Enhanced Cipher text Policy Attribute based Data Access and Sharing in the Cloud system to enhance data security

Omkar Dicholkar[1], Prof. Varsha Bhosale [2]

[1]*M.Tech Scholar. Vidyalankar Instotute of Technology*

[2] *Vice Principal and Associate Professor of Vidyalankar Institute of Technology, Mumbai*

Abstract *Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. All the data stored on cloud will be managed and controlled by cloud service provider. Data owners and service providers are not in the same trusted domain in cloud computing. The service providers should not be a trusted they all are third parties. So there have been increasing the security and privacy concerns on the outsourced data. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data.*

So that the attribute-based encryption (ABE) have been proposed for access control for outsourced data in cloud computing with the complex access control policy.

In this paper, we have proposed hierarchical attribute-set-based encryption (HASBE) access control by extending cipher-text policy and attribute-set-based encryption (ASBE) with a hierarchical structure of users. HASBE provides Flexibility, scalability and fine-grained access control with efficient user revocation. So we are proposing HASBE scheme by creating a sub domain in to the user level Hierarchy that reduce the complexity of the hierarchy and also improve the system performance. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes.

Keywords — *Cloud Computing, Access control, Attributes, Encryption, Scalability, Flexibility*

I. INTRODUCTION

Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Cloud computing refers to the application and service that run on a distributed system using virtualized resources by common internet protocol and networking standard.

Different service-oriented cloud models are utlilized in many commercial cloud computing systems such as Amazon cloud uses the Amazon's S3 which based on Infrastrucutre as service (IaaS) systems, the Google implements the Google App Engine which is based on Platform as serviced (PaaS) systems, and Sales force develops the Customer Relation Management (CRM) System be owned by SaaS systems.

All the data stored on cloud will be managed and controlled by cloud service provider. The data owners and service providers are not in the same trusted domain. All the service provider are third parties in cloud. Therefore increasing the security and privacy are concern and demand in cloud. For protecting the confidentiality of the stored data in cloud computing environment attribute based encryption (ABE) access control models are defined, which prevents cloud service provider(CSP) and other unauthorized users in accessing the data. Cloud owner will store encrypted data on cloud and will share private, pubic keys only with the authorized data consumer [4].

The major issue in cloud computing is the data owners and data consumers are not available always online. Complexity of key management has to be handled as it degrades the performance of cloud. Traditional ABE techniques are not flexible and scalable in terms on user sets and key management.

We considered set based encryption access control model HASBE (Hierarchical Attribute Set Based Encryption) to achieve flexibility and scalability of user sets and key management [15].

II. LITERATURE SURVEY

Sahai and Waters proposed an attribute-based encryption (ABE) scheme in 2005.The ABE scheme used an user's identity as attributes, and a set of attributes were used to encrypt and decrypt data.

In 2006, Goyal et al. proposed an key- policy attribute-based encryption (KP-ABE) scheme. The KP-ABE scheme can achieve fine- grained access control and more flexibility to control users than ABE scheme.

J.Benaloh, M.Chase, E. Horvitz,and K.Lauter[8]: This paper allows to prevent the untrusted servers from accessing sensitive data, traditional methods usually encrypt the data and decrypt data based on valid keys. Then, the data access control becomes the matter of key distribution. These methods require complicated key management schemes and the data owners have to stay online all the time to deliver the keys to new user in the system. Moreover, these methods incur high storage overhead on the server, because the server should store multiple encrypted copies of the same data for users with different keys.

S. Yu, C. Wang, K. Ren, and W. Lou [11]: These schemes require a trusted authority to manage all the attributes in the system and issue secret keys to users. Since the authority can decrypt all the encrypted data, it becomes a vulnerable security point and the performance bottleneck of the system.

Bethencourt et al. proposed a cipher text-policy attribute based (CP-ABE) scheme in the same year, and the CP- ABE scheme built the access policy into the encrypted data; a set of attributes is in an user's key. Ciphertext - Policy Attribute-based Encryption (CP-ABE) [4], [5] 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 and does not require the data owner to distribute keys.

