An Efficient File Hierarchy Attribute-Based Encryption Scheme using Bit Exchanging Method in Cloud Computing

Preethi. M
B.Sc Computer Science
M.O.P Vaishnav College for Women

Shri Soundarya C.V
B.Sc Computer Science
M.O.P Vaishnav College for Women

ABSTRACT
Cloud computing is one of the emerging technologies where resources are provided on pay as you go basis. It is an efficient solution for the fast storage and retrieval of data. It is more than simple internet. The main concepts of cloud computing are confidentiality, integrity, availability, authenticity and privacy. The main issues to be concerned about the growth of cloud are security and privacy. It is important to preserve the data, as well as, privacy of users. One of the factors to preserve data is access control. Access control provides privileges to users on their data and protects it from unauthorised users. Access control is widely used in the medical field in which the access to patient's record is granted only to the scheduler and the concerned doctor. In simpler words, access control is the prevention of unauthorised use of resource. Confidentiality and efficiency must be maintained when access control is given for the system resources. So a number of algorithms are introduced and are implemented in the access control methods. This paper deals with one of the access control mechanisms and the algorithm implemented in it.

General Terms
Cloud computing, storage, encryption, cipher text, decryption.

Keywords
Security, privacy, access control, cp-abe, bit exchange method.

1. INTRODUCTION
The composition of cloud consists of five essential characteristics, four deployment models and three service models. Some of the advantages of cloud are cost efficiency, unlimited storage, backup & recovery and ease access to information. Some of the key factors are security of the data, privacy protection, and reliability. Privacy protection is not more than a technical issue but it is more than of a policy and legal issue. Policies are required to be framed to conform to the legal framework protecting the privacy of individuals and organisations. In order to protect our data from the attacks, one of the security policies is access control that denies or grants access to the system. For achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. The Scope of this paper is to enhance the security of the cloud system by using cipher text keys with bit exchanging method for transferring files across various users more efficiently. This prevents illegitimate users from accessing cloud system.

2. REVIEW OF LITERATURE
[3] gives a basic introduction of cloud computing with its deployment models and service models; gives idea of how to frame privacy as a suitable policy. Cloud based computing architecture to preserve data and privacy of users local information is proposed and information about how the government intercepts with the user data and also tries to explain the parameters of privacy in cloud such as data confidentiality, privacy etc.[2]. [5] gives brief description about institutional and technological environment facing cloud which includes problems in vulnerability, nature of architecture etc. [6] analyses the challenges posed by cloud computing to mitigate the privacy risks in cloud and describes briefly the main privacy challenges of cloud. The Government, institutions and technologies faced many problems regarding the security in cloud[2][5]. Many privacy challenges are faced by the software engineers with cloud. Since lots of companies and organisations are adding cloud services to their databases, it is a key challenge for the software engineers to design the cloud services in such a way that it reduces privacy risks. [1] .Some scenarios of privacy threats are given and some techniques to preserve the privacy were proposed [1][3].

3. ACCESS CONTROL IN CLOUD
Privacy refers to confidentiality of information. Each user has rights to control their information. Since the users do not about the details of where their data is physically located, it poses a major threat of privacy. The importance of preventing users from interfering each other on shared systems was realized in the early stages and corresponding access control methods were developed. It identifies unauthorized users. There are many access control models. These access control methods are effective in unchangeable distributed system.

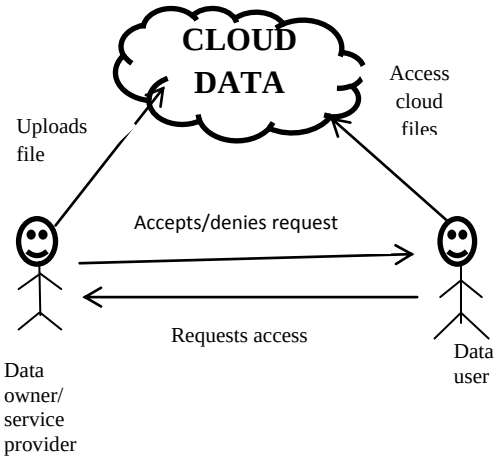

Figure 1: Access Control Function

Table 1-Access control methods in cloud

MAC	DAC	RBAC
Rule based policy	Identity based policy	Traditional based
Implemented for military purpose, financial institutions	Used in web applications and in many operating systems like UNIX	Implemented in medical field for database
Associated with two models	Represented using lists	Has three security principles

