The Secure and Expressive Data Access Control for Cloud Storage

[1]Konda Sindhuja, [2]S Surya Godha Devi
[1,2]Dept. of CSE, KIET, Kakinada, AP, India

Abstract
Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic "all-or-nothing" decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

Keywords
Data access control, auditing, CP-ABE, Cloud storage.

I. Introduction

Cloud processing is the critical parts of PC world. It empowers adaptable, on-request, and ease of figuring assets. In any case, the data is outsourced to some cloud servers, and different protection concerns rise up out of it. The one of the basic services of cloud processing is the putting away limit of cloud which empowers clients (data proprietor) to have their data in cloud by methods for cloud server. It gives the data access to data shoppers. It can likewise give on request assets to storage which can help specialist organizations to lessen their support costs [1]. Ordinarily clients store his/her data in confided in servers. These data are controlled by a trustable chairman [2]. The cloud storage can gives the authorization to clients to get to their data from anyplace on any gadget in proficient way. The client's secret key is put away in their PC [10]. In cloud registering there are a few outlines is proposed to secure the cloud storage. The attribute based encryption approach is the one among sorts of encryption framework [6]. In this sort of framework, every client has the client secret key is issued by the authority. This encryption strategy is the effective adaptable approach which executes attribute-based access control (ABAC) by utilizing data or subjects' attributes as data get to strategies and also public keys [10]. Attribute-Based Encryption (ABE) is a promising methodology for cloud storage that offers fine-grained get to control approach over encoded data [2]. Attribute-based Encryption (ABE) is viewed as a standout amongst the most reasonable plans to lead data get to control in public clouds for it can ensure data proprietors' immediate control over their data and give a fine-grained get to control benefit. It manages confirmed access on scrambled data in cloud storage benefit [8].There are numerous ABE plans proposed, which can be partitioned into two classes: Key Policy Attribute based Encryption (KP-ABE), Cipher content Policy Attribute-based Encryption (CPABE) [2]. In the KP-ABE, a figure content is related with an arrangement of attributes, and a private key is related with a monotonic access structure [3] [1]. Contrasted and KP-ABE, CP-ABE is a favored decision for planning access control for public cloud storage. The CPABE is utilized for data proprietors and based on get to arrangements, to give adaptable, fine-grained and secure access control for cloud storage frameworks [3]. In CP-ABE plot, there is an authority that is in charge of attribute administration and key appropriation. There are two sorts of CP-ABE frameworks: single-authority CP-ABE where all attributes are overseen by a solitary authority, and multi-authority CP-ABE [4]. CP-ABE is utilized to data get to control for cloud storage, some multi-authority CP-ABE plans, has proposed. Exceptionally, in DAC-MACS [1], other than proposing a multi authority CP-ABE plot for cloud storage, the creators asserted that the attribute renouncement component [5]. The client's entrance authorization relies upon the attributes the client holds in the CP-ABE based access control framework, and each attribute might be controlled by numerous data clients [7]. CP-ABE plot was proposed to totally conceal the entrance strategy. In any case, the plan just bolstered the straightforward 'AND' door get to structure [9].In request to enhance the framework security, ensure client protection and spare the storage overhead of figure content, for cloud storage [8].

II. Related Work

Nyamsuren Vaanchig et al (2018)this paper displays a Key-EscrowFree Multi-Authority Ciphertext-Policy Attribute-Based Encryption Scheme with Dual-Revocation by presenting "the fundamental attribute" and making utilization of a declaration authority separated from attribute experts. Contrasted and the current MA-CP-ABE plans, the proposed plot is the most reasonable one to empower data get to control for cooperative cloud storage frameworks. Moreover, the security and execution examination shows that our plan is more secure and sensibly effective to be connected to commonsense situations as synergistic cloud storage frameworks. Mahesh Muthulakshmi, R et al (2018)Data access control is the testing issues in public cloud storage frameworks. In our paper the data security is enhanced utilizing various specialists. Figure content Policy Attribute-Based Encryption (CP-ABE) has been embraced as a promising techinque to give ceaseless, adaptable, fine-grained and secure data get to control for cloud storage with fair yet inquisitive cloud servers. Mehdi Sookhaka et al (2017) This paper gives an exhaustive review on attributebased get to control plans and looks at each plan's usefulness and trademark. We additionally show a topical scientific classification of attribute-based methodologies based on huge parameters, for example, get to control mode, engineering, denial mode, disavowal strategy, renouncement issue, and repudiation controller. The paper audits the cutting edge ABE strategies and arranges them into three fundamental classes, for example, incorporated, decentralized, and hierarchal, based on their designs. Krishnaselvi. L et al (2015) Cloud processing is the conveyance of figuring services over the Internet. Cloud services enable people and organizations to utilize programming and equipment that are overseen by outsiders at remote areas. We propose a subject that hosts different key

