Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 3, March -2015

A Secured Cloud Computing Mechanism for Enhancing Mutual Trust Access Control

Bhatt Akshaykumar[1], Mohammed Hussain Bohra[2]

[1]*M.E Student, Department Of Information Technology PIET, Limda, India*
[2]*Assistant Professor, Department of Computer Science and Engineering*

Abstract - *The development of the Cloud system, large number of vendors can visit their users in the same platform directing their focus on the software rather than the underlying framework. This necessity requires the distribution, storage and analysis of the data on cloud for accessing virtualized and scalable web services. With broad applications of cloud, the data security and access control becomes a major concern. The access to the cloud requires authorization as well as data accessibility permissions. The verification and updation of data must be done with proper knowledge which requires identification of the correct updates and blacklisted users who are intruder to cloud introducing the false data to the system.*

In this thesis work, It address the issue of the security and control mechanism in the cloud, It propose an approach which encompasses the Ant Colony Optimization for solving the specified issues having the k-means clustering for authenticating the system with the updates done by the various authorized users in the cloud. This approach builds a mutual trust relationship between users and cloud for accessing control method in cloud computing environment focusing on the system integrity and its security.

Keywords – *Access control, trust model, mutual trust mechanism, integrity*

I. INTRODUCTION

Access control mechanism has become important issue in cloud computing to ensure the security of the data and users updates on the cloud. The users can make use of the various cloud resources with the acceptance of the certificate from the authorization center for accessing the cloud[6]. The traditional methods for access control were not able to solve the problems such as uncertainty and vulnerability to the attacks from the unauthorized or malicious users. Cloud computing is a distributed environment therefore dynamism and anonymity of the information are some basic features of cloud[4]. Hence, security in such cases becomes important for the data across the various sites and user on various cloud. Some of the major challenges in cloud computing[2] are:

1) Security – The pool computing resources in cloud computing encounters security problems for accessibility and availability of data for different users. Cloud provides reliable infrastructure services for such a major challenge.
2) Cost Reduction – Cloud computing significantly reduces the infrastructure cost and the data communication cost. The cost of transferring the data to different cloud users is reduced by making the number of shares more for each user.
3) Level of Service – The computing resources for a cloud user need to ensure the quality, availability and reliability of these resources to entrusted cloud. The level of service provided is defined by the level of provided is defined by the level of granularity for the users' expectation and cloud offerings.
4) Cloud Operation – As the number of resources, users and the interaction sessions increases, the traffic on a cloud also increases which prohibits he development of the cloud and prevents the users to choose optimal resources for their betterment.

The data security has become an important issue in cloud computing.The cloud users share the same information over different nodes that need to be updated time-to-time.Another security issue is to protect the data at different node during storage[6].The out sourcing of the data has gained a wider attention accompanying the problems with the availability and integrity of the data. One of the advantages of storing the data in cloud is unlimited access to the data irrespective of time and place can be done.However, the data corruption may occur at any level of storage. The data might get damaged while migrating from one platform to another[7].

The data storage security is broadly classified into two groups[3]:

1) To make use of Trusted Third Party (TTP) – it is a reliable independent component trusted by both the cloud users and server. It saves time and reduces communication as well as computation overhead providing confidentiality and integrity for the cloud users.
2) To make use of Without Trusted Third Party (WTTP) – the cloud users use an extra tool that checks the data integrity in order to achievedata storage correctness with the application of WTTP.

II. CLOUD COMPUTING

Cloud computing was mainly developed to enable computation within geographically distributed and different type of resources. There is not any specific definition of cloud but it can be defined as a collection of distributed computers which are able to provide on demand computational resources and services with the help oninternet[1]. As described earlier it provides services like IAAS, PAAS and SAAS to the geographically widespread customers. Well known example is Amazon Elastic Compute cloud which provides virtual computing environment, different configuration of CPU, processor and memory[11].

III. DIFFERENT TRUST MODEL

A. User's behavior trust model

In order to ensure the credibility of user's behavior and avoid risks caused by user's malicious behavior to cloud server, atrust model based on user's behavior is established. It quantifies user behavior information firstly and then introduces the correction factor into trust mechanism, and finally shows the user's trust degree. There are different parameters for obtain user behavior information like resource utilization rate, service availability, user's access frequency, time, environmental conditions and unauthorized operation.User's behavior trust is the comprehensive evaluation and prediction from cloud server according to user's history information[6].

B. Trust model of cloud service node

The behavior trust mechanism of cloud service node is based on ant colony algorithm. In cloud environment trust degree between interacted entities is similar to the pheromone in ant colony algorithm.Cloud users tend to choose entities with highcredibility toprovide resources or services and the ant always select path with high level of pheromone concentration[6]. Ant Colony Optimization (ACO) is a population intelligent problem solving method, and it is easy to combine with other methods. Therefore, it is feasible toapply ACO to the field of trust management incloud computing environment[9].

C. Mutual trust between users and cloud service nodes

The process of interaction, that the status between user and cloud server is equal, so their trust is mutual. Due to the existence of uncertainty and vulnerability in cloud computing and cloud interactions, mutual trust is necessary. Mutual trust is the confidence that both users and cloud service nodes have shown to each other in future interaction[6].

