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 6, June -2015

COMMUNICATIVE, RESOURCEFUL & REVOCABLE DATA WAY IN MANGE WITH SURVEY FOR MULTI-AUTHORITY CLOUD

T.Vinoth kumar[1], Dr.R.Indra Gandhi[2]

[1]*Department of Computer Applications, GKMCET*
[2]*Department of Computer Applications, GKMCET*

ABSTRACT: *The cloud information administrations, it is typical for information to be put away in the cloud, as well as imparted crosswise over various Users. A few systems have been intended to permit both information holders and open verifiers to proficiently review cloud information trustworthiness without recovering the whole information from the cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most appropriate technologies for data access control in cloud storage, because it gives data owners more direct control on right to use policies Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the fundamental techniques to design the data access control scheme. Our attribute revocation method can competently achieve both forward security and rearward security. 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.*

KEYWORDS: *Cloud Computing ,Cipher text-Policy Attribute-based Encryption, Proxy Re-encryption, Revocation.*

1.INTRODUCTION

Cloud storage is a basic organization of appropriated processing which offers organizations for data chiefs to host their data in the cloud. CLOUD storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-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. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies.

There are two types of CP-ABE systems:

- ✓ single-authority CP-ABE where all attributes are managed by a single authority, and
- ✓ multi-authority CP-ABE

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. where attributes are from different domains and managed by different authorities.

2.EXISTING TECHNIQUE

(CP-ABE) Ciphertext Policy Attribute-based Encryption is seen as a champion amongst the most suitable progressions for information access control in coursed stockpiling structures, in light of the way that it
gives the information chief all the more clear control on access strategies. It Cannot Store them in mixed format. Each customer is deceitful and may interest to get unapproved access to data. each customer having the changed key. (CP-ABE) Cipher text Policy Attribute-based Encryption is seen as a champion amongst the most suitable progressions for information access control in coursed stockpiling structures, in light of the way that it
gives the information chief all the more clear control on access strategies. It Cannot Store them in mixed format. each customer is deceitful and may interest to get unapproved access to data. each customer having the changed key.

3.PROPOSED SYSTEM

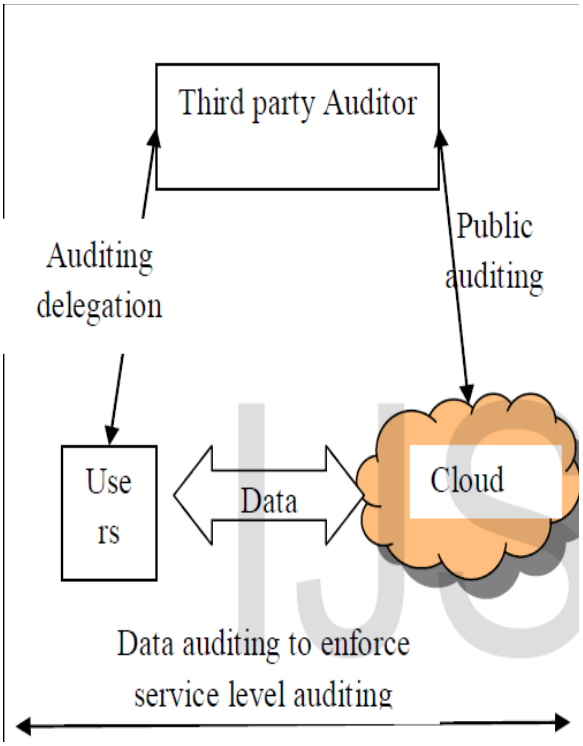
Our proposed data access control scheme is secured in the random oracle model and is more efficient than previous works. we proposed a revocable multi authority CP-ABE scheme that can support efficient attribute revocation. then we constructed an effective data access control scheme, for multi authority cloud storage systems, 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 semi-trusted in some scenarios, our scheme can still guarantee the backward security.

