Confident and Collusion Resistant Robust Public Cloud Storage Access with Attribute Authorities

Shraddha P.Shete
M.E II Year (Computer Engineering)
Amrutvahini College of Engineering, Sangamner,
Dist. Ahmednagar (MS), India

Prof. M. B. Vaidya
Assistant Professor, Computer Engineering
Amrutvahini College of Engineering, Sangamner,
Dist. Ahmednagar (MS), India

Abstract— Data protection and giving aceess control to the data is growing issue now a days .Cipher Text Policy Attribute-Based Encryption has adopted as a favourable technique as it gives pliability, close-grained and safe data access control for cloud storage with fair-but-puzzled cloud servers. In the existing systems that CP-ABE, the attribute authority executes the secret key execution by user lawfulness confirmation and it takes time. In ciphertext-policy attribute based encryption a end user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system which is promising technique and secured over traditional techniques . The proposed system guarantees security requirements and makes performance improvement in key generation.

Keywords— Cipher Text Policy Attribute-Based Encryption (CP-ABE), Honest-but-curious cloud servers, Security

I. INTRODUCTION

Cloud computing gives us best performance for academic, banking and industry to fulfill the requirement of data storage and faster ,speedy performance. Cloud computing gives an important service of cloud storage for data holder. Using cloud storage gives essential benefits same as good accuracy, better understandability, faster organization and also powerful security and so on. The given prototype also brings new provocation over data access control and ensuring data security might be big issue. The cloud storage is carried with cloud service suppliers. They are usually out of the promised domain of data holders and traditional access control architectures in the Client/Server model are not flexible in cloud storage environment. There have been quite a few schemes proposed to address the issue of data access control in cloud storage and Cipher text Policy Attribute- Based Encryption (CP-ABE) is regarded as one of the most secured techniques. CP-ABE allows data owners direct control power based on access schemes, to provide pliable, close grained and safe access control for cloud storage prototypes. The access control is achieved by using secret writing, where the holder's data is encrypted with an access structure over attributes, and a data end user's secret key (private key) is given a label with his/her self attributes. If the attributes associated with the end user's secret key satisfy the access structure, the end user can decode the corresponding ciphertext to obtain the plaintext. The CP-ABE based access control prototypes for cloud storage have been developed into combining categories,that are, one-authority framework and multiple authority framework. CP-ABE architectures delets the traffic jams in performance to allow multiple authorities to completely handle the universal attribute set by the method that each of them is able to distribute secret keys to the end users individually. A strong and efficient diverse architecture is designed with the help of one CA(Central Authority) and multiple AAs (Attribute Authorities) for public cloud storage architectures. Central Authority is one and only one responsible for performance tasks which gives secret keys for lawfulness confirmed end users. To extend safety of data, we propose an auditing principle to verify which one AA (Attribute Authority)is faulty or maliciously performed the lawfulness confirmation procedure.

II. LITERATURE SURVEY

A. "Efficient Decentralized Attribute-based Access Control for Cloud Storage with User Revocation" IEEE ,2014, Author Jianwei Chen and Huadong Ma described that they have presented a novel disintegrated CP-ABE access control scheme for cloud storage prototype, which is well organized and safe. Their framework doesn't need any central authority and coordination between multiple authorities, thus removing the burden of weighty communication and the late in cooperating computation. In addition, we improve the framework by putting forward an on-demand end user re-verification framework. As single authority cannot handle all things in proper time."Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement" IEEE, 2015, Author Zhangjie Fu, Jiangang Shu, Fengxiao Huang in this paper, they solves the problem of personalized multi-keyword ranked search over encoded cloud data.Takes into consideration the end user search past history, they design a end user interest framework for independent end user with the help of semantic ontology Word Net. Through the model, they

have understood automatic evaluation of the keyword priority and cleared the limitation of the artificial method of measuring.

