SLA-Aware Trust Model Cloud Service Deployment

Shyamlal Kumawat
M. Tech Scholar
Department of Computer Science &Engineering
TIT, Bhopal

Deepak Tomar
Professor
Department of Computer Science &Engineering
TIT, Bhopal

ABSTRACT

Cloud computing is changing the way IT resources are utilized. Cloud computing dynamically delivers convenient, on-demand access to shared pools of software resources, platform and hardware as a service through internet. The cloud computing model—made promising by sophisticated automation, provisioning and virtualization technologies. Users want the ability to access these services including infrastructure resources, how and when they choose. To accommodate this shift in the consumption model technology has to deal with the security, compatibility and trust issues associated with delivering that convenience to application business owners, developers and users. Out of these issues, trust has attracted extensive attention in Cloud computing as a solution to enhance the security. This paper proposes a trusted computing technology through a "Service Level Agreement (SLA) - Aware Trust Model” to guarantee various Key Performance Indicators (KPIs) of cloud computing. The direct trust of cloud entities is computed on basis of the interaction evidences in past and sustained on its present performances. Various SLA parameters between consumer and provider are considered in trust computation and compliance process. The simulations are performed using CloudSim framework and experimental results show that the proposed model is effective and extensible.

General Terms

Trust Model, Security

Keywords

Cloud Computing, Security, Trust, Trust models, Cloud Actors, KPI, SLA, IaaS, CloudSim

1. INTRODUCTION

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) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. In recent years, industries such as Amazon, Microsoft, HP, Google, IBM, Citrix and VMware have heavily invested on Cloud infrastructure and core virtualization technologies in Cloud Computing (CC). This shows that there is a growing trend of using cloud platforms for ever rising storage and data processing needs. The highly distributed and non-transparent nature of cloud computing represents a considerable obstacle to the acceptance and market success of cloud services [2]. However, despite the advantages and rapid growth of Cloud Computing, it brings several security and trust related issues that need immediate action.

Trust is an important concept for cloud computing given the need for consumers in the cloud to select cost effective, trustworthy, and less risky services [4]. The issue of trust is also important for Cloud entities to decide on the cloud service provider that can comply with Service Level Agreement (SLA) parameters. Due to the dynamic nature of cloud deployment the matching of SLA templates need to be dynamic and continuous monitoring of Quality of Service (QoS) is necessary to enforce SLAs [5]. SLA template contains many parameters like cloud's resources like main memory, storage processor speed etc. and Key Performance Indicators like availability, response time. This paper proposes a trusted computing technology through SLA – Aware Trust Model that computes direct trust between cloud entities on basis of the interaction evidences in past and sustained on its present performances. The proposed model ensures various Cloud Key Performance Indicators (KPIs) discussed in [13]. The evaluation of KPIs is done under CloudSim [14].

This paper is organized as follows. The concept of Trust, Cloud Entities and SLAs along with their significance in CC context is provided in Section II. Section III presents the survey of existing mechanisms for establishing trust, various trust models and comment on their limitations. The proposed Service Level Agreement (SLA) Aware Trust Model and extensive simulation with results are presented in Section IV and V respectively. Finally, paper is concluded in Section VI with summary and directions for new research.

2. CONCEPT OF TRUST, CLOUD ENTITIES AND SERVICE LEVEL AGREEMENTS

2.1Concept of Trust

Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways [6]. Trust is defined as a mental state comprising Expectancy, Belief and Willingness to take risk in [3]. Thus, trust is a critical factor in cloud computing; in present practice it depends largely on judgment of reputation of cloud providers by cloud users. Trust between machine to machine may use handshake protocols negotiated within certain protocols and trust between machines to human implies that when a system relies on user input and instructions without extensive verification. A major concern with using Cloud capabilities is that vendor-provided services are not as secure as their own premise counterparts, so trust is a consequence of progress towards security or privacy objectives.

2.2 Cloud Entities

In [2], author defined: Cloud Providers (CPs) and Consumers as two primary cloud entities and Cloud Brokers (CBs) and resellers as emerging entities. Recently, NIST has mentioned Cloud Auditors and Cloud Carriers as two more entities in cloud architecture. Here in figure-1, apart from user, all the entities mentioned are included in categories of IT specialists who provide IaaS, PaaS and SaaS with or without add-ons either directly or indirectly on behalf Cloud Provider.

