The Modern Cipher Text Policy over Multi-Authority using ABE Scheme Elements Overturning in Cloud Loading

Shaik Khadeer Pasha[1] P.Rathaiah[2]
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Sri Venkateshwara Engineering College, Suryapet

Abstract— The number of utilize in cloud computing are incrementing tremendously due to its advantage of providing flexible storage requisite. The users are commenced to apportion their sensitive information through the cloud due to its nature of providing accommodation to users. The security of the data has to be assured to the users when storing their details into the cloud server. The main objective of this paper is to amend the security and the efficiency while sharing the data between data owner and the users. Predicated upon the attributes of the users we are going to apportion the data. One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the fortification of policies updates. Cipher text policy attribute predicated encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of quandary. It enables data owners to define their own access policies over their utilizer attributes and enforce the policies on the data to be distributed. In this paper we incline to propose a revocable multi-ascendancy CP-ABE theme, and apply it because the underlying techniques to style the information access management theme. Our attribute revocation methodology will with efficiency distribute the goods each forward security and rearward security. This survey shows that revocable multi-ascendancy CP-ABE scheme is secure in the arbitrary location. Oracle model and is more efficient than anterior multi authority CP-ABE.

Key words: The Read Control, Multi-Authority, CPABE (Cipher Text Policy Attribute Encryption Scheme), Elements Overturning, Cloud Loading

I. INTRODUCTION

CLOUD loading is a consequential accommodation of cloud estimating, which compromises accommodations for data owners to host their data in the cloud. This incipient hypothesis of data hosting and data access accommodations introduces a great task to data read control. Because the cloud server cannot be plenarily trusted by data owners, they can no longer rely on servers to do read control. Ciphertext-Policy Attribute-predicated Encryption (CP-ABE) is considered as one of the most congruous technologies for data read control in cloud loading systems, because it gives the data owner more conspicuous control on read rules.

The CP-ABE scheme, there is an evidence that is conscientious for elements management and key allocation .The evidence can be the check office in a academia, the human resource department in a company, etc. The data owner defines the read rules and encrypts data according to the rules. Each utilizer will be distributed a confidence key redirecting its elements. A utilizer can decrypt the data only when its elements slake the read rules. There are two types of CP-ABE systems: single-ascendancy CP-ABE where all elementes are managed by a single- ascendancy, and multi-ascendancy CP-ABE where elements emanate from different domains and managed by different evidences. Multi-ascendancy CP-ABE is more opportune for data read control of cloud loading systems, as users may hold read distributed by multiple evidences and data owners may withal share the data utilizing read rules defined over read from different evidences.

Multi-ascendancy CP-ABE is mostly considered technology for data access control in cloud storage systems. Users may hold sundry attributes issued by multiple ascendant entities. The data access policy over the attribute is defined by the ascendant entities and not by the data owners. The subsisting system is not applicable for multiauthority cloud storage due to its attribute revocation quandary. If any attribute is revoked denotes all the Cipher text associated with the ascendancy whose attribute is revoked should be superseded or updated. The subsisting system relies on a trusted server.

II. RELATED WORK

Data access control scheme is more paramount hence more works have conducted in this field the paramount and cognate works have been discussed here.

A. Ciphertext-Policy Attribute Based encryption (CP-ABE) [1]:

Ciphertext-Policy Attribute Predicated encryption scheme represented a system for realizing intricate access control on encrypted data. Utilizing this technique encrypted data is kept confidential even if the storage server is untrusted. The proposed system sanctions for an incipient type of encrypted access control where user‟s private keys are designated by a set of attributes and a party encrypting data can designate a policy over their attributes designating which users can decrypt it. It was proved secure only under some general group heuristic, and not in other situations.

B. Single Authority Cipher text-Policy Attribute Based encryption [2] [3]:

Here there subsist only one ascendancy which provides attributes to multiple users. And all the attributes are managed by this ascendancy only. This engendered a security quandary and overhead to the ascendancy as all the users need to be maintained and managed by this ascendancy only. It was not efficient additionally.

C. Multi-Authority Cipher text-Policy Attribute Based encryption [4] [5]:

Here multiple ascendant entities subsist in the system all the ascendant entities are included in the distribution of the attributes to the users. This scheme is more congruous for data access control of cloud storage systems, as users may hold attributes issued by multiple ascendant entities and data owner can apportion the data utilizing access policies

defined on the attributes by different ascendant entities. This reduced the overhead of maintaining different users. Multi-ascendancy CP-ABE scheme represented attribute revocation quandary.

D. Attribute Revocation [6] [7]:

As multiple ascendant entities subsist there will be multiple attributes to the utilizer and the attributes can be transmuted dynamically. That is a utilizer can be given some incipient attributes by the ascendancy or revoked some subsisting attributes. This kind of attribute revocation should be considered accordingly. The incipient scheme surmounts the quandary of revocation [8] but still there subsist security quandaries in the subsisting system.

1) Proposed System:

The proposed system surmounts the quandary subsist in the subsisting system. We proposed an incipient algorithm designated as Amended Security data Access Control. This algorithm ameliorates the security of the system. The data owner when stores the data into the cloud server he encrypts it and then stores it. The keys will be provided to the sanctioned users by revered ascendant entities. So when the utilizer endeavors to access the data to which he is not having the eligible attribute the request gets repudiated and the utilizer gets blocked by the ascendancy. And ascendancy will additionally engender a message about the assailment to the data owner. So that data owner can take further action.

