International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-4, April 2013

A Serial Based Encryption for Enhanced Access Control in Cloud Computing

N.Pandeeswari, P.Ganesh Kumar, P.C.Rubini

Cloud storage allows us to enjoy the on demand cloud application without any hardware implementation. Cloud provides the service a required by the cloud user in a rental basis. Even though the cloud issues the cloud application without any physical implementation results in a security risk since the cloud data can be accessed by everyone. To avoid security issue in the outsourced data a prevention measure is needed to secure the data from unauthenticated users or intruders. A flexible distributed storage integrity mechanism utilising homomorphic tokens and is proposed in this paper to provide security in the outsourced cloud data. This mechanism include the techniques such In order to address security for outsourced data and secure cloud storage, we propose in this paper a flexible distributed storage integrity checking mechanism, utilizing the homomorphism token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very low computation cost and lightweight communication. The auditing result not only guarantees strong cloud storage correctness, but also simultaneously identifies fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack.

I. INTRODUCTION

In an effort to attain improved gain, businesses are progressively more focusing on new and recent ways to have an enhanced infrastructure providing large profit while demanding less investment. All the developing businesses searching for resources are assisted by Cloud computing. The cloud computing is considered as fifth utility after the four basic utilities [1].Cloud computing provides three basic types of services such as Infrastructure as a service (Iaas) provides cloud user almost all equipments such as hardware, storage, servers and networking components, Platform as a service (Paas) which includes hardware and software computing platforms, Software as a service (Saas) Cloud user can access software application. Many software industries utilises the cloud computing as there technical source namely Amazon EC2[2],Amazon's S3[3] uses Iaas where as Google App Engine[5] comes under Pass system and Google Apps[7] and Sales force Customer Relational Management(CRM) belongs to Saas system .

Manuscript published on 30 April 2013.
***** Correspondence Author (s)
N.Pandeeswari, Assistant Professor, M.E Student Dept. of IT, PSNA College of Engineering and Technology Dindigul, TamilNadu, India.
P.Ganesh Kumar, Professor, M.E Student Dept. of IT, PSNA College of Engineering and Technology Dindigul, TamilNadu, India.
P.C.Rubini, M.E Student Dept. of IT, PSNA College of Engineering and Technology Dindigul, TamilNadu, India.

Although the cloud provides exciting services cloud security is a greater issue. One of the issues is data security and privacy commonly called as data confidentiality. Apart from data confidentiality flexible and fine grained access are also required in cloud services. Restricted access control provides cloud security and the famous security models are Bell-La padulla (BLP) [10] and BiBa [11]. A fine grained access control scheme which separates data owner and service provider is Attribute based encryption (ABE) which follows key policy-Attribute based encryption (KP-ABE).This scheme losses flexibility and scalability in terms of attribute management and attribute authority management. Ciphertext policy ABE (CP-ABE) provides better fine grained access at high cost. In this paper we propose a Hierarchical Attribute Set Based Encryption (HASBE) provide hierarchical system structure for flexible and scalable access control. Hierarchical Attribute Set Based Encryption extends Attribute set based encryption with hierarchical structure to provide flexible and scalable fine grained access control.

II. OVERVIEW

In this section Attribute set based encryption is discussed with the help of Attribute Based Encryption (ABE) method. The user is able to decrypt the cipher text if there is a match between decryption key and the cipher text. Based on the attribute set the encryption policy is categorized into two types namely key-policy Attribute based Encryption(KP-ABE) and Cipher text policy Attribute Based Encryption(CP-ABE).In KP-ABE the cipher text is associated with set of attributes and user decryption key is associated with monotonic tree access structure. The user can decrypt the cipher text only when the attribute satisfy the tree structure. But in CP-ABE the user decryption key is created with set of attributes and cipher text is encrypted with tree access policy. The attributes of decryption key which satisfy the tree access policy is used for decrypting the cipher text. The CP-ABE provides more access control than KP-ABE. However the access control provided by CP-ABE [9] is not sufficient for modern enterprise environment which requires more flexibility and efficiency in managing attributes [10] with tree structure. The CP-ABE scheme support only a single set of user attribute but Attribute Set Based Encryption(ASBE) which organises a recursive set of user attribute. The ASBE is implemented by four algorithms namely setup, keygen, encrypt and decrypt. Setup (d).Here d is the depth of key structure. Take d as input parameter and its output is public key (PK) and Master key (MK).KeyGen (MK, u, A) the Master Secrete Key (MK), the identity of user (u) and a key structure (A) are taken as input. The output is secrete key (SK) for the user.