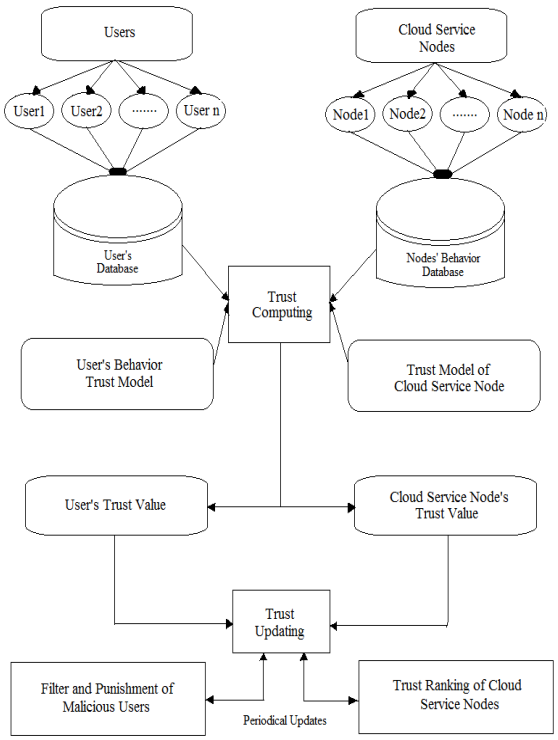

Figure1. Mutual trust structure[6]

Mutual trust mechanism:

The mutual trust mechanism between users and cloud service nodes is based on the following basic ideas as shown in Figure 1[6].

(1) Bidirectional trust structure.Trustrelationship is bidirectional and mutually equal.User selects the cloud service node with ahigher trust degree, and the cloud server willselect trusted users for the sake of preventing malicious user's attacks of the Cloud.

(2) Collection and processing of behaviortrust information. Two types of behavior trust information are distinguished, user's behavior and cloud service node's behavior information.

(3) Computing and updating of trust values.

IV. RESULT ANALYSIS &COMPARISON

The above approach is very helpful in recent cloud environment, but it still needs some modification. In this proposed approach, it improves the accuracy of existing system. It means it did not identify malicious user more clearly. In this approach it considers the minimum centroid value of clusters and compares it with both tables user review table and system review table of database.

Based on this comparison of two database table it decides the malicious activity of user in the cloud.

Scenario	Trust and Risk	Multi-Domain	TOrBAC	TCCP	MTBAC
Confidentiality	Very Good	Increase	Increase	Good	Increase
Integrity	Increase	Increase	Very Good	Increase	Very Good
Trust	Increase	Increase	Very Good	Increase	Very Good
Risk	Yes	No	No	Yes	No

Table1. Comparison

V. CONCLUSION

Access control technology cannot only ensure normal access requirements of valid users, prevent invasions of unauthorized users, but it can also solve security problemscaused by valid user'smis-operation. The proposed approaches for preventing and identifying the malicious user from accessing the information of users in the cloud environment and also track the behavior of each user on cloud server.

The propose approach is started with identifying the activities of each user. Each updates done by the users are considered and by analysis, the contents are identified as relevant or irrelevant. The level of irrelevance of the content provided by the user is use for updating the malicious user.

VI. REFERENCES

[1] Cloud computing bible, 2011. By Barrie sosinsky, publisher – Wiley
[2] Introduction to Cloud Computing, https://www.dialogic.com/~/media/products/docs/whitepapers/12023-cloudcomputing-wp.pdf
[3] NurmamatHelil, Mucheol Kimand Sangyong Han, "Trust and Risk based Access Control and Access Control Constraints", KSII Transaction on Internet and Information Systems VOL. 5, NO. 11, November 2011.
[4] NunoSontos, Krishna P. Gummadi, Rodrigo Rodrigues, "Towards Trusted ColudCompting", Proceedings of the 2009 conference on Hot topics in Cloud Computing,2009.
[5] Mustapha Ben Saidi, AbderrahimMarzouk, "Access Control Protocol for Cloud Systems Based On the Model TorBAC", International Journal of soft Computing and Engineering (IJSCE)", ISSN: 2231-2307, Volume-2, Issue-5, November-2012.
[6] Guoyuan Lin, YuyuBie, Danru Wang and Min Lei, "MTBAC: A Mutual Trust Based Access Control Model in Cloud Computig", IEEE Journals and Magazines, Volume-11, Issue-4, April-2014.
[7] Guoyuan Lin, YuyuBie and Min Lei, "Trust Based Access Control Policy in Multi-domain of Cloud Computing", Journal of Computers, Vol.8, No. 5, pp.1357-1366, 2013.
[8] Abdul Raouf Khan, "Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Science, Volume-7, No.-5, 2012.
[9] Guntsch, Michael, and Martin Middendorf. "A population based approach for ACO" Applications of Evolutionary Computing, 72-81 Springer Berlin Heidelberg, 2002.
[10] Trusted Computing Group, https://www.trustedcomputinggroup.org
[11] Amazon Elastic Compute Cloud (AmazonEC2) http://aws.amazon.com/ec2/

