International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

A Generalized Trust Model for Computational Grids & Clouds

G Mahesh Kumar, S Ramachandram, Jayadev Gyani

Abstract*: In the present era, world is moving very rapidly with internet for sharing of resources and services. There are many heterogeneous and complex applications to be executed within less time. The complex applications require lot of resources such as processing, storage, etc, for execution but due to the constrained resources available within a system, the applications may not execute perfectly. Grid Computing is the technology used to integrate various heterogeneous systems from different boundaries of the world to execute complex applications. This technology creates a virtual organization where huge set of systems are integrated to solve very complicated and critical problems. There are many people who are not able to set up a real organization with lot of infrastructure and other services for execution of applications. Cloud Computing is the technology which provides lot of services like software, hardware, networking and much more for less cost. This technology supports pay-as-you-go model in which the user will pay the amount only for the used services. The major problem is to trust Grid Service Providers, Grid Users, Cloud Service Providers and Cloud Users for doing the transactions, in their respective environment, as there are many systems from various domains participating in the transactions. This paper proposes a generalized Trust Model for Cloud/Grid Computing Environment (T-CGE) to establish very strong trust among the Cloud/Grid Service Providers and Cloud/Grid Users. This paper also demonstrates the reliability statistics by using Cronbach's Alpha to show the relative consistency of data. ANOVA (Analysis of Variance) is used to show the variations among the service parameters of all service providers, and also variations among the service providers. The T-CGE trust model helps the end users to get better and consistent services from their application developers.

Keywords : Grid Computing, Cloud Computing, Grid Service Providers, Cloud Service Providers, Grid Users, Cloud Users, Trust Model.

I. INTRODUCTION

The distributed computing is the technology used to process the applications by extracting data which is distributed and stored on remote systems. The systems involved in computing may be homogeneous / heterogeneous with different size and structure.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
G Mahesh Kumar*, Assistant Professor, Department of Computer Science, Bhavan's Vivekananda College, Sainikpuri, Secunderabad, India. maheshkumar.cs@bhavansvc.ac.in
Dr. S Ramachandram, Professor, Department of CSE, Osmania University, Hyderabad, India. schandram@gmail.com
Dr. Jayadev Gyani, Assistant Professor, Department of CS, CCIS, Majmaah University, Saudi Arabia. jayadevgyani@yahoo.com

The grid and cloud computing are derived from distributed computing.

The most important component of any system is the resource. The systems with huge set of resources can easily process the applications and gives the results very much faster. But every individual system may not hold very huge set of resources for processing a critical application which is very complex to solve. Grid Computing solves the problem mentioned by integrating the idle systems for accessing resources available in those systems to solve complex problems. The entities such as Grid Service Providers and Grid Users must and should be authenticated entity only. Every user relies on the providers for accessing the authentic resources inorder to solve the problems. The applications such as Telecommunications, Automobiles, Scientific Applications, Healthcare, Research and Development, etc., uses Grid Computing technology.

The users who want to establish a virtual organization with low cost, then, Cloud Computing technology is the best solution. This is the process where the people can hire the required services such as hard disk, memory, routers, software, operating systems and many more for minimum cost. The user can scale-up and scale-down the resources when required. The users need to pay only for the resources utilized and no extra cost will be borne by the user. The SLA (Service Level Agreement) is the most important feature in which all the terms and conditions mentioned about the services allocation, payment details and also the penalty issues if it is violated. The Cloud Service Providers needs to be authentic inorder to function according to the SLA. The fields such as Robotics, Automations, Research, Medicare Applications, etc., are using Cloud Computing technology.

Every technology needs to be authentic and trusted. In Cloud/Grid Computing many heterogeneous systems are involved for providing and accessing the services and/or resources, there are chances for misusing of services/resources by the users and providers. There is a requirement of a strong trust model to integrate and use the services from the Cloud/Grid environment. This paper proposes a T-CGE trust model for establishing trust in both Cloud and Grid environment.

II. TRUST

Trust is one of the important factors to do any transaction perfectly. Trust is being defined as a belief and to have faith in others inorder to complete their job with the terms and conditions specified and in an authenticated manner. The Cloud/Grid users require services/resources only from authenticated and reliable service providers.

Trust is categorized into direct trust and indirect trust.

