Multi-Authority System on Cloud using revocable Data Access Control

Akshay Shrirao[1] Ajinkya Deshmukh[2] Dinesh Samudre[3] Samadhan Shinde[4]

[1,2,3,4]Department of Information Technology Engineering

[1,2,3,4]Sinhgad Institute of Technology, Lonavala, India

Abstract— Data access control is an effective way to make sure the data security in the cloud. There is not easy to handle the data in cloud storage management because of an untrustworthy server of the cloud. In cloud storage management there is a one Cipher text-Policy Attribute-based Encryption (CP-ABE) technology that is best suited for accessibility of data. By using this technology it provides permission to data owner instruct control on policies of the accessibility. In this cloud computing technology, a private key of every user defines the set of an attribute. Over the each attributes accessibility policies specified by using an encrypted cipher text. If the attributes satisfy the policy of cipher text then decryption done by the user. But in this technology accessibility of cloud storage is difficult to apply because of revocation problem of an attribute. In this paper, we proposed a revocable Cipher text-Policy Attribute-based Encryption (CP-ABE) multi-authority scheme and apply these techniques in the data accessibility system. This scheme used to find out the number of corrupted authority. The main goal is to meet multi-authority in cloud storage system.

Key words: attribute revocation, cloud storage, Access control, CP-ABE, multi-authority

I. Introduction

In cloud storage management cloud storage is eventful service. This system provides the usage service for the different owner for the purpose of hosting their application and data. Hosting and accessibility services provide the big challenge to access of controlling data. In cloud storage management there is a one Cipher text -Policy Attribute-based Encryption (CP-ABE) technology that is best suited for accessibility of data. By using this technology it provides permission to data owner instruct control on policies of the accessibility. In this technology, Attribute management, and key distribution can perform an authority that is responsible. The access policies and encrypted data are defined according to the policies by the data owner. For reflecting its attributes secret key is issued by each user. If its attributes satisfy the access policies then a user can decrypt the data. Single and multi-authority are the two types of the authority system. In the single authority, management of all attributes is done by the only single authority. In the multi-authority, management of all attributes and do is done by the multi-authority. The accessibility in cloud storage CP-ABE multi-authority scheme is best appropriate. Sharing of the data done by the data owner using access policies from different authorities defines over the attribute. For Example, in the Human resource department, department owner may share the data using the accessibility policies “researcher” and “helper”, the wherein organization helped the attribute “helper” is issued and in human resource, the attribute Researcher is issued by the administrators. However, attribute revocation problem is occurring then these multi-authority schemes is not easy to apply to multi-authority cloud storage system. In this paper, we define a revocable multi-authority CP-ABE scheme, where the attribute revocation problem can be solve by proposing an efficient and secure revocation method. By using this scheme, the forward and backward security can achieve. In the backward security, user required the revoke attribute to decrypt any new cipher text. And in the forward security if it has sufficient attribute then newly comes user can also decrypt the existing ciphertext. In our scheme fully trusted server does not require because key update by each attribute authority, not by the server. Then we construct the expressive, efficient and secure system for multiple authorities.

II. Literature Survey

A. *Cipher Text - Policy Attribute-Based Encryption:*

Author: John Bettencourt, Amit Sahai, 2007.

This paper discusses how several distributed systems if a user passes a certain set of credentials or attributes then a user should only be able to access data. The advantage of this paper is it highly improves the expressiveness of access control scheme, where remove the limitation that in a cipher text at most once each attribute can only appear. But the some disadvantage of this paper is it cannot provide high-level system requirement like usability.

B. *Bounded Ciphertext Policy Attribute Based Encryption:*

Author: Vipul Goyal, Abhishek Jain, 2008.

This paper discusses define supporting advanced access structures and number theoretic assumption for security proof. The advantage of this paper is to increase the performance by decreasing network traffic and the demerits is to decrease the communication capacity.

C. *Bounded Ciphertext Policy Attribute Based Encryption:*

Author: MELISSA CHASE, 2009.

This paper discusses Supporting advanced access structures and number theoretic assumption for security proof in encryption scheme is construction attribute of a ciphertext-policy. The advantages are to improve the efficiency of the attribute revocation method. But it cannot provide high-level system requirement like usability.

III. Existing System

The past ciphertext may be connected with the trait in a past variant, while the recently joined client may be issued a characteristic in another version attributes. Our plan does not require the server to be completely trusted, in light of the fact that the key overhaul is upheld by every trait power not the server. Regardless of the possibility that the server is not semi-confided in a few situations, our plan can at present ensure the regressive security. At that scheme, we apply our proposed multi-power revocable CP-ABE plan as the hidden procedures to develop the expressive, secure and revocable multi-power distributed storage frameworks of information access control plan.

A. Drawbacks Of Existing System:

1) Communication expense is more reason for encryption and unscrambling.
2) in the framework stockpiling overhead on every proprietor.
3) the stockpiling overhead on every client in our plan originates from the mystery keys issued by all.

