International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
57 – 61

A Trust based Approach to Enhance Cloud Security

[1]Nayeem Sheikh, [2]Neeraj Mangla, [3]Sanjeev Rana
M. M. Engineering College, M. M. University Mullana (Ambala) Haryana, India
[1]sheikhnayeem11@gmail.com, [2]erneerajynr@gmail.com, [3]dr.sanjeevrana@yahoo.com

Abstract: Cloud computing is an architecture that provides computing service via the Internet on demand to a pool of shared resources namely networks, storage, servers, services and applications without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the Cloud due to the efficiency of services provided by the pay-per-use pattern. Limited control over the data may incur various security issues and threats, which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. The user data must be stored securely and it must not be tempered by any means either by Cloud Service Provider (CSP) or by any other user. Hence the security is very much important in Cloud. Among the security, the first thing that a user needs is the trust. This is because trust is one of the predominant ways to enhance the security and authorizes the compatibility of different autonomous Cloud providers. Because it is the trust on behalf of which a user chooses a particular CSP [1] [2]. For this, we must have a model to evaluate the trust for different Cloud providers, and provide to the customer while choosing the Cloud provider. There are different trust evaluation models but each one has some limitations. In our work, we have evaluated the trust for different Cloud providers with different approach using various parameters including bandwidth, storage, computations, Virtual Machines(VMs), security etc so that the customers can pick Cloud providers` services and resources [3]. We have calculated the trust for each service providers using the fog simulator and ruby language. It does not need any Internet connection and sign up with the Cloud providers. The fog simulator has many functions and among them "compute" is used to connect with various Cloud providers. This approach is very easy to use and provides better results.

Keywords- *Cloud Computing, Cloud Services, Trust.*

*****

1. Introduction

Cloud Computing is a distributed architecture that provides different on-demand services to the users using the centralized server resources. Cloud Service Providers (CSP) provide different services like software for using different services, platform for building various web services and infrastructure for using computing, storage and other things just like Internet Service Provider (ISP) provide high speed access to internet. Both CSP and ISP provide different services to the customers. But CSP is an on-demand pay-as-u-go resource provisioning model that offers easy access to a pool of resources like applications, development tools, network, servers and storage that can be provisioned and released with minimum management efforts between the user and the provider. Three types of services are provided by the cloud providers[1] [4]. These are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Today organizations are heading towards information technology including cloud computing because they hire services and resources on rent basis and pay according to usage. Organizations also remain updated and don't need to worry about the changing technology to ensure that they are always available to the customers. Cloud Computing seems to be a necessity being framed by the idea of using only infrastructure without installing and managing it. This concept was firstly used for the academics but now it had made its influence in the business industries through Microsoft, Amazon, Google and Salesforce.com. By using cloud new start-ups can enter business easily as the infrastructure cost is greatly diminished. Now the concentration is on business value rather than the starting budget. Cloud Providers offer resources like computing power and storage dynamically on rent basis to the business clients according to the requirement. With the advent of this technology users utilize small portable devices such as personal computers (PCs) and Personal Digital Assistants (PDA's) to access large applications [5] [6].

Clouds are the new technologies in development of the distributed system being grid as its predecessor. The cloud provides abstraction of its services, so no expertise or knowledge regarding it is needed by the users. Higher computing power, high scalability, higher quality of service and higher throughput are achieved by the usage of internet services. High speed internet is needed to access the online business applications being provided by the cloud providers.

2. Literature Survey

The author [7] states that the data recovered from open circulated frameworks can be of unverifiable dependability and filtering through a lot of information can be an intricate technique. The author proposes a sociologically spurred trust and notoriety display for the issue of dependable data recovery and presents a case of its utilization in his paper. Without a confide in display, the errand of distinguishing trustworthy and solid data sources ends up noticeably overwhelming as any organize client can be a wellspring of data. In this manner, this paper plots a multi-disciplinary way to deal with the issue of data dependability, consolidating inspirations established in disseminated

 ISSN: 2454-4248
57 – 61

frameworks security with basic establishments in humanism connected to the issue of dependable data recovery.

According to the author [8] [9] at any given time, the solidness of a group relies on upon the correct adjust of trust and doubt. Besides, we confront data over-burden, expanded instability and hazard taking as a conspicuous element of present day living. The author gives and talks about a trust show that is grounded in true social confide in qualities, and in view of a notoriety component, or informal. The proposed display enables operators to choose which other specialists' suppositions they trust increasingly and enables operators to dynamically tune their comprehension of another specialist's subjective proposals.

