A Parametric Analysis of Cloud Computing Security Models and Threats

Ashish Kumar Gaur
Computer Science and Engineering
Krishna Institute of Engineering and Technology
Ghaziabad, India

Poonam Rana
Computer Science and Engineering
Krishna Institute of Engineering and Technology
Ghaziabad, India

Vineet Sharma
Computer Science and Engineering
Krishna Institute of Engineering and Technology
Ghaziabad, India

ABSTRACT
Cloud computing is a resource sharing paradigm through the Internet. Cloud computing provides the sharing of data, application and also provide the communication among the users. Universal example of cloud services are Microsoft SharePoint and Google apps provided by Google. The cloud computing field is growing rapidly but still there are some security concerns. Lack of security is the only obstacle in wide acceptance of cloud computing. The cloud computing has brought lots of security challenges for the consumers as well as for the service providers. How will the users come to know that their information is not having any availability and security issues? This study aims to find out the most appropriate security model for cloud computing to resolve the maximum of the security threats in cloud computing.

Keywords
Introduction; security threats; security models;

1. INTRODUCTION
The cloud computing has become quite popular for its various range of advantages in different areas such as minor costs, rapid elasticity , ubiquitous network access , disaster recovery ,rapid process, data storage solutions, scalability ,remote mirroring , on demand security measures. Several challenges exist in the cloud computing such as security ,network spoofing and many others[1].

The core idea of cloud computing is to provide the virtualization among the computing environment by centralizing all the resources. Fig(1)[3] represents the cloud architecture as there are 4 deployment models (hybrid cloud, private cloud, community cloud, public cloud), 4 service models (IaaS, SaaS, PaaS and DRaaS) and 5 essential features (On-Demand Self-Service, Measured Service, Broad Network Access, Rapid Elasticity and Virtualized Computing Environment and Resource Pool) described in NIST definition of cloud computing .[5]

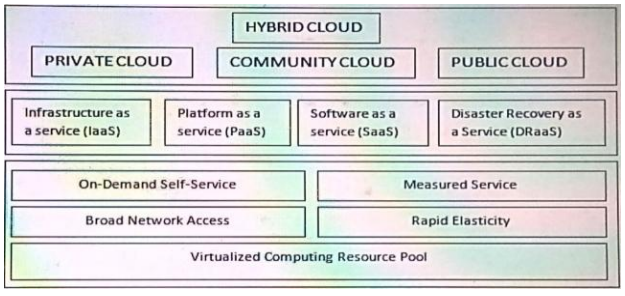

Figure 1 : The Cloud Computing Model

2. CLOUD SERVICE MODELS
2.1 Infrastructure as a service
In IaaS, the service provider provides a infrastructure as a user can develop its own software application without managing the network and hardware. E.g. Amazon , Window Azure.[2]

2.2 Platform as a service
In PaaS, the service provider provides a computing platform and users develop and run their software without managing the programming language execution environment , O.S. , database and web server. E.g. SQL Azure, Google apps.[2]

2.3 Software as a service
In SaaS, the service provider install and operate application software in cloud and a user access the software without managing the cloud infrastructure and platform where the application is running. User can do only user specific application configuration settings. E.g. Gmail, yahoo.[2]

2.4 Disaster Recovery as a service
In DRaaS, the cloud computing is basically used to protect an application or data from natural or human disaster by enabling full recovery in cloud.

3. CLOUD DEPLOYMENT MODEL
3.1 Public cloud
Public cloud is basically based on the facilities offered to the general public, it is managed by the cloud provider and access rights and permissions is fully depend on provider. The users who uses this public cloud they are not tied up to any organization hence those users are considered to be un-trusted users[2].

3.2 Private cloud
Private cloud relates to a single user entity. A user creates its cloud and do not share the resources and data with other cloud. Its infrastructure can be owned by an organization. Private cloud users are trusted users because whether those users are the employee of that organization or attached to that organization on agreement basis[2].

3.3 Community cloud
A community of organizations establish a community cloud , where the data and resources are shared among those organizations. The users of community cloud are trusted users because those users are the part of organizations[2].

3.4 Hybrid cloud
Hybrid cloud is a arrangement of public , private and community cloud. The users in Hybrid cloud may be trusted users or un-trusted users. The trusted users can access any data

or any resource available in hybrid cloud but the un-trusted users are permitted only to access the data or resources in private cloud.[2].

