International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 2, Volume 2 (February 2015) www.ijirae.com

A Novel Approach for SLA Compliance Monitoring In Cloud Computing

*Suneel K S[1], Dr. H S Guruprasad[2]
[1]*PG Scholar, Dept. of CSE, BMSCE, Bangalore*
[2]*Professor and Head, Dept. of CSE, BMSCE, Bangalore*

Abstract - Cloud computing, a realization of utility computing, is an emerging technology. Due to its characteristics, such as flexibility, on-demand service and so on, it is being adopted in IT industry. An organization or an entity which makes use of cloud computing are called clients and the entity responsible for delivering the cloud computing services to its client is called cloud service provider. A break-through feature of the cloud computing is that, maintenance of both IT infrastructure and client's data is cloud service providers (CSPs) concern. Whenever the data of a client is out of its firewall boundary, the control of the client on its data is seized. Criticality of data that is placed in the cloud dictates to establish trust between the client and the cloud service providers. The established trust between the client and the cloud service providers appears in the form of a legal document called as service level agreement (SLA). SLA describes the properties of the services that is to be delivered by the cloud service provider. A deceptive CSP may spoof the properties of the services and only deliver the services with lower properties. This paper proposes an approach to monitor the SLA compliance at CSP that can be implemented at the client end.

Keywords: Trust, SLA, SLA compliance, third-party auditing.

I. INTRODUCTION

According to NIST, cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". Internet, that is used to connect between two systems, is used to provide content to its end user in the form of videos, emails and so on. But, next generation of internet is aimed at providing even more. With cloud computing, the next generation internet provides whole IT as a service to their user. With this, the users of cloud can buy or rent IT according to their requirements [1]. The IT as a service has three layers. Any of these layers can be made use by the cloud user. Three layers of IT as a service are as follows:

(1) Infrastructure as a service (IaaS):

This layer is the lowest layer of ITaS. In this layer, the whole IT infrastructure is provided by the Cloud Service Provider (CSP) to their users. The users are free to install any applications and OS in these infrastructures. But the maintenance of the infrastructure is done by the CSP. Users have rights to choose OS and other parameters regarding the OS. Amazon is a leading provider of IaaS. Amazon's IaaS product is called EC_2. [1]

(2) Platform as a service (PaaS):

This layer is second layer of ITaS. In this layer, CSP provide a packaged IT capability to its users. Users of this service are able to make use of the provided platform regarding to their requirements. The maintenance of the underlying platform is done by CSP. IBM's Rational Developer Cloud, Microsoft's Azure, Google's AppEngine are examples for PaaS. [1]

(3) Software as a service (SaaS):

It is the topmost layer of ITaS. This layer provides software for the users of the cloud computing. The hosting of the software, management and maintenance is the concern of the CSP [1].User or customer can use any of these layers according to their intended requirements. The customer is also billed according to the amount of resource and time of usage of resource. Using virtualization, the utilization capacity of servers that are available to a user is increased. With the help of virtualization, multiple user tasks are multiplexed onto a server. This leads to the efficient utilization of resources by reducing idle time of the servers and leads to the cost effectiveness. Cloud computing uses multi-tenancy as one of its goals that is to be achieved to reduce the cost of resource usage. In multi-tenancy, multiple users make use of same services simultaneously. The cloud computing software present in the cloud infrastructure must coordinate between these multiple users and eliminate imminent conflicts. In cloud computing trust between cloud user and cloud service provider is a great deal of concern. The cloud user may store application related data or any other data in the cloud that is managed by the cloud service provider. Since the data of the cloud user is not within the user's boundary, the data is not secure. If the user data in the cloud represents the business critical aspects of an organization, then a loss of data due to cloud computing infrastructure failure or an unauthorized disclosure of data may introduce chaos in the business activities of the organization. In order to solve the aforementioned problem, the cloud users and cloud service providers both enter into some terms. These terms are documented in a document called a service level agreement (SLA). These SLA's unambiguously describes the role of the cloud user and the service provider in their business. There are many methods that can be used at the CSP side to deceive the SLA between CSP and cloud users that may not be known to the cloud user as a deception. So, in order to overcome this deception, the cloud user usually delegate the auditing of services to an external third-party whose job is to audit the services provided by the CSP and raise flag if there is a breach in SLA by the CSP.

