ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Anonymous Authentication and Access Control of Data Stored in Multi-Clouds

Rajalekshmi V[1], Lashma K[2]

[1]Student, Dept. of CSE, SBCEW, Ayathil, Elavumthitta, Pathanamthitta, Kerala, India

[2]Assistant Professor, Dept. of CSE, SBCEW, Ayathil, Elavumthitta, Pathanamthitta, Kerala, India

ABSTRACT: Providing secure and efficient access to large scale outsourced data is an important component of cloud computing. It provides a new method for information processing. Since many servers are untrusted, security factors like confidentiality, integrity and privacy of client's data concerns more. Data access control is also an important component in cloud computing. To ensure those security factors, we have to control the access of data. To provide more security we can use different types of encryption schemes to encrypt data, that are to be stored in clouds. In this paper, a decentralized access control mechanism is provided for data stored in clouds. Also data is stored in multi-clouds to ensure more security. We can also send highly confidential files using this, by hiding it in an image. Attribute Based Encryption algorithm is used for encrypt data. Data owners encrypt data using some attributes and store the encrypted data in cloud. Those clients who match the attribute can decrypt the actual data. Data owners can be anonymous if they want to be.

KEYWORDS: Cloud computing, Decentralized, Data access control, Attribute Based Encryption, Multi-cloud and Anonymous.

I. INTRODUCTION

While the concept of cloud computing provides a new method for information processing, the security problems must be properly solved before the services can be widely deployed. Since many service providers are untrusted, the confidentiality, integrity, and privacy of the clients' information must be protected by some mechanisms. Cloud computing, is a widely adopted paradigm that offers delivery of services over the internet. Users can store, read, and write their data into clouds. In cloud, sensitive information of different parties is stored normally in remote servers and locations and possibilities of this being exposed to unwanted parties where cloud servers are compromised. The security challenges for cloud computing approach are dynamic and vast. Data location, security and privacy are crucial factors in cloud computing security. Encryption methods, protection for actual hardware, data have any back up, any firewall setup, is information separated from other companies etc. are some of the factors which make sure about the data security in cloud. These services are different for different cloud service providers.

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks [1]. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. 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.

The foundation of cloud computing lies in the outsourcing of computing tasks to the third party [2]. It entails the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept intact is especially vital since the clients do not store these data locally. Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi-cloud servers, the distributed storage and integrity checking are indispensable.

Security and privacy protection in clouds are being explored by many re searchers. Wang et al. [3] addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied. Many homomorphic encryption techniques have been suggested to ensure that the cloud is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives cipher text of the data and performs computations on the cipher text 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. Anonymous access control is a very desirable property in various applications e.g. encrypted storage in distributed environments; and Attribute Based Encryption (ABE) is a cryptographic scheme that is targeted to achieve this property. ABE is an encryption mechanism that is useful in settings where the list of users may not be known apriori, but all users may possess certain credentials which can be used in determining access control and at the same time providing a reasonable degree of anonymity.

This paper is organized as follows. Section 2 describes the related works of this paper. Section 3 explains the overall proposed system and section 4 explains the results. Section 5 concludes the paper and next section is acknowledgement.

II. RELATED WORK

Different algorithms are used to encrypt data in cloud. In [4] IDE (Identity Based Encryption) algorithm is used for encryption. In this algorithm the identity of the user is used as his/her public key and the private key is generated from the known identity. The problems of IDE is it needs a secure channel to send the users private key and also the users private key is known to private key generator. Fuzzy identity of a person is a set of descriptive attributes which a predefined error tolerance capability [5]. Here, these attributes are used as ones known public key. Attribute based encryption method is proposed by Sahai and Waters [6] in 2006. This method provides security and access control in a more efficient way. There are three participants in this schema Authority, data owner (sender) and data user (receiver). The role of authority is to generate keys for data owner's users to encrypt or decrypt data. In ABE, keys are generated according to attributes. These attributes should be predefined which are generated by the authority. The role of data owner is to encrypt data using public key and a set of attributes and that of user's role is to decrypt using private key sent from authority. Decryption is possible only if the attributes in the private key matches with the attributes in the encrypted data. KP-ABE (Key Policy Attribute Based Encryption) was proposed by Goyal [6] in 2006. This is a modified form of ABE and the encrypted data is described using a set of attributes and access policy is built in user's private key.

