ISSN 2277 – 5528
Impact Factor- 3.145

INTERNATIONALJOURNALOFENGINEERING SCIENCES&MANAGEMENT

ATTRIBUTE BASED DECENTRALIZED ACCESS CONTROL ON CLOUD STORAGE

Prof. S.B.Tambe[*1], Prof. N.B.Kadu[2], Nilesh Gholap[3], Anand Bora[4] and Manoj Tembhurne[5]
[*1,2] Asst. Professor, Pravara Rural Engineering College, Loni.
[3,4,5]UG Students, Pravara Rural Engineering College, Loni.

ABSTRACT

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Now-a-days as cloud is most widely used in mostly all fields so there is need of keeping data more secure & confidential which is outsourced on the cloud. As the cloud system is decentralized and distributed, any unauthorized user can access this data so to avoid this we need secure access control. In this system the access control is attribute based and ciphertext is used which is better scheme. This system provides hierarchical control structure to reduce burden of central authority. Computation cost of encryption and decryption is less and the size of ciphertext generated is constant. This proposed scheme is efficient, fine-grained and scalable and also increases performance of the system.

Keywords- *Cipher-text, attribute based access control, decentralized.*

I. INTRODUCTION

As security is essential in all the fields. To accomplish secure data transaction in cloud, suitable cryptography method is utilized. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Nowadays Cloud Computing has spread so widely that many of the organizations are getting into it rapidly. There are many benefits with cloud computing like reducing capital cost, improving flexibility, disaster recovery, etc. but there exists some unavoidable security problems. These problems need to be concentrated as it may create severe problems which may prevent further development.

The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) [4], and Software as a Service (SaaS).In Cloud Computing, users store their data files in cloud server, therefore it is very important to prevent unauthorized access to these resources. In traditional access control methods, it is generally assumed that data owners and the storage server are in the same secure domain and the server is fully trusted. However, in case of the cloud computing environment, cloud service providers may be attacked by malicious attackers due to which the vital private information of users for commercial interests may be leaked as the data owners commonly store decrypted data in cloud servers. Nowadays, Cloud Computing has attracted widespread attention and support in many fields. Cloud computing can provide several computing capabilities, reduce costs and capital expenditures and charge according to usage. Although there are many benefits, there exist many unavoidable security problems as well. To deal with these problems ABE(Attribute based Access Control) can be the suitable solution , as it is a new cryptographic primitive which provides a promising tool for addressing the problem of secure data sharing and decentralized access control[2] .

Attribute based decentralized access control is on access control paradigm which uses policies containing attributes to grant access to the users through those attributes. ABAC uses attributes as the building blocks to define decentralized access control rules and access requests. In an attribute-based access control system, any type of attribute such as resource attributes and user attributes are used to determine access. These attributes are compared to defined fixed value or even to other attribute, which turns it into a relation-based access control. Attributes come in the key-value pairs such as a "Role=Supervisor," which can be used to limit access to a certain feature of a system. In this case only users with designation of supervisor or higher can be given access to that feature or system. For example, "Permit managers to access financial data provided from finance department". This would allow users with the attributes of Role=Manager and Department=Finance to the access data with the attributes of Category=Financial. This leaves another types of users from even getting to the login page and preventing certain types of attacks like brute force, collusion attack and library attacks.

Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing's extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet-based data storage and management. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement.

II. RELATED WORD

Different access control for accessing the data have been proposed from last decades. These schemes like Discretionary, Mandatory, Role-Based Access Control. But these schemes had some limitation and drawbacks so it can't be used in recent cloud storage systems. Also these traditional access policy has inadequate flexibility and also expansion of these on large scale is more difficult. So there is need to strengthen it's adaptability. Their adaptability to dynamically change roles is simply not enough. The role of user changes dynamically in many applications. So to achieve dynamic change of role we need a new access control scheme. High security requirements need a new access control model as the traditional access control scheme doesn't support high level security. To achieve easy public key encryption deployment the concept of identity based encryption was proposed. A users public key is his/her identity. An encryptor can create a cipher text under the receiver's identity without asking for the receiver's public key beforehand. The first fully functional IB scheme was presented by Franklin and Boneh. Similarly to IBE, a number of identity based cryptographic primitives has been proposed.

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys [1].

Sahai and Water proposed a Fuzzy Identity Based Encryption Algorithm in 2005. The conception of attribute was introduced first and an identity was viewed as a set of attributes in 2006, goyal et al. extended this idea and introduced two variants: - 1) Key Policy and 2) Ciphertext Policy. In a Key policy system, decryption keys are associated with access policies, and cipher text is associated with set of attributes. A user can decrypt cipher text if and only if his set of attributes satisfies the access structure. In CP-ABE the situation is exactly reversed, a user's private key is associated with set of attributes and encrypted cipher text will specify an access policy over attributes. Various improved ABE algorithms have been introduced and schemes have been presented.