Direct trust will be established when user and provider make a direct interaction for a given transaction and they know each other, so that one entity can believe the other entity, and third party is not required between them for assurance. **Indirect trust** is the process where the user and provider will not have any frequent interactions and the third party will be recommending them for doing a transaction. In this scenario trust will be in doubt, since the two entities do not know each other directly. This indirect trust can be slowly transformed into direct trust when the two participating entities will believe each other and build good reputation to do a genuine transaction without any further recommendations from a third party.

III. RELATED WORK

Dimitrios Zissis et.al [1] addressed the cloud computing security issues. The security is an important component which is used to build trust in clients. This paper highlighted the vulnerabilities and threats that occur while sharing information. The confidentiality, integrity and authentication techniques have been used inorder to maintain strong trust among clients and also data protection can be done by cryptography.

Atoosa Gholami et.al [2] proposed a trust model for resource selection in cloud computing environment. This paper highlighted the service quality such as bandwidth, cost, response time, and also the execution speed inorder to select a reliable resource.

Rizwana Shaikh et.al [3] proposed a trust model for measuring security strength of cloud computing service. This paper demonstrates the usage of parameters like confidentiality, authorization, authentication, data protection, isolation, virtualization, compliance for security. This model calculates the trust value and measures security strength.

Marco Anisetti et.al [4] proposed a certificate-based trust model for autonomic cloud computing systems. The usage of certificates for providing security and to process chains of trust to establish trust in cloud computing is shown in this paper.

Mohammed Alhamad et.al [5] proposed a SLA based trust model for cloud computing in which Service Level Agreement details are used to find the trust among the various cloud providers.

Praveen S Challagidad et.al [6] proposed trust management in cloud computing. This paper explains the working of Reputation and Trust Management Algorithm with the help of third party trust evaluator to calculate trust value.

Ritu et.al [7] proposed a trust model in cloud computing based on Fuzzy Logic. This model explains the usage of fuzzy logic based on the quality of service parameters such as turnaround time, networking speed, cost, computing power and security level.

Vadym Mukhin [8] proposed the rating mechanism for the trusted relationship establishment for the security of the distributed computer systems. In this mechanism a new node is added to the distributed computer systems and it follows the initial security policy since it does not have any prior statistical information of trust. Many nodes interact in the distributed computer systems, and if the new node intentionally does any un-trusted activity, its rating will be decreased. Similarly any node in the process of communication increases its trust levels if there is no un-trusted activity performed.

Avula Anitha [9] proposed trust management in grid-trust assessment and trust degree calculation of a resource – a novel approach. This paper provides a trust assessment and trust degree calculation mechanism using subjective logic to provide the reliable trusted resources for a grid user and to maintain the integrity & accuracy of results with faster response.

Vincent C. Emeakaroha et.al [10] proposed a paper on establishing trust in cloud services via integration of cloud trust protocol with a trust label system. This paper integrates the cloud trust protocol with trust label system to enable and make complete visibility of operational information about the cloud services to the users.

Neeraj Mangla et.al [11] proposed a trust based cloud framework for service provider selection. This paper shows the architecture of a trust based cloud model for selecting the cloud provider using direct trust, indirect trust and cloud service providers credentials. Hongmei Liao et.al [12] proposed a fuzzy logic based trust model in grid. This paper uses fuzzy logic to compute the trust value.

IV. PROPOSED TRUST MODEL

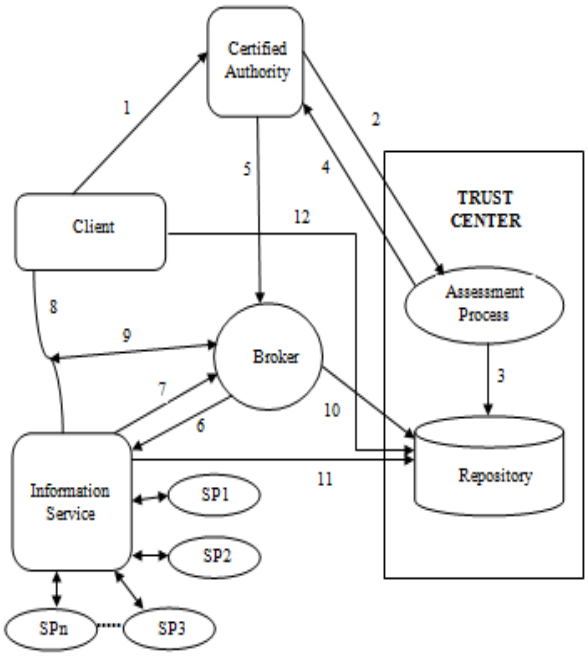

Figure-1: Trust Model for Cloud/Grid Environment (T-CGE)

The above figure-1 depicts a T-CGE trust model used for both cloud and grid users to extract trusted service providers. The main entities of this trust model are as follows:

1. **Certification Authority:** This entity is responsible to accept the authenticated client requests for the trusted service providers information and connects to the Trust Center entity to extract the top trusted service providers information.

