An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing

S. G. Game[1], Prof. P. B. Vikhe[2]
[1, 2] Department of Computer Engineering
[1, 2] PREC, Loni, Maharashtra.

Abstract- *Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption method to solve the issue of secure data sharing in cloud computing. The shared data files generally have the properties of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. In this paper, an effective file hierarchy attribute-based encryption method is proposed in cloud computing. The layered access structures are included into a single access structure, and then, the hierarchical files can be encrypted with the integrated access structure. The cipher text components similar to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption are maintained. Moreover, the proposed scheme is proved to be secure under the universal assumption. Experimental simulation shows that the proposed method is more effective in terms of encryption and decryption. With the number of the files increasing, the advantages of our method become more and more clear.*

Keywords- Cloud Computing, Data Sharing, File Hierarchy, Cipher text-Policy, Attribute-Based Encryption.

I. INTRODUCTION

With the increasing of network technology and mobile terminal, online data sharing has become a new pet, such as Facebook, Myspace, and Badoo. Meanwhile, cloud computing is one of the most capable application platforms to solve the unstable increasing of data sharing. In cloud computing, to keep data from leaking, users require to encrypt their data before being shared. Access control is controlling as it is the first line of security that avoid unauthorized access to the shared data. Recently, attribute-based encryption (ABE) has been interested much more attentions since it can save data privacy and gathers fine-grained, one-to-many, and non-interactive access control. Cipher text-policy attribute based encryption (CP-ABE) is one of appropriate method which has much more adjustability and is more applicable for generic applications.

In cloud computing, authority accepts the user enrolment and creates some parameters. Cloud service provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated cipher text to CSP. User downloads and decrypts the interested cipher text from CSP. 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-based encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved.

II. REVIEW OF LITERATURE

C..K. Chu, W.T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou[1],Cloud computing has emerged as a practical means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage, and backup capabilities, and many more IT functions in recent years. However, cloud computing presents a new set of challenges to tackle. What kind of cloud governance model and policies do we need? What legal languages do we need to include in the cloud service contracts? How can we protect sensitive data and applications in the cloud environment? How do we manage network and host access controls? How do we do security assessment and audit? How do we conduct intrusion detection and incident response? The key security issue in the cloud environment is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls may not be available or accessible by enterprise security teams. The development of contract language and service level agreements with cloud service providers becomes critical. Compliance and auditing concerns are compounded by access control limitations. Security auditing and assessment within cloud provider environments may also be affected. There are various delivery models of cloud computing ranging from software as a service and platform as a service, to infrastructure as a service and others. Each of these delivery models represents a separate set of security conditions to consider, especially when coupled with various cloud types including public, private, and hybrid. This chapter provides an overview of security issues within each of these models and in-depth discussions of fundamental

methodologies, best practices, practical approaches, and pragmatic techniques.

T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J.Liu[2], The semi-trusted servers in cloud environment may outsource the files of their clients to some low expensive servers to increase their profit. To some extent, such behavior may violate the wishes of cloud users and impair their legitimate rights and interests. In this paper, a probabilistic challenge-response scheme is proposed to prove that the clients files are available and stored in a specified cloud server. In order to resist the collusion of cloud servers, common cloud infrastructure with some reasonable limits, such as rational economic security model, semi-collusion security model and response time bound, are exploited. These limits guarantee that a malicious cloud server could not conduct a t-round communication in a finite time. We analyze the security and performance of the proposed scheme and demonstrate that our scheme provides strong incentives for economically rational cloud providers against re-outsourcing the clients data to some other cloud providers.

K. Liang, J. K. Liu, D. S. Wong, and W. Susilo[3], Identity based encryption (IBE) eliminates the necessity of having a costly certificate verification process. However, revocation remains as a daunting task in terms of cipher text update and key update phases as due to the lack of a certificate revocation list in this infrastructure. In this paper, we provide an affirmative solution to solve the efficiency problem incurred by revocation. We propose the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme that supports user revocation but also delegation of decryption rights. No matter a user is revoked or not, at the end of a given time period the cloud acting as a proxy will re-encrypt all cipher texts of the user under the current time period to the next time period. If the user is revoked in the forthcoming time period, he cannot decrypt the cipher texts by using the expired private key anymore. We state that this primitive is applicable to many practical network applications, such as subscription-based cloud storage services. Comparing to some naive solutions which require a private key generator (PKG) to interact with non-revoked users in each time period, the new scheme provides definite advantages in terms of Communication and computation efficiency. Our scheme only requires the PKG to publish a constant-size public string for each time period and meanwhile, the workload of cipher texts update is off-loaded to the cloud server. More importantly, the scheme can be proven secure in the standard model.

