Access Control Scheme for Data in Cloud Authentication

[1]Mr.Gholap Nilesh , [2]Prof. Pritesh Jain
1PG Student, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal
2Assistant Professor, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal

ABSTRACT: ***Cloud computing is a computing paradigm, where a large pool of systems are connected in private, or public networks, to dynamically scalable infrastructure for application, data, and file storage and In this paper, we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.***

Keywords: ***Access Control, Cloud Computing, Key Policy, Attribute-based signatures (ABS), Attribute Based Encryption (KP-ABE), Anonymity Authentication, Key Management***

INTRODUCTION

Cloud computing is an internet based computing that provide shared computer processing resources and data to computers and other devices on demand**.** Cloud computing builds on established trends for driving the cost out of the delivery types of services with increasing the speed and duration with which services are deployed. It reduces the time from initiation of application architecture to actual deployment. As cloud computing has become important, more and more sensitive data is being centrally stored into the cloud by users. To protect the sensitive data from attacker, the data should be in encrypted before uploading on the cloud. However, this gives a new problem for carrying search operation over the encrypted data efficiently. Although the most of searchable encryption techniques allow a user to search on the encrypted data by providing confidentiality, these solutions are not useful for the verification process of searched result. Efficient search is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption [1], [2]. Approach control techniques are very important strategies to provide security for the system where only accredited user should able to approach the resources they required. This is very important in cloud because high priority and sensitive data is being stored in cloud such as online document, personal information (what's up, twitter), and medical information. Access control is a key point, because insider attacks are a high risk. There are three types of access control: user-based approach control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list (ACL) contains the list of users who are accredited to approach data. This is not feasible in clouds where there are many users. In RBAC (introduced by [8]), users are classified based on their individual roles. Data can be approached by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have approach to data but not the junior secretaries. The ABAC is more extend ding scope, in which users are given attributes, and the data has attached approach policy. Only users with valid set of attributes, satisfying the approach policy, can approach the data. For instance, in the above example certain records might be approachable by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience. There has been some work on ABAC in clouds (for example, [3], [4], [6],[5], [7]). All these work use a cryptographic primitive known as Attribute Based Encryption (ABE) anyone using the cloud service needs to know who is managing their data and what types of controls are applied to these individuals. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. Security and privacy assurance in clouds are analyzed and tested by numerous researchers. [3] Gives storage security utilizing Reed-Solomon eradication correcting codes. Utilizing homomorphism 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 approach. In addition revocation scheme is used for time based file assured deletion.

II. RELATED WORK

Access control techniques are very important strategies to provide security for the system where only accredited user should able to approach the resources they required. . Approach control is a key point, because insider attacks are a high risk. Anyone using the cloud service needs to know who is managing their data and what types of controls are applied to these individuals. The model of application centric approach control, where most of the applications keeps list of its users and manages them, is not more feasible in cloud based architectures. The authors [12] take a centralized technique where a single key distribution centre (KDC) distributes secret keys and attributes to all the users. Unfortunately, a single KDC is not only a single data of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. The receiver receiving the attributes and secret keys from the attribute authority and is able to decrypt the information if it has matching attributes. All the technique takes a centralized approach and allows only one KDC, which is a single point of failure. In spite of the fact that Yang et al. [9] proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while approaching the cloud. Ruj et al. [10] proposed a distributed approach 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 approach was not allowed to clients other than the originator. Time-based file assured deletion, which is initially presented in [11], 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.

II. PRAPOSED SYSTEM

In this system it provides authentication of users who store and modify their data on the cloud.we proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while approaching the cloud. In an earlier work, proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication\. In the preliminary version of this paper, we extend our previous work with added features that enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation, that was not addressed. We use ABS scheme to achieve authenticity and privacy.

II. SYSTEM ARCHITECTURE

This is a privacy preserving authenticated access control scheme in which user can create a file and store it securely in the cloud using ABE and ABS protocol.

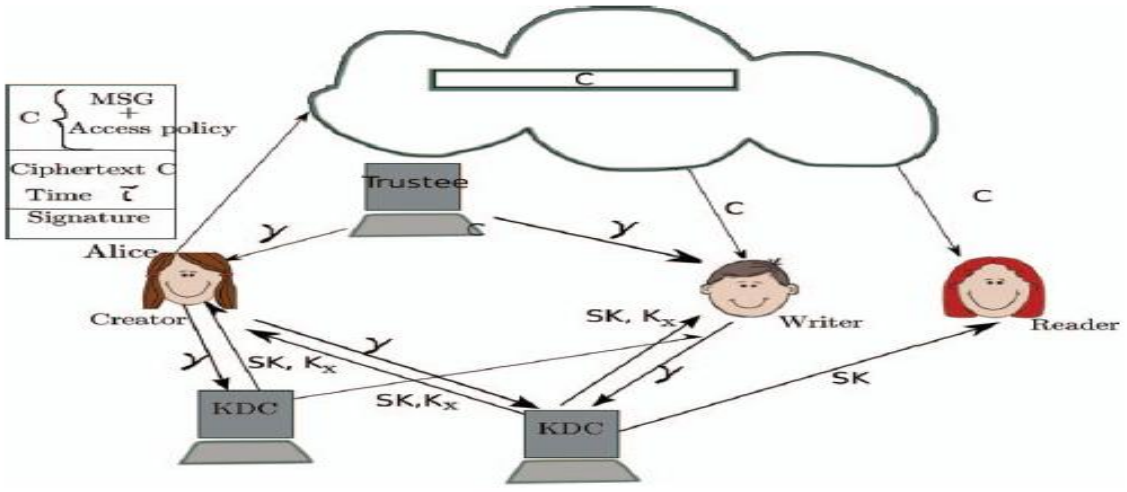

Fig1.1 System Architecture

In this section we propose our privacy preserving authenticated access control scheme. According to our scheme an user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, There are three following users, a creator, a reader, and a writer. Creator Alice receives a token γ from the trustee, now it is assumed to be who is honest. SKs are secret keys given for decryption, KX are keys for signing. The message MSG is encrypted under the approach policy X. The approach policy decides who can approach the data stored in the cloud. The creator define a claim policy Y to prove the authenticity and signs of the message under this claim. The cipher text C with a signature c is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read the message in the cloud sends C. That the

