RAAC With Multiple Attribute Authority For Public Cloud

[1]Mr. Swapnil wani, [2]Mr.javed khan, [3]Miss.Anamika jaiswar, [4]Miss.priyanka gujar

[1]Asst.Professor ,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[1]swapnilwani24@hotmail.com,[2]javedkhan149u@gmail.com,[3]anamika.jaiswar@gmail.com, [4]mkpm36@gmail.com

Abstract: ***Data access control may be a challenging issue publicly cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to supply flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the only attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it leads to a single-point performance bottleneck when a CP-ABE scheme is adopted during a large-scale cloud storage system. Users could also be stuck within the waiting queue for an extended period to get their secret keys, thereby leading to low- efficiency of the system. Although multiauthority access control schemes are proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, thanks to the very fact that every of the authorities still independently manages a disjoint attribute set. In this paper, we propose a completely unique heterogeneous framework to get rid of the matter of single-point performance bottleneck and supply a more efficient access control scheme with an auditing mechanism.***

Keywords-*Access control, Cloud Computing, Robustness, Encryption, Auditing, CP- ABE*.

I. INTRODUCTION

Cloud storage may be a promising and important service paradigm in cloud computing. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to call just a couple of . Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which may be a critical issue to make sure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of knowledge owners, the normal access control methods within the Client/Server model aren't suitable in cloud storage environment. the info access control in cloud storage environment has thus become a challenge.

To address the difficulty of knowledge access control in cloud storage, there are quite few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is considered one among the foremost promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power supported access policies, to supply flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key's labelled with own attributes. as long as the attributes.

II. AIMS AND OBJECTIVE

a) Aim

This work aims at separating the user verification and generation of secret keys. There are many authorities, and each of these authorities will be in charge of the entire attribute sets and therefore will be able to perform the user legitimacy verification independently. To improve the efficiency, introduce single Central Authority and multiple Attribute Authorities. The huge load of user legitimacy verification are going to be divided among the attribute authorities, and therefore the central authority are going to be responsible of only the distribution of secret keys. Different users may find different things relevant because of different importance or priorities of query terms, indicating the necessity of personalized search, which takes personal keyword preference or keyword priority into account.

b) Objective

To address the single-point performance bottleneck of key distribution existed in the existing schemes, propose a robust and efficient heterogeneous framework with single CA(Central Authority) and multiple AAs (Attribute Authorities) for public cloud storage. The heavy load of user legitimacy verification is shared by multiple AAs, each of which manages the universal attribute set and is in a position to independently complete the user legitimacy

 DOI : 10.35291/2454-9150.2020.0232

verification, while CA is merely liable for computational tasks. To the best of knowledge, this is the first work that proposes the heterogeneous access control framework to address the low efficiency and single-point performance bottleneck for cloud storage.

III. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool it's necessary to work out the time factor, economy and company strength. Once this stuff are satisfied, ten next steps are to work out which OS and language are often used for developing the tool. Once the programmers start building the tool the programmers need lot of external support.

Paper 1: Xue, Yingjie, et al. "LABAC: A location-aware attribute-based access control scheme for cloud storage." 2016 IEEE Global Communications Conference (GLOBECOM). IEEE, 2016:

Data access control is a challenging issue in cloud storage. Ciphertext-Policy Attribute- based Encryption (CP-ABE) is a potential cryptographic technique to address the above issue, which is able to enforce data access control based on users' permanent characteristics. However, in some scenarios, access policies are associated with users' temporary conditions (such as access time and location) as well as their permanent ones.

Paper 2: Hong, Jianan, et al. "TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud." IEEE Transactions on Services Computing (2017):

The new paradigm of outsourcing data to the cloud is a double-edged sword. On the one hand, it frees data owners from the technical management, and is easier for data owners to share their data with intended users. On the other hand, it poses new challenges on privacy and security protection. To protect data confidentiality against the honest-but- curious cloud service provider, numerous works have been proposed to support fine- grained data access control. However, till now, no schemes can support both fine- grained access control and time-sensitive data publishing. Based on the scheme, an efficient approach to design access policies faced with diverse access requirements for time-sensitive data.