This paper proposes an efficient methodology to monitor the SLA compliance at the CSP side without using an external third party.

II. LITERATURE SURVEY:

TRUST ISSUE IN CLOUD COMPUTING

Trust between two parties can be defined as the constant belief of reliability and expectedness that exists between two parties. Trust is a complex phenomenon. Usually trust is associated with two defining metrics. First is the 'Risk'. Risk describes the perceived probability of damage. Trust is not necessary when there is no risk. Second is the interdependence. Interdependence is the condition in which both the entities of trust are dependent on one another. [2]

Trust between two parties goes through three phases. [2]

1. *A building phase*- when trust is developed.
2. *A stability phase*- when trust exists between two parties.
3. *A dissolution phase*- when trust is declined between two parties.

Basically trust is divided into two categories. First is the persistent trust that is based on the long term behavior of the entity. Second is the dynamic trust that is based on a specific context of the entity. [2] [3] Explains the formation of prediction of trusts in IT technology. [4] Explains why trust is too hard in cloud computing due to the overload of information and social distance between cloud users and providers. Trust is a great aspect of deal in cloud computing. This is justified by the following example.

Consider a financial corporation that audits the finances of large organization. To make use of cloud computing, the corporation leases required IT infrastructure from a cloud service provider. Employees of the corporation are provided with thin clients and the IT of the finance corporation is hosted as a whole in the cloud. The working data of the employees are the financial details of different organization that is stored in the cloud itself. So, in this situation a little unauthorized disclosure of data at cloud site may cost the financial corporation its reputation and at worst scenarios, the financial corporation is held responsible for the unauthorized disclosure and may have to face the prosecution.

These problems always occur when there is a breach in trust between the cloud user and the provider. Since the cloud computing is an emerging technology, interoperability between the clouds have no yet still evolved. So, it is not easily possible for a cloud user to shift from one cloud service vendor to another. This problem is called vendor lock-in. vendor lock-in introduces difficulty in tackling the action to be taken in case of initial trust breach by the CSP [3].

In order to bring trust to a legal platform, both cloud user and the cloud service provider arrive at some terms and these terms are registered in a legal document and are called as Service Level Agreement (SLA). Although SLA is used to establish trust between cloud users and providers, large organizations hesitate to store their business critical data in the cloud. The reason for this is that once the trust is breached at the cloud provider side, it causes irreparable damage to the organization. Damage due to trust breach is not limited to the financial loss but also may lead to the customer loss, reputation loss to the organization using cloud. [2 & 5]

RISKS AND UNCERTAINTY IN USING CLOUD COMPUTING ENVIRONMENT:

The characteristics of cloud computing listed by NIST, like on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service, meets the current IT demands. Hence, cloud computing is treated as a solution in many IT problems. The rapid elasticity of resources eliminates under-utilization and over-utilization of resources [6]. The pay-as-you-go model of cloud computing eliminates users from the upfront financial commitments. This business model is a well accepted solution for volatile or seasonal businesses [6].

Although the characteristics of cloud computing is very helpful in solving many IT problems, cloud computing, like other emerging technologies, come with certain amount of risks. [7] Lists the ontology of risks in cloud computing. Broadly risks in cloud computing can be divided into four main categories.

1. *Organizational risks*: relying on cloud computing leads to the risks in the organizational aspects such as IT governance, compliance to industrial regulations and so on.
2. *Operational risks*: moving towards cloud computing leads to the change in the usual operational model of the organization. Risks affecting daily organizational business are placed under organizational risks.
3. *Technical risks*: the complex cloud architecture and the associated complex operations may lead towards the technical risks during the adoption of cloud computing by an organization.
4. *Legal risks*: the cloud infrastructure and its complex operations and created IT differences develops many legal issues of risks while using cloud computing.

Main result of risk is called uncertainty. Uncertainty refers to the state of behavior of an entity, which cannot be predicted. Risk along with uncertainty in cloud computing leads to the deprecation of trust between cloud users and cloud service providers. This may lead to the abandoning of cloud computing technology by the users. Many of the large organizations are in their way to build their own cloud to serve their intra-agencies. This paper addresses this issue by providing a way for the cloud user to continually monitor the SLA compliance at the cloud end.

