International Conference on Systems, Science, Control, Communication, Engineering and Technology 2015 [ICSSCCET 2015]

ISBN	978-81-929866-1-6
Website	icssccet.org
Received	10 - July - 2015
Article ID	ICSSCCET040

VOL	01
eMail	icssccet@asdf.res.in
Accepted	31- July - 2015
eAID	ICSSCCET.2015.040

DECENTRALIZED ACCESS CONTROL WITH ADVANCED ENCRYPTION STANDARD AND ANONYMOUS AUTHETICATION FOR USERS IN CLOUD

T.Yawanikha[1], Bavithra Madhuranjani.K.S[2], S.Ganapathiammal[3]

[1]Assistant Professor-IT, Karpagam Institute of Technology, Coimbatore, India

[2]PG Scholar, Hindusthan College of Engineering & Technology, Coimbatore, India

,[3]Assistant Professor-IT, Karpagam Institute of Technology, Coimbatore, India

ABSTRACT: *Cloud computing is one of the recent trends emerging in the field of Information Technology, it mainly focuses on global access of data. Data sharing is an important functionality in cloud storage at the same time, threat is an issue. This system proposes an access control scheme for secure and scalable data storage in cloud and supports anonymous authentication. In the proposed system the cloud verifies the authenticity of the user without knowing the user's identity. The Advanced Encryption Standard algorithm is used to for scalable data sharing where a set of secret keys are comprised as a single key encompassing the power of all secret keys. Access policies with several forms are used securely and they decide who can access the data stored in the cloud. Most systems do not support many users to have write permission which is supported by this system and access policies are hidden. System will process only the encrypted data so that confidentiality will be maintained. This system will also prevent replay attacks. The Key Aggregate mechanism will decrease the bandwidth used for the communication and reduce the rounds of communication.*

Keywords: ***Advanced Encryption Standard, String matching algorithms, Attribute based encryption.***

I INTRODUCTION

Cloud is a market-oriented distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more combined computing resources based on service-level agreements (SLAs) recognized through intervention between the service provider and consumers. In cloud computing, users can farm out their computation and cargo space to servers (also called clouds) using Internet.

Clouds can afford several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).Security is needed because data stored in clouds is greatly sensitive, for example, medical records and social networks. User privacy is also required so that the cloud or other users do not know the identity of the user. Thus it is a complex system which possesses highly securable processes. So it must need a proper systematic scheme to manage data.

Transactions done in the cloud should also be noted periodically. The user should be confirmed and should give suitable permission for them. Permission criteria are carefully handled because users may change the data unnecessarily. Adding this kind of feature may automatically reduce the effectiveness of the algorithm, so the algorithm designed must be very efficient.

Cite this article as: T.Yawanikha, Bavithra Madhuranjani.K.S, S.Ganapathiammal. "DECENTRALIZED ACCESS CONTROL WITH ADVANCED ENCRYPTION STANDARD AND ANONYMOUS AUTHETICATION FOR USERS IN CLOUD." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 183-186. Print.

Consider the following situation: A student from a college found out some malpractices done by some employees in college. Then the student takes steps to tell the details about the malpractice done in the college. Now he will report the malpractice done by the employees of the college to the university which controls the college. While reporting there are some conditions to be checked seriously. First the student should prove the identity because the university should believe that the message came from an authorised person. Second there should not be any interference. Also if any change is done for the original message then it should be found out and the file is recovered. Thus in this paper the above problems are described and rectified.

Existing concepts in cloud are centralized nature so security can't be provided in a perfect manner. The schemes which use symmetric key encryption also not a better choice. Earlier work by Zhao 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. 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.

1.1 OUR CONTRIBUTIONS

The main contribution of this paper is

1) Access control with powerful scheme is used so that only valid users can enter/

2) Authentication of users is done during the registration phase itself.

3) The identity of the user is protected from the cloud during authentication.

4) Encryption is based upon aggregate key encryption which is highly secure.

5) The protocol supports multiple read and write on the data stored in the cloud.

6) Access policies are assigned to users during the registration phase itself.

II RELATED WORK

Attribute based encryption (ABE) was proposed by Sahai and Waters. In ABE, a user has a set of attributes based on the user in addition to its unique ID. In Key-policy ABE or KP-ABE (Goyal et al), 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 Cipher text-policy, CP-ABE, the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase proposed a multi-authority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority 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 reduce or block replay attack we use string matching algorithms which are more efficient and perfect in security. It works more efficient than all other matching algorithms.

III BACKGROUND

In this section, we describe our cloud storage model, adversary model and the assumptions we have made in the paper.

We make the following assumptions in our work.

1) The cloud is insecure and to make it secure, the data is classified and given class indexes.

2) Users can have either read or write or both accesses to a file stored in the cloud.

3) All communications between users/clouds are secured by Secure Shell Protocol, SSH.

4) The cloud supports all sorts of traffics.

IV PROPOSED SCHEME

We explain public-key cryptosystems which produce a set of constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts is possible. The best thing is that it is very easy to combine encryption key into a single key, but encompassing the power of all the keys being aggregated. The secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential and very much authenticated. This matching aggregate key can be easily send to others or be stored in a storage media with very limited secure storage. We provide formal security analysis of our schemes in the standard model. Our schemes give the first public-key patient-controlled encryption for flexible hierarchy and security, which was yet to be described.

Advanced encryption standard scheme consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher text classes via Extract.

