A Review of Efficient file Hierarchy Technique in Cloud Computing for Attribute Based Encryption

Mr.Tanveer Patel,Ranmalkar V.S.
M.E. Student Computer Engineering VACOE, Assistant Professor Computer Engineering VACOE

Abstract: Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing.The shared data files generally have the characteristic 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 efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access Structure. 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. Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous

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

I. INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control [6], [7] is paramount as it is the first line of defense that prevents unauthorized access to the shared data. With the burgeoning of network technology and mobile terminal,online data sharing has become a new “pet”, such as Facebook, MySpace, and Badoo. Meanwhile, cloud is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount that prevents unauthorized access to the shared data. Recently, attribute-based encryption (ABE) has been attracted much more attentions since it can keep data privacy and realize fine-grained ,one-to-many n,and non interactive access control. Ciphertext-policy attribute based encryption (CPABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications.

In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud ser-vice provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext 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 ciphertext and time cost of encryption could be saved.

II. LITRATURE ROCEDURE SURVEY

J. Bethencourt, Amit Sahai, Brent Waters [11],2007 A system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).

L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel [13,]2009 In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the ciphertext is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the access policy specified in the ciphertext. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed. a mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, we demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs). A mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation.

F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan [15,]2014 Lightweight devices, such as radio frequency identification tags, have a limited storage capacity, which has become a bottleneck form any applications, especially for security applications. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic tool, where the encryptor can decide the access structure that will be used to protect the sensitive data. However, current CP-ABE schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes. This drawback prevents the use of lightweight devices in practice as storage of the decryption keys of the CP-ABE for us ers. In this paper, we provide an affirmative answer to the above long standing issue, which will make the CP-ABE very practical. We propose a novel CP-ABE scheme with constant-size decryption keys independent of the number of attributes.

J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption[20], 2015 Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

III. ENCRYPTION TECHNIQUES

A. *Key Policy Based Encryption*

Submit your manuscript electronically for review.

Key-Policy based ABE establish a cryptosystem for fine-grained sharing of encrypted data. In this system, cipher texts are designated with set of attribute and private keys. Private keys are related with access structures that in turn specifies which type of cipher texts the key can decrypt. The main drawback is that the data owner is also a Trusted Authority (TA). If this scheme is applied to a PHR system with multiple data owners and users, it will not efficient because then each user would receive many keys from multiple owners.

B. *Attribute Based Encryption*

Attribute based encryption is the identity based encryption that takes attribute as input. Data is encrypted using a set of attributes, and then no. of users can properly decrypt it. Attribute-Based Encryption (ABE) provides fine-grained access control and also prevents against collusion. A drawback of ABE is use of a single trusted authority (TA) in the system. Single trusted authority (TA) encounters the some of the problems, it creates a load bottleneck, and have key escrow problem since the TA can access all the encrypted files. This opens privacy exposure.

C. *Cipher-text-Policy Attribute Based Encryption*

The Cipher-text is related with the access policy. Party which do the encryption determines the policy of data encryption, while the security key related with a set of attributes. CP-ABE access policy is described using AND, OR Boolean operators, so that it is easy to express the access policy. The drawback of this policy is Decryption keys only support user attributes which are organized logically asa single set, so for satisfying policies users can only use all possible combinations of attributes in a single set issued in their keys.

D. *Hierarchical Attribute-Base Encryption*

HABE is designed for achieving fine-grained access control in cloud storage services. It is a combination of HIBE and CP-ABE. In the HABE scheme, there are multiple keys with different usages. Drawback of HABE is compared with ABE, this scheme cannot support compound attributes efficiently and also does not support multiple value assignments.

IV. EXISTING SYSTEM

Cloud computing is a environment provided with services, storage web space and security where we can store, process data from anywhere and at any time. Data sharing means we can share data or information from one place to another place in secure manner. Today we can search file on cloud but it is not in attribute based. Cipher text-policy attribute-based encryption(CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic 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 base paper an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time cost of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. With the number of the files increasing, the advantages of our scheme become more and more clear.

