International Journal of Science Engineering and Advance Technology

Prevention of Sensitive Information by Enhancing Cloud Access Control

SwamyMandapaka [1], D.Ramesh [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: swamy1209@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract— the scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication, and storage overheads are comparable to centralized approaches. To better protect data security, this paper makes the first attempt to formally address and which are centralized. The communication, computation access control scheme is decentralized and robust; unlike other access control schemes designed for clouds the problem of authorized data. Different from traditional existing systems, the differential privileges of users are further considered in duplicate check besides the data itself by encrypting the file with differential privilege keys. Unauthorized users cannot decrypt the cipher text even collude with the S-CSP. Security analysis of the definitions specified in the demonstrates that our system is secure in terms proposed security model.

Key words: Access control, authentication, attribute-based signatures, attribute-based encryption, cloud storage, private cloud, public cloud

I. Introduction

Clouds can provide many types of services like applications and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).The data stored in clouds is highly sensitive, for example, medical records and social networks. The user validity is who stores the data is also verified. The cloud is also prone that modification of data and server colluding attacks. The data needs to be encrypted means to provide secure data storage. Newly, Wang et al. [2] addressed secure and dependable cloud storage. The clouds should not know the query but should be able to return the records that satisfy the query with security and privacy protection in clouds by using a encryption [3][4]. The user is able to decoding the result, but the cloud does not know what data it has operated on. In such cases, it should be possible for the user to verify that the cloud returns correct data. It is also significant to verify Access control is essential when unauthorized users try to access the data from the storage, so that only authorized users can access the data. That the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques given in There are three types of access control: user-based access control(UBAC), role-based access control (RBAC), and attribute-based access control (ABAC).

In UBAC, the access control list contains the list of users who are authorized to access data. Data should be accessed by users who have matching roles. This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. The roles are declared by the system. For an example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes and satisfying the access policy, can access the data. Only when the users have matching set of attributes, they have decrypting the information stored in the cloud. The merits and demerits of RBAC and ABAC are discussed in There has been some related our contributions in this paper are multirole. a. To identify whether the user is protected from the cloud during authentication. b. The architecture is decentralized, meaning that there should be several KDCs for key management. c. The access control data and authentication are both collusion resistant, that means two users can collude and access data or authenticate themselves, if they are individually not authorized. d. Revoked users cannot be access the data after they have been revoked. e. The proposed system is resilient to replay attacks. A writer those attributes and keys have been revoked cannot write back stale information.

Addressed secure and depend- able cloud storage. Cloud servers prone to Byzantine failure, where a storage server can fail in arbitrary ways. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques. Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to the keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords. Security and privacy protection in clouds are being explored by many researchers. Using homomorphism encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data it has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns

correct results. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed; i have however, it is an important concern to decide how much information to keep in the log. Accountability has been addressed in Trust Cloud. Secure provenance has been studied in.

Considering the following situation: A law student, Alice, wants to send a series of reports about some malpractices by authorities of University X to all the professors of University X to Law department in all universities in the province. , research chairs of universities in the country, and students belonging she wants to remain anonymous while publishing all evidence of malpractice. She stores the information in the cloud. Important to verify that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously. Access control in clouds is gaining attention because it is we address this problem in its entirety in this paper. Access control is important in such case, so that only authorized users can access the data. It is also important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this or even personal information There are broadly three types of access control: user-based sensitive information which can often be related to health, important documents access control (UBAC), role-based access control (RBAC), and attribute based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. Users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. For instance, in the above example certain records might be accessible by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience. An area where access control is widely being used is health care. Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. Access control in health care has been studied in andAccess control is also gaining importance in online social networking where users (members) store their personal information, pictures, and videos and share them with selected groups of users or communities they belong to. Access control in online social networking has been studied in. Such data are being stored in clouds. It is very important that only the authorized users are given access to that information. A similar situation arises when data is stored in clouds, for example, in Drop box, and shared with certain groups of people. It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but there are cryptographic protocols like ring signatures, does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/ she is a valid user who stored the information without revealing the identity. Mesh signatures, group signatures, which can be used in these situations. Ring signature is not a feasible option for clouds where there are a large number of users. Group signatures assume the pre-existence of a group which might not be possible in clouds. Mesh signatures do not ensure if the message is from a single user or many users ABS was proposed by Maji. In ABS, users have a claim colluding together. For these reasons, a new protocol known as attribute-based signature (ABS) has been applied. Combined provides privacy preserving authenticated accessPredicate associated where a single key distribution centre (KDC) distributes secret keys with a message. The claim predicate helps to identify the user as an authorized one, without revealing its identity. Other users or the cloud can verify the user and the validity of the message stored. ABS can be control in cloud. However, the authors take a centralized approach and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world. In a proposed a distributed access controls mechanism in et al. proposed a decentralized approach; their technique does not authenticate users, who want to remain anonymous while accessing the cloud. However, the scheme did not provide user authentication. And other users can only read the file. Write access the other drawback was that a user can create and store a file was not permitted to users other than the creator. 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 in. We use ABS scheme to achieve authenticity and privacy. Unlike, our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write; this is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work. The paper is organized as

follows: Related work is presented in We present our privacy preserving access control scheme in even if it no longer has valid claim policy.

The sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Ciphertext-policy, proposed a multiauthority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users? Multiauthority ABE protocol was studied in, which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green proposed to outsource the decryption task to a proxy server, so that the user can compete with minimum resources. However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang presented a modification of, authenticate users, who want to remain anonymous while accessing the cloud. To ensure anonymous user authentication ABSs were introduced by Maji. This was also a centralized approach. A recent scheme by Maji et al. takes a decentralized approach and provides authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attack.

