A Model to Provide a Reliable Infrastructure for Cloud Computing

Srivaramangai.P, Srinivasan R

Abstract— The cloud computing offers dynamically scalable resources provided as a service over the Internet. It promises the drop in capital expenditure. But practically speaking if this is to become reality there are still some challenges which is to be still addressed. Amongst, the main issues are related to security and trust, since the user's data has to be released to the Cloud and thus leaves the secured area of the data owner. The users must trust the providers. There must be a strong trust relationship exist between the service providers and the users. This paper provides a model based on reputation which allows only reliable providers to provide the computing power and the resources which in turn can provide a reliable infrastructure for cloud computing.

***Index Terms*— cloud computing, security, reliable, trust.**

I. INTRODUCTION

Cloud computing has a lot of common features as Grid computing. It can be argued that the cloud computing has evolved from Grid computing. Grid computing actually provides infrastructure to cloud computing which includes computing and storage resources where as cloud aims at economic based delivering of resources and services. Data Security is of prime importance for any business. A cloud service provider needs to secure its infrastructure, its applications, as well as the stored business data. With cloud computing all the data is stored and processed remotely in another machine. The infrastructure that supports the platform from which the user interacts is unseen by the user. The consumer of services fear that the information stored in cloud may be accessed by hackers. The service providers must also expected to be committed to the local privacy policies of the customers.

Cloud computing contributes a lot to business world. But still Enterprises have a lot of concerns about the reliability and security of these remote clouds. People are not comfortable with the data being stored under the control of third party provider. There is no assurance that the cloud providers will not go out of business. Reliability is the major concerns of the customers of cloud computing.

Manuscript received March 20 , 2012; revised April 12, 2012.

P. Srivaramangai , Senior faculty in Botho college, Gaborone, Botswana 00267-73711179 ; e-mail: srivara.padma@ gmail.com).

R. Srinivasan, Retd.Prof , BSA UNIVERSITY , Chennai, India 0091-9884559965 rs9966@gmail.com .

Cloud computing and its related technologies will only be adopted by users, if they are confident that their data and privacy are secured, and the system is as scalable, robust and reliable as of their own, in their places. Trust and reputation systems have been recognized as playing an important role in decision making on the internet. Reputation based systems can be used in a Grid to improve the reliability of transactions. Reliability is the probability that a process will successfully perform its prescribed task without any failure at a given point of time. Hence, ensuring reliable transactions plays a vital role in cloud computing. To achieve reliable transactions, mutual trust must be established between the initiator and the provider. Trust is measured by using reputation, where as the reputation is the collective opinion of others.

This paper provides a model which introduces a new factor called compatibility which is based on Spearman's rank correlation. The feed backs of the recommenders which are incompatible with those of the initiator are eliminated by using the compatibility factor. Few other factors are also included for measuring the direct trust. This model effectively evaluates the trustworthiness of different entities and also it addresses various malicious behaviors, Two important factors – context and size, are incorporated in evaluating the trustworthiness of entities.

Section 1 of this paper describes the cloud environment and has brought out the importance of the trust mechanism on the successful operation of the cloud. The scope of the research work is defined and the contributions are listed.
Section 2 provides an overview of the related work. Section 3 introduces a new factor called compatibility, which is evaluated using Spearman's rank correlation coefficient and also gives a brief overview of the model. It is shown that using the compatibility factor, eliminates the biased and otherwise incompatible feedbacks and leads to reliable transactions in the cloud. Section 4 presents details about the experiments conducted and also the analysis of the results obtained. Section 6 concludes the paper by summing up the findings and suggesting the scope for future work.

II.RELATED WORK

A number of disciplines have looked at various issues related to trust, including the incremental values assigned by people in transactions with a trusted party and how trust affects people's beliefs and decision making. Considerable work has been done on trust in computer science, most of them being focused in the area of security.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Advanced models in this category compute a weighted average of all the ratings, where the rating weight can be determined by factors such as the raters' trustworthiness / reputation, the age of the rating, the distance between the rating and current score, etc. Xiong and Liu [2004] used an adjusted weighted average of the amount of satisfaction that a user gets for each transaction. The parameters of the model are the feedbacks from transactions, the number of transactions, the credibility of feedbacks and the criticality of the transaction.