4. CLOUD SECURITY THREATS

Cloud Computing also comes with some challenges and security threads.

4.1. Vulnerability in virtualization

Virtualization is one of the important component of cloud and it also contains some security issues.

The core job of virtualization is to assure that the different items operating on the same physical machine are isolated from each other. Which do not meet completely in today's scenario.[1]

4.2. Fault Tolerance and service availability

In cloud computing, user data is stored on the cloud server managed by others. User may suffer with the issue of data unavailability , if there is some kind of system failure at remote side.[9]

4.3. Data Migration

Data migration means to copy data from one data server to other. A user that adopts a cloud computing do not want that his data should be migrated, for the reason of data security.[9]

4.4. Data Confidentiality and Integrity

Using a cloud computing , a user's data is stored on the cloud server and all kind of modifications by several application is done at cloud site . Keeping data in cloud, a user may lose the control over the security of data, data is stored remotely and user may not prevent any unauthorized access or malicious modification in data. [9]

4.5. Load balance

Load balancing is used to implement the failovers in cloud computing . All components of cloud are remotely monitored and when any of the component stop working or become non responsive , the load balancer is informed to stop sending data traffic to that non responsive component. Load balancing also enable the important features as scalability.[10]

4.6. Interoperability

Interoperability is needed to share the applications among the several clouds for any specific critical business application. Cloud Computing is purely based on users, most of time users are fine with this but they have data security issue in their minds.[10]

4.7. Scalable Data Storage

Cloud service allows users to put their data over the cloud having no worry about data storage and data backup. If a user is storing its data on a cloud , it means user need 2 basic features for its data - security and reliability. A user should be able to access its data any time and data should not be loosed to anyone else.[10]

4.8. Performance and Latency

The Latency [12,13] is an issue in cloud with flow of data among clouds. The other latency factor is cryptographic process over data when data moves through the untrustworthy network.

System performance is also a major issue that must be taken into account. Sometimes the service provider's run out of efficiency either by reaching upper throughput threshold over the internet links because of high demand from user's side or by allowing access to many virtual machines . This hurts system performance.

4.9. Motility of data and data remnants

To make best use of all resources , data is sometime moved to other server in cloud, means the data owner may always not know where the data is actually stored. It is practically true in public cloud. Cloud providers enhance the resource usage to offer best cost saving, but cloud provider do not provide any information how the resources are shifted.

When the data is moved to other location , data remnants may be left behind and may be used by unauthorized users. So data remnants must be removed but due to the security procedure, data loose ends may remain. It may be a concern with sensitive data in public cloud.[15]

4.10. Shared , Multi Tenant Environments of the Public Cloud

The multi user (tenant) architecture and provider control the data access security concern in cloud computing. A user in multi occupant architecture should not be able to use other users or tenants data. Whether the cloud service provider employees do not view the business data then , encryption may be a critical safe guard in the multi occupant environment. [15]

5. SECURITY MODELS OF CLOUD COMPUTING

5.1. Separation Model

Figure 2 reveal a possible design of separation model. It is based on the idea to have separate services which are responsible for data processing and data storage. Cloud users consist of data and it is further processed by the data processing service. For the storage of the data, the data is handed to the cloud storage service and this service will make the data persistent and ready for retrieval in the future [9].

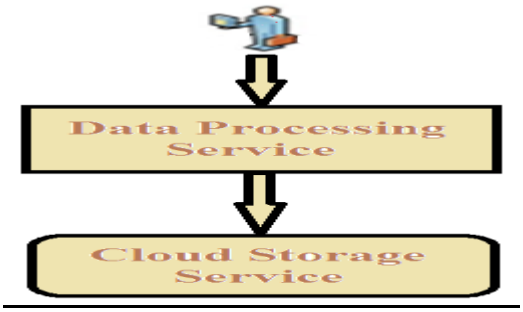

Figure 2 : Separation Model

5.2. Availability Model

Figure 3 reveal a possible design of availability model built over the cloud infrastructure. With this availability model, a user can process its data via a data processing service, and data will be kept on a cloud storage service. To make sure the availability of the services, there are at least two autonomous data processing services, data processing service A and data processing service B respectively, and two autonomous data storage services, cloud storage service C and cloud storage service D respectively[9]. Both cloud storage services are connected through a replication service between them. This replication service ensures that data can be accessed on either the cloud storage service by any of the data processing service.

