IJCSC Volume 4 • Number 2 September 2013 pp.116-123 ISSN-0973-7391

An Overview of Distributed Data Base Security issues in Cloud Computing Environment

Ambika Gupta, Dr. Arun Kumar Yadav
M. Tech. Scholar, Banasthali University, Jaipur, Rajasthan, India
Asst. Prof., ITM University, Gwalior, M.P., India
ambikagupta2007@gmail.com, arun26977@rediffmail.com

ABSTRACT
Cloud computing is a computing paradigm that delivers on demand IT services to consumers. It is a technology which provides development of large-scale, on-demand, flexible computing infrastructures. It is a construct that allows users to access applications that actually reside on Internet-connected devices. It delivers applications, infrastructure and platform as a service over the internet. These services can be accessible through the internet from the web browser and desktop with the end user. But without security embedded into cloud computing, businesses are setting themselves up for a fall. There are so many essential concerns for both cloud providers and users such as Confidentiality, Integrity, Availability, Authenticity and Privacy. Lack of security in this model will certainly affect the performance of the cloud computing environment. This paper presents an elaborated study of the distributed database security in cloud computing environment and investigated the security risks and vulnerabilities associated with it and also we will discuss the securityissues in cloud computing including storage security, data security, network security and virtualization.

Keywords
Cloud Computing, Security, Privacy, reliability, Infrastructure As a Service (IaaS) and Distributed Database.

1. INTRODUCTION

Clouds are the large pool of resources that includes storage, servers, database, network and software, whereas computing is the activity of using these resources. Cloud computing paradigm provides reduced investment, expected performance, high availability, scalability, accessibility and mobility. A Cloud database management system is a distributed database that delivers computing as a service instead of a product. It is the sharing of resources, software, and information between multiple devices over a network which is the internet. It is probable that this number will grow significantly in the future because of user increases day by day. So that, it is required that outsourcing database management tasks to secure the cloud computing environment. Here a system will be to identify the risks (threats and security vulnerabilities) present for having database in a cloud environment as well as to provide guidelines for managing database security in the cloud and to prevent the associated risks. The results of this paradigm will be useful for the planning and building up the future of IT-infrastructure.

World's largest GIS Cloud infrastructure providers are Amazon (Amazon EC2 & S3), Microsoft (Microsoft Windows Azure, Windows Server Hyper-V), and IBM (IBM Cloud) which provide reliable and secure cloud IT infrastructure to the customer's on-demand [1]. Unliketraditional IT, Cloud users typically have little vision or control over the underlying infrastructure, and they must interact with the computing and storage resources via an Application Programming Interface (API) provided by the Cloud vendors.There will be no limit to storage space and no fixed number of servers. Their number can increase or decrease as the database grows or shrinks. Therefore by using internet as backbone the physical data position need not be known and database can be accessed from anywhere as cloud services and storage are accessible from anywhere in the world over an internet connection [2]. This document gives an introductory descriptionof the work will be to identify the risks (threats and security vulnerabilities) present for having database in a cloud computing environment as well as to provide guidelines for managing database security in the cloud and to prevent the associated risks. We also present here distributed database security in cloud computing platform. This ensures secure communication system and hiding information from others.

2. OVERVIEW OF CLOUD COMPUTING

Cloud computing is 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) and ubiquitous access that can be rapidly provisioned and released with minimal management effort or service provider interaction [3,4,5]. Cloud computing framework includes characteristics, service models and deployment models in cloud computing paradigm as shown in figure 1.

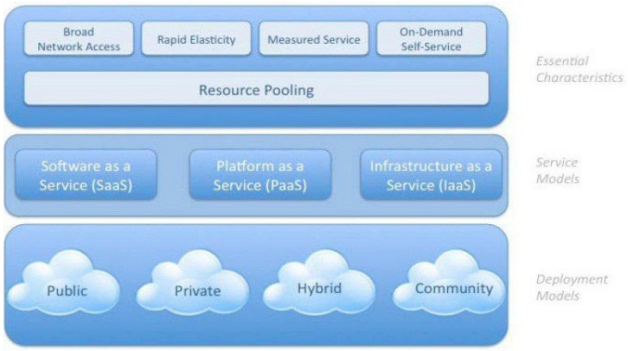

Fig 1: Cloud computing framework

2.1.1 Location Independent Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. In this customer has no knowledge about the exact location of the provided resources but may be able to specify location at a higher level of abstraction. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

2.1.2 Rapid Elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. The user can access as much or as little a service as per the need.

