Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Contract Signing protocol for Cipher text-Policy Attribute-based Encryption of Accountable Data Sharing in Cloud

H. Radha Kumari
Assistant Professor,
Dept of Computer Science & Engineering

Tata Venkateswarlu
Assistant Professor,
Dept of Computer Science & Engineering

Abstract:
Now days, a lot of users are storing their data's in cloud, because it provides storage flexibility. But the main problem in cloud is data security. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. In this work to propose a data access control for multi authority for verifying the integrity of an un-trusted and outsourced storage by third party auditor. In addition, this project proposes method based on probabilistic query and periodic verification for improving the performance of audit services. It ensures efficiency of security by protecting from unauthorized users. These experimental results not only validate the effectiveness of these approaches, but also show our audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit metadata.

Keywords:
Access control, multi-authority, audit, attribute revocation, cloud storage.

1. INTRODUCTION:

In recent years, the cloud computing technologies has developing technology in IT world. The cloud computing has many features like access anywhere from anywhere and at any time. The cloud computing has large data storage or data centers and also uses large servers for web application and services. Access control and authentication methods ensure the authorized users to access the data. But, its main concern is data security.

Because, the cloud server cannot be fully trustworthy by data owners, they cannot believe on servers to do access control. Cipher text-policy Attribute based encryption [1,2] (CP-ABE) is one of the recent technologies for data access control in cloud storage, because it provides the data owner more direct control on access policies. In this scheme, the attribute authority is responsible for the maintaining the attribute and also responsible for key distribution for the attribute. The certificate authority is activates the user and attribute authority registration. The CA can be the Human resource department in an organization, registration office in a university, etc. The data owners encrypt depending on the access policies and attribute [3]. The access policies prevents the unauthorized person to access the data. Multi-Authority CP-ABE is suitable for data access control of cloud data storage. The user may be hold n number of attributes from any attribute authority. The data owners can share the data with attribute based encrypted method along with the access policy. For Example, A Human resource department, the data owners share the data by using the access policy [5] "Project Manager AND Team Leader" or "Project Manager OR Team Leader", where the attribute "Project Manager" have different access rules and the attribute "Team Leader" have different access rules. It is very difficult to apply directly on multi-authority CP-ABE method [6] to cloud storage because the attribute revocation issues for users. This issue happens when the revoked user cannot decrypt any ciphertext that requires the revoked attribute to decrypt (Backward security) [7] and the newly entered users can also decrypt the previous published ciphertext if its public key and sufficient attributes (Forward security).

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

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 attributes management. The authority may be the university Administration office, Staff maintenance (Human resource-HR) [8] department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data depending on the policies.

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 Multi-authority CP-ABE scheme where attributes are from different attribute authorities. This method is more suitable for data access control of cloud storage systems [4]. 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.

2. RELATED WORK:

C. Dong, G. Russello. [9] define a conventional "proof of retrievability" (POR) design for providing the isolated data consistency. Their strategy integrates spot-checking and error fixing code to provide both control and retrievability of data on repository service techniques. S. Vishnupriya [10] created on this design and produced an arbitrary additive function-based homomorphism authenticator that allows unlimited quantity of concerns and needs less conversation elevated with its use of comparatively small size of BLS trademark. Kan Yang et al. [11] suggested an enhanced structure for POR prototypes that generalizes both Juelsand Shacham's work. Afterwards in their following work, A.B. Lewko, T. Okamoto et al. [3] stretched POR design to dispensed systems. Nevertheless, all such strategies are concentrating on static data. The efficiency of their strategies lies mainly on the preprocessing procedures that the user performs before outsourcing the information file F. Any modification to the contents of F, even some bits, must transmit thru the error fixing code and the equivalent arbitrary shuffling procedure, so providing extensive computation and conversation intricacy. In recent times, M. Li, S. Yu, Y. Zheng et al. [4] provided theoretical studies on generalized structure for distinctive models of existing POR process. Yang et al. [11] described the "provable data possession"(PDP) system for providing control of file on untrusted storages. Their strategy used public key-based homomorphic labels for auditing the information file.

