Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 506 – 512

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud

Sarojini G[a*],Vijayakumar.A[a], Selvamani.K[b]

[a,]Final ME Student, Department of Information Technology,Jerusalem College of Engineering,Chennai, 600100, India

[b]Assistant Professor, Department of Computer Science and Engineering,Anna University,Chennai 600025, India

Abstract

In cloud computing, trust management is more important when providing users with virtualized and scalable web services. Many existing systems sharply divide trust value into right or wrong. Trust means an act of faith; confidence and reliability in something that is expected to behave or deliver as promised. Trust is required to solve the problem created due to uncertainty and vulnerability caused by open conditions of cloud computing. This paper presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing. This is to be done by providing trusted services to the cloud users using enhanced mutual trust to be known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This paper proposes the model which considers both the cloud user's behavior trust and cloud service provider's credibility. Trust calculations are based on the behavior which includes history of direct communication between both the user and service provider; based on friends and third party recommendations. The hierarchy based reputation systems has suggested how to safeguard the data objects in the level of file access which ensures the cloud security. The different security measures are used to protect the different cloud services. This proposed system which includes the EMTACA algorithm can assure enhanced, guaranteed and trusted and reputation based cloud services among the users in a cloud environment.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: *Cloud Computing; Behavioral Trust; Mutual Trusted Access Control; Reputation System; Cloud Security; EMTACA.*

*Sarojini G., *VijayakumarA Tel.: +917299977815..

*E-mail address:*sarojinigs@gmail.com, kaniporiyalan@yahoo.co.in.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

doi:10.1016/j.procs.2016.07.375

1. Introduction

2. 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 main idea behind the cloud is that you can access all your information over the internet without having any detailed knowledge of the infrastructure used to enable it. The different cloud types are Public clouds; Private clouds; Hybrid clouds; Virtual Private clouds. Trust in cloud plays a major role in providing services and can be considered as cloud security feature as well. Trust in general is a belief that someone or something is reliable, good, honest and effective. 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. Reputation is another factor which has a major effect while providing cloud services. Reputation in general 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. Trust and Reputation are mutual for both the cloud users and cloud service providers since their status are equal.

3. Literature Survey

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] defined trust relationship as a directed graph path problem. This trust computing method accurately reflected the global trust conditions as well 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 above has many advantages, but there are problems due to the subjective characteristic of trust. Many trust models did not specify the specific implementation issues and the evaluation of performance of trust model is hard. 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. Examples would be in building initial trust bootstrapping coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in cloud environment is also much more challenging than in traditional centralized environments. The trust in the mobile adhoc network is given as a proposed work in the papers. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of cloud services and result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time. Despite a couple of surveys of trust management, a comprehensive survey of trust management in cloud does not exist and is the main aim of this paper. 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.

3. Proposed System

The Fig 1 is the architecture of the proposed system where a particular cloud user request for a service from a service provider. The service provider gets the recommendation value about the requesting user from the third party whose specific service is to provide recommendation. The cloud users also get recommendation about the service provider from other cloud users who are friends with the cloud user who request for the service. Based on the recommendations the cloud manager provides 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.

