World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 3.419

ANONYMOUS AUTHENTICATION TO CLOUD DATA STORAGE USING DECENTRALIZED ACCESS AND LOGGING SYSTEM

Manasi S. Jarande*[1] and Uma R. Godase[2]

[1]Research Student, Department of IT, Sinhgad College of Engineering, Pune, India.

[2]Assistant Professor, Department of IT, Sinhgad College of Engineering, Pune, India.

Article Received on 29/07/2016 **Article Revised on 18/08/2016** **Article Accepted on 06/09/2016**

***Corresponding Author**
Manasi S. Jarande
Research Student,
Department of IT, Sinhgad College of Engineering,
Pune, India.

ABSTRACT

Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be deal with. Security and privacy are very important issues in cloud computing. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Users are authenticated who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. The protocol supports multiple read and writes on the data stored in the cloud. It is proposing privacy preserving authenticated access control scheme. According to the scheme a user can create a file and store it securely in the cloud. The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The 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. The work proposes a new decentralized access control scheme for secure data storage in clouds, which supports anonymous authentication. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized.

KEYWORDS: Access control, Authentication, Cloud computing, Encryption, Attribute-based encryption, Authentication.

INTRODUCTION

Cloud computing can be identified as an alternative to existing information technology [2] as it has built in resource sharing and low maintenance capability. Cloud provides many different types of services like software/application as a service (e.g. Google Apps), infrastructure in form service (e.g. Amazon's EC2) and platform as a service which share common forum for writing an application and saves the cost. The data stored on cloud is valuable as well as highly sensitive. For example, medical records in hospital and project, client related information in any organization. There are numerous services provided to users like Net banking, social networking through internet. When internet comes into picture, at that time security of data also becomes very important factor. Considering cloud as a storage three main issues are integrity, availability and confidentiality. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.[3] Access control plays major role for authentication and authorization of data. It is important because only valid or authorized user should able to access the data. There are different types of techniques are available for access control like Role based access control (RBAC), attribute based access control (ABAC) and user based access control (UBAC). User based access control maintains details of users and it based on that user gets different types of accesses but if there are large number of users then in that case it is not suitable method. Role based access control maintains a hierarchy of user and based on the different roles of user the access is provided. Attribute based access control is wider in scope as it takes the attributes of users and access policy attached with those attributes. Advantages and disadvantages of role based as well as attribute based authentication is discussed in.[4] Anonymous authentication concept contributes main part in this system.[5] Anonymous authentication means that user can send query to the cloud and can acquire the result without revealing its identity. Cloud server does not know the details of user so user data is secure in this method. User revocation in cloud computing is becoming a challenge. In attribute based encryption this challenge is becoming more difficult as multiple users are using the same set of attributes to access the data. Sometime revocation of one user may affect the other user as his/her attributes are shared on cloud but as compare to other systems in ABE, revocation is more flexible.[6] In cloud computing, users can contract out their computation and storage to servers (also called clouds) using Internet. There are number of services provided. Infrastructures (e.g.,

Amazon'sEC2, Eucalyptus, Nimbus), and platforms (e.g., Amazon's S3, Windows Azure can be provided by cloud to help developers. Information stored in clouds is very much sensitive. For example, medical records and social networks are very sensitive. In cloud computing the very big issues are Security and privacy. Very first user should be the valid one that is authenticated user and in second step integrity of the data should get maintained. One of the most fundamental services offered by cloud providers is data storage. Let us assume an example of company or organization there may be several levels of employee. There are many files available which can be accessible by particular department's employee or employee from specific project. That kind of security should be maintained. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To maintain the data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

2. LITERATURE REVIEW

In this literature survey different techniques related to attribute based encryption are studied. These systems and their description are follows.

2.1 Existing System

- **Fuzzy Identity-Based Encryption - By: A. Sahai and B. Waters [4]**

A user has a set of attributes in addition to its unique ID. It introduced a new type of identity based encryption that is FIB. The major difference between IBE and FIB is that in FIB identity is set of attributes. For a cipher text w encrypted for an identity w this scheme allows to decrypt with an identity w' if and only if the identities w and w' are close to each other. This construction makes the scheme suitable for biometric usage. Because each time biometric identity is sampled. There will be difference in each sample, but if enough

attributes are equal, two identities can be considered to be the same. In addition, this can also be used in ABE where the users having mentioned set of attributes can decrypt the cipher text.

