ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.4 , No.5, Pages : 04-06 (2015)
Special Issue of ICETEM 2015 - Held on October 27, 2015 in The Solitaire Hotel, Bangalore, India
http://www.warse.org/IJATCSE/static/pdf/Issue/icetem2015sp02.pdf

Effective Cloud Services using Mutual Trust Access Control Mechanism (MTACM)

Sarojini G[1], Vijayakumar A[2], Selvamani K[3], George Fernandez I[4]

[1]Final M.E.(SE) Student, Department of Information Technology, Jerusalem College of Engineering, Chennai 600100, India,
sarojinigs@gmail.com

[2]Professor, Department of Information Technology, Jerusalem College of Engineering, Chennai 600100, India,
kaniporiyalan@yahoo.co.in

[3]Assisstant Professor, Department of Computer Science and Engineering, Anna University, Chennai 6000025, India,
selvamani@annauniv.edu

[4]Assistant Professor, Department of Information Technology, Jerusalem College of Engineering, Chennai 600100, India,
georgefernandez@jerusalemengg.ac.in

Abstract: In the cloud environment, the trust management is a major component for providing virtualized and scalable web services from the service providers to the various cloud users. Many existing systems are not proficient in providing trusted cloud services. The trust can be defined as an act of faith, belief and certainty based on the application of different technological services. Also the trust in cloud services technology derives the reputation while services are provided to the various users from the cloud service providers (CSP). The trust provides the solutions for the specific problems due to disbelief, uncertainty and vulnerability in cloud services. This proposed system ensures a mutual trust for various users while they are accessing their services in a cloud environment. This type of assurance leads the reputation and secured services in cloud. In this proposed the Mutual Trust Access Control Mechanism is playing a major role to establish safe and secure cloud services. The behavioral based absorption is a specific measure which is effectively used to ensure the trust and reputation in cloud service via the second and third party behavioral recommendation service.

Key Words: Behavioral trust, Cloud Service, Mutual Trust Access Control, Reputation, Trust.

INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal service provider interaction. The cloud ensures the access over the internet without having any knowledge of the complexities of the web services and information services. The cloud services are classified into Public, Privet, Hybrid and Virtual Private Clouds. The public clouds represents services offered to general public. The Private cloud represents services of a single organization. The hybrid cloud denotes the combination of both public and private clouds to overcome individual limitations. The Virtual Private clouds are nothing but a platform running on top of public clouds. In the cloud technology the cloud services are very important in real time based on Infrastructure as a service (Iaas) (e.g. storages, servers, etc) Platform as a service (Paas) (e.g. operating system, middle-ware, etc) Software as a service (Saas) (e.g. application software, web services, etc). The various roles in cloud environment are Cloud Service Consumer, Cloud service provider, Cloud Developer, Cloud Administrator, Cloud Manager, etc. The Trust, Reputation and Security are fundamental requirements in cloud services.

In general sociological terms trust is given as “When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly, when we say that someone is untrustworthy, we imply that the probability is low enough for us to refrain from doing so”. Definition of trust in an organizational context by adding vulnerability associated with risks that one is willing to take as: “The willingness of a party to be vulnerable to the actions of another party based on the expectation that other will perform a particular action important to the person who trusts, irrespective of the ability to monitor or control that other party.” Trust in cloud plays a major role in providing services and can be considered as cloud security feature as well. Trust changes with time and new knowledge. Trust experience will have to be updated periodically. Trust in cloud is required because resources have to be provided efficiently since the resources are limited. Trusted cloud users can only access the cloud and simultaneously users are allowed to select the most credible cloud service providers. This helps in avoiding attacks from illegal and malicious users as well as service providers.

In general reputation is defined as "Reputation is public knowledge and represents the collective opinion of members of a community. Reputation is based on the aggregated trust opinion of a group of agents. Since trust is highly subjective, this aggregated result may not be of equal use to all agents." Reputation is the assessment of the society about performing a task or service. Cloud users require a reputed system to guarantee the safety of their data, investment and service. Reputation is gained through trust which might be through self experience or through existing users' recommendation. Reputation is based on metrics such as Behavioral, Subjective or objective, transaction-based or opinion-based, complete or localized information and rank or threshold based reputation. Reputation is the opinion of one entity towards another entity based on the above metrics. Trust and Reputation are mutual for both the cloud users and cloud service providers since their status are equal.