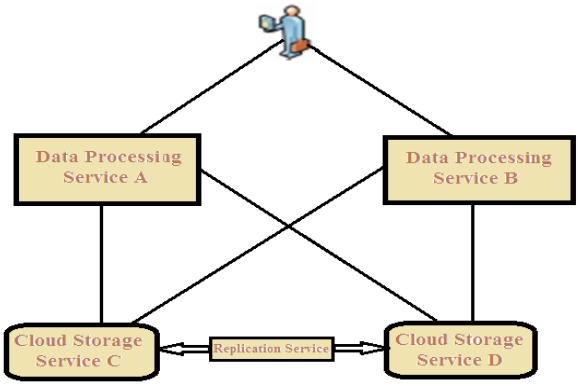

Figure 3 : Availability Model

5.3. Migration Model

Figure 4 reveal a possible design of Migration model where there data will surely be migrated. Cloud customers process their data using a Data Processing Service, and the data are stored on Cloud Storage Service A. The Cloud Data Migration Service is interactive with both Cloud Storage Service A and Cloud Storage Service B. The data is transferred from cloud storage service A to cloud storage service B using the cloud migration service. When the data is moving between Cloud Storage service A and Cloud Storage Service B, cloud users need not worry about their data because the data is kept safe and controlled by cloud provider[9].

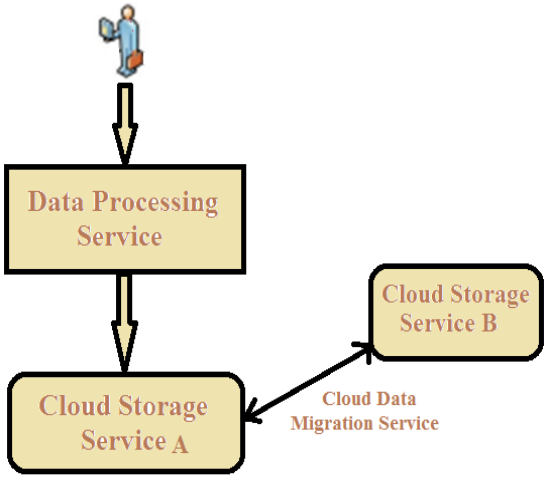

Figure 4 : Migration Model

5.4. Tunnel Model

Figure 5 reveal a possible design of the Tunnel Model. In this model, a tunneling process is activated between the data processing service and data storage service. This tunnel works as a communicator between the Data Processing Service and the Cloud Storage Service. The tunnel is accountable to provide a way between two services to manipulate and retrieve the data. Means the basic core work of tunnel between 2 services is to ensure that, the Data Processing Service will access the relevant data from the Cloud Storage Service [9].

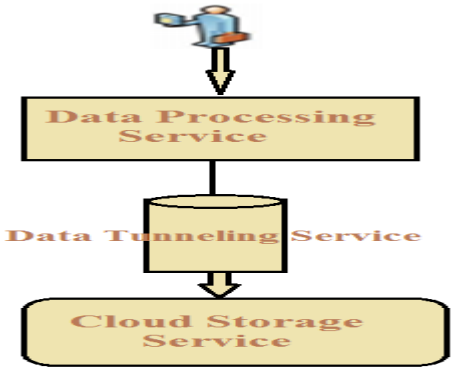

Figure 5 : Tunnel Model

5.5. Cryptography Model

Figure 6 reveal a possible design of the cryptography model. It is an enhanced version of the tunnel model with an extra function, cryptographic operation on data elements. The tunneling provides the interface between the Data Processing Service and Cloud Storage Service , when the data is accessed by Data Processing Service on cloud user's request from the Cloud Storage Service. The data goes through the tunnel and the cryptography service is applied on the tunnel. Hence the data retrieved from Cloud Storage Service will go to Cryptographic Service first and will be transformed into cipher text via data encryption technique using private or public keys. The data is transferred to cloud user via Data Processing Service. Now only a valid user can access the data by decrypting the data using the particular key. This tunnel hides the cryptographic operations from the Data Processing Service and Cloud Storage Service. Cryptographic operations will offer enhanced data protection for data access [9].

