International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 8 ǁ August 2022 ǁ PP. 415-420

Secure Outsourcing with Efficient Revocation inCloud Computing

Ms.Akshaya Suresh
M.Tech student in CFIS
CSE Dept.
College of Engg. KallooppараPathanamthita, Kerala

Mr.Rajkumar T
Assisstant Professor
CSE Dept.
College of Engg. Kallooppara
Pathanamthita,Kerala

Abstract*—Cloud computing has been offering effective storage solutions to personal and big-scale applications.But it becomes a big issue when data owner uploads data to the cloud because the cloud is a third party domain or else an untrusted domain.The important technique to make sure that the confidentiality of data is sure is by encryption.But when a large group of data is being shared to the cloud, the users will face a challenge of managing access control of encrypted data. Attribute-based encryption has become a promising increasing solution for encrypted data access control in clouds. Another important requirement for encrypted data access control system is revocation. After uploading the encrypted attribute-based ciphertext to the cloud, the data owner sometimes want to revoke some recipients that were authorized previously, which means that the outsourced attribute-based ciphertext needs to be updated to a new one that is under the revoked policy. Integrity issue raises when revocation is executed.So a new requirement for security is the revocable cipher-text attribute based encryption schemes.So hence here its confidentiality and integrity is verified.*

Index Terms*—Attribute-based Encryption, Revocation, Cloud computing, Encryption, Cipher-text, Outsourcing*

Date of Submission: 2-08-2022 Date of acceptance: 27-08-2022

I. INTRODUCTION

THE data storage and sharing services in the cloud,users can easily modify and share data as a group. To en-sure share data integrity can be verified publicly,users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. Cloud data owners prefer to upload documents in an encrypted form for the purpose of privacy preserving. It has been offering cost-effective storage solutions to personal and large-scale enterprise applications[1]. %beginshaded The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. The project is a web application that could be used to generate a on-time unique identification key when a user register with self-attribute

Fig. 1. Financial audit system revocation scenario. In the left part that the junior auditor from audit firm A, and the junior auditor from tax office cannotaccess the data from the revoked encrypted file any more.

information. Building the cloud within the organization or IT industry should have the minimal security issues only.Third parties are responsible for providing the services from the cloud. But believing third party alone is an important trouble in the cloud computing. Data confidentiality is an important issue in the third party cloud services. To guarantee the data security in the third party cloud needs the encryption and decryption mechanisms[2]. Thus mechanisms are provided by the access control methods. Access control is a functionality to assure the control over own data in the third party cloud. Many access control mechanisms that is used to ensure the security in the public cloud.

In this paper,mainly there are three modules that exists.Theyare:

- Admin : Admin can manage the auditor and user module and can
- User : User can manage of uploading and downloading of files,then setting permission for files,downloading per-mitted files, and revoke file permission.
- Auditor

In this paper,revocation of the people is done.That is admin can revoke the users or auditors. Particularly, the users can revoke the access for another user.Revocation is an critical component for the security of the system.

II. ATTRIBUTE-BASED ENCRYPTION

Attribute based encryption a system is one of the main access control mechanism used to provide the security to data based on the attributes in the public cloud[3].Attribute based encryption is the enhancement of identity based encryption used to provide the access control in the cloud computing. Identity based encryption not efficient at some point of time. To improve this introduces the attribute based encryption system which working under attributes associated with the cipher texts. In ABE each users should have the keys for attributes. Thus attribute keys used to do the decryption in the cloud computing. Thus attribute keys are also called the access rights in the attribute based encryption. Provide this decryption a key to users is defined as the giving access rights to one user. Through the access rights user can access the public cloud. But one user is not always being a part of data. Some point of time need to remove the user from the authorized users list. It is an important issue in the attribute based encryption[4]. Canceling the user's rights is very complex to do in the ABE. Because it needs the update of attribute keys every time while one of the user's rights is canceling. It is one of the main dis advantages.Such that to cancel particular user in the attribute, need to do the re-encryption in the ABE.

