ISSN (Online): 2456-5717
International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.4 Issue.3 March 2018

Enhanced Fine-Grained Access Control Scheme with Privacy Preserving Data using Hybrid Policy Updating

[1]L.Sesu Ovid, [2]K.Rajasundari
[1]PG Scholar, Dept. of CSE, Francis Xavier Engineering College, Vannarpettai, Tirunelveli.
[2]Asst. Prof., Dept. of CSE, Francis Xavier Engineering College, Vannarpettai, Tirunelveli.

Abstract- **Big Data is a recent emerging platform in Information Technology world. Processing the data in un-trusted environment is a big issue to all the people now a day. Big Data is an easy answer for processing the data in a secured manner. The most important problem in this is security, Hence Here we are trying to introduce a new method for providing secured access control. In order to protect the security and privacy of big data, the cloud storage service needs to enforce effective access control mechanism on user requests. Attribute-Based Encryption is a promising cryptographic access control technique to ensure the end-to-end security of data in cloud. However, the existing ABE researches mainly focus on the efficiency decryption, while the flexibility of policy, the communication cost, and the metadata management of cipher texts are still challenging issues in the big data environment. For the first time, we introduce a new distributed, scalable and fine-grained access control scheme based on classification attributes for the cloud object storage. The classification attributes and threshold policies are incorporated into an access structure, and then the objects are encrypted with the integrated access structure. The constant-size cipher text components associated to attributes can be managed as the corresponding metadata. As a result the encryption complexity and cipher text storage are reduced. In addition, we present a new label-based access control model with multi-authorities to describe the detailed relationships of entities in our scheme. The proposed scheme is proved to be secure under BDHE assumption, and the system implementation provide the practical feasibility and good performance. To provide more security we are utilizing hierarchical structure in the Hierarchical Attribute-Set Based Encryption scheme and Access Control scheme with the use of this we can upload, download, ad delete files from the cloud.**

Keywords- Big Data Hierarchy Encryption - Anonymous Access Control - Cipher Text Policy Attribute Based Encryption.

I. INTRODUCTION

Policy updating issue has not been considered in existing traditional attribute-based access control Schemes. We also update the access policy of the encrypted data in the cloud. Heavy communication overhead of the data retrieval can be eliminated and the computation cost on data owners can also be reduced. Cloud computing provides outwardly unlimited “virtualized” resources to users as services diagonally the whole Internet, while hiding platform and implementation details. Today’s cloud service providers offer both highly available storage and massively parallel computing resource set relatively low costs. As cloud computing becomes common, an increasing amount of data is being stored in the cloud and shared by users with specified privileges, which define the access rights of the stored. Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. When more and more organization and enterprises outsource their data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes. The policy updating is a difficult issue in attribute-based access control systems, because once the data owner outsourced data into the cloud, it would not keep a copy in local systems.

II. RELATED WORK

Hadoop and MapReduce

To support parallel and distributed processing of large volumes of data, most solutions involve Hadoop and the MapReduce algorithm. Hadoop is a framework based on distributed processing of large data volumes across multiple clustered systems. This distribution is based on a file system, Hadoop Distributed File System (HDFS) that provides high performance access to data, is scalable, and offers high availability and tolerance to failures by replication. To ensure parallel processing, most solutions suggest the use of MapReduce, which with the function Map transforms a dataset in hash pairs to distribute the data segments in different nodes of a cluster, and in this way, parallelize processing. After processing, the segments are combined into a single result using the reducer function. The algorithm was initially implemented by Google to solve Page Rank processing, but the most referenced implementation is Apache Hadoop.

III. DEVELOPMENT OF SYSTEM

Attribute Authority

In this module, Attribute Authority analyze each attribute contains single attribute authority and attribute authority can manage arbitrary number of attributes. This work concentrates on multiple attribute authorities. Each attribute authority is responsible for entitling, revoking or re-granting attributes to users according to their roles or identities in its domain. Attribute authority is responsible for generating secret keys, update keys for each user depending upon their global identity issued by data owner.