RELATED WORK

In 1994, Marsh[4] introduced the concept of trust for the first time, and then Baize introduced trust management into network related security applications.

Hassan[5] proposed a novel trust evaluation method suitable for the pervasive environment and it considered the dynamic nature of trust and incorporated uncertainty of trust modeling. So, it was well suited for the pervasive environment and could resist malicious behavior.

George[6] presented the trust relationship as a directed graph path problem. This kind of trust computing method accurately reflected the global trust conditions as well as had a good adaptability and malicious detection capability.

Wang Wej[7] proposed a trusted resource scheduling algorithm based on Bayesian Theory which is able to obtain an accurate assessment of trust with a much smaller time complexity. Besides, some other dynamic trust models based on fuzzy logic, machine learning, which can better meet the demands of dynamic network were also proposed. Although these dynamic trust models introduced lot of advantages, but there are problems due to the subjective characteristic of trust. Many trust models will not specify the specific implementation issues and the critical evaluation of performance of trust model.

Nowadays, integrating Trusted Computing into cloud environment and making it a reliable way to provide cloud service is an important topic in cloud security. Santos et al proposed a trusted cloud computing platform (TCCP) on which IaaS cloud service providers could offer a closed box-type execution environment to its users and ensure the confidentiality of guest virtual machine. In addition, it allows the user to check out whether the service provided by laaS providers is secure or not before even starting the virtual machine.

Shouxin Wagng [9] proposed a subjective trust evaluation approach. A cloud model has been introduced to overcome the limitations of fuzzy set theory with the help of an accurate and sole membership degree which has shown effectiveness.

Audun Josang [10] presented a survey of trust and reputation systems for online service provision with the basic idea of trust and reputation. It is to let parties provide rating to each other after completion of a transaction and use the combined ratings to get trust or reputation value. Several existing and proposed systems measuring trust and reputations have been discussed in this paper.

Sheikh Mahbub Habib [11] proposed a multi-faceted trust management (TM) system to identify reliable trustworthy cloud providers in a cloud computing environment. The system provides mechanisms to identify service providers in terms of attributes like performance, compliance, security etc. Their trust management system for cloud computing considers multiple attributes, sources and roots, trust customization, evaluation, representation and attack resistance.

Hyukho Kim [12] presented a trust model which efficiently reconfigures and allocates computing resources according to user requests. This model collects and analyzes the reliability of servers in a data center based on historical information which is used to prepare best resources for service requests in advance. This model increases the reliability of cloud system by providing highly trustable computing resources. They haven't taken mutual trust between users and cloud service nodes of cloud computing into account.

PROPOSED SYSTEM

In this proposed system the trust computation encompasses three methods. First method is user trust calculation and the second method is cloud service provider trust calculation and the third method is the mutual trust calculation for both the cloud user and the cloud service provider based on which the service provision takes place.

According to user's behavior features, we obtain behavior data, and divide them into different trust attribute categories. Trust attribute features consist of confidentiality, integrity and reputation. To obtain user's behavior data according to source of the data. One is collecting commonly used parameters in cloud interactions, such as resource utilization rate, service availability, application vulnerability and user's access frequency, time, environmental conditions and unauthorized operation. The other is obtaining operation success rate, error repair rate, self-protection capability and mean time to failures.