1.1 Our Contributions

The main contributions of this paper are the following:

1. Distributed access control of data stored in cloud sothat only authorized users with valid attributes canaccess them.
2. Authentication of users who store and modify theirdata on the cloud.
3. The identity of the user is protected from the cloudduring authentication.
4. The architecture is decentralized, meaning that therecan be several KDCs for key management.
5. The access control and authentication are bothcollusion resistant, meaning that no two users cancollude and access data or authenticate themselves,if they are individually not authorized.
6. Revoked users cannot access data after they havebeen revoked.
7. The proposed scheme is resilient to replay attacks. Awriter whose attributes and keys have been revokedcannot write back stale information.
8. The protocol supports multiple read and writes onthe data stored in the cloud.
9. The costs are comparable to the existing centralizedapproaches, and the expensive operations are mostlydone by the cloud.

II. 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 the encrypt or associates the set of attributes every client is assigned an access structure which is normally to the message by scrambling it with the comparing public key for each of which a public key part is characterized. Characterized as an access tree over information attributes, inside hubs of the access tree is 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 full fill 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.

User Privacy in Cloud Computing: User privacy is also required in cloud. By using privacy the cloud or other users do not know the identity and likewise, to provide services the cloud itself is of the other user. The cloud can hold the user accounts for the data in cloud, accountable. The validityof the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy.

Encryption in Cloud Computing: The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even

though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Search on Encrypted Cloud Data: Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Security and privacy protection on cloud data: Users Authentication scheme using public key cryptographic techniques in cloud computing. Many homomorphism encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the user to verify that the cloud returns correct results.

Accountability in cloud: Neither the clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed;

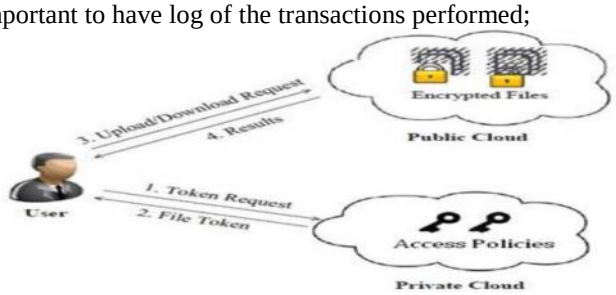

Fig.1. System Architecture

The details of the proposed scheme are shown in Fig.1. The detailed description of model is as follows:

- there are three users, a creator, a reader, and writer.
- Creator Alice receives a token γ from the trustee, who is assumed to be honest. A trustee can be someone like
- the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token γ.
- the access policy decides who can access the data stored in the cloud. The creator decides on a claim
- Policy y, to prove her authenticity and signs the message under this claim.

III. System Analysis

Existing System:

- Existing work on access control in cloud are centralized in nature. Except and, all other schemes use ABE. The scheme in uses a symmetric key approach and does not support authentication. The schemes do not support authentication as well.
- It provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users.

Disadvantages Of Existing System:

- The scheme in uses asymmetric key approach and does not support authentication.
- Difficult to maintain because of the large number of users that are supported in a cloud environment.

Proposed System:

- We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication.
- In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data.
- Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information.
- The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud.

Advantages Of Proposed System:

- Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
- Authentication of users who store and modify their data on the cloud.
- The identity of the user is protected from the cloud during authentication.

IV. Comparison With Other Access Control Schemes In Cloud

We compare our scheme with other access control schemes (in Table 1) and show that our scheme supportsmany features that the other schemes did not support. 1-W-M-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read. We see that most schemes do not support many writes which is supported by our scheme. Our scheme is robust and decentralized; most of the others are centralized. Our scheme also supports privacy preserving authentication, which is not supported by others. Most of the schemes do not support user revocation, which our scheme does. In Tables 2 and 3, we compare the computation and communication costs incurred by the users and clouds and show that our distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud. If we compare the computation load of user during read we see that our scheme has comparable costs. Our scheme also compares well with the other authenticated scheme.

A. Security of the Protocol Theorem 1: Our access control scheme is secure (no outsider or cloud can decrypt ciphertexts), collusion resistant and allows access only to authorized users.

Proof: We first show that no unauthorized user can access data from the cloud. We will first prove the validity of ourscheme. A user can decrypt data if and only if it has a matching set of attributes. This follows from the fact that access structure S Even if it colludes with other users, it

cannot decrypt data which the users cannot themselves decrypt, because of the above reason (same as collusion of users). The KDCs are located in different servers and are not owned by the cloud. For this reason, even if some (KDCs are compromised, the cloud cannot decode data.

Theorem 2: Our authentication scheme is correct, collusion secure, resistant to replay attacks, and protects privacy of the user.

Proof: We first note that only valid users registered with the trustee(s) receive attributes and keys from the KDCs. A user's token is Kbase; K0 where is signature on ukK base with TSig belonging to the trustee. An invalid user with a different user-id cannot create the same signature because it does not know TSig.

Results

Screen Shots

V. CONCLUSION

We propose secure cloud storage using decentralized access control downloading of a file to a cloud with standard Encryption/Decryption is made as easy as possible. The renew key is added with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal, then upload the new renew keys to the files stored in the cloud. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

VI. REFERENCES

[1] SushmitaRuj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, IEEE, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[2] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp.Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[4] 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.

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

[6] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (Cloud Com), pp. 157-166, 2009.

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

[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[9] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trust cloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[11] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[12] 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.