In 2007, Bethencourt et al. [7] proposed a cipher text policy attribute-based scheme, and the access policy in the encrypted data (cipher text). The access control method of this scheme is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access policy is in user's private key, but the access policy is switched to the encrypted data in cipher text policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message. In the access structure of this scheme, it adopts the same method which was depicted in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is very close to the traditional access control scheme. ABE with Monotonic access structure Uses AND gate, OR gate or k out of N threshold gate. This attribute based scheme is proposed by Ostrovsky et al [8] in 2007. The access formula of access structure in User's private key can represent any type through attributes such as negative ones. Hierarchical attribute based encryption (HABE) which is a combination of hierarchical identity based encryption and cipher text policy based encryption, is proposed by Wang et al, in 2011 [9]. To generate keys this scheme uses the property of hierarchical generation of keys in HIBE scheme. Disjunction Normal Form (DNF) is used to express the access control policy and all attributes in one conjunctive clause. MA-ABE (Multi Authority ABE) was introduced by V Bozovic, D Socek, R Stienwandt and Vil-lanyi [10]. To distribute attributes for users, this scheme uses multiple parties. MAABE is composed of k attribute authorities and one central authority. A value dk is assigned to each attribute authority. Here the recipient is defined by a set of attribute not by a single string.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

III. PROPOSED SYSTEM

Proposed system is a distributed access control of data stored in multi cloud so that authorized users with valid attributes can access them. Identity of the user is protected from the cloud during authentication. The architecture is decentralized means there is no a single Key Distribution Center (KDC) for key management. KDC is an in-built property in this paper. Revoked users cannot access the data after they have been revoked. The data owner needs to make a flexible and scalable access control policy to command users' access right, so that only the authorized users can access the data. Besides, for protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud. In the data encryption process, the data owner encrypt the data before uploading to the cloud; if the data user sends through a access request to the owner, then the owner would return the corresponding key to the data user. User can use this key for decryption of data. Attribute Based Encryption is used for encrypt the data. I.e. users with valid attribute can decrypt the data from cloud. Also highly confidential files are sending through this paper.

Here data is stored in multi cloud architecture. When data is uploaded to the cloud, the data gets stored on different cloud servers. If the file is missing from any cloud servers, we can access it from other without any latency. This paper is implemented as a privacy preserving authenticated access control scheme. According to this scheme a user can create a file and store it securely in the cloud.

KP-ABE (Key Policy ABE) is used in this paper. This algorithm is a version of ABE. KP-ABE is an access policy which is encoded into the user's secret key and a cipher text is computed with respect to a set of attributes. An important property which has to be achieved by KP-ABE is called collusion resistance. This basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a cipher text that neither of them could decrypt on their own (which is achieved by independently randomizing users' secret key). For example, imagine a confidential document about nuclear weapons which is encrypted under the attributes NUCLEAR and TOPSECRET. Then, only a user with a key for attributes NUCLEAR and TOPSECRET can decrypt the document, while users with TOPSECRET keys and NUCLEAR keys cannot [11]. In the case of Cloud storage, there is no information or anything about the server hosting the data, so being able to do access control with the encryption scheme is great. Many cloud storage systems are using ABE (Attribute Based Encryption) schemes. In this system they can encrypt data on the client side, using an access structure rather than in the cloud because the cloud is a third party server, so we do not trust it. That's why they are using the client side.

