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

Protect Privacy of Data in Cloud Computing By Using Data Access Control Schema for Multi-authority Cloud Storage

Ahmed Mahdi Abdulkadium
Master of Science (Information System),
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

ABSTRACT:

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted 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. In this paper, we design a protect privacy of data in cloud computing by using data access control scheme for multi-authority cloud storage systems, 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.

Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works. In this project 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).In this paper 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.

Index Terms:

Security, Data Access Control, Multi-Authority, CP-ABE, Revocable multi-authority (CPABE) scheme, Cloud Storage.

INTRODUCTION:

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. In the Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in cloud are very dynamic and scalable.It is unlike grid computing, utility computing, or autonomic computing. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

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

It is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources [1].Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud removes the need for you to be in the same physical location as the hardware that stores your data.

Cloud is a new business model wrapped around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources. It also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. Developers had asked IT professionals to tell what technologies they were currently deploying that support a current or planned cloud environment. Nearly three in four are currently using virtualization to consolidate servers and enabling virtual machine (VM) mobility across multiple servers (73 percent) in order to support a cloud. Nearly half offer automation and metering and charge-back based on usage and enable business units to self-provision resources [2].

LITERATURE SURVEY:

"Ciphertext-Policy Attribute-Based Encryption"

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters [14].

In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control.

However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper they presented a system for realizing complex access control on encrypted data that they call Ciphertext-Policy Attribute-Based Encryption. By using their techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, their methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys.While in their system attributes are used to describe a user's credentials, and a party encrypting data deter-mines a policy for who can decrypt. Thus, their methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).In addition,they provide an implementation of their system and give performance measurements.

"Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization"

AUTHOR: B. Waters [15].

In this paper, they presented the first ciphertext-policy attribute-based encryption systems that are efficient, expressive, and provably secure under concrete assumptions. All of their constructions fall under a common methodology of embedding an LSSS challenge matrix directly into the public parameters. Their constructions provide a tradeoff in terms of efficiency and the complexity of assumptions.

"Multi-Authority Attribute Based Encryption"

AUTHOR: M. Chase [16].

In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext.Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes [SW05]. They answered this question in the affirmative.

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

Their scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes, he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. their scheme can tolerate an arbitrary number of corrupt authorities. They also showed how to apply their techniques to achieve a multi-authority version of the large universe fine grained access control ABE presented by Gopal et al.

"Fully Secure Functional Encryption:Attribute-Based Encryption and (Hierarchical) Inner Product Encryption"
AUTHORS: A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters [17].

In this paper, they presented two fully secure functional encryption schemes: a fully secure attribute-based encryption (ABE) scheme and a fully secure(attribute-hiding) predicate encryption (PE) scheme for inner-product predicates. In both cases, previous constructions were only proven to be selectively secure. Both results use novel strategies to adapt the dual system encryption methodology introduced by Waters. They constructed their ABE scheme in composite order bilinear groups, and prove its security from three static assumptions. Their ABE scheme supports arbitrary monotone access formulas. Their predicate encryption scheme is constructed via a new approach on bilinear pairings using the notion of dual pairing vector spaces proposed by Okamoto and Takashima.

PROBLEM STATEMENT:

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. Existing methods either rely on a trusted server or lack of efficiency. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

Draw Backs:

- 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 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. Our proposed data access control schema is providing privacy in the random oracle model and more efficient than previous works. 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 :

- 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 ciphertext.

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

• We guarantee data privacy in cloud storage by preventing un authorized access of users who do not have the right attributes to accessing and downloading file from a cloud.

• A revocable multi-authority schema provided privacy in the random oracle model.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

1) 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.

2) 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.

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

4) Cloud Server:

The owner sends the encrypted data to the cloud server together with the ciphertexts. 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 ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

5) 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.

KEY TECHNOLOGY:
ABE (Attributed-Based Encryption)

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE).

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

The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

Cipher text-Policy ABE

In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text.

Policies may be defined over attributes using conjunctions, disjunctions and (k,n)-threshold gates, i.e., k out of n attributes have to be present (there may also be non-monotone access policies with additional negations and meanwhile there are also constructions for policies defined as arbitrary circuits). For instance, let us assume that the universe of attributes is defined to be {A,B,C,D} and user 1 receives a key to attributes {A,B} and user 2 to attribute {D}. If a ciphertext is encrypted with respect to the policy (AC)D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.