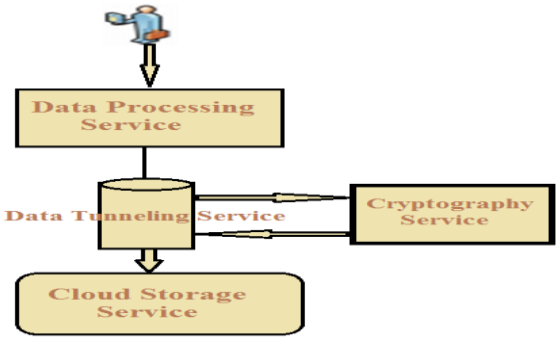

Figure 6 : Cryptography Model

5.6. The Cloud Multiple tenancy Model of NIST

Multiple Tenancy[8] basically means to allow multiple applications of cloud providers presently running in a physical server to offer cloud service for users. The cloud user process are divided in physical server using virtualization. Multiple virtual machines (VMs)[6] are used for virtualization in physical memory to share resources among various users. Different user applications run in different VMs, to separate virus, intrusion and faults of one from other VMs.

Difficulties with this model are data isolation, design extension, configuration self definition and performance customization. Software as a service with this model has 2 core features ,

5.6.1. Based on the web services provided, it is rather easy to scale-out and scale-up to serve to a no of users presently operating in the cloud

5.6.2. It provides the additional business logic which has the extended service platform for its customers while satisfying the needs of larger enterprises.

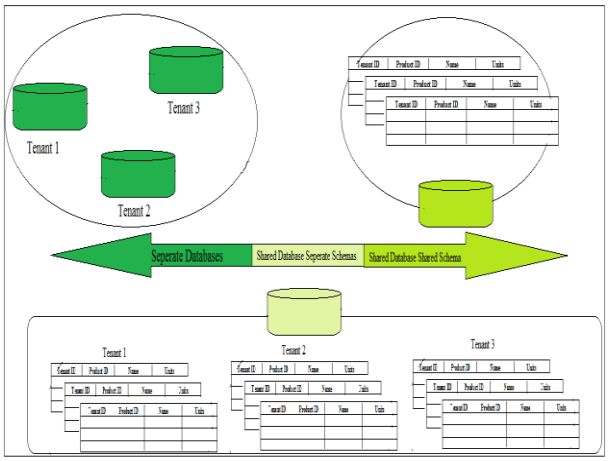

Figure 7 : Multi Tenant Model

5.7. Jerico Formu's Cloud Cube Model-

The security attribute information implied in the service and deployment models of cloud computing[5] is described in the model. Jerico Formu's cloud cube model is a figuration of combination of physical data location of resources , managers of resources , attribute details of management , cloud service model and deployment models of cloud computing [11].

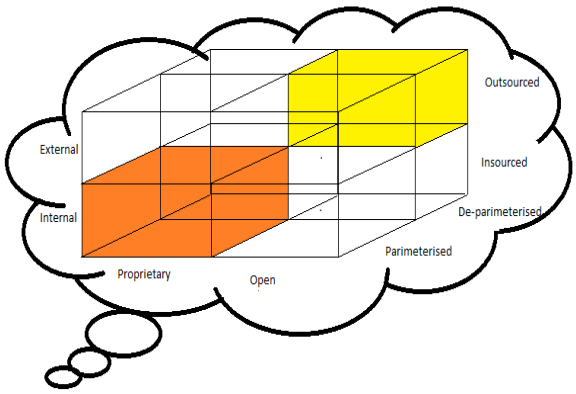

Figure 8 : Jerico Formu's Cloud Cube Model

The model parameters are

5.7.1. Internal/External-

This parameter allows where the actual data needs to be stored. The model parameter is said to be external if the owner data is located outside the boundaries of owner data and vice versa. The data stored in external physical location is more secure then the data in internal physical loc. To provide the best security for the data we should use the combination of internal and external physical locations [11].

5.7.2. Proprietary/Open-

This parameter is used to define the proprietorship of cloud's services. The level of interoperability can be defined under this parameter (the capability to transmit data from1 model to another without any constraints). A private cloud has the access rights of facilities controlled by a cloud service provider ,which can be termed as proprietary and data sharing among cloud may be restricted by the owner of cloud service provider. A public cloud is termed as open and uniform because the data sharing is done with minimal no of constraints and more availability of service provider[11].

5.7.3. Parameterized/De-parameterized-

This parameter is used to define the architectural structure of security protection , that proposes where the customer application is running in the traditional security boundary or outside the traditional security boundary [11].If the customer's application operates within traditional IT security boundary signaled by firewall that blocks the incorporation of different security zones it is said to be parameterized. De-parameterized means the disclosure of a customer's application operation [5].