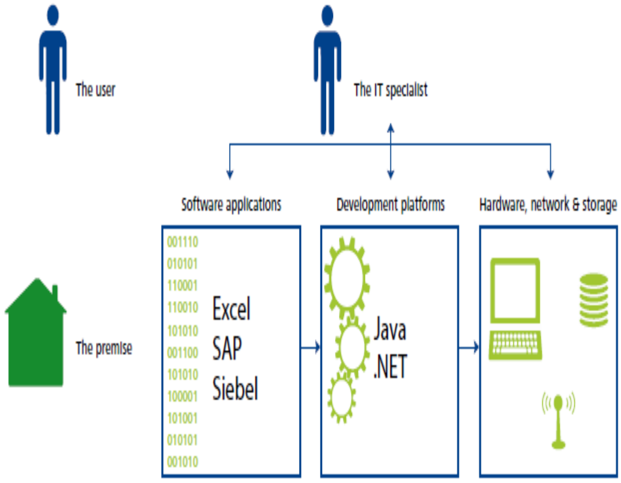

Fig 1: Cloud Entities

2.3 Service Level Agreements

An SLA is a legal contract or agreement between the provider of an IT service and the consumer of that service about the level of service or QoS, to be delivered. Examples of QoS attributes are response time, throughput, availability, security, and so on. In this proposed work the SLAs determines the opinion about the Cloud Infrastructure Provider with the Cloud user's view point. The trust is calculated and established using several SLAs indicators (CPU, Memory, Disk space, Bandwidth and Operating System).

3. RELATED WORK

3.1 Existing Mechanism for Trust Establishment

The entities are divided into Cloud Server Provider (CSP) and Cloud User (CU) in cloud computing. Trust evaluation depends on interactions evidences between the CSP and the CU. The interaction evidence is dynamic. And it has fine timeliness. Below we present various trust establishment process.

3.1.1 *Based On Interaction Evidence*

In cloud computing, Cloud User (CU) send service requests to Cloud Service Provider (CSP), and then CSPs provide the corresponding services for CUs [8]. Cloud Entities rate each other after each successful and unsuccessful interaction. In our work, trust calculation is based on interaction evidences and assessment between CSPs and CUs.

3.1.2 Direct Trust

Each interaction is considered as evidence. By querying the evidence set E, we can count up the number of valid interactions in time windows. Direct trust between entities is computed by direct interactions.

3.1.3 Reputation

Trust and reputation are correlated, but having different significance. , trust is established between two entities while the reputation of an entity is the aggregated opinion of a community towards that entity. The entity obtains the recommendation and rank information from other entities which have ever interacted with the evaluated entity directly [8]. In case of no direct interaction with the evaluated entity, its recommendation information will not be considered. Usually, an entity that has high reputation is trusted by many entities in that community; an entity, which needs to make trust judgment on a trustee, may use the reputation to calculate or estimate the trust level of that trustee [3]. Reputation systems are widely used in e-commerce networks. The reputation of cloud services or cloud service providers will certainly impact cloud users' choice of cloud services; and as a result, cloud providers

3.1.4 SLA Verification Based Trust

After establishing the initial trust and employing a cloud service, the cloud user needs to verify, recalculate and evaluate the trust. Here QoS monitoring and SLA verification is an important basis of trust management for cloud computing. This provided important baseline for the proposal presented in this work. Few significant SLA parameters include Random Access Memory (RAM), Storage Space, Network Bandwidth, Processing Capacity and Operating System. The RAM is used for providing virtualization on the node and thus providing better speed to execute the task (cloudlet). The high RAM ensures availability. Storage provides reasonable trust value on the node. Better the bandwidth, better the communication between the nodes. Operating System should be reliable enough that it would not be crashed at the run time. Processing capacity means average work load processed by the node.

3.2 Trust Models

In [9], a trust model is proposed on basis of past credential and present capabilities of CSP. In it trust value is calculated on basis of four parameters: availability, reliability, turnaround efficiency and data integrity. Authors in [8] proposes a trust evaluation model based on D-S evidence theory and sliding windows for cloud computing. The timeliness and recommendation trust of the interaction evidence is considered by introducing sliding windows and fusion approach. The direct trust of entities is computed based on the interaction evidence by D-S evidence theory. Finally, the combination exposes the credibility of entities.