2. **Trust Center:** This entity acts as a server, holds a repository for storing service providers services information and also clients service utilization details. This entity uses an Assessment Process to extract the top trusted service providers information.
3. **Repository:** This entity is used to store the details of SLA, services provided by service providers and client service utilization details after their transaction is over.
4. **Broker:** This entity is used to communicate with the Information Service entity to check the services/resources availability of the top service provider. It is also part of the negotiation made among the clients and service providers for the finalization of the SLA.
5. **Information Service:** This entity will be maintaining a list of service providers which has services/resources available for service.
6. **Client:** This entity is an end user, requests for the services/resources from the authenticated and trusted service providers.
7. **Service Provider (SP):** This entity provides the services required by client on registering with their available resources with Information Service.

The flow of operations in the T-CGE trust model is as follows:

1. Client requests the Certified Authority for the top trusted service providers information.
2. Certified Authority requests Trust Center for top trusted service providers information based on the client requirements.
3. Trust Center uses Assessment Process to extract top trusted service providers information from the repository.
4. Extracted trusted service providers from repository through Assessment Process is given to Certification Authority.
5. Certification Authority requests the Broker for services/resources availability with the top service providers identified from the repository.
6. Broker requests Information Service for the availability of services/resources with trusted service providers for the client requirement.
7. Extraction of service providers list that satisfy client requirements.
8. Arranging the discussion/negotiation between the client and service providers through Information Service.
9. The Broker fix-up SLA between client and service provider through Information Service according to the client requirements.
10. Updating the SLA details with the repository by Broker for further assessment process.
11. Repository updation of service providers services for the client through Information Service.
12. Repository updation by client for the service satisfaction, enhancement of services on the SLA implementations by service providers.

The parameters that are considered for this proposed trust model, for computing the trust value, are response time, fault tolerance, reliability, security, elasticity and SLA.

a) **Response Time:** The elapsed time between the client request and response. This is being measured in milliseconds.
b) **Fault Tolerance:** This is the process wherein one system is down when the client request was under process; then, immediately that request needs to be handled by another system without any halting of the process which leads to problems for the clients.
c) **Reliability:** This is the process wherein all the transactions need to be performed in the genuine and authenticated manner.
d) **Security:** This parameter is used to perform a secure transaction by providing the factors such as confidentiality, integrity and privacy of data.
e) **Elasticity:** This is the process where the services/resources can be increased or decreased according to the client requirement at any point of time.
f) **Service Level Agreement:** This ensures that all the services/resources mentioned in SLA are available without any interruption, and if any violation of SLA occurs, the penalties to be imposed on the service providers or the users are also mentioned.

V. EXPERIMENTS AND RESULTS

The T-CGE trust model is used to retrieve the trusted service providers for facilitating the client as per their requirements. In this trust model, to perform the experiments, parameters such as Response Time, Fault Tolerance, Reliability, Security, Elasticity and Service Level Agreement are used for supporting both Cloud users and Grid users. This trust model is a generalized model wherein both Cloud and Grid users can use to get the services/resources from the trusted service providers.
The experiment includes 20 service providers wherein each service provider has been considered with 1000 records of data set and total of 20000 records from the authenticated source.

