International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||07||Pages||6207-6210||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i7.50

Reputation Systems in Cloud: A Review

Neeraj[1], Major Singh Goraya[2], Damanpreet Singh[3]

[1,2,3] Sant Longowal Institute of Engineering and Technology, Longowal, India

Abstract: ***The requisition of cloud is increasing at a high rate because of its enormous benefits such as on demand access, pay as you use,and lower upfront cost. Due to huge demand of cloud based services, the number of cloud service providers(CSPs) is also increasing rapidly.To make more money the CSPs exaggerates with the Quality of service (QoS) of their services as mentioned in service level agreement (SLA).The confusion arises for the service user (SU) in the selection of CSP. Thus, selecting a trustworthy CSP is a bigger challenge for the serviceusers (SUs). Security is also a major concern. To overcome all these problems there is a need of defining reputation system for identifyingthe trusted cloud service provider. Because of this reason resource management and reputation management is addressed individually andjointly in previous research work where resource management handles the load and reputation management helps in selecting thetrustworthy service provider. In this paper, we have discussed various reputation modals and their efficiency.***

Keywords: *Cloud, Quality of service(QoS), Reputation management, Service level agreement(SLA).*

1. Introduction

Cloud computing, a model for enabling access from anywhere, easy to use, on demand service with high agility, is the interconnection of remotely accessed distributed servers that provide the reliable services to the end user [1]. Cloud provides three types of services such as: Infrastructure as a service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and four deployment models Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud.

Cloud provides enormous benefits therefore the demand of cloud based services is increasing day by day. Due to huge demand, many big IT organizations such as Google, Microsoft, Amazon, Rackspace etc., established themselves as a role of cloud service provider [2]. Every organization has their own offerings. Some CSPs exaggerates their offerings so it is very tedious for a service user (SU) to choose a trustworthy Cloud Service provider (CSP). Reputation mechanisms plays a vital role to make a final decision in selection of cloud based services. The reputation system was first introduced in online auction site such as eBay.com [3]. There are also some websites such as Bizrate.com which finds the ranking of retailers based on customer reviews.

Further, to explore the reputation systems the initial searches are performed. The articles found this topic suggesting the need of reputation to include in the useful part of research. The focus of this paper is to provide an overview of existing reputation systems.

The paper is structured as follows, the next section introduces the need of reputation systems. Section 3 introduces the various reputation systems. Section 4 concludes the research work.

2. Why Reputation Systems?

Internet has created much opportunities for interaction with word wide service providers. For accessing the Quality of service (QoS) and the reliability of other entities in cloud environment there are currently a few methods. Reputation systems plays a key role to solve this issue by enabling the cloud service consumer to access the reliable quality of service and reliability in accessing to different entities before they start their services and also decides that they must interact with the party in the future. Reputation system restores the shadow of each transaction so that other people can plan.

3. A Brief Survey of Reputation Systems

Most of the work is done in the field of reputation management and reputation management on the systems. System Reputation is assessed using feedback from the peers. The primary studies on the reputation systems are as follows:

3.1. The Beta Reputation Systems

In [3], A. Jøsang and R. ZIsmail proposed a Beta reputation system. The system contains reputation engine and a propagation mechanism (centralized). The engine is based on beta probability density function which can be used to represent probability distribution of binary search. The system is much more flexible and relatively simple to implement in practical applications. Beta reputation system can be used in both centralized and decentralized manner.The beta reputation system is based on theory of statistics.

3.2. Eigen Trust in P2P Network

S.D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina, designed an algorithm that is The EigenTrust Algorithm for Reputation Management in P2P Networks [4]. This algorithm is based on peer to peer file sharing network and the algorithm decreases the number of downloads of inauthentic files. The file sharing network assigns each peer a global trust value on the basis of peer's history of uploads. This helps the peers in selection of trustworthy peers from whom they download, the network efficiently finds out the malicious peers and isolates

them from the network. The algorithm evaluates the global reputation of each node by their local reputation. It is also necessary to normalize them in some way because a malicious node will assign the high reputation to another malicious node. Therefore, a normalized trust value c_{ij} is calculated as follows:

$$c_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)} \quad (1)$$

There are so many drawbacks normalizing in this way that is if the value of $\sum_j \max(s_{ij}, 0) = 0$ then the c_{ij} is undefined if $c_{ij} = c_{ik,}$ it shows that peer *j* has the same reputation as the peer *k* in the eyes of peer *i*. But it is not that both are reputed or malicious. So, the algorithm uses aggregation of local trust values in a distributed manner. The peer *i* will weight their opinions.

$$t_{ik} = \sum c_{ij} c_{jk} \quad (2)$$

There are three practical issues:

A priori notions of trust: At the start of the network first few peers are considered trustworthy because there is no database available. So, network starts positively because the early peers would not want to destroy the network to which they are the starter.