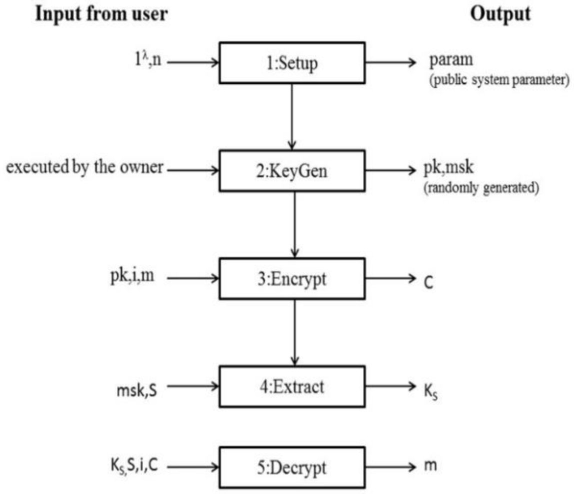
The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt.
The aggregate key cryptosystem is explained as follows the Figure 2 shows the flow of variables for generating the aggregate key and decryption of the messages using the aggregate key. Setup (1^{λ}; *n*): executed by the data owner to setup an account on an untrusted server. On input a security level parameter $1^{\lambda}$and the number of cipher text classes n (i.e., class index should be an integer bounded by 1 and *n*), it outputs the public system parameter *param,* which is omitted from the input of the other algorithms for brevity. KeyGen: executed by the data owner to randomly generate a public/master-secret key pair (*pk*; *msk*). Encrypt (*pk*; *i*;*m*): executed by anyone who wants to encrypt data. On input a public-key *pk*, an index *i* denoting the cipher text class, and a message m, it outputs a cipher text C. Extract (*msk*; *S*)*:* executed by the data owner for delegating the decrypting power for a certain set of cipher text classes to a delegatee. On input the mastersecret key *msk* and a set *S* of indices corresponding to different classes, it outputs the aggregate key for set *S* denoted by *KS*. Decrypt (*KS*; *S*; *i*; *C*): executed by a delegate who received an aggregate key *KS* generated by Extract. On input *KS*, the set S, an index i denoting the cipher text class the cipher text *C* belongs to, and *C*, it outputs the decrypted result , *m* if i is an element of *S*.

4.1 Setting Up The Cloud And Enabling Data Transfer

The cloud is setup using the Amazon EC2^{TM} and the security configurations are made. The cloud instances are setup in such a way that it will support all types of traffic like TCP, UDP etc. The various instances in the Amazon cloud communicates each other using socket programming. Initial module is setup using AES encryption for generating keys for the users. Basic file upload and download is done using socket programming.

4.2 User Authentication and enabling Advanced Encryption Standard

The data in the cloud is classified, and each class of data will be given a class index. All the keys of the data associated with the same class will be combined using the algorithm so that the data in the same class can be accessed using the aggregate key. When registering, the user will provide the keyword for authentication purpose. The users who are registered will be divided into several levels and these levels will be given separate key for data access. The keys will be generated based on the access rights of the user. Since the users with the same access rights will be given same keys, the number of keys used will be reduced.



4.3 User Revocation

The users with same access rights will have same set of keys. Before revoking the access rights of the user, it should be ensured that the user is not having the ability to access the data even if they possess the matching aggregate keys. So for doing that the data will be clustered again and the aggregate key will be generated. This aggregate key will be send to all users excluding the revoked user. So the previous set of aggregate keys will become useless. In doing the process, the security features will be enhanced and the system can be trusted more

V CONCLUSION

The data security is the highest discussed topic. As more crypto graphical tools come into existence, more it secure but at the same time, data security is threatened by attackers who can break through any kind of algorithm. The proposed scheme is secure like any algorithm that is used. The only difference is that the algorithm will reduce the rounds of communication, thereby enhancing the cloud environment. The scheme used here only tries to compress the set of secret keys and to make an aggregate key. Since users with same access rights will have same set of encryption keys, the complexity of the system will also get reduced. Since the keys are generated for a scalable amount of data, if the amount of data to be shared is increased, the number of classes of data will change and the aggregate

Cite this article as: T.Yawanikha, Bavithra Madhuranjani.K.S, S.Ganapathiammal. "DECENTRALIZED ACCESS CONTROL WITH ADVANCED ENCRYPTION STANDARD AND ANONYMOUS AUTHETICATION FOR USERS IN CLOUD." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 183-186. Print.

keys generated will also differ. The limitation in the scheme is the predefined number of cipher text classes. As far as cloud is concerned, the amount of data to be shared is increasing at a rapid and exponential rate. This problem can be rectified by registering additional key pairs for future purpose.

VI REFERENCES

1) SushmitaRuj, Milos Stojmeovic, Amiya Nayak" Decentralized Access Control with Anonymous Authentication of Data Sharing in Cloud"IEEE Transaction on Parallel and Distrinbuted System, Vol.25,no.2,2014.
2) Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" Vol.25,pp.468-477,2014
3) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
4) B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
5) S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.
6) F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.
7) 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.
8) S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.

Cite this article as: T.Yawanikha, Bavithra Madhuranjani.K.S, S.Ganapathiammal. "DECENTRALIZED ACCESS CONTROL WITH ADVANCED ENCRYPTION STANDARD AND ANONYMOUS AUTHETICATION FOR USERS IN CLOUD." *International Conference on Systems, Science, Control, Communication, Engineering and Technology (2015)*: 183-186. Print.