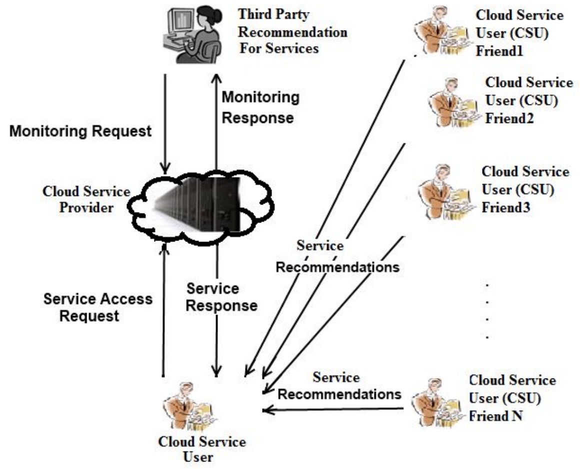
Third Party Recommendation For Services
Monitoring Request
Monitoring Response
Cloud Service Provider
Service Access Request
Service Response
Cloud Service User
Service Recommendations
Service Recommendations
Cloud Service User (CSU) Friend1
Cloud Service User (CSU) Friend2
Cloud Service User (CSU) Friend3
Cloud Service User (CSU) Friend N

Fig 1 System Architecture

The Fig 1 represents the schematic architecture of the proposed system which encompasses the cloud services based on cloud users request for the services from the service providers. The service provider acknowledges the recommendation value of the requesting user who may obtain the subsequent service. The cloud user obtains recommendation about the service provider from other cloud users who are friends with the cloud user who request for the service. The recommendations are the basis for the cloud manager to provide the service that was requested from the trusted and reputed service provider. The cloud manager monitors the service interaction between the cloud users and cloud service providers.

User Trust Calculation

The proposed trust model for cloud computing authentication cannot be used to determine whether the user’s trust. To ensure the credibility of the behavior of the user and to avoid risks of user's malicious behavior towards the cloud server, a trust model based on user's behavior is proposed. This model first quantifies user's behavior information and secondly introduces the correction factor and finally the feedback system into trust mechanism, which figure outs trust degree of the user.

In the first step of quantification of user behavioral trust is done by collecting various parameters which include resource utilization rate, service availability, application vulnerability, user’s access frequency, time, environmental conditions, unauthorized access, etc. Few other operational parameters such as operation success rate, error repair rate, self-protection capability of the user followed by the mean time to failure. The calculation also includes trust attribute categories like Confidentiality, Integrity and Reliability which are further categorized into control factor level and network level. An hierarchy is followed for the above attributes which is formed as a matrix and another weight matrix is formed whose transpose is taken and the product results in the final trust value of the user.

$$Tu = \{t1,t2,\ldots,tn\} \qquad (1)$$

$$Wu = \{w1,w2,\ldots,wn\} \qquad (2)$$

$$\text{Final User Trust Tuser} = Tu*WuT \qquad (3)$$

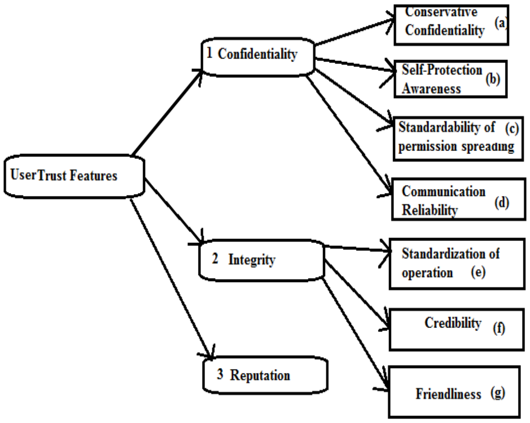
UserTrust Features
1 Confidentiality
2 Integrity
3 Reputation
Conservative Confidentiality (a
Self-Protection Awareness (b)
Standardability of (c) permission spreading
Communication Reliability (d)
Standardization of operation (e)
Credibility (f)
Friendliness (g)

Fig 2 Attributes of User’s Behavior

Fig 2 shows the various attributes using which the user’s trust value is calculated in the equation (1) and weights are assigned to each attribute based on its importance and the user who provides the recommendation which is given in the equation (2).

To compute the final trust, the cloud manager assigns appropriate weights to the attributes like if the user wants to provide more weight for direct communication history and self trust rather than recommendation from friends and third party who gets lesser weights and the product of both as given in equation (3) is the final value obtained.