Inactive Users: If peer does not ever download any type of file from any other peer so it's not possible to assign reputation to such type of node.

Malicious Collectives: There are some malicious peer's groups who assign the high reputation to their group peers and assigns low reputation to the peers who are not in their group.

The pre-trusted clients should be less and they should be selected based on their reputation that can be based on their education and field of working.

In this paper, another algorithm is Distributed EigenTrust where peer can assign reputation to itself. Each peer can evaluate its own global trust value:

$$t_i^{(k+1)} = (1-a)\left(c_{1i} t_1^{(k)} + \cdots + c_{ni} t_n^{(k)}\right) + a p_i \quad (3)$$

3.3. P-Grid Peer to Peer Platform- Kerl Aberer and Zoran Despotovic [5], designed an information system that is *P* grid, is a decentralized global trust model and is based on binary trust i.e. an agent is either trustworthy or malicious. Each agent performs transaction *t (p,q)* correctly or not. If any agent cheats then it becomes untrustworthy in global perspective. If an agent *p* files a complaint against agent *q* then it is denoted as *c(p,q)*. But if an agent *q* files a complaint against agent p then p also files a fallacy complaint against *q* while *q* is only honest. In this way, malicious agent confuses the other agents to decide that who is honest. The problem with node *p* starts when it assigns complaint to all other agents. Thus, in this way we can evaluate that node *p* is cheater. Thus, we can find the reputation of an agent *p* as:

$$T(p) = |\{c(p,q) | q \in p\}| \{c(q,p) | q \in P\}|$$

High value of reputation indicates that the agent is malicious; the global reputation of any agent is calculated based on the complaints. Thus, on the perspective of data management the data is aggregated along the incorrect direction. To store the data in a peer to peer network in a scalable way P-Grid is used.

3.4. Novel Peer to Peer Trust Model –HaimeiXu, Yulin Liu, Shouqing Qi and Yanjun Shi [6], designed a Novel peer to peer trust model which is based on probability and statistics. The trust value of any peer is evaluated by using maximum likelihood estimation and hypothesis testing.Every peer wants to communicate with high reputed peer. According to history of transaction, any peer can be classified as in given Fig 1. Hypothesis testing uses Bernoulli distribution to find out malicious nodes. This model is free from the iterative methods complexity and enhances the success full download ratio effectively. But when the network becomes complex then how to calculate trust value and how to store that global trust value makes PStrust difficult.

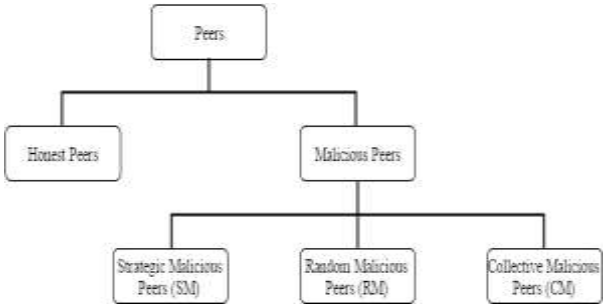

Figure. 1: Types of Peers

3.5. ThTrust: Shaojie Qiao, Xingshu Chen and Changie Tang [7], proposed a global trust model based on the transaction history. This model uses an easy method to evaluate global reputation value by observing their historic transaction, a new method, global transaction table is used to store the trust value for each peer. A peer takes services from the server based on their global reputation value and the server responds to a high reputation node and denies the clients who have lower reputation value. A peer can increase their own reputation value by providing good services and the reputation of peer will be decreased if they have unauthentic files. If we store the reputation value locally and every node store its own reputation value that it leads to cheating behaviors for malicious peers change their trust value. To remove this type of problem the concept of global reputation came in existence.