4.DATA STORAGE IN CLOUD

Distributed storage is a model of information stockpiling where the computerized information is put away in coherent pools, the physical stockpiling degrees various servers and physical environment is ordinarily claimed and oversaw by a facilitating organization. The distributed storage suppliers are in charge of keeping the information accessible and available at all times, and the physical environment ensured and running. Associations and people purchase or lease stockpiling limit from the suppliers to store client, association, or application data. Security of put away information and information in travel may be a worry when putting away touchy information at a distributed storage supplier. Clients with particular records-keeping prerequisites.

CLOUD STORAGE AND SECURITY:

In the distributed cloud servers, the correctness and availability of the data files being stored. One of the key issues is to effectively detect any unauthorized data modification and corruption. The Third Party Auditing allows to save the time and computation resources with reduced online burden of users. The raptor code is used instead of erasure code. Encode the input symbols using a traditional erasure correcting code,



Fig(i).Third party auditor

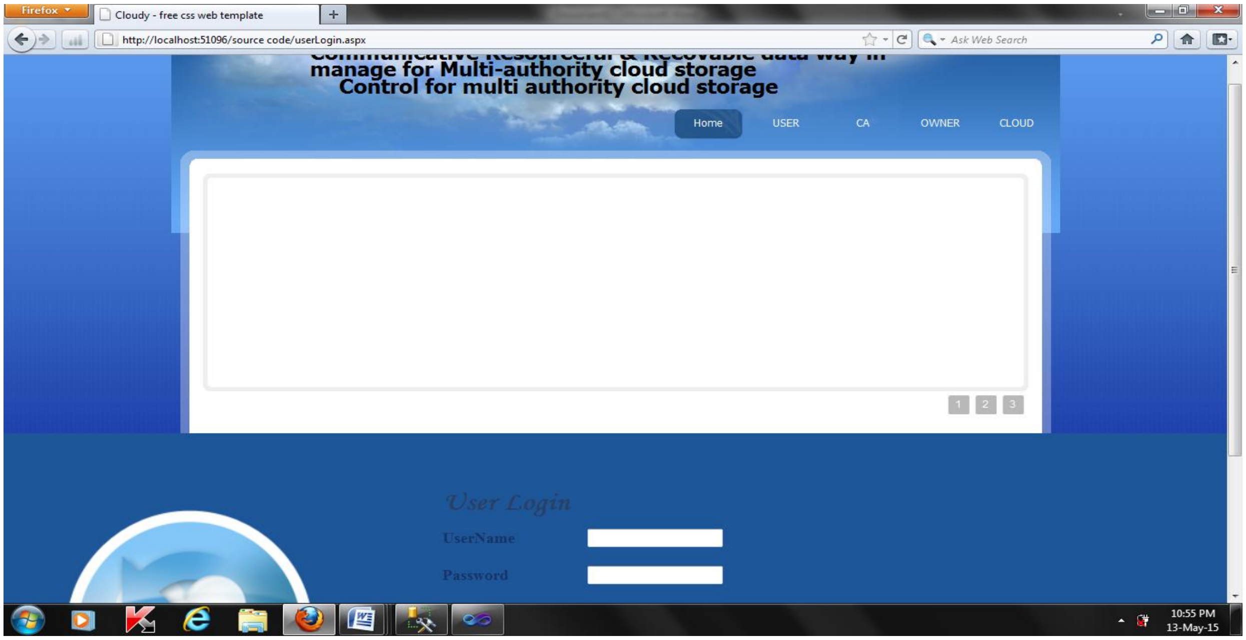
Data Encryption algorithm is used to control the outsourced data and provide the quality of the cloud storage service for the users, an efficient data encryption, data decryption, key rotation and cryptographic hash techniques. To detect the dishonest party we implemented the verification techniques using hash function at TTP. The simulation result for accessing the outsourced data from the CSP shows that the proposed cloud security system is highly secure than the existing security systems. To support, insertion, deletion and updation dynamic operations on encrypted data block, Security system can be further extended.

