International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

Data Storage Security and Access Privilege Control in Cloud using Server Aided Attribute Based Encryption

[1] Ashish S [2] Sarala S M
[1] Dept. of Electronics & Communication Engineering in Siddaganga Institute of Technology, M.S. Ramaiah Institute of Technology [MSRIT] Bangalore, India
[1] ashish.mite@gmail.com [2] saralasm@msrit.edu

***Abstract*—Cloud computing technique is a new and precise data storage and access technology, in which the dynamic sharing of resources of the computer takes place dynamically via the Internet. This technology has gathered a remarkable amount of attention from educational and research institutes and industry. This computing virtualization enables flexible and low cost computing thus enabling it to be outsourced to the cloud servers thus making privacy a least concern. Although various schemes have been put forward to overcome the issue of privacy and safeguarding its information, it is quite understandable that the users of cloud would want to keep their identities private, and to review privilege control while they still get their privacy and so accessing this information should not cause reentrancy and an overhead during the communication. This paper, discusses a scheme for control on a semi-anonymous privilege scheme which ensures to address both data privacy and privacy of the user identity. Server Aided Cipher-text policy works by the principle that decentralizing the control authority will lessen the probability of the identity leakage and in this way it helps to achieve semi -anonymity. The data is encrypted in two hierarchies one credential uses AES encryption which occurs at the local slot and one in the medium with server host, SA-CPABE technique is used to accomplish this task.**

***Keywords:*—Anonymity, Advanced encryption standard (AES), SA-CBAPE, Cipher-text policy.**

I. INTRODUCTION

Cloud computing technique works by sharing the resources of computing instead of having end to end user specific and personal devices or local servers to manage operations. Using this computer resources are shared dynamically through the Internet. In the past decade, Rapid variation of Cloud Computing has shown us the view on how information or data is stored, exchanged, and privatized. Users can establish a virtual link which enables now to browse and interact via emails. Over time as the technology progressed, the developers ventured into creating online stores. The aim of online platforms was to completely replicate the scenario of real life into the virtual life.

The cloud computing has three challenges that should be taken care or handled before progressing. This includes data confidentiality, which merely acts on confidential information which is embedded in cloud and not totally under control of the users in most cases. This increases the risk level very much. Secondly, the risk associated with identity information being leaked is elevated because the identity of the user is authenticated according to his information. Users today give highest priority to safeguard their identity and privacy. Cloud computing has to take care of preserving these things. Preferably, one server authority should not completely know client's personal information. Also, the cloud system should not be resilient to attacks in which partial part of the system is hacked in and is accessible to the attackers. To overcome this problem many techniques have been put forward and are used to breach the above mentioned problems. All the above mentioned problems are fundamental and should be solved to extend the essence of the technology. To answer these there are various techniques that have typically been evaluated and some are outdated due to the progress in the security technology. One among these methods is developed by Shamir, and is called the identity based encryption.

The Identity based encryption, the user who send the message will specify an identity. This identity is used so as to match with only one other user (receiver) with exactly same identity. In the IBE, the sender/receiver information is contained in the private key and compromises in the key sharing can result in information leakage. To mitigate this problem associated with IBE – Fuzzy Identity-Based Encryption, known as Attribute-Based Encryption (ABE) proposed. In this method a user could decrypt the message if a set of attributes were same as those specified by the encryption. This however can't be used to generalize the system. General tree-based ABE schemes which include Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher-text-Policy Attribute-Based Encryption (CP-ABE),

are respectively used to overcome the issues associated with fuzzy IBE. They look identical, but the difference comes from the fact that the algorithms have a different key structure and cipher-text. Another important difference is that the encryption is carried out and the choice of policy is made by different parties. In the backdrop of KP-ABE, a cipher-text is linked with a set of attributes or dimensions, which partially and jointly illustrate the cipher-text's encryption protocol.

The decryption of the cipher-text happens if and only if the dimensions and properties in the cipher-text match with class tree in his private key. However the above environment does not suit the requirements of the methodology. At this present scenario small and medium scaled organizations cannot afford to build up their own cloud environment to use the fundamentals of identity. Key generators usually have access to user identities which are reflected by their attributes, The user is issued a private key by taking into account these user attributes. The primary intention of the users would be to keep their identities secret and private, but in the meantime accessing this information should not cause reentrancy and an overhead during the communication. Bhubaneswar et.al[4] designed a scheme known as the Fortified Access control for Multi-Authority Cloud Storage Systems. In FAC system the data access control process is made robust to make sure that the cloud data is safe. Fortified access control solves the issues related to data privacy, but also the use of multiple authorities in the cloud storage system, the scheme can efficiently provide a justifiable access control scheme and provide the feature of anonymous access to the cloud data.
Jung et.al [9] discusses a scheme for anonymously control the privilege by designing a control scheme *Annoy Control*. This scheme successfully mitigates the issues of data privacy and associated user identity privacy problems in existing cloud storage schemes. The scheme uses multiple authorities in computing, thus achieving anonymous cloud data access and very precise privilege control. The *AnonyControl* scheme is secure and efficient as shown by the security proof as well as by the performance analysis of the system.