Stakhanova [2004] proposed a decentralized reputation based trust model for selecting the best peer. A local table is maintained for each entity to store the transaction records of all the other entities. Each entity table stores the id of all the other entities in the network, their reputation values, the number of bad transactions that occurred and the total number of transactions performed. A concrete formula is presented for calculating the Trust value of the entities willing to provide the resource. Stakhanova actually calculates the mistrust value, and if the value is above a given threshold value, reject the resource.

Tajeddine et al. [2005] proposed an impressive reputation based trust model. This model was extended, and they developed a comprehensive model called PATROL in [2007]. Their works are based on the TRUMMAR model which was developed by Derbas et al [2004] for mobile agents.

Sonnek et al [2007] proposed a model which addresses the unreliability of nodes in a larger scale distributed system. In this model they say that the reliability is not a property but it is a statistics based on a node's performance and behavior. They propose algorithms which employ estimated ratings for reputation.

Xudong N and Junzhou Luo [2008] introduced a trust model which incorporate VO trust relationship in to traditional Grid entities. This model used the clustering analysis to evaluate trust for Grid entities.

Junzhou Luo et al [2008] proposed a model for trust degree based access control in Grid environments. It analyzes the differences between intro domain and inter domain trust .

Benjamin Linder, Scalent System's CEO, [2008] says: *"What I find as CEO of a software company in this space, Scalent Systems, is that most enterprises have a hard time trusting external clouds for their proprietary and high-availability systems. They are instead building internal "clouds", or "utilities" to serve their internal customers in a more controlled way."*

In articles [2009] the security issues with Google Docs different issues are discussed. The Google response to one of them is given in article [2009] Google docs blog spot. There is nothing new in the nature of these vulnerabilities; only their setting is novel. In fact, IBM has repositioned its Rational AppScan tool, which scans for vulnerabilities in web services as a cloud security service in Blue Cloud Initiative [2009].

Hongmei Liao et al [2009] proposed a Reputation model which is based on fuzzy theory. They argue that the trust is fuzzy in nature so it is justified to use fuzzy logic to express and compute trust and reputation.

Alhamad, M et al [2010] proposed a trust model for cloud users to select the reliable resources. It is based on a particular SLA frame work.Zhao-xiong [2011 a] proposes a weighted trust model for cloud . He used a Weighted Trust Information Transfer Algorithm (WTIT Algorithm) and Weighted Trust Information Combination Algorithm (WTIC Algorithm) for making the decision about the trust.

Priyank Singh Hada [2011 b] proposed a mobile agent based trust model for cloud computing. In this paper they give a model for cloud architecture .The model uses mobile agent as security agents to acquire useful information from the virtual machine .This information can be utilized by the users to keep track of privacy of their data and virtual machines.

III. The Model for Reliable Providers

In this approach, the initiator host (client) calculates the reputation value of the target host (provider) based on its previous experiences and gathered feedbacks from other hosts (here the recommenders are the clients). The recommenders who give feed backs can be from the same administrative control (neighbor) or from different trusted domain (friends) or from a completely strange domain (stranger). Direct trust is calculated by using the parameters context and size of the job. Indirect trust is calculated by considering the feedbacks from all other hosts and the feed backs are multiplied by corresponding credibility factors. Total trust comprises of direct trust and indirect trust in which higher weightage is given for direct trust. If the total trust is greater than the minimum prescribed threshold value the model accepts the resource. The provider can be the trusted provider.

In order to allocate weightage to feed backs given by different recommenders , credibility factor is defined. The factor takes values between zero and one; they are based on three parameters, compatibility, activity and specificity . The credibility factor is given by the expression 1 where a, b and c are fractions with a>b>c and a+b+c=1.

Credibility = a*compatibility+b*activity+c * specificity (1)

Where compatibility is given by expression 2.

$$Compatability = 1 - \frac{6\sum_{i=1}^{n}\sum d_i^2}{n(n^2-1)} \quad (2)$$

Where dri gives the difference in ranks.

$$activity = \frac{\text{number of interactions of the recommender entity as a user}}{\text{Total number of interactions by all recommenders as users}} \quad (3)$$

$$\text{Specificity} = \frac{\text{number of interactions of the recommender entity as a provider}}{\text{Total number of interactions by all recommenders as providers}} \quad (4)$$

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The expression 3 and 4 give the activity and specificity.