Paper 3: Xue, Kaiping, and Peilin Hong. "A dynamic secure group sharing framework in public cloud computing." IEEE Transactions on Cloud Computing 2.4 (2014): 459-470:

With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud-based group sharing frameworks.

IV. EXISTING SYSTEM

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has so far been regarded as one of the most promising techniques for data access control in cloud storage systems. This technology offers users flexible, fine-grained and secure access control of outsourced data. It was first formulated by Goyal et al. in .Then the first CP-ABE scheme was proposed by Bettencourt et al. in , but this scheme was proved secure only in the generic group model. Subsequently, some cryptographically stronger CP-ABE constructions but these schemes imposed some restrictions that the original CP-ABE does not have. In , Waters three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as. To improve efficiency of this encryption technique, Emera et al. proposed a CP-ABE scheme with a continuing ciphertext length. Unlike the above schemes which are only limited to express monotonic access structures, Ostrovsky et al. proposed a more expressive CP-ABE scheme which can support non-monotonic access structures. Recently, Hohenberger and Waters an ABE technique for CPABE which enables the user to do as much pre-computation as possible to save online computation. It's a promising technique for resource-limited devices.

V. PROBLEM STATEMENT

An efficient heterogeneous framework with single CA/multiple AAs to deal with the matter of single-point performance bottleneck. The novel idea of proposed scheme is that the complicated and time- consuming user legitimacy verification is executed only once by one selected AA. Furthermore, an auditing mechanism is to ensure the traceability of malicious AAs. Thus scheme can not only remove the single- point performance bottleneck but also be able to provide a robust, high-efficient, and secure access control for public cloud storage.

VI. PROPOSED SYSTEM

The heterogeneous architecture with single CA and multiple RAs, a robust and auditable access control scheme (named RAAC) for public cloud storage to promote the performance while keeping the flexibility and fine granularity features of the existing CP- ABE schemes. In this scheme, seperate the procedure of user legitimacy verification from the secret key generation, and assign these two sub-procedures to two different kinds of authorities. There are multiple authorities (named attribute authorities, AAs), each of which is in charge of the whole attribute set and can conduct user legitimacy verification independently. Meanwhile, there is only one global trusted authority (referred as Central Authority, CA) in charge of

 DOI : 10.35291/2454-9150.2020.0232

secret key generation and distribution. Before performing a secret key generation and distribution process, one of the AAs is selected to verify the legitimacy of the user's attributes and then it generates an intermediate key to send to CA.

VII. ADVANATGES

- Secure against the collusion attack.
- Secure User Revocation, Public auditing.
- Lower computational complexity and communication overhead.
- Total overhead is small.

VIII.COMPARTIVE STUDY

SR NO.	PAPER TITLE	AUTHOR NAME	METHOD	ADVANTAGE	DISADVANTAGE
1.	Efficient public integrity verification with secure group client repudaition.	Jiang and his colleagues 2016	Vector commitment, Asymmetric Group Key Agreement, verifier-local revocation group	Secure against the collusion attack.	More computatio n cost.
2.	Public verification for combined information with effective client repudiation.	Wang and his colleagues	Homomorphic Authenticable Proxy	Secure User Revocation, Public auditing.	Collusion of repudiated customer and cloud.
3.	Multi-authority proxy Reencryption based on CP-ABE for cloud storage system.	Xue and his colleagues	MPRE-CPABE scheme and WAS scheme.	Low computational cost of key distribution.	Longer computational time of setup.
4	Efficient chameleon hashing-based privacy preserving auditing.	Zhang and his colleagues	Identity privacy preserving public auditing Protocol	Identity privacy preserved, low computation cost	Cloud server has large computatio n cost.