4. ROLE BASED ACCESS CONTROL (RBAC)

In RBAC, the decisions are based on the user responsibilities and roles within the cloud. The role for the user is assigned based on the least privilege concept – i.e. the role with the least amount of permissions or functionalities that is necessary for the job to be done. This method is implemented in three ways based on the design constraint. They are $RBAC_0$, $RBAC_1$, $RBAC_2$ and $RBAC_3$. $RBAC_0$ is based on the least privileges. $RBAC_1$ is based on the use of hierarchies and $RBAC_2$ is based on the hierarchy within the $RBAC_1$. $RBAC_3$ is based on the both constraints and hierarchy. At the same time, the users can execute multiple roles. In some cases the only one role can be assigned to one user and it recognize the same roles to other users jointly. It is proven that this method is more efficient than DAC and MAC. In this method also, the users are assigned roles based on the user identity. RBAC permissions are associated with roles and users are assigned to appropriate roles. Only the administrator has the authorisation to create roles and grant permission for those roles. Without RBAC, it is not possible to find what permissions assigned for which users. RBAC can be implemented based on the user-pull architecture and server-pull architecture. User-pull architecture means user pulls their roles from server and server-pull architecture means web server pulls their roles from the server. Comparing the advantages and disadvantages, RBAC is considered as the best model of the three identity based access controls methods. In order to reduce the difficulty in assigning roles to users, CP-ABE algorithm is implemented.

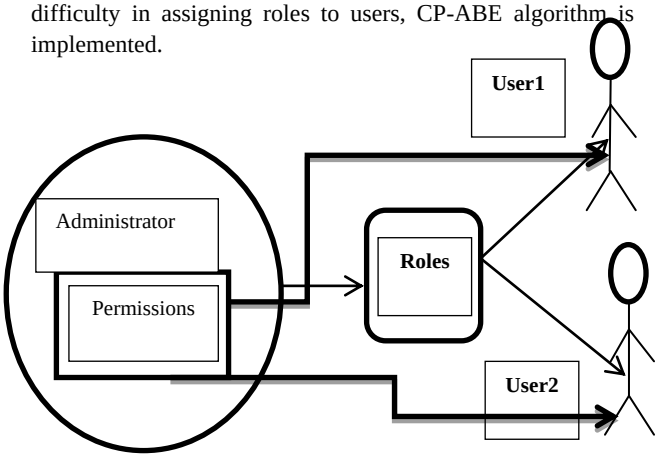

Figure 2: Role Based Access Control

5. CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION METHOD

Cloud computing is a new computing technology and has many security and privacy issues. The users should ensure that the confidentiality of data is maintained in a proper manner from outsiders and other competitors. During the encryption, the access policies may not be flexible enough as well. So a number of algorithms are introduced and are implemented in the access control methods. Some of the algorithms are Attribute-based Encryption (ABE), Attribute-Set-based Encryption (ASBE), Hierarchical Attribute-Set-based Encryption (HASBE), Key Policy Attribute-based Encryption (KP-ABE) and Cipher text Policy Attribute-based Encryption (CP-ABE). In distributed systems, the data can be accessed only if the users have a certain set of attributes. This can be achieved if the data is stored in a trusted server with specific constraints to it. But in this case, confidentiality will be lost. In the traditional mechanism, the user's public key is used to encrypt the data. The data is uploaded in the cloud after encrypting it with the user's public key. When required, the user can download the file by decrypting it using his generated secret key. Some of the problems faced in this method are that if the owner wants the data, he should get the public key from the user and the same data is encrypted with multiple public keys which results in wasting of storage space. Unlike the traditional method, in which the cipher text are encrypted to one particular user, ABE(Attribute based Encryption) has both cipher texts and users' decryption keys are associated with a set of attributes. The cipher text can be decrypted by the user only if there is a match between the decryption key and the cipher text. The ABE scheme has entities authority, sender and receiver. The function of the authority is to generate keys according to the attributes for the usage of encryption and decryption and the generation of keys are made of attributes. The primary advantage of ABE is key strength, which enable users to have a stronger encryption, than other encryption algorithms. Also ABE has some disadvantages in its practical uses which consumed large amounts of user's energy, may be

unrealistic, which hinder the applicability and popularity of ABE to secure data on cloud.

