The Data Sharing with Access Privilege to User Revocation of Cloud Data

[1]Pitta Kantarao, [2]Dakineni Durga Prasad
[1,2]Dept. of Computer Science, BITS, Visakhapatnam, India

Abstract

Cloud computing empowers on request access to shared origination of assets, this is the most recent pattern in today's IT industry. Among various administrations gave by cloud, cloud storage benefit permits the data proprietors to store and share their data through cloud and in this manner turn out to be free from the weight of storage administration. Cloud storage is rapidly turning into the technique for choice. Securing documents remotely rather than by locally brags a variety of inclinations for both home and expert customers. Cloud storage signifies "the storage of data online in the cloud", in any case, the cloud storage is not totally trusted. Whether the data set up away on cloud are or not transforms into a huge worry of the customers additionally get to control turns into a troublesome occupation, especially when we share data on cloud servers. To handle this issue outsourcing Revocable IBE plot for proficient key era and key redesigning procedure is present. Additionally to enhance the effectiveness of cloud server as far as storage new secure data self-destructing system in cloud registering is utilized. On the off chance that the qualities connected with the figure content fulfill the keys get to structure and both the time moment is in the permitted time interim then the figure content is decoded. After a client indicated end time the data at cloud server will be safely self-destructed.

Keywords

Cloud Computing, Outsourced, IBE, Access control, Access key, Cloud Storage, Integrity, Policy, Revocation

I. Introduction

Identity based encryption system permit any client to produce an open key from a referred to character esteem, for example, an ASCII string. There is trusted outsider, called the Private Key Generator (PKG), who creates the comparing private keys. For encryption and decoding operations, PKG first distributes an ace open key, and after that create the relating expert private key (alluded as ace key). Utilizing this ace open key, any client can create an open key comparing to the identity by consolidating the ace open key with the character esteem. To get a relating private key, approved client can utilize character ID contacts PKG, which utilizes the ace private key to create private key for identity ID. Thus, client can encode messages with no earlier appropriation of keys between members. This is extremely helpful in situations where redistribution of keys is badly designed on account of specialized limitations. In any case, for unscrambling of message, the approved client must get a proper private key from PKG. In this approach the issue is that PKG must be exceptionally trusted, as it has capacity to create any clients private key and unscrambling of message without approval. Since any client's private key can be produced utilizing outsider's mystery, this system has inborn key confirmation. An alternate systems have been proposed which evacuate this including endorsement based encryption and secure key issuing cryptography. In PKI setting, revocation is finished by affixing legitimacy periods to endorsements or utilizing mixes of methods. However, this require administration of declarations which is definitely the weight that IBE endeavors to mitigate. Boneh and Franklin proposed that their private keys can reestablished by client occasionally and senders utilize recipients identity with current day and age. Be that as it may, this component would brings about an overhead at PKG. In another word, every one of the clients despite the fact that their keys have been renounced or not, need to contact with private key generator(PKG) occasionally to demonstrate their characters and overhaul new private keys. It is required that PKG must be on the web and the safe channel must be kept up for every one of the exchanges, which will end up being a bottleneck for IBE system as the quantity of clients develops. Numerous organizations vast and little utilize cloud registering today either specifically or in a roundabout way rather than conventional on location choices. There are various reasons like Reduction of costs, Universal get to and numerous more in view of which cloud registering is so broadly utilized among organizations today. In this manner it require another working worldview for bringing cloud administrations into IBE revocation to settle the issue of effectiveness and storage overhead. A credulous approach is hand over the private key generators (PKG) ace key to the Cloud Service Providers (CSPs). The CSPs then just upgrade all private keys by utilizing the customary key overhaul procedure and exchange the private keys to unrevoked clients. Be that as it may, this approach depends on an improbable presumption that CSPs are completely trusted and are permitted to get to the ace key for IBE system. In any case, by and by people in general clouds are likely outside of the same trusted space of clients and are interested about clients singular protection. Thus, a test is the means by which to plan a safe revocable IBE conspire so we can lessen the overhead calculation at PKG with an untrusted CSP is raised.

