ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Secured Attribute Revocation of Data in Multi-Authority Cloud Storage Using Attribute Based Encryption

Yarlagadda Shravani[1], S V Ramanamurthy[2], M.Rajakumar[3]

M.Tech, Dept. of CSE, Pragati Engineering College, Kakinada, India[1]

Professor, Dept. of CSE, Pragati Engineering College, Kakinada, India[2]

Associate Professor, Dept. of CSE, Pragati Engineering College, Kakinada, India[3]

ABSTRACT: Now-a-days Cloud security is an essential key parameter while storing and sharing data in cloud storage servers. The main objective of this paper is to provide attribute revocation among multi-authority cloud server framework. In order to perform this attribute revocation we have been proposed a novel multi-authority CP-ABE scheme along with effective decryption, and also design an attribute revocation method that can achieve both forward security and backward security.

KEYWORDS: Cloud Storage, Data Access Control, Cloud Servers, Multi-Authority, and Attribute Revocation, CP-ABE Scheme.

I. INTRODUCTION

Cloud computing is an emerging technology nowadays, which performs several primitive services like SaaS, IaaS, and PaaS. In order to the data store and sharing, we have been used IaaS services which perform various data storage server related functionalities and all. Where security is also an essential perception while storing and sharing data in cloud when data accessibility among multi-authority in this connection we have been integrating two primitive policies:

- Cipher-text-Policy ABE (CP-ABE)
- Key Policy ABE (KP-ABE)

These are the policies which perform primitive operation on attribute-based encryption architectures; Now-a-days broad research has been accomplished for CP-ABE, since it does not require the data owner to distribute keys and gives them more direct control on acquiring provisions. However, a client may hold set of attributes which are distributed by different authorities who are in control of attribute management and key distribution in CP-ABE policies [14]. For another, the data owner may share his/her information to clients controlled by various authorities. Presented CP-ABE schemes dealt with a single authority, it cannot be pragmatic to data access control for multi-authority systems since no authority is able to verify attributes through different organizations and to issue secret keys to all the users in the system. The main objective of this paper is to provide attribute revocation among multi-authority cloud server framework.

There are two exciting issues in the design of multi-authority access control schemes for cloud storage systems, Where the first issue is the collusion problem where several users holding attributes from different authorities may collude together to attain illegal access to the data. And the second issue is the attribute revocation, which allows accessing the data those who were having access privileges, once the user may exit or revoke from the organizations, he/she will no longer have access privileges to access the data on cloud servers.

In this paper, we design a productive multi-authority CP-ABE technique without utilizing a global authority and propose Multi-Authority Cloud Storage systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

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 cipher-text-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 cipher-text 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] are more natural to accomplish access control, we focus on the CP-ABE to realize our scheme

In the paper [15]-[16], 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 proposed papers with 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 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 cipher-text need to be updated. The scheme is designed for the 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.

III. SYSTEM AND SECURITY MODEL

We consider a secure distributed cloud storage framework for multi authorities, as shown in Fig.1. - The framework shown in this paper includes five unique elements:

- Global Certificate Authorities (CAs),
- The Attribute Authorities (AAs),
- The Cloud Server (server),
- The Data Owners (Owners)
- The Client (Users).

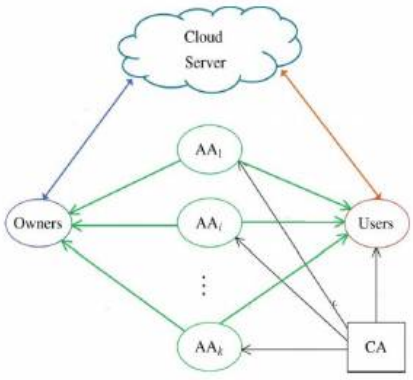

Fig1. System Model of our Scheme

Global Certificate Authorities (CA): Each CA is a globally trusted certificate in the framework. It will give registration to all users and attribute authorities in this framework. In addition, the CAs are responsible for the transference of global secret key and global public key for each authentic client in the framework. In any case, the certificate authority is never involved in the data management and also not involved in the secret key generation.

Attribute Authority (AA): Each AA is an independent authority and is in control of entitling and revoking user's attributes according to their role or identity. Each characteristic is connected with one single AA. Be that as it may,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

every AA can deal with a particular number of attributes. It is in control of creating a public key for every user it archives and a Secret key for every client associates with their attributes. It has total information about the structure and meanings of each attribute. It is responsible for generating a public key and to generate a secret key for each user.

The Cloud Server (Server): The cloud server stores the owners' information and gives information get to administration to clients. In this paper, the cloud server creates the unscrambling token of a cipher-text for the client by utilizing the client' Secret keys issued by the AAs. What's more, the server likewise does the service setup of the cipher-text when attribute denial occurs.

