OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SECURE DATA IN CLOUD STORAGE USING EFFICIENT AND REVOCABLE MULTI AUTHORITY SCHEME

Miss Jyoti R. Patil [1], Mr. Prashant M. Mane [2]

ME student, Department of Computer Engineering, Zeal college of engineering, Pune , India[1]

Assistant Engineer, Department of Computer Engineering Zeal college of engineering, Pune., India[2]

patiljyotirr@gmail.com [1] , prashant.mane @gmail.com [2]

Abstract: **The cloud ensures the data security by data access control. The challenges in cloud storage system are data access control, data outsourcing and the unreliable cloud server. Ciphertext-Policy based on attributes Encryption (CP-ABE) is viewed as appropriate amongst the most techniques; as it gives information proprietors have more straightforward control over access approaches. Furthermore, it is extremely hard to apply the ways out information straightforwardly to existing CP-ABE programs to get control for distributed storage frameworks due to issues of trait repudiation. In that, design the multi authority scheme for revocable data access control system in cloud storage system, where more authorities exists and each authority can give attributes independently. A convertible multi-specialist CP-ABE is proposed and applies it as the hidden techniques to plan the information get to control blueprint. By applying the strategy for alterable characteristics both forward and in reverse security can be procured viably. The aftereffects of the investigation and the recreation demonstrate that our data is proposed the entrance control conspire is secure in the irregular prophet show and is more effective than existing.**

Keyword*: Access control, multi-authority, CP-ABE, attribute revocation, cloud storage.*

---∴∴∴---

I INTRODUCTION

Cloud storage is an important cloud computing service, providing services to data owners to host their data in cloud. This new paradigm of data and Access to data services is a great challenge for data access control. Because the cloud server cannot be completely building on data owners, they can no longer rely on servers encrypt encrypted access control by attributes (CP-ABE) is considered one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct access control [4]. In the CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority may be the registration office at a university, the human resources department in a company, etc [1]. The data owner characterizes get to approaches and encrypted information in view of strategies every client will get a mystery key mirroring its characteristics. A user can only decrypt data when their attributes meet the access policies [7]. In multiple cloud storage systems, the user's attributes can be dynamically modified. A user can have the right some new attributes or revoked some current attributes. And your permission to access the data should be changed consequently. However, the methods of revoking existing attributes rely on a reliable or missing server efficiency is not enough to deal with the problem attribute revocation problem in data access control multi-author cloud storage systems [3]. In this, we propose system for the first time a revocable multi-authority authority CP-ABE, where an efficient and secure system the revocation method is proposed to resolve the attribute revocation problem in the system.

II REVIEW OF LITERATURE

Qi Li, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, Danwei Chen [1]. Present MAACS, a new fine-grained attribute-based access control scheme formality-authority cloud storage applications. Our MAACS consists of a new adaptively secure MA-CP-ABE scheme with decryption outsourcing and a revocation approach. We lighten the decryption cost for data users by outsourcing the complicated bilinear pairing computation to the clouds. In MAACS, a data provider can define flexible access policies

over descriptive attributes and encrypt the sensitive data before uploading it to the cloud severs. A user is authorized only if he possesses proper attributes that satisfy the access policy deployed in the data.

Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE [2]. Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the fetch policies based attributes from many attribute authorities and encrypts the content keys under the policies. Then, the owner sends the encrypted data to the cloud server together with the cipher-texts.

B. Waters [3]. In this paper three constructions within our framework. Right off the bat framework is specifically checked secure under the supposition that we call the parallel example Bilinear of e-Hellman (PBDHE), which can be viewed as a speculation of the BDHE presumption. Our the following two constructs provide performance commercials to achieve testable security respectively under the decisive (slope) Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman Assumptions.

A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters [4]. In this document, we present two fully secure functional encryption schemes. Our first result is a fully secure attribute encryption system (EBA). ABE previous constructions have been shown only selectively safe. We get total security by adjusting the double System encryption methodology latest introduced by Waters and previously used get IBE and HIBE systems fully safe. The main challenge in dual system application Encryption for ABE is the richest encryption of passwords and encrypted texts. In an IBE or HIBE system, Keys and encrypted texts are associated with the same kind of simple object: identity. In an ABE system, encrypted keys, and texts are associated with more complex objects: attributes and access to formulas.
M. Chase and S.S.M. Chow [5]. In more authority ABE scheme, multiple attributes, authorities monitor different set the attributes and output the corresponding decryption user and digit keys may require a user keys for the appropriate attributes of each authority before decoding a message that Chase [5] has given more authority ABE that uses the concepts of a trusted central authority. (CA) and Global Identifiers (GIDs). However, CA in that the building has the power to decipher each encrypted text, which in some way seems contradictory to the original objective of distributing control over many potentially unreliable authorities.