Although, the pre calculation of the labels imposes significant computation elevated that can be extravagant for an intact file. In their following work, S. Yu, C. Wang et al. [5] explained a PDP strategy that utilizes just symmetric key-based cryptography. This technique has lower elevated than their past strategy and permits for block updates, deletions, and appends to the retained file that has also been reinforced in our work. Anyhow, their strategy concentrates on solitary server situation and does not supply data access guarantee against server failures, leaving both the distributed scenario and information error rehabilitation problem unexplored. The specific support of data dynamics has further been examined in the two current works. Wang et al.suggested incorporating BLS-based homomorphic authenticator through Merkle Hash Tree to assist completely data dynamics, whilst Erway et al. [9] evolved a skip list-based strategy to allow provable data control with completely dynamics assist.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The progressive cryptography work accomplished by Bellare et al. also supplies a set of cryptographic generating blocks like hash, MAC, and signature features that may be applied for storage consistency affirmation while encouraging powerful operations on data. Anyhow, this part of work comes into the conventional data consistency defense mechanism, where localized replicate of data has to be operated for the affirmation. It's not yet obvious how the work can be modified to cloud storage situation where consumers not have the data at local sites but even require providing the storage correctness effectively in the cloud. The Storage as well as Computation Cost of Token Pre calculation for 1 GB Data File using Different System configurations In another relevant work, focused to determine data control of various replicas around the dispersed storage technique.

They prolonged the PDP strategy to encapsulate several replicas with no encoding every replica individually, supplying assurance that various replicas of data are really preserved. Lillibridge et al. provided a P2P support strategy in which inhibits of a data file are dispersed around m þ k peers with an erasure code. Peers can obtain arbitrary blocks from their support peers and validate the consistency with distinct keyed cryptographic hashes associated on every block. Their strategy can determine data decline from free-riding associates, but cannot guarantee each data are unrevised. Filho as well as Barreto projected to check data consistency using RSA-based hash to describe unchea table data control in peer-to-peer file sharing channels.

3. SYSTEM MODEL:

We designed a data access control for Multi-Authority cloud storage as fig (1) shows, there are six types of entities in system: The cloud server(server), the data owner, the attribute authority (AA), the Certificate authority (CA), the data users (User) and the third party auditor (TPA).

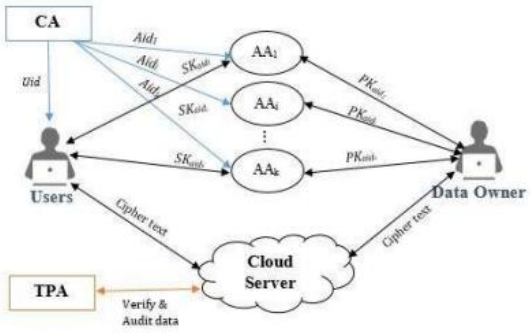

Fig.1: Revocable authentication cloud storage.

The CA is a global trusted certificate authority, which accepts the user and AA registration. The CA is distributes the global public key and global secret key for each legal user. But it is not involved in any attribute management and also creation of secret keys that are associated with attributes. For example, CA is like a Unique Identification Authority of India (UIDAI), for Indian government. Each user will be issued a Unique Identification Number (AADHAAR Number) as its identity. Every AA is a separate attribute authority. AA is responsible for create an attribute and revoke the attributes for user. The attribute is created by the role or identity of user. Each AA has maintaining the n number of attributes. AA generates the public key and private key for the each attribute it manages. The user has a global identity in the system. They may be creating a set of attributes which comes for multiple attribute authority and also receives a secret key for their attributes. The data owners encrypt the data along with the access policies with the set of public key of the attributes. The data owner updates the ciphertext into the cloud server. The user can decrypt when the attributes satisfy the access policy along with the ciphertext, the user can decrypt the ciphertext. The cloud server maintains the data owner's ciphertext. The server does not edit or updates any contents in the ciphertext. Third party auditor (TPA) is used to audit the files on the cloud server. It increases more security for the data, because it prevents data from the attackers and hackers.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

4. Contract Signing between Client and Cloud: A Signcryption approach

The overall procedure begins here with the work of RSA signature algorithm else referred to as Signcyption. There, the 1st user divides his private key d towards d1 and d2 such that d=d1+d2 by appropriate park. The signature of this individual has to be replaced with another and this signature is $\sigma_A = h(m)^{d1} \bmod n$.The fragmentary signature created by the 1st individual is to ensure that he has zero-knowledge base also this is accomplished by Gennaro prototype. The associations we have are untrustworthy because system failure or router's assaults. However, TTP is trustworthy since the information inserted attain the location for certainly but with a little stoppage.