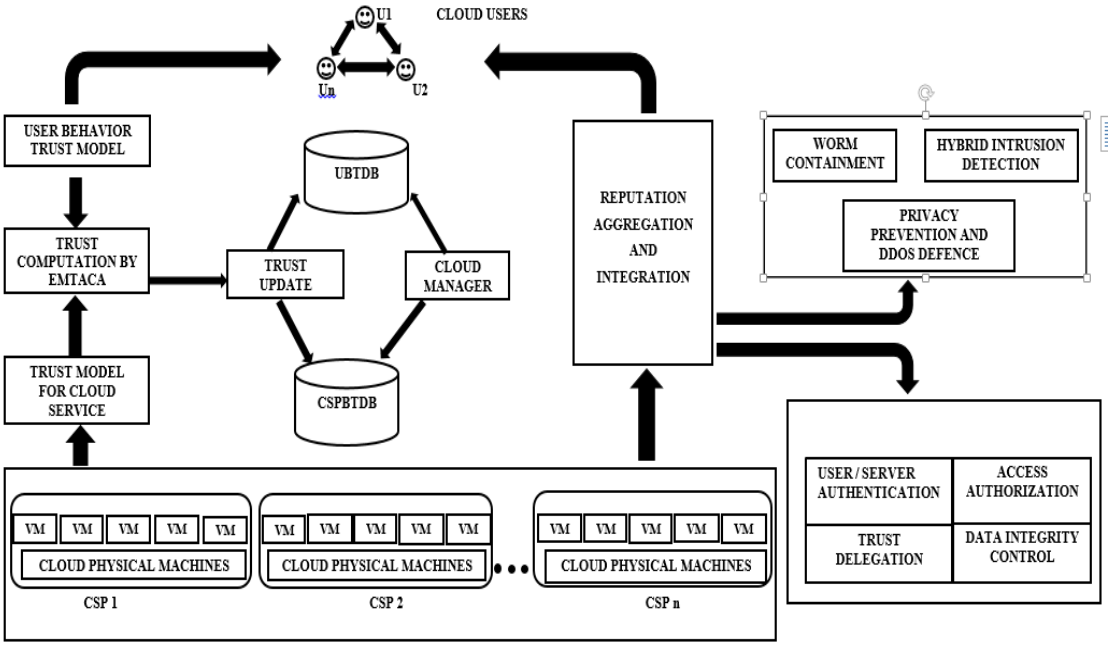

Figure 1: Architecture of Trust and Reputation System

3.1 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.

3.2 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.

3.3 Enhanced Mutual Trusted Access Control Algorithm (EMTACA)

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.

Enhanced Mutual Trusted Access Control Algorithm

(1) If the user satisfies the check by cloud manager
(2) If the user's behavior trust level $T_{user} \geq$ Trust threshold TT_{user} in User behavior trust database(UBTDB) then
(3) Proceed to step (6)
(4) else
(5) Refuse to provide service to the user
(6) Read the user request
(7) If Cloud Service Provider Trust level $T_c(t) \geq$ Trust Threshold TT_{cloud} in Cloud Service Provider behavior trust database (CSPBTDB) then
(8) Add Cloud Service Provider in candidate provider queue
(9) Display the candidate provider queue to the user
(10) Cloud user selects the best cloud service provider
(11) Cloud Manager provides service access rights to the user
(12) User's Trust degree is updated in UBTDB and CSPBTDB

3.4 Reputation Aggregation and Integration

Cloud security enforcement has many aspects. Reputation is "overall quality or character as seen or judged in general as". The Reputation slab is responsible for maintaining the reputation of a node. This duty encompasses many tasks. This block manages reputation representation, updates reputation based upon the new observations made by the "Watchdog", integrates the reputation information based on other available information, ages the reputation, and creates an output metric of trust. Reputation systems are widely used in diverse domains. E-commerce systems, such as *eBay, Yahoo* auctions and Internet-based systems such as Keynote, maintain reputation metrics at a centralized trusted person. Additionally, they use a well defined number for representing reputation. As a result, these systems use several arguable heuristics for the major steps of reputation updates and integration. In fact, much closer to our context are standing systems such as those planned for ad-hoc

networks, CONFIDANT and CORE, and PEER-to-PEER networks.

These systems are dispersed and also maintain a numerical representation of the reputation by borrowing tools from the realms of game theory. Malware-based attacks like worms, viruses and DoS exploit the system vulnerabilities and compromise the system functionalities or provide the intruders an unauthorized access to critical information. Thus, security defense is needed in cloud systems to protect all cluster servers and datacenters as protection of servers form malicious software attacks like worms viruses and malwares, protection of hypervisors or VM monitors from software based attacks and vulnerabilities, protection of VMs and monitors from service disruption and denial of service attacks. Virtualization can enhance cloud security. But virtual machines (VMs) add an additional layer of software which could become a single-point of failure. Virtualization techniques are elaborated below for security enhancement in open clouds.With virtualization, a single physical machine can be divided or partitioned into multiple VMs (E.g. Server Consolidation). This provides each VM with better security isolation and each partition is protected from the possibility of Denial of Service (DoS) attacks from other partitions and also the security attacks in one VM are isolated and contained from affecting the other VMs.With virtualization, the VM is decoupled from the physical hardware. The entire VM can be represented as a software component and can be regarded as a binary or digital data. This implies that the VM can be saved, cloned, encrypted, moved, or restored with ease. VMs enable a higher availability and faster disaster recovery.DIDS design demands trust negation among PKI domains. Security policy conflicts must be resolved at design time and updated periodically.

