A MultiKey Based Privileged Access Control in Clouds

Jahnavi Sushma Kadali,
M.Tech
Department of Computer Science and Engineering
SRKR Engineering College
Bhimavaram, India

K. V. S. S. R. Murthy
Asst. Prof
Department of Computer Science and Engineering
SRKR Engineering College
Bhimavaram, India

***Abstract*— The prominent feature of cloud computing is to provide on-demand services to users, which facilitates them to store their data securely in a cloud server. Providing access control scheme for secure cloud storages and the anonymous data sharing for user's privacy are the significant issues met in cloud security. Access control policy verifies that only valid users were able to decrypt the content with varying multiple key distributions between involved content sharing parties. Its efficiency is constrained since these access policies are stored in the cloud and stands to be exposed during a cloud security breach leaving user's data vulnerable. So we would like to conceal the attributes and access policy of a user using a dynamic access policy deriving solution termed Policy Compare. It adapts based on the owner, receiver, content attributes along with Multiple key distributions generated for the data content.**

Keywords—Access control; Cloud Storage; Data Sharing; Key Distributions

I. INTRODUCTION

Clouds can offer several kinds of services like programs, infrastructures, and platforms to assist designers write programs. Privacy and security are, thus, essential issues in cloud computing. To supply secure data storage, the information must be encoded. Efficient explore encoded information is also an essential concern in clouds. The clouds shouldn't be aware of query but should have the ability to return the records that fulfill the query. This really is accomplished by way of searchable file encryption [2]. Privacy and security protection in clouds are now being investigated by many people scientists. Many homomorphism file encryption techniques [3] happen to be recommended to make sure that the cloud can't browse the data while carrying out computations in it. Using homomorphism file encryption [3], the cloud receives cipher text from the data and performs computations around the cipher text and returns the encoded worth of the end result.

The consumer has the capacity to decode the end result however the cloud doesn't understand what data it's operated on. Accountability of clouds is an extremely challenging task and involves intricacies and police force. Access control in clouds is attaining attention because it is crucial that only approved customers get access to valid service. A lot of details are being kept in the cloud, and point about this is sensitive information. You will find broadly three kinds of access control: user-based access control (UBAC), role-based access control (RBAC) [4], and attribute-based access control (ABAC). A place where access control is broadly getting used is healthcare. Clouds are used to keep sensitive details about patients [5] to allow use of doctors, hospital staff, scientists, and policy makers. You should control the access of information to ensure that only approved customers have access to the information. Using ABE [6], the records are encoded under some access policy and kept in the cloud [7]. Customers receive teams of characteristics and corresponding keys. Only if the customers have matching group of characteristics, would they decrypt the data kept in the cloud. This is possible only when clouds must take a decentralized approach while disbursing secret keys and characteristics to customers. It's also quite natural for clouds to possess many KDCs in numerous locations on the planet.

Providing access control scheme for secure cloud storage along with the user privacy is the prominent one. Maintaining anonymity while sharing data in cloud is one among the major factor needed to be considered. Suppose if a person wants to share some sensitive information like corruption in a government organization, without revealing his/her identity because of the risk of being threatened by the government bodies. In such cases user privacy is also important along with the secure storage of the data in cloud. But in some cases the information may reveal forcefully due to the legal aspects. Sometimes by being anonymous is not only the solution for this, even though the person may remain anonymous to the users in the cloud but their identity may reveal forcefully due to legal aspects.

II. LITERATURE SURVEY

A. Cloud Computing

Now a day's Cloud Computing [9] is attaining lots of attention by its on demand service offerings to users. Cloud offers many remote services to users and customers via internet. Examples for the cloud services are Amazon Ec2, Google Accounts, Drop Box, Google Drive etc. User can access the cloud service from anywhere, anytime and on any kind of device. Clouds offer the major services like public cloud, private cloud and hybrid cloud. Private clouds are primarily used by the organizations and these services may exist off-site by providing data security. Public clouds providing open services to any user through internet. Hybrid cloud is a composition of public and private clouds which offers both the features of private and public clouds.

B. Software As A Service (SAAS)

SAAS [8] is one of the major service delivery models, offers the on demand software services to the users. Software services includes develop, buy, sell and use of the software. In this

model software is available as service to the users where the cloud user can access those services via users web browser without being worry about the deploying, installation and the maintenance of the software. It is the duty of the cloud provider to manage the application's security, availability and performance. SAAS [8] uses a multitenant architecture to end users desired application through internet to the customers.

The characteristics of SAAS include customisation, On-demand self services and the accessibility. Customisation is very little in SAAS user has very limited access to customise the overall application. End-user must be able to use the service with minimal management effort or cloud provider interaction. Any SAAS application gets accessible to users through any network device like pc, laptop, mobile and PDAs.