T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu[4],Identity based encryption (IBE) is useful for providing end to-end access control and data protection in many scenarios such as cloud applications and wireless sensor networks However, there are some practical threats for the data owner or the sensor, who encrypts raw data; and the data user or the control centre , who decrypts the cipher text and recovers the raw data. In this paper, we tackle the open problem of proposing a leakage resilience encryption model that can capture leakage from both the secret key owner (the data user or control centre) and the encrypt or (the data owner or sensor), in the auxiliary input model. Existing models only allow he leakage of the secret key and do not allow adversaries to query more leakage information after seeing the challenge cipher text of the security games. We solve this problem by defining the post challenge auxiliary input model in which the family of leakage functions must be defined before the adversary is given the public key. The post-challenge query will return the leakage of the encryption randomness used by the encrypt or. This model is able to capture a wider class of real-world attacks. To realize our model, we propose a generic transformation from the auxiliary input model to our new post-challenge auxiliary input model for both public key encryption (PKE) and IBE. Furthermore, we extend Canetti et al.s technique, that converts CPA-secure IBE to CCA-secure PKE, into the leakage-resilient setting.

III. SYSTEM ARCHITECTURE

A promising approach to access control in content sharing services is to empower users to enforce access controls on their data directly, rather than through a central administrator. However, this requires flexible and scalable cryptographic key management to support complex access control policies. A native access control solution is to assign one key for each user attribute, distribute the appropriate keys to users who have the corresponding attributes, and encrypt the media with the attribute keys repeatedly Another method is to classify users into different roles based on their attributes, assign role keys to users, and then encrypt the content using the role keys. However, this approach results in high complexity, i.e., the number of keys for each user and the number of cipher texts for one message are on the order of where is the number of all possible user attributes. Both of these solutions suffer from the rigid and inflexible definition of the underlying access control policies. A Remedy to this problem is employing Cipher text Policy Attribute-Based Encryption (CP-ABE). In CP-ABE, a Cipher text is embedded with an access control policy, or access policy for short, associated with user attributes. A recipient of the cipher text is able to decrypt the cipher text only if her attributes satisfy the access policy in the cipher text. CP-ABE can be viewed as a one-to-many public key encryption scheme and hence enables

a data owner to grant access to an unknown set of users. Nonetheless, existing CP-ABE schemes merely deliver one encrypted message per cipher text to all authorized users and are not optimal for efficient sharing of scalable media. In an Existing system solution is flexible, but it is vulnerable to collusion attack. The Existing method is to classify users into different roles based on their attributes, assign role keys to users, and then encrypt the content using the role keys. However, this approach results in high complexity. Existing CP-ABE schemes merely deliver one encrypted message per cipher text to all authorized users and are not optimal for efficient sharing of scalable media. To control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the users identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The present scheme is also secure against user collusion attacks due to use of attribute-based encryption. The experiments demonstrate that the present scheme is applicable on smartphone, especially when a cloud platform is available. To Present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery.

IV. SYSTEM ANALYSIS

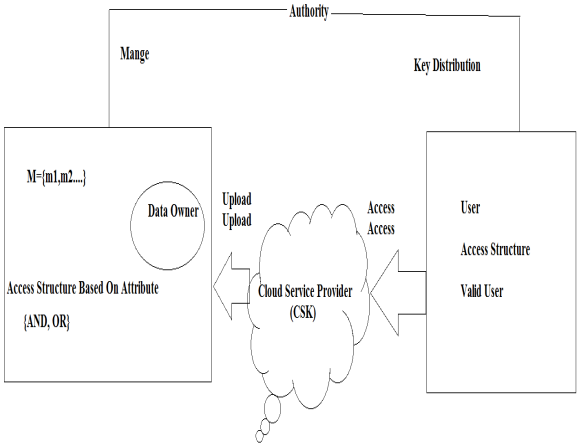

Figure 1. System Architecture

CSP : It is main site to handle number of cloud user. All Activation cloud user. All file encryption here, it is not readable. Encryption means conversion of plain text to cipher text. All files are in attribute based. It is convert to readable form when having respective key. Every key is changeable.

V. MATHEMATICAL MODEL

Set theory : Let S = I,P,R,O,K
Where,
S: Public integrity auditing system by using attribute.
I: Set of inputs.
P: Set of processes.
R: Rules or constraints.
K: Keyword
O: Set of outputs/Final output.
I = i1, i2,.....,in
Where,
i1,i2,...,in = Files shred by the users.
P=p1, p2, p3, p4, p5, p6, p7
Where,
p1: Key generation
(SK,PK,MSK)
p2: Generate commitment string
p3: Open
p4: Verify
p5: Update.
p6: Proof Update.
R = r1
Where,
r1: Unauthorized user should not be able to access files shared by users.
r2: Proper Attribute should be extracted.
Where,
O1:Valid user cloud access any file.

- Output :-

KeyGen :(P K, M SK, S). The operation inputs P K , M SK and a set of attributes S and creates a secret key SK .

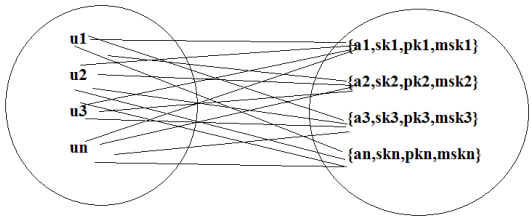

Figure 2.