1. Response Time

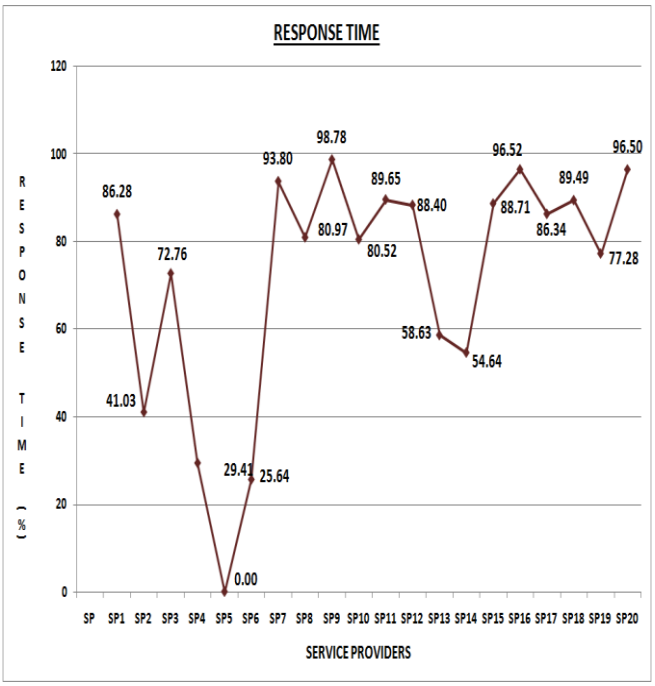

Figure-2: Results of Response Time

In the above figure-2, Response Time [13] parameter is shown for 20 service providers i.e., SP1 to SP20 where SP respresents Service Provider. The service provider SP9 has been given the first rank since it's response time is very fast compared to other service providers as it is shown 98.78% with highest response rate , that is with minimum delay. The SP5 is very slow in giving response for the user since it has maximum delay compared with other service providers.

2. Fault Tolerance

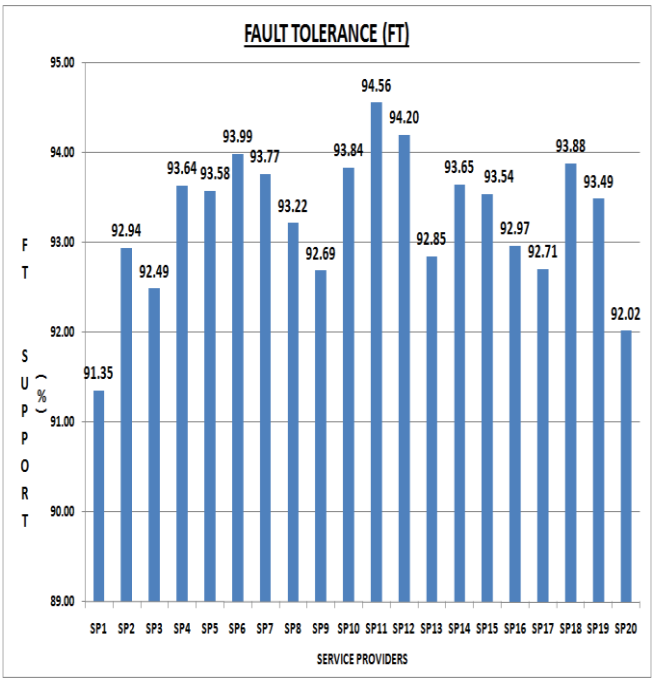

Figure-3: Results of FaultTolerance

In the above figure-3, Fault Tolerance [14] parameter is considered for 20 service providers i.e, from SP1 to SP20, and where SP11 is having the highest Fault Tolerance capacity with 94.56% and SP1 is having the least Fault Tolerance capacity with 91.35%.

3. Reliability

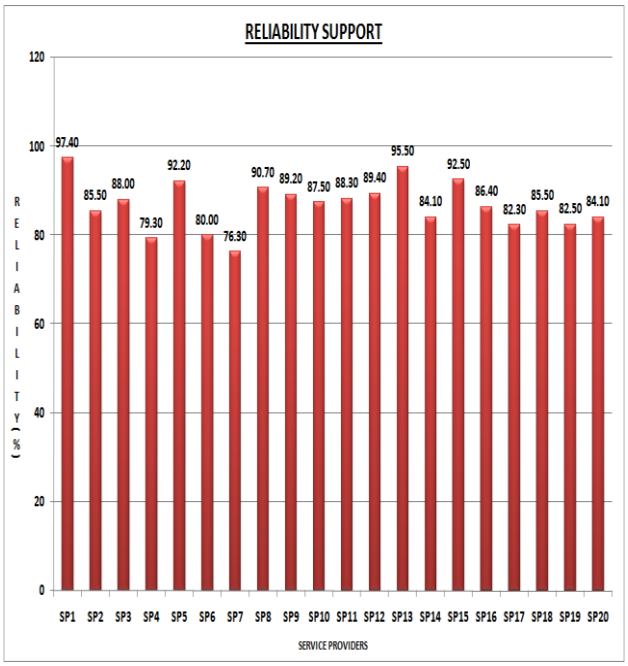

Figure-4: Results of Reliability

In the above figure-4, Reliability [15] parameter is being depicted for 20 service providers i.e., from SP1 to SP20. In this, SP1 is leading with 97.40% and SP7 is having 76.30% with least reliability.