The author [10] in their paper depicts that the Trust is a standout amongst the most imperative intends to enhance security and empower interoperability of current heterogeneous autonomous Cloud stages. The authors initially examined a few trust models utilized as a part of vast and disseminated condition and afterward presented a novel Cloud trust model to comprehend security issues in cross-Mists condition in which Cloud client can pick distinctive suppliers' administrations and assets in heterogeneous areas can participate. The model accomplishes both character confirmation and conduct validation. . Recreation tests demonstrate the proposed model can set up confide in connection amongst client and supplier and between various Cloud stages quick and safe.

The author [11] [12] describes that the Cloud service provider must assure us for the required security and trust so that we use a particular Cloud. Among the security, the most important security concern for both provider and user is how provider gives assurance of trust and how user will trust the provider. Because it is the trust between provider and user, that forms a bond between the two parties. The author gives a scene and examines impetuses and obstacles to receive Distributed computing from Cloud shoppers' point of view. Trust-helped brought together assessment structure by utilizing trust and notoriety frameworks can be utilized to evaluate reliability (or trustworthiness) of Cloud suppliers. Thus, Cloud-related particular parameters (QoS) are required for the trust and notoriety frameworks in Cloud conditions. The author distinguishes the basic properties and relating research difficulties to coordinate the QoS parameters into trust and notoriety frameworks. The author have characterized the present patterns of trust foundation and distinguished their confinements by methods for utilization situation where a human services supplier, confront the test of choosing the most reliable Cloud supplier. The authors have shown the estimation of brought together trust assessment structure (i.e., a trust administration framework) by methods for TR models and their required properties for building up confide in Cloud conditions.

3. Trust Model

We have proposed a novel model for trust evaluation of different cloud providers in large and completely for distributed and cross computing environments. The details of the model are that we are differentiating the cloud roles into client and server. The important property of this model is that it uses recommended trust as the important parameter with other parameters like bandwidth, storage, computation, virtual machine and servers. The trust is divided into direct and indirect or recommended trust. While using the cloud for the first time, the customer uses the recommended trust provided by the well-known providers for trust calculation. After the trust value is obtained, both trust and recommended trust is updated.

Domain trust agent maintains trust for the providers. Domain trust is used when two providers cooperate with each other for the first time. Providers also use the recommended trust values from well-known providers for the first time.

The description the table is as: service provider is the name or id of the cloud service provider. Service types are parameters like bandwidth, storage, servers and recommended trust. Load time is the time taken by the cloud provider to provide the corresponding servers and services. Trust value is simply the final trust value.

Trust decision is very important for using the cloud services. Both customer and the providers need a trust decision while using or cooperating the providers for the first time. For making the trust decision a threshold is necessary as a standard. The threshold can be altered by the cloud entity and trust domain as per the security required. If the trust value exceeds threshold then the provider is ready to use otherwise not used.

4. Result and Discussion

The essential motive of this work is to calculate the trust value for the Cloud Providers on behalf of which we can suggest the customer which Cloud to use. We are using different parameters like bandwidth, storage, computation, virtual machines, reliability and recommended trust to evaluate the trust value of the Cloud Providers. We are first calculating the load time for each service provider and then the trust value on behalf of load time and recommended trust value. Finally, we are taking the average of multiple scenarios (average of multiple trust values).

The multiple Cloud Providers for which we are calculating the trust values are shown in the figure 1. The load time and trust value for different Cloud Providers are calculated using the following command as given in figure 2. The load time is calculated on the basis of different parameters of the system like servers available, processing speed, VMs, storage scheme and security etc as shown in table 1.

