International Journal of Science Engineering and Advance Technology

The Multi Owner Data Distribution using Identity Based Encryption on Cloud Storage

[1]V.R.S.S.D.Sireesha
[1](P.G.STUDENT) M.Tech in CSE
Dept. computer science and engineering
Kakinada Institute of Engineering and Technology for Women,
Korangi,AP,INDIA

[2]Mrs. A.Vishnupriya
[2] Assistant Professor in CSE
Dept. computer science and engineering
Kakinada Institute of Engineering and Technology for Women,
Korangi,AP,INDIA

Abstract—

Data sharing has never been anything but difficult to the progression of cloud computing. The storage data gives number of advantages to both the general public and people. Storage-as-an administration possible by cloud specialist co-ops (CSPs) is paid capacity that empowers associations to assign their delicate data to be put away on out of reach servers. This paper proposes a cloud based storage technique that permits the data proprietor to profit by the comforts offered by the CSP and empowers trust between them. Character based (ID-based) ring mark, which evacuates procedure of authentication check, can be utilized as a substitute. In this paper, we proposed the security of ID-based ring mark by giving forward wellbeing: If a top mystery key of any client has been bargained, all previous created marks that incorporate this client still longer substantial. This property is particularly imperative to any expansive scale data conveyance framework, as it is impractical to ask all data proprietors to again confirm their data regardless of the possibility that a mystery key of any client has been bargained. It permits the proprietor to financing or disavow induction to the outsourced data.

Index Terms: Identity based encryption (IBE), revocation, outsourcing, cloud computing.

I. Introduction

Cloud computing is a general term for anything that includes conveying facilitated presidencies, adaptable administrations like data sharing, getting to and so on., over the web on request premise. It utilizes the web and focal remote servers to keep up data and applications. Cloud computing permits purchasers and organizations to utilize applications without establishment and get to their own documents at any PC with web get to. This innovation takes into consideration substantially more productive figuring by bringing together storage, memory, preparing and transfer speed. Cloud computing is separated into three sections: "application" "storage" and "availability". Every section fills an alternate need and offers diverse items for organizations and people the world over. Multi-proprietor data trade is a model for sharing business data of substantial associations, which permits proprietors to make, oversee and control their data/data in cloud. Cloud storage allows an expansive number of clients having diverse parts and get to consents to share and store their data. In arrangement based data sharing, every client has a get to strategy for the framework and every document has some record get to approach which may vary for various clients. In a disseminated domain various duplicates of data is there to enhance accessibility. Henceforth the respectability and get to control are significant concerns. A cloud framework may have many cloud specialist co-ops (CSPs) to enhance the execution of said framework. In view of accessibility and work stack, the framework chooses a CSP for the customer getting to it. Hundreds or a large number of

customers may get to the framework all the while; consequently the accessibility is a noteworthy issue. It can be enhanced by CSPs with data replication. The data proprietors might need to set a few limitations to customers who are attempting to get to the data. In this situation, the disseminated data ought to keep all insights about the diverse get to control arrangements set to data. Be that as it may, again the approved customers ought to be arranged by; it will be an issue in a circulated framework with numerous customers. This framework essentially permits open clients and custom clients. On account of open clients the arrangement is same for all and just open records can be gotten to by them, it is not a testing issue. The second classification, custom clients are some way or another a noteworthy issue. Custom clients are chosen clients who have extraordinary authorizations for getting to a few documents/data. The authorizations might be same or diverse for every custom client. The framework must monitor all the get to arrangements of custom clients and give data/record as indicated by those strategies. We are proposing a framework which bargains various proprietors and numerous approaches to give secured data partaking in cloud.