Key Policy Attribute based encryption algorithm has mainly 4 steps.

i. Set up
ii. Key generation
iii. Encryption
iv. Decryption

In the first step, set up, initialization is done. I.e., the owner can create data files of his/her own. The file can be txt, doc, pdf, audio, video etc. The owner wants to store this file securely in the cloud. For the secure storage of his/her data, the file must be encrypted and a key must be generated to encrypt the file. Since we are using ABE algorithm, the key generated is used as the attribute to encrypt the file. The encryption of file is based on this attribute. During the encryption this attribute is used as the key. AES (Advanced Encryption Standard) algorithm is used for encryption. With the attribute that is already predefined, the file is encrypted and store in the cloud. Since this paper is anonymous, the identity of the owner will remain as anonymous. No one can see who uploaded the corresponding file. This anonymous technique is useful in the cases where for e.g. if anyone wants to upload a highly confidential data and he/she do not want to reveal his/her identity then they can use this technique.

After encryption, the encrypted data is uploaded to cloud. The uploaded data is stored to more than one cloud servers, say three. Using any cloud service providers, created three cloud servers. When the data owner uploaded his encrypted data to cloud, that single data is get stored on these three cloud servers. If any user wants to get access on these data files, then he/she must send request to the corresponding owner of the file. Owner will send the key to the requested user. Then if the attributes are matched i.e. attribute used to encrypt the data and the attribute which is mailed by the owner to user matches, then user can decrypt the file. The three cloud servers have has significant storage space and computation resource to maintain the data. Whatever the owner uploads to cloud it is encrypted and get stored in this three clouds in encrypted format.

Highly confidential files can be transferred using this paper. i.e. If two data owners want to send any highly confidential data then using the same attribute encryption the data can be encrypted and can hide in an image and then

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

the image is sent to the other owner. The second owner can unhide the data from image only if he had the matching attributes. The first data owner will send the key by mail if the other one has matching attribute.

IV. SIMULATION RESULTS

The data file gets stored in the three cloud servers successfully. Through this paper redundancy is achieved. Since the same file is get stored in all the cloud servers we created, if any one of them loss, data can be retrieved from the other ones without any latency and the users don't get any information about the loss. H.Wang [2], in his paper multi cloud architecture is described. In that paper, the file is divided into different blocks and each block is get stored on each cloud servers. In that case if anyone the block gets damaged, then there is no use with other blocks, because if any of the blocks are missed then it will become an incomplete file. If client want that file he/she must again request to the owner and if the attributes are matched the owner will sent the key to client. This takes more time to get a file. So in this paper, instead of dividing file into blocks, the complete file is gets stored on all these clouds. So there does not occur any latency to get the file in case any of the one is missing or get damaged.

Anonymous property is also can be viewed in this paper. The identity of owner is kept anonymous and no one can view who is the owner of the file. Also when we consider the time taken to complete the encryption process, attribute based encryption algorithm with AES is less time consuming than other encryption algorithms.

