Review for Secure Data Communication and Protection

Divya A. Wani[1], Shital A. Patil[2]

[1]*Department of Computer Engineering, SSBT's COET, Bambhori*
[2]*Department of Computer Engineering, SSBT's COET, Bambhori*
[1]*divyawani07@rediffmail.coml,* [2]*shital.a.patil2014@gmail.com*

Abstract

Today we have abundant sources available online. Due to growth in of multimedia applications, protection of application becomes very important issue in communication and also storage purposes. To enhance protection for communication and protection there are various techniques. In this paper concept of cloud computing, technique which is been implemented is CP-ABE [Cipher Policy-Attribute Based Encryption] is introduced. In CP-ABE attributes are attached to user's secret key and access policy is been attached to cipher text. In role based access control, access permissions are assigned through roles. It needs to be implemented through access monitors which will run on data servers.

Keywords: cloud computing, CP-ABE, RBAC, data protection.

1. Introduction

In cloud computing, an expanding number of enterprises and associations use cloud servers as their framework stage. Today, role based access control (RBAC) show is the most well-known model utilized in big business frameworks. The model has extreme security issues when connected to cloud frameworks. A great RBAC demonstrate utilizes reference screens running on information servers to execute approval. The servers in the cloud are out of the control of big business areas and must be considered untrusted naturally. Subsequently, building a data protection mechanism for cloud-based enterprise frameworks has become a challenge. In RBAC, access permissions are assigned through roles and can't be straightforwardly relegated to a through roles and can't be specifically appointed to a client, which is inadequately fine-grained.

The term cloud computing is the processing administrations in Information Technology like platforms, infrastructures, or applications could be organized and utilized through the web. Infrastructure whereupon cloud is based upon is an expansive scaled distributed framework in which shared pool of resources are for the most part virtualized, and administrations which are offered are distributed to customers as far as virtual machines, sending condition, or programming. Consequently, it tends to be effortlessly reasoned that as per the necessities and current remaining tasks at hand, the administrations of cloud could be scaled powerfully. [1] The same number of assets are utilized, they are estimated and after that the installment is made based on utilization of those assets. As per the meaning of, cloud computing is it is a critical isolated figuring model that is coordinated by financial reasonability of equality, in which stake of restrict, principal, stacking, platform in which an offices are provided according to the demand of outside remote customers through the web. There are a few instances of cloud administrations like web mail, online record and business applications.

Cloud computing gives a common pool of resources, including information storage room, systems, PC preparing power, and concentrated corporate and client applications. cloud storage indicates the capacity on cloud with relatively economical capacity and support alternative for small enterprise. The actual storage location might be on single storage condition or replicated to different server storage dependent on significance of information. The component model of cloud storage comprises of four layers: storage layer which stores the information, fundamental administration layer which guarantees security and strength of cloud storage itself, application interface layer

which gives application benefit stage, and access layer which provides platform. The fundamental cloud storage condition is spoken to above in figure 1.

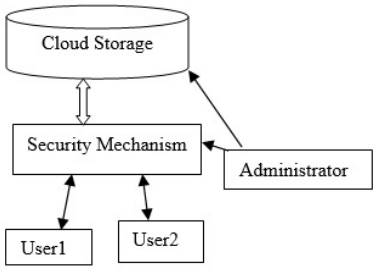

Figure 1. Cloud Structure Environment

Cloud computing is the utilization of equipment and programming to convey an administration over a system. Clients can get to documents and use applications from any gadget that can get to the Web. cloud computing is a developing worldview which has turned into the present most smoking exploration territory because of its capacity to decrease the expenses related with registering. In the present time, it is most intriguing and luring innovation which is putting forth the administrations to its clients on interest over the web. Since cloud computing stores the information and its spread assets in nature, security has turned into the fundamental snag which is hampering the organization of cloud conditions. There are number of clients utilized cloud to store their own information, with the goal that information stockpiling security is required on the capacity media. The significant worry of cloud condition is security amid transfer the information on cloud server. Information storage at cloud server pulled in mind boggling measure of thought or spotlight from various networks. For redistributing the information there is a need of outsider.