Cloud Service Provider Trust Calculation

In general cloud users tend to select service providers who provide credible services. Trust value helps the user to choose the most credible service provider. The trust value ranges from 0 to 1 where 0 implies that the service provider is not trusted and any value near 1 implies that the service provider is a trusted node. This trust value calculation can be based on various factors. The earlier one to one communication between the user and the service provider and the distance between them leads to a direct trust value. Recommendation by a third party or by a user who has previously interacted with the service provider.

Time at which the response is provided from the service provider after the request of a particular user is received for service provision. Direct Trust Value is represented as DTCSP and recommendation based trust value is represented as RTCSP and weights are given to both the values which computes the final trust value represented as TCSP.

$$TCSP = \alpha * DTCSP + \beta * RTCSP \qquad (4)$$

Where α and β are the weights assigned to the respective trust values. The above equation (4) has the trust calculation for the cloud service provider which has the product of the direct trust and recommended trust with the appropriate weights.

Mutual Trusted Access Control Mechanism (MTACM)

The cloud users and the cloud service providers have an equal status in the cloud environment so their Trust value also has an equal status and they are to be mutual. Mutual trust can also be defined as the confidence that both the cloud user and service provider show towards each other during an uncertainty or malicious attack. Mutual trust is achieved by a common threshold trust value kept for both the cloud users and service provider. If and only if both these entities achieve the trust threshold value the service request and service provision can be made which is represented as Trust based Decision.

$$\begin{aligned} TD = {} & 1 \text{ if } TU \ \&\ TCSP \geq \text{Threshold} \\ & 0 \text{ if } TU \ \&\ TCSP \leq \text{Threshold} \qquad (5) \end{aligned}$$

The above equation (5) compares the trust value with the threshold value and the cloud manager decides to provide service based on the result.

CONCLUSIONS AND FUTURE ENHANCEMENTS

This proposed system is on trusted services in cloud computing environment and proposes a mutual trust access control mechanism. Unlike the traditional mechanism, the proposed mechanism takes both the user's behavior trust and the cloud service node's trust into consideration which adapts to the characteristics of uncertainty, dynamism and distribution in cloud environment. User's behavior is based on various attributes in user's trust calculation and each type of attribute has certain weight. Similarly trust calculation of the cloud service node is based on certain other attributes. Finally, the mutual trust between users and the cloud service nodes are used in efficient service provisioning.

As a future development of this proposed work reputation can be included along with trust based service provisioning. The reputation can be made for the service providers based on which it will be much easier for the cloud users to select the best service provider available.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing (draft),” NIST special publication, vol. 800, no. 145, pp. 7-11, 2011.

[2] Sumin Jiao, Zhixiao Yang, Bin Zhang, “A Reputation Computation Model for Trusted Networks Considering Uncertainties based on Cloud Theory “Computer Research and Development (ICCRD), 3rd International Conference on (Volume:1).,pp. 473–476, 2011.

[3] Feng Li & Jie Wu, ‘Uncertainty modeling and reduction in MANETs’, IEEE Transactions on Mobile Computing, vol 9, no. 7, pp.1035-1048, 2010.

[4] Marsh S P. Formalising "Trust as a Computational Concept". Ph. D dissertation. University of Stirling, Scotland 1994.

[5] Jameel H, Hung L X, Kalim U, "A Trust Model for Ubiquitous Systems Based on Vectors of Trust Values". In Proc. of the 7th IEEE International Symposium On Multimedia. Washington: IEEE Computer Society Press., pp. 674-679, 2005.

[6] Sun Y, Yu W, Han Z, Liu KJR. "Information Theoretic Framework of Trust Modeling and Evaluation for ad-hoc Networks". IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, vol 249,no 2: pp.305-319, 2006.

[7] Wei Wang, Guosun Zeng. "Trusted Dynamic Level Scheduling Based on Bayes Trust Model". Science in China Series F-Information Sciences, vol 50 no3 pp.456-469,2007.

[8] Chen Jincui, Jiang Liqun. "Role-Based Access Control Model of Cloud Computing". Energy Procedia, vol 13: pp.1056 -1061, 2011.