This scheme is categorised as key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE). Cipher-text policy attribute based encryption is one of the best methods to be implemented in the access methods due to its expressiveness.To solve the challenging problem of secure data sharing in cloud computing,Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology. Attributes that are attached to the secret keyplays an important role in cp-abe. The attributes change dynamically. They never remain static. CP-ABE algorithm is used to generate a public key to encrypt the data and a secret key which contains the attributes to decrypt the data and it restricts access to data for unknown users. By using this method, data can be protected in an encrypted format in even in an untrusted server. Cipher text is associated with a set of attributes. Only when the user satisfies the required attributes, he can decrypt it. In this method, access policy is used. Access policy is restricting the users from accessing the data. Two logical gates are engages in access policy. They are AND and OR gates. When the number of attributes goes on increasing, the security should be increased which results in need of larger decrypt keys. Using larger decrypt keys is not a good idea. So cp-abe is used. The access policy here is completely based on permission relationship where the relationship is between user attributes and resource attributes.

6. CP-ABE IN RBAC

When using the role based access control method, CP-ABE can be implemented in it for security purposes. The permissions which are assigned to a role during its creation should be verified; a single role may be given two or more permissions also. Clustering can be done among the users. Fine grained permission assignment should be created for role based access structure. The important functions are user assignment for role and Permission assignment for user. User assignment for role: This function is used to identify users for a particular role. The operations such as union, intersection, compliment, membership can be used. Permission assignment for user: This function is to assign permissions for the roles in an organisation. Any number of permissions can be granted based on the role. Let us consider an example. Let A be a medical university and B be a hospital. The hospital B wanted to increase their popularity. So it wants all the university professors to know about its research in a specialisation, say neurology. Now the hospital encrypts the data and gives access only to the professors who are in neurology department. To decrypt the data, the users should have the attributes. Here, the CP-ABE method is implemented. Any professor can access that data if and only if he has the attributes access to it. So the main concept here is that only when the users have the attributes to access the data, they can decrypt it. The user can never access the data if he misses the attribute.

Even though CP-ABE has many powerful mechanisms, it has its own drawbacks. Some of them are lack of proper encryption, duplicate or mischievous data into the file etc. The main disadvantages of CP-ABE are that it requires more efficiency and non-existence of attribute revocation mechanism. In order to increase the efficiency in encrypt the data, bit exchange method is implemented along with it.

7. BIT EXCHANGE METHOD

Algorithm: **Bit exchange method to increase the efficiency in encrypting the data**

Step 1*: Convert each byte of the secret data into 8 bit format.*
Step 2*: Apply right bit shift operation to the converted data.*
Step 3*: Split the resultant into two 4 bits value.*
Step 4*: Perform XOR operation for the two numbers.*
All the steps are repeated until all the secret data is encrypted. The main advantages of bit exchange method are High security, easy for implementation and produces lossless component.