5.REVOCABLE MULTI AUTHORITY CP-ABE

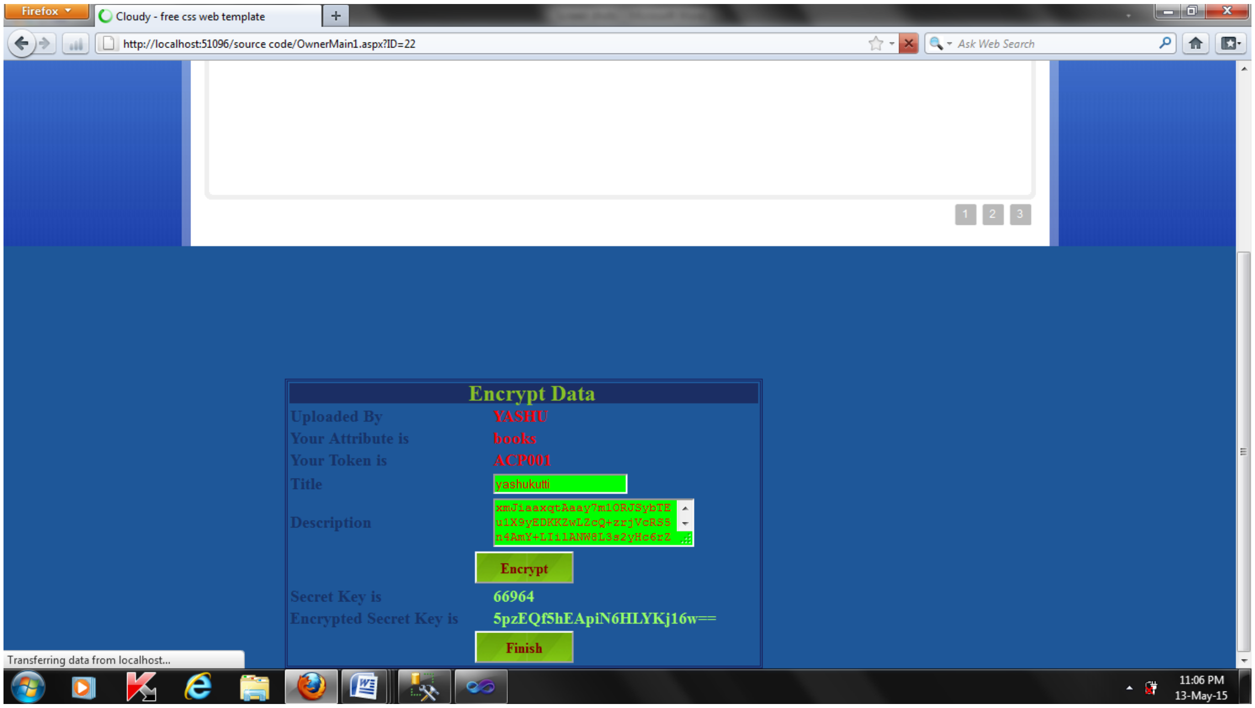
To solve the existing security issue in this paper, we first propose a revocable multi authority CP-ABE plan, where an effective and secure renouncement system is proposed to take care of the trait disavowal issue in the framework. As portrayed in our quality disavowal technique is effective as in it acquires less correspondence expense and reckoning cost, and is secure as in it can attain to both retrogressive security (The repudiated client can't unscramble any new ciphertext that obliges the denied credit to decode) and forward security (The recently joined client can likewise decode the beforehand distributed ciphertexts1, in the event that it has sufficient characteristics). At that point, we apply our proposed revocable multi-power CP-ABE conspire as the hidden strategies to build the expressive and secure information access control plan for multi-power distributed storage frameworks.

There are five types of entities in the system:

- ❖ Certificate authority (CA),
- ❖ Attribute authorities (AAs),
- ❖ Data owners (owners),
- ❖ Cloud server (server)
- ❖ Data consumers (users).