Authors in [13] defined a volume based metric, i.e. the cost of one unit of (a) CPU, (b) storage, (c) RAM, and (d) Network bandwidth where a, b, c and d are weights for each resource attribute respectively. The sum (a+b+c+d) =1. The weight of each attribute can vary from application to application. For example, for some applications RAM is more important than CPU units, therefore for this application d>a. The proposed trust model evaluate the trust value of the node to find whether a node is reliable and that is performed on the basis of SLA parameters mentioned in [5, 10,11]. In [2, 3] a survey of existing mechanisms for establishing trust, and comment on their limitations are presented. Mechanisms based on evidence, attribute certification, and validation based on those limitations are rigorously discussed. Finally a framework for integrating various trust mechanisms together to explore trust issues in the cloud is presented. The corresponding research challenges to integrate the QoS parameters into trust and reputation systems are identified in [2]. In [7] authors have proposed a Trust Model between users and cloud providers establishing trust in three turns and when cloud users are satisfied at first two turns then at third turn they can rely on cloud provider. In first turn user must be satisfied with previous experience of cloud provider, and at second turn user must have knowledge about SLAs (Service Level

Agreements) security issues at different levels. User or Organization can trust on reliable cloud provider at third turn.

Similarly authors in [12] proposed a trust calculation process and trust model to ensure a reliable files exchange among nodes, in a private cloud, in accordance with the established metrics on basis of history interactions/queries between the nodes. These values are similar to weights in [13] and ranging between [0, 1]. The trustworthiness evaluation is based on node storage space, operating system, Network bandwidth and processing capacity. The simulations are done using CloudSim framework to show the efficiency of the model in selecting more reliable node in private cloud. The model has scope of evaluating it further with weights of SLA parameters and other performance indicators. The Trusted Computing Platform TCP in [15] presented a scheme for building trustworthy is used to provide authentication, confidentiality and integrity [17, 18]. This scheme displayed positive results for authentication, rule-based access and data protection in the cloud computing environment. Zhimin et al. [16] propose a collaborative trust model for firewalls in cloud computing and the trust relations among the nodes are divided in intra and inter domain trust relations. The model in [15] considers the transaction contexts, historic data of entities and their influence in the dynamic measurement of the trust value. Trust is measured by a trust value on the entity's context and historical behavior, and is not fixed. In [18], the "Trust as a Service" (TaaS) framework to improve ways on trust management in cloud environments, is proposed. In it an adaptive credibility model distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks. . In addition, TMS allows trust feedback assessment and storage to be managed in a distributed way. The approaches have been confirmed by the prototype system and experimental results

Since cloud users do not have direct control over their data on Cloud Provider's storage resources (datacenters, virtual machines) etc, so the trust evaluation would be a critical issue for Cloud user. Recent work deems various strategies with single SLA parameters, but those approaches are limited to simple workflows and single task applications [11]. The existing works raise various issues like: the parameters taken for trust calculation are qualitative rather than quantitative. Scheduling and Deployment of service requests considering multiple SLA parameters such as amount of CPU requirement network bandwidth and memory are still open research challenges. In this paper, we present a novel trust model considering multiple SLA parameters for enabling reliable transactions in Clouds. The direct trust of cloud entities is computed on basis of the interaction evidences in past and sustained on its present performances in recommendation trust table. Finally, the combinations of the recommendation trust expose the trustworthiness of entities in terms of SLA parameters like Availability, Response time etc.

4. PROPOSED SLA – AWARE TRUST MODEL

4.1 Details for Model

The trust model enables secure transaction (like task execution, storage or file exchange), between the cloud entities. As an example, if node-A want to exchange the file with another node let say B then, node-A first calculates the trust value of the node-B. The direct trust of cloud entities is computed on basis of the interaction evidences in past and sustained on its present performances. Various SLA parameters between consumer and provider are considered in trust computation and compliance process. In case the trust value of cloud node does not exist in Trust table a query is sent to the node of the cloud for getting the values of five SLA metrics. For calculating, the trust of node-B by node-A in a private cloud C a query is sent. V^c represents the trust and suitability of the particular node in a private cloud. So, the trust can be defined as

$$\boldsymbol{T^c = V^c} \qquad .....(1)$$

T^c represents the trust of cloud node calculated by consumer or user in the private cloud C.