and third get-together reviewer for security. In addition, our confirmation and access control conspire is decentralized and powerful, dissimilar to different access control plans intended for clouds which are concentrated. Here just legitimate clients can decode the put away data. Ciphertext-Policy Attribute-Based Encryption (CPABE) Even however the definitions and developments of various CPABE plans are not generally precise, the employments of the entrance structure in Encrypt and Decrypt calculations are almost the same. Here we receive the definition and development from [6, 10]. A CP-ABE conspire comprises of four calculations: Setup, Encrypt, Key Generation (KeyGen), and Decrypt. Setup(λ,U) → (PK,MSK). The setup calculation takes the security parameter λ and the attribute universe portrayal Uas the data. It yields the public parameters PK and an ace secret key MSK. Encrypt(PK,M,A) → CT. The encryption calculation takes the public parameters PK, a message M, and an entrance structure An as data. The calculation will scramble M and deliver a ciphertext CT with the end goal that exclusive a client whose attributes fulfills the entrance structure will be capable todecrypt the message. We will expect that the ciphertext verifiably contains A. KeyGen(MSK, S) → SK. The key age calculation takes the ace secret key MSK and an arrangement of attributes S as data. It yields a secret key SK. Decrypt(PK,CT, SK)→M. The unscrambling calculation takes the public parameters PK, a ciphertext CT which contains an entrance approach An, and a secret key SK as info, where SK isa secret key for a set S of attributes. In the event that the set S of attributes fulfills the entrance structure A, the calculation will unscramble the ciphertext and restore a message M. Powerful And Auditable Access Control (RAAC): In this paper, propelled by the heterogeneous engineering with single CA and numerous RAs, we propose a hearty and auditable access control plot (named RAAC) for public cloud storage to advance the execution while keeping the adaptability and fine granularity highlights of the current CPABE plans. In our plan, we isolate the strategy of client authenticity check from the secret key age, and allocate these two subprocedures to two various types of experts.

III. System Model and Security

A. Assumptions

We give the definitions of the system model, the security assumptions and requirements of our public cloud storage access control.

1. System Model

The system model of our design is shown in Fig. 1, which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers(here, we mention it as cloud server.).

- The central authority (CA) is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the system initialization phase, it assigns each user a unique Uid and each attribute authority a unique Aid. For a key request from a user, CA is responsible for generating secret keys for the user on the basis of the received intermediate key associated with the user's legitimate attributes verified by an AA. As an administrator of the entire system, CA has the capacity to trace which AA has incorrectly or maliciously verified a user and has granted illegitimate attribute sets.
- The attribute authorities (AAs) are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users. Unlike most of the existing multi-authority schemes where each AA manages a disjoint attribute set respectively, our proposed scheme involves multiple authorities to share the responsibility of user legitimacy verification and each AA can perform this process for any user independently. When an AA is selected, it will verify the users' legitimate attributes by manual labor or authentication protocols, and generate an intermediate key associated with the attributes that it has legitimacyverified. Intermediate key is a new concept to assist CA to generate keys.
- The data owner (Owner) defines the access policy about who can get access to each file, and encrypts the file under the defined policy. First of all, each owner encrypts his/her data with a symmetric encryption algorithm. Then, the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to public keys obtained from CA. After that, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext CT) to the cloud server to be stored in the cloud.
- The data consumer (User) is assigned a global user identity Uid by CA. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The user can freely get any interested encrypted data from the cloud server. However, the user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy embedded in the encrypted data.
- The cloud server provides a public platform for owners to store and share their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

