ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

A Methodology for Development and Verification of Access Control System in Cloud Computing

Ankit Valdaya[1], Ratish Agarwal[2], Sachin Goyal[3]

R.G.N.C.L.C, National Law Institute University, Bhopal, Madhya Pradesh, India [1]

Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh, India [2,3]

Abstract: In Cloud Computing, the feature of multi-tenancy gives privacy, security and access control challenges, because of sharing of physical resources among un-trusted tenants so, a suitable encryption technique with key management should be applied before outsourcing the data. In this paper we develop the methodology of policy based file access using attribute based encryption with cipher text scheme to secure the storage and sharing the cloud data with the cloud user. In this we also discuss the policy of revocation for file assured deletion so that no one can recover the deleted file from cloud and also discuss the policy for access to data storing centre so that the right user will access the right file in cloud.

Keywords: access control in cloud computing, attribute based encryption, policy based access control, revocation of file assured deletion.

I. INTRODUCTION

In Information Technology (IT) the field cloud computing is growing area. It provides access to use the services like networks, servers, storage, applications and etc. It also provides the services in on demand bases that can be rapidly provisioned and released with minimal management effort or service provider interaction. In recent years its advantage of virtualization and high reliability lead to change in computer networks. These are storage, computing and software resources. Basically cloud computing means the pool of shared and virtualized resources and by the use of them large scale resources were assembled through cloud computing. Cloud computing generally provides scalable, low cost and location independent platform. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. There are many challenges in cloud computing for data security because users give their sensitive data to cloud.

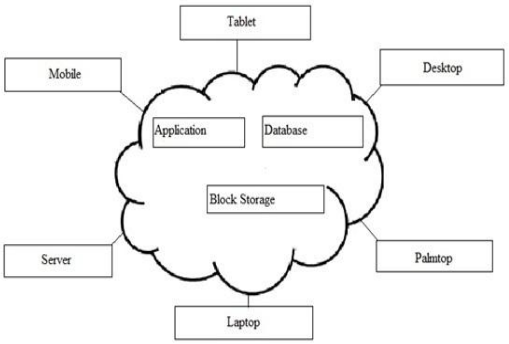

Figure (1)
Cloud providing services to different user's with different devices

There are a variety of methods to access a cloud data centre, because users use varying devices and network environments. Therefore, when various users access a cloud data centre, their context information is always different. Figure 1 shows data sharing with cloud storage. In which the cloud give the services to different users with methods or devices.

Access control is considered as the best security solution for protection of data in cloud. The traditional access control schemes suppose that the data is stored on trusted data servers but in cloud computing the owner of the data and servers of cloud both are in two different domains. So to encrypt the data which is outsourced in cloud computing Attribute Based Access Control (ABAC) system is introduced, in this only authorized user can decrypt to access the data. The access control policy is embedded in every object. This policy is direct contrast to most currently available access control systems which rely straight to the trusted host to maintain policies and mediate access.

II. PRELIMINARIES

In this section we discuss some basic preliminary information regarding Cloud Computing, its Models, Attacks on Cloud Computing, Access Control and its models

A. Cloud

In cloud computing cloud is the accessible infrastructure in order to bring all feasible services to the cloud and make it possible to access those services regardless of time and locations.

B. Computing

In cloud computing the meaning of computing is providing the IT capabilities, adaptable and scalable service to its multiple users.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

C. Cloud computing models

Basically there are three models of cloud computing these are –

1. *Software as a service (SaaS):* In this service the client use the applications provided by the cloud infrastructure through web browser.

2. *Platform as a service (PaaS):* In this service client can create applications by the use of various programming language which is provided by the cloud.

3. *Infrastructure as a service (IaaS):* In this service of cloud computing it provide storage, network, processing and many other computer resources to install and run the software like applications and operating system.

D. Cloud computing attacks

The use of cloud computing are increased and the attacks on cloud computing is also increases along with the development of cloud application attacks. Following are the attacks on cloud computing.

- Denial of Service (DoS) attacks
- Side Channel attacks
- Authentication attacks
- Man-in-Middle cryptographic attacks
- Inside-job attacks

E. Multi-tenancy

Multi-tenancy is an architecture in which multiple clients can use a single instance of the software. In this each client is known as tenant, they can customize their service according to their requirement. In cloud computing the architecture of multi-tenancy gives advantage of virtualization and remote access.

F. Access control

It is a system which allows or denies the access by some policy or procedure and also monitors the attempts which are done to get the access of the system. Access control is also providing security to cloud computing from various attacks which are discussed above. There are various access control models are use to provide the security. Methods of access control are effective in unchangeable distributed system, where there are only a set of Users with a known set of services.

G. Access Control Model

There are three main types of access control models these are –

1. *Mandatory Access Control (MAC):* This access control model is mainly use where priority is placed on confidently. In this administrator define the usage and policy of access control which cannot be change by the user only administrator can change the policy that show which user has access to which programs and files.