However, since the data is outsourced to the cloud, the CP-ABE scheme should also provide the following properties

- **High performance:** In the cloud-computing environment, users may access data anytime and anywhere using any device. When a user wants to access data using a thin client with limited bandwidth, CPU, and memory capabilities, the CP-ABE scheme should be of high performance.
    - **Full delegation:**In a large-scale enterprise with many employees, each employee needs to request secret keys from the attribute authority (AA), when he joins the enterprise. If all these employees require their secret keys from one AA, there will be a performance bottleneck on the AA. CPABE scheme doesn't support full delegation which can embody the hierarchical structure in the enterprises.
    - **Scalable revocation:** In the case of a large-scale enterprise with a high turnover rate, a scalable revocation scheme is a must. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. CPABE scheme lacks in full revocation.

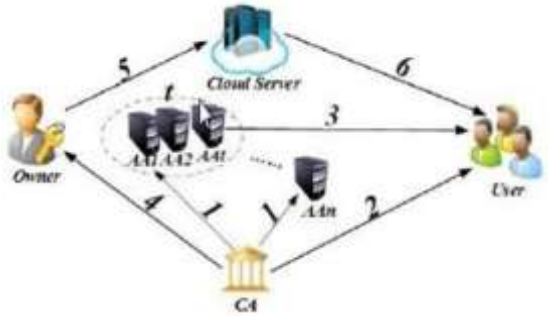
Based on the above-mentioned analysis, it is needed to propose a secure data-sharing scheme, which simultaneously achieves high performance, full delegation, and scalable revocation. Although some multi-authority CP-ABE schemes [5]–[6] have been proposed for data encryption, they cannot be directly applied to data access control for multi-authority cloud storage systems

III. PROBLEM STATEMENT

Various layouts based on attribute based-encryption are proposed to secure the cloud storage, but most of the target on the data content privacy and the access control, while less attention given to the privilege control and the identity privacy. Data sharing in the cloud is very feeble to cyber-attacks since data stored on cloud servers, and multiple users access data from unknown servers, resulting in Data security and privacy as critical issues for remote data storage. This uncertainty of Data Privacy and User Integrity is the foundation of the study.

IV. EXISTING METHODOLOGY

The project structure of Threshold Multi-Access Control System (TMACS) shown in Figure 1.



In TMACS, Attribute authority (AA's) should first register the Certificate authority (CA) to pick up the corresponding identity and authentication (help, aid. cert).

At that point Attribute authority (AA) will be engaged with the development of the framework, helping Certificate authority (CA) to complete the foundation of framework parameters.

Certificate authority (CA) acknowledges users' registration and issues the declaration (uid, uid.cert) to each legitimate user.
With the authentication, the user can contract with any t Attribute authority (AA) s one-by-one to pick up his/her secret key (SK). Owners who need share their data in the cloud can gain the public key (PK) from CA.

At that point, the owner can encrypt his/her data under predefined access policy and transfer the ciphertext (CT) to the cloud server. Users can uninhibitedly download the ciphertexts (CT) that he/she occupied with from the cloud server.

Nonetheless, he/she can't decrypt the ciphertext (CT)

unless his/her attributes.

So, according to chase schema, the owner will hold the master key and will decrypt all the files. For e.g., In a Medical Organization, if the Doctor is the having the master key he will be able to decrypt all the confidential files of all the patients, including the ones whom he is not authorized to view too.

V. PROBLEM SOLUTION

But with this new proposed scheme, this drawback is overcome by following an access structure which will decide the policy is defining who should be authorized to access that data or file.

We propose hierarchical attribute-set-based encryption (HASBE) by extending cipher-text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users as to achieve scalable, flexible and fine- grained access control. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes.