A. Revocable attribute based proxy re encryption

Attribute based proxy re-encryption(ABPRE), which com- bines the notions of proxy re-encryption(PRE) and attribute- based encryption(ABE),allows a semi-trusted proxy with re- encryption key to transform a cipher-text under a particular access policy into a cipher-text under another access policy, without revealing any information about the underlying plain- text. This primitive is very useful in applications where en- crypted data need to be stored in untrusted environments,such as cloud storage.In many practical applications, and in order to address scenarios where users misbehave or the re-encryption keys are compromised,an efficient revocation mechanism is necessary for ABPRE[5].

The ciphertext-policy ABE (CP-ABE) provides a way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes[6]. Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

B. Motivations

Although existing ABE schemes with ciphertext delegation enables the revocations of access policy for the ABE cipher- text, they cannot protect the data integrity. Hence, here a secure scheme that ensures data confidentiality as well as data integrity is needed. All of these concerns motivates to design an attribute-based encryption mechanism that:

- achieving revocation from the encrypted attribute-based encryption ciphertext while keeping the data integrity;
- does not require unnecessary operations of decryption andre-encryption for the data owner;
- the data owner is not required to be online for the revocation process.

In Cipher text Policy Attribute based Encryption scheme,the encryptor can fix the policy, who can decrypt the en- crypted message. The policy can be formed with the help of attributes[7]. In CP-ABE, access policy is sent along with the ciphertext. However, user revocation is a challenge in many one to many and many to many communication systems. In attribute based systems, this issue is difficult since each attribute is shared by multiple users;that is, revocation of a single user may affect others who share the same attributes. Moreover, user revocation in attribute-based systems needs to be flexible and support different granularities. That is, it may be required to revoke either the entire access privilege or just partial access right of the user, i.e., a subset of her attributes. In ABPRE systems, user revocation is even more difficult since it may affect the re-encryption keys and thus the corresponding delegators.

III. RELATED WORKS

Cipher text-policy Attribute based encryption: Here a new methodology for realizing Cipher text-Policy Attribute Encryption (CPABE) under concrete and no interactive cryp- tographic assumptions in the standard model is proposed.The solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system[8]. In most efficient system, cipher text size, encryption, and de-cryption time scales linearly with the complexity of the access formula.Here there are three constructions of framework.The first system is proven selectively secure under a assumption that can be called as the decisional Parallel Bilinear Daffier- Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption[9].The next two constructions provide performance trade-offs to achieve prov- able security respectively under the (weaker) decisional Bi- linear Diffie-Hellman Exponent and decisional Bilinear DiffieHellman assumptions.

The techniques provide a framework for directly realizing provably secure CPABE systems.Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device.Disadvantage is that it has limitation in termsof specifying policies and managing user attributes[10].

Attribute based encryption is used to do the encryption and decryption based on the set of access policies. Access policies used to ensure the data secrecy. But these policies not included in the attribute based encryption. To do the policies secrecy functional encryption, key policy attribute based encryptions, cloud mask, predicate based and hierarchical predicate encryp-tions are used.

Attribute based revocation:

The distinct of Public Key Encryption mechanism, ABE scheme takes attributes as the public key and associates the cipher-text and user's secret key with attributes, so that it provides more flexible access control mechanism over en- crypted data.Attribute-based encryption (ABE) can guarantee confidentiality and achieve fine-grained data access control in a particular cloud storage system[11]. Due to the fact that every attribute in ABE may be shared by multiple users and each user holds multiple attributes, any single-attribute revocation for some user may affect the other users with the same attribute in the system. Therefore, how to revoke attribute efficiently is an important and challenging problem in ABE schemes.In order to solve these problems,first give a concrete attack to the existing ABE scheme with attribute revocation. Then, formalize the definition and security model, which model collusion attack executed by the existing users cooperating with the revoked users. Finally,present a user col- lision avoidance cipher text-policy ABE scheme with efficient attribute revocation for the cloud storage system. The problem of attribute revocation is solved efficiently by exploiting the concept of an attribute group. When an attribute is revoked from a user, the group manager updates other users secret keys. Although ABE has shown its merits, attribute revocation and user revocation are the bottlenecks and limit its application into practical environment. Recently, these issues have become a primary concern of users. Especially, the attribute revocation issue is even more difficult for CP-ABE schemes, because every attribute is shared by multiple users, and each user holdsmultiple attributes.

