ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data management using Virtualization in Cloud Computing

A.S.R. Krishna Kanth
M.Tech (CST),
Department of Computer Science & Systems Engineering,
Andhra University, India.

M.Sitha Ram
Research Scholar
Department of Computer Science & Systems Engineering, AU College of Engineering, Visakhapatnam.

M.Satyanarayana
Research Scholar
Department of Computer Science & Systems Engineering, AU College of Engineering, Visakhapatnam.

Abstract :

Data security is the most important feature for accessing data in the cloud. Due to data outsourcing and distrust cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. we design a data management using virtualization system, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. The attribute revocation method can efficiently achieve both forward security and backward security.

Keywords:

CP – ABE, Data Management, Cloud Storage, Multiple - Authority.

I.INTRODUCTION:

The cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. It is the delivery of hosted services over the Internet. Cloud Computing is subcategorized into three types namely Private Cloud, Public Cloud, and Hybrid Cloud. Private cloud services are delivered from a business data centres to internal users. It offers a versatility and convenience by preserving management, control and security. Public cloud model involves a third - party provider where it delivers the cloud service over the internet.

These cloud services where sold on demand. The users pay for the CPU cycles, storage or bandwidth for which they consume. Hybrid cloud is a combination of public cloud services and on – premises private cloud. The consumers can run mission – critical workloads that must scale on demand. The main aim of hybrid cloud is to create a unified, automated, scalable environment. The cloud computing has been divided into three broad service categories. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). IaaS provides a virtual server instance and storage, as well as application program interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and start, stop, access and configure the VM and storage as desired. Hence these are the three main services of the cloud computing. IaaS providers offer a small, large, extra large memory or compute – optimized instances in addition to customized instances for various workload needs. The PaaS model, providers host development tools on their infrastructure. Users access those tools over the internet using APIs, web portals or gate way software after it is developed. SaaS is a distribution model that delivers software applications over the internet. These are often called web services. SaaS applications and services from any locations using a computer or mobile device that has Internet access. Cloud management involves the software and technologies designed for operating and monitoring applications, data and services residing in the cloud. Cloud management tools help ensure cloud computing based resources are working optimally and properly interacting with users and other services. Cloud management involves the software and technologies designed for operating and monitoring applications, data and services residing in the cloud. Cloud management tools help ensure cloud computing based resources are working optimally and properly interacting with users and other services. Cloud management involve numerous tasks including performance monitoring security and compliance auditing and management, and initiating and overseeing disaster recovery and contingency plans.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There are two types of CP-ABE systems: single-authority CPABE [2], [3], [4], [5] where all attributes are managed by a single authority, and multi-authority CP-ABE where attributes are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities.

In multi-authority cloud storage systems, users' attributes can be changed dynamically. A user may be entitled some new attributes or revoked some current attributes. And his permission of data access should be changed accordingly. However, existing attribute revocation methods[7] either rely on a trusted server or lack of efficiency, they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

In this paper, we first propose a revocable multi authority CPABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new cipher text that requires the revoked attribute to decrypt)and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes).

Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

Advantages of the proposed system consists of, We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation. We greatly improve the efficiency of the attribute revocation method. We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a cipher text.

II. PROBLEM STATEMENT:

We first propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new cipher text that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

Existing system:

This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

Disadvantages of existing system:

•Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, since it holds the master key of the system.

•Chase's protocol does not support attribute revocation.

Proposed system:

In this paper, we propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.
Advantages of proposed system

•We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation. We greatly improve the efficiency of the attribute revocation method.

•We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a cipher text.

III. SYSTEM ARCHITECTURE:

Data access control system in multi-authority cloud storage, as described in Fig. 1. There are five types of entities in the system: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users).

Certificate Authority:

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity.

