ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Effective Revocable and Fine-grained Access Control Scheme for Multi-Authority in Public Cloud

T.Neetha

Associate Professor, Dept. of CSE, Brilliant Grammar School Educational Institutions Group of Institutions Integrated Campus, T.S, India

ABSTRACT: Cloud computing is one of the emerge technologies in order to outsource huge volume of data inters of storage and sharing. To protect the data and privacy of users the access control methods ensure that authorized users access the data and the system. Fine grained-approach is the appropriate method for data access control in cloud storage. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. Specifically, in this paper we investigate on revocable multi-authority Fine-grained-Scheme performance.

KEYWORDS: cloud storage, data access control, cloud servers, multi-authority, and attribute revocation, CP-ABE scheme.

I. INTRODUCTION

All Data access control is an efficient way to ensure the data security in the cloud. Cloud storage services allows data owner to outsource their data to the cloud. Attribute-based encryption (ABE) [1] is a new concept of encryption algorithms that allow the encryptor to set a policy describing who should be able to read the data. In an attribute-based encryption system, all the attribute sets are distributed by an authority. A user should be able to decrypt a ciphertext if and only if their attribute set satisfy. 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 conventional 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 (ciphertext-policy ABE - CP-ABE). In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Fine–grained schema is considered as one of the most suitable scheme for data access control in cloud storage. This scheme provides data owners more direct control on access policies at cloud level [2]. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. So This paper produce Fine –grained scheme on efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities cooperate and each authority is able to issue attributes independently

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

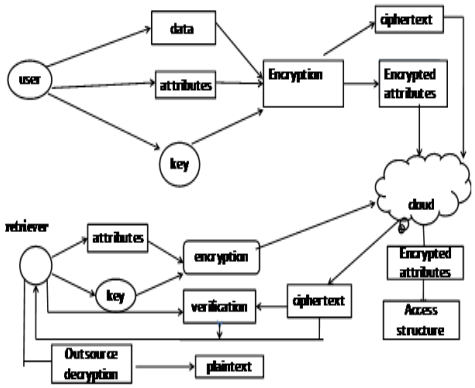

Fig1: Example diagram for data sharing with cloud storage.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem the cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized user's access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

II. LITERATURE SURVEY

Shamir [10] proposed the concept of identity-based cryptography and Boneh et al. [11] constructed the first practical system identity-based cryptography. Sahai et al. [12] presented a fuzzy identity-based encryption scheme which is the earliest prototype of attribute-based encryption (ABE). Goyal et al. [7] further clarified the concept of ABE and proposed two complimentary forms of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CPABE). According to Goyal's KP-ABE scheme, Bethencourt et al. [13] proposed a CP-ABE scheme that was closer to real access control systems. CP-ABE relates the user's secret key with a set of attribute and associates the ciphertext with an access structure tree. If the attribute set satisfies the access structure tree, then the user has the ability to decrypt the data. As CP-ABE schemes [13]-[20] are more natural to accomplish access control, we focus on the CP-ABE to realize our scheme

In the paper [21]-[23], they discussed the usage of ABE to realize fine-grained access control for outsourced data. In these schemes, a trusted single authority is responsible for the management of attribute and the key distribution. Nevertheless, this setting easily leads to data leakage and the single authority becomes a bottleneck in the large scale cloud storage systems. There are many papers proposed some new encryption methods to solve problems about multi-authority ABE.

In [1], Yang et al. designed an efficient attribute revocation method that can achieve both forward security and backward security while only incurred less communication cost and less computation cost of the revocation, where only those components associated with the revoked attribute in the secret keys and the ciphertext need to be updated. The scheme is designed for multi-authority cloud storage system. However, the global certificate authority in the system model is set to be trusted. However, in real storage systems, the authority can fail or be corrupted, which may leak out the data since the authority masters some important information.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

III. SYSTEM AND SECURITY MODEL

We consider a protected distributed storage framework for multi authorities, as appeared in Fig.1. The framework show in this paper includes five unique elements: global certificate authorities (CAs), the attribute authorities (AAs), the cloud server (server), the data owners (owners) and the data consumers (users).