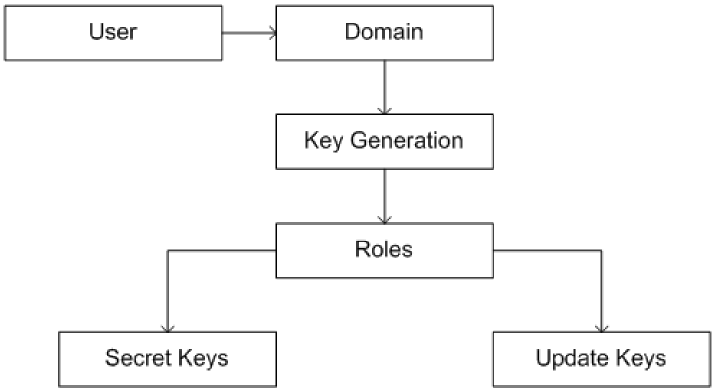

Fig.1. Attribute Authority

Big Data Hierarchy Encryption

In this module, the Big Data Hierarchy Encryption developed in which an identity is considered as a set of descriptive attributes. This scheme is considered as the first Attribute-based Encryption (ABE) scheme, and it is receiving attention from the research community due to its flexibility to enable encrypted communications among groups of entities. Based on ABE, two alternative approaches were proposed. In the Key-Policy Attribute-Based Encryption (KP-ABE) scheme, a message is encrypted under a set or list of attributes, while private keys of entities are associated with combinations or policies of attributes. In contrast, in the Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme, a cipher text is encrypted under a policy of attributes, while keys of participants are associated with sets of attributes. Thus, CP-ABE could be seen as a more intuitive way to apply the concepts of ABE; on the one hand, a data producer can exert greater control over how the information is disseminated to other entities. On the other hand, a user's identity is intuitively reflected by a certain private key.

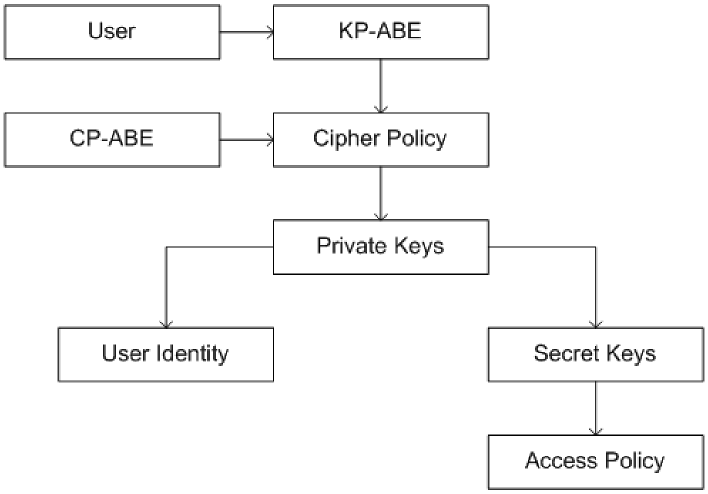

Fig. 2. Big Data Hierarchy Encryption

Anonymous Access Control

In this module, Anonymous Access enables selective disclosure of identity information to provide anonymity. Unlike traditional identity management mechanisms, users are able to obtain credentials to prove that they satisfy certain identity attributes, without disclosing any other additional information. Identity attributes are encoded into cryptographic proofs that can be selectively disclosed in a fine-grained way. The system is intended to provide a common architecture for privacy access systems.