2. *Discretionary Access Control (DAC):* This access control gives full control to the user to determine the controls on files and programs. In this model user give permission according to need. The discretionary access control model is also known as need to know access model.

3. *Role Based Access Control (RBAC):* This access control model is mainly talks about giving the access rights to the particular role rather than giving it to any user. In role based access control model the privilege is assigned to the role so then any person who have that role may have the privilege. In this each role can assigned to one or more user and each user can have one or more role.

III.REVIEW OF LITERATURE

As a new information service mode, cloud computing has brought new security risks and challenges. So the number of Research Papers has been published by the several authors in this area to provide more and more security in access control of cloud computing. Some of the important research papers on this are as follows:

Cloud computing is a new paradigm which enables users to reduce their costs and is advantageous to both the serving and served organizations. The most effective way of protecting cloud computing services, resources and users is access control. Here in this paper [1] Guoyuan Lin, Yuyu Bie and Min Lei intend to provide a trust-based access control mechanism for cloud computing considering its multi-domain aspects. Firstly, trust is introduced into cloud computing environment and trust relationships between users and cloud platform are built. It also analyzes the difference between intra-domain trust and inter-domain trust. Furthermore, a role-based access control framework combined with trust degree in multi-domain is given from this paper. 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 simulation results show that the proposed method is more suitable to cloud environment and definitely can improve the reliability and validity of the system.

In cloud computing at present there is no authorization recycling approach so in this paper [2] Reeja S L develops an authorization recycling approach using CSAR (Co-operative Secondary Authorization Recycling) in Cloud computing Systems. By this each application server recycles previously received authorizations and shares them with other application servers to mask authorization server failures and network delays. The CSAR approach exploits the increased hit rate offered by a co-operative cache of access control decisions. The CSAR supports approximate authorizations that are not precached and must be computed dynamically. The authorizations from other SDPs need to be verified to ensure authenticity, integrity, and correctness. With role-based access control, access decisions are based on the roles that individual users have as part of an organization. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization. This is performed by using a simulation tool known as CloudSim.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

It provides basic classes for describing data centres, virtual machines, applications, users, computational resources, and policies for management of diverse parts of the system.

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. Here [3] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou were discussed that the problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. So by addressing this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Access control is one of the most important security mechanisms in cloud computing. Attribute-based access control provides a flexible approach that allows data owners to integrate data access policies within the encrypted data. So in this [4] Yan Zhu∗, Hongxin Hu†, Gail-Joon Ahn†, Dijiang Huang†, and Shanbiao Wang discussed present an efficient temporal access control encryption scheme for cloud services with the help of cryptographic integer comparisons and a proxy-based re-encryption mechanism on the current time. We also provide a dual comparative expression of integer ranges to extend the power of attribute expression for implementing various temporal constraints. We prove the security strength of the proposed scheme and our experimental results not only validate the effectiveness of our scheme, but also show that the proposed integer comparison scheme performs significantly better than previous bitwise comparison scheme.

Cloud computing is an advanced emerging technology. In this world the storage of data is a big headache for all. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. The main issue in cloud computing is security. Here [5] Bibin K Onankunju introduce a new method for providing secured access control in cloud computing. This model provides a secure access control in cloud computing. To provide more secured access control it adopts a hierarchical structure and it uses a clock. Using this we can easily upload, download, and delete files from and to the cloud. This model ensure both security and access control in cloud computing. The main operations in this model are registration, file upload, file download and file deletion.

In this paper [6] "JieHui Ju, ZhongYou Wang, WenJuan Li, WeiZheng Bao and Ya Wang" focuses on the research of optimizing the safety and utility, proposing safety policy optimized model in cloud computing environment based on stochastic programming theory, building mathematical models which are on the basis of ensured data security to enhance the users' utility, model analysis and optimization, and ultimately get the best optimized configuration of security policy in the cloud computing environment to guide the formulation and dynamic adjustment of access control policy in cloud computing environment, and to meet the users' requirements, such as response time, resources availability and other utility requirements.

In this paper [7] Seul-ki Choi and Jin Kwak says that to provide secure and efficient access control methods in cloud computing environments, many system models have been proposed that employ attribute-based encryption and proxy re-encryption schemes. Most of these access control schemes are based on the user's authentication information and access privileges. However, when users request access privileges through non-secure environments such as mobile devices and wireless networks, we need to be able to restrict access requests, depending on the user's context-aware information. To achieve this, in this paper we propose an access restriction scheme for access to cloud data that is based on context-aware information.