Advantages

1. Error tolerant means that the identity that was used for encryption is not needed to be exactly same as the one used for decryption but they have to be equal in sufficient many attributes.
2. It is secured against collusion attack- The process of receiving private key is very natural because authentication does not require any additional certificate only user should satisfy the biometric properties. So, no two users can prove the same identity.

- **Attribute-Based Encryption for Fine-Grained Access Control of Encrypted- By: V.Goyal, O. Pandey, A. Sahai and B. Waters[15]**

The goal of this system is to provide security and access control. Attribute base access control is more extended in scope, in which users are given attributes, and the data has attached access policy. Considering the user attributes revocation concept is implemented. A revoked attributes and keys of users cannot write again to stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes.

Advantages

1. Main advantage of attribute based encryption is secret key is associated with attributes which provide the strongest criteria for the security of the system.
2. Implementation for Revocation of user becomes easy.

- **Decentralizing Attribute-Based Encryption - By: A.B. Lewko and B. Waters [16]**

In this paper Multi-Authority Attribute-Based Encryption (ABE) concept is implemented. In this system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. This system does not require any central authority. In this system each component has come from a potentially different authority, where there is no coordination between such authorities. It provides new

techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

Advantages

1. Here the system is not depends on any single authority hence an absence of any authority does not collapse the system. Because of number of authorities this system maintains effectively with global co-ordination.

- **Outsourcing the Decryption of ABE Cipher Texts - By: M. Green, S.Hohenberger, and B. Waters[14]**

One of the main efficiency drawbacks of ABE is that the size of the cipher text and the time required to decrypt it grows with the complexity of the access formula. In this work, implementer proposed a new paradigm for ABE that largely eliminates this overhead for users. The core change to outsource able ABE systems is a modified Key Generation algorithm that produces two keys. The first key is a short type secret key that must be kept private by the user. The second is what we call a "transformation key", TK that is shared with a proxy.

Advantages

1. Provide efficient technique by using which the required time for encryption and decryption of data is done efficiently.

3. SYSTEM ARCHITECTURE

This section contains the whole detail description of system and different parts of the system. Main idea of the system is given with the help of following main sections.

- Anonymous Authentication
- Logging
- Revocation

3.1 Anonymous Authentication

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, research chairs of universities in the country, and students belonging to Law department in all universities in the province. She wants to remain anonymous while publishing all evidence of malpractice. She stores the

information in the cloud. Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. The problems of access control authentication and privacy protection should be solved simultaneously. This system addresses this problem in its entirety into implementation. She wants to remain anonymous, while publishing all is the key solution of above mentioned problem. All information is stored in the cloud. It is important that users should not be able to know her identity, but must trust that the information is from a valid source. For this reason she also sends a claim message which states that she "Is a law student" or "Is a student counselor" or "Professor at university X."To implement this solution below steps are used in this system's implementation. Figure 1 is showing solution to this problem.