II. Related Work

IBE is an imperative different to open key mystery composing, that is anticipated to change enter administration in an extremely authentication based Public Key Infrastructure (PKI) by exploitation human-understandable characters (e.g., unmistakable name, email address, IP address, and so on) as open keys. Along these lines, sender exploitation IBE doesn't got the opportunity to discover open key and declaration, however specifically scrambles message with beneficiary's character. thus, recipient getting the individual key identified with the comparing character from individual Key Generator (PKG) is prepared to translate such figure content. however' IBE licenses relate degree eccentric string on the grounds that general society enter that is considered as partner degree engaging favors over PKI, it requests relate degree prudent revocation instrument. In particular, if the individual keys of a few clients get traded off, we have a tendency to ought to offer an intend to disavow such clients from framework. In PKI setting, revocation instrument is acknowledged by attaching legitimacy periods to declarations or exploitation concerned blends of strategies. all things being equal, the lumbering administration of testaments is precisely the weight that IBE endeavors to ease chief authorized by Boneh and Franklin, IBE has been inquired about seriously in crypto rationale group. On the aspect of development, these first plans were demonstrated secure in irregular prophet. Some future frameworks accomplished verifiable secure in standard model underneath specific ID security or versatile ID security. As of late, there are different cross section based developments for IBE frameworks. all things being equal, with respect to on voidable IBE, there's almost no work gave. As said some time recently, Boneh and Franklin's proposal [4] is extra a suitable answer however illogical. Hanaoka et al. anticipated how for clients to sporadically restore their own keys while not associating with PKG. Notwithstanding, the thought required in their work is that each client must have an alter safe equipment gadget. Another answer is moderator supported revocation: amid this setting there's an uncommon semi-trusted outsider alluded to as a go between UN organization helps clients to interpret each figure content. In the event that partner degree personality is denied then the mediator is mentored to avoid serving to the client. Clearly, it's unfeasible since all clients territory unit not able to interpret all alone and that they got the chance to speak with moderator for each coding. As of late, Lin et al. anticipated a territory sparing voidable IBE instrument from non-monotonic Attribute-Based mystery composing (ABE), however their development needs times added substance matching operations for one coding wherever the measure of disavowed clients is. As to such an extent as we as a whole know, the voidable IBE subject presented by Boldyreva et al. remains the chief powerful answer promptly. Libert and Vergnaud enhanced Boldyreva¨s development to acknowledge versatile ID security. Their work focused on security expanded, however acquires the comparative burden as Boldyreva¨s unique development. As we have a tendency to said some time recently, they're short in storage for every individual key at client and double tree structure at PKG. Another work with respect to North American nation starts from Yu et al. The creators used intermediary re-encryption to propose a

voidable ABE topic. The beyond any doubt power exclusively should redesign antiquated partout with regards to property revocation remaining in on each event sum and issue intermediary re-encryption key to intermediary servers. The intermediary servers can then re-encode figure content exploitation the re-encryption key to make positive all the unrevoked clients will perform independent coding. we have a tendency to indicate that an outsider administration provider is presented in each Yu et al. what's more, this work. something else, Yu et al. used the outsider (work as an intermediary) to appreciate revocation through re-scrambling figure message that is only adjust to the uncommon application that the figure content is keep at the outsider. Notwithstanding, in our development the revocation is acknowledged through change individual keys for unrevoked clients at cloud benefit provider that has no restrictions on the circumstance of figure content.

III. **Problem Definition**

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.

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:

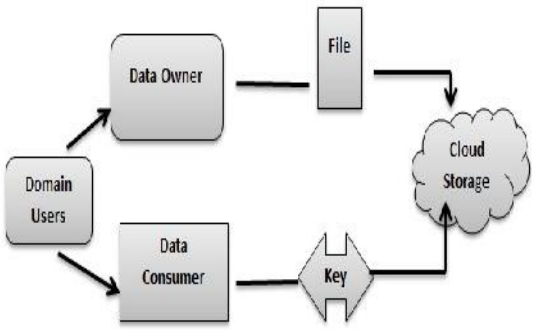

Figure 1 Proposed Model

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.

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.

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.

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.

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.

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.

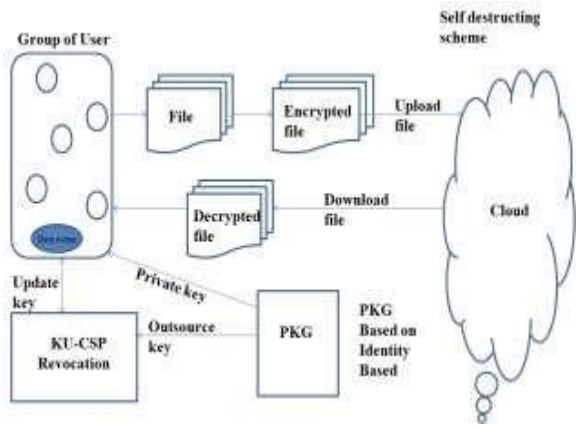

Fig 2: Proposed System

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 and Franklin mechanism, R. Schlegel, D. S. Wong, and C. Tang, ―A con- ditional 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, and 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 and 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 and J. Ren, ―Generalized digital certificate for user authen- tication 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 and 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, and 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, and W. Jonker, ―A typeand-iden- tity-based proxy re-encryption scheme and its application in healthcare,‖ in Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.