2.Related Work

Attribute based encryption (ABE) offers help for independent information insurance. In ABE, both a client's private key and the figure content are related with a few characteristics. At the point when the characteristics utilized in the figure content and the properties in a client's private key match, the client can unscramble effectively. Thusly, ABE accomplishes both encryption and access control all the while. There are various types of ABE in that only two variations are described, in particular, key-strategy ABE (KP-ABE) and figure content arrangement ABE (CP-ABE) [1]. In KP-ABE, the figure content is related with a lot of characteristics and the private key is related with an entrance strategy. In CP-ABE, the idea is switched: the figure content is related with an entrance arrangement and the private key is related with a lot of traits. Between these two variations of ABE, CP-ABE is increasingly appropriate for an endeavor domain, and it is a perfect essential plan for executing an independent information security component.

Despite the fact that ABE is fit for authorizing access control, it is contradictory with the generally utilized RBAC display since it can't bolster job legacy. Zhu et al. [1], tended to this issue by giving an ABE conspire property chain of importance in which every job was mapped to at least one characteristics relying upon a movement intermediary. By and by, to give adaptable access control, properties containing complex administrators, for example, the NOT administrator are likewise helpful. In any case, this strategy has no arrangement. To improve the approach articulation capacity of ABE, specialists have displayed different plans to help either NOT or examination administrators. Among them, just the All-inclusive CPABE (ECP-ABE) plot can deal

with a wide range of administrators all the while and can be effectively stretched out to help different administrators.

The RBAC show was first proposed by Ferraiolo and Kuhn in 1992 and was broadly contemplated in the mid-1990s. The RBAC display presented jobs among clients and authorizations. Consents are allotted to jobs as opposed to clients; clients must be allocated to a job to pick up the authorizations relegated to that job. The RBAC demonstrate significantly improved authorization the executives; thus, it has turned into the most generally utilized access control show in the previous couple of years. By creating distinctive strategies, RBAC can accomplish the prerequisites of both optional access controls (DAC) and obligatory access controls (Macintosh) [11]. A few investigations have concentrated on consolidating RBAC with different encryption plans to ensure information. Crampton presented another portrayal of RBAC arrangements, in particular, utilizing the halfway request connection to depict the approaches. This methodology changes RBAC approaches into data ow strategies; at that point, it utilizes cryptographic authorizations of the arrangements to build a cryptographic RBAC instrument. Zhu et al. proposed a job key chain of command show (RKH) comprising of a cryptographic RBAC display that can bolster job progressive systems [3]. In RKH, every job compares to an exceptional job key, and clients are doled out a selective client key related with every job to which they have a place. Since clients must keep up a private key relating to every job, this strategy builds the weight of key administration for client's particularly when a client is appointed numerous jobs. RBAC can likewise be joined with ABE to secure information in distributed computing. Zhu et al. proposed a RBAC perfect ABE to move the RBAC framework into ABE based information assurance. In this plan, every job is mapped to at least one characteristics relying upon a movement intermediary. At that point an ABE conspire with quality chain of command was exhibited to scramble information with the mapped properties. Zhou et al. proposed a job based encryption (RBE) plot that joined RBAC with CP-ABE for secure distributed storage. In RBE, information is encoded with the jobs open parameters, and clients who are appointed to the job can unscramble the figure content. RBE can't bolster job legacy. In the cryptographic job based access control demonstrate actualized by means of CP-ABE, every job is related with an entrance tree. Clients whose traits fulfill the jobs strategy tree can get consent for decoding. This plan can manage dynamic strategies that incorporate consent and job task changes and document refreshes. It requires the information proprietor to play out every one of the activities, which is both irrational and doubtful in a distributed computing situation.