When a mobile device is used for data access and encryption, the overhead in terms of time and computation complexity can be a very crucial aspect in power consumption of the device. This becomes a fundamental phenomenon to be addressed in case of battery operated devices. This is one of the important aspects addressed in the paper.

II. PROPOSED SYSTEM

The proposed system is schematically shown in the block diagram as shown in Figure1. It describes a total of four entities that constitute the system: the data owners (owners), the cloud server (server), the data consumers (users), the Multi-attribute authorities. The control on the access policies and encryption is vested in the hands of the owners. They then host the data on cloud in offloading. The server works to provide data access service to users. This is accomplished by storing the owners' data. These authorities have a multifold responsibility. Namely setting, revoking and updating user's attributes within the administration domain. These authorities are trusted by the users.

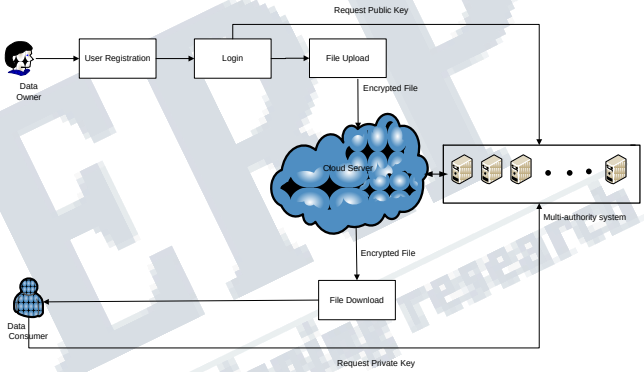

Figure 1Block diagram of the proposed system

III. FIRST LEVEL ENCRYPTION

Before uploading to the server, the uploading file will be subjected to a level of encryption. This is done using AES encryption.

A. AESENCRYPTION

Advanced Encryption Standard (AES) algorithm finds its application in the areas where security and speed are the major concerns. The advantage of the algorithm is that it can be implemented easily on both hardware and software. The encryption is carried out

B. SERVER AIDED-CPABE

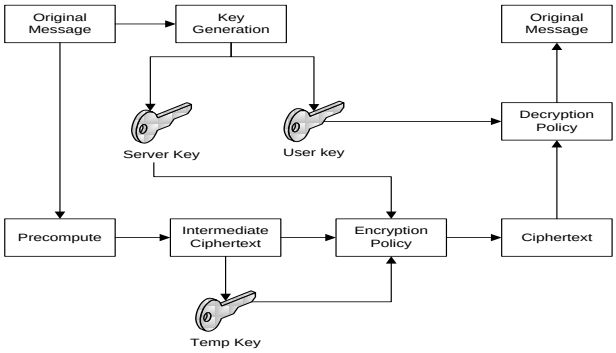

Figure 2Block diagram of the SA-CBABE

This model consists of a multi-authority system. Here every user has an ID. The users can interact with each of the key generating authority using different attributes which constitutes to pseudonyms. This on data blocks of 128 bits. The number of rounds of encryption depends on the key size and it can either 10, 12 or 14 rounds. The algorithm comes with the advantage that it fits in easily in small devices.

The algorithm involves transformations such as Sub bytes, Shift rows, Mix columns and add round keys. This constitutes to the encryption using AES.Decryption process involves the reversal of the steps involved in encryption. This is accomplished by using inverse operations. These operations are Inverse shift rows, Inverse substitute bytes, Add round key, and Inverse mix columns. The third step consists of XO Ring the output of the intermediates technique finds no replications to the method above. A user's pseudonyms are associated to his private key, but the authorities will not know about the private keys, and thus they will not be able to map onto a particular user based on his multiple pseudonyms. This also prevents them from identifying the same user in different transactions. In order to enhance this viewpoint the attributes are divided into N disjoint sets. And each of these set is maintained by one of the N authorities. By having this setup we ensure that an authority will only issue key components upon which it has control of. The advantage of this setup is that even if an authority is capable of linking an attribute to a user ID, it knows only a part of user attributes which cannot be used to deduce a user identity. This corresponds to the CP-ABE. However, we additionally tag it with the server for the second way of encryption which is called Server aided CP-ABE which happens at the host side providing along the security and the access privileges for the unit. However the detailed steps which associates with SA-CPABE is illustrated with the six steps below [6].

Setup: is identified with the small expression. The setup point issues two arguments one is the security parameter and the other one is total attribute description and thus showcasing the output with the public parameters PP (the data to be encrypted) and the master secret key MSK.

$$(\boldsymbol{\lambda}, \mathbf{U}) \rightarrow \mathbf{PP, SK} \qquad \mathbf{(1)}$$

KeyGen: The key generation function accepts three parameters as the argument one is the PP (public parameter), the secret key (MSK), and an attribute set S (User's Attribute) and outputs a user key K_{user} (Private Key) and a server key K_{server} (Public Key). The user keeps K_{user}locally, and gives K_{server} to its decryption server.

$$(\mathbf{PP}, \mathbf{MSK}, \mathbf{S}) \rightarrow \mathbf{K_{user}}, \mathbf{K_{server}} \mathbf{(2)}$$