5.7.4. In-sourced/Out-sourced:

This parameter is used to define the 4th dimension that has two states in each of the eight cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). In-sourced means that employees of the organization presents the cloud service , and Out-sourced means that third party is involved for the representation of cloud services.

5.8. The Cloud Risk Accumulation Model of CSA

By the layer dependency of cloud service, it is too hard to determine the security risks of cloud. As Platform as a service layer is built upon Infrastructure as a service layer and Software as a service layer is built upon Platform as a service layer, this shows the relationship among service capabilities of different layers in cloud computing, and the security risks are also inherited between service layers [5].

- Infrastructure as a service layer provides no distinctive function similar to application service but it provides maximum extensibility for users. IaaS provide the functionality to the user for the security of data , applications and operating system etc [5].
- Platform as a service layer provides us with the power of developing customized applications based on the PaaS platform for its users and with extra flexibility and extensionality to implement additional security than SaaS [5].
- Software as a service layer provides the least customer extensibility, but the most highly integrated service and security among 3 service layers. Users does not pay extra effort on security in the SaaS layer [5].

5.9. The mapping model of cloud, security and compliance

This model compares and checks recent good method to find out the spaces between cloud architecture and compliance framework and the corresponding security control strategies that are provided by cloud service providers, customers figure 9. This model contributes to determine the situation, whether accept or refuse the security risks of cloud computing [5].

This model initially checks the security risks in cloud environment and then it finds the gap matrix according to the cloud architecture and cloud compliance framework and then it uses some good security controls.[2]

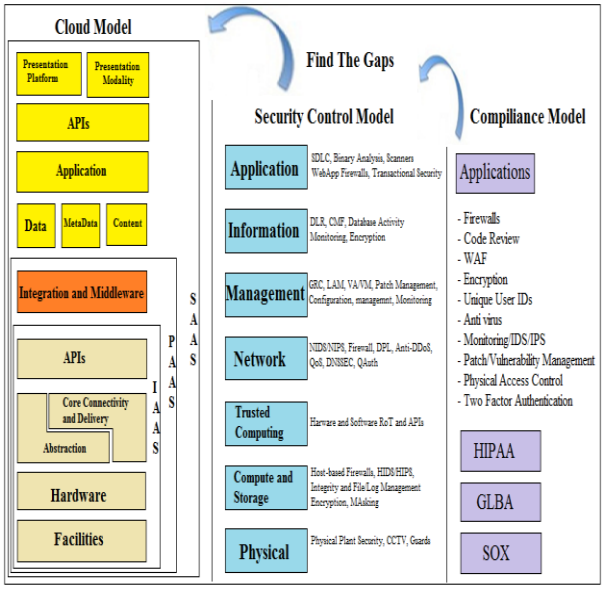

Figure 9 : Mapping Model

5.10. Multi Cloud Database Model

Multi Cloud database model [9] represents the cloud with database storage in multi cloud service provider. It does not provide security for single cloud database , security and privacy of data will be provided by implementing a shared database by multiple cloud provider. By doing so ,it reduces the security risk in cloud computing environment and minimizes the negative impact of data encryption techniques.

This Model uses a secret data sharing approach to replicate data among several cloud , this schema provide more security and privacy to user data. To control the operations performed between users and cloud providers, this model perform actions on data source.[8]

6. CONCLUSION

In this study different security and privacy related research papers were studied . Cloud computing services are used equally by larger and smaller scale enterprises. Cloud computing has both advantages as well as disadvantages. Security is the key problem in cloud computing and cloud computing is suffering from harsh security threats from customer point of view as fault tolerance and service availability, data migration, data confidentiality and integrity, scalable data storage, performance and latency and many more. For these security threats , we have also some security models which try to model the cloud computing infrastructure as a secure infrastructure. These models have some disadvantages and are not providing the complete security to user's data. A comparison of all those models are as…