Firefox
Cloudy - free css web template
http://localhost:51096/source code/userLogin.aspx
Ask Web Search
Communicative Resourceful & Recoverable data way in
manage for Multi-authority cloud storage
Control for multi authority cloud storage
Home
USER
CA
OWNER
CLOUD
1
2
3
User Login
UserName
Password
10:55 PM
13-May-15

Fig(i).Home page into the process


Firefox
Cloudy - free css web template
http://localhost:51096/source code/OwnerMain1.aspx?ID=22
Ask Web Search
1 2 3
Transferring data from localhost...
11:06 PM
13-May-15

Encrypt Data

Uploaded By YASHU
Your Attribute is books
Your Token is ACP001
Title yashukutti
Description xmJiaaxqtAaay7m1ORJSybTE u1X9yEDKKZwLZcQ+zrjVcRS5 n4AmY+LIilANW8L3s2yHc6rZ
Encrypt
Secret Key is 66964
Encrypted Secret Key is 5pzEQf5hEApiN6HLYKj16w==
Finish

Fig(ii).Implementation Data for Process

SYSTEM AND SECURITY MODEL

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. Each user will be issued a Social Security Number (SSN) as its global identity.

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities. Each owner first divides the data into several compo-nents according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granula- rities of information from the same data.

SECURITY ANALYSIS:

We prove that our data access control is secure under the security model we defined, which can be summarized as in the following theorems.

Theorem I:

When the decisional q-parallel BDHE assumption holds, no polynomial time adversary can selectively break our system with a challenge matrix of size l_ n_, where n_ _ q. Proof. The proof is given in the supplemental file available online.

Theorem II:

Our scheme can achieve both Forward Security and Backward Security.

Backward Security:

During the secret key update phase, the corresponding AA generates an update key for each non-revoked user. Because the update key is associated with the user's global identity uid, the revoked user cannot use update keys of other non-revoked users to update its own secret key, even if it can compromise some non-revoked users.

INITIALIZATION:

The system initialization contains

- CA Setup
- AA Setup.

CA Setup The CA sets up the system by running the CA setup algorithm CASetup, which takes a security parameter as input. The CA first chooses two multiplicative groups G and GT with the same prime order p and a bilinear map e : G G ! GT . It also choose a hash function H : f0; 1 g_ ! G that matches the string to an element in G, such that the security will be modeled in the random.

GPP ¼ ðg; ga; gb; HÞ:
GSKuid ¼ uuid; GSK0uid ¼ u0uid:
It then generates the user's global public keys as
GPKuid ¼ guuid ; GPK0uid ¼ gu0uid

AA Setup :

Let Said denote the set of all attributes managed by each attribute authority AAaid. It chooses three random numbers _aid; _aid; _aid 2 Zp as the authority secret key

SKaid ¼ ð_aid; _aid; _aidÞ;
is used for data encryption, _aid is used to distinguish attributes from different AAs and _aid is used.

6. PERFORMANCE ANALYSIS:

In this section, we analyze the performance of our scheme by comparing with the Ruj's DACC scheme and our previous scheme in the conference version in terms of storage overhead, communication cost and computation efficiency. We conduct the comparison under the same security level. Let jpj be the element size in the G; GT ; Zp. Suppose there are nA authorities in the system and each attribute authority AAaid manages naid attributes. Let nU and nO be the total number of users and owners in the system respectively. For a user uid, let nuid;aidk ¼ jSuid;aidk j denote the number of attributes that the user uid obtained from AAaidk . Let ' be the total number of attributes in the ciphertext.

7.CONCLUSION

During this paper, we have a tendency to projected a revocable multi-authority CPABE theme that may support economical attribute revocation. Then, we have a tendency to made a good information access management theme for multi-authority cloud storage systems. The revocable multi-authority CPABE may be a promising technique, which may be applied in any remote storage systems and on-line social networks etc.

REFERENCES:

1. R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data," Proc. Advances in Cryptology (CRYPTO '05), pp. 223-240, 2005.
2. R. Ostrovsky and W. Skeith, "Private Searching on Streaming Data," J. Cryptology, vol. 20, no. 4, pp. 397-430, 2007.
3. R. Ostrovsky and W. Skeith, "Algebraic Lower Bounds for Computing on Encrypted Data," Proc. Electronic Colloquium on Computational
Complexity (ECCC '07), 2007.
4. P. Paillier, "Public Key Cryptosystems Based on Composite Degree Residue Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99),pp. 223-238, 1999.