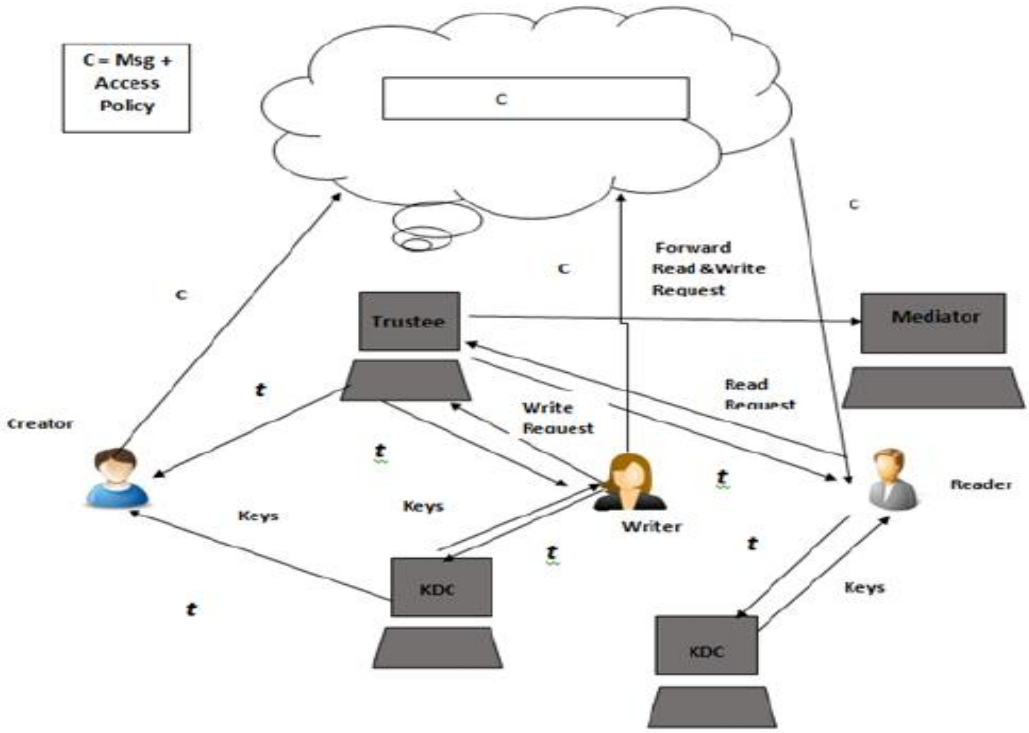

Fig 1: DAAC System Architecture

Steps to Fix the Problem

1. The scheme uses the protocol Attribute Based Access Control. There are three main users, a creator, a reader, and a writer.
2. Creator Alice receives a token t from the trustee, now it is assumed that trustee is honest one. This token is given only if the user is proved as a valid user.
3. The message MSG which is to share is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator defines a claim policy Y to prove the authenticity and signs of the message under this claim.

4. The ciphertext C with a signature c is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read the message it sends request to trustee. Trustee then forwards this request to Mediator. Mediator verifies it and then cloud sends Cipher text C to user. That the user has attributes matching with the access policy, it can be decrypted and get back the original message.
5. 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.
6. When a reader wants to read some data stored in the cloud, it tries for decrypting and using the keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.
7. Here Mediator is responsible for approving/verifying the user request. Once the request is approved by the user, user is free to perform required operation.

3.2 Logging

In order to achieve the accountability of the system, logging system is implemented.

Figure is showing the general flow logging system which is implemented into the system.

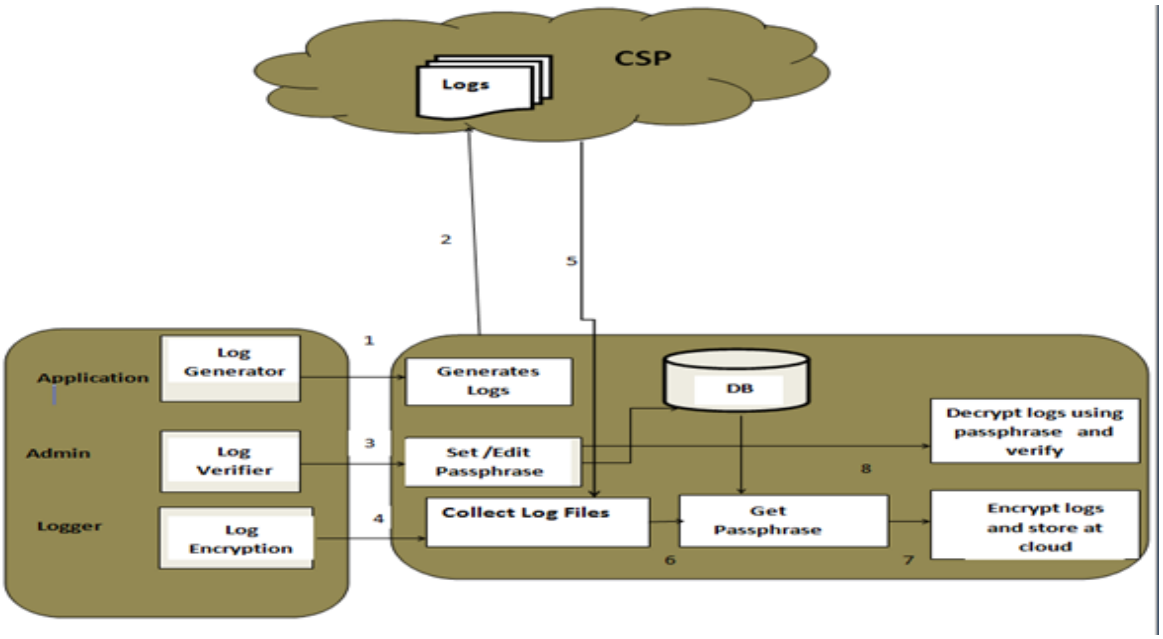

Fig 2: Logging System

As shown in figure 2 there are three main part of this logging system.