IV. SURVEY OF PROPOSED SYSTEM

In this part, we can see and analyze the performance of the two schemes; one is the single authority scheme and multi-authority scheme, in the term of cost of communication efficiency and storage overhead. In the scheme, there are multiple authorities and each authority managed the attribute. In this paper for authenticating also, we propose two new techniques encrypted messages are more efficient than previous approaches. In the first method, we define the fact that encrypted message is also to be authenticated, with any of the secure encryption techniques, in the authentication process to append a short random string to be used. Then the random strings (character) are independently used for different operations, to allow for more efficient authentication and faster authentication algorithm can useful from the directness of unconditional (multi-authority) secure authentication, without manage the one-time keys. In the second method, block cipher based encryption algorithm is used to make the extra assumption further the first method improve the computational efficiency of the method. The driving motive behind our verification is that encryption algorithm used to authenticate exchanged messages might not be the most efficient solution in such systems and can lead to waste of resources already available, the security that is provided by the encryption algorithm.

A. Advantages Of Proposed System:

1) Make it more functional to distributed storage frameworks, in which information proprietors are not included in the key era. In particular, a client's mystery key is not identified with the proprietor's key, such that every client just needs to hold one mystery key from every power rather than different mystery keys related to various proprietors.
2) Enhance the proficiency of the characteristic renouncement system.
3) exceedingly enhance the expressiveness of our entrance control plan, where we uproot the confinement that every property can just show up at most once in a ciphertext.

V. SYSTEM ARCHITECTURE

Consider the following figure consist of multi-authority cloud storage for data access control system.

There are five types of entities in following system:

1) CA - Certificate Authority
2) AA - Attribute Authorities
3) Owner - Data Owners
4) Server - Cloud Server
5) Users - Data Consumers

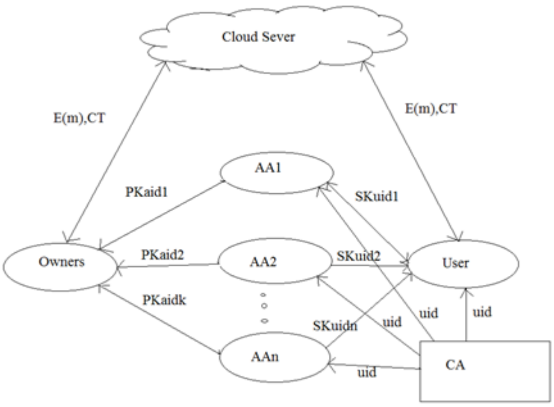

Fig. 1: System model of data access control in multi-authority cloud storage system

A. Ca- Certificate Authority:

It is the global trusted certificate authority in system. It setup the system and the registration of all the users is accepted and AAs in the system. For each licit user in the system, the CA assigns a global unique user identity to it and generates a global public key for this user. CA is not associated in any attribute management and the generation of secret keys that are associated with attributes.

B. Aa- Attribute Authorities:

Each AA in system is an independent attribute authority that is responsible for assigning and revoking user's attributes according to their role. In our plan, every attribute is associated with a single AA, but each AA can control an arbitrary number of attributes. Every AA is answerable for generating a public attribute key for each attribute it manages and each user a secret key reflecting his/her attributes.

Every user has a global identity in the system architecture. A user may be assigned a set of attributes. it come from multiple attribute authorities in the system. The user will receive a secret key associated with its attributes assigned by the corresponding attribute authorities in the system.

C. Owner - Data Owners:

Data owner firstly split data into different component depending on logic granularities and also encrypt each component with different content key using symmetric key encryption key technique. Data owner assign the access policies over attributes from multiple attribute authorities and also encrypts the content key using different attribute policies. Then Data owner send data with cipher texts to the cloud server.

D. Server-Cloud Server:

Cloud server receives all data from data owner and Cloud server will manage data efficiently and prevent the unauthorized access. Cloud server provides different services to user.

E. Users-Data Consumers:

User can access the data from cloud server sending request to the cloud. User will access the data when the data decrypted which is in the form of cipher text. These cipher text is decrypted by user satisfying different access policy defined in the cipher texts. Hence user will decrypt any number of data and content key and obtain the information from original data.

VI. Conclusion and Future Work

We define a scheme for Cipher text - policies attribute based encryption. Our scheme allows for a new type access control encryption where private keys of the user are specified by a set of attributes and each authority can provide access policies to the revocable user. In these techniques, we define a revocable multi-power CP-ABE plan that can bolster effective quality denial. We create a compelling information access control method for multi-power distributed storage frameworks. We likewise demonstrated that our plan was provable secure in the irregular prophet model. The revocable multi-power CP-ABE is a promising procedure, which can be connected in any remote stockpiling frameworks and online informal organizations and so on.

VII. Acknowledgment

We want to thank the distributers and also analysts for making their assets accessible. We additionally thank commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

References

[1] P. Mell and T. Grance, ‘‘the NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.
[2] J. Bettencourt, A. Sahai, and B. Waters, ‘‘Cipher text-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321 - 334.
[3] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ‘‘Bounded Cipher text Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008, pp. 579-591.
[4] M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.
[5] 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.
[6] A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute-Based Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’11, 2011, pp. 568-588.
[7] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261-270.