International Journal of Engineering & Technology, 7 (4.6) (2018) 33-35

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Attribute based Access Control Scheme in Cloud Storage System

Banoth SeethaRamulu[1]*, H.Balaji[2] Bashetty Suman[3]

[1] *Associate Professor, Department of CSE,VardhamanCollege of Engineering,Shamshabad,Hyderabad,TS,India*
[2] *Associate Professor, Department of CSE, Sreenidhi Institute of Science and Technology, Ghatkesar,Hyderabad, TS,India*
[3]*Department of Computer Science and Engineering MLR Institute of Technology, Hyderabad*
**Corresponding author E-mail: deekshi109@gmail.com*

Abstract

Cloud Computing is an emerging technology now a days , where cloud is most preferable when there is data backup, storage and data distribution service with low cost. But cloud is semi honest in nature due to not reveled storage and security structure thus while storing and sharing cloud data , its suppose to honest and secured. When data owners outsource their data in secured manner system should assure the security, data integrity and confidentiality. Here we noticed secure access controlling is the prime objective for sensitive data management.in this regards we have been used ABE (Attribute based encryption) for the above objective. This paper concentrates on secure storage and sharing system.

Keywords: *Attribute Based Encryption, Secure Access Control, Data Owner, User, Cloud.*

1. Introduction

Today, as a growing and effective computing model, cloud computing has gained recognition and support in many areas. In the cloud, there are many legal jurisdictions, for example, real estate, rental benefits, outsourcing applications, and the central idea of the credit industry in the computer industry. Recently, many IT legends have their corporate cloud framework, p. Amazon EC2 [1], Amazon S3 [2], Google App Engine [3] and Microsoft Azure [4]. Cloud computing provides adaptive computing capability, which can reduce the cost of capital costs and use and usage. Cloud computing has many security issues due to the natural features that are unexpectedly avoided by the dynamic cloud computing, cloud scene and ecosystem ecological concepts of objects such as the global view, despite many advantages. One of the complex issues is how to ensure the safety of customer data. Security problems, data security, and cloud insurance protection are not a joke to continue to progress and spread of cloud computing if not treated correctly.

In 2009, there were many cloud-based security incidents in many IT companies, including Google, Microsoft and Amazon. These events influenced data administrations for a large number of buyers. In this way, it is important to take into account security problems in cloud computing. In cloud computing, users store their data records on servers in the cloud. In this way, it is necessary to identify unauthorized access to such assets and secure a secure exchange of assets. In traditional Access Control Policies, we agree that the data owners and the storage server are in the same secure location and that the server is completely reliable. However, in cloud computing environment, cloud companies can be attacked by a revenge attack. These attacks can release private customer data for commercial purposes, as data owners regularly store data that is decoded on cloud servers. Step-by-step diagnostic control of data coded by step by step instructions and to ensure the need to understand the progress and cluster use of classroom data records in a secure environment.

In addition, the number of users from the cloud computing will be increased in a cloud computing environment, how to determine positive control, customizable and refined most organized in cloud computing designs. B, Seetharamulu [16], in 2016 Proposes Attribute based access Control scheme for secure data cloud in P2P networks. This article presents a model based on a cryptography conspiracy based on cryptographic control (CP-ABE), a constant amount of meaning that you understand versatile control, cloud outsourcing, and data encryption in advanced computer control. Our commitments: The CP Custodian EBA Nomination receives cryptographic accuracy cryptography and maintains the productivity development, measurement and assessment of the bilinear connectivity consistently and reduces the excess calculation overhead data transmission. Secondly, we're planning a progressive access control framework. This structure supports the legacy of approval to reduce the weight and risk of a particular specialist. Finally, we demonstrate that our plan has a vicious security based on the optimal cryptography that we have chosen and that we have interrupted our plan implementation. We offer product modes before applying our plan in the cloud environment.

2. Related work

Access control is a standard security issue. Many Access Control models have been proposed since 1970, p. DAC [5], MAC [6], Bel-La Todd [7], Biba [8] etc. In 1996, Sandhu et al. Proposed role-based access control model [9] (RBAC). Many improved RBAC models have been proposed and widely used in practice. As information technology develops, traditional access control is not appropriate for access control for the following reasons in

cloud computing: For all, the accessibility of the access system is inadequate and it is difficult to expand to a hierarchical and large-scale application in the cloud computing environment. Secondly, these Access Control Systems should improve their efficiency according to a cloud computing environment. Thirdly, their dynamic adaptability is not enough for the characters. The user role is dynamic in most applications.

3. The system model and Proposed Scheme

This section is the first to provide a sampling model of our planning and emergency safety suspicions in the cloud computing environment. The frame design uses a layered structure of root professionals, high-level space experts and low level domain experts to identify trait management and expertise. The structure of the cloud computing can pump the weight and the risk of a special focus of the specialist in the environment. Furthermore, we proposed to check the CP-ABE level with a cipher with the cipher in fixed size and examine detailed scores for our plan. The consistent incentive encrypted text and encryption can solve the scope of scaling and decryption despite the ability to draft this plan. The data owner first encoded the data document using a symmetric DEK key, and the DEK uses the proposed consumer with a specific access control policy. The data owner transfers the previously encrypted text and stores it on cloud servers. Regardless of how to obtain a client and to understand the data records, it depends on how to achieve the equal key, which is selected by the client access attributes clause.