II. Related Work

Adel Binbusayyis* and Ning Zhang had proposed Decentralized Attribute Based Encryption Schemes. Existing progresses in the direction of decentralized ABE can be ordered into two classifications relying upon how the trait powers are organized: multi-power ABE and various leveled ABE. In the setting of multi-power ABE, a few credit powers participate to deal with the characteristics in a system. Every characteristic power is given a remarkable arrangement of qualities. A client may need to ask more than one power with a specific end goal to acquire his/her qualities. One of the security difficulties is the means by which to oppose the conspiracy assault of vindictive clients. The Chase work accomplishes intrigue resistance by presenting a Global Identifier (GID) given to every client mystery key. Every one of the clients mystery key parts from various powers will be attached to his GID. In any case, to make the figure content be free of the clients GID, a focal power must be utilized to issue an exceptional mystery key for the client utilizing his mystery key and alternate powers mystery keys. Lekwo and Waters proposed a multiauthority ABE conspire that does not require either focal power or collaboration between the different powers. They utilize a hash work on the client worldwide ID to oversee agreement resistance and tie clients mystery key segments together. Notwithstanding, this plan is not sufficiently reasonable to be connected on our situation in light of the fact that every power needs to know all clients GID ahead of time. Likewise, they don't consider how to decrease the workload on a trait power when it needs to handle huge number of clients in expansive scale system. [6]Wan et. al. proposed a various leveled property set-based encryption (HASBE) plot. Like our CP-DABE plot, their plan requires a client just to speak with his/her managing trait power, as opposed to with more than one quality power as the case in. Be that as it may, the HASBE plot has two downsides contrasted and our CP-DABE conspire. The first is that our CPDABE calculations are speedier than the HASBE calculations as far as the computational cost. In the decoding calculation, for instance, in the HASBE conspire, the unscrambling requires two matching operations for each leaf hub used to fulfill the tree, one blending for each deciphering hub on the way from the leaf hub used to the root, and one exponentiation for every hub on the way from the leaf hub to the root. In any case, in our CP-DABE plot, the unscrambling calculation requires just a single matching guide for every ascribe used to fulfill the get to structure. The second downside is that the HASBE plan is just demonstrated secure in the bland security show, while our CP-DABE plan is formally demonstrated against picked plaintext assaults under the decisional Bilinear Diffie-Hellman Exponent supposition. [12]Qingwei Zhang, Mohammed Almulla proposed Revocation Schemes. Client revocation is the demonstration of expelling benefits from a client so that the client can no longer get to the data records. To deny a client, the data proprietor needs to upgrade every one of the properties keys (i.e. trait open keys and characteristic ace keys) that have been utilized to infer the denied clients keys (i.e. client trait mystery keys). As a result of overhauling the characteristics keys, the data proprietor likewise needs to upgrade all other influenced clients keys (i.e. client quality mystery keys) and re-scramble every data that have been related from with any of these denied traits. [13]Pervez, Z. et. al. proposed making another get to arrangement with every data document, which contains all the approved clients IDs. To deny a client, the data proprietor will just need to expel the renounced clients ID from the get to strategy. This is a clear arrangement, however not down to earth for extensive systems since the data proprietor should know the every one of the clients IDs from the earlier. To handle this issue, a lapse time based revocation procedure is proposed, which relates an ascribe called close time to every client mystery key.

III. Problem Definition

A. Problem Definition

Cloud computing relies on sharing computing resources rather than having local servers or personal devices to handle applications and used as a metaphor for the internet so the phrase cloud computing means a type of internet based computing. To apply traditional supercomputing or high performance computing normally used by military and research to perform such as financial portfolios to deliver personalized information to provide storage or to power large uses networks of large groups of servers.

Cloud computing provides clients with a virtual computing infrastructure on which they can store data and run applications, introducing new security challenges since cloud operators are expected to manipulate client data without necessarily being fully trusted.