[9] S. Wang, L. Zhang, N. Ma, and S. Wang, “An evaluation approach of subjective trust based on cloud model,” in Computer Science and Software Engineering, 2008 International Conference on, vol. 3, pp. 1062–1068, 2008.

[10] A. Jøsang, R. Ismail, and C. Boyd, “A survey of trust and reputation systems for online service provision,” Decision support systems, vol. 43, no. 2, pp. 618–644, 2007.

[11] S. M. Habib, S. Ries, and M. Muhlhauser, “Towards a trust management system for cloud computing,” in Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 10th International Conference on, pp. 933–939, 2011.

[12] H. Kim, H. Lee, W. Kim, and Y. Kim, “A trust evaluation model for QoS guarantee in cloud systems,” International Journal of Grid and Distributed Computing, vol. 3, no. 1, pp. 1-8, 2010.

[13] Rizwana A. R. Shaikh, M. Sasikumar, 2012 “Trust Model for a Cloud Computing Applications and Services,” Computational Intelligence &

Computing Research (ICCIC), IEEE International Conference on, pp. 1-4, Dec. 2012.

[14] M. Kuehnhausen, V. S. Frost, and G. J. Minden , "Framework for assessing the trustworthiness of cloud resources," in Proc. IEEE Int. Multi-Discipl. Conf. Cognit. Methods Situation Awareness Decision Support, pp. 142–145, Mar. 2012,.

[15] A. Das and M. M. Islam, "SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems," IEEE Trans. Depend. Secure Computing, vol. 9, no. 2, pp. 261–274,Mar./Apr. 2012 .

[16] Xiaoyong Li, Junping Du , "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing"International Institution of Engineering and Technology on (Volume:1).,pp. 39–50, 2012.

[17] Lin Guoyuan, Wang Danru, BieYuyu, Lei Min , "MTBAC: A Mutual Trust Based Access Control in Cloud Computing," China Communications, pp. 154–162, 2014.

[18] Guoyuan Lin, Yuyu Bie, Min Le, "ACO-BT M: A Behavior Trust Model in Cloud Computing Environment," International Journal of Computational Intelligence Systems, pp. 1-11, 2013.

[19] Guoyuan Lin, Yuyu Bie, Min Lei. "Trust Based Access Control Policy in Multi-Domain of Cloud Computing". Journal of Computers., vol 8 no 5 1357-1365, 2013.

G. Sarojini is a Final year student of M.E. Degree in Software Engineering from Jerusalem College of Engineering, Chennai 100, India. She received B.Tech Degree in Information Technology from Panimalar Engineering College, Chennai, India and has industrial experience of around five years in testing domain. Her area of interest includes Cloud Computing and Software Testing.

A. Vijayakumar is working as Professor in Department of Information Technology, Jerusalem College of Engineering, Chennai 100 , India. He received Ph.D in the area of mobile ad hoc networks, M.E. Degree in Computer Science and Engineering from Annamalai University, Tamilnadu, India and B.E. Degree in Computer Engineering from Madurai Kamaraj University Madurai, Tamil Nadu, India. His research interest includes mobile ad hoc networks, network security and Cloud Computing.

K. Selvamani is working as Assistant Professor in the Department of Computer Science and Engineering, College of Engineering, Guindy, Anna University, Chennai-25. He received his P.h.D Degree under the Faculty of Information and Communication Engineering from Anna University, Chennai.25. M.E. Degree in Computer Science and Engineering from Bharathiyar University Coimbatore, India(2000) and B.E. Degree in Electrical and Electronics Engineering from Annamalai University, Tamilnadu, India. He has more than 15 years of experience in Teaching. He published more than 20 International Journals and presented the papers in 20 International coferences His research interest includes Web Applications, Computer Networks and Artificial Intelligence.

I. George Fernandez is working as Assistant Professor in Department of Information Technology, Jerusalem College of Engineering, Chennai 100 , India. He received M.Tech in Information Technology from SNS College of Technology, Coimbatore, India and B.E in Computer Science Shirdi Sai Engineering College, Bangalore. His area of interest includes Cloud Computing and Networks.