ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Privilege Identity Anonymity Control Attribute-Based Encryption Scheme in Cloud Computing

[1] Chittemreddyniranjan Reddy, [2] D.Gousiya Begum

[1]M.Tech Student, Dept. of CSE, SKU College of Engineering, Anantapur, Andhra Pradesh, India

[2]Assistant Professor, Dept. of CSE, SKU College of Engineering, Anantapur, Andhra Pradesh, India

ABSTRACT: Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problemof 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**.**

I. INTRODUCTION

In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control 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. 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. 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.
In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud service provider (CSP) is the manager of cloud service 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.

In the KP-ABE, a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user’s identity (e.g. IIT AND (Ph.D. OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when are-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to there-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE [. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users‟ attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypted holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots**.**

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE [11] 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 attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

II.LITERATURE SURVEY

2.1 Attributebased encryption for fine-grained access control of encrypted data:

As extra sensitive data is shared and stored on the web, there will be a need to encrypt data stored at
these websites. One drawback is that it can be selectively shared only at a rough-grained level (i.e., giving a different party your exclusive key). We develop a new cryptosystem for fine-grained sharing of encrypted information that we call Key-policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, Cipher texts are labeled with units of attributes and confidential keys are associated with entry constructions that control which Cipher texts a consumer is capable to decrypt. We display the applicability of our building to sharing of audit-log know-how and broadcast encryption. Our building helps delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). It's the first decentralized ABE scheme with privacy-keeping founded on regular complexity assumptions.

2.2 A Practical public key Cryptosystemprovably secure against chosen Ciphertext Attack:

This paper presents a novel framework for development of hybrid encryption schemes secure against chosen Cipher text assault. Our new framework yields new and extra effective CCA-secure schemes, and supplies insightful explanations about present schemes that don't match into the earlier frameworks. This could influence in finding future upgrades. Furthermore, it enables immediate conversion from a category of threshold public-key encryption to a hybrid one without considerable overhead, which is not achievable within the previous strategies.

2.3 A New Paradigm of hybrid encryption scheme:

In this paper, we show that a key encapsulation mechanism (KEM) does no longer need to be IND-CCA secure within the development of hybrid encryption schemes, as used to be earlier believed. That is, we present a extra efficient hybrid encryption scheme by way of making use of a KEM which is not always IND-CCA secure.

However, our scheme is secure within the experience of IND-CCA below the DDH assumption in the common mannequin. This outcomes is additional generalized to universal two projective hash families.

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which drastically enhances the flexibility of access control mechanisms. Due to the excessive expressiveness of ABE insurance policies, the computational complexities of ABE key-issuing and decryption have become prohibitively excessive. Despite that the prevailing Outsourced ABE solutions are able to dump some intensive computing duties to a 3rd get together, the verifiability of outcome again from the 1/3 occasion has yet to be addressed. Aiming at tackling the challenge above, we advise a brand new cozy Outsourced ABE procedure, which supports each secure outsourced key-issuing and decryption. Our new method offloads all entry coverage and attribute related operations in the key-issuing system or decryption to a Key Generation Service Provider and a Decryption Service Provider (DSP), respectively, leaving only a constant

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

number of straightforward operations for the attribute authority and eligible customers to participate in the neighborhood. In addition, for the first time, we endorse an outsourcedABE construction which presents examine capability of the outsourced computation results in an effective approach.

2.4 Outsourcingthe decrypting ABE Ciphertexts:

Attribute-Based Encryption (ABE) is a brand new imaginative and prescient for public key encryption that makes it possible for users to encrypt and decrypt messages headquartered on person attributes. For instance, a consumer can create a Cipher text that can be decrypted best with the aid of different users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for a lot of cloud storage and computing functions. However, one of the predominant efficiency drawbacks of ABE is
that the dimensions of the Cipher text and the time required to decrypt it grows with the complexity of the entry system. On this work, we recommend a brand new paradigm for ABE that mostly eliminates this overhead for users. Think that ABE Cipher texts are saved in the cloud. We show how a user can provide the cloud with a single transformation key that makes it possible for the cloud to translate any ABE Cipher text satisfied through that consumer's attributes right into a (steady-measurement) El Gamal-form Cipher text, without the cloud being ready to read any part of the consumer's messages. To exactly define and reveal the benefits of this procedure, we furnish new protection definitions for each CPA and replayable CCA safety with outsourcing, several new constructions, an implementation of our algorithms and designated performance measurements. In a traditional configuration, the consumer saves significantly on both bandwidth and decryption time, without growing the quantity of transmissions.