2.1 Background of Attribute Based Encryption

ABE is an augmentation of open key encryption that enables clients to encode and unscramble information dependent on characteristics.The greatest advantage of ABE is that its encryption key and decryption key are not in a one-to-one relationship; an encryption key can correspond to multiple decryption keys. The underlying basis of ABE is a fuzzy identity-based encryption (FIBE) proposed by Sahai and Waters. Goyal et al. further developed FIBE and introduced the idea of KP-ABE, in which the figure content is related with a lot of properties and the private key is related with an access tree. Later, Bethencourt et al. proposed the first CP-ABE scheme called the BSW scheme.[8] CP-ABE reversed the idea in KP-ABE; in CP-ABE, the cipher text is associated with an access tree while the private key is associated with a set of attributes. The original ABE schemes were proposed based on a tree structure that is relatively expressive and can support AND, OR and threshold operators (an (m; n) threshold means a solution must satisfy at least m constraints among total n constraints; to refer to an (m; n)-threshold as \threshold" for short). Subsequently, some approaches, based on the Linear Secret Share Scheme (LSSS) were proposed. The expressive ability of LSSS nearly equals that of a tree structure except that each attribute can be used only once in a LSSS structure. There are also some schemes that support only the threshold operator were proposed. In fact, the

AND operator is an (n; n)-threshold; therefore, those schemes also can support AND operator. In addition to AND, OR and threshold operators, there are some more complex operators such as NOT and comparison operators that are particularly useful in practice, but cannot be directly expressed.

To address this problem, some studies focused on improving the expressive ability of CP-ABE. Cheung and Newport presented the first CP-ABE scheme supports policies containing the NOT operator, henceforth referred to as CN. Its expression ability is still not sufficient because CN supports only the AND, NOT operators. Based on CN, some CP-ABE schemes have been proposed to achieve various goals such as hidden access policy, constant cipher text length, constant private key length and so on. Similar to CN, these approaches support only AND, NOT operators. Junod and Karlov proposed an attribute-based broadcast encryption (ABBE) scheme based on CP-ABE that can support AND, OR and NOT operators. Ostrovsky et al. presented a KP-ABE scheme that can represent non-monotonic access policies and supports NOT as well as AND, OR and threshold operators. Other schemes have been proposed to support the NOT operator using the same technique. Policies containing comparison operators are also frequently used in practical applications. Although the schemes discussed so far can support the NOT operator, none of them can handle the comparison operators. BSW uses a bag of bits to express policies containing comparison operators. In this approach numerical values must be represented in binary form, which is complex and difficult to use in practice. Zhu et al. presented a comparison-based encryption (CBE) scheme to express various comparison-based policies; It does not support the NOT operator [5]. Lang et al. proposed an Extended CP-ABE (ECP-ABE) scheme which is very expressive. By introducing extended leaf nodes, the access tree was enhanced to support all types of logical and arithmetic comparison operators, including AND, OR, threshold, less than, greater than, less than equal to, greater than equal to and NOT, among others. ECP-ABE is the first scheme that can support policies containing all the operators simultaneously. Waters presented a functional encryption mechanism whereby an access policy can be expressed using regular language.

Table 1. Comparative Review of Various Techniques

Year	Author	Concept Introduced	Description
1992	Ferraiolo, et al.	Role Based Access Control.	Introduced roles between users and permissions.
2010	Junod,et al.	An efficient public key attribute based broad-cast encryption	Provides seperate public key .
2011	Crampton, et al.	Cryptographic enforcement of role-based access control.	Introduced a new character-inaction of RBAC policies.
2013	Zhu,et.al.	A new cryptographic RBAC system based on role key hierarchy.	Each role corresponds to a unique role-key, and users are assigned an exclusive user-key.
2013	Hohenberger,et.al.	Attribute based encryption with fast decryption	Linear secret share scheme were proposed.
2015	Zhu,et al.	From RBAC to ABAC	Each role is mapped to one or more attributes

			depending on a migration proxy.

3.Proposed Solution

In CP-ABE, the cipher content is related with an entrance approach, and the private key is connected with a lot of characteristics. On the off chance that and just if the characteristics in a client's private key fulfill the entrance strategy is the client ready to unscramble the figure message effectively. The CP-ABE scheme consists of 4 algorithms: Setup, Keygen, Encrypt and Decrypt. The model of the CP-ABE scheme is illustrated in Figure 2. There are three parties in the model: the private key generator (PKG), the encryption party and the decryption party. PKG is a trusted party. It is responsible for initializing the system and generating the master key mk and the public parameters pk with the Setup algorithm, authenticating users attributes and generating private keys for users with the Keygen algorithm. The public parameters pk are sent to the encryption party and decryption party, and the private key is sent to the decryption party. The encryption party is the owner of message M. Its responsibility is to specify an access policy T and encrypt M with T. The decryption party is a requestor of the encrypted data. If it has no private key, it first sends a private key request to PKG. Then, using the private key, it decrypts the cipher text obtained from the encryption party.