2.1.3 Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

2.2 Service Models of Cloud Computing

In cloud system, there are three Service/Delivery Models.

2.2.1 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. It is a complete operating environment with applications and management. Some providers of Software as a Service are Google Apps, Salesforce.com, and SQL Azure etc.

2.2.2 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. It provides virtual machines, applications, services, deployment frameworks and control structures. The service providers are Force.com, Google App Engine and Windows Azure Platform.

2.2.3 Infrastructure as a Service (Iaas)

IaaS provides virtual machines, virtual storage and virtual infrastructure. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating system, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). Amazon Elastic Compute Cloud(EC2) provides Infrastructure as a Service.

2.3 Deployment Models of Cloud Computing

Cloud computing environment have three deployment models.

2.3.1 Private Cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. Private clouds offer some of the benefits of a public cloud computing environment such as elastic on demand capacity. Services in private cloud like virtualization, multi tenancy, security and access control.

2.3.2 Community Cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. Community cloud is one where the cloud has been organized to serve a common function.

2.3.3 Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. These clouds include infrastructure services offered by companies such as Amazon, Go grid etc. and platform services such as Microsoft Azure, Google App Engine etc.

2.3.4 Hybrid Cloud

A hybrid cloud allows elasticity, pay per use, network isolation and secure connectivity. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

2.4 Architecture of Cloud Computing

Cloud computing has a layered design architecture as shown in figure 2. Physical Cloud resources along with core middleware capabilities form the basis for delivering IaaS and PaaS. The user-level middleware aims at providingSaaS capabilities[6].

2.4.1 Cloud Applications

This layer includes applications that are directly available to end-users. These applications may be supplied by the SaaS providers and accessed by end-users either via a subscription model or on a pay-per-use basis. In this layer, users can also deploy their own applications.

2.4.2 User Level Middleware

This layer includes the software frameworks, such asWeb 2.0 Interfaces(Ajax, IBM Workplace), that help developers in creating rich, cost-effective user-interfaces forbrowser based applications. The layer also provides those programming environments and compositiontools that ease the creation, deployment, and execution of applications in clouds. Finally, inthis layer several frameworks that support multi-layer applications development, such as springand Hibernate, can be deployed to support applications running in the upper level.

2.4.3 Core Middleware

This layer implements the platform-level services that provide run-time environment for hosting and managing User-Level application services. The core services at this layerinclude Dynamic SLA Management, Accounting, Billing, Execution monitoring, management,and Pricing (are all the services to be capitalized?). The well-known examples of services operatingat this layer are Amazon EC2, and Google App Engine. The functionalities exposed by thislayer are accessed by both SaaS (the services represented at the top-most layer in Figure 1) andIaaS (services shown at the bottom-most layer in Figure 1) services. Critical functionalities thatneed to be realized at this layer include messaging, service discovery, and load-balancing. Thesefunctionalities are usually implemented by Cloud providers and offered to application developersat an additional premium. For instance, Amazon offers a load-balancer and a monitoring servicefor the Amazon EC2 developers/consumers. Similarly, developers building applications on Microsoft Azure clouds can use the .NET Service Bus for implementing message passing mechanism.

2.4.4 System Level

The computing power in Cloud environments is supplied by a collection of data centers that are typically installed with hundreds to thousands of hosts [7]. At the System-Level layer, there exist massive physical resources (storage servers and application servers) that power the data centers. These servers are transparently managed by the higher-level virtualization [8] services and toolkits that allow sharing of their capacity among virtual instances of servers. These VMs are isolated from each other, thereby making fault tolerant behavior and isolated security context possible.

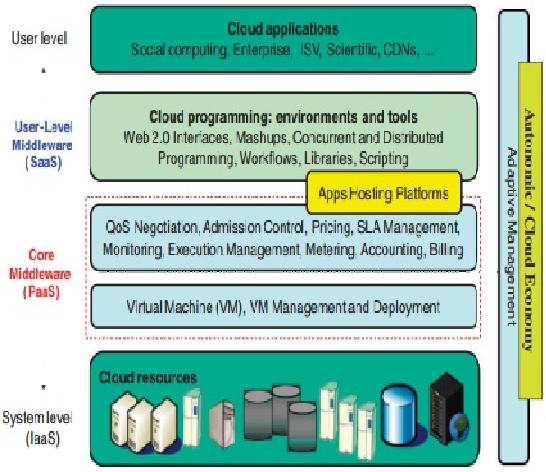

Fig 2: Layered design Architecture of Cloud Computing

3. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing have some security issues in cloud computing those we have to overcome for efficient and best practices [9].