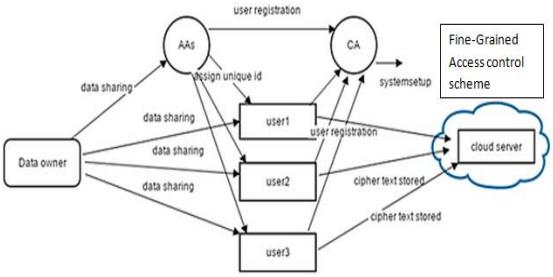

Fig1.System Model of our Scheme

CA: Each CA is a global trusted certificate in the framework. They acknowledge the enlistment of the considerable number of clients and AAs in this framework. In addition, the CAs are in charge of the conveyance of global secrete key and global open key for each legitimate client in the framework. In any case, they are not included in any quality administration and the production of secret keys that are connected with attributes.

AA: Each AA is an autonomous quality power. Each AA is in charge of issuing, repudiating and upgrading client's credits as indicated by their own particular part or personality in its space. Each characteristic is connected with one single AA. Be that as it may, every AA can deal with a subjective number of properties. It is in charge of creating an open quality key for every property it oversees and a Secret key for every client partners with their properties. Each AA has positive control over the structure and semantics of its characteristics.

Cloud server: The cloud server stores the proprietors' information and gives information get to administration to clients. In this paper, the cloud server creates the unscrambling token of a ciphertext for the client by utilizing the client' Secret keys issued by the AAs. What's more, the server likewise does the overhaul operation of the ciphertext when attribute repudiation happens.

Data owner: The data owners in this framework characterize the get to approaches of information. Under the strategies, the information proprietors encode the information before outsourcing them in the cloud. Without depending on the server to acquire the information get to control, all the legitimate clients in the framework can get to the ciphertext. In any case, the get to control happens inside the cryptography. Just when the client's attributes fulfill the get to arrangement characterized in the ciphertext, can the client decode the ciphertext?

Client(User): A cloud client could be an endeavor or one single client. Every client in the framework is doled out with a few shares of a personality from the CAs, which can be accumulated and ascertained as its exceptional worldwide client character. To decode a ciphertext that can be gotten to unreservedly from the cloud server, every client may present their Secret keys issued by a few AAs together with its worldwide open key to the server. At that point the framework requests that it produce a decoding token for some ciphertext. After accepting the decoding token, the client can unscramble the ciphertext utilizing its worldwide Secret key. The server can create the right decoding token, just when the client's attributes fulfill the get to strategy characterized in the ciphertext. To store the Secret keys and the worldwide client's open key on the server, in this manner, if no Secret keys are upgraded for the further unscrambling token era, the client require not present any Secret keys. Keeping in mind the end goal to meet the security prerequisites, our information get to control plan is a gathering of calculations joining an arrangement of CP-ABE algorithms: CASetup, AASetup, UserRegister, KeyGen, Encrypt, TKGen, Decrypt and a set of attribute revocation algorithms: UKeyGen, KeyUpdate, CiphertextUpdate.

Security Model

We consider the case that the server may send the owners' data to the clients who don't have admittance authorization in distributed storage frameworks. We accept that the server will execute accurately the undertaking relegated by the property power yet the server is likewise inquisitive about the substance of the scrambled information. The clients who

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

are untrustworthy may connive to get unapproved access to information. The AA can be undermined or traded off by the aggressors. The CA may run over blackout and security breaks in the distributed storage frameworks. This area portrays the security display for multi-power CP-ABE frameworks by the accompanying diversion between a challenger and a foe. Like the personality based encryption plans [10]–[11], the security show permits the enemy to question for any mystery keys that can't be utilized to decode the test ciphertext. We accept that the foes can degenerate powers just statically like however key inquiries are made adaptively. Give A S a chance to mean the arrangement of the considerable number of powers.