SERVICE LEVEL AGREEMENT (SLA) NEED AND COMPONENTS:

The SLA addresses both the needs of CSP and the cloud users. Some of them are [8 & 11]

1. SLA clearly describes the responsibilities of both cloud user and the cloud service provider.
2. It describes the QoS requirement of the cloud user and the QoS to be provided by the CSP.
3. List of services that the cloud user is being provided to the cloud user by CSP along with their description.
4. Describes the security risks and privacy management policies.
5. It provides, cloud user, the clear image of the cloud infrastructure.
6. The legal context that has been negotiated by the cloud users and cloud providers.

The overall contents present in SLA can be divided into four categories [9]

1. *Agreement-related elements*: These include contract based information between cloud users and the service providers.
2. *Service-related elements*: These contain service related information between cloud user and cloud service provider.
3. *Document-related elements*: document related context is placed in this category.
4. *Management-related elements:* This category includes SLA management details like Validity of SLA. [8] Defines a list of components of SLA between cloud user and cloud service provider. Some of them are listed below

1. *Business level objectives*: The business level objectives of the cloud user must be specified in SLA. Business level objectives specify business goals that are to be achieved by an organization. This is an organizational aspect rather than technical aspect.
2. *Responsibilities of both parties*: The clear cut responsibilities of both the end parties of SLA are registered here. These responsibilities are negotiated during the contract by the cloud service providers and the cloud users.
3. *Cloud security*: Since the data stored in the cloud may be sensitive, the arrangements for preserving the privacy, integrity and confidentiality of data in cloud must be known to both the parties of SLA. These security mechanisms for the protection of data in cloud are documented in SLA.
4. *Privacy in cloud:* since the data is stored in the cloud and manipulated in cloud itself, from the cloud user perspective the data is being outsourced to external third party. This notion motivates them to negotiate the privacy in cloud. The negotiated privacy mechanism is documented in SLA. It also includes the responsibility of cloud service provider when the privacy is compromised.
5. *QoS*: quality of service is of great concern to the cloud users. QoS includes various non-functional aspects of the service that is to be fulfilled by cloud service providers along with the functional aspects of service. QoS is defined by performance, availability, scalability and many more metrics.
6. *Provider failure*: Whenever there is a failure in providing resources at cloud service provider side, the contingency plan to address the situation is negotiated and registered in SLA.[10] Describes the general components of the SLA for cloud computing.
    - *Monitoring*: type of monitoring is performed and the party who does the monitoring od the cloud service that is provided by CSP is defined in this category.
    - *Billing*: Clear picture about the billing methodology and the metrics for billing is mentioned in this category.
    - *Security*: The security mechanisms that the CSP provides for the stored data of the cloud user in the cloud are documented here.
    - *Networking:* The IP addresses used, load balancing and throughput is described here.
    - *Privacy*: The privacy policy that has been negotiated by both cloud providers and cloud users are registered in this component.
    - *Support services*: These are supporting services that are required to deliver the service to the cloud user provided by the CSP.
    - *Local and International policies*: Since cloud infrastructure is distributed over national and international borders, local and international policies are documented. It is a legal component rather than technical component.

TABLE 1.1 GENERAL COMPONENTS OF SLA DOCUMENT

SLA
Monitoring
Billing
Security
Networking
Privacy
Support Service
Local and International Policies