4.2 Trust Calculation Process

SLA template contains many parameters like cloud's resources (physical memory, main memory, processor speed etc.) and properties (availability, response time etc.)[5]. The trust value is calculated as per the responses received from nodes in the cloud, containing five SLA parameters previously described in related work. Our proposed SLA – Aware Trust model also used weight based metric to calculate trust. To become aware the trust model enables the node to store the trust in a table which is known as approval table. We integrated the work in [12] with the proposed SLA aware trust model to present a new solution of defining the reliable criteria for the selection process of cloud providers. The weights assigned are: Storage capacity 30%, processing capacity should be 25%, RAM with weight of 25%, Network Bandwidth 10% and the remaining 10% to the Operating System.

The sum of weights assigned should be less than or equal to 1. According to the weight (w) of the attribute the trust of the node is calculated using the formula. The calculation of trust of B by A in the cloud C is represented by and described as:

$$\boldsymbol{T_{A,B} = \sum_{K=1}^{n} V((m1*w)/n}$$

This value is calculated based on the historical interactions of the node, being represented by T^c. The value of T^c range between 0 and 1, whereas **n** represents successful or unsuccessful tasks performed at cloud. Here **m** represents the value of metric obtained from node in cloud. The obtained value lies between $0 \leq m_i \leq 1$ and i represent the number of SLA metrics

5. SIMULATION AND RESULT ANALYSIS

5.1 Simulation Environment

CloudSim [14] fronted by Buyya, provides a simple, and extensible simulation framework that facilitate seamless simulation, modeling and experimentation of emerging cloud computing services is used for simulation of our trust model. Its functionalities provides modeling and simulation of large scale data centers, virtualized cloud hosts, energy-aware computational resources, profit based clouds, federated clouds, user-defined policies for allocation of virtual machines and also policies for allocation of host resources to virtual machines. For our simulations, CloudSim uses Sun's Java version 1.7. Apache Ant is used to compile CloudSim.

5.2 Simulation Parameters

We attempted to depict the simulation scenario used in our work in figure-2. The simulation is performed by characterizing three data centers at different locations owned by an IaaS provider, four hosts, that runs 30 virtual machines and a user submitting and performing 100 cloudlets. The values of simulation parameters chosen for our simulation are mentioned in Table - 1. As mentioned in [12], the reliable value of trust should have Trust ≥ 0.6. The final trust T^c of node obtained in our work is also ≥ 0.6, which proves the node to be trustable.

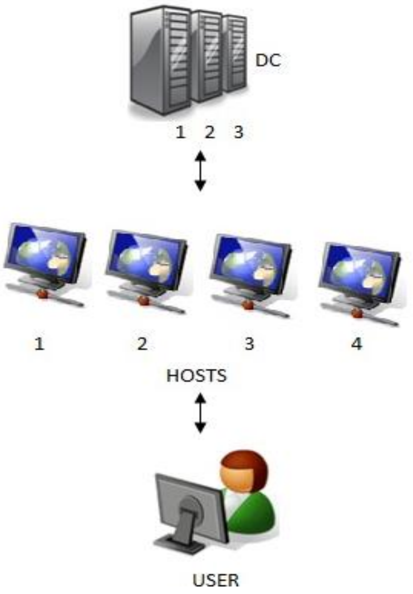

Fig2: Simulation scenario

Datacenter	Architecture	X86
	Operating System	Linux
	Virtual Machine Manager	Xen
Host	MIPS	5000
	RAM	1740 MB
	Storage	163840 MB
	Bandwidth	1024 Kbps
	VM Scheduler	Time shared
Virtual Machine	MIPS	
	Processing Elements	1
	RAM	512 MB
	Storage	10,000 MB
	Bandwidth	1000 Mbps
	Cloud Let Scheduler	Time Shared
	Virtual Machine Manager	Xen
Cloudlet / Task	Length	1000
	Full Size	300 MB
	Output Size	300 Mb
	Processing Elements	1

