IPHV7I20036X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

DECENTRALIZED ACCESS CONTROL OF DATA STORAGE IN CLOUD USING KEY POLICY

[#1] A.DIVYA -M.Tech Pursuing,
[#2] M. Saidi Reddy-Associate Professor, HOD
Department of Computer Science & Engineering,
Malla Reddy College Of Engineering & Technology, Hyderabad.

ABSTRACT: *Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. As guaranteeing as it may be, this standard additionally delivers a lot of people new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. In any case, in completing thus, these results unavoidably present a substantial processing overhead on the data possessor for key distribution and data administration when fine-grained data access control is in demand, and subsequently don't scale well. The issue of at the same time accomplishing fine-grainedness, scalability, and data confidentiality of access control really still remains uncertain. This paper addresses this open issue by, on one hand, characterizing and implementing access policies based on data qualities, and, then again, permitting the data owner to representative the majority of the calculation undertakings included in fine-grained data access control to un-trusted cloud servers without unveiling the underlying data substance. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption (KP-ABE) . Extensive investigation shows that the proposed approach is highly efficient and secure.*

Keywords: *Access Control, Cloud Computing, Key Policy Attribute Based Encryption (KP-ABE)*

I. INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet. It is a new business solution for remote reinforcement outsourcing, as it offers a reflection of interminable storage space for customers to have data reinforcements in a pay-as-you- go way [1]. It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now store their data reinforcements remotely to third-party cloud storage suppliers as opposed to keep up data centers on their own. Numerous services like email, Net banking and so forth… are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity.

To accomplish secure data transaction in cloud, suitable cryptography method is utilized. The data possessor must encrypt the record and then store the record to the cloud. Assuming that a third person downloads the record, they may see the record if they had the key which is utilized to decrypt the encrypted record. Once in a while this may be failure because of the technology improvement and the programmers. To overcome the issue there is lot of procedures and techniques to make secure transaction and storage.

IPHV7I20036X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Recently [2] addressed Anonymous authentication for data archiving to clouds. Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients to conceal their details from other clients of that cloud.

Security and privacy assurance in clouds are analyzed and tested by numerous researchers. [3] gives storage security utilizing Reed-Solomon eradication correcting codes. Utilizing homomorphic encryption, [4] the cloud gains cipher text and furnishes an encoded value of the result. The client has the capacity to translate the result; however the cloud does not comprehend what data it has worked on.

In this paper key policy Attribute Based Encryption scheme is used to control unauthorized access. In addition revocation scheme is used for time based file assured deletion.

II. RELATED WORK

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud. [5][6] Studied the access control in health care.

Access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social networking has been studied in [7].

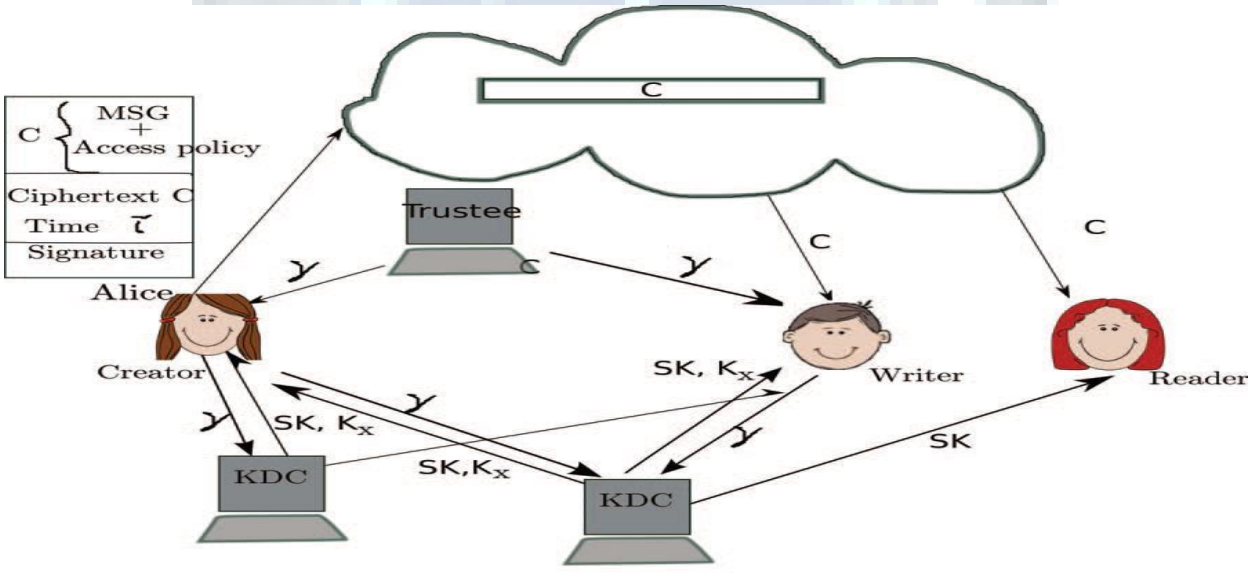


Fig 1 Cloud Architecture

The work done by [8] gives privacy preserving authenticated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. The scheme

In [9] uses a symmetric key approach and does not support authentication.