ISSN: 2454-4248
57 – 61

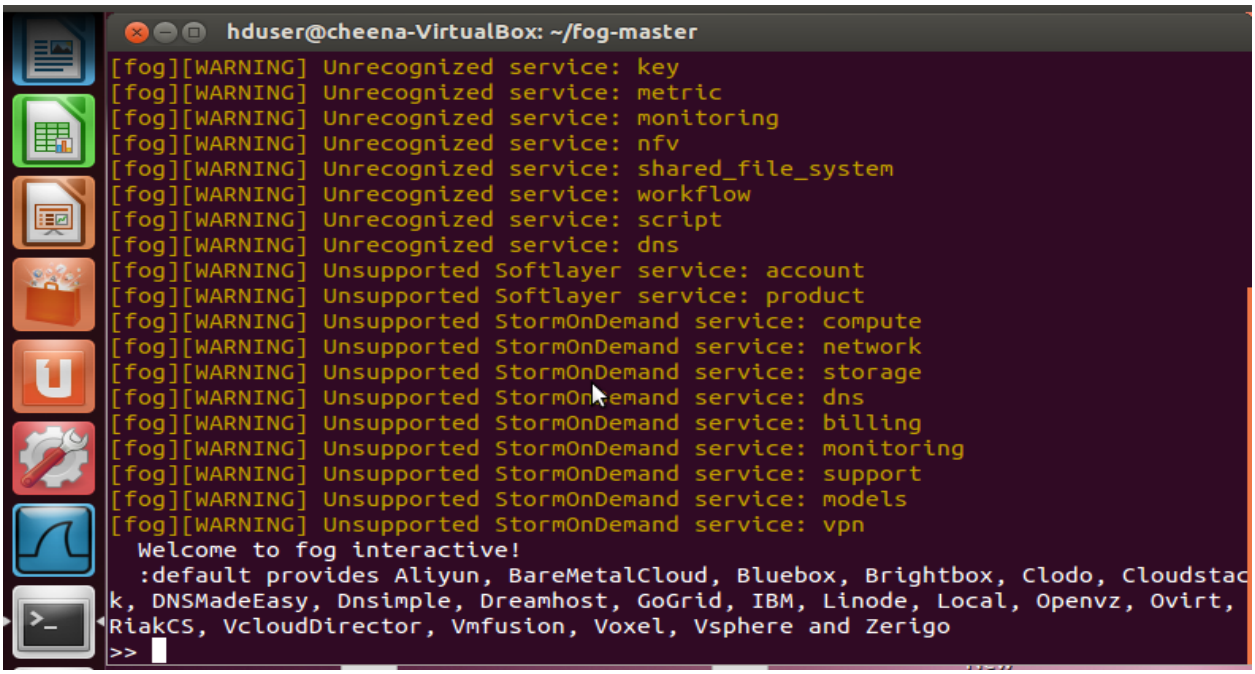

Figure 1: Default service providers.