Encrypt :(P K, ck, A). The operation inputs P K , ck = {ck1,..., ckk} and a hierarchical access tree

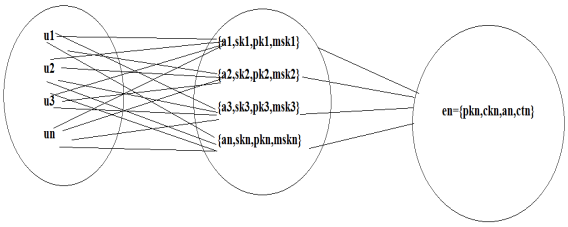

Figure 3.

Decrypt :(P K, CT, SK). The algorithm inputs P K , CT which includes an integrated access structure A, SK described by a set of attributes S. If the S matches part of A, some content keys cki(i ∈ [1, k]) can be decrypted. If it matches the whole A, all the content keys can be decrypted. Then, the corresponding files mi(i ∈ [1, k]) will be decrypted with the content keys by the symmetric decryption algorithm,

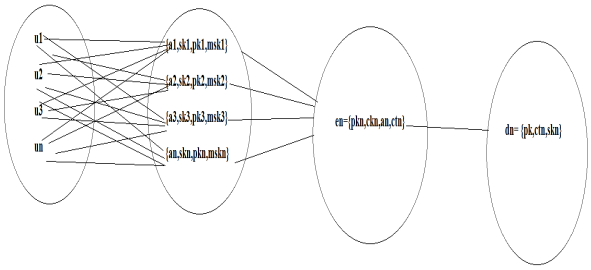

Figure 4.

VI. IMPLEMENTATION DETAILS

The FH-CP-ABE scheme consists of four operations: Setup, KeyGen, Encrypt and Decrypt. It is described as follows:

1) (PK, MSK) ←Setup(1κ). The probabilistic operation takes a security parameter κ as input and outputs public key PK and master secret key MSK.
2) (SK) ←KeyGen(PK, MSK, S). The operation inputs PK, MSK and a set of attributes S and creates a secret key SK.
3) (CT) ← Encrypt(PK, ck ,A). The operation inputs PK, ck = {ck1, . . . ,ckk } and a hierarchical access tree A .At last, it creates an integrated ciphertext of content keys CT.
4) (cki (i ∈ [1, k])) ← Decrypt(PK,CT, SK). The algorithm inputs PK, CT which includes an integrated access structure A, SK described by a set of attributes S. If the S matches part of A, some content keys cki (i ∈ [1, k]) can be decrypted. If it matches the whole A, all the content keys can be decrypted. Then, the corresponding files mi (i ∈ [1, k]) will be decrypted with the content keys by the symmetric decryption algorithm.

VII. RESULT AND DISCUSSION

Following fig.shows accuracy at the time of decryption of file.

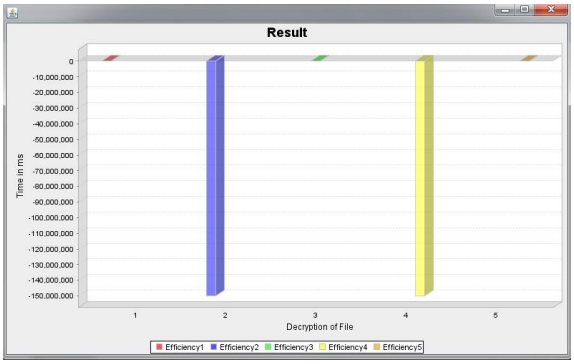

Figure 5. shows the accuracy of decryption of file

VIII. CONCLUSION

To Proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption is saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

IX. ACKNOWLEDGMENT

I dedicate all my works to my esteemed guide, Prof. P.B. Vikhe , whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to H.O.D. Computer Department who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this system.

REFERENCES

[1] C.-K. Chu, W.-T.Zhu, J. Han, J.-K. Liu, J. Xu, and J.

Zhou, Security concerns in popular cloud storage services, IEEE Pervasive Computing., vol. 12, no. 4, pp. 5057, Oct./Dec. 2013.

[2] T.Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, TIMER: Secure and reliable cloud storage against data re-outsourcing, in Proc. 10th Int.Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346358.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing, in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014,pp.257272.

[4] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks, in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014, pp. 130147.

[5] K. Liang et al., A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing, IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 16671680,Oct.2014

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, k-times attribute-based anonymous access control for cloud computing, IEEE Trans. Comput., vol. 64, no. 9, pp. 25952608, Sep. 2015.

[7] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, Fine-grained twofactor access control for Web-based cloud computing services, IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484497, Mar. 2016.

[8] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in Proc. 13th ACM Conf. Comput. Commun.Secur., Oct. 2006, pp. 8998.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, Efficient attribute-based encryption from R-LWE, Chin. J. Electron., vol. 23, no. 4, pp. 778782, Oct. 2014.