Data owner (Owners): The data owners in this framework characterize the information under certain strategies to encode the information before outsourcing them in the cloud. Without depending on the server to acquire the information to get control of all the authentic clients in the framework and get to the cipher-text. In any case, the control happens inside the cryptography, just when the client's attributes fulfill the arrangement characterized in the cipher-text.

The Client (User): A cloud client could be an endeavor or a 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 global client character. To decode a cipher-text that can attained unreservedly from the cloud server, every client may present their Secret Keys issued by a few AAs together with its public key to the server. At that point, the framework requests that it produce a decoding token for some cipher-text. After accepting the decoding token, the client can unscramble the cipher-text utilizing its global Secret key. The server can create the right decoding token, just when the client's attributes fulfill the strategy characterized in the cipher-text. To store the Secret keys and the global client's public 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 proposed design meet the design of CP-ABE algorithms:

- CA Setup, AA Setup, User Register, Key Gen, Encrypt, TK Gen, Decrypt

and a set of attribute revocation algorithms: U Key Gen, Key Update, Cipher text Update.

SECURITY MODEL

We consider the case that the server may send the owners" data to the clients who don't have admission authorization in distributed storage frameworks. We accept that the server will execute accurately, the undertaking relegated by the property authority yet, the server is likewise inquisitive about the substance of the scrambled information. The clients who 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-authority CP-ABE frameworks by the accompanying diversion between a rival and an adversary. 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 cipher-text. We accept that the opponents can degenerate authority just statically like however key inquiries are made adaptively.

IV. ATTRIBUTED-BASED ACCESS CONTROL WITH MULTIPLE CERTIFICATE AUTHORITIES

Construction of the Proposed Access Control Scheme [14]

We construct a secure access control system for multi-authority cloud storage without a global fully trusted Certificate Authorities based on an adapted CP-ABE scheme in [1]. Let CAs, AAs, and Users denote the set of globally trusted Certificate Authorities, set of Attribute Authorities and the set of Users in the system respectively

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

1. CA setup and
2. AA setup

CA Setup: All the CAs run the CA setup algorithm. First, it will take a security parameter as an input. CAs chooses a random number respectively as the master key (MSKi) 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.

AA Setup: The attribute authority setup algorithm is run by the CA. It takes the authority identity (*aid)* as input. It outputs a pair of authority secret key (Sk_{aid}), authority public key (Pk_{aid})

Key Generation Phase: Each AA runs the key generation algorithm (Key Gen). The AAk generates its authority public key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Attribute Revocation Phase: Considering an attribute Xk of a user Uμ is revoked from AAk, there are three phases included in the process of the attribute revocation:

1. Update Key Generation
2. Key Update
3. Cipher-text Update.

Update Key Generation: By running the update key generation algorithm UKeyGen, AAk generates a new attribute version key Vxk to substitute the previous one, taking the authority secret key SKk, the current attribute version key Vxk and the user's global public keys GPKUj 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).**

Cipher-text Update: The cipher-text 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 cipher-text **(Backward Security).**

V. CONCLUSION

In this paper, we have been providing attribute revocation among multi-authority cloud server framework. Where which explores secured access controlling and attribute revocations which lead by our novel CP-ABE scheme and design an attribute revocation method that can achieve both forward security and backward security.

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.

[3] J. Bethencourt, A. Sahai, and B. Waters, ''Cipher-text- Policy AttributeBasedEncryption,'' 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: Attribute Based 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 of encrypted 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 Annual International 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 21stAnnual 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 International Conference 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, "Cipher-text-policy attribute-based encryption," in Security and Privacy, 2007.SP'07. IEEE Symposium on, (2007), pp. 321-334.

[14] Lin Xin, Xingming Sun, Zhangjie Fu, Liang-Ao Zhang and Jie Xi," Effective and Secure Access Control for Multi-Authority Cloud Storage Systems", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.217-236 http://dx.doi.org/10.14257/ijsia.2016.10.2.20.

[15] J. Hur and D. K. Noh, ―Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, (2011), pp. 1214–1221.

[16] S. Jahid, P.Mittal, and N.Borisov, ―Easier: encryption-based access control in social networks with efficient revocation,‖ in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11). ACM, (2011), pp. 411–415.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

BIOGRAPHY

Mrs.Y Shravani: Pursuing M.Tech, CSE Dept, Pragati Engineering college, Surampalem. She acquired her Bachelor of Computer Science degree in 2014 from Pragati Engineering college, Surampalem.

Mr.S V Ramanamurthy : Currently working as Professor and Dean , CSE Department, Pragati Engineering College, Surampalem. Worked in Software Industry for 32 Years both in India and Abroad in reputed companies like TCS, Australia Post etc., Senior Member of IEEE and Life Member of CSI.

Mr. M Rajakumar: is currently working as an Associate Professor in Department of CSE, Pragati Engineering College. He acquired Bachelor of Technology and Master of Technology [Ph.D] from Jawaharlal Nehru Technical University, Kakinada. He published nearly 8 papers in International Journals. His area of interest includes Network Security and Cryptography.