Volume 2, Issue 10, October-2015, pp. 861-866 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Deniable Access Control for Multi-Authority Cloud Storage

[1]Ch.Anusha, [2] A.Harshavardhan

[1]*M.Tech (CSE), Priyadarshini Institute of Technology & Science for women's*

[2]*Assistant Professor (Dept.of CSE), Priyadarshini Institute of Technology & Science for Women's*

Abstract:- Now days, plenty of users are storing their data's in cloud, as a result of it provides storage flexibility. However the most downside in cloud is information security. Information access management is efficient thanks to make sure the information security within the cloud. Because of information outsourcing and untrusted cloud servers, the information access management becomes a difficult issue in cloud storage systems. Cipher text-Policy Attribute based mostly encoding (CP-ABE) is thought to be one in every of the foremost appropriate technologies for information access management in cloud storage, as a result of it provides information homeowners additional direct management on access policies. However, it's tough to directly apply existing CP-ABE schemes to information access management for cloud storage systems as a result of the attribute revocation downside. during this paper, we have a tendency to style associate degree communicative , economical and voidable information access management theme for multi-authority cloud storage systems, wherever there are multiple authorities co-exist and every authority is in a position to issue attributes severally. Specifically, we have a tendency to propose a voidable multi-authority CP-ABE theme, and apply it because the underlying techniques to style the information access management theme. Our attribute revocation methodology will with efficiency bring home the bacon each forward security and backward security. The analysis and simulation results show that our projected information access management theme is secure within the random oracle model and is additional economical than previous works.

Index Terms— Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

I. INTRODUCTION

All Data access control is an effective approach to guarantee the information security in the cloud. Cloud storage administrations permits information proprietor to outsource their information to the cloud. Trait based encryption (ABE) is another idea of encryption calculations that permit the encryptor to set a policy describing who ought to have the capacity to peruse the information. In a quality based encryption framework, private keys distributed by a power are connected with sets of traits and cipher texts are related with formulas over properties. A client ought to have the capacity to unscramble a cipher text if and just if their private key attributes fulfill the equation. In conventional open key cryptography, a message is scrambled for specific recipient utilizing the collector's open key. Character based cryptography and in particular identity based encryption (IBE) changed the customary comprehension of open key cryptography by permitting people in general key to be a subjective string, e.g., the email location of the beneficiary. ABE goes one above and beyond and characterizes the personality not nuclear but rather as an arrangement of properties, e.g. parts, and messages can be scrambled with appreciation to subsets of characteristics (key-approach ABE - KP-ABE) or policies defined over an arrangement of traits (ciphertext-strategy ABE - CP-ABE).

In ciphertext-arrangement quality based encryption (CP-ABE) a client's private-key is connected with a setoff properties and a ciphertext indicates an entrance approach over a characterized universe of qualities within the framework. A client will have the capacity to unscramble a ciphertext, if and just if his traits fulfill the policy of the particular ciphertext. Figure content Policy Attribute-based Encryption (CPABE)is considered as a standout amongst the most suitable plan for information access control in distributed storage. These plan provides data proprietors more straightforward control on access approaches. In any case, CP-ABE plans to information access control for distributed storage frameworks are troublesome in light of the characteristic disavowal issue. So This paper produce review on effective and revocable information access control plan for multi-power cloud storage frameworks, where there are multiple authorities collaborate and every power can issue attributes freely. CP-ABE in this manner permits to acknowledge verifiable approval, i.e., approval is incorporated into the encrypted information and just people who fulfil the related

strategy can unscramble information. Anothernicefeature is that clients can get their private keys after information has been encoded with deference to policies. So information can be scrambled without learning of the genuine arrangement of clients that will be capable to decrypt, yet just indicating the strategy which permits unscrambling. Any future clients that will be given a key as for traits such that the strategy can be fulfilled will then have the capacity to decode the data.

