2nd International Conference on Emerging Trends in Engineering and Management Research (ICETEMR-17)
(IETE) Institution of Electronics and Telecommunication Engineers, Pune, India
28th May 2017, www.conferenceworld.in
ISBN: 978-93-86171-46-7

# "TWO FACTOR (2F) DATA ACCESS ON OPEN GLOOM STORAGE IN NETWORK SECURITY"

**Prof. Swati T. Ghorsad[1], Prof. Thamraj N. Ghorsad[2], Prof. R.V Wasu[3]**

*[1,2]Assistant Professor Department of Computer Science & Engineering*

*Dr. SauKamaltai Gawai Institute of Engineering& Technology, Darapur, Amravati, (India)*

*[3]Professor Department of Electronics & Telecommunication Engineering,*

*V.Y.W.S Polytechnic, Badnera, Amravati, (India)*

## ABSTRACT

*Attribute-based encryption, especially for cipher-text-policy attribute-based encryption, can fulfill the functionality of ne-grained access control in open Gloom storage systems. Since users' attributes may be issued by multiple attribute authorities, multi-authority cipher-text-policy attribute-based encryption is an emerging cryptographic primitive for enforcing attribute-based access control on outsourced data. However, most of the existing multi-authority attribute-based systems are either insecure in attribute-level revocation or lack of efficiency in communication overhead and computation cost. In this paper, we propose an attribute-based access control scheme with two-factor(2F) protection for openGloom storage systems. In our proposed scheme, any user can recover the outsourced data if and only if this user holds sufficient attribute secret keys with respect to the access policy and Endorsement key in regard to the outsourced data. In addition, the proposed scheme enjoys the properties of constant-size cipher-text and small computation cost. Besides supporting the attribute-level revocation, our proposed scheme allows data owner to carry out the user-level revocation.*

***Keywords*: Attribute-based encryption, openGloomstorage, two-factor protection, attribute-level revocation, user-level revocation.**

## INTRODUCTION

Gloom storage is one of the most fundamental services, which enables the data owners to host their data in the Gloom and through Gloom servers to provide the data access to the data consumers (users). However, it is the semi-trusted Gloom service providers (CSPs) that maintain and operate the outsourced data in this storage pattern.To prevent the unauthorized entities from accessing the sensitive data, an intuitional solution is to encrypt data and then upload the encrypted data into the Gloom. In an ABE i.e. Attribute based encryption system, each user is ascribed by a set of descriptive attributes. The user's secret key and cipher-text are associated with an access policy or a set of attributes. Decryption is possible if and only if the attributes of cipher-text or secret key satisfy the access policy. Such an advantage makes ABE simultaneously fulfill the data confidentiality andCoarse-grainedaccess control in Gloom storage systems. However, there remain several challenges to the application of CP-ABE in Gloom-based data access control. On one hand, there is only one attribute authority (AA) in the system responsible for attribute management and key distribution. This precondition cannot satisfy the practical requirements once users' attributes are issued by multiple AAs. On the

ISBN: 978-93-86171-46-7

other hand, in most existing schemes, the size of cipher-text linearly grows with the number of attributes involved in the access policy, which may incur a large communication overhead and computation cost. This will limit the usage of resource-constrained users. Last but not the least; the attribute-level abrogation is very difficult since each attribute is conceivably shared by multiple users. A number of CP-ABE schemes with respect to data access control for multi-authority Gloom storage systems have been proposed. In order to achieve the abrogation functionality, the proposed schemes need secure communication channels to update the attribute secret keys for the non-revoked users. But, Yang et al's DAC-MACS scheme cannot guarantee the backward security in active attack model. The reason is that any revoked user still retrieves his/her ability to decrypt some confidential data as a non-revoked user when he/she intercepts the cipher-text update keys delivered from the involved AA. In some schemes Data Owners are voiceless in the permission abrogation.Our proposed TFDAC-MACS can provide two-factor data encryption protection for multi-authority Gloom storage systems. Each user needs to satisfy two requirements when recovering the outsourced data. One is the attributes of this user satisfy the access policy, and the other is this user has the Endorsement key.

## II. EXPERIMENTAL VIEWS

Two Factor Authentications enable users to secure their logins and transactions. The two-factor system of authentication provides a much greater security shield against phishing and identifies theft. There are many two-factor authentication solutions on the market today, but for thousands of organizations worldwide.

## III. SYSTEM DESIGN

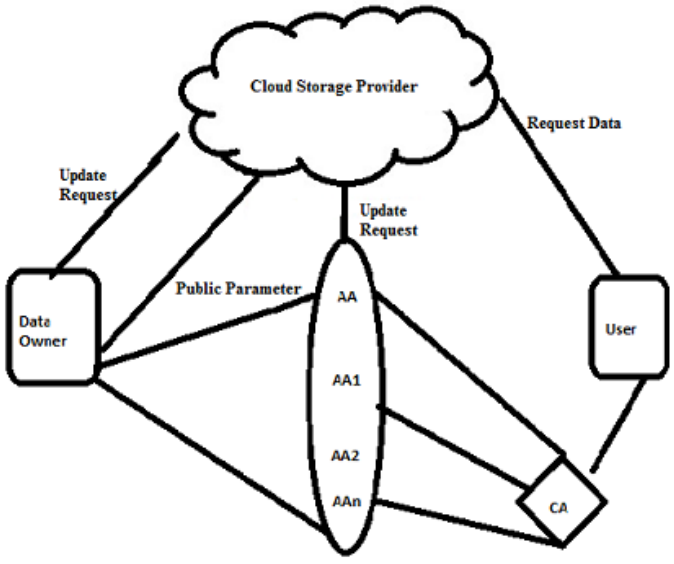


**Fig. System Design**

The CA sets up the system and responses the registration requests from all the AAs and users. However, the CA is not involved into any attribute-related management. Each AA administers a distinct attribute domain and generates a pair of public/secret key for each attribute in this attribute domain. Without any doubt, each attribute is only managed by a single AA. Once receiving the request of attribute registration from a user, the AA