3.6. Group Trust: Abhilash Gummadi, Jong P. Yoon [8], designed a trust model which focuses on two important security issues:

Peer Selection: The model deals in prevention of selection of malicious peers based on the behavior. Success of transaction depends on the selection of trustworthy peer.

Request Resolution: When there is bombarding of request to a peer to reduce the reputation, this is called request resolution. There are two solutions for this problem:

- Ignore all the malicious requests. Mark the requests using some strategy.
- Adopt "Cookie Exchange System" for handling requests. A requesting peer stores a cookie issued by responding peer. When a transaction takes place, the responding cookie validates the cookie and then decide accordingly.

In group trust, group refers to a collection of peers which follow some protocols; the protocol decides the minimum condition of a group.

3.7. Voting Agreement: Yu Wang and Yuelong Zhao [9], proposed a trust model that is based on voting agreement, solves the problem of the peers which are new and have not taken part in the transaction. It can evaluate the actions taken by other side according to the transaction history and the other peers' recommendations. P2P model is currently classified in following categories:

- The centralized trust model: the system is centralized and has deficient performance in scalability and single point failure.
- The role-based trust model: the peers join the communities based on their interest. The communities are the group of peers with similar interest.
- Overall trust degree model: the overall trust degree is gained by the mutual satisfaction of the local nodes.
- The negative feedback based trust model: the malicious nodes in the system are very less so the system ignores the report *c(p,q)*.

3.7. Reputation Based Trust Model: Li Xiong and Ling Liu [10], designed a model a coherent adaptive trust model which compares the trustworthiness of peers on the behalf transaction-based-feedback system. This model takes care of following types of problems:

- If the feedback approach suffers from the fallacy past experienced records in a respective community. Problem in differentiating that the feedback is provided by less trustworthy peers or trustworthy peers. System lacks to set up context sensitive feedback filters. Lack of temporal adaptivity not able to decay old transactions.
- System does not motivate the peers to rate others.

The model takes following factors to solve the above issues:

- Feedback in terms of amount of satisfaction: In a P2P community, the feedbacks are given to both client and service provider after the completion of transaction.
- Number of transactions: The peer can increase their reputation by increasing the number of transaction so transaction is a crucial factor in evaluating reputation. The model maintains the correct ratio of reputation and transaction so that it can evaluate reputation value.
- Credibility of feedback: A peer may send false feedback because of jealousy. So, the number of transactions of a peer should be judged if the peer gets positive feedback from all other peers then give less weight age to negative feedback.
- Transaction Context Factor: Sometimes E-Commerce communities become honest for small transactions and become dishonest for larger transaction to earn more profit.
- Community Context factor: Some business community requires temporal adaptivity, it is desired to consider recent trend. Model gives low weight to past transaction than new transactions.

3.8. Global Trust Model: Karl Aberer and Zoran Despotovic [11], proposed a model that presents a way for reputation based trust management at both levels data management and semantic level. This method is based on peer-to-peer system and it scales well when the peers increase. Global trust model considers only binary trust, either a peer is trustworthy or not. Agent performs transactions if agent cheats then it becomes untrustworthy. If an agent files a *P* files a complaint against malicious behavior of *q*, file a complaint *c(p,q)*. It may also happen an agent can assign fallacy feedback because of jealousy or any other reason. In this case all the feedbacks of the node are checked if most of them are positive then ignore the negative feedback by assigning low weightage.

3.9. TsTIT Trust Model: In [12], Yu Jin, ZhimnGu and Zhijie Ban, proposed a two-level trust model for a large network. TsTIT model is a partially decentralized time sensitive reputation management system. TsTIT system is composed of series of trust clusters in which some nodes are selected as cluster headers based on CPU cycles, memory, online time and trust. There are two types of trust:

- *Intra-cluster Trust:* It is a bidirectional trust relationship which describes the reliability of the member mentioned by the cluster header.
- *Inter-cluster Trust:* It shows the service reliability of the cluster assigned by another cluster.

Therefore, the management of intra-cluster is centralized while inter-cluster trust is decentralized.

In TsTIT, if the time distance is of trust value evaluation and updating is beyond a period then the weight of this trust value is zero. The advantage of this design is that the nodes will contribute the system continuously and keep the system alive.