The Criteria of an Hierarchical Attribute based Encryption Scheme

Data confidentiality:

Before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud cannot know the information about the encrypted data.

Fine- grained access control:

In the same group, the system provides the different access right to individual user. The users are on the same group, but each user can be granted the different access right to access data. Even if users in the same group, users access rights are not the same.

Scalability:

When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system.

Flexibility:

Flexibility of the cloud allows companies to adjust to any problems that may occur during day-to-day operations. It also allows to use extra resources at peak times, to satisfy consumer demands

Collusion Resistance:

The dishonest users cannot combine their attributes to decrypt the encrypted data. Collusion resistance is one of the important security property required in the ABE systems. If multiple users collude, they may be able to decrypt a ciphertext by combing their attributes even if each of the user's cannot decrypt the ciphertext alone.

User Revocation:

Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more and it can be achieved following ways:

1. Forward security: Forward Security is achieved when any new user is joined. If the new user has sufficient attributes new keys will be generated and provided to the new users. Hence the new user can access previously published data also.

2. Backward Security: When any attribute is revoked then user will be automatically removed from the list of that authority and hence he will not get the new key. When the user does not have the attribute and the newly generated key he cannot access the data. Hence backward security is achieved.

VI. OUR CONSTRUCTION

The proposed scheme is implemented on the college management system. College provides various courses like Engineering graduation, Diploma, post graduation etc under the wings. We had considered courses as domains. College will be trusted authority. Data owner and Data consumer can be principle, HOD, teaching stff, non teaching staff and student etc.

New scheme:

Trusted Authority:

Trusted Authority (TA) will login into the system and stays always online. In our system College act as a trusted authority. It can create and manage domain authority.

Domain Authority:

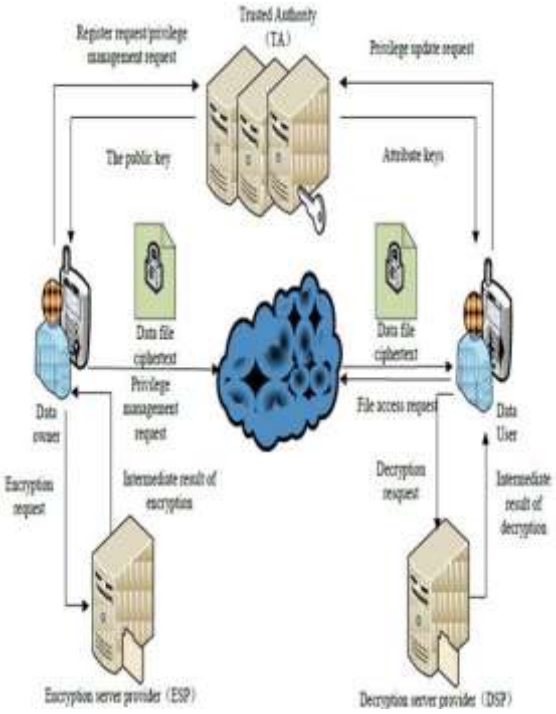
Domain Authority (DA) is created and authorized by TA. DA can create and manage users like Data Owner (DO) and Data Consumer (DC). It is responsible to create Domains. Domains authorities will be diploma, engineering graduation and post graduation etc. DA also can change the domain. Users can move to the other set in same domain or different domain with the authorization of domain authority.

Data owner and consumer:
DO and DC can register them and are authorized by DA. DO will share their files on the cloud in encrypted form. For each uploading file DO define policy. DC can access the uploaded file when they satisfy the desire file policy. If there is no match

found DC cannot access the file.

System Architecture:

Trusted Authority will be always online. Trusted Authority will create and manage Domain authorities. DA is responsible for creating and managing domains and users. In our system the proposed scheme will considered the Engineering, diploma as domain etc. Each school has its own departments. User role, gender, age, department, designation etc will be user attributes. User sets are formed by grouping users with their attribute similarities. Data owner can upload files on cloud in encrypted form and consumer with access privileges can download encrypted files and decrypt file by using keys shared by data owner.