Privacy preserving PHR:

Personal health record (PHR) service is an emerging model for health information exchange. In PHR systems, patient's health records and information are maintained by the patient himself through the Web. In reality, PHRs are often outsourced to be stored at the third parties like cloud service providers[12]. However, there have been serious privacy concerns about cloud service as it may expose user's sensitive data like PHRs to those cloud service providers or unauthorized users because it is a third party authority. Using attribute-based encryption (ABE) to encrypt patient's PHRs in cloud environment, secure and flexible access control can be achieved.To be specific,the scheme achieves the goals:

- scalable and fine-grained access control for PHRs byusing multi-authority ABE scheme, and
- efficient on-demand user/attribute revocation and dy- namic policy update.

Attribute based encryption for fined grained access:

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key).Here a new cryptosystem for fine grained sharing of encrypted data that can be called as Key-Policy Attribute Based Encryption (KP- ABE) is developed. In this cryptosystem, cipher texts are labelled with sets of attributes and private keys are associ- ated with access structures that control which cipher texts a user is able to decrypt[13].Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. The information given to a party is called the share (of the secret) for that party. Every SSS realizes some access structure that defines the sets of parties who should be able to reconstruct the secret by using their shares.The main disadvantage is that key policy attribute based encryption is applied so less privacy. **Verifiable outsourced Decryption:** The outsourced decryption ABE system highly reduces the computation cost for users who intended to access the encrypted files stored in cloud. However, the correctness of the transformation cipher text cannot be guaranteed because the user does not have the original cipher text.In order to improve the computation performance and reduce communication overhead,here a new verifiable outsourcing scheme with constant cipher text length is proposed[14]. To be specific, the scheme achieves the following goals:

- The scheme is verifiable that ensures the user checks whether the transformation is done correctly by the CSP efficiently.
- The size of ciphertext and the number of expensive pairing operations are constant, which do not grow with the complexity of the access structure.
- The access structure in this scheme is AND gates on multivalued attributes and prove that scheme is verifiableand it is secure against selectively chosen-plaintext attackin the standard model.

IV. PROPOSED SYSTEM

In this proposed system,we consider the integrity and con- fidentiality security for a revocable ABE scheme. The original data owner, the cloud server, an authoritative party, and the receivers are all components of a revocable attribute-based encryption with data integrity system.

- The scheme's security settings and keys are managed by the authority centre (for instance, the PKG). For instance,the system's public parameters and the members' private keys.
- Access to shared data is managed by the data owner. He uses a ciphertext-policy attribute-based encryption to encrypt the data before uploading it to the server.
- The cipher-texts are stored and the revocation processes are carried out by the cloud server (such as AWS).
- A recipient decrypts the cipher-text (original or revoked ciphertext) after receiving it, and they can also checkthat it is accurate.

Access Structure: The access controls for attribute-based encryption take the form of Boolean formulae. Access trees are used to establish these access regulations. The access structure of an access policy is referred to as this. The set of rules is provided by access policies. Each cipher text's set of rules in cloud storage. These regulations are meant to protect data privacy so that only authorized users may access the data.