5.3 Result Analysis

For each successful cloudlet execution, the trust value of a VM will be increased by 2.5% until the trust level arrives at 0.85 and above 0.85, trust increases 5% until it reaches the maximum trust of 1.0 [12]. In our proposed work the trust of a virtual machine and ultimately of cloud provider is increasing for each successful cloudlet execution. Thus, result analysis shows that all tasks were performed successfully and it also shows that the trust between the nodes of a private cloud and the client and all created virtual machines are above the trusted value (0.6), so they are considered reliable. 12 virtual machines are successfully created and performed the cloudlets in our simulation.

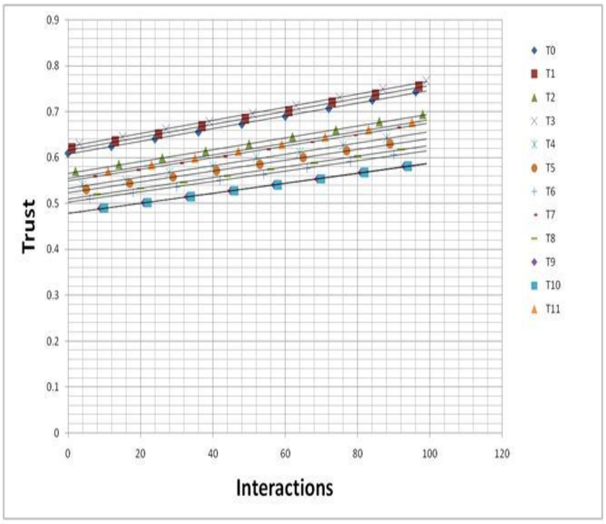

Fig 3: Trust Vs interactions

Verify that the trust of all Virtual Machines lies above the reference value as in [12]. Thus the trust of the node at Service Provider end tends to increase over time as the successful cloudlets occur, as can be seen Figure 3 and 4

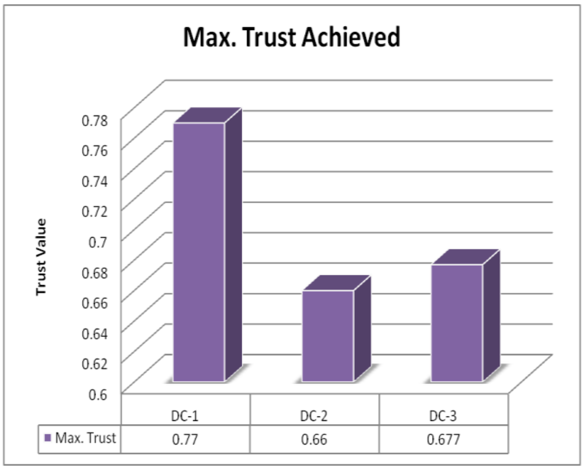

Fig 4: Max Trust

The proposed trust model is evaluated for following key KPIs mentioned in [13].

5.3.1 Availability: It is the percentage of time a customer can access the service and it is given by:

$$\frac{\text{(Total service time)} - \text{(Total time for which service was not available)}}{\text{Total service time}}$$

In our proposal Availability achieved is almost 97%.

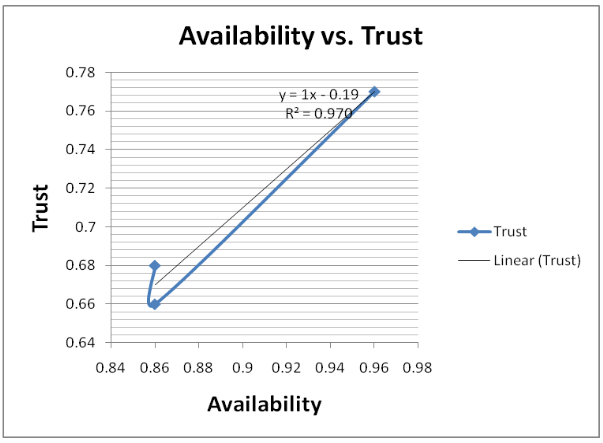

Fig 5: Availability Vs Trust

Figure 5 shows the graph between Availability and Trust. Trust and Availability is showing linear relationship in our proposed work

