ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Secure Access Control Requirement Analysis in Cloud Computing

Faisal Mushtaq[1]
Department of Computer Science and Engineering
B.S.Abdur Rahman University
Vandular Chennai-48-India

S. Aranganathan[2]
Department of Computer Science and Engineering
B.S.Abdur Rahman University
Vandular Chennai-48-India

Abstract: ***Cloud Computing is one of the essential and most dominate technology in now a days. It provides various services to be used for the user, for that access control is one of the service/technology among them. The main goal of access control system is restricting any user to exactly what he/she should be able to do and secure data/information from any unauthorized access. Cloud service providers monitor easily who assess them from different access request to a same side of cloud user and giving him/her ability to need a strong access control model, for controlling admission to their different resources with the ability to use different multiple services with related to authentication, authorization and login time sharing of resources. It also has unique security challenge which includes multitenant hosting of security policy, algo's and domains. This paper also presents a detailed way of access control Requirement analysis for cloud computing and look after important privacy issues, which are not fulfilled by existing models. This work proposes an access control system to meet all cloud access control requirements. The system can not only ensure the secure untrusted users, but has the ability to support different access permissions which is on the same cloud user and given him/her the permission to use multiple number of services securely.***

Keywords: Cloud computing, access control, Security in Cloud, Permission and Authentication.

I. INTRODUCTION

Cloud computing is computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to the computer services and resources. Cloud computing relies on restricting sharing of resources to achieve coherence and economy of scale. Privacy is increasingly important in the online world. It generally accepted that due consideration of privacy issue promotes user confidence and economic development. However, the secure releases, management and control of personal information into the cloud represent a huge challenge for all IT companies, involving pressures both legal and commercial. For this Security is one of the primary concerns and a major barrier to adopt cloud computing. Cloud computing may suffer from conventional distributed systems' security attacks such as malicious Viruses, Trojan Horses and Man-in the Middle attack, Distributed Denial-Of-Service (DOS) attack , insecure application programming interface, abuse and nefarious use of cloud computing and malicious insiders. Cloud services could be inaccessible due to these attacks and generate negative impact. It is important and essential requirements for cloud service providers to ensure its services are fully usable and available at all time. Moreover, cloud computing has brought new concerns such as moving resources and storing data in the cloud computing is a shared environment, which uses sharing infrastructure. Hence, data may face issues like privacy and unauthorized access. These issues can get more complicated when different service providers use various types of technologies and cause potential heterogeneity issues. Furthermore, virtualization brings its own issues such as data leakage.

This paper analyses the challenges posed by cloud computing and the standardization work being done by various standards development organization to mitigate privacy risks in the cloud, which include the role of privacy-enhancing technologies.Access control includes authorization, authentication and access approval. A more of access control would cover

only access approval, whereby the system owner makes a decision to grant or reject an access request from an already authenticated subject process, based on what the subject is authorized to access. The fundamental goal of any access control system is restricting a user to exactly what s/he should be able to do and protect information from unauthorized access. Cloud service providers need a strengthened access control system for controlling admission to their resources with the ability to monitor precisely who access them. Different access permissions to a same type of cloud user, and giving him/her ability to use multiple services with regard to authentication and login time. Sharing of resources among potential untrusted tenants, multitenancy and multitasking mechanisms to support transfer customers' credentials across layers to access services.The issue of access control in the domain of distributed applications, in collaborative, distributed, cooperative environments like cloud computing, with respect to various users access the same resources and different services, with different access rights, is called the distributed access control. Various users have different access rights towards the available resources in the system, which need to be concisely specified and correctly enforced.

In access control the service providers and the service consumers do not have a pre-established trust value between them, in the case of open service-oriented systems. Therefore, the authentication of the strange users and the authorization of their access rights are very important, in handling the access requests of the service consumers in distributed computing environments like Cloud Computing. Trust establishment between consumers users, Service provide users and Identity Providers also assumes very high importance in the current scenario of system. In the open distributed systems, generally the user entities have a lot of autonomy and arbitrariness. The service provider and the service requestor may not have a pre-established trust relationship. In Service Oriented Architecture "SOA", which is emerging as an important paradigm for distributed computing, the service requestor and the service provider usually come from different domains. Also, they are independent to each other and may be using different system platforms. Therefore, the access control in distributed environments like SOA or cloud computing is required to cross the borders of security domains, to be implemented between various systems.