In this paper [8] V.Karthik, K.S.Arvind discusses that Cloud computing, as an emerging computing standard. Cloud computing enables users to remotely store their data in a cloud and also benefit from services on-demand. With rapid development of cloud computing, more enterprises will outsource their sensitive data for sharing in a cloud. To maintain the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The major problems of this approach include establishing Decomposing Access Control Polices, delegated access control for the encrypted data, proof of ownership allow storage server to check a user data ownership based on hash value and the access rights from users when they are no longer authorized to access the encrypted data. In the proposed approach the privacy of users is protected while enforcing attribute based ACPs and utilizing the two layer of encryption reduce the overhead at Owner, opposed to unauthorized access to data and to any data leak during sharing process, providing levels of access control verification.

IV. MOTIVATION BEHIND RESEARCH

Even we have achieved the flexibility, scalability in cloud computing but this technique fails to proven the integrity of data. So that owner of data facing problem of missing and data corruption because of less control over data. Some users take the cloud service to store their data so that

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

they can retrieve it from anywhere, but their data is not secure because if attacker got access to the services then he/she can do anything with the user's data. The Key Generation Centre (KGC) could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users key.

V. OBJECTIVE OF PAPER

The objective behind this research paper is to develop a methodology to improve the access control system in cloud computing. This methodology for development and verification of access control system in cloud computing will give more security to the data and their user who have their confidential data on cloud. So that it can prevent data from unauthorized access.

VI. PROPOSED METHODOLOGY

In this paper the methodology for research is based on the previous research papers on the topics which are related to access control in cloud computing and also from the various books and projects on cloud computing and its access control system. So the proposed methodology for the above stated problem is policy based file access using attribute based encryption with cipher text policy scheme. Researchers think that this methodology will secure cloud storage and data sharing system. And by this method the data confidentiality and privacy can be cryptographically enforced against any curious key generation centre or data storing centre.

A. Structure of Proposed Model

The structure of the proposed model is shown in Fig. 2. It involved data owner, user, KGC and data storing centre.

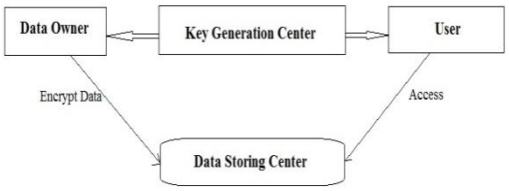

Figure (2) Proposed Model

Here Key Generation Centre (KGC) is a key authority that generates public and secret parameters. Data owner upload his data into data storing centre which give ease to share the data. Data owner defines the attribute based access policy then encrypt the data under the policy to secure storage and distributing the data. Data storing centre is also uses the file upload and download policy to ensure the secure data storage and sharing with the user. User is an entity who wants to access the data.

B. Policy of Revocation for File Assured Deletion

In this if the data owner request then the policy of file may be revoked after the expiring of the time period of the contract and after completely moves from one cloud to another cloud. The policy will be revoked if the above thing happens and after this the key manager will completely remove the public key of the file from KGC. By this we can say that the file is assuredly deleted.

C. Policy for Access to Data Storing Centre

Ability to limit and control the access to data storing centre via communication links. To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files. Each user has associated with policies for each file. So the right user will access the right file. For making file access the attribute based encryption scheme is utilized.

VII. CONCLUSION

In this paper we propose the methodology for development and verification of access control system in cloud computing so to achieve more secure cloud storage and data sharing system we give the methodology that is policy based file access using attribute based encryption with cipher text policy scheme. Revocation of file is important that will remove the files of revoked policies so no one can recover and access the revoked file after deletion. We also give the policy for access to data storing centre to securely access the data from it. The proposed scheme is efficient and scalable to securely manage user data in the data sharing system.

REFERENCES

[1] Guoyuan Lin, Yuyu Bie, Min Lei "Trust Based Access Control Policy in Multi-domain of Cloud Computing", JOURNAL OF COMPUTERS, VOL. 8, NO. 5, MAY 2013

[2] Reeja S L "Role based access control mechanism in cloud computing using co – operative secondary authorization recycling method", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 10, October 2012).

[3] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing"

[4] Yan Zhu∗, Hongxin Hu†, Gail-Joon Ahn†, Dijiang Huang, and Shanbiao Wang "Towards Temporal Access Control in Cloud Computing", The 31st Annual IEEE International conference on computer communication

[5] Bibin K Onankunju "Access Control in Cloud Computing", International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 ISSN 2250-3153

[6] JieHui Ju, ZhongYou Wang, WenJuan Li, WeiZheng Bao and Ya Wang "Research on the Security based on Utility Theory in Cloud Computing Environment" International Journal of Security and Its Applications, Vol.8, No.4 (2014), pp.321-328

[7] Seul-ki Choi and Jin Kwak "Context-Aware Information-Based Access Restriction Scheme for Cloud Data" International Journal of Multimedia and Ubiquitous Engineering, Vol.8, No.6 (2013), pp.97-104

[8] V.Karthik, K.S.Arvind "A Survey on Delegated Access Control in Public Cloud" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2014

[9] B. SakthiSaravanan., R.Dheenadayalu, A.Vijayaraj "Improving Efficiency and Security Based Data Sharing in Large Scale Network" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013