Multi-authority ABE principle was concentrated on in [10], which obliged no trusted power which requires each client to have characteristics from at all the KDCs.

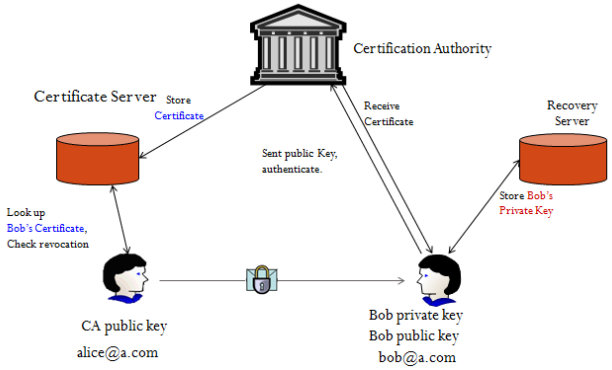
In spite of the fact that Yang et al. [11] proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud. Ruj et al. [12] proposed a distributed access control module in clouds. On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store an record and different clients can just read the record. write access was not allowed to clients other than the originator.

Time-based file assured deletion, which is initially presented in [13], implies that records could be safely erased and remain forever difficult to reach after a predefined time. The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key is further encrypted with a control key by a separate key Manager.

Public Key Infrastructure (PKI)

In public key infrastructure (PKI) systems [1], a certificate is used to bind an encryption key to a user identity (such as an email address) via a registration process. When this process is tightly controlled and combined with digital signing technologies, the certificate can give a strong assurance that only the indicated user can access messages encrypted with The key contained in the certificate. To communicate securely to a certificate holder, a potential sender (who also must have a certificate) needs to obtain the certificate of the recipient, and then use it to encrypt the message. PKI, particularly in combination with smartcards, can provide robust user authentication and strong digital signatures. When strong controls are enacted around certificate registration, and when user's private keys are well protected from compromise (i.e., stored on a smartcard), certificates enable strong authentication. PKI seems to be an ideal mechanism for enabling encryption as well, but a few significant hurdles present themselves. First, there is the pre-enrollment problem. Here recipients must already have a certificate before they can be sent a message. Second, the sender must obtain the certificate of the recipient, which is generally published via a directory, this introduces problems of trust (does the sender trust the issuer of the recipients certificate) and information leakage (has the directory given spammers and phishes a source of fully qualified email addresses). Finally, while the binding between certificate and identity was true at the time of issuance, there is no guarantee that it remains true after that single point in time. This means that senders must first confirm the validity of recipient's certificates before sending, this is the certificate revocation problem. Even if certificates can be found for all recipients, the validity of these certificates must be determined before a message can be sent. Typical approaches for checking certificate status have been to publish CRLs (certificate revocation lists), which must be frequently updated, or stand up high volume OCSP (online certificate status protocol) servers, which must be accessed by every sender before every send. In either case, senders must be on-line to obtain current information, or to send to recipients with whom they have not previously communicated. Users will always be entering and leaving systems, permissions will change, and private key compromises will occur, anytime any of these eventshappens, all other users will need to be informed via one of the indicated mechanisms. And in the real world, both in the public and private sector, communications must often be secured to recipients who do not even have certificates to begin with. PKI is suited for providing strong authenticating mechanism for providing the full range of message security services.

IPHV7I20036X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245



Advantages:
* Strong authentication of users (especially with Smart cards)
Disadvantages:
* Users (senders AND recipients) must be pre-enrolled. Certificate directories can leak critical information.