3.1. The models of our scheme

As shown in Figure 1, the sample model consists of five types of meetings: Data Owners, Customers, Cloud Organization Specialist, Routing Expert and many space experts. Cloud centric collaboration takes care of cloud servers and provides the purpose of data storage. Data owners can combine their mutual data documents and store them in the cloud. A recording memory definition in a cloud environment Figure 2, ID is the number of separate tests of a document, depicted here, the dek symmetric key cryptosystem dek and CT uses a calculation ABE. The input structure is comparing the attributes only to the client and suggested in the ciphertext, so you can express the ciphertext (we believe that the specialty of the client is a cloud client). Unbelievable Clients cannot access the data document. Next, we understand the control based on attribute-based cryptography with a fixed size ciphertext. To access interactive data papers, clients have previously downloaded the encoded data record and then decode the start of the CT record, depending on the symmetric key features model. Input procedures have revealed the attributes of the attributes. The customer data document is obtained using the symmetric key to decrypt the encrypted text of the data record.

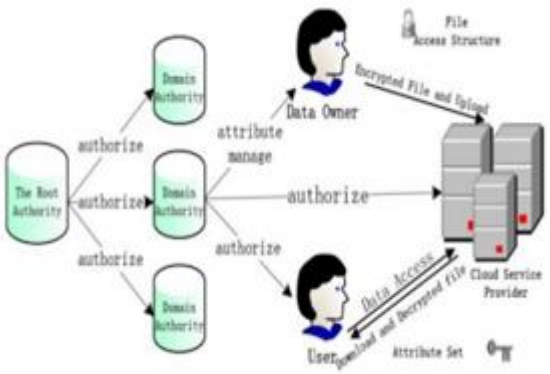

Fig. 1: System Model.

The Root Specialist has the best expert and is responsible for creating frame settings and accepting experts in the best place. Each area specialist is responsible for overseeing the space experts at the next level or for the owners / customers in their area. This expert design of the gained features reduces the calculation and disperses the focal specialist's weight and danger. A site expert manages the data of each owner / buyer. Your parent's expert oversees or hires expert professionals.

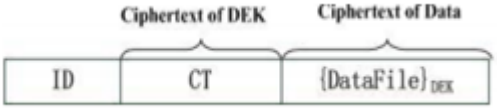

Fig. 2: Format of data file stored on the Cloud

In the security model, we expect Clients to access read-only data records. In addition, we agree that the Cloud Expert organization and semi-limited understanding have presented and fully understand the legitimate customer's commitment to work requests. In either case, you may want to combine private documents with clients to collect the log data stored in the cloud for your particular purpose or try to steal with potential clients. Moreover, we hope that channels of integration between all the frames of the framework model are safe. In addition, our plan is protected by encrypted text attacks, accepting the decision. QBDHE hypothesis is difficult to explain in the standard model.

3.2. Our Scheme

Crypto scope Size Issue the CP-ABE uses the encryption algorithm with our system's constant encryption text size, [10] based on a hierarchical system model, in order to solve the simplest dependency on the number of symptoms in general patterns.

4. Performance Analysis

4.1 Application Scenario Analysis

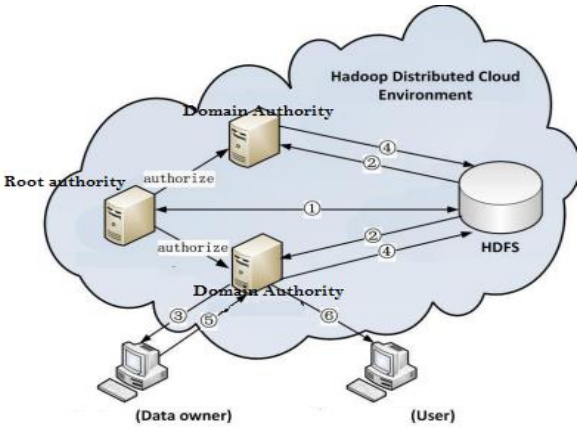

Fig.3: The HDFS Architecture for cloud

Figure 3 shows the distribution cloud environment with three centers: C1, C2 and C3. Hadoop Platform is installed on all nodes. Node C1 is a Master Node, while nodes C2 and C3 are addicted nodes. User nodes are users of new owners and data. All nodes have different IP addresses. Each component of our system modes stores privacy information on encryption and decryption independently in HDFS and we believe that third party information is not accessible except for power.

According to Figure 1 and Proposed Scheme, the C1 domains function as root power, act as C2 and C3. This procedure involves the following steps:

Step 1: As a root authority, C1 generates the user attribute set A , the public key PK and the secret key of domain authority SK_{DA} in accordance with the system attribute set U. C1 then sends the

quadruple (U,A,PK,SK_{DA}) to HDFS (Hadoop Distributed File System) which is denoted by the order number in Fig.3.