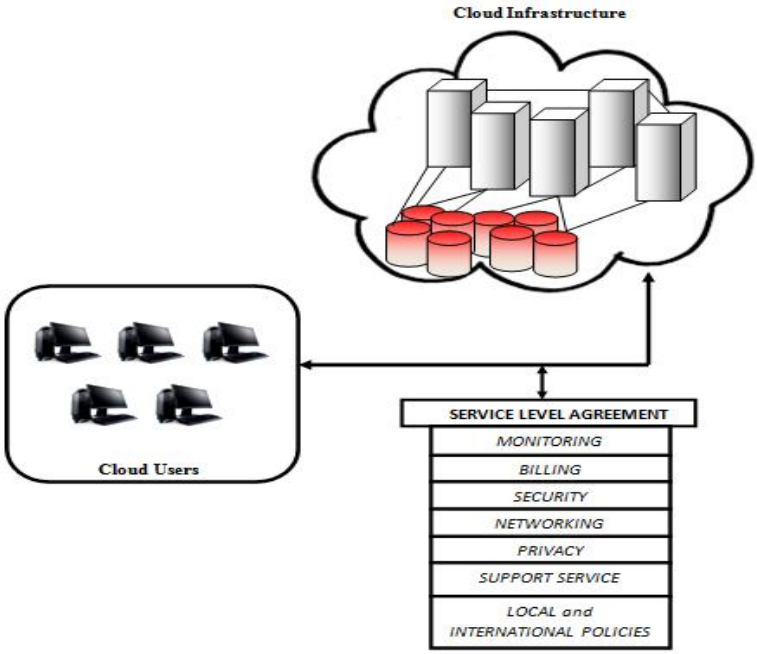

Fig 1.1 General architecture of cloud environment along with SLA

Third-party auditing in cloud computing:

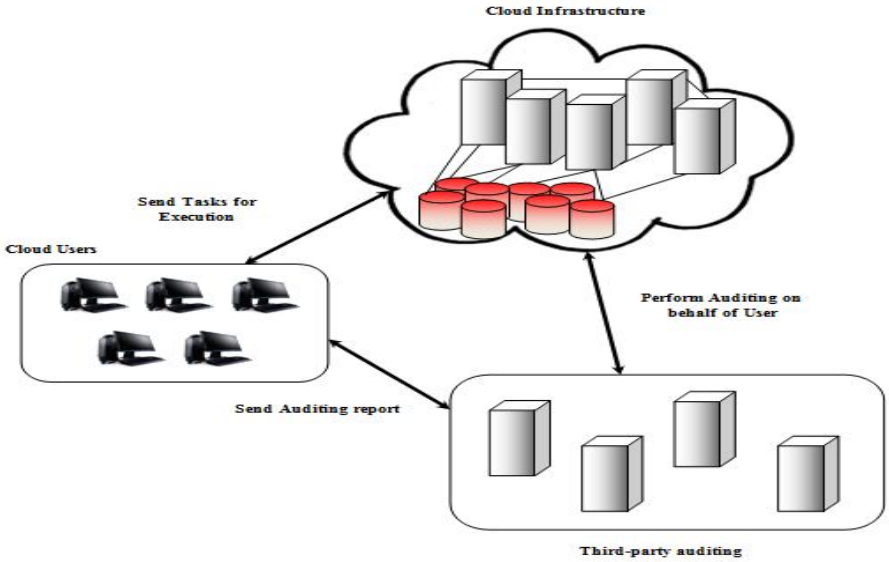

Fig 1.2 Cloud computing architecture with Third-Party Auditing.

Although SLA is setup between cloud users and providers, some entity must monitor the SLA compliance at the cloud provider level. Usually it is client's responsibility also to continually monitor the SLA compliance at the provider end and if there is any deviation from the agreed SLA, then proper action to be taken by the client itself. In order to monitor the SLA compliance, auditing of the operations at the cloud is performed by the clients. The main reason for auditing is to keep track of resources that have been used by the cloud user on time basis [11]. Auditing gives the information regarding the aspects of the resource usage by the cloud user and any discrepancies in meeting SLA by the cloud provider.

Due to inability to cope up with the auditing, some cloud users delegate the auditing to a separate entity. This separate entity is called third-party. The main responsibility of third party is to audit the cloud operation from cloud user behalf and submit the audit report to the cloud user. A deceptive cloud service provider may spoof third-party auditor in many ways such that the SLA breach is hidden from the third-party auditor. [12] Defines two ways in which a deceptive cloud service provider may spoof third-party auditor.

1. A deceptive CSP may use two separate virtual servers. One for TPA and another for cloud user's task execution. The virtual server given to TPA behaves according to SLA and the virtual server given for users are kept below the service level specified in SLA. This results in un-discoverability of SLA breach.

2. A CSP may evaluate the auditing pattern of the TPA and only during the auditing the service levels that are specified in SLA are preserved. Between two consecutive auditing, the service level is pushed down from the specified service level in SLA.
3. In worst cases, both TPA and CSP may join hand in hand, so that ultimately the cloud user is affected. A TPA may disclose the pattern of its auditing to the CSP and using this information CSP may breach SLA, which cannot be detected by the cloud user.

The above mentioned tricks used to deceive cloud user either by cloud service provider or third-party auditor or both, dictates cloud users to equip themselves to detect the SLA breach. This paper proposes a methodology that a cloud user can use to monitor the SLA compliance at the cloud provider end.