Cloud computing provides cryptography even in order to realize scalable flexible and fine grained access control of outsourced data, we analyze encryption methods and priority hierarchical structure of users.

Encryption is the conversion of data into a form called a cipher text that cannot be easily understood by unknown persons and decryption is the process of converting encrypted data return into its original form. Use of encryption/decryption is art of communication cipher often incorrectly called a code can be employed to keep the enemy from obtaining the contents of transmissions. In order to easily recover the contents of an encrypted signal the correct decryption key is required alternatively a computer can be used in an attempt to break the cipher. Fact that encryption might be accidently utilized on something that was not meant to be encrypted and the person who was meant to obtain the message may not be able to read the message sent to them, may not be strong enough and therefore others may be able to easily interpret information. Hierarchical structure of system users to achieve scalable flexible and fine grained access control low initial capital investment and maintenance.

B. Analysis for the Above Problem

Cloud server is either proportional to the number of system attributes or linear to the size of the user access structure tree achieved. Our construction also protects user access privilege information again cloud server.

Method for Hierarchical Attribute Solution:

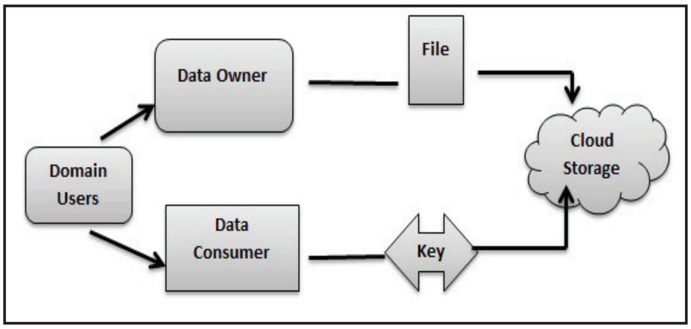

Fig. 1: Proposed Model

Data owner uploads the data in the cloud server for the security purpose, owner encrypts the file and store in the cloud and owner as rights to change the policy over data files by updating the expiration time.

Data Consumer user can only access the data files with the encrypted key if the user has the privilege to access the file. For all user level all the privilege is given by the domain authority and the data users are controlled by the domain authority.

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 consumer download encrypted data files.

Authority person is responsible for generating and distributing system parameters and root master keys as well as authorizing the high level domain authorities. Domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain.

IV. Encryption Methods in Cloud Computing

To achieve security and quality of data, it is very important to provide encryption and signature based scheme.

A. Identity Based Encryption

Identity based encryption cryptography is a third party server uses a simple identifier as an email address to generate key that can be used for encrypting and decrypting electronic data. Typical public key cryptography greatly reduces the complexity of the encryption process for users. Identity based encryption depends on the third party identity based encryption server that generates private keys, information stores permanently is a secret master key a large random number that is exclusive to the security domain. The server uses this key to create a common set of public key parameters that are given to each user, the persons who are installed the identity based encryption software setup. When an outsourcing sender creates an encrypted message the identity based software on his system uses three parameters to generate the public key for the message.

B. Linear Search Algorithm

A symmetric encryption algorithm is used to encrypt the plain text for the cipher text of each keyword under symmetric encryption scheme a pseudo random sequence is generated with a length less that of the cipher text. At the same time check sequence is generated based on the pseudo random sequence and the cipher text. The sum of the lengths of the pseudo random sequence and the check sequence equals the length of the cipher text, the sum of the lengths pseudo random sequence equals the length of the cipher text.

C. Identity Based Signature

Identity based signature scheme is deterministic if the signature on a data by the same user is same, setup generates a private key provides the security parameter as the input to this algorithm generates the systems parameters and master private key. User extract his identity to private key generates as input and obtains the private key D and send to user through a secure channel. For generating a signature on a message m the users provides his identity private key D parameters and the message as input, the algorithm generates a valid signature on message by the user.