Existing system, all the work of healthcare provider, doctor & patient details and hospital's details done by manually cannot to be monitored by the admin and cannot access the user security authorization. As to the security fact, one of the main issues is access control of patient's personal health information, namely it is only the authorized physicians that can recover the patients' personal health information during the data sharing in the m-healthcare cloud computing system. In practice, most patients knows the confidentiality and privacy of their personal health information as it make them in trouble for each kind of unauthorized collection and disclosure. So that, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with problems and solution also described.

A. *Disadvantage*

1.It is not providing much more security
2.Manually maintains the patients' details
3.Feedback cannot written by patient previously
4.It is some what complicated not straightforward .

B. *Survey Conclusion*

As we described in fundamentals there as existing systems but they have not focused primarily on attribute based encryption scheme. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. The proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. Attributebased encryption (ABE) has been attracted much more attentions since it can keep data privacy and realize fine-grained, one-to-many, and non-interactive access control. Ciphertextpolicy attribute based encryption (CP-ABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications. Our system gives better results.

V. PROPOSED SYSTEM

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 ciphertext 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. Cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users to encrypt their data before shared.

.

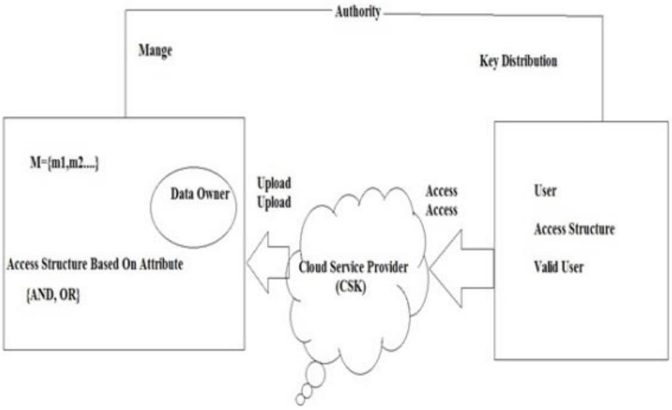

Fig. System Architecture

In this system, an efficient encryption scheme based on layered model of the access structure in proposed in cloud computing, this is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control. The contributions of our scheme are three aspects:

Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.

Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attack(CPA) under the Decisional Bilinear DiffieHellman(DBDH) assumption.

Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

It should be noticed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center.

A. System Features(Modules)

The fig shows the implementation of the proposed system , the implementation is divided into different modules as follows:

1.Data Owner:

The Data Owner first Register with cloud server and login (username must be unique).Send request to Key transmission to generate ABE Key on the user name. Browse file and request Private Key to encrypt the data, Upload data to service provider. Verify the data from the cloud.

2.Public Key Generator (Key Transmission):

Receive request from the users to generate the Key, Store all keys based on the user names. Check the username and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revoke the user after updating the private key for the corresponding file based on the user).

3.End User:

1.In this module receiver first has to Register and login, Request secret key, Request available files in the cloud and receive files.
2.Every key come respective unique id.

4.Data Sharing:

1.Data Share group wise as per authorized account.
2.Every File key changeable

B. Proposed Algorithm

The AES and DES algorithm are used for encryption and decryption**.**

Encryption:

Encryption means convert plain text into cipher text. AES algorithm for encryptions as follows**.**

Input:

Encryption object as follows,

1. Encrytedstring ->NULL
2. Secret key->key

Literal type as follows,

Byte plaintext, encrypted Text

Output:

```
1. START
2. Init -> (ENCRYPT MODE, key)
3. Plaintext --> UNICODE FORMAT
4. EncryptedText - do Final (plaintext)
5. EncryptedString -> Base64.encodeBase64 (encrypted Text)
6. Return encrypted String.
```

Decryption:

Decryptions are used to decrypt the message. Convert the cipher text into plain text .

Input:

Decryption object as follows,

Decrypted String -> NULL

Secret Key -> key

Literal type as follows,

Byte cipher text, decrypted Text

Output:

```
1. START
2. Init - (DECRYPT MODE, key)
3. Ciphertext - UNICODE FORMAT
4. DecryptedText - do Final(ciphertext)
```

5. DecryptedString - Base64.encodeBase64 (decrypted Text)

6. Return decrypted String.

C. Features of Proposed System

1.We are helping to save or protect the data or information which are essential to everyone who is using data sharing in any field.
2.Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing.
3.With the number of files increasing, the advantages of our scheme become more and more conspicuous.
4.System works better and better after use because we are using cipher text policy attribute based encryption technology in cloud computing.
5.User interface is user friendly so that anybody can use it easily

D. Benefits of System

1.Data sharing can be done in secure manner because of cipher text policy.
2.Data can be access in hierarchical manner.
3.Time is decreases for searching the files because Access layer structure is used.
4.File structure can be managed properly.
5.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.