B. "Towards Efficient Content-aware Search over Encrypted Outsourced Data in Cloud" IEEE, 2016 by Zhangjie Fu, Xingming Sun, Sai Ji in this paper, they designed an effective methods to solve the problem of semantic search based on concept hierarchy. They make contributions in both on search accuracy and search effectivesness. For the feature of search accuracy, an broad concept hierarchy is build to expand search terms in search stage. For the feature of search efficiency, a tree-based index structure is build to plan all the documents index vectors.

C. TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud" IEEE, 2015 by Jianan Hong, KaipingXue This paper focuses at close-grained access control for time tactful data in cloud storage framework. There is one issue which is to concurrently gain efficient timeouts and fine coarseness with low overhead, which isn't given in related work. In this paper, they proposed a framework to gain this goal. Our scheme seamlessly incorporates the concept of timed-release encoding to the framework of cipher text-policy attribute-based encoding. With a suit of proposed methods, not require any central authority and coordination among multiple authorities, thus removing the burden of heavy communication and the delay of collaborative computation. In addition, we enhance the scheme by putting forward an on-demand user revocation scheme. As single authority fails to handle all things in proper time.

III. PROPOSED METHODOLOGY

In this system, we propose a novel diversed methods to eliminate the problem of traffic jam in performance and gives a more safe and promising access control method with an auditing method. Our architecture employs multiple attribute authorities to share the load of end user lawfulness confirmation. Meanwhile, in our scheme, a central authority is introduced to give secret keys for lawfulness verified end users.

A. Architecture

Our scheme has five different phases, which are *System Initialization*, *Encoding*, *Key Generation*, *Decoding*, and *Auditing & Tracing*. The server is maintained online and managed by the cloud service provider.

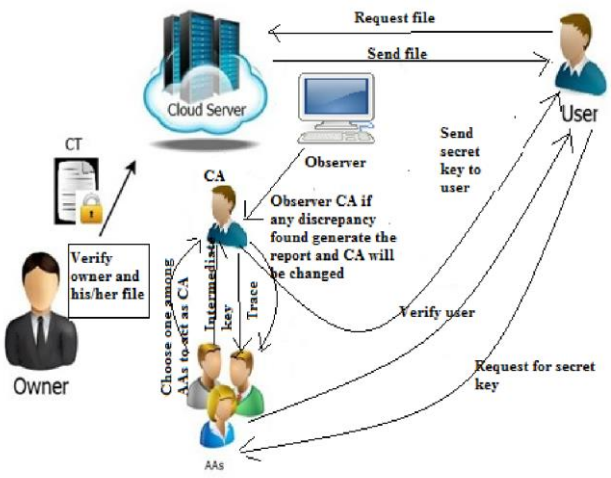

Figure 1: Basic Concept of CP-ABE System

B. Algorithm:

Cipher-text-Policy Attribute-Based Encryption (CP-ABE) scheme consists of four algorithms.

- **Initialize (λ, U) (PK, MSK)** - The setup algorithm takes the security parameter and the attribute universe description U as the input. It gives the public parameters PK and a master secret key MSK as output.
- **Encode (PK, M, A)** - CT. The encryption algorithm takes the public parameters PK as input, a message M, and an access structure A as input. The algorithm will encode Message and gives a cipher-text such that one and only one end user whose attributes satisfies the access framework will be able to decode the message M. We will assume that the cipher-text implicitly contains A.

- **Key creation (MSK, S) -** SK. The key creation algorithm takes input as the master secret key MSK and a set of attributes S . It gives a secret key SK as output.
- **Decode (PK, CT, SK) -** M. The decoding algorithm takes the public parameters PK, a cipher text CT which has an access policy A, and a secret key SK as input, where SK is a secret key for a set S of attributes. If the set S of attributes satisfies the access framework A, the algorithm will decode the cipher-text and give a message M.