3.1 Security

When anyone talks about the security, the question arise is where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security. However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can attack virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

Here are some particular security threats that must be overcome in order to benefit fully from this cloud computing paradigm those are listed and discussed below:[10]

3.1.1 Violation of Law

Company has violated the law (risk of data seizure by (foreign) government).

3.1.2 Incompatibility

Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud)[11].

3.1.3 Encryption/Decryption keys

Who controls the encryption/decryption keys? Logically it should be the customer.

3.1.4 Ensuring the integrity

Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.

3.1.5 Restriction of data

Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country.

3.2 Privacy

Cloudcomputing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

3.3 Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.

3.4 Legal issues

Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones". On the otherhand, worries stick with safety measures andconfidentiality from individual all the way through legislative levels.

4. RELATED WORK

Manyresearches on security in cloud computing has already been proposed. Identification based cloud computing security model have been worked out by different researchers [12]. But only identifying the actual user does not all the time prevent data hacking or data intruding in the database of cloud environment.Yao's Garbled Circuit is used for secure data saving in cloud servers [13, 14]. It is also an identification based work. The flaw in this system is that it does not ensure security in whole cloud computing platform. Research related to ensuring security in whole cloud computing environments was already worked out in different structures and shaped.Recently, Yahoo and HP have led the establishment of a global Cloud computing test bed, calledOpen Cirrus, supporting a federation of data centers located in 10 organizations [15]. Building such experimental environments is expensive and hard to conduct repeatable experiments as resource conditions vary from time to time due to its shared nature. Also, their accessibility is limited to members of this collaboration. As Cloud computing R&D is still in the infancy stage [16], a number of important issues need detailed investigation along the layered Cloud computing architecture (see Figure 2). There are a number of systems being developed all around the world. Some of these provide security by having a public key infrastructure (PKI) on each layer of cloud computing architecture and managing the Security holes associated with Iaas implementation. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions. There are some projects in the different parts of the world going for managing the security threats [9]. The Swedish Armed Forces is a national administrative authority which is responsible for the security of Sweden and works under the Ministry of defense. An organization of this scale undoubtedly possesses extremely critical and sensitive information which ought to be protected from unauthorized access at all costs. Therefore, one of the most crucial tasks for the Swedish Armed Forces is to protect its information systems to ensure the Confidentiality, Integrity and Availability of critical and sensitive data. According to Ingvar Stahl the security requirements for database systems within the Swedish Armed Forces is no different from other IT-security requirements and needs to be in accordance with laws and regulations imposed by the parliament and the Swedish government. Besides the governmental regulatory laws, the Swedish Armed Forces have also their own internal rules and regulations that need to be followed strictly. One of the most important internal security rules is documented in what is known as "KSF (Kravpa SakerhetsFunktioner)" or "Requirements for Security Functionalities" if translated into English. KSF describes the minimum level of requirements for access control, intrusion detection and prevention, safeguard against malicious code and unauthorized interception, alarming signals as well as log management. The current solutions for database security in the Armed Forces are dependent on the sensitivity of the data that is being protected. Within the Armed Forces, the information that needs to be stored is classified into different security levels and based on the confidentiality of the data different mechanisms are used for protection of the system. For example, for extremely confidential data, two folded security mechanism is used and smart cards are needed to access the system otherwise for access to normal data one would be able to login to the system with passwords only. Permissions for access to different systems are also defined by the roles of the intended users. There are often, but not always, special database administrators that manage the monitor the databases [17].

4.1 Data Security

Cloud vendors face major issues in confidentiality, integrity and availability in data security. Confidentiality refers to who stores the encryption keys. Integrity refers to no common policies that exist for data transfer. Lastly, the most problematic issue is availability i.e. it is very hard to make applications and resources. Data security includes Privileged user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigative Support, Long-term viability [18, 19].

4.2 Key Security Challenges

In cloud computing system there are some security challenges.