II. SYSTEM MODEL AND SECURITY MODEL

System Model

We consider information access control systeminmulti-authoritycloud capacity, as portrayed in Fig. 1. There are five sorts of entities in the framework: a testament power (CA), attribute authorities (AAs), information (proprietors), the cloud server (server) and information buyers (users).The CA is a worldwide trusted endorsement power in the system. It sets up the framework and acknowledges the enlistment of all the clients and AAs in the framework. For each lawful client in the framework, the CA appoints a worldwide exceptional client personality to it furthermore creates a worldwide open key for this client. Notwithstanding, the CA is not included in any characteristic management and the making of mystery keys that are associated with qualities. For instance, the CA can be the Social Security Administration, an autonomous office of the United States government. Every client will be issued a Social Security Number (SSN) as its worldwide personality. Each AA is an autonomous quality powers that is responsible for entitling and denying client's attributes according to their part or personality in its space. In our scheme, each characteristic is connected with a solitary AA, but each AA can deal with a subjective number of attributes. Every AA has full control over the structure and semantics of its traits. Every AA is in charge of producing a public property key for every quality it oversees and a secret key for every client mirroring his/her characteristics. Every client has a worldwide character in the framework. A user maybe entitled an arrangement of qualities which may come from multiple trait powers. The client will get a secret key connected with its traits entitled by the corresponding characteristic powers. Every proprietor first partitions the information into a few components according to the rationale granularities and scrambles each data segment with different substance keys by using symmetric encryption techniques. Then, the proprietor defines the access strategies over qualities from various attribute authorities and encodes the substance keys under the policies. At that point, the proprietor sends the scrambled information to the cloud server together with the ciphertexts.2 they do not rely on the server to do information access control. Be that as it may, the access control happens inside the cryptography. That is just when the user's traits fulfil the entrance arrangement characterized in the ciphertext; the client can decode the ciphertext. Thus, users with distinctive qualities can decode different number of substance keys and accordingly acquire diverse granularities of data from the same information.

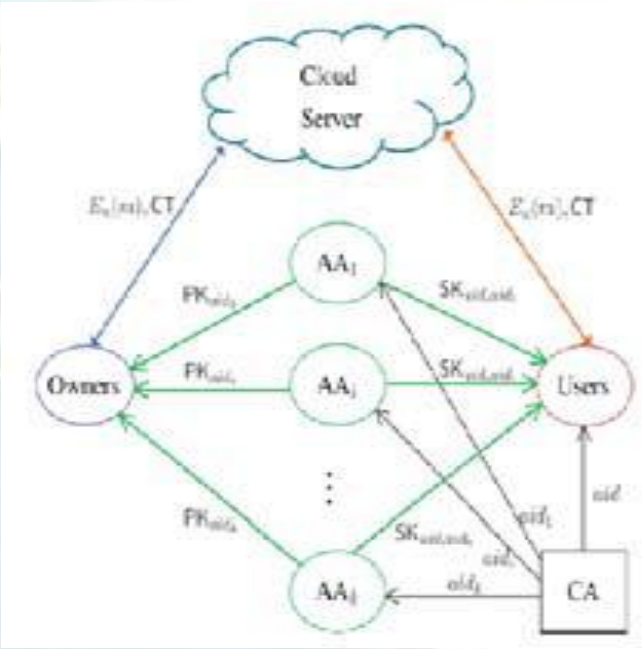

Fig. 1 : System model of data access control in multi-authority cloud storage.

In multi-authority cloud storage systems, we make the following assumptions:

- The CA is fully trusted in the system. It will not collude with any user, but it should be prevented from decrypting any cipher texts by itself.
- Each AA is trusted but can be corrupted by the adversary.
- The server is curious but honest. It is curious about the content of the encrypted data or the received message, but will execute correctly the task assigned by each attribute authority.
- Each user is dishonest and may collude to obtain unauthorized access to data.

III. CP-ABE

One of the most suitable technologies for data access control in cloud storage systems is Cipher text-Policy Attribute-based Encryption (CP-ABE). It provides the data owner to direct control on access policies. The Authority in this scheme is responsible for key distribution and attribute management. The authority may be the university Administration office, Staff maintenance (Human resource-HR) department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data depending on the policies.