5.3.2 Throughput: Throughput is the number of tasks completed by the Cloud service per unit of time. Throughput depends on several factors that can affect execution of a task. Let an user application have 'n' tasks and they are submitted to run on 'm' machines from the Cloud provider. Let Te(n,m) be the execution time of n tasks on m machines. Let To be the time overhead due to various factors such as infrastructure initiation delays and inter task communication delays. Therefore, the total throughput of a Cloud service is given by

$$\frac{n}{Te(n,m)+To}$$

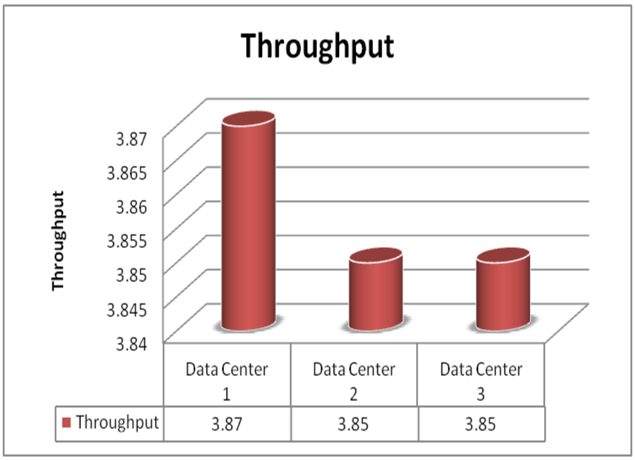

Fig 6: Throughput

5.3.3 System efficiency: indicates the effective utilization of leased services. Therefore, higher values for efficiency indicate that the overhead will be smaller. System efficiency is given by:

$$\frac{Te(n,m)}{Te(n,m)+To}$$

System Efficiency: The efficiency achieved is 96.7% in our proposal.

5.3.4 Service response time: The efficiency of service availability can be measured in terms of the response time, i.e. in the case of IaaS, how fast the service can be made available for usage. The service response time will represent the time taken by the Cloud provider to serve this request. One sub factor we measured is Average Response Time and it is give $\sum T_i/n$ Where T_i is time between when user i requested for an IaaS service and when it is actually available and n is the total number of IaaS service requests.

Total Submission of response time of VMs: 398

Total no. of task: 100

Response Time: 3.98

Other KPIs include Suitability, Adaptability, Elasticity, Usability, Reliability and Cost etc. Results show that, our SLA – Aware Trust model outperforms and provides better efficiency, availability and throughput

6. CONCLUSION

Cloud computing is a very broad term used for the recent development of internet-based computing. The general characteristics and trustworthy security of cloud computing will helps the development and adoption of this rapidly evolving technology. There are ten characteristics of cloud computing in their sum-up: user friendliness, virtualization, Internet centric, variety of resources, automatic adaptation, scalability, resource optimization, pay-per-use, service SLAs (Service- Level Agreements) and infrastructure SLAs. The characteristics of cloud computing are much more complex in [19]. Of course, there's no blanket solution to convince consumers that a cloud is fully trustworthy. The importance of trust varies from organization to organization, depending on the data's value. Furthermore, the less trust and enterprise has in the cloud provider, the more it wants to control its data even the technology [20].

In this work different interrelated research literature on trust were extensively studied and a survey of existing mechanisms for establishing trust and trust models are presented and commented on their limitations. In this work the concept of Trust, Cloud Entities and SLAs along with their significance in CC context is presented. Also, the proposed Service Level Agreement (SLA) concept and KPIs are defined.

SLA – Aware Trust Model is proposed and incorporated in private IaaS cloud and per formability analysis is done by means of extensive simulations on open platform, CloudSim. The simulation results demonstrate that the proposed model is extensible and effective in terms of KPIs. Our proposed SLA – Aware Trust model used weight based metric to calculate trust. To become aware the trust model enables the node to store the trust in a table which is known as approval table. We integrated the work in [12] with the proposed SLA aware trust model to present a new solution of defining the reliable criteria for the selection process of cloud providers. The future simulations using a real scenarios for cloud computing will allow to evaluate the performance of nodes on basis of qualitative performance indicators. Furthermore, the proposed model will be evaluated for finding the trust value on basis of metrics for varying application requirements in real time, and select more trustable, suitable as well as reliable nodes.

