Two factor protection for accessing data using efficient revocation in cloud storage system

[1]Anusha S,[2]Deepika N
Student, Assistant Professor
[1]Computer Science Department,
[1]New Horizon College Of Engineering,India

Abstract— cloud storage is similar to the model of the computer data storage in which the digital data is stored in logical pools. The cloud storage provider are responsible for keeping the data available and accessible to the authorized user and the physical environment protected and running. Attribute based encryption is one of the public key encryption in which the developed secret key of the user and the cipher text are depended upon attributes provided .In such system the decryption of the cipher text is only possible if the set of attributes of a user key matches the attributes of the cipher text.The user attributes may be issued by multiple attribute authorities because of this reason multiple authority cipher text policy attributed encryption is an upcoming cryptographic primitives for enforcing attribute based access control on the data. Now a days most of the multi authority attribute based system either insecure in attribute level revocation or lack of efficiency in communication over head and computation cost. In this paper we deal with this problem .We propose scheme which uses constant size cipher text and small computation cost. The scheme also allows the data owner to carry out the user level revocation.

IndexTerms— Attribute-based encryption, multi-authority cloud storage, two-factor data protection,attribute level revocation,user level revocation

I. INTRODUCTION

Cloud storage is one of the most essential offerings , which allows the facts proprietors to host their facts in the cloud and through cloud servers to offer the Data access get admission to the information clients. It is very difficult to maintain and operate a semi trusted cloud service provider(csp) that keep and operate the data in the storage pattern. To prevent the unauthorized people from accessing the sensitive data ,one of the fundamental solution is to encrypt the data and then upload that encrypted data on to a cloud. Some of the traditional technique identity based encryption(IBE) cannot be used because they decrease the flexibility and scalability of data access control because a single known user can only decrypt the encrypted data. In a attribute base encryption the user key and cipher text are a associated with a set of attributes. The decryption of data can only be done by providing set of attributes of the cipher text or the secret key satisfy the access policy. This makes attributes based encryption more efficient because it provides data confidentiality and fine grained access control in the could storage system.

II. LITERATURE SURVEY

1.fine grained two factor access control for web based cloud computing
In this paper attribute based access control mechanism is implemented with both the used secret key and a light weight security device and the advantage here is the used cannot access until he holds both the things. Attribute based control in the system also restricts to get right entry to the ones customer with the same set of attributes with preserving user privacy.

2.secure document sharing and access control on the cloud for corporate use
Now a days providing data confidentiality is a challenging against curious cloud service providers. Fine grained data access is the most trending topic public cloud. The drawbacks of CP-ABE and KP_ABE is overcome to make the system, attack free and two factor authentication is used in which first factor is traditional user id and password authentication and second factor is the mobile based authentication. In CP-ABE technique the access policy attribute will be stored in the secret key .if any user wants to update the attribute of a document the he as to delete or decrypt existing document and again encrypt it. to overcome this problem we will store all these policy attributes separately in a meta data file.

3.sign to login cloud service of biometric two factor authentication using mobile devices
The data protection is done based on identification and authentication of data. The most common method for authentication is by using password for recovering the data . for a most efficient authorization ,the authorized user must produce a unique identifier and password .the two factor authentication of the system is widely used in online banking ,social networks etc.currently they are using the biometric authentication technologies. One of the biometric authentication method is used is the handwriting dynamics of a signature or fixed password. Bayesian network are used for comparison of biometric images.

4.middle man:an efficient two factor authentication framework

With the increase in the cyber crime most of the business are implementing the two factor authentication mechanism to ensure the decrease in the risk of the malicious user. The user is allowed to login to a server by using an ios app that is developed to receive a dynamic one time password.

III. PROBLEM STATEMENT

The problem of revocation is a vital and cumbersome problem in systems based mainly on attributes. For the revocation of the attribute grade, any consumer who is revoked more effectively loses access privileges to the components, since some attributes are deleted. That is, each consumer who has been revoked can, however, obtain the right of entry to the events provided that their remaining attributes comply with the right of entry to the policy.

IV. EXISTING SYSTEM

CP-ABE is a promising cryptographic mechanism for handling fine-grained access. Several CP-ABE schemes have been proposed that understand the manipulation of access to information for cloud storage structures with multiple authorities. To obtain the revocation functionality, the proposed schemes want comfortable communication channels to update the secret attribute keys for non-revoked clients. Backward security cannot be guaranteed in the active assault version. The reason is that any revoked person still recovers his ability to decipher some confidential facts as a non-revoked consumer when he intercepts the encryption text replacement keys added from the AA.

V.PROPOSED WORK

We suggest a fully attribute-based admission for the control scheme with element protection for cloud storage systems from multiple authorities. In our proposed scheme, any consumer can improve subcontracted records if and only if this person has enough secret keys to recognize the admission to coverage and the authorization key with respect to the subcontracted information. In addition, the proposed scheme enjoys the residences of regular length cipher text and small computation value. In addition to assisting in the revocation of the attribute grade, our proposed scheme allows the owner of the statistics to perform the revocation at the consumer stage.

VI.IMPLEMENTATION

The cloud manager will register by providing the username, password along with the attributes such as department, grade and year of experience. The registration is complete and the cloud manager service is started. now the cloud manager is termed as the authorized user and he tries to login into the cloud for accessing the services provided by cloud. The user tries to login by providing giving the registered username and password and the cloud manager ip address. After the successful login of the user now he can upload the file on to the cloud. For the asset file ,the rules are defined and this file is termed as the asset rule file. The asset file will be successfully uploaded on to the cloud. The cloud service provider we are using the Amazon aws console for storing all our data files. Under the aws console,s3 service is used for storing the asset file that we created. The bucket which used for storing the data is security breach .the amazon s3 cloud can accessed by providing the authorized username i.e; email id and associated password. The data is encrypted by the attributes provided which can be only decrypted by providing the same set of attributes for the file. Asset file access can be done by providing asset file name, if the permissions are not present for accessing the file then we cannot download the file. Asset rule updating is done and then the file is downloaded.

VII.CONCLUSION

In this paper, we propose a new data access control scheme for multi-authority cloud storage systems. Two-factor protection mechanism is used to enhances the confidentiality and security of outsourced data of the data owner. If a data user wants to recover the outsourced data, this user data owner or the authorised person is required to hold all required attribute secret keys with respect to the access policy of the data and authorization key with regard to the outsourced data so that no other unauthorised user can access the file. The proposed scheme provides the most efficient technique i.e; the user-level revocation for data owner in attribute-based data access control systems. difficult security analysis and experimental results indicate that proposed scheme is suitable to data access control for multi authority cloud storage systems.

VII.REFERENCES

1.fine grained two factor access control for web based cloud computing
2.secure document sharing and access control on the cloud for corporate use
3.sign to login cloud service of biometric two factor authentication using mobile devices
4.middle man:an efficient two factor authentication framework
5.Towards Formal Verification of Role-Based Access Control Policies