- **Application**

Log application is mainly responsible for maintaining all the activities of the user.

This application is responsible for generating user activity log hourly basis. These logs can be used for further verification purpose.

- **Admin**

It is one of the users of the system. Admin has authorized access to the logs. These log files are stored at one location by log generating application.

- **Logger**

Logger is mainly responsible for encrypting of the log files.

Steps performed in Logging functionality

1. Log generator generates logs and store at cloud location.
2. Admin does login and set passphrase at the first time of logging.
3. Logger gets a passphrase and encrypts the log files at other location.
4. Admin can get the original logs by decrypting the logs using passphrase.
5. Admin has authority to edit the passphrase.

3.3 Revocation by Trustee

There are basically two types of revocations are implemented in this system as shown in the figure 3. The implemented revocations are Attribute Revocation and User Revocation.

- **Attribute Revocation**

There is case when any one of the attribute is not necessary for applying an access policy. So, this functionality enables to use any attribute whenever required. For this implementation flag is maintained to keep or revoke an attribute from the system. According to ON of OFF state of flag trustee can view the structure of attribute within the system.

The lists are

ASL (Attribute Structure List)

The structure of this list is as shown in figure 3.

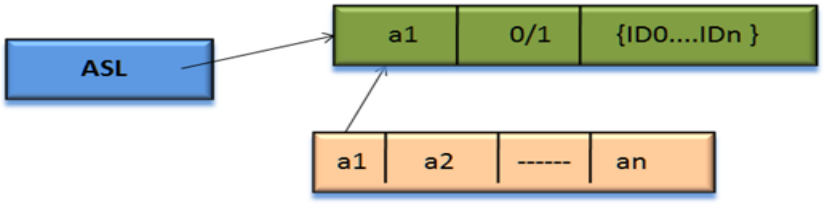

Fig 3: Attribute Structure List

Here, ASL has two main parts attribute list and their detail fields. Each attribute has flag and user list. Flag indicates whether an attribute is in system or not. ID is nothing but the user id

that uses all those attributes. When the flag is ON then user list is empty as all users are open to use this attribute. In case of OFF condition list contains the users which are not allowed to access the file associated with those attributes.

URL (User Revocation List)

There are many scenarios whenever there could be situation when user needs to be revoked from the system. In that case trustee has the right to revoke those users from the system. Figure 4 shows the structure of URL.

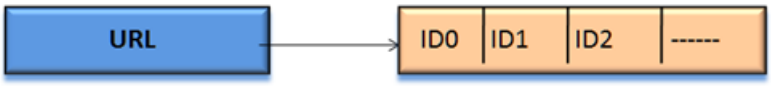

Fig 4: User Revocation List

4. RESULT ANALYSIS

There are some key differences into the existing and proposed system. These differences make the proposed system stronger. Below table is showing the summary of comparison. As per the table 1 these parameters are important to isolate the result of the existing and current system.

Table 1: Existing System vs. Current System

Sr. No	Parameter	Need	Existing	Proposed
1.	Encryption of Access Policy	Unauthorized User should not able to edit access policy.	No	Yes
2.	Mediator Availability.	To reduce the load of Trustee and to make system faster.	No	Yes
3.	Attribute Revocation	To maintain the dynamic nature of the system	No	Yes
4.	Logs Generation	To implement the concept of Trust Cloud	No	Yes
5.	Logs Encryption/Decryption.	To maintain the anonymous authentication of the system as well as to maintain Trust clouds	No	Yes.

4.1 Encryption of Access Policy

If we keep the access policy in original format then any unauthorized user can access and see the plain original data. In order to keep it safe encryption of access policy of each file is important.

4.2 Mediator Availability

Trustee and Mediators are two main actors from the system. Trustee has to perform many activities hence to reduce the load of trustee the concept of mediator is implemented. Where

trustee forwards the read or write request to Mediator. Mediator approves this request based on the access policy.