E. Limitations

Laptops/computers with better specifications are needed to support our system.

F. Performance Measurement

Discounted cumulative gain (DCG) is a measure of Efficiency Quality of Attribute based Anonymous User. In information retrieval, it is often used to measure effectiveness of algorithms or related applications. Using a graded relevance scale of documents in a search engine result set, DCG measures the usefulness, or gain, of a document based on its position in the result list. The gain is accumulated from the top of the result list to the bottom with the gain of each result discounted at lower efficiency of file upload. Two assumptions are made in using DCG and its related measures.

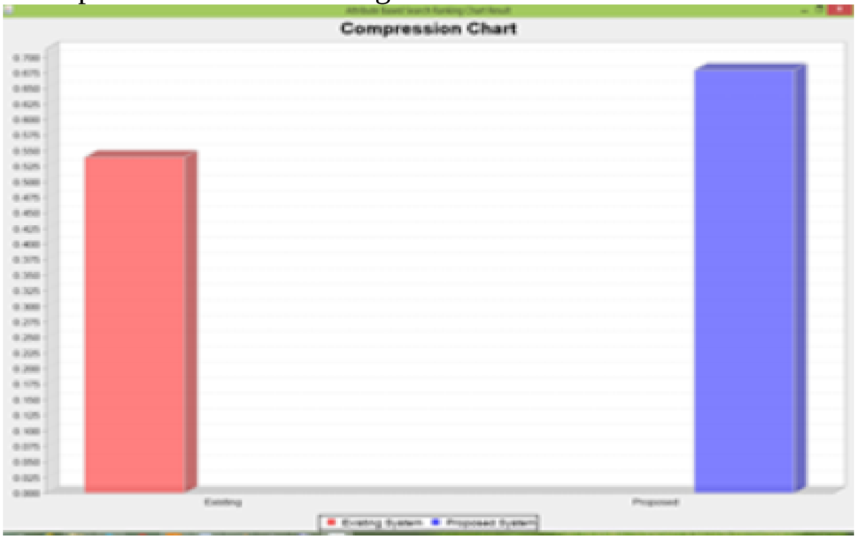

Fig.DCG of proposed VS existing system

1.Highly trustee User are more useful when appearing earlier in a result list (have higher trustee)
2. Highly Revocation Process are more useful than marginally Un-Revoke Process.
which are in turn more useful than Un-Revocation. DCG originates from an earlier, more primitive, measure called Cumulative Gain.

VI. Conclusion

A 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 authentication files by computing secret key once. Thus, the time cost of decryption as also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

REFERENCES

[1] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Securityoncerns in popular cloud storage services," IEEE Pervasive Comput.,vol. 12, no. 4, pp. 50–57, 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. 346–358.
[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secur.,
[4] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryp-tion 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. 130–147.
[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. 1667–1680, 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 comput-ing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.
[7] J.K.Liu,M.H.Au,X.Huang,R.Lu,andJ.Li,"Fine-grainedtwo-factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.
[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457–473.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., Oct. 2006, pp. 89–98.
[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. 778–782, Oct. 2014.
[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
[12] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur., Oct. 2007, pp. 456–465.
[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. 10th Int. Workshop Inf. Secur. Appl., Aug. 2009, pp. 309–323.

[14] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing," J. Universal Comput. Sci., vol. 19, no. 16, pp. 2349–2367, Oct. 2013.
[15] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, pp. 763–771, May 2014.
[20] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," Future Generat. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015

Patel Tanveer Kamludeen is Pursuing Master of Engineering with specialization in Computer Engineering, from Vishwabharati Academy's College of Engineering, A'Nagar, Savitribai Phule University of Pune, Maharashtra, India.He Has more than 5 year of experience.

Ranmalkar V.S. is working as an Assistant Professor in Vishwabharati Academy's College of Engineering.