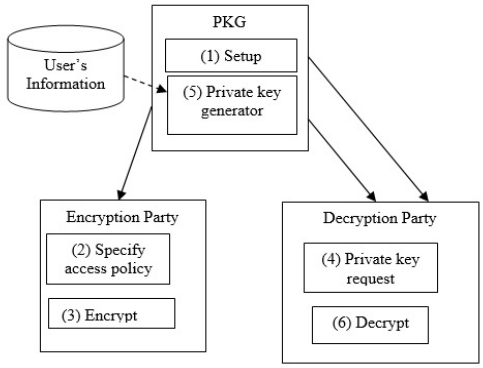

Figure 2. The CPABE Model

By integrating DC-RBAC with ECP-ABE, the RBAC-CPABE scheme is proposed, which can enforce access policies of DC-RBAC and encrypt data with ECP-ABE.The RBAC-CPABE scheme consists of the following algorithms:

1.**Setup:** the system initializes and generates the public parameters pk and the master keys mk.

2. **PolicySpecify:** the data owner specifies the access policy in the form of DC-RBAC policy rules. Then, the policy is mapped to an extended access tree T*.

3.**Encrypt:** the encryption party first transforms the extended tree T* to a standard tree T and then encrypts data using T. It produces a ciphertext CT that contains T*.

4. **Key Request:** a user who wants to decrypt CT first needs to analyze the structure of T* and extract the leaf nodes and extended leaf nodes. Then, the user applies for a private key by sending PKG the extracted parts.

5.**KeyGenerate:** first, PKG extracts the attributes associated with the leaf nodes from user's attribute set. For the extended leaf nodes, PKG verifies the user's attributes using the attribute verification algorithm. Finally, PKG obtains a new attribute set w* and generates the private key skw corresponding to w*.

6. **Decrypt**: the algorithm returns the plain text m when w* satisfies the DC-RBAC policy. Otherwise it returns an error symbol.

4.Conclusion

The overview suggests that to avoid data protection problem in cloud computing, role based access control mechanism is used. By using cipher text attribute based encryption scheme results will generate in minimum time. Self-contained data protection mechanism is integrated with CP-ABE provides the possibility for integrating encryption and access control.

References

[1]. Liu and et al., "Achieving flexible and self-contained data protection in cloud computing", IEEE of Computer Science Engineering, Journal of IEEE Access, (2017)
[2]. Alrawais and et. al., \An Attribute Based Encryption Scheme to Secure Fog Communications", Journal of IEEE Access, (2016)
[3]. Doshi and et.al, "Updating attribute in CP-ABE: A New Approach", National Institute of Tecnology,(2004)
[4]. Xiong and et.al., "A Searchable Encryption of CPABE Scheme in Cloud Storage", IEEE of CSE, (2013)
[5]. Zhu and et.al., "Role Based Cryptosystem: A new cryptographic rbac system based on role key hierarchy", IEEE Transactions on Information Forensics and Security, vol. 8, no.12, pp.2138-2153, (2013)
[6]. Sahai and et.al., "Fuzzy Identity Based Encryption", Aarhus Springer, Berlin, pp.457-473, (2005)
[7]. Goyal and et. al., "Attribute Based Encryption for Fine Grain Access", ACM Conference on computer and communication Security, pp.89-98, (2006)
[8]. BethenCourt and et.al., "Ciphertext Policy Attribute Based Encryption", IEEE Symposium on Security and Privacy, pp.321-334., (2007)
[9] Huang and et.al., "From RBAC to ABAC: constructing flexible data access control for cloud services", IEEE transactions on service computing, vol.8, no.4, pp.601-616, (2015)
[10] Crampton and et.al., "Cryptographic enforcement", pp.191-205, (2011)
[11] Ferraiolo and et.al., "Role Based Access Control", National Computer Security Conference, (2010)