Step 2: C2 and C3 domains the role of the domain. They get (U, A, PK, SKDA) from HDFS, and the user generates the SK's secret key, which represents the number in Figure 3.

Step 3: C2 User system attribute sets, set user attribute, public key PK and secret user channel or secretive stream channel, as well as the owner of the data in the order as SK, SSL. It starts by encrypting the original data file using the Symmetric DEK encryption key. To encrypt the DEK and to create an encrypted CT file, run the algorithm, $Encrypt(PK, M, \Upsilon_{t,S})$ the DEK's access structure suggests. Finally, data owners have created a file, whose format is shown in Figure 2 and a note to the C2 in the cloud environment, indicating the command number in Figure 3. Saving the C2 file In HDFS, the order is shown in Figure 3.

Step 4: When requesting access to files stored in a user cloud, C2 downloads the file from HDFS (shown in its format Figure 2), shown in Figure 3 and sends the file to the user shown in Figure 3. Customer catches the code from CT, $Decrypt(\Upsilon_{t,S}, PK, SK_u, CT)$ and tries to decrypt CTs. If the user property is not associated with the set t, access structure, the user cannot decrypt the CT and resume the original data file. Otherwise, the user can use the secret key or SK to decrypt the CT and get the DEK. The user then extracts the encrypted text from the download file's file and decrypts the encrypted text using DEK to get the original data file.

5. Conclusion

Secure communication is an important part of cloud computing. Character-based access control data has privacy, which is not reliable to server, detailed control and approval of problematic large-scale dynamics for traditional access control light. This document proposes progressive features based on structural features based on the weight of cloud computing and reduces the risk of separating professionals. The CP-ABE project consists of a constant-sized consortium cipher dealing with the problem of cryptographic measurement, which is directly dependent on features. Our plan puts the calculation and encryption in cryptographic cryptography measurement and constant evaluation. In this way, the program improves the effect of the frame. We have done some digital reconstructions and the tests that occur are opening up an analysis. Moreover, we show that this project is CCA2 safety in the hypothesis of the Q-bilinear-Diffie-Hellman Exponent Decision. Finally, we will also display an application model in the appropriate Hadoop Cloud Environment. It shows that our plan has excellent flexibility and versatility in cloud computing. Furthermore, we want to investigate CP-ABE's calculation to make it more compatible and more productive, as well as more convenient to control the cloud environment.

References

[1] Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2/

[2] Amazon Web Service (AWS). http://s3.amazonaws.com/

[3] Google App Engine (GAE). http://code.google.com/appengine/

[4] Microsoft Azure. http://www.windowsazure.com

[5] R.W. Conway, W.L. MaxWell and H.L. Morgan, “On the implementation of security measures in formation systems,” Communations of the ACM, vol. 15, no. 4, pp:211-220, April. 1972.

[6] D.E. Denning,”A Lattice Model of Secure Information Flow,” Communications of the ACM, vol. 19, no. 5, pp:236-243, May. 1976.

[7] D.E. Bell and L.J. LaPadula, “Secure Computer System: Unified Exposition and Multics Interpretation,” Technical Report TRA885320, The MITRE Corp., Bedford, MA, Mar. 1976.

[8] K.J. Biba, “Integrity Considerations for Secure Computer Systems,” Technical Report TR-A423930, The MITRE Corp., Bedford, MA, Apr. 1977.

[9] R. Sandhu, E.J. Coyne and H.L. Feinstein, “Role-based access control models,” IEEE Computer, vol. 29, no. 2, pp:38-47, Feb. 1996.

[10] A. Ge, R. Zhang and C. Chen, “Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts,” Public Key Cryptography : 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010),LNCS 7372, pp: 336-349, 2012

[11] R.Srinivas, Ajay Kumar,” Attribute-Based Encryption for Reliable and Secure Sharing of PHR in Cloud Computing”, International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 679-682, 2015.

[12] PRAVEEN KUMAR , S.NAGA LAKSHMI,” Efficient Data Access Control for Multi-AuthorityCloud Storage using CP-ABE.”, International Journal of Computer Engineering in Research Trends., vol.2, no.12, pp. 1182-1187, 2015.

[13] B.Natraj Kumar, M.Sri Lakshmi,DrS.Prem Kumar,”Investigation on Revocable Fine-grainedAccess Control Scheme for Multi-AuthorityCloud Storage Systems”,International Journal of Computer Engineering in Research Trends., vol.2, no.8, pp. 486-491, 2015.

[14] V. Himaja,K.Lakshmi,Dr.S.Prem Kumar,” Decentralized Access Control to Secure Data Storage on Clouds”, International Journal of Computer Engineering in Research Trends., vol.3, no.1, pp. 13-18, 2016.

[15] K.Manohar, R. Anil Kumar, N.Parashuram,”Key Aggregate Searchable Encryption forGroup Data Sharing Via Cloud Data Storage”,International Journal of Computer Engineering in Research Trends., vol.2, no.12, pp. 1132-1136, 2015.

[16] B. Seetharamulu; Dr. G. V. Uma “Secure Data Access in P2P Cloud Using ABAC” Asian Journal of Research in Social Sciences and Humanities.,Vol. 6, No. 6, June 2016, pp. 1400-1409.