Defense scheme is needed to protect user data from server attacks. The user private data must not be leaked to other users without permission. Google platform essentially applies in-house software to protect resources. The Amazon EC2 applies HMEC and X.509 certificates in securing resources. Reputation is public knowledge and represents the collective opinion of members of a group and it is based on the cumulative trust opinion of a group of agents. Since trust is highly skewed, this cumulated result may not be of equal use to all agents. Reputation is derived using the beliefs such as competence in which reputation as a subject is able to produce the expected result and play a positive role in the agent's plan; dependence belief: the agent's belief that it is necessary to rely on the subject to achieve its goal(s); disposition belief: the belief that a subject is not only capable of performing a given task but is also currently available to perform that task; motivation belief: the belief that a subject is motivated to cooperate with the agent and that this inspiration is expected to prevail in the face of conflicting motives; persistence belief: the belief that a subject will trail through on its obligation; self-confidence belief: the belief that the subject is confident to do the given task; enthusiasm belief: the belief that the subject is willing to perform the given task.

4. Results and Discussions

The figure 2 depicts is the performance evaluation graph of the simulation result. This includes the existing system which is Mutual Trust Based Access Control with the Enhanced Mutual Trusted Access Control Algorithm.

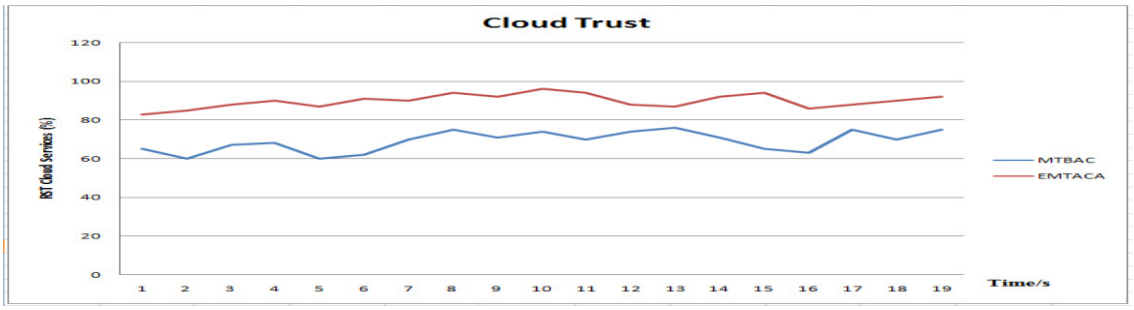

Figure 2 Performance Evaluation Graph

5. 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. Finally, the mutual trust along with reputation between users and the cloud service nodes are used in efficient service provisioning. As a future development of this proposed work authentication and authorization can be included along with trust and reputed service provisioning. The uncertainty can be reduced by introducing reputation as a model which is planned to be included as a future enhancement.

References

[1] 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.

G. Sarojini is doing Final year student of M.E. Degree in Software Engineering in Department of Information Technology from Jerusalem College of Engineering, Chennai 100, India. She received B.Tech Degree in Information Technology from Panimalar Engineering College, Chennai, India (2007) and she has more than five years on working experience in software industries. Her area of interest includes Cloud Computing and Software Testing.

A. Vijayakumar is working as Professor and Head in Department of Information Technology, Jerusalem College of Engineering, Chennai 100 , India. He received Ph.D in Information and Communication Technology from College of Engineering Guindy, Anna University Chennai (2015). He has completed his Masters in Engineering (M.E.) specialized in Computer Science and Engineering from Faculty of Engineering and Technology, Annamalai University, Tamilnadu, India(2004). Has under graduation (B.E.) in Computer Engineering from Arulmigu Kalasalingam College of Engineering, Srivilliputur, Madurai Kamaraj University

Madurai, Tamil Nadu, India (1992). He has more than 22 years of work experience in Academic and Software industries. He has published over 10 International Journals and presented his work in 20 International Conferences. His research interest includes Wireless Ad hoc Networks, Network security, Data Warehousing and Mining, Cloud Computing, Cloud Security and Big Data.

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 (2012). 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 17 years of experience in Teaching. He published more than 30 International Journals and presented the papers in 45 International conferences His research interest includes Web Applications, Computer Networks, Artificial Intelligence and Cloud Computing.