4. Security

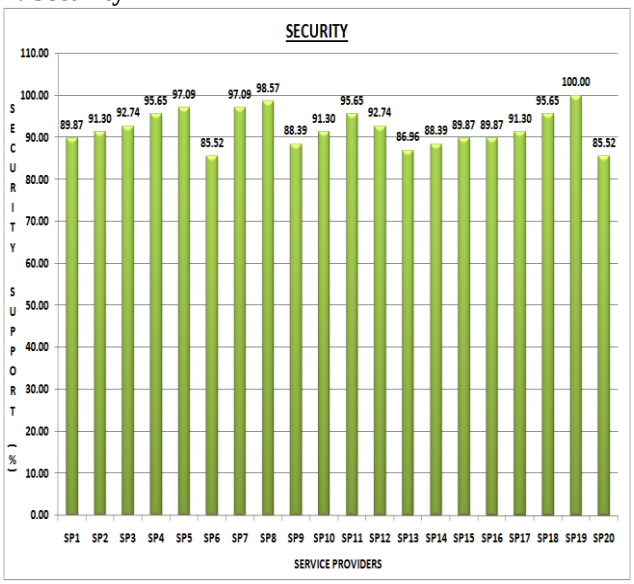

Figure-5: Results of Security

The above figure-5, depicts the Security parameter for all the 20 service providers i.e., from SP1 to SP20. The service provider SP19 is providing 100% security and SP6 & SP20 are providing the least security with 85.52%.

5. Elasticity

Elasticity parameter in figure-6, is shown below for 20 service providers, i.e., from SP1 to SP20. Among all the service providers, SP20 is leading with 100% elasticity and SP2 is with the least elasticity of -88.46%.

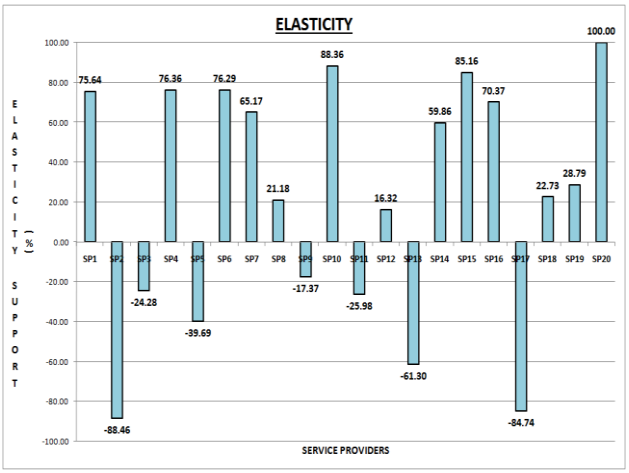

Figure-6: Results of Elasticity

6. Service Level Agreement(SLA)

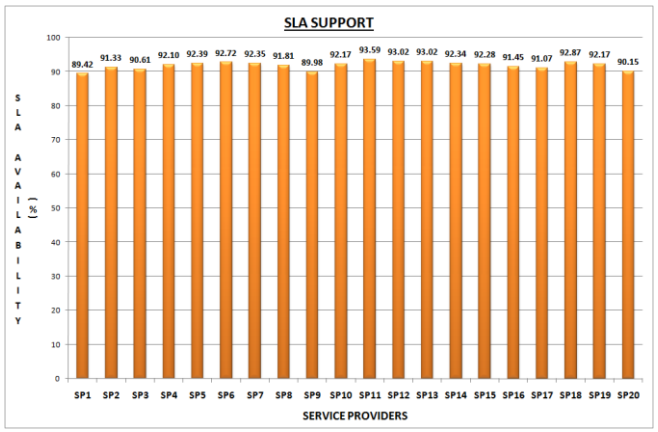

Figure-7: Results of SLA

The above figure-7, depicts the SLA Availability [14] for all the 20 service providers i.e., from SP1 to SP20, in which SP11 is having maximum SLA Availability with 93.59% and SP1 with least rating of 89.42%.