D. Attribute Based Encryption

The attribute and policies associated with the message and the user decides which user can decrypt a cipher text; the authority will create secret keys for the users based on attribute for each user. Users in the system have attributes receives a key from an authority for its set of attributes. Cipher text contains a policy predicate over the attribute space.

E. Homomorphic Encryption

Homomorphic encryption is cryptography which promises to make cloud computing perfectly secure a web user would send encrypted data to a server in the cloud, without decrypting it and send back a still encrypted result data. Sometimes however the server needs to know something about the data its handling otherwise some computational tasks become prohibitively time consuming if not outright impossible. Suppose for instance the task we outsourced to the cloud is to search a huge encrypted database for the handful of records that match an encrypted search tem. Homomorphic encryption ensures that the server has no idea what the search term or which records matches it. As a consequence however it has no choice record in the database. The user's computer can decrypt that information to see which records matched and which did not match then assuming much of the computational burden that was trying to offload to the cloud in the first.

V. Proposed System

In order to achieve efficient revocation, we introduce the idea of "partial private key update" into the proposed construction, which operates on two sides: (1) Utilized "hybrid private key" for each user in our system, which employs an AND gate connecting two sub-components namely the identity component (IK) and the time component respectively (TK). IK is generated by PKG in key-issuing but is updated by the newly introduced KU-CSP in key update; (2) In encryption, we take as input users identity as well as the time period T to restrict decryption, more precisely, a user is allowed to perform successful decryption if and only if the identity and time period embedded in his/her private key are identical to that associated with the ciphertext. Using such skill, we are able to revoke users decryption through updating the time component for private key by KU-CSP. Moreover, we remark that it cannot trivially utilize an identical updated time component for all users because revoked user is able to re-construct his/her ability through colluding with unrevoked users. To eliminate such collusion, randomly generated an outsourcing key for each identity, which essentially decides a "matching relationship" for the two sub-components. KU-CSP maintain a list UL to record user"s identity and its corresponding outsourcing key. In key-update, we can use OKID to update the time component TK[ID] T for identity ID . Suppose a user with identity ID is revoked at Ti . Even if he/she is able to obtain TK[ID`]Ti+1for identity ID` , the revoked user still cannot decrypt ciphertext encrypted under Ti+1.

The following fig. 2 shows the proposed system architecture.

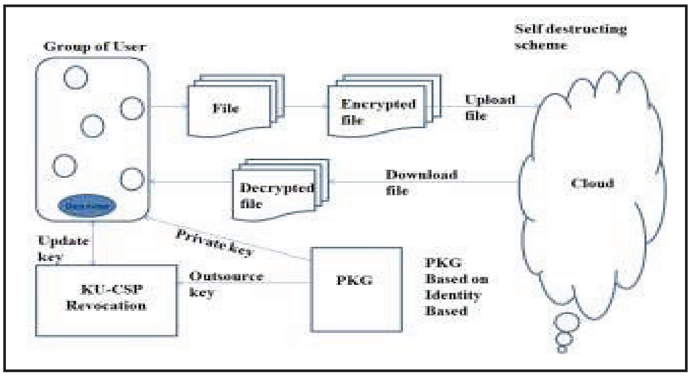

Fig. 2: Proposed System

A. System Overview

The user registers himself at server and then login with valid username and password in to system. After login, user request for keys to KU-CSP [1]. The user / owner encrypt the files using the keys and uploaded these files at cloud server for specific time interval and become free from the burden. When any user leave the group ,the list of remaining user is send to KU-CSP, where the KU-CSP generate the new key or update the keys to maintain the security of the system and send the new keys to the key requested user. At cloud server if the specified time for the file is end then the file is destructed / delete from the server and it is no longer available for users. This increases the storage space at cloud server.