Attribute Authorities:

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

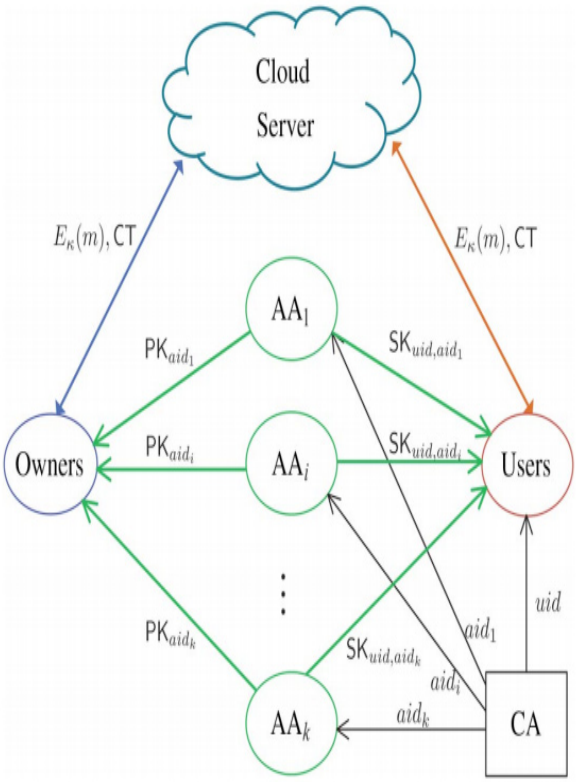

Fig. 1 System architecture for cloud storage

Data Consumers:

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:

Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:

The owner sends the encrypted data to the cloud server together with the cipher texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the cipher text. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.Hence these are the description of the modules which are present in the system architecture of the CAP – ABE attribute based encryption. CAP – ABE means cipher text policy attribute based encryption here each module performs different kinds of operations.

Security Model:

In multi-authority cloud storage systems, we make the following assumptions:

•The CA is fully trusted in the system. It will not collude with any user, but it should be prevented from decrypting any cipher texts by itself.

•Each AA is trusted but can be corrupted by the adversary.

•The server is curious but honest. It is curious about the content of the encrypted data or the received message, but will execute correctly the task assigned by each attribute authority.

•Each user is dishonest and may collude to obtain unauthorized access to data.

IV. OVERVIEW:

To design the data access control scheme for multi authority cloud storage systems, the main challenging issue is to construct the underlying Revocable Multi authority CP-ABE protocol. In [6] chase multi-authority CP-ABE protocol, however, it cannot be directly applied as the underlying techniques because of two main reasons: 1) Security Issue: Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system; 2) Revocation Issue: Chase's protocol does not support attribute revocation. We propose a new revocable multi-authority CP-ABE protocol based on the single-authority CP-ABE proposed by Lewko and Waters . That is we extend it to multi authority scenario and make it revocable. We apply the techniques in Chase's multi-authority CP-ABE protocol to tie together the secret keys generated by different authorities for the same user and prevent the collusion attack. Specifically, we separate the functionality of the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of users and AAs in the system. It assigns a global user identity uid to each user and a global authority identity aid to each attribute authority in the system. Because the uid is globally unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption. Also, because each AA is associated with an aid, every attribute is distinguishable even though some AAs may issue the same attribute. To deal with the security issue instead of using the system unique public key (generated by the unique master key) to encrypt data, our scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevents the certificate authority in our scheme from decrypting the cipher texts.

Secret Key Generation:

Each user uid is required to authenticate itself to the AAaid before it can be entitled some attributes from the AAaid. The user submits its certificate Certificate(uid) to the AAaid. The AAaid then authenticates the user by using the verification key issued by the CA. If it is a legal user, the AAaid entitles a set of attributes Suid,aid to the user uid according to its role or identity in its administration domain. Otherwise, it aborts. Then, the AAaid generates the user's secret key SKuid,aid by running the secret key generation algorithm SKeyGen.

Data Decryption:

All the legal users in the system can freely query any interested encrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different AAs.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Only the attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content key.

Attribute Revocation:

As we described before, there are two requirements of the attribute revocation: 1) The revoked user (whose attribute is revoked) cannot decrypt new cipher texts encrypted with new public attribute keys (Backward Security); 2) the newly joined user who has sufficient attributes should also be able to decrypt the previously published cipher texts, which are encrypted with previous public attribute keys (Forward Security).