The scheme proposed in this paper is conceptually closer to the traditional access control model such as role based access control model (RBAC).The demerits of this scheme relates to the size of cipher text, and computation of encryption and decryption depends directly on the number of attributes. As there are large number of users in cloud computing environment means it is impractical to complete authorization and distributes secret keys using only single attribute authority. A hierarchical attribute based encryption scheme was proposed by Wang in 2011, to provide full delegation and high performance with fine grace access control. A new versatile crypto system referred to as cipher text policy hierarchical ABE with short cipher text was proposed by Deng.

III. MOTIVATION

Existing methods works on access control in cloud are centralized in nature. Except some all other schemes use ABE. The schemes use a symmetric key approach and does not support authentication. The most previous schemes do not support authentication as well. Much of the previous work takes a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, the expert emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world [20].

ISSN 2277 – 5528
Impact Factor- 3.145

IV. OBJECTIVE

1. Distributed access control of data stored in cloud so only authorized users with valid attributes can access them.
2. Authentication of users who store and modify their data on the cloud.
3. The identity of the user is protected from the cloud during authentication.
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. Revoked users cannot access data after they have been revoked.

V. PROPOSED SYSTEM

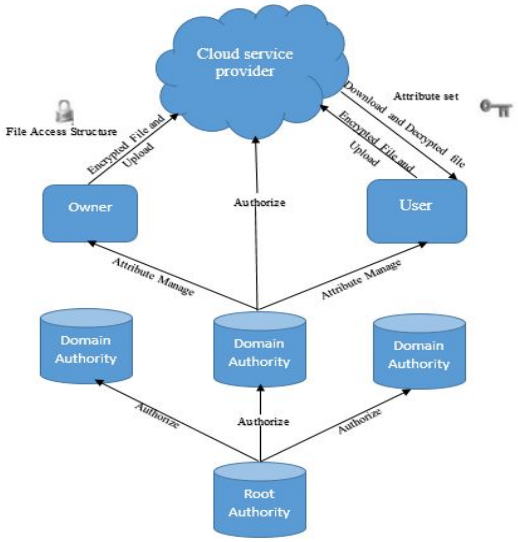
The structure of the system is tree-liked which is formed with root authority, top-level domain authorities and low-level domain authorities to realize attribute management and authority. The structure can divide the burden and risk of the authority of the single central attribute authority in a cloud computing environment. Model proposes a hierarchical CP-ABE access control scheme with constant-size ciphertext. In this size of ciphertext is fix and the computation of encryption and decryption at a constant value for improving the efficiency of the system. The data owner first encrypts the data file using a symmetric key DEK and then encrypts DEK by using the proposed scheme with a specific access control policy. The data owner uploads the final ciphertext and stores it

in the cloud servers. Whether a user can access and decrypt the data file depends on how to obtain the symmetric key, which is decided by the user's set of access attributes.

The system model consists of five types of modules:

1) Data owners
2) Users
3) A cloud service provider
4) Attribute Authorities:-

a) Root authority



b) Number of domain authorities.

Fig 1: Architecture of System

ISSN 2277 – 5528
Impact Factor- 3.145

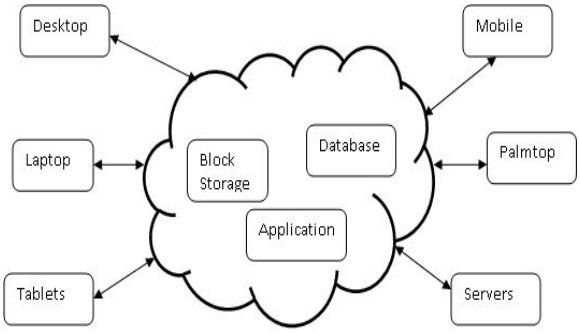


Fig 2: Data sharing with cloud storage.

The cloud service provider manages the cloud servers and provides a data storage service. Data owners encrypt their shared data files and outsource them to the cloud. The format of a stored file in a cloud environment, where ID is the identity number of a file, DEK is a symmetric key, and CT is the ciphertext of DEK by an ABE algorithm. Since the access structure is implied in ciphertext, only the user with corresponding attributes can decrypt the ciphertext. Unauthorized users cannot access the data file. Hence, we realize access control based on ABE with constant size ciphertext. To access the shared data files, users download an encrypted data file from the cloud and then decrypt the first part of the file CT based on the set of attributes to get the symmetric key. The access policies are expressed in terms of the set of attributes. The user obtains the data file by using the symmetric key to decrypt the ciphertext of the data file. The root authority has the top authority and is responsible for generating system parameters and authorizing top-level domain authorities. Each domain authority is responsible for managing domain authorities at the next level or the data owners/users in its domain. This inherited structure of attribute authority reduces the computation and burden of the authority of central attribute authority.