After this calculation the indirect trust is calculated by using the expression 5 and 6. If there are more than one domain the IT1 represents the trust from the nodes in the same domain and IT2 represents the trust from the different domain.

$$IT1 = \frac{\sum_{t=1}^{n} \delta_{1t}\ rep\ \frac{y}{z_t}}{\sum_{t=1}^{n} \delta_{1t}}$$

(5)

$$IT2 = \frac{\sum_{t=1}^{n} \delta_{2t}\ rep\ \frac{y}{t_t}}{\sum_{t=1}^{n} \delta_{2t}}$$

(6)

Direct trust is calculated by using the expression in 7.

where δ_1 and δ_2 are credibility factors.

$\sum_{t=1}^{n} \delta_{1t}\ rep\ \frac{y}{z_t}$ represents weighted sum of reputations of y as represented by neighbours.

$\sum_{t=1}^{n} \delta_{2t}\ rep\ \frac{y}{t_t}$ represents weighted sum of reputations of y as represented by friends.

For calculating the direct trust , the model assumes that the feedback values given by the user for one kind of job provided by an entity, are different from another kind of job by the same entity. So the model uses three types of trusts, namely, DT1, DT2 and indirect trust. DT1 represents the trust of the user on the provider as a result of the same kind of transactions, and DT2 for different types of transactions. Indirect trust is calculated by the same expression as that of the previous models. Further, this model considers the fact that the reputation values are not always constant. When there is no transaction between two entities for a long period of time then the value of reputation is brought down. Thus this model adopts a function called the decay function, which decreases the value of reputation when there is no transaction, over a given interval. After the elapse of a specific period with out any transaction this decrement is done.

Computation of Trust:

In this model three types of jobs are considered. The jobs can be the transfer of files, printing or computing. Further, the size of the jobs can fall under three categories- small, medium and large. The system assigns the complexity factor based upon context and size (Table 1). Nine different combinations of contexts and sizes of jobs are considered and a complexity factor is assigned for each of the combinations. Thus there are nine types of transactions; from Table 1, it follows that the complexity factor is highest (=1) for large computational jobs, and the smallest (=0.25) for simple file transfer jobs.

Let us consider a scenario where A is the user and wants to use the resource, say the printer of the provider P. Let the job size be medium. Thus, from Table 1, the transaction type is 5. Before submitting the job to P, the user A has to be satisfied about the trust worthiness of P. The system refers to all the previous transactions between the user A and the provider P. If there are any transactions of the same type-s, context and size being the same as per the current requirement, then the average of the reputation values of all these transactions is taken as DT1.Thus $DT1_{x,y,s}$ the direct trust of the user x on y based on the same type of transactions as the present requirement, is given by expression 7.

Table 1 Complexity Table

job type	Context	Size	Complexity Factor
1	C1	S	0.25
2	C1	M	0.4
3	C1	L	0.5
4	C2	S	0.4
5	C2	M	0.5
6	C2	L	0.6
7	C3	S	0.6
8	C3	M	0.8
9	C3	L	1

C1: File transfer, C2: Printing, C3: Computing

$$DT1_{x,y,s} = \frac{\forall \text{ types } s\ \sum_{i=1} r_i}{f_s}$$

(7)

where f_s refers to the frequency of the same type of transactions and r_i corresponds to the reputation value based on the i_{th} transaction.

The direct trust between x and y based on differing type of transactions $DT2_{x,y,d}$ is given by expression 8.

$$DT2_{x,y,d} = \frac{\sum_{k=1}^{n} \sum_{i=1}^{n} or_{iik}}{n}$$

(8)

where n is the number of differing transaction types. If A and P have transacted all the types of transactions, n will be (9-1=) 8. However, if P is not the provider for computational jobs, then n will be (6-1=) 5.

IV . EXPERIMENTS AND RESULTS

The Model has been tested by simulation for applicability in Grid. Since Grid computing can provide a powerful infrastructure for cloud computing this model can be applied for cloud also to provide a reliable infrastructure. The model is compared with one of existing model Patrol Model [2007] and the results are found to be productive. The results are

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

given in the following table. In the simulation, 50 users and 50 providers are taken in to account. For the simulation study users 1-5 and providers 1-5 are malicious. A transaction table is also maintained to keep track of all the transactions. A transaction table is also maintained to keep track of all the transactions. Table 2 gives a summary of the results. In Table 2, column 'YY' refers to the situation, where the Patrol model and proposed model allow transactions to proceed, while column 'NN' corresponds to the denial of transactions by both. Columns 'YN' and 'NY' correspond to disagreement cases. In all there are 15 disagreement cases and Table 3 details them. In all these cases the disagreement is due to the malicious providers or initiators.