Trust Model with Service Parameters for all Service Providers

SERVICE PROVIDER	RESPONSE TIME	FAULT TOLERANCE	RELIABILITY	SECURITY	ELASTICITY	SLA SUPPORT	TOTAL	TRUST VALUE
SP1	86.28	91.35	97.40	89.87	75.64	89.42	529.96	88.33
SP2	41.03	92.94	85.50	91.30	-88.46	91.33	313.64	52.27
SP3	72.76	92.49	88.00	92.74	-24.28	90.61	412.31	68.72
SP4	29.41	93.64	79.30	95.65	76.36	92.10	466.46	77.74
SP5	0.00	93.58	92.20	97.09	-39.69	92.39	335.57	55.93
SP6	25.64	93.99	80.00	85.52	76.29	92.72	454.16	75.69
SP7	93.80	93.77	76.30	97.09	65.17	92.35	518.48	86.41
SP8	80.97	93.22	90.70	98.57	21.18	91.81	476.45	79.41
SP9	98.78	92.69	89.20	88.39	-17.37	89.98	441.67	73.61
SP10	80.52	93.84	87.50	91.30	88.36	92.17	533.69	88.95
SP11	89.65	94.56	88.30	95.65	-25.98	93.59	435.77	72.63
SP12	88.40	94.20	89.40	92.74	16.32	93.02	474.08	79.01
SP13	58.63	92.85	95.50	86.96	-61.30	93.02	365.66	60.94
SP14	54.64	93.65	84.10	88.39	59.86	92.34	472.98	78.83
SP15	88.71	93.54	92.50	89.87	85.16	92.28	542.06	90.34
SP16	96.52	92.97	86.40	89.87	70.37	91.45	527.58	87.93
SP17	86.34	92.71	82.30	91.30	-84.74	91.07	358.99	59.83
SP18	89.49	93.88	85.50	95.65	22.73	92.87	480.12	80.02
SP19	77.28	93.49	82.50	100.00	28.79	92.17	474.22	79.04
SP20	96.50	92.02	84.10	85.52	100.00	90.15	548.29	91.38

Table-1: Consolidated Service Parameters

The above table-1 depicts the consolidated service parameters values along with the trust value for all the service providers ie., SP1 to SP20.

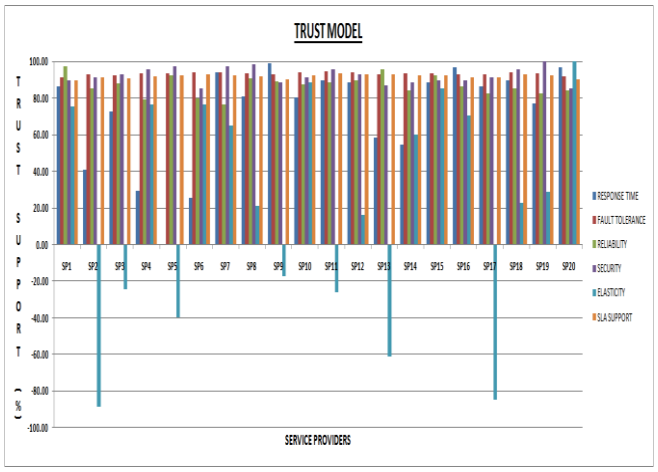

Figure-8: Results of Service Parameters

The above figure-8, depicts the trust model with all six individual service parameters for all the service providers ie., SP1 to SP20 considering the values from table-1. It helps to compare all the service parameters with respective to each and every individual service provider. This figure guides the clients to identify the services provided by the service providers, and also helps service providers to improve their quality of service parameters in which they are lacking.

Final Trust Model

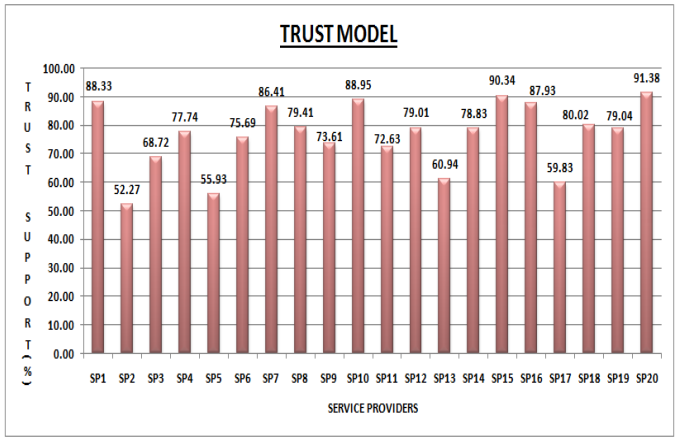

Figure-9: Results of Final Trust Model

The above figure-9, shows the aggregate results of all the six service parameters for 20 service providers i.e., from SP1 to SP20 as the Trust Value depicted in table-1. In this, SP20 is given first rank as top 1 service provider with 91.38% and SP2 is given the last rank since it has only 52.27%.