Encrypt (PK, M, T) Public key (PK), message (M) and access tree (T) are taken as input. The output is cipher text (CT).Decrypt (CT, SK) the Cipher Text (CT) and Secrete Key (SK) are taken as input. It outputs the message(m) only the key structure(A) associated with Secrete Key(SK) satisfies the access tree(T), associated with cipher text(CT) the m is the original message(M).The delegation algorithm which defines the translation of user attribute from single set to large number of recursive set. The delegation algorithm is implemented in proposed system.

The traditional encryption method secures the user file with encryption and the decryption key is issued to authorize user only. Here efficient key management scheme is required and flexibility is reduced by large number of user. In case the legitimate user wants to be revoked related data has to be re-encrypted and new keys must be distributed to the user. In this scheme the data owner has to be alive all time for encryption and revocation and key distribution process. But ABE provides flexible scalable fine grained access control solution. The KP-ABE provides access control solution together with re-encryption process for revoked user. The problem in it is the encryptor is not able to decide who can encrypt the data except choosing descriptive attributes of data and has no choice but to trust the key issuer. Hierarchical Attribute Set Based Encryption (HASBE) provide fine grained access control by combining Hierarchical identity based encryption and CP-ABE.

III. DESIGN CONSIDERATION

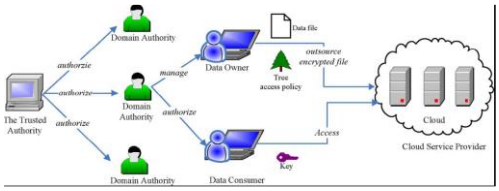

Fig 1 System Model

In Fig 1 there are five parties namely data owner, data consumer, trusted authority, domain authority, cloud service provider. Cloud service provider manages the data storage in the cloud. Data owner encrypt the data files and store them in the cloud for sharing with data consumer. Data consumer decrypts the desired file from the cloud by downloading the encrypted file. Each data owner/consumer is administered by the domain authority. Each domain authority is administered by parent domain authority or root authority. Data owner, data consumer, domain authority and trusted authority are organised in a hierarchical manner. In this scheme neither data owner nor data consumer is always online. Only the domain authority, trusted authority and cloud service provider are online. Here the cloud service provider is the untrusted one because it colludes with the malicious user. Each party is associated with public and private key pairs in which the later is kept secured by the parties. The domain authority is trusted by the sub ordinate domain authority who tries to get the data beyond its privilege. This creates the security lagging in the domain authority side. The communication channel between all parties is secured by Standard Security Protocol (SSL).

IV. IMPLEMENTATION

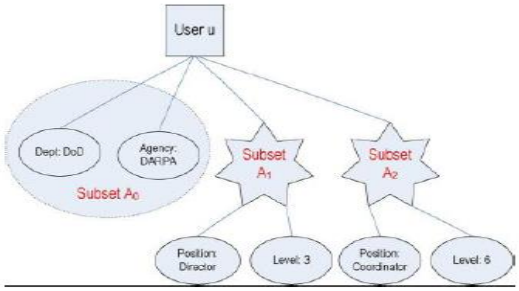

Fig 2 Key structure

In HASBE scheme a recursive set based key structure is used shown in Fig 2. The level of recursion depends on the of depth of key structure in the recursion set. A key structure with depth 2, members of the set at depth 1 can be either set or attribute element but members of set at depth 2 must be a attribute element. Consider the above figure where {Dept : DoD , Agency : DARPA , Position : Director , Level : 3} , Position : Coordinator , Level : 6}} is a key structure of depth 2. It represents the attribute of a person who is both a director of level 3 for a unit and coordinator of level 6 for the unit in Defence Advanced Research Project Agency (DARPA) of the department of defence (DOD). The key structure defines unique labels for each set. For key structure of depth 2 the index of the depth 2 is sufficient for uniquely identifying the sets.

Access Structure:

The above access structure demands that only a director in DOD or NSA of level larger than 5 can access the data files protected by the access policy. In CP-ABE scheme, a person who has private keys corresponding to attributes on the key structure shown in Fig 2. Would be access the data files which compromise the security of the access policy in Fig 3 Such problems are efficiently prevented using attribute base attribute based encryption .

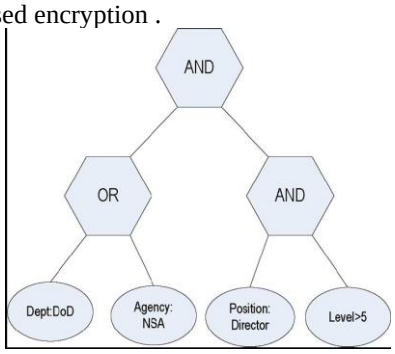

Fig 3 Attribute Access structure

The access structure is same as the tree structure specified in [10] where the non leaf node specifies threshold gate where the leaf node specifies the attribute. In CP-ABE the person who has private keys can able to access the data files which compromises the security. This problem is eliminated in Attribute Set Based Encryption which forbids combining attributes across multiple sets. Several functions are defined for accessing key structure. We define parent(x) as a parent node of x and index(x) as the index number of node x. The function att(x) is defined only if x is a leaf node. The fig specifies the attribute access structure with AND and OR operation. The access structure is same as the tree structure specified in [10] where the non leaf node specifies threshold gate where the leaf node specifies the attribute.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Encryption of the data is done using hierarchical set based encryption algorithm with access structure as specified above.

