: The psychology of the dangerous insider*", Security Awareness Bulletin, Vol. 2, pp. 1-10, 1988.

[14] Thompson P., "*Weak models for insider threat detection*", in Proc. of the Defense and Security Symposium, Florida, 2004.

[15] Dropbox: Yes, We Were Hacked, August 2012. http://gigaom.com/cloud/dropbox-yes-we-were-hacked/

[16] *Nguyen* N.T., *Reiher* P.L., *Kuenning* G., "*Detecting Insider Threats by Monitoring System Call Activity*", in Proc. of the IEEE Workshop on Information Assurance, pp. 45-52,2003.

[17] Salem M., *Hershkop* S., Stolfo S.J., "*A Survey of Insider Attack Detection Research*", Insider Attack and Cyber Security, Springer, 2008, Vol. 39, pp. 69-90, 2008.

[18] *Lekkas* D., *Gritzalis* D, "*Long-term verifiability of healthcare records authenticity*", International Journal of Medical Informatics, 76(5-6), pp. 442-448, 2006.

[19] *Kandias* M., *Mylonas* A., *Virvilis* N., *Theoharidou* M., *Gritzalis* D., "*An Insider Threat Prediction Model*", In: Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business, pp. 26-37, LNCS-6264, Springer, Spain, 2010.

[20] *Gritzalis* D., *Theoharidou* M., *Kalimeri* E., "*Towards an interdisciplinary information security education model*", in Proc. of the 4th World Conference on Information Security Education (WISE-4), Moscow, May 2005.

[21] *Lambrinoudakis* C., *Gritzalis* D., *Tsoumas* V., *Karyda* M., *Ikonomopoulos* S., "*Secure electronicvoting: The current landscape*", in Secure Electronic Voting, Gritzalis D. (Ed.), pp. 110-122, Kluwer, USA 2003.

[22] *Iliadis* J., *Gritzalis* D., *Spinellis* D., *Preneel* B., *Katsikas* S., "*Evaluating certificate status information mechanisms*", in Proc. of the 7th ACM

Computer and Communications Security Conference (CCS-2000), pp. 1-9, ACM Press, October 2000.

[23] *Claessens*, J., *Preneel*, B., *Vandewalle*, J., "(*How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions*", ACM Transactions on Internet Technology, Vol. 3, No. 1, pp. 28-48, 2003.

[24] *Mather*, T., *Kumaraswamy*, S., *Latif*, S., "*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)*", O'Reilly Media, USA, 2009.

[25] *Mylonas* A., *Dritsas* S, *Tsoumas* V., *Gritzalis* D., "*Smartphone Security Evaluation – The Malware Attack Case*", in Proc. of the 8th International Conference on Security and Cryptography (SECRYPT-2011), pp. 25-36, Spain, July 2011.

[26] *Parrilli* D. "*Legal Issues in Grid and Cloud Computing*", In: Stanoevska-Slabeva K., Wozniak T., Ristol R., "Grid and Cloud Computing: A Business Perspective on Technology and Applications", pp. 97-118, Berlin, Springer, 2010.