A. CP-ABE Types

In CP-ABE scheme for every user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes to satisfy the access policies.
There are two types of CP-ABE systems:
• Single-authority CP-ABE
• Multi-authority CP-ABE
In Single-authority CP-ABE method, where all the attributes are managed by only one a single authority. In a Multiauthority-ABE scheme where attributes are from different attribute authorities. This method is more suitable for data access control of cloud storage systems. Data users contain attributes should be issued by multiple authorities and data owners. Data users may also share the data using access policy defined over attributes from different authorities.
In our scheme, the data owner does not require to trust the server. Because, the key is based on attribute and maintained by the attribute authority. We designed new revocation method for multi-authority CP-ABE. Then, we apply them to design a fully secure and efficient data sharing for multi-authority scheme. The important advantages of this work can be summarized as follows,
i. We proposed third party auditor (TPA) which used for auditing the data.
ii. We develop a new revocation method for user attribute revocation.

B. CP-ABE Algorithm
A CP-ABE scheme has four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

1. Setup (λ; U)
The setup algorithms takes input as security parameter and attribute universe description. It outputs the global public parameters PK and a global master key MK.

2. Encrypt (PK; M; A)
The encryption algorithm takes as input the public parameters PK of attributes, a message M, and an access structure A over the involved attributes. The algorithm will encrypt M and produce a ciphertext (CT) that only a user having a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.
3. Key Generation (MK; S)
The key generation algorithm takes as input the global master key MK and a set of attributes that clarify the key. It outputs a private key SK.

4. Decrypt (PK; CT; SK)
The decryption algorithm takes as input the public parameters PK, a ciphertext (CT), which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

IV. FRAME WORK

The data access control for Multi-Authority cloud storage system consists following methods.

1) System Initialization

• **CA Setup** (1λ): (GMK, GPP, (GPK'uid, GPK'uid), (GSKuid; GSK'uid), Certificate(uid)).
• The CA setup algorithm is run by the CA. It takes no input other than the implicit security parameter λ. It generates the global master key GMKof the system and the global public parameters GPP.For each user uid, it generates the user's global public keys (GPKuid, GPK'uid), the user's global secret keys (GSKuid ,GSK'uid) and a certificate Certificate (uid) of the user.
• **AASetup (**Uaid):(SKaid, PKaid, {VKxaid, PKxaid } xaid,Uaid). The attribute authority setup algorithm is run by each attribute authority. It takes the attribute universe Uaid managed by the AAaid as input. It outputs a secret and public key pair (SKaid, PKaid) of the AAaid and a set of version keys and public attribute keys {VKxaid, PKxaid }xaid,Uaid for all the attributes managed by the AAaid.

2) Attribute Authority's key generation and management

Secret Key Distribution
A randomized algorithm takes as input the authority's secret key SK, a user u'sUID, and a set of attributes Aku in the authority AAk'sdomain (We will assume

that the user's claim of these attributes has been verified before this algorithm is run, Au = {Aku , k = 1, . . . , n}). Output a secret keyDu for the user u.

Access issue id Distribution

The collected attributes from all attribute authorities (Aa) will be sent to the users for the encryption purpose.

3) Data Encryption

The data owner runs the encryption algorithm to encrypt the content keys. By using symmetric encryption method the data is encrypted with content keys. A randomized algorithm takes as input a set of public key of attributes involved in encryption, a message M, the global public parameters GPP and outputs the ciphertext C.

4) Data Decryption

The users first run the decryption algorithm and use them to V decrypt data's from the ciphertext C. It takes input the V ciphertext C, it have access policy with itself for verifying the V access rules of the users. If the access policy is satisfied with V the users attribute, the decryption algorithm will decrypt the V ciphertext C.

5) Attribute revocation:

The attribute revocation has been solved by assigning new version key VK for non-revoked attribute. It takes as inputs the secret key of Attribute authority, revoked attribute id and current version key. Its outputs as new version key and new attribute key.