Table 2 : Result Summary for Study 1

Simulation	YY	NN	YN	NY	TOTAL
Noof transactions .	54	81	7	8	150
Percentage	36	54	4.6	5.4	100

Models compared: Patrol model & proposed model taken in order

Table 3: Details of Disagreement cases for study 1

S.NO	User	Provider	PATROL Model	Proposed Model
1.	33	1	YES	NO
2.	26	5	YES	NO
3.	25	2	YES	NO
4.	19	3	YES	NO
5.	2	14	YES	NO
6.	34	3	YES	NO
7.	22	33	NO	YES
8.	21	18	NO	YES
9.	13	23	NO	YES
10.	22	33	NO	YES
11.	11	21	NO	YES
12.	28	8	NO	YES
13.	42	12	NO	YES
14.	23	16	NO	YES
15.	13	22	NO	YES

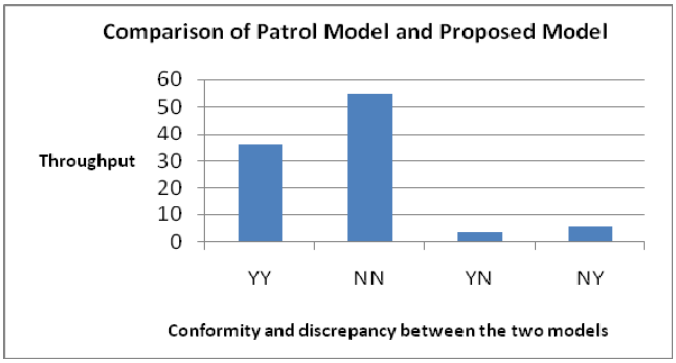

Figure 1 Comparison of the Results of the PATROL Model & Proposed model

Figure 1 shows the allocation by the two models. The agreement between the existing model and the proposed model is found to be 90% and the disagreement is 10%, and each of the disagreement cases has been analyzed.

Here, the throughput specifies the percentage of the number of reliable successful transactions. Since this model considers the two way reputation along with the context and size of the job, the accuracy of the output is further increased. This model decides whether to grant the transactions or not, based upon the previous transactions and referrals from the other entities.

The simulation study 2 is conducted by varying the number of transactions. The model was initially tested with 150 transactions. Since the Grid consists of a large number of resources with a large number of transactions, the model was tested by increasing the number of transactions. The number of entities was fixed at 100. The percentage of malicious entities is 10%. The number of transactions was varied from 10 to 7000, and the results were noted. From Figure 2 it can be seen that the percentage of reliable and successful transactions is higher with the proposed Model as compared to the Patrol model.

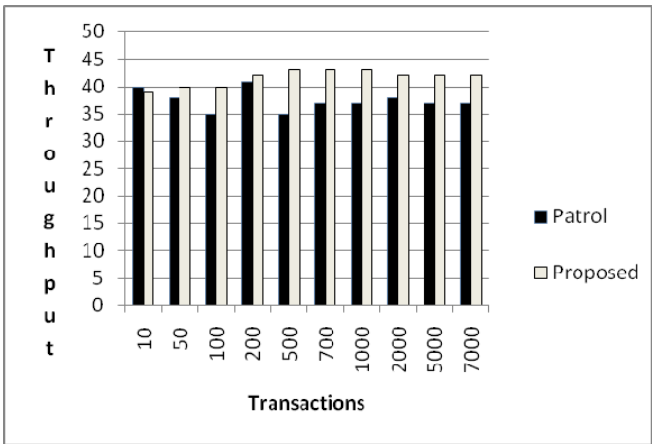

Figure 2 Comparison of the models by varying the numbers of transactions

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The accuracy of the model can be defined as:

$$\text{Accuracy} = \frac{\text{Number of correct Decisions} \times 100}{\text{Total number of Decisions}} \quad (9)$$

Table 4 : Comparison of the Accuracy values for the Two Models

Malicious Nodes	Patrol Model	Proposed Model
0%	98%	100 %
10%	94 .6%	100 %
20%	93%	100 %

From Table 4 it follows that:

(i) Of the 2 models the Patrol model has the lowest accuracy.