II. Related Work

The access control is one of the fundamental requirements in order to avoid unauthorized access to systems and protect organizations assets. Although different access control models IS presented in [1] and policies have been developed such as Mandatory Access Control (MAC) and Role Based Access Control (RBAC) for different environments, these two models may not fulfill cloud's access control requirements. Cloud computing has a diverse set of users with different sets of security requirements. It also has unique security and privacy challenges such as multi-tenant hosting of security and private policies, rules and domains.

The access control of distributed resources is most important in securing the cloud computing. The work presented in [2], it analyze the various access control mechanisms adopted in the distributed computing domain, considering their pros and cons. The propose architecture for the Distributed Access Control (DAC) in the Cloud Computing paradigm, taking into consideration the access control requirements of the cloud service providers and consumers. This also gives the working model for the proposed access control architecture.

In the work explained in [3], described that cloud environment is a large open distributed system. It is necessary to preserve the information, as well as, privacy of users to access data. Access Control methods ensure that authorized user's access the data and the system. This work discusses various features of attribute set based access control mechanism, which is suitable for cloud computing environment. It tends to the design of attribute set based access control mechanism for cloud computing system. Access control is generally a policy or methods that allows or restricts access to a system. It may, also monitor and record all attempts made to access to a system. Access Control may identify users access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, which includes the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and

resources (Objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services.

In [4], different existing techniques for access control which are proposed by others, after that the work will explain the proposed technique for access control in cloud computing. One of the other main methods for access control is FADE. The method in provides fine-grained access control and assured deletion for outsourced data on cloud server. But this kind of scheme is not effectively applicable for it. If any data owner and service providers are in the same kind of domain, then only it act like as an effective type of scheme. One of the other schemes for access control is HASBE. The main drawback of the scheme in is that it is not flexible compared to other schemes. A method for access using KP-ABE (Key Policy Attribute Based Encryption) and PRE (Proxy Re-Encryption) .Due to the overhead of encryption and decryption, this method is not scalable. It also introduce a method for temporal access in cloud computing. In these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain.

The work carried out in [5], a dynamic access control mechanism to achieve cross domain authentication. In this related work, it will focus on the following three main categories of access control models for cloud computing which includes Role-based models, Attribute-based encryption models. This work will review the existing method on each of these above access control models and their variants approaches, characteristics, pros and cons and identify further related research directions for developing access control models for cloud computing environments. Access control is a fundamental aspect of information security that is directly tied to the primary characteristics such as integrity and availability. Cloud computing server providers provide the following basic functionalities from the perspective of access control.

Access control is a procedure that prohibits other users accessing to the data, by granting a part of the users the permissions to access to the data stored in the clouds method is given in [6]. It is an important measure to actualize the user data‘s confidentiality and protect the user’s privacy. It has very important significance to construct a common, efficient, precise and flexible access control model in cloud computing environment. This makes the cloud storage access control has become a challenging research subject. In order to manage the accessing to the shared information/data reasonably, the resource manager presented the level of security and security policy to regulate the user to read the shared information. Access control is to limit the subject (user) to access to the object (file) in order to ensure that the use of data resource is legal.

Proposed access control is of vital importance, given in [7], since it provides security mechanisms to protect against inappropriate ate access to file or data. Unfortunately, classical access control models such as RBAC or ABAC are not sufficiently expressive for highly scalable and dynamic environments such as those are found in the Cloud side and a combination of element sets of these models is necessary in order to properly express varied data protection needs. In this work, we present a new approach called CatBAC (Category Based Access Control model), for building dedicated access control models starting from an abstract meta-model.