IX. ALGORITHM

Require: U:the original user interest model; w:the new query word; θ: an impact factor, fixed as

1; Ensure: U 0 :the updated user interest model 1: if w in U then
2: update the score of w, score = 1 + score × θ;
3: else
4: create a new node with score 1 labeling w; 5: end if
6 synonym set=GetSynonymSet();
7: for every synonym w 0 in synonym set do 8: if w 0 in U then
9: update the score of w 0 , score = α + score × θ; 10: else
11: create a new node with score α labeling w 0 ; add a edge w − w 0 and label synonym relation;
12: end if
13: end for
14: hypernym hyponym set= GetHypernym hyponymSet();
15: for every hypernym/hyponym w 0 in hypernym hyponym set do
16: if w 0 in U then
17: update the score of w 0 , score = β + score × θ;
18: else
19: create a new node with score β labeling w 0 ; add a edge w − w 0 and label hypernym/hyponym relation;
20: end if
21: end for
22: meronym holonym set= GetMeronym HolonymSet();
23: for every meronym/holonym w 0 in meronym holonym set do
24: if w 0 in U then 25: update the score of w 0 , score = γ + score × θ;
26: else
27: create a new node with score γ labeling w 0 ; add a edge w−w 0 and label meronym/holonym relation;
28: end if
29: end for
30: return U 0 ;

X. MATHEMATICAL MODEL

A CP-ABE scheme consists of four algorithms: Setup, Encrypt, Key Generation (KeyGen), and Decrypt.

Setup(λ, U) → (PK,MSK). The setup algorithm takes the security parameter λ and the attribute universe description U as the input. It outputs the public parameters PK and a master secret key MSK.

Encrypt(PK,M,A) → CT. The encryption algorithm takes the public parameters PK, a message M, and an access structure A as input. The algorithm will encrypt M and produce a ciphertext CT such that only a user whose attributes satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitlycontains A.

KeyGen(MSK,S) → SK. The key generation algorithm

 DOI : 10.35291/2454-9150.2020.0232

takes the master secret key MSK and a set of attributes S as input. It outputs a secret key SK.

Decrypt(PK,CT,SK)→M. The decryption algorithm takes the public parameters PK, a ciphertext CT which contains an access policy A, and a secret key SK as input, where SK is a secret key for a set S of attributes.

XI.SYSTEM ARCHITECTURE

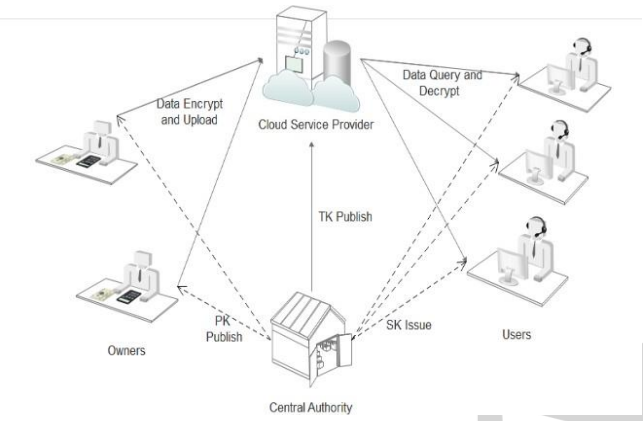

Fig.1: System Architecture

Description: The system model of design is shown in Fig, which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers.

- **The central authority (CA)** is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the system initialization phase, it assigns each user a unique Uid and each attribute authority a unique Aid.

- **The central authority (CA)** are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users. each file, and encrypts the file under the defined policy.

- **The data consumer (User)** is assigned a global user identity U id by CA. The user possesses a set of attributes and is equipped with a secret key associated with attribute set.

- **The data owner (Owner)** defines the access policy about who can get access to.

- **The data consumer (User)** is assigned a global user identity U id by CA.

XII. DESIGN DETAILS

Fig.2 : Login

XIII. CONCLUSION

Thus, We have tried to implement the paper "Kaiping Xue, senior member, IEEE, Yingji Xue, Jianan Hong,Wei Li, Hao Yue, Member, IEEE, David S.L Wei, senior Member, IEEE, and Peilin Hong","RAAC:Robust and Auditable Access Control With Multiple Attribute Authorities For Public Cloud Storage",IEEE2017, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CP- ABE cryptographic technique into proposed novel framework, provides a fine-grained, robust and efficient access control with one- CA/multi-AAs for public cloud storage.

REFERENCE

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology Gaithersburg, 2011.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

 DOI : 10.35291/2454-9150.2020.0232