C. Access Control

Enormous amount of information is being stored in cloud access control is needed because there may be some private information which stands to be exposed to all the users in cloud. In general terms access control is nothing but the process of restricting or denying the entrance in the same way access control in cloud defines that the process of restricting users to view and manipulate particular content being stored in cloud.

There are broadly three ways to define access control in cloud they are User-Based Access Control (UBAC), Role-Based Access Control (RBAC) [10] and Attribute-based Access Control (ABAC). In User-Based Access control consists of a list of users with their access privileges only the users who are in the list can access the data. In RBAC access control is assigned based on their individual roles which are defined by the system, Example for RBAC is roles based on their job like faculty members. ABAC has largely extended scope, where the users given some attribute and access policy joined with data. Only the users with those matching attributes and the satisfying access policy have the data access privileges.

D. Attribute Based Encryption

Providing Security for the sensitive data storing in cloud is one of the issue needed to be concerned. Security is ensured when the data is stored in an encrypted form. This can be achieved by using Attribute-Based Encryption (ABE).In ABE [12] a user's keys and the ciphertexts are attached with a set of descriptive attributes. A particular key can decrypt a ciphertext if and only if the matching attributes in both the user's key and ciphertext. By using this ABE data security is ensured for the sensitive data. In key-policy ABE or KP-ABE (Goyal et al. [11]), the sender contains an access policy to encrypt the data. A user whose attributes and keys have been revoked can no longer access the information. The receiver who receives attributes and secret keys from the attribute authority are able to decrypt information only if they have matching attributes.

E. Attribute Based Signature

Secure storing of data in cloud is not just sufficient but maintaining user's anonymity is also been considered. A user may want to share some information by being anonymous. For being anonymous a protocol was proposed by the Maji et al [13] called as Attribute Based Signature (ABS) [13]. In ABS, users have a claim predicate related with a message. The claim predicate used to identify the user as an authorized user, without revealing their identity. Other users on cloud can verify the user and the validity of the message stored. ABS can be joined with ABE to achieve authenticated access control without revealing the identity of the user to the cloud.

III. EXISTING SYSTEM

Considering a decentralized access control [1] scheme for secure cloud storages and the need for anonymous data sharing's for user privacy preciously a system that verifies the authenticity of the data and its owner was proposed which serves well with respect to an access control policy in which only valid users were able to decrypt the content with varying multiple key distributions between involved content sharing parties. Here privacy protecting authenticated access control plan was proposed. Based on that plan a person can produce a file and store it safely within the cloud. This plan includes utilization of the two methods ABE and ABS correspondingly.

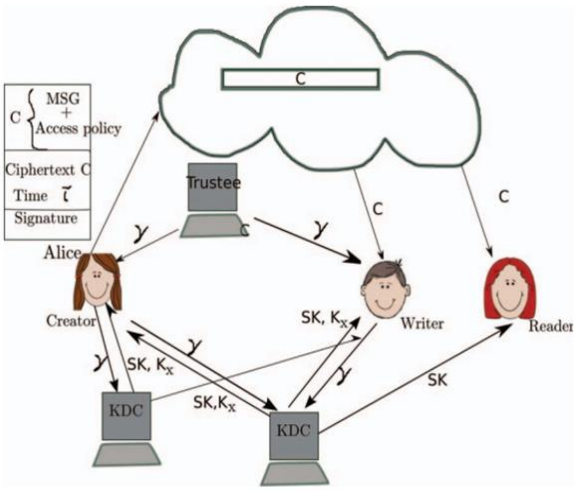

Figure 1: Secure Cloud Storage Model

Here by referring Figure 1 proposes a secure cloud storage model contains three users namely creator, reader and writer. Creator is the one who uploads some data in cloud where as the reader wants to reads the data and writer wants to writes the data. Trustee is a person who generates tokens to the users. There are multiple KDC's which are scattered. Creation first asks for the token, after receiving token from the trustee there by the creator approaches KDC [15] for secret key SK and K_X for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove their authenticity and signs the message under this claim. The Ciphertext C along with the signature is sent to the cloud for verification. The cloud verifies Signature and stores the Ciphertext C. Whenever the user wants to read, the cloud sends C. If that particular have the matching attributes with the access policy, message gets decrypted as a plain text. Write originate same as that of the creation.

A. *Single KDC Vs Multiple KDC's*

Key Distribution Centre (KDC) [15] in cryptography is used to distribute keys and attributes to all users. All the other approaches take a centralized approach and allow only one KDC which is not only a point of failure but also difficult to maintain due to the large number of users in cloud environment. Although Single Key Distribution Center (S-KDC) approaches of other system for securing data is much better than plain data access, the cloud data sharing system is still open to a wide range of data access. However these schemes falls short of flexibility creations and revocations with respect to S-KDC and lacks data access mode specifications in dealing with multiple-levels of attribute validations and have complicated expressions while describing access policies.