V. OUR DATA ACCESS CONTROL SCHEME

In this segment, we first give an outline of the challenges and systems. At that point, we propose the itemized construction of our entrance control plan which comprises of five phases: System Initialization, Key Generation, Data Encryption, and Data Decryption

Furthermore, Attribute Revocation. To outline the information access control plan for multi authority distributed storage frameworks, the primary challenging issue is to build the fundamental Revocable Multi authority CP-ABE convention. In, Chase proposed a multi-power CP-ABE convention, in any case, it can't be straightforwardly connected as the fundamental procedures on the grounds that of two principle reasons: 1) Security Issue: Chase's multi-authority CP-ABE convention permits the focal power to decode all the cipher texts, since it holds the expert key of the system;2) Revocation Issue: Chase's convention does not support attribute denial. We propose another revocable multi-power CP-ABE protocol in light of the single-power CP-ABE proposed by Lewko and Waters in. That is we stretch out it to multi authority scenario and make it revocable. We apply the techniques in Chase's multi-power CP-ABE protocol to entwine the mystery keys produced by different authorities for the same client and keep the collusion attack. In particular, we isolate the usefulness of the authority into a worldwide endorsement power (CA) and multiple trait powers (AAs). The CA sets up the system and acknowledges the enrolment of clients and AAs in the system. It allocates a worldwide

Client character uid to each user and a worldwide power personality help to every property authority in the framework. Since the uid is all inclusive novels in the framework, mystery keys issued by distinctive AAs for the same uid can be entwined for unscrambling. Additionally, on the grounds that each AA is connected with a guide, each trait is distinguishable even in spite of the fact that a few AAs may issue the same property. To manage the security issue in, rather than utilizing the system one of a kind open key (created by the exceptional master key) to scramble information, our plan requires all attribute authorities to produce their own particular open keys and uses them to encode information together with the worldwide open parameters. This keeps the endorsement power in our plan from decrypting the cipher texts. To take care of the trait denial issue, we allocate repugnance number for every quality. At the point when an attribute revocation happens, just those parts associated with the renounced quality in mystery keys and cipher texts need to be redesigned. At the point when a property of a client is denied from its comparing AA, the AA produces another version key for this repudiated property and creates an overhaul key. With the overhaul key, every one of the clients, aside from the renounced user, who hold the denied traits can upgrade its mystery key (Backward Security). By utilizing the overhaul key, the components connected with the disavowed trait in the ciphertext can likewise be redesigned to the present rendition. To improve the effectiveness, we assign the workload of ciphertext upgrade to the server by utilizing the intermediary encryption method, such that the recently joined client is also able to unscramble the beforehand distributed information, which are encrypted with the past open keys, in the event that they have sufficient properties (Forward Security). Besides, by updating the cipher texts, every one of the clients need to hold only the

most recent mystery key, as opposed to keep records on all the previous mystery keys.

VI. SECURITY ANALYSIS

We prove that our data access control is secure under the security model we defined, which can be summarized as in the following theorems.
Theorem 1. When the decisional q-parallel BDHE assumption holds, no polynomial time adversary can selectively break our system with a challenge matrix of size l_ n_, where n_ _ q.
Proof. The proof is given in the supplemental file available online. g
Theorem 2. Our scheme can achieve both Forward Security and Backward Security.

Backward Security: During the key key update part, the corresponding AA generates associate degree update key for every non-revoked user. as a result of the update secret's related to the user's international identity uid, the revoked user cannot use update keys of different no revoked users to update its own secret key, albeit it will compromise some non-revoked users. Moreover, suppose the revoked user will corrupt another AAs (not the AA like the revoked at-tributes), the item Hðxaid Þvxaid _aid_aid within the secret key will forestall users from change their secret keys with update keys of different users, since ordered is barely well-known by the AAaid and unbroken secret to all the users. This guarantees the back-ward security.