File upload/download:

Only Data owners can upload the file and can set policies. Policy will be different for each file. Policy will be created using attributes of the users. Attributes can be role, gender, age, department, location etc.In our scheme we had used schools, Roles, and age for creating policies. Attributes are combined by using AND, OR and NOT logic. If data consumer will fulfill the data owner defined policy he/she can download and decrypt the file.

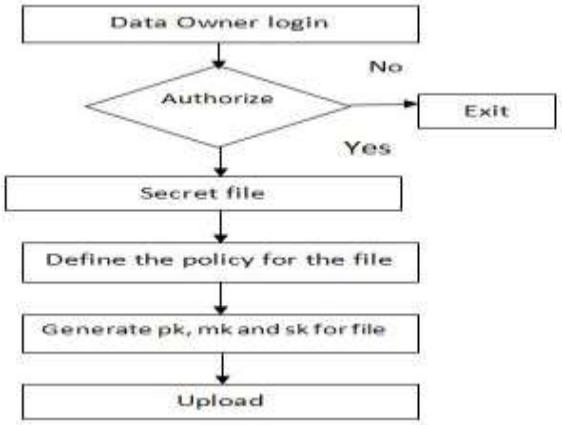


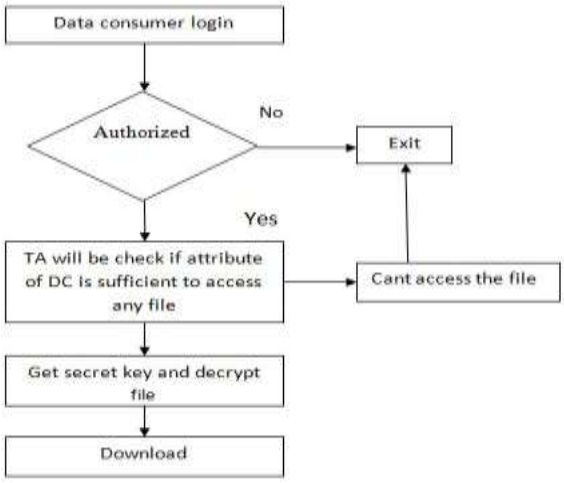
Figure 1:File uploading system

Key Generation:

In our proposed scheme to provide enhanced security we use 3 keys say Private, Public and Master key. Public key is available for every user. Private and public key are used to decrypt the data file and Master key allows authorized user to access authorized data files. Public key will be generated with username. Private Key is the result of operation between file attributes of user. Master key will be generated using public key and private key.

Encryption/Decryption

In our system required encryption and Decryption is performed by using Blowfish Algorithm



VII. ANALYSIS

We analyzed the performance of each operation of enhanced scheme as below We are now ready to describe the main operations of Proposed scheme: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

System Setup:
The trusted authority calls the algorithm to create system public parameters PK and master key MK0.PK will be made public to other parties and MK0 will be kept secret.

Top-Level Domain Authority Grant:
The trusted authority will first verify whether it is a valid domain authority. If so, the trusted authority calls to Create DA (PK, MK0, A) generate the master key for DAi. After getting the master key, DAi can authorize the next level domain authorities or users in its domain.

New Domain Authority/User Grant:
When a new user, denoted as u , or a new subordinate domain authority, denoted as DAi+1 , wants to join the system, the administrating domain authority, denoted as DAi , will first verify whether the new entity is valid. If true, DAi assigns the new entity a key structure A corresponding to its role and a unique ID.

New File Creation:
To protect data stored on the cloud, a data owner first encrypts data files and then stores the encrypted data files on the cloud. Each file is encrypted with a symmetric data encryption key DEK, which is in turn encrypted with HASBE. Finally, the encrypted data file is stored on the cloud.