Reliability of the Data

Reliability refers to the context to which responses are consistent. Cronbach Alpha helps to measure the internal consistency of data to study for further analysis. If the α value is $\geq$0.6, such data can be acceptable for further study. In the present study, Cronbach Alpha α is computed for various service providers and the services provided by them using SPSS.

Table-2: Reliability Statistics of T-CGE Trust Model

Cronbach's Alpha	N of Items
0.638	20000

In the above table-2, Cronbach Alpha was found as 0.638, suggesting that the items have relative consistency. This result indicates the validity and reliability as GOOD. Hence, the data is used for statistical analysis.

ANOVA: Analysis of Variance(ANOVA) used to test the significant differences between means.

HYPOTHESIS

H_{10}: There is no significant difference in the service providers.
H_{20}: There is no significant difference in the services provided by the service providers.

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Rows	15549.21	19	818.3793	1.119781	0.344692	1.69707
Columns	76751.33	5	15350.27	21.00364	4.38E-14	2.310225
Error	69429.65	95	730.8385			
Total	161730.2	119				

Table-3: ANOVA Results of T-CGE Trust Model

In the above table-3, F(19,95) = 1.119781, p = 0.344692> 0.05, hence there is no significant difference between the various service providers. We accept H_{10} and conclude that there is no significant difference between the various service providers. When the comparisons are drawn to analyze the parameters provided by the service providers it was observed that there is a significant difference between the parameters provided. Calculated F value is 21.00364 and p value is .000 which is less than 0.05 and denotes variations in the parameters. Hence, we reject H_{20} and conclude that there is a significant difference between the services provided by the service providers.

VI. CONCLUSION & FUTURE WORK

Distributed Computing is a phonemenon used by all organizations throughtout the world for sharing of resources and services. The shared services/resources needs to be authentic and also the entities involved in the shared transactions should be authentic. At present there are a number of entities who misuse the services/resources intentionally to create a bad reputation of the service providers. The trust establishment between the entities either client, server or any communicating device is very critical. This paper has proposed a generalized T-CGE ie., Trust Model for Cloud/Grid Environment, used for establishing trust among the entities involved in Cloud Computing and Grid Computing. The experiments were done by collecting the datasets from the authenticated source and results generated by demonstrating which service providers are good when individual parameters are considered and which service providers are top, when on aggregate results are considered. These results also help the service providers to know where they stand in the competition on par with other service providers. They can also verify the service parameters in which they are poor and aim for improving those parameters for providing good quality of services for the clients. The reliability test was done using Cronbach Alpha which shows the internal consistency of data. In our result the Cronbach Alpha value is 0.638, demonstrating that there is a relative consistency among the items selected and is used for further analysis. ANOVA is also used to check the variation among the service parameters and service providers by framing the hypothesis. In future, we can try to enhance this model by developing some algorithms to track the malicious clients who intentionally want to corrupt the services/resources provided by service providers. It is also recommended that the cloud providers needs to maintain the end user satisfaction and feedback for assessing the best clients(application developers).

