DATA ACCESS CONTROL WITH MULTI-AUTHORITY IN MULTI-CLOUD STORAGE SYSTEMS

T.R.Muhibur Rahman[1], Durganjali T[2], Bindurani HM[3], Harshitha P[4], Tameem K[5]
[1]Assoc. Professor, Department of Computer Science and Engineering,
Ballari Institute of Technology and Management, Ballari, Karnataka, India.
[2,3,4,5]8thsem, CSE student, Ballari Institute of Technology and Management, Ballari, Karnataka, India.

Abstract: Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. Every uploaded file is split into multiple clouds thereby enforcing multi-cloud concept. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. Moving data into the cloud offers great convenience to users since they don’t have to care about the complexities of direct hardware management. The ever cheaper and more powerful processors, together with the software as a service computingarchitecture, are transforming data centers into pools of computing service on a huge scale. This application provides an interface to users to view the details like the available assets and future releases (Assets getting released byemployees in near future). This helps to prevent unnecessary orders to vendors to supply an asset which is very difficult in current system (manual system). This system maintains the Item details like Asset/item type, item description, oracle item code, quantity etc. This system clearly keeps track of the status of assets by holding the location details, receipt entry, issue entry, date of transaction, etc which helps in proper utilization. At any point of time, IT Infrastructure team view the state and status of an asset, requirement of assets. This system provides effective way to manage the important information in a very secure manner by authenticating users at various levels.

Objectives:

- To provide security to client data.
- To effectively enforce the concept of multi-cloud where each uploaded file is partitioned and placed in different clouds
- To support multi-authorities and make each authority issue attributes independently.
- To achieve cloud efficiency and user satisfaction.
- To provide OTP system to login. To track the change requests from client automatically.

II. LITERATURE REVIEW

[1]In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on „„Attribute Based Data Sharing with Attribute Revocation,"". This paper use semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CPABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks. Provide importance to attribute revocation which is difficult for CP-ABE schemes. Drawback: The storage overhead could be high if proxy servers keep all the proxy re-key.

[2]In 2011, S J. Hur and D.K. Noh, worked on „„Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,"". This paper proposes an access control mechanism based on cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. This dual encryption mechanism takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. The advantage of this scheme is securely managing the outsourced data. This scheme achieve efficient and secure in the data outsourcing systems. Drawback: Huge issue in Enforcement of authorization policies and the support of policy updates

[3]In 2011, S. Jahid, P. Mittal, and N. Borisov, worked on „„Easier: EncryptionBased Access Control in Social Networks with Efficient Revocation.The proposed Easier architecture that supports two approaches are fine-grained access control policies and dynamic group membership. Both scheme achieved by using attribute based encryption, however, is that it is possible to remove access from a user

without issuing new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is the Easier architecture and construction provides performance evaluation, and prototype application of our approach on Face book. Drawback:

 Does not Achieve Stronger Security Guarantees

International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 3, Issue 12, December 2014 1726
ISSN: 2278 – 909X All Rights Reserved © 2014 IJARECE

[4], In 2013, S. Jahid, P. Mittal, and N. Borisov, worked on „„Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption, This model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved. Drawback:

 Existing attribute revocation methods rely on a trusted server orlack of efficiency also theyare not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems. Each Attribute authorities (AAs) is trusted but can be corrupted by the adversary. Each user is dishonest and may try to obtain unauthorized access to data.

III. EXISTING SYSTEM

This existing paradigm of data hosting and data access services introduces a great challenge to dataaccess control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. Current system stores complete file on a single cloud.

Disadvantages of Existing System

- Security threat due to storage of complete data in a single cloud.
- The cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control.
- Chase’s multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system.
- Chase’s protocol does not support attribute revocation.

IV. PROPOSED SYSTEM

In this paper, we first propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt)and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient .attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semitrusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

Advantages Of Proposed System:

- We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation.
- We greatly improve the efficiency of the attribute revocation method.
- We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a ciphertext.

Software Requirements and Specifications

1. Functional Requirements

The main purpose of functional requirement is to define all the activities or operations that take place in the system. These are derived through interactions with the users of the system. Since the Requirements Specification is a comprehensive document & contains a lot of data, it has been broken down into different Chapters in this report.

But the general Functional Requirements arrived at the end of the interaction with the users are listed below.

1. Administrator can upload the files in to multiple clouds.
2. Administrator can add and delete files.
3. Administrator can view all user registration.
4. Administrator can give the permission to the user.
5. User can read or download the files.
6. User can send the file request to the admin.
7. User has option to change the password.

2. Non Functional Requirements

Reliability:

- The system must be highly reliable as it would be handling critical data regarding the project.
- Unauthorized person should not able to access the details.
- This system must perform all of its operations with high accuracy.

Availability

- The system must be readily available to the students who need to apply for placement.

- The system must work in relatively fast and must provide the data on request as soon as possible without affecting the quality & accuracy

Security

- The System must be highly secured and must authenticate users strictly.
- The System would require handling confidential data and thus must provide security towards both front & back end.