user has attributes matching with the approach policy, it can be decrypted and get back the original message.Write also proceeds in the similar way as file creation. By designating the verification of the data to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypting and using the secret keys it receives from the KDCs. If it has enough attributes matching with the approach policy, then it decrypts the information stored in the cloud.

4.1 Data Storage in Clouds:

The KDCs are given keys for encryption/decryption and ask for signing/verifying.

- The users obtain attributes and secret keys from one or more KDCs.
- The message is encrypted using the equation C = ABE: Encrypt(MSG; key)

4.1.2 Reading from Clouds

- When a user request a data from cloud, the cloud sends Ciphertext c using SSH Protocol.
- Decryption proceed using the equation ABE: Decrypt(C; SKi;u)

4.1.3 Writing to the cloud

- To write to an already existing file the user must send his/her message during file Creation.
- The cloud verifies WK (writing key) and only if the user is authenticated he/she can write on the file.

4.2 Algorithm

(a) ABE (Attribute Based Encryption) it works under the following stages.

- **Setup:** This is a random algorithm that takes no input other than security parameter. It outputs the public parameters P and a master key K.
- **Encryption**: This is a random algorithm that takes as input a message m, a set of attributes n, and the public parameters P. It outputs the cipher text C.
- **Key Generation: This** is a random algorithm that takes as input an approach structure A, the master key K and the public parameters P. It outputs a decryption key D.
- **Decryption:** This algorithm takes as input the ciphertext C that was encrypted under the set n of attributes, the decryption key D for approach control structure A and the public parameters P. It outputs the message M if n 2 A.

(b) ABS (Attribute Based Signature) An Attribute-Based Signature (ABS) scheme is depend on a possible attributes A and message space M, and consists of the following four algorithms.

- ABS. Setup (to be run by a signature trustee): Generates public reference information TPK.
- ABS. Setup (to be run by an attribute-issuing authority): generates a two keys PK and SK.
- ABS. AttrGen: On input (SK, A_A), outputs a signing key SK.
- ABS.Sign:On input (PK = (TPK, PK), SK, m ϵ M, Υ), where (A) = 1, outputs a signature σ
- ABS. Ver: On input (PK = (TPK, PK), m, Υ, σ) outputs a Boolean value 0 or 1.

4.3 Mathematical model

Representation in the set format:

- Set Theory: User Model: Set (P) = {p0, p1, p2, p3, p4, p5}

  p0 = Enter proper data for registration

  p1 = Enter proper data for login

  p2 = upload file to be stored on cloud

  p3 = Send user data to be stored on online Cloud

  p4 = Apply Correct keys for Reading and updation of file

  p5 = Modify stored file and store again

- Upload Data for Storage: Set (Q) = {q0, q1, q2}

  q0 = Store written article from user temporary

  q1 = Collect keys provided by user

  q2 = Store article in online cloud

- Encryption Technique: Set(R) = {r0, r1}

  r0 = Collect article data temporary

  r1 = Appy encryption algorithm (Pailier)

- Decryption Technique: Set (U) = {u1, u2, u3}

  u1 = select secret keys which apply in encryption process

  u2 = convert encrypted data into original format

  u3 = create downloaded file ready for User

- Login Module:Set (V) = {v1, v2, v3}

  v1 = Collect user Crediential for login

  v2 = Check authentication for database data

  v3 = If valid the show homepage either show Authentication fail

Union and Intersection of project:

Set (P) = {p0, p1, p2, p3, p4, p5}

Set (Q) = {q0, q1, q2}

Set(R) = {r0, r1}

Set(S) = {s1, s2, s3}

Set (T) = {t1, t2, t3}

Set (U) = {t2, t3, u1, u2, u3}

Set (V) = {v1, v2, v3}

Let S be set represents various parameters such as input (I), output (O), function (F) and failure Case (FC)

S= {(I), (O), (F), (FC)}

Input (I)-I is the subset of set S which represents input given by the user. Input contains set of files is passed as input.

I = {file 1, file 2, file n}

Output (O) -O is the subset of set S which represents file storage using encryption with kdc key generation file upload successful on online cloud.If read key of article is correct then it display or view at client side and user wants update article then used write key.

O = { Decryption of file using ready key and write key for update , file download successful }

Function (F) - Set the Articles.F= {Function} Failure Case (FC)-If read key is not correct.

IV. CONCLUSION

We have introduced a decentralized approach 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.

REFERANCES

[1] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. 2010, pp. 441–445.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, 2010, pp. 136–149.

[3] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Secure Comm, 2010, pp. 89–106.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, 2010, pp. 261–270.

[5] 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, 2011, pp. 83–97.

[6] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, 2010, pp. 735–737.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE Trust Com, 2011.

[8] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *IEEE Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[9]. 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.

[10]. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[11] . Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.