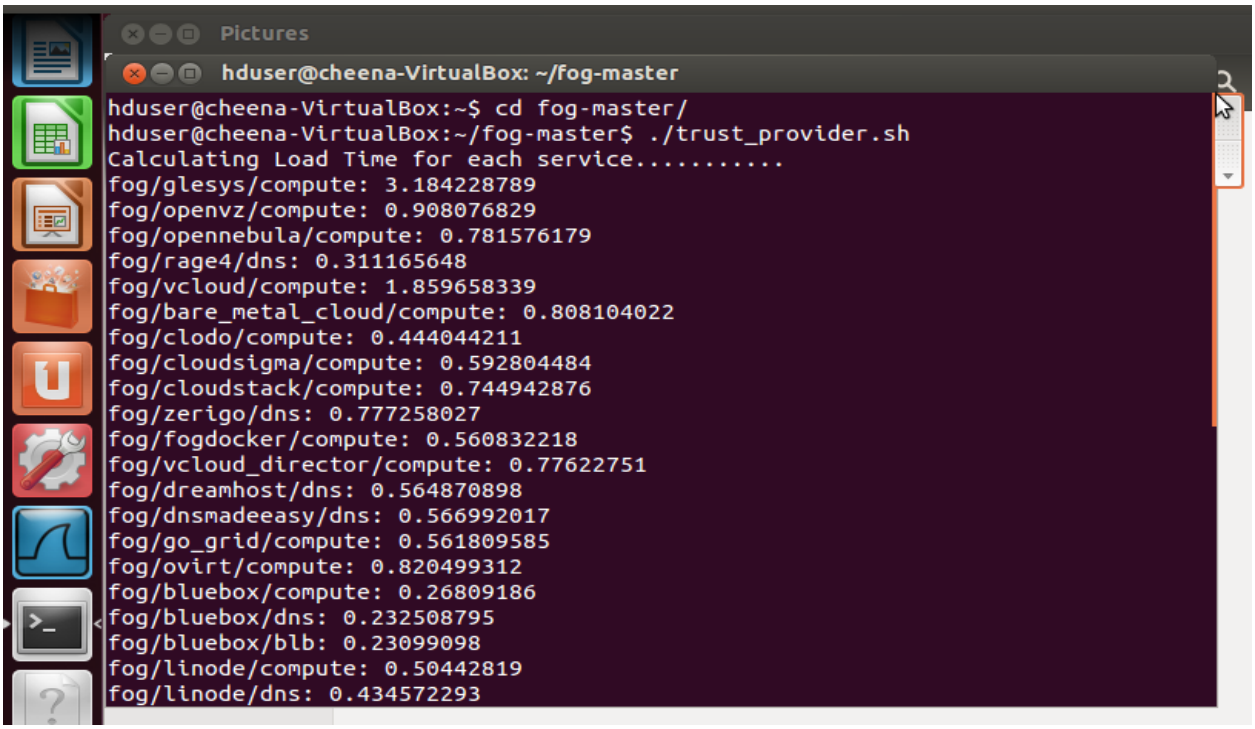

Figure 2: The figure describes the output of Load Time for each Service Provider.

Table 1: Load Time for each Provider

Service Provider	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Avg Load Time
Cloudstack	1.686436589	0.253989054	0.24203318	0.234418751	0.240863531	0.531548221
Zerigo	0.863946168	0.320226141	0.316754965	0.315765923	0.321116291	0.427561898
Vcloud	0.324649068	0.315334221	0.314187653	0.314672578	0.317204469	0.317209598
Ovirit	0.318684314	0.31213823	0.312588326	0.318095763	0.315917428	0.315484812
Baremetal cloud	0.326542287	0.320874359	0.311794472	0.312215159	0.313904222	0.3170661

 ISSN: 2454-4248
57 – 61

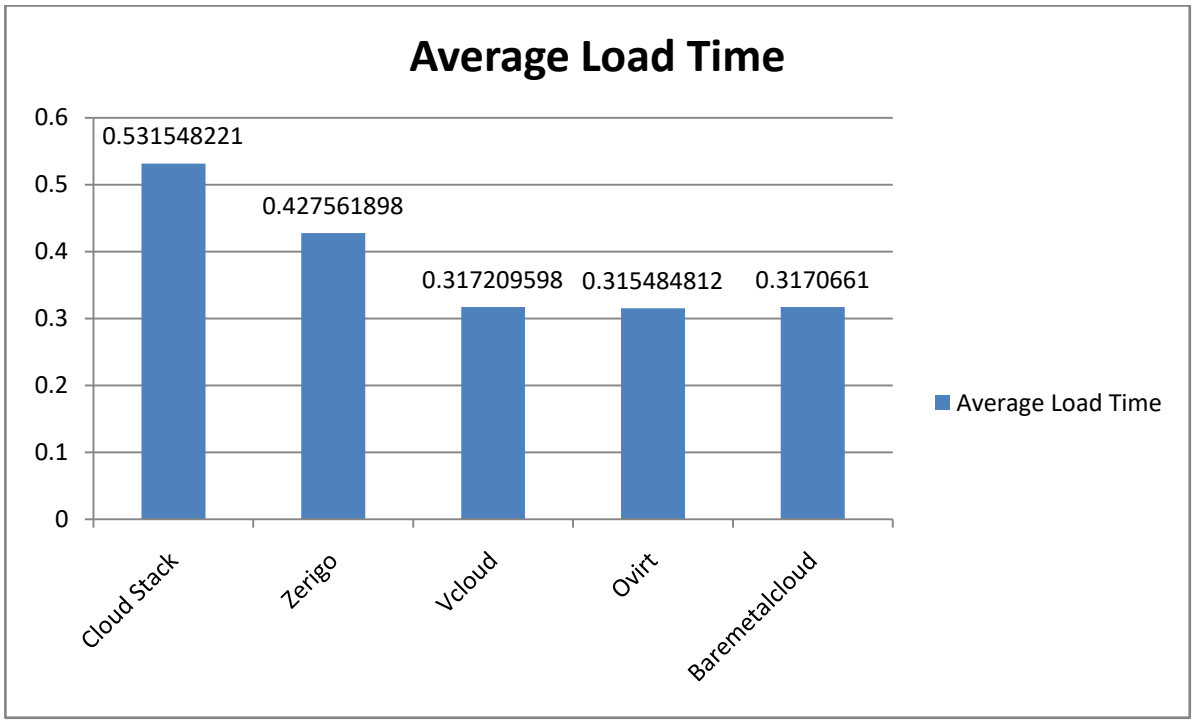

Figure 3: Average Load Time for different Service Providers.