IV. RESULT AND DISCUSSIONS

All types of testing goes with a planned method, which is pre-defined to. All tests takes into consideration not only a normal system condition but also address abnormal and recovery feature of the architecture. The system is tested in a forced surroundings, nominally in excess of 150 percent of its rated capacities. Test featured like test cases, data, tools, configuration, and methods are documented in a software information document. Every test shall be defined in trackable methods and have cleared-non cleared criteria added Test cases which are planned in confirmance to the test process and listed with detailed test descriptions. These test cases use cases based on projected operational mission scenarios. The testing process also includes stress / load testing for stability purpose (i.e., at 95 percentage CPU use, system stability is still guaranteed). The test process thoroughly tests the frameworks and methods. Software testing has a trackable open box testing, closed box testing and other test processes checking implemented software against design documentation lists and requirements defined. Open Box Testing is tests that run an application with information of the internal work of the code base. Open box testing is used in three of the six basic types of testing: unit, integration, and regression testing. Unit testing is implemented on a small piece, or single unit of the code. When a unit is added into the main code base, it is more difficult to search a bug in that single unit. Integration testing specifies at how all parts of an application interact with. Open box integration tests focuses on the interfaces between the parts. Regression testing varies that changes done to the system have not damaged the whole system. Unit tests and integration tests can be again run in regression testing to check the ways that the application work properly and curely. A closed box test of integration created has active, interface, error recuperation, force and out-of-bounds input testing. All closed box software tests are tracked to control thw requirements of user. In addition to static requirements, a closed box of completely integrated framework against outline sequences which are ordered of events is created to model operations. Performance testing for systems is gathered as an integral part of the close box test processes.

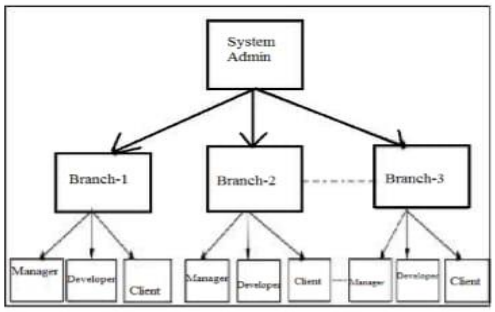

Fig. 2. Work Break-Down Structure

V. CONCLUSIONS

It has been proposed a new diversed module to remove the traffic jam in performance and increase the effectiveness of the existing CP-ABE systems. With the effeciently recontructing CP-ABE cryptographic technique into this novel module, the proposed scheme gives a close-grained, strong and effective access control with one-CA/multi-AAs for public cloud storage. This scheme employs multiple AAs to share the load of the time-taking lawfulness confirmation and standby for serving new arrivals of end user's requests. It has been proposed an auditing method to track an attribute authority's potential wrong behaviour. It has been conducted detailed security and performance analysis to verify that this scheme is secure and efficient. The security analysis shows that the scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers.

VI. REFERENCES

[1] Zhangjie Fu, Kui Ren, Enabling personalized search over encrypted outsourced data with efficiency improvement 2015 IEEE.
[2] Zhangjie Fu, Xingming Sun and Sai Ji, Towards efficient content-aware search over encrypted outsourced data in cloud IEEE INFOCOM 2016
[3] Jianan Hong, KaipingXue TAFC: Time and attribute factors combined access control on time sensitive data in public cloud 2015 IEEE
[4] Yingjie Xue, JiananHong,Wei Li and KaipingXue, LABAC: A location-aware attribute-based access control scheme for cloud storage 2016 IEEE
[5] Wei Li, KaipingXue, Yingjie Xue, and Jianan Hong TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage 2015 IEEE.
[6] KaipingXue, A dynamic secure group sharing framework in public cloud computing 2013 IEEE.
[7] Jianwei Chen and Huadong Ma Efficient decentralized attribute-based access control for cloud storage with user revocation 2014 IEEE
[8] Attribute-based access to scalable media in cloud-assisted content sharing Junbeom Hur Improving security and efficiency in attribute-based data sharing 2013 IEEE.

-