In previous work the system stores the data at cloud server and the user itself has delete the data stored at cloud if he no longer needed the data, it increases overhead of user and also uses more space at cloud server, to overcome the drawback of previous system, the system pro-poses data self-distractive scheme, In this user upload the data at cloud server for specific time duration (for example, 2/2/2016-2/2/2017,).at cloud server data is valid for only one year i.e. from start date to end date specified by user after completion of time period data is self-destructed from the cloud and it frees the space at cloud server.

B. Self-Destructing Scheme

A Self-Destructing Scheme called key-policy identity based encryption with time specified attributes scheme, which is based on inspection that, in sensible cloud application situation, every data item can be linked with a set of attributes and each attribute is linked with a specification of time interval, indicating that the encrypted data item can only be decrypted between on a specified date and it will not be recoverable that day. In which every users key is associated with an access tree and each leaf node is associated with a time instant the data owner encrypts his/her data to share with users in the system. As the logical expressionof the access tree can signify any desired data set with any time interval, it can attain fine-grained access control. If the time instant is not in the specified time interval, the ciphertext cannot be decrypted, i.e., this ciphertext will be self-destructed and no one can decrypt it because of the expiration of the secure key. Therefore, secure data self-destruction with fine-grained access control is attained. In order to decrypt the ciphertext effectively, the valid attributes should gratify the access tree where the time instant of each leaf in the users key should belong to the in the matching attribute in the ciphertext.

C. Algorithm

1. Setup ( ): PKG run the setup algorithm. It chooses a random generator g 2R G as well as a random integer x 2R Zq and sets g1 = gx. Then, A random Element PKG picked by g2 2R G and two hash functions H1; H2: f0; 1g! GT. Finally, output the public key PK= (g; g1; g2; H1; H2) and the master key MK = x.
2. KeyGen (MK, ID, RL, TL, and PK): PKG firstly checks whether there quest identity ID exists in RL, for each user‟s private key request on identity ID, if so the key generation algorithm is terminated. Next, PKG randomly selects X1 2R Zq and sets x2 = x x1. It randomly chooses, and computes. Then, PKG reads the current time period Ti from TL. Accordingly, it randomly selects Ti 2R Zq and computes, where and finally, output SKID = (IK [ID]; TK [ID] Ti) and OKId = x2.
3. Encrypt (M, ID, Ti+, and PK): Assume a user needs to encrypt a message M under identity ID and time Ti period. He/She chooses a random value s 2R Zq and computes, C0 = Me (g1; g2) s; C1 = gs; EID = (H1 (ID)) s and Finally, publish the ciphertext as CT = (C0; C1; EID; ETi).
4. Decrypt (CT; SKID; PK): Assume that the ciphertext CT is encrypted under ID and Ti, and the user has a private key SKID = (IK[ID]; TK[ID]Ti), where IK[ID] = (d0; d1) and
   TK[ID]Ti = (dTi0; dTi1).
5. Revoke(RL; TL; {IDi1; Idi2; ::::Idik}) : If users with identities in the set {IDi1; Idi2; ::::Idik} are to be revoked at time period Ti, PKG updates the revocation list as RL0 = RL{IDi1; Idi2; ::::Idik} as well as the time list. Through connecting the recently created time period Ti+1 onto original list TL. Finally send a copy for the updated revocation list as well as the new time period Ti+1 to KUCSP.
6. Key Update (RL; ID; Ti+1; OKID): Upon receiving a key update request on ID , KU-CSP firstly checks whether ID exists in the revocation list RL , if so KU-CSP returns and key-update is terminated. Other-wise, KU-CSP gets the corresponding entry (ID; OKID = x2) in the user list UL.

Then, it randomly selects Ti+1 2R Zq.

7. Data self-destruction after end: Previously the current time instant tx lags behind after the threshold value (expiration time) of the valid time interval tR; x, the user cannot obtain the true private key SK. Therefore, the ciphertext CT is not capable to be decrypted in polynomial time, ease the selfdestruction of the shared data after end.

D. Complexity Analysis

Time Complexity of ECC is O (n).