HASBE SCHEME

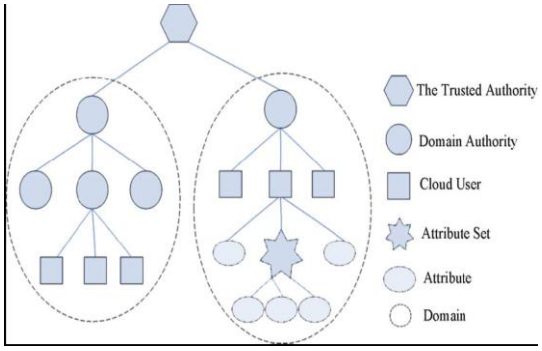

Fig 3 Hierarchal structure of system user

HASBE extends ASBE to handle the hierarchical structure of the system user in Fig 3. Recall that system model consist of a trusted authority multiple domain authority and numerous data owners and data consumers. The mater key and system parameters are generated and distributed by trusted authority. Another responsibility for trusted authority is to authorize the top level domain authority. The domain authority is responsible for issuing keys to the subordinate domain authority and user. The user namely data consumer and data owner are assigned a key structure which contains the attribute associated with user decryption key.

The HASBE scheme consists of seven main parts:

A. System setup

The trusted authority calls the setup algorithm for creating public key (PK) and master key (MK). PK is made public to other parties and MK will kept secret.

B. Top level domain authority grant:

The domain authority consists of unique ID and recursive attribute set. If a new domain user wants to join the trusted authority calls create algorithm for generating master key for new domain user.

C. New domain authority/user grant:

When a new subordinate authority or new user wants to join the system the parent domain authority checks if the user is valid one. If true, the parent domain authority assigns the new key structure and unique ID for the user.

D. New file creation:

For secure cloud storage the data files of the data owner has to be encrypted HASBE scheme with symmetric encryption key. A unique ID, symmetric encryption key, tree access structure is chosen and encryption is done to structure the data file with chosen access structure by HASBE scheme.

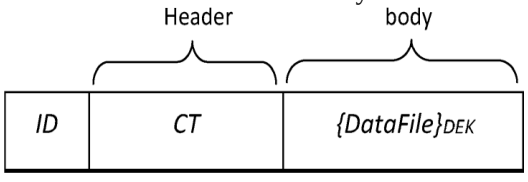

Fig 5 File format in cloud

E. User Revocation:

User revocation is done when the attribute expiration time is finished. When there is a revocation the domain authority assigns the new master key with new attribute expiration time. The reencryption of data file is done when the attribute time expires and user has to be revoked.

F. File retrieval from cloud:

When the data consumer wants the data from the cloud it downloads the file cloud and decrypt it. The decryption is done by decryption algorithm Decrypt ( ) to obtain symmetric encryption key and decrypt the data file with the key.

G. File deletion:

Encrypted data files can be deleted only at the request of data owner. To delete the encrypted data file the data owner sends the file unique ID to the cloud. Only upon the authentication of data owner and request the cloud deletes the file. The file deletion process is done after perfect authentication process. The authentication is done by secrete key.

V. CONCLUSION

In this paper we introduced the HASBE scheme for realising scalable flexible and fine grained access control in cloud computing. The HASBE scheme contains hierarchical structure of system user in which ASBE encryption algorithm is implemented. HASBE not only supports compound attribute set but also provides flexibility in attribute combination. The security aspect of HASBE is proved with the help of CP-ABE policy. Finally the proposed scheme is implemented and comprehensive performance analysis is conducted which shows its advantage over existing system.

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" ieee transactions on information forensics and security, vol. 7, no. 2, april 2012.

[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/

[4] Google App Engine [Online]. Available: http://code.google.com/appengine/

[5] K. Barlow and J. Lane, "Like technology from an advanced alien culture: Google apps for education at ASU," in Proc. ACM SIGUCCS User Services Conf., Orlando, FL, 2007.

[6] B. Barbara, "Salesforce.com: Raising the level of networking," Inf. Today, vol. 27, pp. 45–45, 2010.

[7] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2003.

[8] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[10] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[11] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption forfine-grained access control in cloud storage services," in Proc. ACMConf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)