Maintainability

- The maintainability of the system must be high.
- Proper documentation must be provided so as to perform enhancement, adaptation and to fix bugs (if any).

V. IMPLEMENTATION MODULES

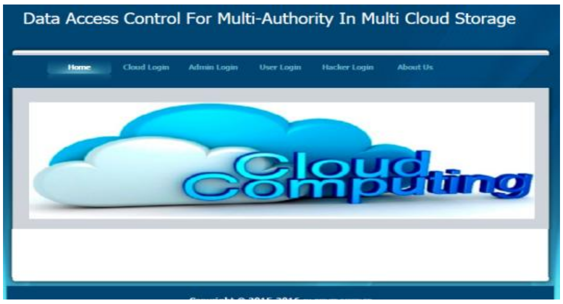


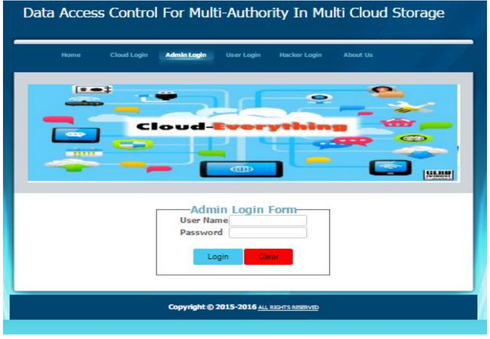
Fig 1. Home page

Cloud module

- Login: Cloud can login with the username and password.
- View files: Cloud can view the details of the files and action will be taken to upload files into the cloud.
- View Users: Cloud can view user details.
- Logout: Cloud will logout from home page.

Admin module

- Login: Admin will login into his/her home page by entering the username and password.


Data Access Control For Multi-Authority In Multi Cloud Storage
Home
Cloud Login
Admin Login
User Login
Hacker Login
About Us
Cloud-Everything

Admin Login Form
User Name
Password
Login
Clear

Copyright © 2015-2016 ALL RIGHTS RESERVED

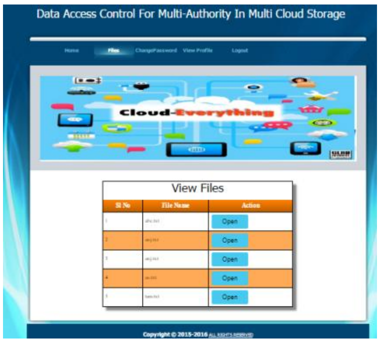
- Upload: Admin can upload the files in to the cloud and he /she can view the details of the uploaded files.
- User details: Admin has the authority to view the requested user details.
- Restriction: Admin has the authority to put restrictions to particular files, the restrictions are:

1. read and 2.read/write.

- View hacker: Admin can view how many times the hacker try to access the particular file.
- Logout: Admin will logout from his/her home page.

User Module

- Registration: New user will register by entering his/her personal details with OTP verification.
- Login: After registration user can login with the username and password.
- Files: User can view the files.


Data Access Control For Multi-Authority In Multi Cloud Storage
Home
Files
ChangePassword
View Profile
Logout
Cloud-Everything

View Files

Sl No	File Name	Action
1	abc.txt	Open
2	[illegible]	Open
3	[illegible]	Open
4	[illegible]	Open
5	[illegible]	Open

Copyright © 2015-2016 ALL RIGHTS RESERVED

- Change password: User can change the current password.
- View profile: User can view and edit the his/her personal details.
- Logout: The user will logout.

VI. CONCLUSION

We proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

[1] P. Mell and T. Grance, ‘The NIST Definition of CloudComputing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-PolicyAttribute-Based Encryption,’’ in Proc. IEEE Symp. Security andprivacy (S&P’07), 2007, pp. 321-334.

[3] B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization,’’ in Proc.4th Int’l Conf. Practice and Theory in Public Key Cryptography(PKC’11), 2011, pp. 53-70.

[4] M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ inProc. 4th Theory of Cryptography Conf. Theory of Cryptography(TCC’07), 2007, pp. 515-534.

[5] M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Securityin Multi-Authority Attribute-Based Encryption,’’ in Proc. 16thACM Conf. Computer and Comm. Security (CCS’09), 2009,pp. 121-130.

[6] J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control withEfficient Revocation in Data Outsourcing Systems,’’ IEEETrans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221,July 2011.

[7] S. Jahid, P. Mittal, and N. Borisov, ‘‘Easier: Encryption-BasedAccess Control in Social Networks with Efficient Revocation,’’ inProc. 6th ACM Symp. Information, Computer and Comm. Security(ASIACCS’11), 2011, pp. 411-415.

[8] K. Yang and X. Jia, ‘‘Attribute-Based Access Control forMulti-Authority Systems in Cloud Storage,’’ in Proc. 32th IEEEInt’l Conf. Distributed Computing Systems (ICDCS’12), 2012,pp. 1-10.