4.3 Attribute Revocation

To maintain the dynamic nature of the system whenever need of attribute is into the system at the time it is activated or deactivated.

4.4 Logs Generation and Logs Encryption/Decryption

1. The system is anonymous in nature so there maybe possibility that the user or CSP reject any operation which actually done by them. In such scenarios logs are important and they can be used as a proof. It also plays major role in auditing and reporting.
2. At the same time the main nature of system i.e. anonymity should be maintained. That is no one except an authorized person can see the activities of the user. So it is necessary to make logs more secure and for this purpose encryption and decryption of logs is done. Hence only authorized person that is Admin can decrypt the logs and can see the detail activities.

4.5 Computation Cost Analysis

Experimental analysis is done for system on 4GB RAM machine. The current system uses AES algorithm to encrypt the file data before uploading file on cloud. To perform encryption operation this system requires 2.6 ms for file size of 6MB and 1.3 ms for 3MB file. As comparing with existing system it requires 2.9 ms and 1.45 ms of file size 6 MB and 3MB respectively. Figure is showing graphical representation of the same. As shown in graph as compared to existing system time required for encryption of data in proposed system is less.

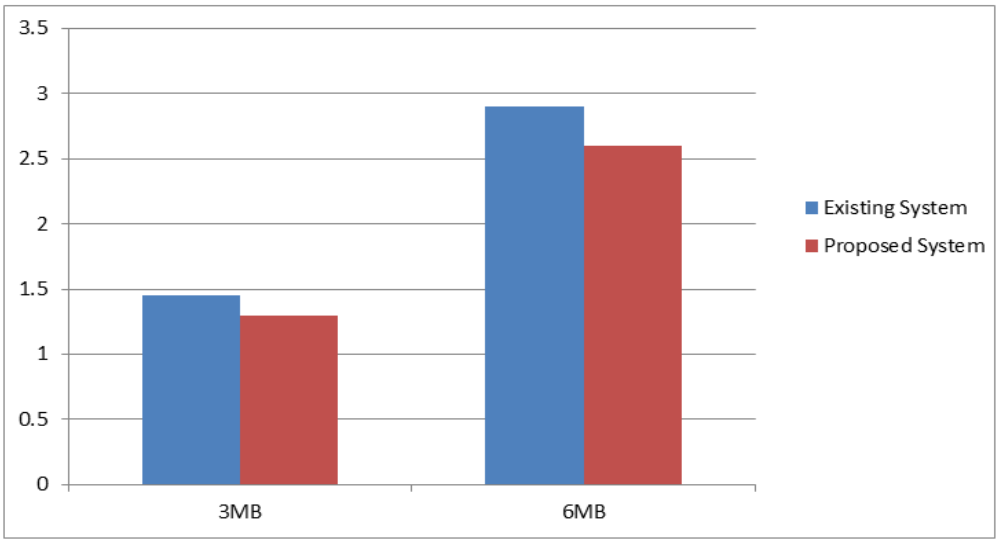

Fig 5: Graph for time requirement to encrypt the file data.

REFERNCES

1. S. Ruj and M. Stojmenovic, “Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,” 2014; 25(2): 384–394.
2. X. Jing and Z. Jian-jun, “A brief survey on the security model of cloud computing,” in Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2010; 475 – 478.
3. R. Chandramouli and P. Mell, “State of security readiness,” in Crossroads. ACM, 2010; 23–25. Efficient Search.
4. A. Sahai and B.Waters, “Fuzzy identity based encryption,” in Advances in Cryptology, vol. 3494 of LNCS. Springer, 2005; 457 – 473.
5. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, 2007; 321-334.
6. Dan Cao, Xiaofeng Wang, Baokang Zhao, Jinshu Su and Qiaolin Hu, "Mediated attribute based signature scheme supporting key revocation," Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference on, Jeju Island, Korea (South), 2012; 277-282.
7. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, “Trustcloud: 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.
8. A.Shamir, "Identity-Based Cryptosystems and Signature Schemes," Advances in Cryptology-CRYPTO’., 1984; 84: 47-53.
9. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABECiphertexts,” Proc. USENIX Security Symp., 2011.
10. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, 2006; 99- 112.
11. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy AttributeBased Encryption," Proceedings of the IEEE Symposium on Security and Privacy, Washington, DC, 2007; 321-334.