A.B. Lewko and B. Waters [6]. When we build our system, our biggest technical obstacle is to make it complicated. Encryption systems based on previous attributes have given resistance to collusion when the ABE system authority \ bound "set of different components (representing different attributes) of a user private key that randomizes the key. However, in our system each component comes from a potentially different authority, where no coordination between them is assumed authorities. We create new techniques for linking key components and avoid collusion attacks between users with different global identities.

S. Yu, C. Wang, K. Ren, and W. Lou [7]. In CP-ABE, each user is associated with a set of attributes and data encrypted with attribute structures. A user can decrypt a Encrypted text if and only if its attributes satisfy the encryption text access structure In addition to this fundamental property, practical applications quotes generally have other requirements. In this role we focus on an important issue of withdrawing attributes that is cumbersome for CP-ABE systems. In particular, address this challenging problem by considering it more practical scenarios where semi-trusted proxy servers are available.

M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou [8]. In that they propose another patient-focused structure and an arrangement of instruments for controlling access to PHR information put away on semi-put stock in servers. We focus on the scenario of the owner of more data and we divide users into the PHR system in multiple security domains that considerably reduce the complexity of key management for owners and users. A high level of patient privacy is guaranteed simultaneously by leveraging EBAs by more authorities. Their outline takes into account dynamic changes of access strategies or record characteristics, bolsters compelling repudiation of client/asks for traits and softened glass access up crisis situations.

J. Hur and D.K. Noh [9]. In this role, it proposes a fetch control mechanism that uses cryptographic message attribute-based encryption to enforce fetch manage policies the efficient attribute and the ability to revoke the user. The metric fetch control can be achieved through a double coding scheme that uses attribute-based cryptography and selective distribution of the group key in each attribute group. Let's show how implement the proposed mechanism to manage outsourced data safely.

S. Jahid, P. Mittal, and N. Borisov [10]. We achieve this by creating a proxy that participates in the process of decryption and imposes the revocation limitations The proxy is a minimum trust and cannot decrypt encrypted texts or provide access to previously revoked ones users. We describe the architecture and construction of EASIER, provide performance evaluation and application of prototypes of our focus on Facebook.

III SYSTEM OVERVIEW

Problem Statement:

User secret key isn't identified with the proprietor's critical, to such an extent that every client just needs to hold

one mystery key from every specialist rather than various mystery keys related to different proprietors. 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 cipher text.

Statement Scope

The scope is 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.

Objectives

The main objective of the project is to 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 attribute independently.

To change the structure of the scheme and create it more virtual to cloud storage systems, in which data owners are not involved in the key generation.

To enhance the proficiency of the trait renouncement strategy.

IV SYSTEM ANALYSIS

In framework, propose a revocable multi specialist CP-ABE plot, where a productive and secure repudiation strategy is proposed to tackle the trait renouncement issue in the framework. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, both backward security forward securities. 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 server is not semi-trusted in some.

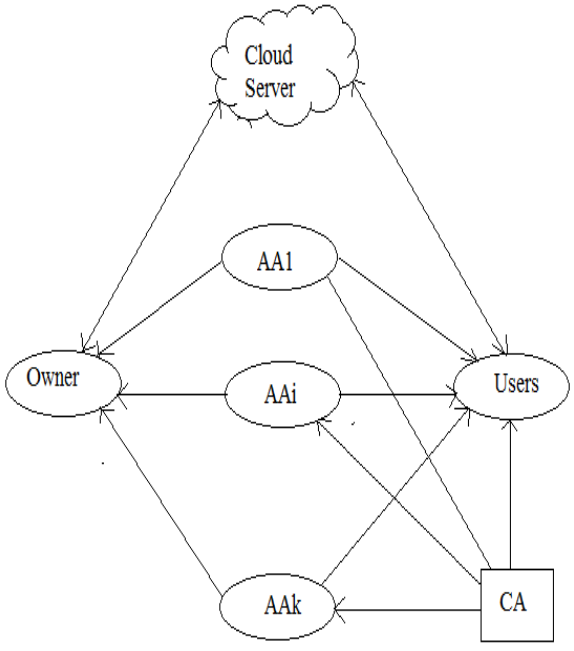

Figure 1: Proposed System Architecture

V ALGORITHM

Key Policy Attribute-Based Encryption (KP-ABE)

KP-ABE is an open key cryptography crude for one-to-numerous sharing data. In KP-ABE, data is conjoins with characteristics for everything about an open key part is characterized. The encoding or partners the arrangement of ascribes to the message by scrambling it with the relating open key segments. Every client is appointed an entrance structure which is typically characterized as an entrance tree over information properties, i.e., inside hubs of the entrance tree are limit entryways and leaf hubs are related with traits. User private key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE plan is composed of four algorithms which can be defined as follows:

The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

The setup algorithm chooses a group G of prime order p and a generator g.

