A Secured Cloud Computing Mechanism for Enhancing Mutual Trust Access Control

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

[1]M.E Student, Department Of Information Technology PIET, Limda, India

[2]Assistant Professor, Department of Computer Science and Engineering PIET, Limda, India

[1]bhattakshay007@gmail.com, [2]mohammed.jeeranwala@gmail.com

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*

1. 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 are:

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 achieve data storage correctness with the application of WTTP.

2. 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 on internet[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[12].

3. RELATED WORK

3.1 MUTUAL TRUST BASED ACCESS CONTROL

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[5].

The mutual trust mechanism between users and cloud service node is based on the following basic ideas as shown in the figure 1.

(1) Bidirectional trust structure. Trust relationship is bidirectional and mutually equal. User selects a cloud service node with a higher trust degree and the cloud server will select trusted users for sake of preventing malicious user's attack on the cloud.
(2) Collection and processing of behavior trust 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.

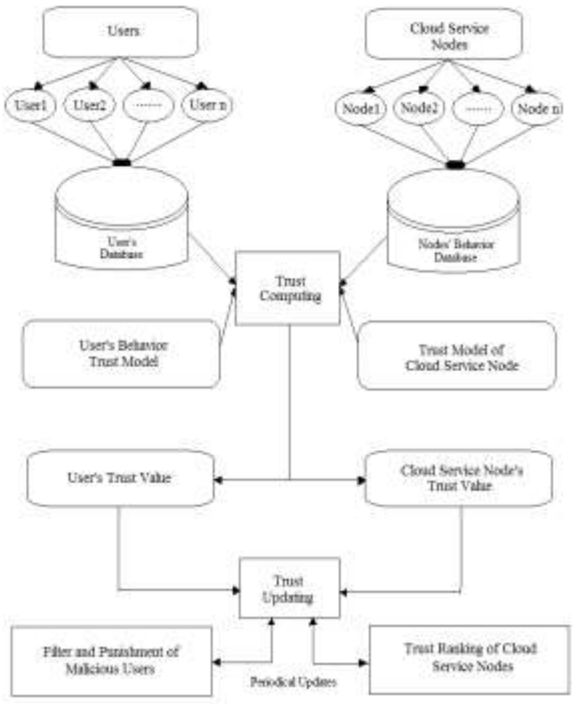

Figure 1: Structure of MTBAC[5]

3.2 TRUST BASED ACCESS CONTROL POLICY IN MULTI-DOMAIN

Guoyuan Lin proposed a most effective way of protecting cloud computing services, resources and users is access control. It intends to provide a trust based access control mechanism for cloud computing considering its multi-domain aspects. It also analyze the difference between inter-domain and intra-domain trust. A role based access control framework combined with trust degree in multi-domain is introduced. Access control in local domain directly applies RBAC model combined with trust degree, whereas in multi-domain it contains the conception of role-translation. The proposed approach improves the reliability and validity of system[6].

3.3 TRUST AND RISK BASED ACCESS CONTROL

It proposed the access control in dynamic environments needs the ability to provide more access opportunities of information to users, while also providing protection to information from malicious users. Trust and Risk are essential factors and can be combined together in access control decision-making to meet the above requirement. It propose the combination of trust and risk in access control to balance information accessibility and protection. The decision is made on the basis of trust of users and risk value of permissions. A potential relations between user and relations between permission in access control. The main approach is not providing all more access opportunities to trustworthy users in accessing permissions in access control[2].

3.4 CLOUD COMPUTING WITHOUT TRUSTED THIRD PARTY

R. Ranchal et al made an approach for identity management of the cloud without using trusted third party. The model makes use of active bundle which acts as a middleware between user and cloud services. This middleware agent includes data, privacy policies and protection schemes. The system being independent of trusted third party users reduces the risk of correlation attacks and channel attacks. A predicate over encrypted data is done. The integrity of the system is maintained to check if the data is tampered. If the integrity is found to be lost the data is destroyed itself[7].

3.5 TOWARDS TRUSTED CLOUD COMPUTING

It propose the solution for client of cloud computing services currently have a no means of verifying the confidentiality and integrity of their data and computation. It propose the design of trusted cloud computing platform (TCCP). TCCP enables infrastructure as a service (IaaS) providers such as Amazon EC2 to provide a closed box execution environment that guarantees confidential execution of guest virtual machines. It allows users to attest to the IaaS provider and determine whether or not the service is secure before they launch their virtual machines[3].

4. PROPOSED WORK

The proposed algorithm terminates yielding the centroid points. These points are obtained from the contents of the user review and system review tables. As the decision of the contents that are being edited by the various users are relevant or not is done after the cluster centroid values are obtained. Therefore three different cases arise here:

Case1:

If the content is unedited, both the centroid points from the user and system tables will have the similar values. In such case the updated content remains the same in system review table.

Case 2:

If the content updated in the user review table is a negative edit such as the relevant contents already existing are deleted by the anonymous user the User ID and details are tracked and are blocklisted. The blocklisted user can never again login with same user details or access the cloud resources. In such case no update is made to the system review table.

Case 3:

When the updates made by the user is relevant. The degree of relevance is also decided on the basis of the centroid values obtained for each table. The relevant data will always have a lower centroid value as compared to the existing system review content. Therefore the decision becomes easier with the optimized clustering approach for the update on the content with the degree of relevance of the update made by the user and the content in the system review table.

5. RESULT ANALYSIS AND COMPARISON

In this proposed approach, it improves the accuracy of existing system. The existing approach do not identify malicious user more clearly. It considers the minimum centroid value of clusters and compares it with both tables user review table and system review table of database using population based ant colony optimization. Based on this comparison of two database table it decides the malicious activity of user in the cloud. Once the user is detect as malicious, the same person can't get access again or resource in the cloud.

6. CONCLUSION

Access control technology can not only ensure normal access requirements of valid users, prevent invasions of unauthorized users, but it can also solve security problems caused by valid user's mis-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.

7. REFERENCES

[1] Cloud computing bible, 2011. By Barrie sosinsky, publisher – Wiley.

[2] Nurmamat Helil, Mucheol Kim and 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.

[3] Nuno Sontos, Krishna P. Gummadi, Rodrigo Rodrigues, "Towards Trusted Colud Compting", Proceedings of the 2009 conference on Hot topics in Cloud Computing,2009.

[4] Mustapha Ben Saidi, Abderrahim Marzouk, "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.

[5] Guoyuan Lin, Yuyu Bie, 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.

[6] Guoyuan Lin, Yuyu Bie 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.

[7] Ranchal, R. Bhargava, B., Othmane, L. B., Lilien, L., Kim, A., Kang, M., & Linderman, M. "Protection of identity information in cloud computing without trusted third party." Reliable Distributed Systems, 2010 29th IEEE Symposium on. IEEE, 2010.

[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] Tsang, P. P., Kapadia, A., Cornelius, C., & Smith. “Blocking misbehaving users in anonymizing networks. Dependable and Secure Computing, IEEE Transactions on, 8(2), 256-269, 2011.

[11] Trusted Computing Group, https://www.trustedcomputinggroup.org

[12] Amazon Elastic Compute Cloud (AmazonEC2) http://aws.amazon.com/ec2/