In [8], Access control is an emerging and challenging issue in supporting cloud service environment. This work presentes a new access control mechanism called cloud service access control (CSAC). The CSAC mechanism considers payment status and service level as the two essential characteristics of cloud system. .Inconsistent access control policies are detected by a set of proposed policy conflict and to analysis rules. Inappropriate user accesses are inhibited by access control policies according the proposed access denying rules.

In this work it describes a trust-based dynamic access control model for cloud computing environment model presented in [9], inspired by the GTRBAC model, where the users can validate their legal identities and acquire their access control privileges for the resources according to the role information and the trust degree in the lightweight certificates of multiple users. The trust-degree in the certificate can be calculated by the direct trust-degree (DT) and recommendation trust-degree

(RT), while the access permission for the resources can be decided by comparing the trust-degree with trust-degree. Access control has become an important component of the information security. On the other hand, applications of cloud computing have become a hot area in last few years, people also pay more attention to the security issues associated with it. In response to the complex environment in the cloud computing, the work often adopts dynamic access control.

III. Proposed Working System

For every cloud user, the system keeps an attribute corresponding to each of the user In this proposed structure, the system which includes the different attributes like Trust Authority, Attribute Set, Cloud User, Domain, and Unique Attribute. In this structure first the trust authority act as a root of trust and authorizes the top level domain authorities system and this level domain authorities authorize the cloud endusers. Here it considers both the owner and the user as cloud user side but it may vary with the user and at the end our system use a clock to generate the key or token with respect to time.

Working system

Thepresent model of our system is shown in figure 1. In this working model it includes four different attribute parts which are:

1. Cloud owner
2. Cloud server
3. Cloud user
4. Clock for time

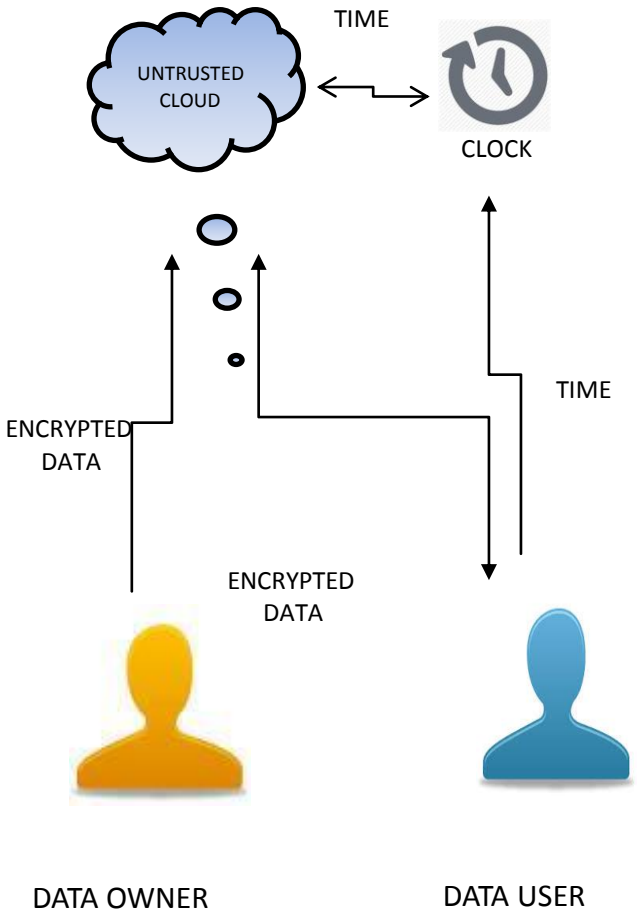

Figure 1: working structure of access control

In the first phase the data owner is uploading his/her file to the cloud side. To make this upload file secured, he/she will encrypt that file and then after upload this file in cloud server. For that only the data owner of this file knows that the key to

decrypt the file, so the file is secure in the cloud server. Secondly when the data user wants to access the file from cloud server side, then the data user send a request to get an uploaded file. After that the cloud will forward that request to the owner of the file. Based on the request the cloud owner will check all the attributes of that user who request. If the user has a valid attributes, then the owner send a unique key to the user side. When the owner send the private key to the user, further on the clock will start counting, within a certain period of time the key becomes invalid for user, within a clock time the user should access the file request, to access it