The average load time for different service providers is shown in figure 3. The trust value for each cloud provider is evaluated on the basis of load time and other different system parameters just like load time. The figure 4 and table 2 shows the trust value of different service providers.

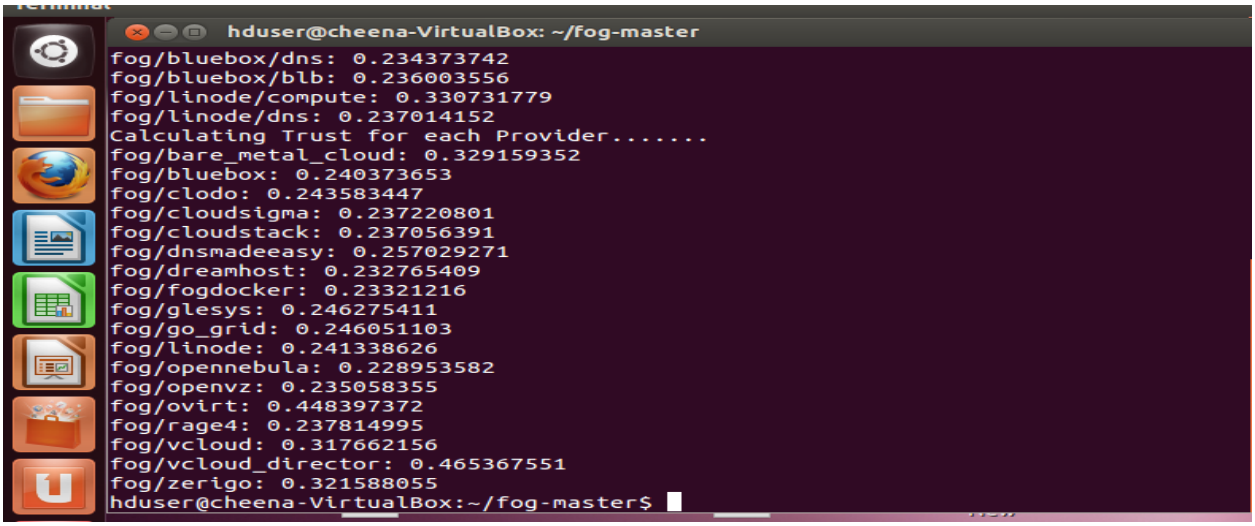

Figure 4: Trust value obtained for different Service Providers

Table 2: Trust value for service providers

Service Provider	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Avg trust
Cloudstack	0.236862121	0.246458527	0.244839967	0.244538445	0.244278514	0.243395515
Zerigo	0.700899352	0.371289496	0.317968416	0.314828533	0.318721969	0.404741553
Vcloud	0.564297659	0.342689025	0.311321392	0.313321454	0.314709331	0.369267772

 ISSN: 2454-4248
57 – 61

Ovirit	0.316791873	0.352667168	0.31505755	0.315137598	0.318697185	0.323670275
Baremetal cloud	0.322717309	0.309372278	0.313859733	0.314235282	0.314949724	0.315026865