Cipher text policy attribute based encryption (CP-ABE)

Attribute-based encryption (ABE), as introduced by Sahai and Waters, allows for fine grained access control on encrypted data. In its key-policy (the dual cipher text-policy scenario proceeds the other way around), the primitive enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which cipher texts the key holder will be allowed to decrypt. These results were extended by Goyal et al. [6] into richer kinds of attribute-based encryption, where decryption is permitted when the attribute set satisfies a more complex Boolean formula specified by an access structure. Since ABE is the generalization of IBE, every arbitrary string is utilized as a valid public key for an attribute. The trusted authority, called the key generation center (KGC), is responsible for the generation of private keys for every user after user authentications. The KGC generates private keys for users by applying the KGCs master secret keys to their associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storage of public key certificates under traditional public key infrastructure (PKI). CP-ABE scheme consist of four fundamental algorithms. Setup, KeyGen, Encrypt, and Decrypt. In setup phase, setup the public parameter PK and a master key MK. In the key generation phase generate the secret key based on set of attributes and master key. In the encryption phase message is encrypted with access policies and public key. And produce a cipher text. In decryption phase decrypted by using private key and access structure, and returns a message.

Certificate Based Encryption (CBE)

Certificate less public key encryption (CLE) and certificate based encryption (CBE) [4] are two novel public key cryptographic primitives requiring no authenticity verification of the recipient's public key. Both of them are motivated to simultaneously solve the heavy certificate management problem inherent in the traditional public key encryption (PKE) and the key escrow problem inherent in the identity-based encryption (IBE). It is an attractive cryptographic task to formally explore the relation between CBE and CLE. In 2005, Al-Riyami and Paterson proposed one general conversion from CLE to CBE. Shortly later, Kang and Park pointed out a law in the security proof of Al-Riyami-Paterson conversion. In 2012, Wu et al. proposed another generic conversion from CLE to CBE. Compared with Al-Riyami-Paterson conversion [5], Wu et al.s method can be proved secure, but it has to additionally involve collision resistant hash functions. It remains an open problem whether the generic conversion due to Al-Riyami and Paterson, which is very neat, is provably secure.

We aim to solve this open problem. First, we formalize CLEs new security model, featured by introducing a new security property overlooked by previous security models. With this new security model as the basic technique, we succeed in proving that the Al-Riyami-Paterson generic conversion from CLE to CBE is secure .Certificate-based encryption (CBE) is a new public key encryption mechanism introduced by Gentry. As in the traditional PKI, each client in CBE generates its own public/private key pair and the Certificate Authority (CA) then generates a certificate which can guarantee the authenticity of the client's public key. In CBE, the certificate has an additional feature, namely it also acts a partial private key. A (IBC) successful decryption requires both the private key and the up-to-date certificate. This provides an implicit verification of one's certificate and eliminates third-party queries for certificate status required in traditional PKI. Since CA does not know the clients private key, there is no key escrow problem in CBE. It has six fundamental algorithms. Such as setup, setup key pair, certification, Consolidate, Encrypt and decrypt. In set up phase set the security parameter returns the master key and system parameters. Key pair is generated from input parameter and output the public key and secret key. Certify by using master key, security parameters and producing the client identifying information and public key.

Advantages:
*Certificate management. Certification revocation listis not needed. No key escrow.
Disadvantages:
* Certificate can leak the critical information.

III. PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows

Setup:
This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:
It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:
It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption:
It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion

The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased.

To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

IV. CONCLUSION

We have introduced a decentralized access control system with anonymous authentication, which gives client renouncement also prevents replay attacks. The cloud does not know the identity of the client who saves data, however just checks the client's certifications. Key dissemination is carried out in a decentralized manner. One limit is that the cloud knows the access strategy for each one record saved in the cloud.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Comm. of the ACM, 53(4):50–58, Apr 2010*.
2. Sushmita Ruj, Milos Stojmenovic and Amiya Nayak,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.*
3. Wang, Q.Wang, K.Ren, N.Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T.Services Computing, Vol. 5, no.2, pp. 220-232, 2012.*
4. C.Gentry, "A fully homomorphic encryption scheme", *Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.*
5. personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in *SecureComm, pp. 89–106, 2010.*
6. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ACM ASIACCS, pp. 261–270, 2010.*
7. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS, 2011*.
8. F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, *vol. 6672. Springer, pp. 83–97, 2011*.
9. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *ACM Cloud Computing Security Workshop (CCSW)*, 2009.
10. M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009.*
11. Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", *IACR Cryptology ePrint Archive*, 419, 2012.
12. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEE TrustCom, 2011*.
13. . Perlman, "File System Design with Assured Delete," *Proc.Network and Distributed System Security Symp. ISOC (NDSS), 2007.*

AUTHOR'S PROFILE:

[1]. A.DIVYA , Pursuing M.Tech in Department of Computer Science & Engineering at Malla Reddy College Of Engineering & Technology, Hyderabad,Telangana.India.

[2]. M. Saidi Reddy, pursuing Ph.D, working as Associate Professor & Head of The Department of Computer Science & Engineering, Malla Reddy College Of Engineering & Technology, Hyderabad, Telangana.India.