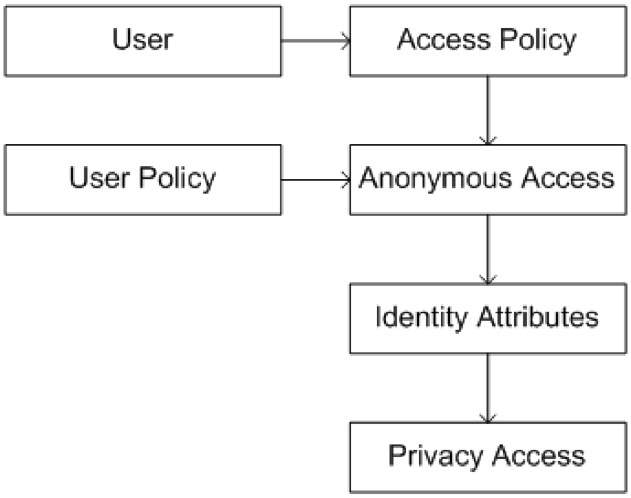

Fig. 3. Anonymous Access Control

Cipher Text Policy Attribute Based Encryption

In this module, CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. CP-ABE moves in the overturn way of KP-ABE. The access structure of this scheme or algorithm, it inherit the same method which was used in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data prefer which key can get well the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the impression of this scheme is similar to the traditional access control schemes. The encryptor who denotes the threshold access structure for his interested attributes while encrypting a message.

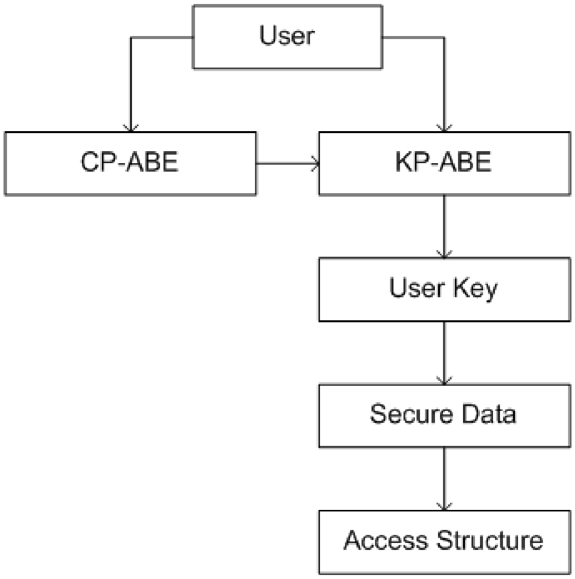

Fig. 4. Cipher Text Policy Attribute Based Encryption

Algorithm

1. Setup: The AA acts a PKG for an IBE scheme, running Setup to generate the private key master −key and the public values params.
2. Attribute List: User 1 obtains list of standard attribute types {ai}. (Note: no certificates.)
3. Policy: User 1 determines his/her access policy f for a resource key κ in terms of the attribute set {ai}.
4. Encrypt: User 1 computes cipher text c = f[κ] using the AND and OR constructions described above.
5. Post: User 1 broadcasts or posts the cipher text c in a public location.
6. Decryption: If he possesses private IBE keys ("implicit" certificates) corresponding to attributes satisfying f, then User 2 can decrypt c, yielding κ.
7. Authorization: Otherwise, User 2 may request from the AA the private IBE keys ("implicit" certificates) for attributes to which User 2 is entitled.

IV. CONCLUSION

The classification attributes and threshold policies are incorporated into an access structure, and then the objects are encrypted with the integrated access structure. The constant-size cipher text components interconnected to attributes can be managed as the matching metadata. In addition, the proposed system present a new label-based access control model with multi-authorities to describe the detailed relationships of entities in our scheme. Besides, the proposed system proved to be secure under Big Data Hierarchy Encryption (BDHE) assumption, and the system implementation demonstrates the practical feasibility and good performance. To provide more security we are utilizing hierarchical structure in the Hierarchical Attribute-Set

Based Encryption scheme and Access Control scheme with the help of this we can upload, download, and delete files from the cloud.

REFERENCES

[1] N.tamil elakkiya, s. Usha, “Data Centric Access Control in the Cloud Environment,” Year: 2017

[2] Junshe Wang, Jinliang Liu, and Hongbin Zhangl, Access Control Based Resource Allocation in Cloud Computing Environment, Year: 2017,

[3] Arulsakthi, k. Sudha, “An Efficient Two - Factor Access Control For Web-Based Cloud Computing Services Using Jar File,” Year: 2017.

[4] Priya Thomas, “Attribute-Based Access Control Scheme For Security Of Cloud Storage Systems Using Rns Cryptography, Year: 2015.

[5] Pooja Choudhary, Jaisankar Natarajan, “Secure Access Control With Dynamic Policy Updating For The Data In Cloud System, Year: 2017.