4. Conclusion

In this paper, we have surveyed reputation systems and a lot of parameters that are taken into consideration when the system is designed. As more as the people are depending on online services, the reputation became a major concern in facilitating their interactions. Service provider reputation plays a key role because the successful transaction depends on the selection of a service. There are also a lot of security concerns that takes place when a malicious service provider is selected. Various papers are written in this field, we have clubbed some papers to understand the various influencing parameters.

References

[1] N. Garg, M. S. Goraya, "A Survey on Energy-Aware Scheduling Techniques in Cloud Computing Environment" International Journal of Computer Science and Information Security (IJCSIS), 14(10), 2016.

[2] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, "Cloud computing – The business perspective", Decision Support Systems, 51, pp. 176-189, 2011.

[3] A. Josang and R. Ismail, "The Beta Reputation System," Proc. 15th Bled Conf. Electronic Commerce, 2002.

[4] S.D. Kamvar, Mario T. Schlosser, Hector Garcia-Molina, "The EigenTrust Algorithm for reputation management in P2P networks", in: Proceedings of the 12th International World Wide Web conference, ACM, New York, NY, USA, pp. 640-651, 2003.

[5] K. Aberer, P. Cudr´e-Mauroux, A. Datta, Z. Despotovic, M. Hauswirth, M. Punceva, and R. Schmidt: P-Grid: a Self-Organizing Structured P2P System. ACM SIGMOD Record, 32(3), 2003.

[6] H. Xu, Y. Liu, S. Qi, Y. Shi, "A Novel Trust Model Based on Probability and Statistics for Peer to Peer Networks", in: International Conference on Quality, Realibility, Risk, Maintenance, and Safety Engineering, pp. 2047-2050, 2013.

[7] Shaojie Qiao, Xingshu Chen, Changjie Tang, "ThTrust: Transaction History Based Peer-to-Peer Trust Model", in First International Symposium on Data Privacy and E-Commerce, IEEE Computer Society, pp.242-247, 2007.

[8] A. Gummadi, J. P. Yoon, "Modelling Group Trust for Peer-to-Peer Access Control", Proceedings of the 15th International Workshop on Database and Expert Systems Applications, IEEE Computer Society, 2004.

[9] Yu Wang and Yuelong Zhao, "Voting Agreement Based Trust Model for Peer to Peer E-commerce", in International Conference on Computer Science and Software Engineering, IEEE Computer Society, pp. 1213-1216, 2008.

[10] Li Xiong and Ling Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities", Proceedings of the IEEE International Conference on E-commerce, IEEE Computer Society, 2003.

[11] Karl Aberer and Zoran Despotovic, "Managing Trust in a Peer-2-Peer Information System", Proceedings of the tenth international conference on Information and knowledge management - CIKM'01, 2011.

[12] Yu Jin, ZhiminGu and Zhijie Ban, "TsTIT: A Time-sensitive Two- level Trust Model Based on Reputation for Large-scale Peer-to-Peer Networks", second International Conference on Communications and Networking in China, 2007.

Authors Profile

Author 1. Neeraj

Neeraj received the B.Tech. degree in computer science and engineering from Gautam Buddh Technical University Lucknow, India, and the master's degree in computer science and engineering from Sant Longowal Institute of Engineering and Technology, Longowal, India. He then worked as a Research Scholar in the Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, Sangrur, India, until May. 2016. His area of research interest includes Cloud Computing, distributed computing, decision making in distributed environment, and IoT.

Author 2. Dr. Major Singh Goraya

Major S. Goraya received the B.E. degree in computer science and engineering from Sant Longowal Institute of Engineering and Technology, Sangrur, India, in 1997 and the master's and PhD degrees in computer science and engineering from Punjabi University, Patiala, India, in 2003 and 2013, respectively. He is currently working as Associate Professor in the Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, Sangrur, India. His research interests include resource scheduling in grid computing, cloud computing, distributed computing, and green energy.

Author 3. Dr. Damanpreet Singh

Damanpreet Singh received the B.Tech. degree in computer science and engineering, M.Tech in computer science and engineering and Ph.D. in computer science and engineering He is currently working as Associate Professor in the Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, Sangrur, India. He is member of Institute of Electrical and Electronics Engineers (IEEE), Computer Society of India (CSI), and life member of Indian Society for Technical Education (ISTE). His research interests include Adhoc Networks, Wireless Sensor Networks, Digital Signal Processing, Optimization Techniques.