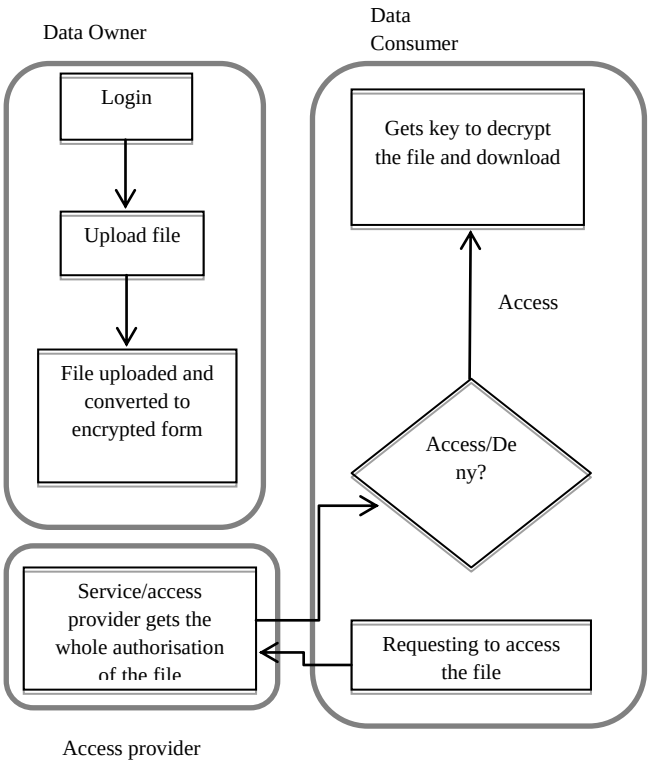

Figure 3: Bit exchange method applied with CP-ABE algorithm

Figure 3 reveals the encryption and decryption process employed in CP-ABE method. The owner, consumer and the access/service provider are given the attributes to access based on their roles. The provider has the entire privilege to provide access to the consumer. Any number of files can be uploaded by the data owner and the files can be of any size. So, the efficiency of encrypting the large files reduces gradually. In order to have a good efficiency, the bit exchange method is realised. The scheme is implemented over the integers. It can be applied to ensure data confidentiality and fine grained access control. The advantages of this system are it prevents

malicious users to access or delegate the deployed files and Fine grained access control over traditional systems.

In cloud computing, the data owner wants to share the data from the cloud in the sense owner encrypt the data then uploaded into the cloud storage. In order to avoid the unauthorised user to access the cloud data, all the sensitive data are encrypted. Users need to encrypt their data before being shared to avoid leakage of data. Access control is paramount as it is the first line of defence that prevents unauthorized access to the shared data.

The input design mainly focuses on controlling the amount of input required,error control, delay avoidance, avoiding extra steps and keeping the process simple. To provide security and ease of use with retaining the privacy, a good input method is designed.

A quality output is one, which meets the requirements of the end user and presents the information clearly. Efficient and intelligent output design is laid to improve the system's relationship to help user decision-making.

The analysis of the experiment shows that it has four phases .The setup, encryption, key-generation and finally the decryption. In the setup phase, the algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used for encryption by the users who sends message. MK is known only to the authority and used for secret key generation.

In the algorithm, the inputs for the encryption phase are public parameter PK, a message M, and an access structure T. The output of the encryption phase is cipher text CT.

In the third phase, algorithm takes as input a set of attributes associated with the user and the master secret key MK. If the attributes matches T,it outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T.

Decryption, which is the last phase takes as input the cipher text CT and a secret key SK for an attributes set. If the secret key SK satisfies the access structure associated with the cipher text CT, it returns the message M.

Cipher text-policy attribute based encryption (CP-ABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications. The shared files usually have hierarchical structure. That is, a group of files are divided into a number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved.

Since there are some privacy threats in protecting data in cloud, access control methods are used. One such method is Role based access control which has a major disadvantage in protecting the data and providing privileges for large number of roles. In order to overcome this problem, CP-ABE algorithm is implemented. To achieve greater efficiency in protecting the data, Bit Exchange Method is employed.

8. CONCLUSION

This paper gives a conclusion by stating that CP-ABE algorithm with Bit Exchange Method in Role Based Access Controls policy is better than the other existing policies. It is effective to secure the data that are highly confidential and provides greater efficiency. It does not mean that the other access control methods cannot be given lesser importance. Based on the importance of the data, the access control methods can be implemented for providing the security and privacy to the users. This method provides more security to data if CP-ABE algorithm is applied with Bit Exchange Method.The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, it can be applied to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

As the technology is improving day by day, there is a possibility to break the encrypted code in which the most efficient attack is still brute force. So there is another algorithm called the DES algorithm which also provides higher efficiency. DES is a 64 bit block cipher which means that it can encrypt data 64 bits at a time. The extended work of this paper is to find how much efficiency does DES algorithm gives and to compare both the implementation. As a result of the comparison, the method with the greater efficiency can be found and applied in the required real time applications, which will be greatly used to increase the reliability and safety of the data.