REFERENCES

1. Dimitrios Zissis, Dimitrios Lekkas, "Addressing Cloud Computing Security Issues", Future Generation Computer Systems 28(2012), Page(s) 583-592, http://dx.doi.org/10.1016/j.future.2010.12.006.
2. Atoosa Gholami, Mostafa Ghobaei Arani, "A Trust Model for Resource Selection in Cloud Computing Environment", Journal of Informatics and Computer Engineering, Volume 2(2), January 2016, Page(s) 41-48.
3. Rizwana Shaikh, Dr. M. Sasikumar, "Trust Model for Measuring Security Strength of Cloud Computing Service", Procedia Computer Science 45(2015), Page(s):380-389, doi:10.1016/j.procs.2015.03.165.
4. Marco Anisetti, Claudio A. Ardagna, Ernesto Damiani, "A Certification-Based Trust Model for Autonomic Cloud Computing Systems", IEEE International Conference on Cloud and Autonomic Computing, 2014, IEEE Computer Society, Page(s):212-219.
5. Mohammed Alhamad, Tharam Dillon, Elizabeth Chang, "SLA-Based Trust Model for Cloud Computing", IEEE International Conference on Network-Based Information Systems, 2010, Page(s): 321-324, DOI 10.1109/NBiS.2010.67.
6. Praveen S Challagidad, Mahantesh N Birje, "Trust Management in Cloud Computing", International Conference on Smart Technology for Smart Nation, IEEE, Page(s): 295-298.
7. Ritu, Sushma Jain, "A Trust Model in Cloud Computing based on Fuzzy Logic", IEEE International Conference On Recent Trends In Electronics Information Communication Technology, 2016, Page(s): 47-52.
8. Vadym Mukhin, "The Rating Mechanism for the Trusted Relationship Establishment for the Security of the Distributed Computer Systems",International Journal of Computer Network and Information Security, Volume 6, 2014, Page(s): 41-47.
9. Avula Anitha, "Trust Management in Grid-Trust Assessment and Trust Degree Calculation of a Resource – A Novel Approach", Journal of Computer and Communications,Volume3,2015,Page(s): 34-41, http://dx.doi.org/10.4236/jcc.2015.36005.
10. Vincent C. Emeakaroha, Eoin O' Meara, Brain Lee, Theo Lynn, John P Morrison, "Establishing Trust in Cloud Service via Integration of Cloud Trust Protocol with a Trust Label System", International Conference on Cloud Computing and Services Science, 2017, Page(s): 590-597.
11. Neeraj Mangla, Sanjeev Rana, Manpreet Singh, "Trust Based Cloud Framework for Service Provider Selection", Advances in Computational Sciences and Technology, Volume 10, 2017, Page(s): 2519-2525.
12. Hongmei Liao, Qianping Wang, Guoxin Li, "A Fuzzy Logic-Based Trust Model in Grid", IEEE International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, IEEE Computer Society, Page(s): 608-614.

13. Source: ftp.pdl.cmu.edu/pub/datasets/hla/
14. Source: http://fta.scem.uws.edu.au/index.php?n=Main.DataSets
15. Source: www.uoguelph.ca/~qmahmoud/cgi-bin/display.pl

AUTHORS PROFILE

G Mahesh Kumar holds the position of Assistant Professor, Department of Computer Science, Bhavan's Vivekananda College, Sainikpuri, Secunderabad, Telangana, India. He is currently pursuing his Ph.D. in Computer Science & Engineering from JNTU Hyderabad. He has done his Masters in Infromation Systems, M.Tech(CSE) from Osmania University. He has presented & published papers in national and international conferences. He has published research papers in international journals. He teaches subjects such as Java Programming, Advanced Java Programming, Python Programming, Mobile Computing, Software Engineering, Information Security, BigData Analytics for both undergraduate and post-graduate students. His research areas include Grid Computing, Cloud Computing, and Mobile Computing.

Dr. S. Ramachandram received his bachelor's degree in Electronics and Communications Engineering (1983), M.Tech(CSE) (1985) and Ph.D. in Computer Science & Engineering (2005). He is presently working as a Professor, Department of Computer Science & Engineering, University College of Engineering, Osmania University, Hyderabad, Telangana, India. His research areas include Cloud Computing, Mobile Computing, Grid Computing, Server Virtualization, Software Engineering and, Big data Analytics. He has authored several books on Software Engineering, Operating Systems, handled several national & international projects and published several research papers at international and national level. He is the former Vice-Chancellor, Osmania University. He also held several positions in the university as a Principal, Vice-Principal, University College of Engineering, Osmania University, Chairman Board of Studies, Nodal Officer for World Bank Projects and chair of Tutorials Committee. He is a member of Institute of Electrical and Electronic Engineers (IEEE), Computer Society of India (CSI) and Institute of Electronics and Telecommunication Engineers (IETE).

Dr. Jayadev Gyani, currently holds the position of Assistant Professor in Majmaah University, Al-Majmaah, Kingdom of Saudi Arabia. He received his Doctoral degree in Computer Science from University of Hyderabad in 2009 and Master of Technology in Computer Science and Engineering from Osmania University, INDIA in 1994.He worked at several levels such as Lecturer, Assistant Professor, Professor & Head of CS department. His overall teaching experience is 24 years. He handled several subjects such as Software Engineering, Algorithm Analysis and Design, Programming Languages, Assembly Language Programming, Software Evolution, Software Architectures, Low-Level Design of Software, Design Patterns, Artificial Intelligence, Parallel Architectures and Parallel Programming. He taught students at Undergraduate and Post- Graduate Levels. He has been guiding research students from JNTU, Hyderabad and JNTU, Kakinada. His research interest includes Software Engineering, Bigdata Analytics, Distributed computing, Machine learning algorithms and their applications.