4.2.1 Authentication

As cloud users store their information to various services across the Internet, it can be accessible by unauthorized people. Henceforth for authenticating users and services cloud should have identity management system.

4.2.2 Access control

To identify and allow only authorized users, cloud should have a fine access control policies. Such services should be flexible, easily manageable and their privilege distribution is administered efficiently. Also the access control services should be incorporated based on Service Level Agreement (SLA).

4.2.3 Policy integration

The end users may access many cloud providers such as Amazon, Google, LoadStorm and other providers. They may have their own policies and approaches and hence there might be conflicts among their policies. Hence we need to have a mechanism to detect these inconsistencies among their policies and to have solutions for them.

4.2.4 Service management
To meet customers' needs, many cloud providers together form a new composed service and provides a packaged service to customers. At this scenario, there should be a service integrator to get the finest interoperable services.

4.2.5 Trust management
As the cloud environment is service oriented, a trust management approach should be developed. It should include trust negotiation factors for the cloud providers and cloud users. The idea is, the providers need to have some level of trust on the users to release their services to, and their users should have some level of trust on the providers to choose their services [20, 21, 22].

4.3 Security Model in Infrastructure as a Service
Security Model for IaaS (SMI) as a guide for measuring and enhancing security in each layer of IaaS delivery model as shown in Figure 3.
Security Model for IaaS (SMI) model consists of three sides: IaaS components, security model, and the restriction level. The front side of the cubic model is the components of IaaS, and the security model side includes three vertical entities where each entity covers the entire IaaS components [9].
The components of security model for IaaS consist of several major concerns of cloud computing environment.

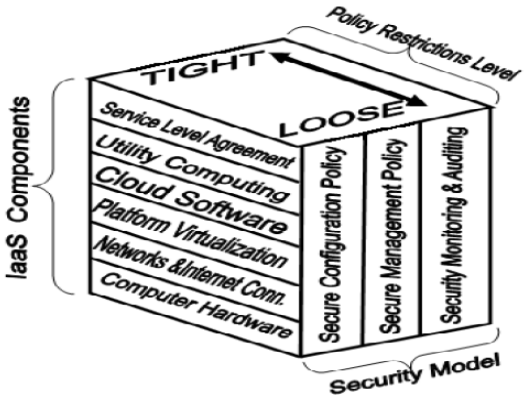

Fig 3: Security model for IaaS

4.3.1 Service level agreement (SLA)
Service Level Agreement in cloud system guarantees quality of services (QoS). It has several phases such as SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement. The SLA contract definition phase is used to determine the benefits and responsibility of each party whereas the SLA monitoring and SLA enforcement are used to manage the trust between the service provider and customer.

4.3.2 Utility computing
Utility computing is a concept of grid computing which works on heterogeneous platform. It packages the resources such as computation, bandwidth, and storage as metered services and delivers them to the client. It shapes two of the main features of the Cloud Computing, first user can only pay for their usage time not for whole resource, second it provide scalable system.

4.3.3 Cloud software
Cloud software joins the cloud components together. Either Cloud software is open source or commercial closed source. We can't ensure the vulnerability in available software.

4.3.4 Platform virtualization
Virtualization is a fundamental technology platform for Cloud Computing services, facilitates aggregation of multiple systems into a single hardware platform by virtualizing the computing resources such as network, CPUs, memory, and storage. Hardware abstraction hides the complexity of managing the physical computing platform and simplifies the computing resources scalability.

4.3.5 Secure configuration policy (SCP)
It guarantees a secure configuration for each layer in IaaS hardware, software, or SLA configurations.

4.3.6 Secure management policy (SMP)
Secure resource management policy controls the management roles and privileges.

4.3.7 Security monitoring and auditing (SMA)
Security monitoring and auditing is significant to track the system life cycle.

4.4 Survey Report by IDC

A survey was conducted by International Data Corporation (IDC) IT group to rate the cloud services and its issues in 2008. The Figure 4 shows the rating of cloud computing issues. And also it shows that security is the major concern in cloud computing environment [10].