9. REFERENCES

[1] Siani Pearson, Taking Account of Privacy when Designing Cloud Computing Services,External Posting Date: March 6, 2009 [Fulltext] Approved for External Publication Internal Posting Date: March 6, 2009 [Fulltext]

[2] S. Rajarajeswari1 and K. Somasundaram2, Data Confidentiality and Privacy in Cloud Computing,Indian Journal of Science and Technology, Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/87040, January 2016,ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645

[3] J.M.Suri and B.K.Nath,Security and Privacy in Cloud Computing

[4] Tim Mather, SubraKumaraswamy, and ShahedLatif ,Cloud security and privacy

[5] NirKshetri,Privacy and security issues in Cloud Computing,PTC'11 Proceedings

[6] Privacy in Cloud Computing -ITU-T Technology Watch Report March 2012

[7] Yunchuan Sun, Junsheng Zhang, YongoingXiong, GuangyuZhu ,Data Security and Privacy

[8] [12] S.Aparna, Devi Dath,Preserving privacy of public clouds through access control mechanisms

[9] Abdul Raoufkhan,Access control in cloud computing environment , VOL. 7, NO. 5, MAY 2012 ISSN1819-6608 ARPN Journal of Engineering and Applied Sciences

[10] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc.,IEEE Transactions on Parallel and Distributed Systems, 2012

[11] JebaPriya, Punithasurya, 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, September 2012 – www.ijais.org

[12] NatarajanMeganathan,Review of access control models for cloud computing

[13] S. Yamada, N. Attrapadung and B. Santoso, "Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication," in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[14] BokefodeJayant. D ,ApteSulabha S, ModaniDattatray G, Ubaleswapnaja An Analysis of DAC MAC RBAC Access Control based Models for Security,International Journal of Computer Applications (0975 – 8887) Volume 104 – No.5, October 2014

[15] MadhuraMulimani, RashmiRachh, Analysis of Access Control Methods in Cloud Computing, Posted: 8 July 2016 doi:10.20944/preprints201607.0012.v1

[16] Ryan Ausanka-Crues,Methods for Access Control: Advances and Limitations

[17] ErlandJonsson ,ComputerSecurity,Department of Computer Science and Engineering Chalmers University of Technology Sweden

[18] Sadeghi,cubaleska,Operating system security,, Cubaleska @RUB, 2008 – 2009

[19] Computer Security ,CIS/CSE 643: (Syracuse University)

[20] Information systems control and Audit-Institute of CA in India- ISBN:978-81-8441-077-8,The Publication department on behalf of the institute of chartered accountants of India,ICAIBhawan

[21] Darwin v tomy, Dhanalakshmi.S, Dr.S.Karthik,Implementing HASBE Scheme for setting up access controls in out-sourced data Clouds ,ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 4, April 2013

[22] Shuriya.bPhd Scholar, Department of Computer Science and Engineering, RVS Technical campus Coimbatore,Role based Access Control using Cp-Abe Algorithm ,Volume : 4 | Issue : 7 | July 2014 | ISSN - 2249-555X

[23] Venkateshprasad.Kalluri1, D.Haritha2 ,CIPHER-Text Policy Attribute Based Access to Cloud,ISSN :0975-9646, Venkateshprasad.Kalluri et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2796-2799

[24] Vijaya Lakshmi Paruchuri1, N Lakshmipathi Anantha2, Vara Lakshmi Konagala1 and Debnath Bhattacharyya3,Ciphertext-Policy Attribute-Based Encryption for Access Control of Data in Cloud ,International Journal of Software Engineering and Its Applications Vol. 10, No. 8 (2016), pp. 13-22 http://dx.doi.org/10.14257/ijseia.2016.10.8.02

[25] Yan Zhu, Di Ma, Chang Jun Hu, DijiangHuang.How to Use Attribute-Based Encryption to Implement Role-based Access Control in the Cloud

[26] BalamuruganB,Extensive Survey on Usage of Attribute Based Encryption in Cloud, Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, august 2014

[27] XinfengYe,Privacy preserving and delegated access control for cloud applications

[28] J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption," in Proc. IEEE Transactions on information forensics and security, vol.8, NO.8, pp.1343-1354, 2013.