Table 1 : Comparison Of All Models Discussed Above

Sr no.	Model Name	Technique Used	Advantage	Disadvantage
1	Cloud Multiple tenancy model of NIST	Virtualization	Resources are shared among various users	Data isolation , architecture extension , configuration self definition.
2	Jerico Formu's Cloud cube model	Cloud in cubic form	Figuration description of resource owner , controller , location , service and deployment model	Difficult to feed data in form of cube due to large no of parameters.
3	The Cloud Risk Accumulation Model by CSA	Relationship among SaaS , IaaS and PaaS	Shows the layers dependencies.	Understanding layer dependencies is critical to analyze security risk of cloud computing.
4	The mapping Model of Cloud , Security and Compliance	Analyze security risks, find gap matrix and its compliance	Contribute to determine whether accept or reject security risk of cloud computing	Compliance from work of cloud computing is not naturally existed with in cloud model
5	Multi Cloud Data Base Model	Data replication	Reduce security risk in cloud	Does not provide security for single database.
6	Separation Model	Different service for data processing and data storage	Prevent frauds and errors by preventing one single service provider	Service provider are dependent to each other.
7	Availability model	Data replicated and synchronized via replication service	Provide data redundancy	Built up between at least 2 independent data processing service
8	Migration model	Migration of data	No loss of data because data is controlled by cloud provider	Costly , time consuming
9	Tunnel model	Tunneling between 2 data services	Work as a communication channel between 2 data services	Tunneling technique should be good for all data services
10	Cryptography model	Encryption and decryption using key or digital signature	Increase the data confidentiality	Overhead to encrypt and decrypt

7. REFERENCES

[1] S. Subashini , V. Kavitha , " A Survey on Security issues in service delivery models of cloud computing ", Journal of Network and Computer Application , ELSEVIER , 2011

[2] Ritesh G. Anantwar , Dr. P.N. Chatur , Swati G. Anantwar, "Cloud Computing and security models : A Survey", IJESIT , Vol. 1 , Issue 2, November 2012.

[3] Peter Mell, Timothy Grance. "The NIST Definition of Cloud Computing (Draft)". NIST. 2011.

[4] AlZain, M.A.; Soh, B. , Pardede, E. "MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. Dependable, Autonomic and Secure Computing (DASC)". IEEE Ninth International Conference on , vol., no., pp.784,791, 12-14, 2011.

[5] Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan, "Study on the security and strategies of cloud computing" , International Conference on Power Electronics and engineering Application, Elsevier ,2011

[6] "VMware. Inc. Understanding full virtualization, paravirtualization and hardware assist. Technical report", VMware, 2007.

[7] "Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing(v2.1)." December, 2009.

[8] Barindar Kaur and Sandeep Sharma , "Parametric Analysis of Various Cloud Computing Security Models" , International Journal of Information and Computation Technology , ISSN 0974-2239 vol. 4, Number 15, 2014.

[9] Gansen Zhao , Chunming Rong , "Deployment Models : towards Eliminating Security concerns from Cloud ", International Conference on High Performance Computing and Simulation , IEEE , ISBN 978-1-4244-6828-7 , 2010.

[10] Bhaskar Prasad Rimal , Eunmi Choi , Ian Lumb , "A Taxonomy and Survey of Cloud Computing Systems ", 5th International Joint Conference on INC, IMS and IDC , 2009.

[11] Rohit Bhadauria , Ritu Chaki , Nabendu Chaki , Sugata Sanyal , " A survey on Security Issues in Cloud Computing ", ACTA TECHNICA CORVINIENSIS - Bulletin of Engineering , ISSN : 2067 - 2809 , Fascicule 4 [October - December] , Tome VII [2014]

[12] Neal Leavitt, "Is Cloud Computing Really Ready for Prime Time?" IEEE Computer Society, CA, USA, Computer, vol. 42, issue. 1, pp. 15-20, ISSN: 0018-9162, January 2009.

[13] Robert Minnear, "Latency: The Achilles Heel of Cloud Computing,",

[14] Cloud Expo: Article, Cloud Computing Journal, March 9, 2011, http://cloudcomputing.sys- con.com/node/1745523.

[15] Mohamed Al Morsy , John Grundy and Igno Muller , " An Analysis of The Cloud Computing Security Problem ", 17th Asia - Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop , Sydney , Australia , 30 November - 03 December 2010.

[16] Virtualization and cloud computing : Security Threats to evolving data centers, Trend Micro.

[17] G. Zhao, et al., Deployment models: Towards eliminating security concerns from cloud computing. in: Int. Conf. on High Performance Computing and Simulation (HPCS), June 28 - July 2, 2010, Caen, France, pp. 189 – 195.