Secret Sharing Schemes: In attribute-based encryption, a secret sharing technique is employed to distribute the keys. Access tree, which is part of ABE, is used to design policies. The keys for each attribute are generated using these access trees. There are several nodes in an access tree. The access tree is represented by leaf nodes. The keys for each leaf node must be generated from the root node using a secret sharing scheme. The secret sharing system is what this is known as. Therefore,

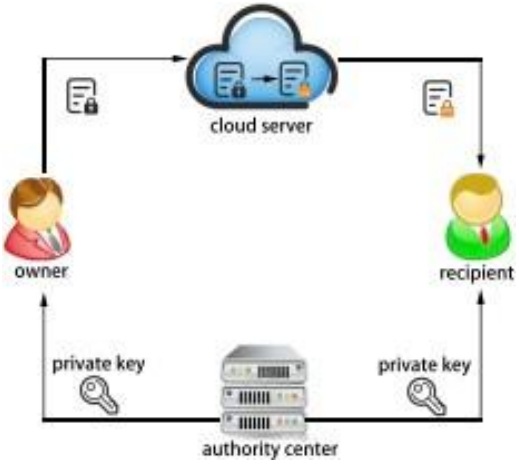

Fig. 2. Basic architecture

the secret keys for each attribute in the access tree are created using a secret sharing mechanism. The planned algorithm employs a polynomial function to create the keys for leaf nodes, each of which has a unique set of attributes. The secret

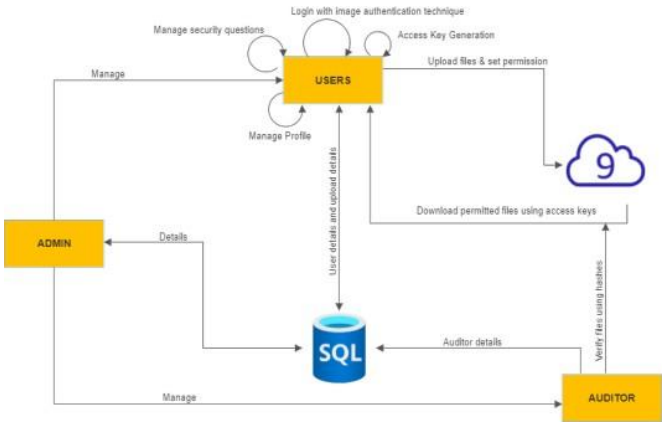

Fig. 3. Architecture derived from Fig 2.

key and the placeholders' key can both be used to decrypt data. The original data from the cloud storage was obtained using both of these decryptions. This two level of decryption is used to ensure the data security and confidentiality in the cloud storage. The partial decryption is created using updated placeholder key. The entire decryption may then be performed using the secret key. From this can infer that two level decryption is performed in the attribute based encryption of cloud storage. In attribute-based encryption, nothing can be accomplished using the secret key alone. In order to ensure effective dynamic attribute cancelling in cloud storage, this kind of decryption is used.

In this proposed system,there are mainly three modules:

- Admin: Admin section is the central authority because it manages the user and auditor module. Admin's details and managed details are all stored in the database.They manages these things:

1) Manage users:-In manage users the admin can add up a user to that particular firm using a particular password and username.Admin will be registering the users because this is mainly done in a IT firm.Admin can add all the user personal details.

2) Manage auditors:-Here admin can add auditors for verifying the integrity of the file results and the username and password is also managed by the admin.The auditor details is also added by the admin.

3) Manage security questions:-Here admin can add the different types of security questions for users so that the users can add the security questions when registering up.

- User:As said Users is managed by admin module and can manage all the case request and manages their profile like changing credential.When user first time is registered admin module asks for the security questions so that they can change the login credentials.Permitted users can download files from cloud.They can manage the following :

1) Upload files:-After the successful login the user can upload the files to the cloud they can add the title and description of the file content and upload it.

2) Set permission for files:-Here the user set permis- sion for the files that is they can give the number of days for a particular user to access that particular file.
3) Download permitted files:-Here the user can down- load the authorized or permitted number of files from the server and can access it.
4) Revoke file permission:-Here the user can also re- voke the permission of an another user so that the other user can't read or they will not get the access to read that particular file.