This scheme assumes users access the data files in a read-only way. We also assume that the cloud server provider is semi-trusted in the sense which abides by the agreement and faithfully carries out the operating request of a legal user. However it may try to pry into the private files of users or collude with malicious users to harvest file information stored in a cloud for its own benefit. Moreover, we assume communication channels between all parties of a system model are secured.

Setup: This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption: It takes a message, public key and set of attributes. It outputs a cipher text. Key

Generation: It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption: It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

Design the security model, assumes that the cloud server supplier is untrusted in the sense that it may collude with spiteful users (short for data owners/data consumers) to yield file comfortable accumulated in the cloud for benefit. In the hierarchical structure of the system users, each party is related with a public key and a private key, with the latter being reserved clandestinely by the party. The conditioned authority acts as the root of trust and allows the top-level domain authorities. A domain authority is trusted by its lesser domain authorities or users that it controls, but may try to get the private keys of users outside its domain. Users may trying to access data files either within or outside the scope of their access privileges, so malevolent users may collude with each other to get sensitive files beyond the privileges.

VI. MATHEMATICAL BACKGROUND

Bilinear pairings on elliptic curves. Let G be a cyclic group of prime order q generated by g. Let GT be a group of order q. We can define the map $e : G \times G \rightarrow GT$. The map satisfies the following properties:

1) e(aP, bQ) = e(P, Q) ab for all P, Q ∈ G and a, b ∈ Zq, Zq = {0, 1, 2,...,q − 1}.

2) Non-degenerate: e(g, g) ≠ 1. We use bilinear pairing on elliptic curves groups. We do not discuss the pairing functions which mainly use Weil and Tate pairings and computed using Miller's algorithm. The choice of curve is an important consideration, because it determine the complexity of pairing operations. A survey on pairing friendly curves can be found in [32]. PCB library (Pairing Based Cryptography) [30] is a C library which is built above GNU GMP (GNU Math Precision) library and contains functions to implement elliptic curves and pairing operations. The curves chosen are either MNT curves or supersingular curves. Considering the requirements, elliptic curve group of size 159, with an embedding degree 6 (typed curves of PBC) can be used. Pairing takes 14 ms on Intel Pentium D, 3.0 GHz CPU. Such operations are very suitable for a cloud computing environment [6]. Comparative study of different algorithm as shown in Table 1,2 [9].

Table 1: Comparative study of different algorithm

	DKG	JZSS	⋯	JZSS	DKG
Sk_1	$a_{1,0}$	$a_{1,1}$	⋯	$a_{1,m}$	$b_{1,m+1}$
Sk_2	$a_{2,0}$	$a_{2,1}$	⋯	$a_{2,m}$	$b_{2,m+1}$
⋯	⋯	⋯	⋯	⋯	⋯
Sk_n	$a_{n,0}$	$a_{n,1}$	⋯	$a_{n,m}$	$b_{n,m+1}$
Public keys	$g_1 = g^{a_0}$				$g_2 = g^{b_0}$

The secret keys Ski , i = 1, · · · , n for the respective *AAi* are ai,0, · · · , a(i),m, b(i),m+1. The respective public keys of two DKG protocols are g a0 , gb0 , which would be treated as a part of system public keys. According to the DKG protocol, we have a0 = Pt+1 l=1 akl ,0γkl , b0 = Pt+1 l=1 bkl ,m+1γkl P . We also have 0 = t+1 l=1 akl ,jγkl , j = 1, 2, · · · , m according to the JZSS protocol. 5 – (b) Each authority AAk, k = 1, · · · , n also needs to randomly choose another set of secret keys tk,1, · · · , tk,nk from Zq, each of which corresponds to the j-th attribute mastered by the authority AAk in the universe U. The corresponding public keys are Tk,1 = g tk,1 , · · · , Tk,nk = g tk,nk . – (c) the secret key SKk for each authority AAk, k = 1, · · · , n are ak,0, ak,1, ak,2, · · · , ak,m, bk,m+1, tk,1, · · · , tk,nk.

	DKG	JZSS	⋯	JZSS	DKG
Sk_1	$a_{1,0}$	$a_{1,1}$	⋯	$a_{1,m}$	$b_{1,m+1}$
Sk_2	$a_{2,0}$	$a_{2,1}$	⋯	$a_{2,m}$	$b_{2,m+1}$
⋯	⋯	⋯	⋯	⋯	⋯
Sk_n	$a_{n,0}$	$a_{n,1}$	⋯	$a_{n,m}$	$b_{n,m+1}$
Public keys	$g_1 = g^{a_0}$				$g_2 = g^{b_0}$