Some Operations Are Involved In This Model:

a) User/Owner Registration

For accessing or upload a file both user and owner have register there and for this registration both user/owner will send a registration request to the cloud server domain authority. The cloud authority checks and verifies that is the new user member accepting there terms and conditions provided by the authority, then after the domain authority forward that request to the trusted domain side. Then the trusted authority provided a permanent unique ID for each user/owner and according to that user/owner set a password for that to access cloud server information.

b) *Data Owner File Upload*

In the second attribute the owner Upload a fileinto the untrusted cloud, the data owner encrypt the file by using his/her secure key. Then send the upload request to the cloud. The cloud domain authority check whether owner is registered or not. If confirm his/her registration then the domain authority forward encrypted file to trust authority and last upload this requested file into untrusted cloud.

c) File Access From User Side

To access or download file from untrusted cloud, first the data user send a request to the domain authority, The authority verifies his/her registration, if he/she then forward the request to the data owner then the owner check all the attributes of the user. If the user have all valid attributes then after owner send his/her key to access the file, Further on clock will start counting. After certain time, the clock stops and key becomes invalid. So that user should access this file within clock counting.

d) Delete/Remove File

Only data owner has permission to delete the file from untrusted cloud, for that a registration time domain authority provide some permanent ID number to each of the data owners. Now after to delete a uploaded file firstly the request is send to the domain authority, the request contains both the owners ID and name of the file, Then the domain authority request to owner to enter a password, if password matches then the domain authority will forward the deletion request to the trusted authority side and trusted authority check the data file and delete the file from cloud.

IV. CONCLUSION

It is highly anomization model for providing security and access control in cloud operations are uploading and downloading file from owner and user side computing. It is hierarchical structure which is based on the attribute set and it using a clock for decryption of data using key based on time. This working model ensures both access control and security in cloud computing side. The main fundamental operation are uploading and downloading file from owner and user side.

References

1. Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An Access Control Model for Cloud Computing", Journal of Information Security and Applications Vol 19, 2014.

2. Manoj V. Thomas, K. Chandra Sekaran, "Access Control Model for Cloud Computing Environments", International Conference on Advanced Computing, Networking and Security 2013.
3. Abdul Raouf Khan, "Access Control in Cloud Computing", ARPN Journal of Engineering and Applied Sciences, 2012.
4. Bibin K Onankunju, "Security Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Vol 3,2013.
5. Natarajan Meghanathan, "Review of Access Control Models for Cloud Computing", Journal of Information Computer Science & Technology (CS & IT), 2012.
6. Xinlu Li, Xiaoxia Zhao, "Information on Access Control Model in Cloud Computing Environment", International Conference on Cloud Computing and Big Data, 2013.
7. Salim Khamadja, Kamel Adi, Luigi Logrippo, "Designing Flexible Access Control Models for the Cloud", Journal of Research and Secure Information (LRSI),2011.
8. Chi-Lun Liu, "Cloud Service Access Control System Based on Ontologies", Journal Advances in Engineering Software Vol 69, 2014.
9. Zhanjiang Tan, Zhuo Tang , Renfa Li, Ahmed Sallam, Liu Yang, "Research on Trust-Based Access Control Model in Cloud Computing", Journal of Information Security Science and Engineering, 2012.
10. Jinbo Xiong, Zhiqiang Yao, Jun Ma, Ximeng Liu, Qi Li, "Structured Document Model and Its Secure Access Control in Cloud Computing",International Conference on Cloud Computing and Big Data, 2013.

AUTHOR(S) PROFILE

Faisal Mushtaq, is doing M.Tech degree in Computer Computers Science and Engineering from BSA University vandular chennai India, and B-Tech from BGSBU Jammu and Kashmir, India in 2012.