- Auditor:This module is managed by the admin mod- ule.User encrypted files are stored in cloud.To check the correctness or to verify the contents of the file is doneby auditor module by hashing algorithm.

1) Verify File integrity:-Here the auditor can see the files that is uploaded by the different users.Auditors will check the integrity of the files,that is they will check if the file is tampered or not.

A. ALGORITHM:AES

Advanced Encryption Standard (AES), commonly referred to as Rijndael[15], as a standard for the encryption of elec- tronic data in 2001. For AES, NIST selected three members of the Rijndael family, each with a 128-bit block size but three different key lengths: 128, 192, and 256 bits. AES was adopted by the American government and is now used on a worldwide basis. The AES algorithm is an asymmetric-key method, which means the data is encrypted and decrypted using the same key.Round keys are a particular set of uniquely produced keys that are utilised throughout the encryption process. These are used along with other operations on an array of data that comprises exactly one block of data (the data that will be encrypted). State array is the name of it.

V. CONCLUSION

Here a new framework to robustly and efficiently upload the files,download the files and revoke the files can be done from the cloud.Here AES algorithm method is used for encrypting the files and then it gets uploaded to the cloud.Here there are three modules that is Admin,User and Auditor module where the auditor will check the integrity of the files.Admin can add a particular user,auditor and manage them.Investigated the integrity requirement for revocable CP-ABE and put forward a notion of revocable CP ABE scheme with data integrity (RABE-DI), which ensures data integrity during the revocation process.Here a concrete RABE-DI scheme and proved its semantic security and integrity is presented.Here also con- ducted an implementation to demonstrate the practicality of the proposed RABE-DI scheme.This work opens many interesting problems. One of them is to design a revocable attribute- based encryption scheme with data integrity, which achieves the replayable chosen-ciphertext security. Experiment results demonstrate that this scheme is effective for verifying the correctness.So an efficient algorithm is created.Here mainly enhance the privacy and revocable technique,and in future canadd deduplication of data for utilizing space efficiently.

REFERENCES

[1]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, pp. 1–30, 2006.
[2]. C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," *Comput. J.*,vol. 59, pp. 970–982, 2016.
[3]. C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "Revocable attribute-based encryption with data integrity in clouds," *IEEE Transac-tions on Dependable and Secure Computing*, pp. 1–1, 2021.
[4]. M. S. Gunjal and D. B. L. Gunjal, "Efficient revocation and secure attribute-based proxy re-encryption scheme," 2017.
[5]. F. Luo and S. M. Al-Kuwari, "Revocable attribute-based proxy re- encryption," *Journal of Mathematical Cryptology*, vol. 15, pp. 465 – 482, 2021.
[6]. W. Jizhong and W. Chunxiao, "Full secure identity-based encryption scheme over lattices in the standard model," *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pp. 412–415, 2015.
[7]. K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security,"*2013 5th International Conference on Intelligent Networking and Col- laborative Systems*, pp. 552–559, 2013.
[8]. D. P. Pachpute, "Cipher text-policy attribute-based encryption in cloud computing for data sharing," 2017.
[9]. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *IACR Cryptol. ePrint Arch.*, 2012.
[10]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography*, 2011.
[11]. J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance cp-abe with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, vol. 12, pp. 1767–1777, 2018.
[12]. H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation,"*International Journal of Information Security*, vol. 14, pp. 487–497, 2014.
[13]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp- tion for fine-grained access control of encrypted data," *IACR Cryptol. ePrint Arch.*, vol. 2006, p. 309, 2006.
[14]. J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length,"*Secur. Commun. Networks*, vol. 2017, pp. 3 596 205:1–3 596 205:11, 2017.
[15]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," *IACRCryptol. ePrint Arch.*, vol. 2004, p. 86, 2005.