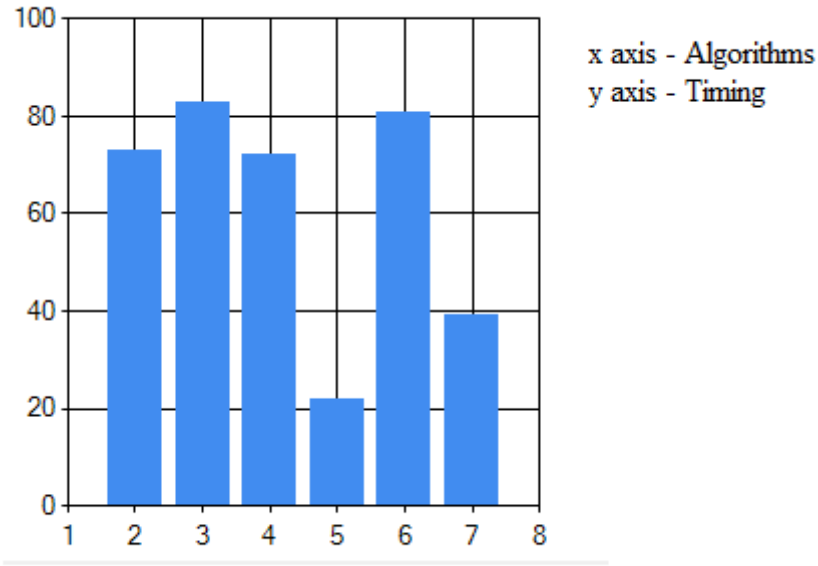

Fig.1. Time taken graph

In fig.1 x axis shows the algorithms and y axis shows the ratio of time taken to complete the encryption and decryption process. Here we can see that attribute based encryption with AES algorithm, algorithm 5, takes less time than others. Other algorithms we compared are Blowfish, DES, Triple DES, Rijndael etc. All other algorithms takes more time to complete the encryption and decryption process.

V. CONCLUSION AND FUTURE WORK

This paper implements a decentralized access control technique with anonymous authentication of data which is stored in multi cloud servers. Key distribution is done in a decentralized way. This scheme is robust and decentralized. It also supports privacy preserving authentication. While the concept of cloud computing provides a new method for information processing, the security problems must be properly solved before these services can be widely deployed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Since many service providers are untrusted, the confidentiality, integrity, and privacy of the client's information must be protected by some mechanisms. To achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service for users, this paper provides an effective and flexible distributed scheme with explicit dynamic data support, including create, read and write. Data is highly secured by ABE. Only those who have matching attributes can decrypt the data. Since data are stored in multi cloud, if any loss occurs we can get the data without any latency. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials.

VI. ACKNOWLEDGEMENT

Thanks to almighty, guide and our colleagues.

REFERENCES

1. S. Ruj, M. Stojmenovic, and A. Nayak, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, IEEE Transactions on parallel and distributed sytems, vol.25, no.2, pp.384-394.February 2014.
2. H.Wang, Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage, IEEE Transactions on service computing, vol.8,no.2, pp-328-340, March 2014.
3. S. Kamara and K. Lauter, Cryptographic Cloud storage, Proc. 14th Intâl Conf. Financial Cryptography and Data Security, vol.6054, pp. 136-149 2010.
4. H. Li, Y.Dai, L. Tian, and H.Yang, Identity-Based Authentication for Cloud Computing, Proc. First Intl Conf. Cloud Computing (CloudCom), Vol.5931, pp. 157-166,December 2009.
5. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, Fuzzy Keyword Search Over Encrypted Data in Cloud Computing, Proc. IEEE INFO-COM, pp.1-5, March 2010.
6. 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.
7. J. Bethencourt, A. Sahai, and B. Water, Ciphertext-Policy Attribute-Based Encryption, Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
8. R. Ostrovsky, A. Sahai, and B. Waters, Attribute- Based Encryption with Non-Monotonic Access Structures, Proceedings of the 14th ACM conference on Computer and communications security, pp.195-203, 2007.
9. G. Wang, Q. Liu, and J. Wu, Hierarchical Attribute Based Encryption for Fine-Grained Access Control in Cloud Storage Services, Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp.735-737, 2010.
10. Bozovic, D. Socek, R. Steinwandt, and V. I. Vil-lanyi, Multi-authority Attribute-Based Encryption with honest-but-curious Central Authority, International Journal of Computer Mathematics, Vol.8, Issue.3, pp.268-283, 2012.
11. http://crypto.stackexchange.com/questions/18123/what-is-themotivation-behind-key-policy-attribute-based-encryption?lq=1

BIOGRAPHY

Rajalekshmi V is an M.tech Student in the Computer Science Engineering Department, Sree Buddha College of Engineering for Women, M G University. She received Bachelor of technology in Computer Science Engineering in 2013 from Kerala University, India. Her research interests are Cloud computing, Computer Networks etc.