(ii) Accuracy decreases as the percentage of malicious nodes increases.

A note of caution has to be issued at this stage. The accuracy so evaluated is the percentage of 'correct' decisions under specified conditions: i) malicious user ii) malicious provider (iii) specified contexts. These are the accuracy values obtained under the simulation study. The accuracy under 'field conditions' may be lower since field constraints may not exactly fit with the models considered. However, in all the cases, the relative ordering of the accuracy levels among the models will remain unaltered. Table 5, presents a comparison of the throughputs for the 2 models with various percentages of malicious nodes.

Table 5 : A comparison of the throughput of the two models

Malicious Nodes	Patrol Model	Proposed Model
0%	43%	44%
10%	40.6 %	41.4 %
20%	39 %	41 %

From Table 5 it can be concluded that the throughput decreases with an increasing percentage of malicious nodes; the throughput remains essentially at the same level, when the number of nodes is zero percent.

V .Conclusion

This paper suggests a model for improving the reliability in Grid computing. Since cloud computing is evolved from Grid computing and security is one of most burning issue in cloud computing this model can be very well used in cloud computing to improve the reliability. It is shown that the reliability of the transaction is improved with the inclusion of different parameters. The experimental results have established the usefulness of this model.

REFERENCES

[1] "Disaster-Proofing" http://www.forbes.com/2008/11/24/cio- .[Jan 25,2012].

[2]. "Security issues with Google Docs" : http :// www. peekay.org/security-issues-with-Google-docs. March.26,2009 [Jan 23,2012]

[3] "Google docs ": http://googledocs.blogspot.com/2009/03/just-to-clarify.html.. [Jan 25,2012]

[4]. BlueCloud.http://www- ibm.com/26642.wss. [Jan 24,2012]

[5] Priyank Singh Hada, Ranjita Singh and Mukul Manmohan. " Security Agents: A Mobile Agent based Trust Model for Cloud Computing", *International Journal of Computer Applications* 36(12):12-15, December 2011. Published by Foundation of Computer science, New York, USA.

[6] Alhamad, M.; Dillon, T.; Chang, E " SLA based trust model for cloud computing", published in the proceedings of 2010 13th International Conference on Network-Based Information Systems.

[7] Zhao-xiong ZHOU, He XU, Suo-ping WANG ,"A Novel Weighted Trust Model based on Cloud", Advances in Information Sciences and Service Sciences. Volume 3, Number 3, April 2011.

[8] Stakhanova N., Ferrero S., Wong J. and Cai Y., [2004], "A reputation-based trust management in peer-to-peer network systems, International Workshop on. Database and Expert Systems Applications, pp. 776-781.

[9] Tajeddine, A., Kayssi, A., Cheab, A. and Artail, H. (2005) 'A comprehensive reputation-based trust model for distributed systems', The IEEE Workshop on the Value of Security through Collaboration (SECOVAL), September 5–9, Athens, Greece, Vol. 1, Nos. 3–4, pp.416–447.

[10]Tajeddine A, Ayman Kayssi, Ali Chehab, and Hassan Artail, [2007]," PATROL: a comprehensive reputation-based trust model", Int. J. Internet Technology and Secured Transactions, Vol. 1, Nos. 1/2, pp 108-131.

[11]Xiong L., and Liu L. , (2004) 'PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities' , IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 7, pp 843-857.

[12]Junzhou Luo, Xudong Ni "A clustering analysis and agent-based trust model in a grid environment supporting virtual organizations", International Journal of Web and Grid Services (IJWGS),Volume 5 - Issue 1 – 2009.

[13]Jason Sonnek, Abhishek Chandra, jon B. Weissman, IEEE Transactions on Parallel and Distributed systems, vol. 18, no. 11, november 2007.

[14] Junzhou Luo, Zhiang Wu, Jiuxin Cao, Tian Tian, "Dynamic Multi-Resource Advance Reservation in Grid Environment," The Journal of SuperComputing, Springer , Netherlands, 2008.

[15] Hongmei Liao,QianpingWang,Guoxin Li,"A Fuzzy Logic-Based Trust Model in Grid, International Conference NSWCTC '09.2009, Page(s): 608 – 614.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)