A. Registration Protocol:

The recipient of the data has only to enroll i.e. only the enrollment of the initiator with TTP is sufficient. He then receives a long-term coupon with CA. After that, the appropriate procedures are carried out: (for our comfort, let the transmitter be CLOUD and recipient as CLIENT.)

i. Client 1st establishes an RSA modulus $n = pq$, where p and q are two -bit secure primes, i.e., there exist two primes p' and q' such that $p = 2p'+1$, $q = 2q'+1$. After, Client chooses her arbitrary public key $e \in_R \square^*_{\phi(n)}$, and determines her private key $d = e^{-1} \bmod \phi(n)$, where $\phi(n) = (p-1)*(q-1)$. Finally, Client enrolls her public key with a CA to obtain her certificate C_A, which attach her identity and the related pubic key (n,e) collectively.

ii. Client arbitrarily divides d into $d1$ and $d2$ such that $d = d1 + d2 \bmod \phi(n)$ by selecting $d1 \in_R \square^*_{\phi(n)}$, and calculates $e_1 = d_1^{-1} \bmod \phi(n)$. She also creates a sample message-signature pair (ω, σ_ω), where $\omega \in \square^*_n \setminus \{1,-1\}, ord(\omega) \geq p'q'$ and $\sigma_\omega = \omega^{d1} mod\, n$. Then, Client transmits $(C_A, \omega, \sigma_\omega, d2)$ to the TTP but maintains (d, d_1, d_2, e_1) furtive.

iii. The TTP first verifies for the corroboration of Client's permit C_A. After that, the TTP verifies that the triple $(\omega, \sigma_\omega, d2)$ s equipped properly. If all is in accurate order as per its convention, TTP preserves d2 and creates a coupon V_A by calculating $V_A = Sign_{TTP}(C_A, \omega, \sigma_\omega)$. This confirms the TTP's signature on memo $(C_A, \omega, \sigma_\omega)$, which assurances that the TTP can concern a suitable partial signature for Client by utilizing the furtive $d2$.

B. Signature Exchange Protocol:

Earlier all this, a contract has to be consented in between Cloud as well as Client also they must sign it. It must be a deadline, and recognize the Client, Cloud, also TTP.

a) At first, the initiator Client should compute her fragmentary signature $\sigma_1 = h(m)^{d1} \bmod n$, and then transmits the triple $(C_A, \omega, \sigma_\omega)$ towards responder Cloud. Here, $h(.)$ is a cryptographically safe hash function.

b) After getting (C_A, V_A, σ_1), Cloud first confirms that C_A is whether provided by CA, and V_A is Client's coupon established by the TTP. Perhaps, Cloud monitors if the details of Client, Cloud, and the TTP are properly revealed as element of the contract 'm'. If all such verifying are ok, Cloud begins the below active zero-knowledge prototype with Client to verify whether σ_1 is Client's applicable fractional signature on contact.

i) Then Cloud chooses two numbers $i, j \in_R [1, n]$ at arbitrary, and a concern c to Client is transmitted by computing $c = \sigma_1^{2i} \sigma_w^{\ j} \bmod n$.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

ii) Obtaining the challenge c, Client determines the response $r = c^e \bmod n$ She then yield her contract $\bar{r} = TCcom(r,t)$ to Cloud utilizing an arbitrary number t, where $TCcom$ is the pledge algorithm.

iii) After obtaining the commitment $\bar{r}$, Cloud transmits Client the pair (i, j) to accept that he is performed with the challenge c correctly.

iv) Client confirms for correct planning of c, that is $c \equiv \sigma_1^{2i}\sigma_\omega^j \bmod n$. If ok, Client extracts his commitment $\bar{r}$ by determining the replies (r,t) to Cloud. With this (r,t) , Cloud realizes σ_1 as applicable if and only if $r \equiv h(m)^{2i}\omega^j \bmod n$ and $\bar{r} \equiv TCcom(r,t)$.

c). Cloud monitors the σ_1 Client's valid biased signature and the target t revealed in contract m is whether sufficient for fixing the dispute motion from the TTP. Then only he transmits his signature σ_B to Client.