IV. ATTRIBUTED-BASED ACCESS CONTROL WITH MULTIPLE CERTIFICATE AUTHORITIES

Construction of the Proposed Access Control Scheme

We construct a secure access control system for multi-authority cloud storage without a global fully trusted certificate authority based on an adapted CP-ABE scheme in [1]. Let CA S , A S and U S denote the set of global trusted certificate authorities, the set of attribute authorities and the set of users in the system respectively. Let G and GT be the multiplicative groups with the same prime order p and : T e G GG×→ be the bilinear map. Let g be the generator of G . Let * H:{0,1} → G be a hash function such that the security is in the random oracle. Our access control scheme consists of five phases: System Initialization, Key Generation, Encryption, Decryption and Attribute Revocation.

System initialization phase: The system initialization phase generates system global parameters and authority secret and public key pairs. It consists of two algorithms: CA setup and AA setup

CA Setup: All the CAs run the CA setup algorithm CASetup. First, it will take a security parameter as input. Then the CAs chooses a random number respectively as the master key MSK_i of the system and then compute the global master key MSK from the verifiable secret sharing scheme based on bilinear-pairs mentioned above, as well as the system parameter. Afterwards

AA Setup: All the AAs in S_A run the AA setup algorithm.

Key Generation Phase: Each AA runs the key generation algorithm KeyGen. The AA_k generates its authority public key

Attribute Revocation Phase: Considering an attribute X_k of a user U_μ is revoked from AA_k, there are three phases included in the process of the attribute revocation: Update Key Generation, Key Update and Ciphertext Update.

Update Key Generation: By running the update key generation algorithm UKeyGen, AA_k generates a new attribute version key $V_{xk}$to substitute the previous one, taking the authority secret key SK_k , the current attribute version key V_{xk} and the user's global public keys GPK_{Uj}as inputs.

Key Update: The key update can prevent the revoked user from decrypting the new data which is encrypted by the new public keys **(Forward Security).**

Ciphertext Update: The ciphertext update can make sure that the newly joined user can still access the previous data which is published before it joins the system, when its attributes satisfy the access policy associated with the ciphertext **(Backward Security).**

V. CONCLUSION

This investigation explains a revocable multi-authority Fine-grained scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-authority cloud storage systems is proposed. It eliminates Decryption overhead for users according to attributes .This secure attribute based cryptographic technique for robust data security that's being shared in the cloud .This revocable multi-authority Fine-grained scheme with Verifiable outsourced decryption and proved that it is secure and verifiable.

REFERENCES

[1] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in INFOCOM, 2013 Proceedings IEEE, (2013), pp. 2895-2903

[2] 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

[3] 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.
[4] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: AttributeBased Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology- EUROCRYPT'10, 2010, pp. 62-91.
[5] 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.
[6] S. 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.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control ofencrypted data,‖ in Proceedings of the 13th ACM Conference on Computer and Communications Security(CCS'06). ACM, (2006), pp. 89–98.
[8] 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.
[9] Mr.SanthoshkumarB.J, M.Tech, Amrita VishwaVidyapeetham, Mysore Campus, India "Attribute Based Encryption with Verifiable Outsourced Decryption." In International Journal of Advanced Research in Computer Science and Software Engineering"Volume 4, Issue 6, June 2014, ISSN: 2277 128X.
[10] A. Shamir, ―Identity-based cryptosystems and signature schemes,‖ in Proceedings of the 4st AnnualInternational Cryptology Conference: Advances in Cryptology - CRYPTO'84. Springer, (1984), pp. 47–53.
[11] D. Boneh and M. K. Franklin, ―Identity-based encryption from the weil pairing,‖ in Proceedings of the 21st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'01. Springer, (2001), pp.213–229.
[12] A. Sahai and B. Waters, ―Fuzzy identity-based encryption,‖ in Proceedings of the 24th Annual InternationalConference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology -EUROCRYPT'05. Springer, (2005), pp. 457–473.
[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security andPrivacy, 2007.SP'07. IEEE Symposium on, (2007), pp. 321-334.