Existing System:

- Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE was proposed.
- Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang *et al.* proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE.
- Wan *et al.* proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A Cipher text policy hierarchical ABE scheme with short Cipher text is also studied.

- In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened.

Disadvantages of Existing System:

- In Existing System time and cost for encryption is high.
- No any special multiple hierarchical files are used.
- Decryption system time and computation cost are very high.

Proposed System:

- In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which 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 attacks (CPA) under the Decisional Bilinear Diffie-Hellman (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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Advantages of Proposed System:

- CP-ABE feasible schemes which has much more flexibility and is more suitable for general applications
- Multiple hierarchical files sharing are resolved using layered model of access structure.
- In proposed system both Cipher text storage and time cost of encryption are 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.
- The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

III.MODULE DESCRIPTION

3.1. Authority:

Auditing schemes mainly focus on the delegation of auditing tasks to a AA(Attribute Authority)so that the overhead on clients can be offloaded as much as possible. However, such models have not seriously considered the fairness problem as they usually assume an honest owner against an untrusted CSP. Since the AA acts on behalf of the owner, then to what extent could the CSP trust the auditing result? What if the owner and AA collude together against an honest CSP for a financial compensation? In this sense, such models reduce the practicality and applicability of auditing schemes. It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the FH-CP-ABE Scheme

Outsource key updates for cloud storage auditing with key-exposure resilience. We propose the first cloud storage auditing protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the AA(Attribute Authority) and are transparent for the client. In addition, the AA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the cloud.

3.2. Cloud Service Provider (CSP):

It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible.

In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud.

The S-CSP provides the data outsourcing service and stores data on behalf of the users.

To reduce the storage cost, the S-CSP eliminates the storage of redundant data via deduplication and keeps only unique data.

In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.

3.3. Data Owner:

It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it uploads file to Cloud

Data owner have the set of files, they create the index file ad send that file to the Cloud application server Finally Data owner encrypt that file and get encrypted key to the Authority .as well as send the encryption key directly to the data consumers

3.4. Data Consumer:

It wants to access a large number of data in cloud system. The entity first downloads the corresponding cipher text. Then it executes Decrypt operation of the proposed scheme

A user is an entity that wants to outsource data storage to the CSP and access the data later. Each user is issued a set of privileges in the setup of the system. Each file is protected with the encryption key and privilege keys to realize the authorized with differential privileges.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

IV. SYSTEM ARCHITECTURE

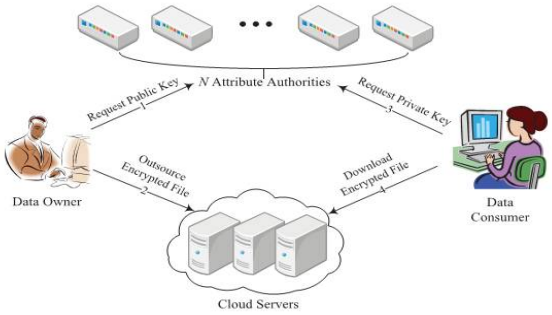

Fig 1 System Architecture

V. CONCLUSIONS AND FUTURE WORK

In this paper, we 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 are 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.

REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[2] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13thCCS*, 2006, pp. 89–98.
[4] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.
[5] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Trans.Comput.*, vol. 53,

BIOGRAPHY

C.NIRANJAN REDDY has received the B.Tech (Computer Science and Engineering) degree from Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, A.P. In 2015, and pursuing M.Tech (Computer Science and Engineering) in Sri Krishna Devaraya University College of Engineering and Technology. , Anantapur district (A.P).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Dudekula Gousiya Begum received her B.Tech Degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2007, M.Tech in Computer Science & Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2012. She has experience of 8 years in teaching graduate level and 4 years in teaching postgraduate level and she presently working as Lecturer inDepartment of CSESri Krishna Devaraya University College of Engineering,. Ananthpuram, district (AP).