File Access:
When a user sends request for data files stored on the cloud, the cloud sends the corresponding cipher texts to the user. The user decrypts them by first calling Decrypt (CT, SKu) to obtain DEK and then decrypt data files using DEK

Comparisons between Different Techniques :

No.	Technique	Algorithm	Scalability	Efficiency	Security
1	ABE	DES	HIGH	LOW	LOW
2	CPABE	DES	LOW	HIGH	LOW
3	KPABE	DES	LOW	HIGH	LOW
4	IBE	AES	LOW	LOW	HIGH
5	MA-CPABE	AES	HIGH	HIGH	LOW
6	PROPOSED SYSTEM	RSA	HIGH	HIGH	HIGH

VIII. CONCLUSION

In this paper, we had explored HASBE and introduced an enhanced HASBE access control model, which is highly Scalable and flexible in terms of user set management .We had proved that, the complexity in HASBE can be reduced by increasing the number of domains with respective to the number of users and their requirements. In future we want to extend our scheme for efficiently handling compoundattributes.

Reference

[1] E.Angel Anna Prathiba and B.Saravanan" HASBE for Access ControlbySeparateEncryption/DecryptioninCloudComputing" International Journal of Emerging Trends in Electrical andElectronics(IJETEE)Vol.2,Issue.2,April-2013.

[2] Sanchal Ramteke, Purva modi, Apurva Raghojiwar, Vijaya Karad, Prof.P.O. Kale "HASBE-A Hierarchical Attribute-Based Solutionfor Flexible and Scalable Access Control in Cloud Computing" International Journal of Scientific and Research Publications, Volume4,Issue1,January20144ISSN2250-3153.

[3] SultanUllah,ZhengXuefengandZhouFeng"TCLOUD:A MultiFactor Access Control Framework for Cloud Computing" International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013

[4] Rajanikanth aluvalu, lakshmi Muddana," A Survey on Access Control Models in Cloud Computing"-in Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_7.

[5] Sonam Chugh, Sateesh Kumar Peddoju " Access Control Based Data Security in Cloud Computing" International Journal of EngineeringResearchandApplications(IJERA)ISSN:2248-9622 www.ijera.comVol.2,Issue3,May-Jun2012,pp.2589-2593.

[6] Bibin K Onankunju "Access Control in Cloud Computing" International Journal of Scientific and ResearchPublications,Volume 3, Issue 9, September 2013 1 ISSN 2250-3153.

[7] A.Vishnukumar, G.Muruga Boopathi, S.Sabareessh"

Scalable Access Control in Cloud Computing Using Hierarchical Attribute Set Based Encryption (HASBE) " International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378,Volume-1, Issue-4, February 2013.

[8] N.krishnaL.Bhavani"HASBE:AHierarchicalAttributeSetBased Encryption For Flexible,Scalable And Fine Grained Access Control In Cloud Computing" International Journal of Computer &OrganizationTrends–Volume3Issue9–Oct2013.

[9] S. Gokuldev, S.Leelavathi " HASBE: A Hierarchical Attribute- Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering Science and Innovative Technology(IJESIT)Volume2,Issue3,May2013.

[10] Guojun Wang, Qin Liu, Jie Wu" Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services".

[11] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2,APRIL 2012

[12] Md.Akram Ali, Ch.Pravallika, P.V.S. Srinivas " Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 5, September 2013

[13] S.Dhivya bharathi, S. Sathyalakshmi" A Novel Method of HASBE withImprovedEfficiencyandDelegationMechanisminCloud"

[14] D. Hephzi Rachel, S. Prathiba" An Enhanced HASBE for Cloud Computing Environment" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 4, April 2013,pg.396–401.

[15] Punithasurya K, Jeba Priya S "Analysis of Different Access Control Mechanism in Cloud" International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.2, September2012.

[16] Jawahar Thakur , Nagesh Kumar" DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering(IJEATE)- (ISSN 2250-2459,Volume1,Issue2,December2011.