E. Mathematical Model

System S is represented as S= {U, CS, KU-CSP}
1. User US = {R, L, Q, E, V}
Where,
R= Registration Process
L= Login Process
Q= Key Request Process
E= File Encryption Process
V= Revocation Process

2. KU-CSP={PK,SK}
Key Generation PK={pk1, pk2, pk3 ...pkn} Where PK is the set of generate public keys.
SK= {sk1, sk2, sk3 ...skn}
Where SK is the set of generate private keys related to public key.

3. Cloud Server CS ={U, D}
Where,
U = Upload file
D= {T, F}
Where,
D = Self-Destructive Process
T=Time Interval
F=Number of files

F. Dataset

The System uses multiple files with various sizes from 1 KB to 100 MB as dataset.

G. Experimental Setup

The system used Netbeans (version 8.0) tool for development and Java framework (version jdk 1.8) on Windows platform as a front end. Any standard machine is capable of running the application. The system doesn't need any specific hardware to run.

VI. Conclusion

In this paper, concentrating on the basic issue of character repudiation, we bring outsourcing calculation into IBE and propose a revocable plan in which the repudiation operations are assigned to CSP. With the guide of KU-CSP, the proposed plan is full-highlighted: (1) It accomplishes consistent productivity for both calculation at PKG and private key size at client; (2) User needs not to contact with PKG amid key update, as it were, PKG is permitted to be disconnected from the net after sending the denial rundown to KU-CSP; (3). No secure channel or client verification is required amid key-overhaul between client and KU-CSP.Moreover, we consider acknowledging revocable IBE under a more grounded enemy model. We exhibit a propelled development what's more, demonstrate to it is secure under RDoC model, in which in any event one of the KU-CSPs is thought to be completely forthright. In this manner, regardless of the possibility that a repudiated client and both of the KU-CSPs conspire, it can't to offer.

References

[1] Boneh, Franklin mechanism, R. Schlegel, D. S. Wong, C. Tang," Conditional proxy broadcast reencryption scheme supporting timed- release", In Proc. 9th Int. Conf. Inf. Security Practice Experience, 2013, pp. 132– 146.

[2] Adel Binbusayyis, Ning Zhang, C. Tang,"A CCAsecure identity-based conditional proxy re-encryption without random oracles", In Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–146.

[3] A. B. Lewko, B. Waters,"Decentralizing attributebased encryption", In EUROCRYPT'11. Springer, 2011, pp. 568–588.

[4] J. Kenney,"Dedicated Short-Range communications (DSRC) standards in the united states", Proceedings of the IEEE, Vol. 99, No. 7, pp. 1162– 1182, Jul. 2011.

[5] L. Harn, J. Ren,"Generalized digital certificate for user authentication and key establishment for secure communications", Wireless Communications, IEEE Transactions on, Vol. 10, No. 7, pp. 2372–2379, Jul. 2011.

[6] Wan et. al, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Public Key Cryptogra- phyPKC 2011. Springer, 2011, pp. 5370.

[7] PierangelaSamarati, Sabrina De Capitani di Vimercati, "Data Protection in Outsourcing Scenarios: Issues and directions", E-Business and Telecommunications: 6th International Joint Conference, ICETE, 2011.

[8] C.-K. Chu, J. Weng, Chase, S. S. M. Chow, J. Zhou, R. H. Deng,"Conditional proxy broadcast re-encryption", In Proc. 14th Aus- tralasian Conf. Inf. Security Privacy, 2009, pp. 327–342.

[9] Q. Tang,"Type-based proxy re-encryption and its construction", In Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008, pp. 130–144.

[10] L. Ibraimi, Q. Tang, P. Hartel, W. Jonker,"A typeand-identity-based proxy re-encryption scheme and its application in healthcare", In Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.

Pitta Kantarao is currently pursuing his M.Tech(CST) in BITS, Visakhapatnam. He received his B.Tech from Kaushik College of Engineering, Visakhapatnam.

Dakineni Durga Prasad is working as an Assistant professor in Baba institute of technology and science. He is having 9 years of experience.