III. PROPOSED METHODOLOGY

The following functions are needed to define the algorithm.

1. *Information-fetch task generator function (Gen(SLA))* :
   This function generates a task that contains instructions to fetch the relevant data regarding SLA compliance at the cloud. Input to this function is the SLA between cloud user and the service provider. Output of this function is a information-fetch task.
2. *Evaluator (Eva(I)):*
   This function evaluated the percentage of SLA breach at the cloud provider side. Input of this function is the information obtained from the information-fetch task.

ALGORITHM

Let $C=\{c_1,c_2,\ldots\ldots\ldots,c_n\}$ be the set of user tasks that is to be submitted to the cloud for execution at cloud.
Each c_i is a tuple $c_i = <ID_i, S_i>$ where $1<=i<=n$.

- ID_i- represents a unique id to represent a task 'i' in a set of tasks C.
- S_i-represents the services required by the task 'i' in a set of tasks C.

Let A be the SLA between cloud user and service provider.
For each set of tasks C that is to be submitted to the cloud for execution at cloud, do the following

1) Generate an information-fetch task by using *Gen (A)*. Let I be the information-fetch task.
2) Send the tasks along with generated information-fetch task to the cloud for execution at cloud.
3) Whenever a set of tasks arrive at cloud, their hash value is calculated and a log is generated that contains hash value of the tasks and their arrival time stamp.
4) Get the results from the cloud after the successful execution. Let the result of the execution of task I be R.
5) Using the evaluate function (*Eva (R)*) evaluate the SLA breach at the cloud.

If the percentage of SLA breach is greater than acceptable threshold T_H in SLA breach, Then raise the SLA breach notification at the cloud user end.

IV. RESULT ANALYSIS

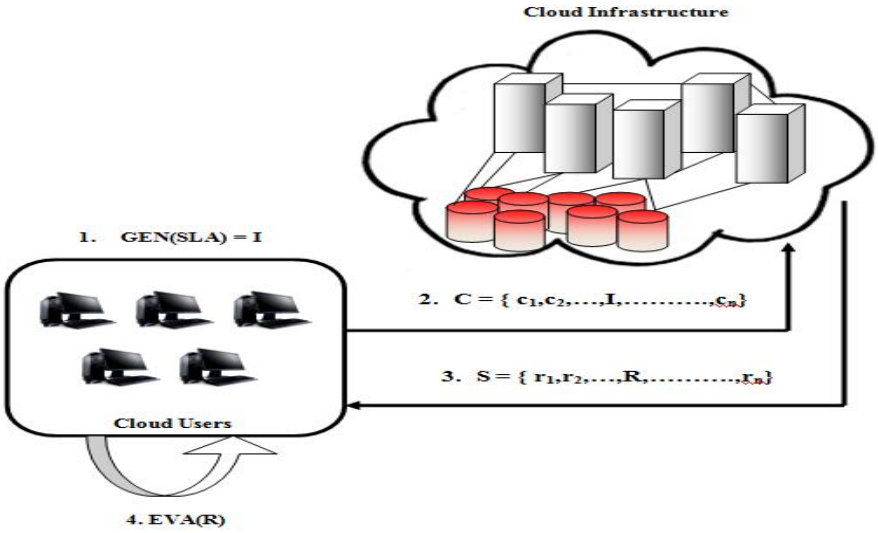

Fig 1.3 working model of the proposed algorithm.

1. ***Cloud user generates a information-fetch task by using Gen(SLA) function and by providing SLA between cloud user and service provider as input to the function.***
2. ***Along with the set of tasks that is to be sent to the cloud for execution, information-fetch task is sent to the cloud.***
3. ***When cloud is provided with a set of tasks, a log is created by registering the arrival time and the hash of the tasks. After this, cloud executes the set of tasks and sends the results back to the cloud user.***

4. ***Cloud user uses the function Eva(R) to evaluate the percentage of the SLA breach by using result returned for information-fetch packet from the cloud. Depending on the percentage of SLA breach, further action is taken by the cloud user.***

CLOUDSIM:

CloudSim is a simulation tool-kit that can be used to simulate and analyze different cloud environments. Results of the CloudSim can be used to analyze problem and its solution. It was developed by cloud research scientists at MIT, Australia [13]. Main advantages of using CloudSim include time effectiveness, flexibility and applicability [14]. [15] Defines the modeling of the CloudSim tool-kit. CloudSim simulator is built on JAVA platform. Every entity in cloud computing environment is represented using classes in JAVA. The proposed algorithm is simulated using CloudSim simulator and the result is analyzed and results show algorithm can be implemented at the cloud user side and allow the continuous monitoring of SLA compliance. Since the timing of the information-fetch task cannot be anticipated by the cloud service provider, it will be harder to deceive cloud user.