B. Security Assumptions and Requirements

In our proposed scheme, the security assumptions of the five roles are given as follows. The cloud server is always online and managed by the cloud provider. Usually, the cloud server and its provider are assumed to be "honest-butcurious", which means that they will correctly execute the tasks assigned to them for profits, but they would try to find out as much secret information as possible based on data owners' inputs and uploaded files. CA is the administrator of the entire system, which is always online and can be assumed to be fully trusted. It will not collude with any entity to acquire data contents. AAs are responsible for conducting legitimacy verification of users and judging whether the users have the claimed attributes. We assume that AA can be compromised and cannot be fully trusted. Furthermore, since the user legitimacy verification is conducted by manual labor, mis-operation caused by carelessness may also happen. Thus, we need an auditing mechanism to trace an AA's misbehavior. Although a user can freely get any encrypted data from the cloud server, Pages:he/she cannot decrypt it unless the user has attributes satisfying the access policy embedded inside the data. Therefore, some users may be dishonest and curious, and may collude with each other to gain unauthorized access or try to collude with (or even compromise) any AA to obtain the access permission beyond their privileges. Owners have access control over their uploaded data, which are protected by specific access policies they defined.

To guarantee secure access control in public cloud storage, we claim that an access control scheme needs to meet the following four basic security requirements:

- Data confidentiality. Data content must be kept confidential to unauthorized users as well as the curious cloud server.
- Collusion-resistance. Malicious users colluding with each other would not be able to combine their attributes to decrypt a ciphertext which each of them cannot decrypt alone.
- AA accountability. An auditing mechanism must be devised to ensure that an AA's misbehavior can be detected to prevent AAs' abusing their power without being detected.
- No ultra vires for any AA. An AA should not have unauthorized power to directly generate secret keys for users. This security requirement is newly introduced based on our proposed hierarchical framework.

IV. Data Access Control Models and Techniques

Data Access Control is one of the most important technologies to ensure adequate security of cloud computing. There was some traditional access control model which originated in the year of 1970s with the aim to prevent malicious users from accessing resources and avert them to use the potential resources illegally. Access control mechanisms are a necessary and crucial design element to an application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help to limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Before selecting the data access control mechanisms, there are several fundamental steps that lend a hand speed up and elucidate the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Designing complicated and inconvenient data access controls around uncategorized or non-sensitive data can be counterproductive to the eventual goal or principle of the web application.
2. Determine the relative interaction that data owners and creators have within the web application. Some applications may restrict any and all creations or ownership of data to anyone but not the administrative or built-in system users.
3. Specify the process for granting and revoking user access control rights on the system, whether it is a manual process, automatic upon registration or account creation, or through an administrative front-end tool.
4. Clearly, delineate the types of role driven functions of application support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).
5. Try to align access control mechanisms as close as possible to the organization's security policy. Much of information from the policy can map very well over the carrying out of access control (acceptable time period of certain data access, types of users allowed in seeing certain data or performing certain tasks, etc.). These types of mappings usually work in the most excellent way with Role Based Access Control.

There are a plethora of accepted data access control models in the information security territory. Cloud computing is dynamic in nature and it supports the following traditional Access Control Models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC). Data Access Control actually refers to the control over access to the various system resources after a user's account testimonials and distinctiveness have been legitimated and access to the system approved. For example, a specific user, or group of users, might only be given access to certain files after logging into a system, while simultaneously being deprived of access to all other resources.

A. Discretionary Access Control

Discretionary Access Control (DAC) is used to limit access to information based on the distinctiveness of consumers and/or membership in certain clusters. Access decisions are typically based on the authorizations granted to a user based on the credentials that the owner presented at the time of authentication (username, password, hardware/software token, etc.). Typically in DAC models, the owner of information or any resource is able to change its permissions. The downside of this method is overseer not been able to administer these authorizations on files/ information loaded on the web server.

B. Mandatory Access Control

Mandatory Access Control (MAC) is the strictest among all levels of control and is primarily used by the government. MAC takes a hierarchical approach in controlling access to the resources. In this environment, the system administrator has sole responsibility for defining access control to all resource objects such as data files. In this model, security labels are assigned to all resource objects. These security labels contain two kinds of information - a classification (top secret, confidential etc.) and a category (management level, department or project to which the object is available).