Pre-compute: The pre-computation algorithm takes as input the public parameters PP and outputs a temporal key TK and an intermediate cipher-textIC. The user keeps TK locally, and stores IC on its storage server to save local storage resources.

$$(\mathbf{PP}) \rightarrow \mathbf{IC}, \mathbf{TK} \qquad \mathbf{(3)}$$

Encrypt: In the encryption side, three arguments are passed to the function as inputs an intermediate cipher-text IC, a temporal key TK, a message M, and an access structure A thus producing an intermediate encrypted output CT.

$$(\mathbf{IC}, \mathbf{TK}, \mathbf{M}, \mathbf{A}) \rightarrow \mathbf{CT} \qquad \mathbf{(4)}$$

Transform: The cipher-text transformation algorithm takes as input a server key $K_{server}$for attribute set S and a ciphertext CT that was Encrypted under A. It outputs the partially decrypted cipher-text CT if $S \in A$ and the error symbol $\perp$ otherwise.

$$(\mathbf{K_{server}}, \mathbf{CT}) \rightarrow \mathbf{CT} \qquad \mathbf{(5)}$$

Decrypt: The decryption algorithm takes as input a user private key $K_{user}$for S and a partially decrypted ciphertext CT that was originally encrypted

Under A. It outputs the message M if $S \in A$ and the error symbol $\perp$ otherwise.

$$(CT, K_{user}) \rightarrow M \qquad (6)$$

IV. RESULTS

Below table describes encryption and decryption time taken by the proposed system SA-CP-ABE. We can see the time taken by three different system ABE, CP-ABE and

proposed A-CP-ABE system which shows time taken by our proposed system is less compared with other two systems.

	File size	100 K.B	200 KB	300KB
Encryption Time	ABE	12	24.1	39
	CP-ABE	11.8	24	35.1
	SA-CP-ABE	10.5	20	30.5
Decryption Time	ABE	8	15.9	19.2
	CP.ABE	7	8.2	19.4
	SA.CP-ABE	6.3	11.2	16.8

Table1: Time taken in (MS) for encryption and decryption

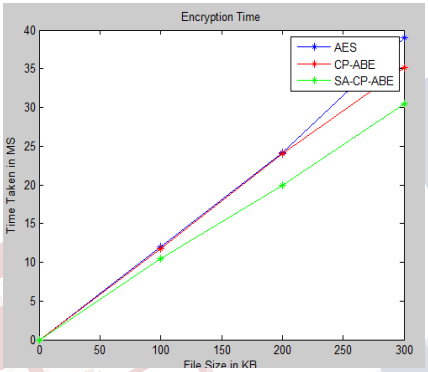

Figure 3: Comparison of Encryption time

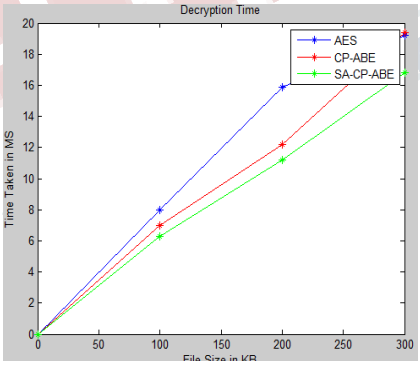

Figure 4: Decryption time comparison

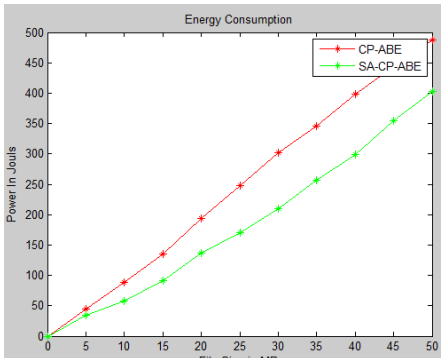

Figure 5: Power consumption comparison. Power consumed when Encryption done in local server and when encryption done by offloading to server using SA-CP-ABE when encryption done by offloading to server using SA-CP-ABE

V. CONCLUSIONS

The study helps to enhance the security associated with data when it is transmitted. The algorithm which is used in the proposed system gives the better security to the secret data compared to CPABE in terms of power consumption and encryption time. Since server offloading after precipitation is done, it helps in reducing the power consumption of the device.

REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO. Springer, 1985, pp. 47–53.

[2] John Bethencourt, Amit Sahai "Cipher-text-Policy Attribute-Based Encryption", IEEE, PP. 1-8, 2007.

[3] Bhuvaneswari Thangara" FAC-MACS: Fortified Access Control for Multi-Authority Cloud Storage Using CPABE",Volume 4, Issue 2, March-April 2015

[4] Taeho Jung" Privacy Preserving Cloud Data Access With Multi-Authorities", arXiv: 1206.2657v6 [cs.CR] 11Apr 2013.

[5] Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE Trans.Inform. Forensics Security, vol. 7, no. 2, pp. 826-832, April 2012

[6] Taeho Jung" Privacy Preserving Cloud Data Access With Multi-Authorities", arXiv: 1206.2657v6 [cs.CR] 11Apr 2013.