Forward Security: After every trait denial operation, the rendition of the renounced characteristic will be upgraded. At the point when new clients join the framework, their mystery keys are as-associated with traits with the most recent rendition. Be that as it may, already distributed figure writings are scrambled under at-tributes with old form. The figure content redesign calculation in our convention can upgrade already distributed figure writings into the most recent quality variant, such that recently joined clients can at present decode beforehand distributed figure writings, if their characteristics can fulfil access arrangements connected with figure writings. This assurances the forward security.
Hypothesis 3. Our entrance control plan can oppose the arrangement assault, notwithstanding when a few AAs are defiled by the enemy. One another, albeit a few AAs may issue the same properties. Besides, the mystery key is likewise connected with the client's all inclusive interesting character uid. In this way, clients can't intrigue together to increase illicit access by consolidating their characteristics together.
Be that as it may, when a few AAs is ruined by the adversary, the intrigue resistance turns out to be more confounded. In particular, the foe may dispatch Attribute Forge Attack, characterized as takes after. Assume a client uid0 has a property "xaid0 "" from AAaid0 , while the enemy does not hold the characteristic "xaid0 "" from AAaid0 . The foe endeavours to fashion ("clone") the attribute"xaid0 "" from the client uid0's mystery key by intriguing with some different AAs. In our plan, the thing gu0uid tuid;aid _aid in the mystery key development opposes this assault. At the point when the enemy ruins any AAs, he/she can get all the worldwide mystery key GSKuid for every one of the clients in the framework (in light of the fact that every AA has full information on one of the client's worldwide mystery keys GSKuid). Assume all the Kxaid ;uid in the mystery key is developed without this thing. The enemy can achievement completely fashion the quality "xaid0 "" as Privacy-Preserving Guarantee: Although the CA holds the worldwide expert key GMK, it doesn't have any mystery key issued from the AA. Without the information of g_aid , the CA can't decode any ciphertexts in the framework. Our plan can likewise keep the server from using so as to get the substance of the cloud information the intermediary encryption technique.

VII. PERFORMANCE ANALYSIS

In this segment, we investigate the execution of our plan by contrasting and the Ruj's DACC plan and our past plan in the meeting adaptation, as far as capacity overhead, correspondence expense and calculation proficiency. We lead the examination under the same security level. Let jpj be the component size in the G; GT ; Zp. Assume there are nA dominant presences in the framework and every characteristic power AAaid oversees naiad traits. Let nU and nO be the aggregate number of clients and proprietors in the framework separately. For a client uid, let nuid; aidk ¼ jSuid;aidk j denote the number of qualities that the client uid acquired from AAaidk. Let "be the aggregate number of qualities in the ciphertext.

IX. CONCLUSION

In this paper, we proposed a revocable multi-power CPABE plan that can bolster proficient trait repudiation. At that point, we built a viable information access control plan for multi authority distributed storage frameworks. We likewise

demonstrated that our plan was provable secure in the arbitrary prophet model. The revocable multi-power CPABE is a promising strategy, which can be connected in any remote stockpiling frameworks and online informal communities and so on. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a promising method that is intended for access control of scrambled information. There are two sorts of CP-ABE frameworks: single power CP-ABE where all characteristics are overseen by a solitary power, and multi-power CP-ABE, where qualities are from distinctive spaces and oversaw by diverse powers. Multi authority CP-ABE is more fitting for the entrance control of distributed storage frameworks.

References

[1] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

[2] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc.16thACM Conf. Computer and Comm. Security (CCS'09),2009, pp. 121-130.

[3] A.B. Lewko and B. Waters, ''Decentralizing Attribute- Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.

[5] M. Li, S. Yu, Y. Zhen, K. Ren, and. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[6] J. Hurl and D.K. Noh, ''Attribute-Based Access Control with
Efficient Revocation in Data Outsourcing Systems,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[7] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. 10th IEEE Int'l Conf.TrustCom, 2011, pp. 91-98.

[9] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc.32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.

[10] D. Boneh and M.K. Franklin, ''Identity-Based Encryption from the Weil pairing,'' in Proc. 21st Ann. Int'l CryptologyConf.: Advances in Cryptology - CRYPTO'01, 2001, pp.213-229.

[11] A.B. Lewko and B. Waters, ''New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques,'' in Proc. 32st Ann. Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'12, 2012, pp. 180-198.

[12] P. Mell and T. Grace, ''The NIST Definition of Cloud Computing,'' National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