d). after obtaining σ_B, Client has to confirm whether it is Cloud's applicable signature. If it is, she transmits Cloud the fractional signature σ_2 by processing $\sigma_2 = h(m)^{d2} \bmod n$. As Cloud obtains σ_2, he creates $\overline{\sigma_A} = \sigma_1\sigma_2 \bmod n$, and takes σ_2 as applicable if and only if $h(m)^2 = \bar{\sigma}_A^{2e} \bmod n$. Now, Cloud can get Client's ordinary RSA signature σ_A on significance m from $\bar{\sigma}_A$. If all this do not occur, Cloud intends the help of TTP for link before the exploration of the date.

5. Results & Discussion:

CASE 1: CLIENT IS HONEST, BUT CLOUD IS CHEATING.

If Cloud tricks in any probable way, he cannot study other facts except μ is valid Upon getting the valid assessment of M $_1$, Cloud has to create an option whether he should propel his signature M $_B$ on contract m to Client.

If Cloud can, trusted initiator Client yield back her next partial signature $M_2=h(m)^{d2}$ as Cloud anticipates. In that state, Cloud receives Client's signature on contract m by placing $\mu_A = \mu_1\mu_2$ mod n while Client also gets Cloud's signature μ_B concurrently. If Cloud doesn't submit ^B or only transmits a wrong | μ_B to Client, he can't obtain the significance of μ_2 from ice. Also, in this location, Cloud also can't obtain the value of M_2 from the TTP to ensure Client doesn't get his signature | μ_B. After those values are provided, Cloud certainly obtains μ_2 from the TTP but Client obtains (m, | μ_B) from the TTP, also. Thus, once more, Cloud as well as Client takes the other's signature on contract m as well.

CASE 2: CLOUD IS HONEST, BUT CLIENT IS CHEATING.

In our signature change prototype, Client may deceive in any or a few of the subsequent steps: step (i), step (2), and step (4). Initially, along with the requirement of our signature exchange prototype, to obtain the signature on contract from the truthful responder Cloud, the originator Client has to induce Cloud processing as a valid fractional signature in step (2). Step (2) is verification prototype for RSA indisputable signatures, also that their prototype meets the property of reliability. The reliability indicates that the probable cheating Client (prover), still computationally absolute, can't induce Cloud (verifier) to admit an unacceptable as suitable with non-negligible prospect. So, we determine that to obtain from Cloud, Client has to propel suitable (with valid CA and VA) in step (1) and complete truthfully in step (2). Client is not so ridiculous by creating and submitting to Cloud. Cloud can constrain her concealed key (and then calculate signature | μ_B.

6. CONCLUSION:

In this paper, we proposed an effective attribute revocation method for the Multi-authority CP-ABE method.

Volume No:2, Issue No:10 (March-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Also, we proposed third party auditor can audit the data for data loss and attack in the multi-authority CP-ABE method. We construct the effective data access method for multi-authority cloud storage. This technique, which can be applied in any social networks and cloud data center's etc. Incorporating secure cloud storage with the projected cryptographic remedy and with a searchable encoding strategy for the data to be viewed, it will perform as a better strategy to the individual to provide safety of data. The cloud safety with cryptography is definitely in use for safe data storage that can be improved for secure data relaying as well as storage. An intriguing concern in this system is if we can develop a strategy to attain both public verifiability and storage correctness guarantee of compelling data. Also, including our research on compelling cloud data storage, we even intend to examine the issue of fine-grained information error localization.

REFERENCES:

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[3] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute- Based Encryption and (Hierarchical) Inner Product Encryption," in Proc. Advances in cryptology-EUROCRYPT'IO, 2010, pp. 62-91.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, andW. 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.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[6] J. Hur and D. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, 2010.

[7] 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.

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM Conference on Computer and Communications Security, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 735-737.

[9] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[10] S. Vishnupriya, C. swathi and Lina Dinesh, "Improved Privacy of Cloud Storage Data users by Using Enhanced Data Access Control Scheme for Multi-Authority Cloud Storage," in International Journal of Computer Science & Communication Networks, vol 4,2014, pp 165-168.

[11] Kan Yang and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," in IEEE transactions on parallel and distributed systems, vol. 25, no. 7, july 2014, pp 1735-1744.