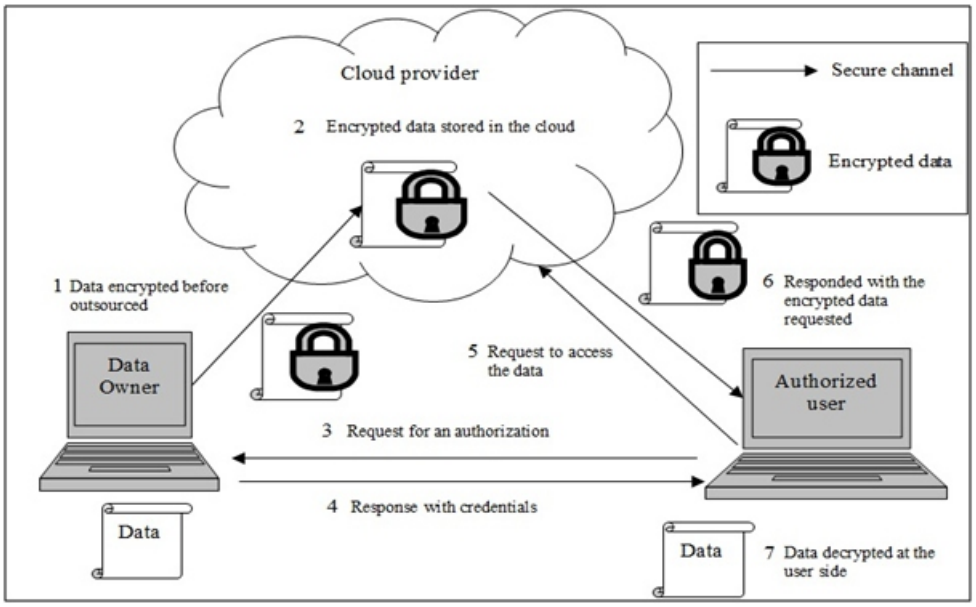

Figure 3.1 Structure of CP-ABE

ALGORITHM DETAILS

AES (Advanced Encryption Standards)

The Advanced Encryption Standard (AES) is a symmetric-key encryption standard approved by NSA for top secret information and is adopted by the U.S. government. AES is based on a design principle known as a substitution permutation network. The standard comprises three block ciphers: AES-128, AES-192 and AES-256. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide; AES was selected due to the level of security it offers and its well documented implementation and optimization techniques. Furthermore, AES is very efficient in terms of both time and memory requirements. The block ciphers have high computation intensity and independent workloads (apply the same steps to different blocks of plain text).

Chart I	Key Length (Nk words)	Block Size (Nb words)	Number of Rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table (3.1) AES Blocks

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

Explanations:

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Most AES calculations are done in a special field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. For the algorithm AES-128 the key length is four, the block size is four and the number of rounds or iterations is 10, whereas for AES-192, where the key length is six and block size is four, the number of iterations is 12 and for AES-256 the number of iterations is 14. Each time a round is executed a new key is introduced. The AES algorithm subbyte transformation is effected using an S-BOX wherein the data block 16 is comprised of four words 30, 32, 34, 36 each of four bytes

High-level description of the algorithm

1.Key Expansion—round keys is derived from the cipher key.

2.Initial Round Add Round Key—each byte of the state is combined with the round key using bitwise xor.

3.Rounds

1.Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a look up table.

2.Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

3.Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4.Add Round Key

4.Final Round (no Mix Columns)
1.Sub Bytes

2.Shift Rows

3.Add Round Key

RESULTS:

Figure 7.1 Home Page

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

Figure 7.3 User Registration Page

CONCLUSION:

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure in the random oracle model. It also provided privacy of cloud storage data users, means that only the user who has activated and the right attributes can access to the data on cloud storage, in this case we provided security on the data by protected from unauthorized access by using an efficient data access control schema for multi_authority cloud storage. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc, even in the data privacy that we do not want to share with anyone.

FUTURE WORK:

In the future work, we will provide a secure multi-owner data sharing scheme for dynamic group in the cloud. By providing group signature and dynamic broadcast encryption techniques, any cloud user can securely share data with others. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we will analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

RGEFERENCES:

[1] Sunita Rani and AmbrishGangal, " Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints ", (IJCSIT) ,Vol. 3 (3) , 2012 ,4302 – 4304.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[3] Lawyerdonedea Crop. (What Every User Needs To Know Before Moving To The Cloud).

[4] Melanie Pinola. (What Is Cloud Computing? And Example Of Cloud Computing).

[5] Megha Sachdeva1, Pooja Rana2, Rajeev Kapoor3 And MohdShahid4(Cloud Computing – Pay As You Go Technology) Proceedings Of The 5th National Conference; Indiacom-2011.

[6] Http://Explainingcomputers.Com/Cloud.Html.

[7] Sun Microsystems White Paper, —Introduction to Cloud Computing Architecture, June 2009.

[8] " Advance Computer Technology " a book by Dr. Deven shah. Edition- 2011.

[9]Ramgovind S, Eloff MM, Smith E ," The Management of Security in Cloud Computing ", School of Computing, University of South Africa, Pretoria, South Africa ©2010 .

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

[10] http://searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-Choosing-a-VPN-type-to-connect-to-the-cloud.

[11] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R.Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, andB. Zhao, " Oceanstore: An Architecture for Global-Scale Persistent Storage, " Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000 .

[12] (Planning Guide Cloud Security) Seven Steps For Building Security In The Cloud From The Ground Up Sponsors Of Tomorrow May 2012 Intel It Center.

[13] Security For Cloud Computing 10 Steps To Ensure Success © 2012 Cloud Standards Customer Council.

[14] 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.

[15] 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.

AUTHORS BIOGRAPHY:

Ahmed Mahdi Abdulkadium, pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U, Basheer Bagh, Hyderabad, India.