If the utilizer has done it by mistake the sanctioned utilizer can contact the data owner to unblock him. If the utilizer has not done it then withal the utilizer can contact the data owner and can ascertain more security by asking the data owner to transmute the authenticate details.

This incipient algorithm additionally provides data integrity. It apprises about the assailment by the un-sanctioned utilizer to data owner when data owner verifies about it. That is, when the data owner needs to check the files stored on the cloud frequently. If any modifications are found in the file on the server by any unauthorized access then this algorithm apprises the data owner that the file is not safe, it is modified.

Our system is proposed to do the following:

- Our system not only provides forward and rearward security but it withal provides ameliorated security by providing access control on sanctioned users.
- The algorithm proposed by us amends the security by apprising about the assailment to the data owner.
- We withal provided the data integrity. As the data owner comes to ken about the verification in the data stored when he verifies it.

2) System Architecture:

The figure shows the system architecture and it consists of the modules: Data owner, Cloud Server, Data Encryption and Decryption, Ascendancy, Data Consumer and Ameliorated Security

This architecture states that the owner outsources the data with the semi-trusted cloud servers with encrypted cryptosystems. When users want to access the data from cloud servers, users has to be maintained by the Certificate Ascendancy who issues the authentication certificate to utilizer to access data. After obtaining the certificate utilizer and owners share the data with the attributes verification for data access.

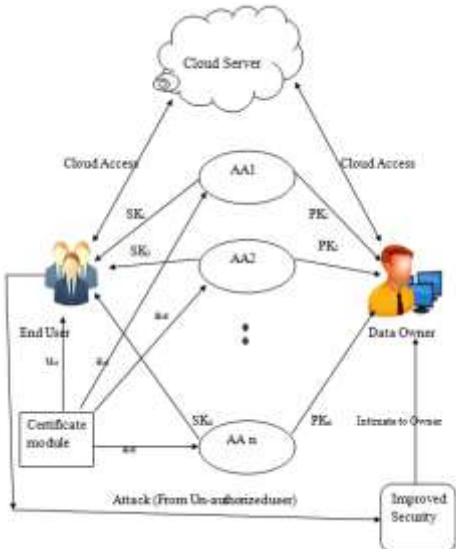

Fig 1: System Architecture Diagram Model.

In this system each utilizer has an ecumenical identity. The utilizer can have set of attributes which emanate from multiple attribute ascendant entities. The corresponding attribute ascendant entities entitle its utilizer associated with a secret key. The data is divided into several components by the owner and each data component is encrypted with different content keys utilizing symmetric encryption.

The access policies over the attributes are defined are defined by the owner and encrypts the content keys under the policies. The owner then sends the encrypted data together with the ciphertexts to the cloud server. The utilizer is able to decrypt the ciphertext only when the user‟s attributes slake the access policy defined in the ciphertext. The different number of content keys is decrypted by users with different attributes and from same data different information‟s are obtained.

III. IMPLEMENTATION

A. Certificate Authority:

The CA is an ecumenical trusted certificate ascendancy in the system. It establishes the system and accepts the registration of all the users and AAs in the system. For each licit utilizer in the system, the CA assigns an ecumenical unique utilizer identity to it and withal engenders an ecumenical public key for this utilizer. However, the CA is not involved in any attribute management and the engenderment of secret keys that are associated with attributes. For example, the CA can be the Convivial Security Administration, an independent agency of the Coalesced States regime. Each utilizer will be issued a Convivial Security Number (SSN) as its ecumenical identity.

B. Attribute Authorities:

Every AA is an independent attribute ascendancy that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics

of its attributes. Each AA is responsible for engendering a public attribute key for each attribute it manages and a secret key for each utilizer reflecting his/her attributes.

C. Data Consumers:

Each utilizer has an ecumenical identity in the system. A utilizer may be entitled a set of attributes which may emanate from multiple attribute ascendant entities. The utilizer will receive a secret key associated with its attributes entitled by the corresponding attribute ascendant entities.

D. Data Owners:

Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by utilizing symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute ascendant entities and encrypts the content keys under the policies.

E. Cloud Server:

Then, the owner sends the encrypted data to the cloud server together with the ciphertexts. They do not rely on the server to do data access control. But, the access control transpires inside the cryptography. That is only when the user's attributes gratify the access policy defined in the cipher text; the utilizer is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

IV. EXPERIMENTAL WORK

Fig 2: Admin Uploading Data to cloud.

Fig 3: Attribute Authority Activate to user page.

V. CONCLUSION

As the number of users in cloud computing incrementing security issues are withal incrementing accordingly. The main security issue can be how to control the unauthorized data access in cloud. In this paper we proposed an efficient data access control scheme with ameliorated security. Our scheme not only restricts the unauthorized access but additionally ascertains secure access by the sanctioned users. Along with that data integrity is additionally provided. This scheme is proposed for multi-ascendancy cloud storage system. This scheme can be applied in convivial networks which are online and withal in the remote storage systems.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[2] P. Mell and T. Grance, „„The NIST Definition of Cloud Computing,"" National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[3] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, „Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,"" in Proc. Advances in cryptology-EUROCRYPT'10, 2010, pp. 62-91.

[4] M. Chase and S.S.M. Chow, „„Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,"" in *Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09)*, 2009, pp. 121-130.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, „„Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,"" *IEEE Trans. Parallel Distributed Systems*, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[6] K. Yang, X. Jia, "Expressive Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", in *IEEE Transactions on Parallel and Distributed Systems,* vol.25, no.7, pp 1735-1744, July 2014.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. 10th IEEE Int'l Conf. TrustCom, 2011, pp. 91-98.

[8] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.