Step 1: A trusted authority generates a tuple

G= [p, G,G_1,g € G, e] ← Gen(1^k)

Step 2: For each attribute a I where 1≤ i ≤ n, the authority generates random value

{$a_{i,t}$, € Z_p^*} 1 ≤ t ≤ n_i and compute {$T_{i,t} = g_{i,t}^a$} 1 ≤ t ≤ n_i

Step 3: Compute Y= $e(g,g)^{\propto}$ where α €Z_p^*}

Step 4: The public key PK consists of [Y, p, G,G_1, e,{{ $T_{i,t}$ = $g_{i,t}^a$}1 ≤ t ≤ n_i}1 ≤ i ≤ n]

The master key MK is

[α, {{$a_{i,t}$, € Z_p^*} 1 ≤ t ≤ n_i} } 1 ≤ i ≤ n]

Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-believable proxy is able to change a encoded text encrypted under Alice's public key into another cipher text that can be opened by Bob's secret key without seeing the underlying plaintext. More formally, a PRE scheme allows the proxy, given the proxy re-encryption key rk a↔b, to translate cipher texts under public key pk a into cipher texts under public key pk b and vice versa.

V EXPERIMENT RESULTS

In the result analysis of proposed system describe two method is like below,

Upload Time:-

In that measure the time taken for upload file of proposed system. In that gives the upload time with file

splitting. It is simple to search that our scheme incurs less upload and encrypt time than existing scheme.

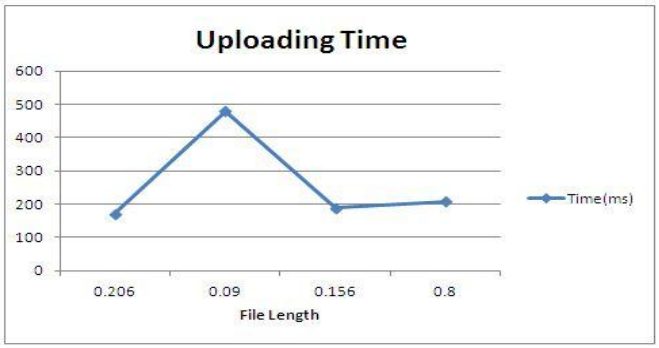

Figure 2: Graph for Upload Time

Table 1: Upload time for propose system

File Name	File Size	Time
aa.txt	206	171
abc.txt	90	480
abcd.txt	156	188
xyz.txt	80	209

Download Time:-

In that measure the time taken for download file of proposed system. In that gives the upload time with file merging and decrypt. It is simple to search that our scheme incurs less download and decrypt time than existing scheme.

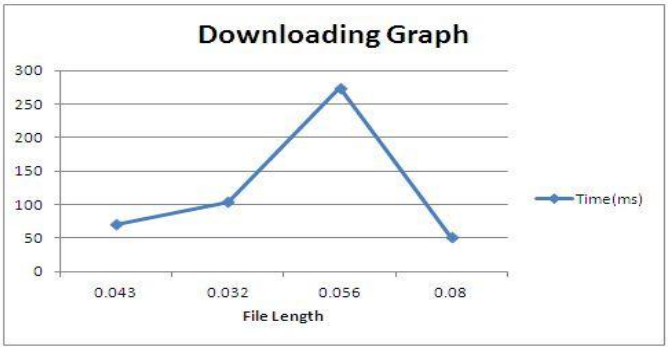

Figure 2: Graph for Download Time

Table 1: Download time for propose system

File Name	File Size	Time
aa.txt	43	71
abc.txt	32	104
abcd.txt	56	274
xyz.txt	80	51

VI CONCLUSIONS

In that, propose a revocable multi-authority CPABE plot that can bolster successful attribution disavowal. Then, develop an effective information get the control for cloud storage systems with multiple authors. Who we are has also shown that our scheme has been proven safe in the random oracle model. The CPABE can be denied multi-specialist is a promising method, which can be connected to any one remote stockpiling frameworks and online informal organizations, and so on.

REFERENCES

[1] Qi Li, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, Danwei Chen "Secure, efficient and revocable multi-authority access control system in cloud storage"

[2] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage".

[3] B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, 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] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91.

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

[6] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[9] J. Hur and D.K. Noh, ''Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[10] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.