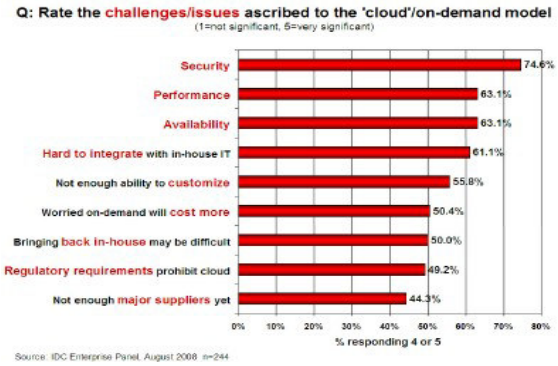

Fig 4: Analysis of major issues of cloud computing

5. CONCLUSION

Cloud computing is the future of IT industries. It helps the industries to get efficient use of their IT hardware and software resources at low cost. This paper totally discusses distributed database security issues in distributed cloud computing environment. This paper also analyzes cloud computing vulnerabilities, security threats those faced by cloud computing paradigm. We don't put too much attention on other issues of cloud computing such as reliability, consistency and availability.

6. FUTURE WORK

The future of cloud computing is to enhance the vision of cheap communications and to provide the quality of services for customers. In future, we can propose a better architecture and an algorithm by which data can be more secured so that the efficient distributed database security can be achieved. Furthermore, the work can be extended towards the other issues/concerns of cloud computing about consistency, data replication, transaction synchronization and traffic management. So that cloud system provide faster communication channel and satisfy various demands of users.

7. References

[1] Muzafar Ahmad Bhat, RazeefMohd Shah, Bashir Ahmad, "Cloud Computing: A solution to Geographical Information Systems (GIS)", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 2 Feb 2011, pp. 594-600

[2] Arpita Mathur, Mridul Mathur, Pallavi Upadhyay, "Cloud Based Distributed Databases: The Future Ahead", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011, pp. 2471-2481

[3] National Institute Of Standard and technology. csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc, 2009

[4] Open Security Architecture http://www.opensecurityarchitecture.org/

[5] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks

[6] Rodrigo N. Calheiros1, Rajiv Ranjan2, C´esar A. F. De Rose3, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", SOFTWARE – PRACTICE AND EXPERIENCE, Softw. Pract. Exper. 2011, pp:23–50

[7] Weiss A. Computing in the clouds. NetWorker2007; 11(4):16–25.

[8] Smith JE, Nair R. Virtual Machines: Versatile Platforms for Systems and Processes. Morgan Kaufmann:Los Altos, CA, 2005

[9] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012

[10] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" , International Journal of Advanced Research in Computer Science and Software Engineering 2 (9), September- 2012, pp. 115-120

[11] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky olicies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382

[12] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", CloudCom 2009, LNCS 5931, pp. 157–166, 2009

[13] Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency", CASED, Germany, 2011

[14] Sven Bugiel, Stefan Nurnberger, Ahmad-Reza Sadeghi, Thomas Schneider, "Twin Clouds: Secure Cloud Computing with Low Latency"- Extended Abstract, CASED, Germany, 2011

[15] Avetisyan AI, Campbel R, Gupta I, Heath MT, Ko SY, Ganger GR, Kozuch MA, O'Hallaron D, Kunze M, Kwan TT, Lai K, Lyons M, Milojicic DS, Lee HY, Soh YC, Ming NK, Luke J-Y, Namgoong H. Open cirrus: A global cloud computing testbed. IEEE Computer 2010; 43(4):35–43

[16] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM 2010; 53(4):50–58

[17] ImalSakhi, "Database security in the cloud", http://kth.diva-portal.org/smash/get/diva2:557762/FULLTEXT01.pdf

[18] Herminder Singh & Babul Bansal "Analysis Of Security Issues And Performance Enhancement In Cloud Computing" International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 345-349, July-December 2010

[19] Hassan Takabi and JamesB.D., "Security and Privacy Challenges in Cloud Computing Environments", Security & Privacy, IEEE, vol 8, Issue 6, pp 24-31, Dec 2010

[20] Nelson Gonzalez, Charles Miers, "A quantitative analysis of current security concerns and solutions for cloud computing", Third IEEE International conference on Cloud Computing Technology and Science, pp 231-238, 2011

[21] Subhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud Computing Security-Trends and Research Directions", IEEE World Congress on Services, pp 524-531, 2011

[22] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing" 2nd IEEE International Conference on Cloud Computing Technology and Science, pp: 693-702, 2010.