7. ACKNOWLEDGMENTS

Authors are genially giving appreciation to the researchers of different security and trust models, of cloud computing and to all those who have attempted hard to build cloud simulation tools to make research works easy to accomplish.

8. REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing, National Institute of Standards and Technology", ver. 15, 9 July 2010.

[2] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max M¨ uhlh¨auser, "Trust as a facilitator in cloud computing: a survey", Journal of Cloud Computing: Advances, Systems and Applications, Springer 2012. http://www.journalofcloudcomputing.com/content/1/1/19 .

[3] Jingwei Huang and David M Nicol, "Trust mechanisms for cloud computing", Journal of Cloud Computing: Advances, Systems and Applications, Springer Open Journal 2013, http://www.journalofcloudcomputing.com/content/2/1/9.

[4] Alhamad, M., Dillon, T., Chang, E., "SLA-Based Trust Model for Cloud Computing", 13th International Conference on Network-Based Information Systems 2010.

[5] Chauhan T, Chaudhary S, Kumar V, Bhise M, "Service level agreement parameter matching in cloud computing", 978-1-4673-0127-5, World Congress on Information and Communication Technologies (WICT), IEEE 2011.

[6] Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, Paul Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges – Final Report", Directorate-General Information Society and Media, European Commission 2010.

[7] Shakeel Ahmad, Bashir Ahmad, Sheikh Muhammad Saqib and Rashid Muhammad Khattak, "Trust Model: Cloud's Provider and Cloud's User", International Journal of Advanced Science and Technology Vol. 44, July, 2012.

[8] Xiaonian Wua, Runlian Zhang, Bing Zeng, Shengyuan Zhou, "A trust evaluation model for cloud computing", Procedia Computer Science 17 (2013) 1170 – 1177, Information Technology and Quantitative Management (ITQM), Elsevier 2013.

[9] Paul Manuel, "A trust model of cloud computing based on Quality of Service", DOI 10.1007/s10479-013-1380-x, Springer 2013.

[10] Emeakaroha, V.C., Brandic, I. Maurer, M., Breskovic, I., "SLA-Aware Application Deployment and Resource Allocation in Clouds", Computer Software and Applications Conference Workshops (COMPSACW), 978-1-4577-0980-7, IEEE 2011.

[11] Pawar, C.S., Wagh, R.B., "Priority Based Dynamic Resource Allocation in Cloud Computing", 978-1-4673-4854-6, International Symposium on Cloud and Services Computing (ISCOS), IEEE 2012.

[12] Edna Dias Canedo, Rafael Timóteo de Sousa Junior, Robson de Oliveira Albuquerque and Fábio Lúcio Lopes deMendonça, "File Exchange in a Private Cloud supported by a Trust Model", 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 978-0-7695-4810-4/12, IEEE Computer Society 2012.

[13] Saurabh Kumar Garg, Steve Versteeg, Rajkumar Buyyaa, "A framework for ranking of cloud computing services", Future Generation Computer Systems 29 (2013) 1012–1023, Elsevier 2012.

[14] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, "Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities", 978-1-4244-4907-1/09, IEEE 2009.

[15] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[16] Zhimin Y., Lixiang Q., Chang L.,Chi Y., and Guangming W,"A collaborative trust model of firewall-through based on Cloud Computing," Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design. Shanghai, China. pp. 329-334, 14-16. 2010.

[17] Akhil Behl, Kanika Behl, "An Analysis of Cloud Computing Security Issues", 2012 World Congress on Information and Communication Technologies IEEE 2012.

[18] Xue Kai, Liu Zhao, Yang Shuguo, Research on Secure Frame of Cloud Computing, Computer & Telecommunication, 2010.

[19] D. Malcolm, "The five defining characteristics of cloud computing, http://news.zdnet.com/2100-9595_22-287001.html.

[20] Khaled M. Khan and Qutaibah Malluhi, "Establishing trust in cloud computing" IT Pro September/October 2010 Published by the IEEE Computer Society 1520-9202 IEEE 2012.