V. CONCLUSION

The simulated results of the proposed methodology justify its applicability. Simulation is done using CloudSim. The time at which the information-fetch task is executed is critical in identifying the SLA breach. The Log that contains the hash value of all the tasks along with its arrival time is used to force CSP towards non-repudiation. This methodology can be further enhanced by using optimal number of information-fetch tasks and by using probability theory to decide the time of execution of information-fetch packet.

ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] "Handbook of cloud computing", ISBN 978-1-4419-6523-3 e-ISBN 978-1-4419-6524-0, DOI 10.1007/978-1-4419-6524-0, pp 21.

[2] Dan C Marinescu, "Cloud Computing Theory and Practices", page no- 281.

[3] Matthias Söllner, Axel Hoffmann, Holger Hoffmann, Jan Marco Leimeister, "Towards a Theory of Explanation and Prediction for the Formation of Trust in IT Artifacts", Association for Information Systems AIS Electronic Library (AISeL), Special Interest Group on Human-Computer Interaction, 2011 Proceedings.

[4] Nicolai Walter, Ayten Öksüz, Marc Walterbusch, Frank Teuteberg, Jörg Becker, ""May I help You?" Increasing Trust in Cloud Computing Providers through Social Presence and the Reduction of Information Overload", Association for Information Systems AIS Electronic Library (AISeL), International Conference on Information Systems (ICIS), 2014 Proceedings.

[5] Marco Comuzzi, Guus Jacobs, Paul Grefen, "Understanding SLA Elements in Cloud Computing", Collaborative Systems for Reindustrialization, pp-385-392, Springer Berlin Heidelberg.

[6] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, "The Characteristics of Cloud Computing", ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, Pages: 275-279, DOI: 10.1109/ICPPW.2010.45.

[7] Dutta, A., Peng, G.C. and Choudhary, A. (2013). "Risks in enterprise cloud computing: the perspective of IT experts". Journal of Computer Information Systems, 53 (4), pp. 39-48.

[8] S.B.Dash, H.Saini , T.C.Panda, A. Mishra, "Service Level Agreement Assurance in Cloud Computing: A Trust Issue", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2899-2906.

[9] Talal H. Noor, Quan Z. Sheng, Sherali Zeadally, Jian Yu, "Trust management of services in cloud environments: Obstacles and solutions", ACM Computing Surveys (CSUR), Volume 46 Issue 1, October 2013,Article No. 12, publication date : 2013-10-01, doi :10.1145/2522968.2522980.

[10]Mohammed Alhamad, Tharam Dillon, Elizabeth Chang, "Conceptual SLA Framework for Cloud Computing", 4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010).

[11]Mohammad Monsef , Namjit Gidado, "Trust and Privacy Concern in Cloud", 2011 European Cup, IT Security for the Next Generation Technical Topics: "In the Cloud"-Security.

[12]Mohammed Hussain and Mohamed Basel Al-Mourad, "Effective Third Party Auditing in Cloud Computing", 2014 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), DOI: 10.1109/WAINA.2014.158.

[13]Rodrigo N Calheiros, Rajiv Ranjan, Anton Beloglazov, Cesar A F De Rose, Rajkumar Buyya, "CloudSim: A Toolkit for the Modeling and Simulation of Cloud Resource Management and Application Provisioning Techniques", Journal of software Practice and Experience, Vol 41, Issue 1, Jan 2011, pp 23-50, DOI: 10.1002/spe.995.

[14]Rizwana Shaikh, M. Sasikumar ,"Cloud Simulation Tools: A Comparative Analysis", International Journal of Computer Applications (0975 – 8887),International conference on Green Computing and Technology, 2013.

[15]Rajkumar Buyya, Rajiv Ranjan, Rodrigo N Calheiros,"Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities", 7th High Performance Computing and Simulation Conference, Leipzig, Germany, June 21-24, 2009, ISBN:978-1-4244-4907-1.