V. WORKING OF THE SYSTEM:

We design a web browser which consists of all the five entities, Certificate Authority, Attribute Authorities, Data owners, Cloud Server, Data Consumers. In this system taking first the data consumer (user), the user must have to register with their details. The user must have to register in order to use the cloud services. After the registration the user must have to get the rights in order to upload the data into cloud, the certificate authority is responsible for giving rights to the new user. The certificate authority activates the new user and gives the rights in order to access the cloud service. The user can upload their data into cloud after being certified by the certificate authority. The data owner (admin) monitors the data that is uploaded in the web browser, the data owner is responsible for uploading the data into cloud which is kept by the user. The data owner verifies the data and uploads it into the cloud. The attribute authority is responsible for giving the data from the cloud to the users. The attribute authority sends the secrete key to the user, the secrete key authentication is required in order to download the file from the cloud. The secrete key generation is useful for the user in order to maintain the security to the data present in the cloud. Unauthorized users cannot be able to get the data from the cloud. The secrete key is sent by the attribute authority to the registered mail id of the user, so that the data can be downloaded from the cloud securely. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the distrusted cloud. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. The fig.2 implies that any user in the group can securely share data with others by the distrusted cloud.

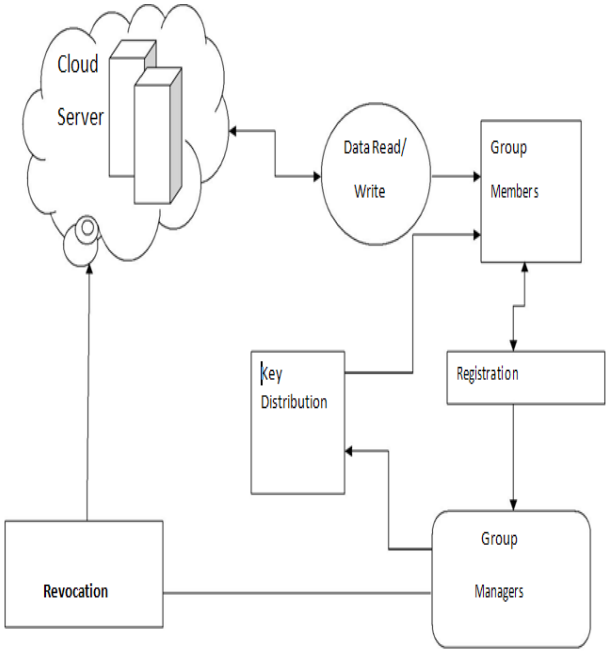

Fig. 2 Processes for uploading/downloading data from the cloud server.

We know that the cloud server cannot be fully trusted by data owners, thus traditional attribute revocation methods are no longer suitable for cloud storage systems. The proposed attribute revocation method does not require a fully trusted server. But, it incurs a heavy communication cost since it requires the data owner to transmit a new cipher text component to every non-revoked user. From the Fig.2 we can explain that the members must have to register in the web site domain in order to access the cloud storage. After the completion of the registration process the details of the user are displayed to the cloud authorities so that the user will be given rights for using the cloud storage. In order to download the file from the cloud, the attribute authorities will send the key to the user, so that the user must have to enter the key to get the data stored in the cloud server. Here the term group managers refer to certificate authority, attribute authorities, data owner, cloud server. These entities play a major role for data access.

VI. CONCLUSION:

In this paper we conclude that the success of the paradigm necessitates the design of a scalable and elastic system that can provide the data management as a service. We considered the issues in deploying data management in the cloud infrastructure. we constructed an effective data access control scheme for multi-authority cloud storage systems.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES:

[1] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption,’’in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.

[3]B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.

[4]V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008, pp. 579-591.

[5]A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.

[6]M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.

[7] M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Security in Multi-Authority Attribute-based Encryption,’’ in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09),2009, pp. 121-130.

[8]A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute-Based Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’11, 2011, pp. 568-588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261-270.

[10]M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ‘‘Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,’’ IEEE Trans.Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[11]J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,’’ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[12]S. Jahid, P. Mittal, and N. Borisov, ‘‘Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,’’ in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS’11), 2011, pp. 411-415.

[13]S. Ruj, A. Nayak, and I. Stojmenovic, ‘‘DACC: Distributed Access Control in Clouds,’’ in Proc. 10th IEEE Int’l Conf. TrustCom, 2011, pp. 91-98.

[14] K. Yang and X. Jia, ‘‘Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,’’ in Proc. 32th IEEE Int’l Conf. Distributed Computing Systems (ICDCS’12), 2012, pp. 1-10.

[15] D. Boneh and M.K. Franklin, ‘‘Identity-Based Encryption from the Weil Pairing,’’ in Proc.21st Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’01, 2001, pp. 213-229.

[16]A.B. Lewko and B. Waters, ‘‘New Proof Methods for Attribute- Based Encryption: Achieving Full Security through Selective Techniques,’’ in Proc. 32st Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’12, 2012, pp. 180-198.