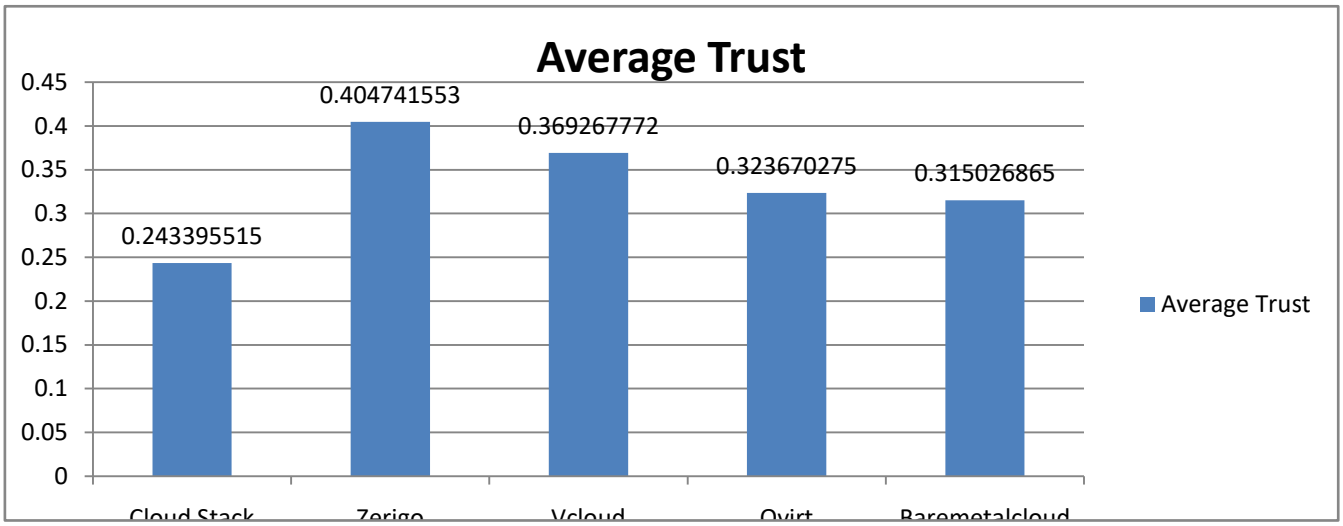

Figure 5: Graph showing the average trust value for Service Providers

Figure 5 shows the average trust value for each service provider in graphical form which is calculated with the help of table 2.

5. Conclusion and Future Work

Cloud Computing is the emerging technology today but it has many security and privacy issues. Among the issues trust is of great concern for both users and providers. A lot of work is going on for trust evaluation using different models. But in our work we have evaluated the trust for different cloud providers with different approach using parameters like bandwidth, storage, computation, VMs, security and other parameters. The best thing is that it uses recommended trust for the evaluation of trust. We have calculated the trust for each service providers using the fog simulator and ruby language. It does not need any internet connection and sign up with the cloud providers. The fog has many functions and among them compute is used to connect with various cloud providers. This approach is very easy to use and provides better results.

For the future enhancement, to establish trust between the user and provider with better results, we can use different parameters and different approach for trust evaluation.

References:

[1]. Padhy RP, Patra MR, Satapathy SC. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2011 Dec; 1(2):136-46.

[2]. Habib SM, Hauke S, Ries S, Mühlhäuser M. Trust as a facilitator in Cloud computing: a survey. Journal of Cloud Computing: Advances, Systems and Applications. 2012 Aug 23; 1(1):1.

[3]. Li W, Ping L. Trust model to enhance security and interoperability of Cloud environment. InIEEE International Conference on Cloud Computing 2009 Dec 1 (pp. 69-79). Springer Berlin Heidelberg.

[4]. Wu X, Zhang R, Zeng B, Zhou S. A trust evaluation model for Cloud computing. Procedia Computer Science. 2013 Dec 31; 17:1170-7.

[5]. Kim H, Lee H, Kim W, Kim Y. A trust evaluation model for Cloud computing. InGrid and Distributed Computing 2009 (pp. 184-192). Springer Berlin Heidelberg.

[6]. Guo Q, Sun D, Chang G, Sun L, Wang X. Modeling and evaluation of trust in Cloud computing environments. In Advanced Computer Control (ICACC), 2011 3rd International Conference on 2011 Jan 18 (pp. 112-116). IEEE.

[7]. Rashidi A, Movahhedinia N. A model for user trust in Cloud computing. International Journal on Cloud Computing: Services and Architecture (IJCCSA). 2012 Apr; 2(2):1-8.

[8]. Abawajy J. Establishing trust in hybrid Cloud computing environments. In2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications 2011 Nov 16 (pp. 118-125). IEEE.

[9]. Sun X, Chang G, Li F. A trust management model to enhance security of Cloud computing environments. In2011 Second International Conference on Networking and Distributed Computing 2011 Sep 21 (pp. 244-248). IEEE.

[10]. Alhamad M, Dillon T, Chang E. A trust-evaluation metric for Cloud applications. International Journal of Machine Learning and Computing. 2011 Oct 1; 1(4):416.

[11]. Kanwal A, Masood R, Shibli MA. Evaluation and establishment of trust in Cloud federation. In Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication 2014 Jan 9 (p. 12). ACM.

[12]. Whaiduzzaman M, Gani A. Measuring security for Cloud service provider: A Third Party approach. In Electrical Information and Communication Technology (EICT), 2013 International Conference on 2014 Feb 13 (pp. 1-6). IEEE.