Forced by the limitations of the S-KDC, this system emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. Since the M-KDC follows a decentralized approach [1], KDC's are distributed throughout the world in various locations. A key advantage of the M-KDC scheme is that adding users/revoking users or updating access control policies can be performed efficiently by updating only some public information. Revoked users cannot access data after they have been revoked.

B. *Attribute-Based Encryption Scheme (For Data Protection)*

Without utilizing a single static public key cryptography and by allowing users to dynamically derive different symmetric keys for encryption and decryption purposes along with attribute access control validations raises security levels in our cloud data storages. The ABE [12], [1] scheme provides data confidential to other users including the cloud provider. The steps involved in ABE are as follows:

- System Initialization
- Key Generation and Distribution by KDCs
- Encryption by Sender
- Decryption by Receiver

C. *Attribute –Based Signature Scheme (For Annonymous Authentication)*

The ABS [13], [1] scheme for the anonymous authentication provides users authenticity by remaining anonymous to other users in cloud. ABS steps are as follows:

- System Initialization
- Key Generation and Distribution by KDCs
- Encryption by Sender
- Decryption by Receiver

IV. PROPOSED SYSTEM

User's privacy along with the authenticity of the data performs well with respect to an access control policy in which only valid users were able to decrypt the content with multiple key distributions between data sharing among users. In the above system access policies are being stored in the cloud which may expose to forceful revelations.

Suppose if a person wants to project some sensitive information like corruption in a particular government organization by hiding the identity because of the risk of being threatened by that organization. In those cases identity hiding only works with the remaining users in the cloud but the access policy of that person remains in the cloud server which may reveal by the cloud owner due to the legal aspects. By considering those factors, in our proposed system we would like to conceal the attributes and access policy of a particular user using a dynamic access policy deriving solution named as Policy Compare.

Its algorithmic implementation is really as follows:

Algorithm 1 PolicyCompare

Input: new policy (M', ρ') with $l' \times k'$ matrix
Input: previous policy (M, ρ) with $l \times k$ matrix
Output: $I_{1,M'}, I_{2,M'}, I_{3,M'}$ ▷ three subsets of row indexes in M'

1: $I_M \leftarrow$ index set of rows in M
2: **for** $j = 1$ to l' **do**
3: **if** $\rho'(j)$ in M **then**
4: **if** $I_M != \emptyset$ & $\exists i \in I_M$ s.t. $\rho(i) == \rho'(j)$ **then**
5: add (j, i) into $I_{1,M'}$
6: delete i from I_M
7: **else**
8: find any $i \in [1, l]$ s.t. $\rho(i) == \rho'(j)$
9: add (j, i) into $I_{2,M'}$
10: **end if**
11: **else**
12: add $(j, 0)$ into $I_{3,M'}$
13: **end if**
14: **end for**

Figure 2: PolicyCompare Algorithm

In figure 2: it first calls the policy comparing algorithm PolicyCompare to compare the new access policy with the previous one, and outputs three sets of row indexes which are shuffled to create a perturbed access policy which cannot be reconstructed by the server but yet stored at the server. It adapts based on the owner, receiver, content attributes along with Multiple key distributions generated for the data content.

We attempt to offer the following objectives using our suggested plan:

A. *Objectives offered:*

- Distributed access charge of data kept in cloud to ensure that only approved customers with valid characteristics have access to them
- Provides Authentication for the customers who store and modify their data around the cloud.
- The identity from the user is protected against the cloud during authentication.
- The architecture is decentralized, and therefore there might be several KDCs for key management.
- The access control and authentication are generally collusion resistant, and therefore no two customers can

collude and access data or authenticate themselves, if they're individually not approved.

- Revoked customers cannot access data after they've been revoked [14].

V. CONCLUSION

We've presented a Multi-Key based privileged access control in clouds which provides a better anonymity to cloud users, by hiding their access policies which are stored in cloud server. Since it uses an M-KDC approach, key distribution is completely done in a decentralized way. Considering its dynamic efficient nature while upholding privacy and security with respect to cloud data storages it is a much better system compared to prior approaches.

REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" .

[2] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.

[3] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[4] 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, June 2010

[5] 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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[6] Vipul Goyal and Omkant Pandey "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data".

[7] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[8] Akanksha Singh, Smita Sharma, Shipra Ravi Kumar and Suman Avdesh Yadav "Overview of Pass and Saas and its application in Cloud Computing".

[9] K.V.Mahesh Kumar "Software as a service for efficient cloud computing".

[10] David F. Ferraiolo and D. Richard Kuhn "Role-Based Access Controls".

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[12] Amit Sahai1 and Brent Waters "Fuzzy Identity-Based Encryption".

[13] Hemanta Maji, Manoj Prabhakaran and Mike Rosulek "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance".

[14] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[15] http://www2.ic.uff.br/~michael/kr1999/7-security/7_05-keydist.htm.