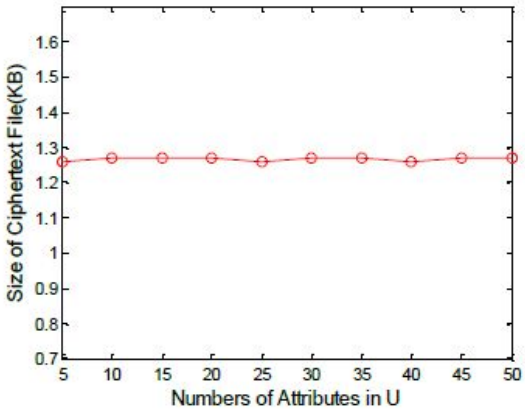
Table 2: Comparative study of different Scheme

Scheme	Approach
Secure and efficient access to outsoursed data	Centralised
Effective Data Access Control for Multiauthority Attributebased encryption	Decentralised
Realising Fine Grained and access control to outersoursed data with attributebase cryptosystem	Centralised
Proposed System	Decentralised

Performance Analysis

ISSN 2277 – 5528
Impact Factor- 3.145

In this, we analyse the performance of proposed system by using graphical representation. As previously mentioned, file's ID, cipher text of Decryption Key (DEK) and cipher text together stored in cloud. But here size of ciphertext is constant, it doesn't depends upon number of attributes as shown in following fig.



Simulating configuration is Windows with core of minimum 2.00 GHz, 20GB Hard Disk and 256 MB of RAM.

VII. CONCLUSION

Attribute-based access control provide data confidentiality. This system solves the drawbacks of role-based access control by replacing attributes instead of roles. We use constant size ciphertext instead of depending linearly on no. of attributes which helps to improve efficiency and performance. This shows our scheme has good adaptability and scalability in cloud computing. Our scheme can maintain the size of ciphertext and the computation of encryption and decryption at a constant value. Therefore, the scheme can improve the efficiency of the system.

VIII. FUTURE SCOPE

The above system gives information about secure transfer of data files i.e., text files between different nodes plays a vital role in cloud computing. As we know cloud computing is vast concept. So there are various futures concepts we can use in this system such as:-

1) Secure transfer of files such as pdf, images, and mp3 and video files.

2) In further research, we focus on increasing set of attributes for providing high security.

3) We will try to make system more simple, efficient, scalable and portable.

REFERENCES

1. *Jianwei Chen and Huadong Ma, "Privacy-Preserving Decentralized Access Control for Cloud Storage Systems" in 2014 IEEE International Conference on cloud computing.*
2. *Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2/*
3. *Amazon Web Service (AWS). http://s3.amazonaws.com/*
4. *Z. Wan, J. Liu and R.H.Deng, "HASBE: A Hierarchical Attrib-ute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp: 743-754, Apr. 2012.*
5. *J. Shao, Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption",In-formation Sciences,vol.206,pp:83–95,2012.*
6. *S. Ruj, A. Nayak and I. Stojmenovic, "DACC: Distributed Ac-cessControl in Clouds," Proc. 10th Int'l Con. Trust, Security and Privacy in Computing and Communications (TrustCom),IEEE, pp: 91-98, Nov. 2011.*
7. *L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol",InformationSciences,vol.181,no.19,pp:4318–4329, 2011.*

8. *Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in Computer Security–ESORICS 2011. Springer, 2011,*pp. 278–297.
9. *H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.*
10. *S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scala-ble, and Fine-grained Data Access Control in Cloud Compu-ting," Proceedings –IEEE INFOCOM,pp:1-9, 2010.*
11. *Google App Engine (GAE). http://code.google.com/appengine/*
12. *Sagar B. Tambe, Prof. Shiv Sutar, Mr. Mahesh D. Nirmal," C/C++ Cloud Compiler Using MainFrame" (IJCTEE) Volume 3, Special Issue, March-April 2013, An ISO 9001: 2008 Certified Journal.*
13. *Sagar B. Tambe, Ravindra C. Thool, Vijaya R. Thool, "Power Consumption and Congestion Control of Rendezvous Node for Wireless Biosensor Network," Published in Springer Book Chapter, Book ID: 352823_1_En, Book ISBN: 978-981-10-0127-7, Chapter No: 67, (ICT4SD–2015) Conference Proceedings by Springer, 2015.*
14. *Sagar B. Tambe, Ravindra C. Thool, Vijaya R. Thool, "Cluster Based Wireless Mobile Healthcare System for Physiological Data Monitoring," Elsevier Conference on Information Security and Privacy, Nagpur, Available Online At www.Sciencedirect.com, Procedia Computer Science 78(2016) 40-47.*
15. *J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2007, pp. 321–334.*
16. *M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, 2007, pp. 515–534.*
17. *S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, 2012.*
18. *C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.*
19. *J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.*
20. *Avaliable Online http://www.ijcsit.com/docs/Volume%206/vol6issue03/ijcsit20150603101.pdf*