When a user requests to access a resource, the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's testament matches the MAC security tag properties, the access is permitted. It is important to note, does both the classification and categories match. A user with top-secret classification, for example, cannot access a resource if they are not only a member in one of the required categories of that object. MAC requires a careful planning to implement. Once it is put into operation, it enforces a high system administration overhead due to necessitate evenly updating of object and accounting labels to have a room for new data, new users and modifications in the categorization and classification of existing users.

C. Role Based Access Control

Another name of this is called as Non-discretionary Access Control and uses real-world approach in structuring access control. Access under RBAC is based on user's profession function within the organization to which the computer system fits in.

Essentially, RBAC assigns special permissions to particular cadres in an organization. For instance, an accountant in a business will be allocated to the Accountant role, achieving access to all the resources legalized for all accountants on the system. Similarly,

the developer role can be assigned to software engineer. A user under RBAC may only be assigned a single role in an organization. The accountant illustrated above obtains the same authorizations as all other accountants, nothing more and nothing less.

D. Rule-Based Access Control:

Rules-Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. In this model, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a meticulous account or group endeavors to access a resource, the operating system verifies the rules contained in the ACL for that resource.

Rules-Based Access Control includes conditions such as allowing access to an account or a group to a network connection in certain hours of the day or days of the week. As all access permissions are controlled solely by the system administrator, the user cannot change anything.

VI. Security Issues Associated With the Cloud

Cloud computing is a prominent and fast growing technology has captured several professional attentions that allow many to store their data securely and the same can be accessed efficiently. Cloud service provider provides a variety of different service models such as Software-as-aService, Platform-as-a-Service, Infrastructure-as-a-Service and deployment models as Private, Public, Hybrid, and Community. Nowadays many professionals have started to use cloud environment as it provides the user a storage capability to store and process their data. However, the challenges like data security and access control system are the main concern of Cloud Service provider.

The cloud, of course, can be a valuable tool in helping IT achieve this objective, but it is important to understand how, where and when cloud services should be used and when they shouldn't. Cloud works best and most cost-effectively when it is part of an overall data management strategy. Because data lifecycles evolve as an organization's data mix changes, you don't want to be locked into using the cloud. Rather, you want to be able to leverage cloud services when appropriate.

The issues related to data access control in Cloud computing environment can be solved with properly implemented data access control techniques with state-ofthe-art security solution and today's implementers can avoid such a issues made by the predecessors.

VII. Proposed System

Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Cipher text-Policy Attribute-Based Encryption (CPABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding cipher text to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario, and multi authority scenario. Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set.

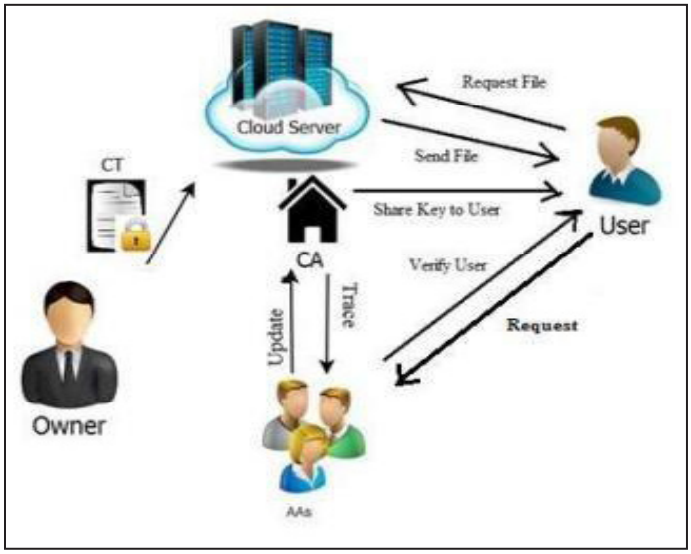

Fig. 1: Proposed Architecture diagram

VIII. Conclusion

In this paper, we proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users' requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and colluded malicious users, as well as the honest-butcurious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution. Further performance analysis based on queuing theory showed the superiority of our scheme over the traditional CPABE based access control schemes for public cloud storage.

References

[1] Kaiping Xue "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", IEEE2016.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.
[5] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.
[6] J. Hur, "Improving security and efficiency in attributebased data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271– 2282, 2013.
[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.
[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.
[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.
[10] A. Lewko and B. Waters, "Decentralizing attribute based encryption," in Advances in Cryptology– EUROCRYPT 2011. Springer, 2011, pp. 568–588.