ISBN: 978-93-86171-46-7

generates the corresponding attribute secret keys for this user. Additionally, each AA is responsible to execute the attribute abrogation of users. Before uploading a shared data to the Gloom storage servers, the data owner defines an access policy and encrypts the data under this access policy. After that, the data owner sends the cipher-text and its corresponding access policy to the CSP. Meanwhile, the data owner is responsible for issuing and revoking the user's Endorsement. Each user is labeled with a set of attributes, besides a global unique identifier. In order to obtain the shared data, each user needs to request the attribute secret keys and Endorsement from AAs and data owner, respectively. Any user can download the cipher-text from the CSP. Only the authorized user who has the specific attributes can successfully recover the outsourced data. It becomes obvious that the CSP provides data storage service and enforces the process of cipher-text update. The cipher-text update occurs in the following two cases:

(1) Any of AAs revokes users' one or moreattributes;

(2) The data owner revokes one or more authorized users.

## IV. IMPLEMENTATION

The proposed framework has been implemented using JSP and java class libraries. It acts as a middleware to connect with public Gloom system to store and retrieve files. It uses drivehq.com free storage service to upload and download the file. The following are the modules of the framework.

## V. SYSTEM INITIALIZATION

First, the CA generates some global public parameters for the system, and accepts both the AA registration and user registration. Then, each AAand data owner respectivelygenerates the public parameters and secret information used throughout the execution of system.Then, each AA and data owner respectively generates the public parameters and secret information used throughout the execution of system.

## VI. SECRET KEY AND ENDORSEMENTGENERATION:

When a user submits a request of attribute registration to AA,the AA distributes the corresponding attribute secret keys to this user if his/her certificate is true. When a user submits an Endorsement request to data owner, the data owner generates the corresponding Endorsement key and delivers it to this user.

## VII. DATA ENCRYPTION

For each shared data, the data owner first defines an access policy, and then encrypts the data under this specified access policy. Thereafter, the data owner outsources this cipher-text to the CSP. The encryption operation will use a set of public keys from the involved AAs and the data owner's Endorsement secret key.

## VIII. DATA DECRYPTION

All the users in the system are allowed to query and download any interested cipher-texts from the CSP. A user is able to recover the outsourced data, only if this user holds the sufficient attribute secret keys with respect to access policy and Endorsement key with regard to outsourced data.

ISBN: 978-93-86171-46-7

## IX. ATTRIBUTE-LEVEL ABROGATION

For attribute-level abrogation, the AA who manages the revoked attribute, issues a new public key to this revoked attribute, and generates attribute update keys for non-revoked users and a set of cipher-text update components for CSP. Each non-revoked user who holds the revoked attribute will update the corresponding attribute secret key upon receiving the attribute update key. Based on the set of cipher-text update components, the cipher-texts associated with the revoked attribute will be updated by the CSP.

## X. USER-LEVEL ABROGATION

In order to revoke a user's access privilege, the data owner generates a new Endorsement secret key used for Endorsement; a set of Endorsement update keys for non-revoked users and a set of cipher-text update components for cipher-text update. When receiving the Endorsement update key, eachnon-revoked user updates the Endorsement key and obtains the new version. All the involved cipher-texts will be updated by the CSP based on the set of cipher-text update components.

## XI. CONCLUSION

In this paper, we proposed a revocable multi-authority (CPABE) Cipher text Policy - Attribute Based Encryption scheme that can support efficient attribute abrogation. Then, we constructed an effective data access control scheme for multi-authority Gloom storage systems. The experimental results show the proposed scheme solves the user abrogation and collusion attack problem. 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] M. Armbrust*et al.*, ``A view of Cloud computing," *Common. ACM*, vol. 53, no. 4, pp. 50_58, 2010.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, ``DAC-MACS:Effective data access control for multiauthority Gloom storage systems," *IEEE Trans.Inf. Forensics Security*, vol. 8, no. 11, pp. 1790_1801, Nov. 2013.

[3] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, ``New publicly variabledatabases with efficient updates," *IEEE Trans. Dependable Secure Com-put.*, vol. 12, no. 5, pp. 546_556, Sep. 2015.

[4] K. Ren, C.Wang, and Q.Wang, ``Security challenges for the public Gloom,"*IEEE InternetCompute.*, vol. 16, no. 1, pp. 69_73, Jan./Feb. 2012.

[5] S. Kavitha and S. Subashini, ``A survey on security issues in servicedelivery models of cloud computing," *J. Newt. Compute. Appl.*, vol. 34, no. 1, pp. 1_11, Jan. 2011.

[6] S. Kamara and K. Lauter, ``Cryptographic cloud storage," in *Proc. 1stWorkshop Real-Life Cryptograph. Protocols Standardization (RLCPS)*, vol. 6054. 2010, pp. 136_149.

[7] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, ``New algorithms for secureoutsourcing of modular exponentiations," *IEEE Trans. Parallel Distribute.Syst.*, vol. 25, no. 9, pp. 2386_2396, Sep. 2014.

[8] D. Boneh and M. Franklin, ``Identity-based encryption from the Weilpairing," in *Proc. CRYPTO*, vol. 2139. 2001, pp. 213_229.

[9] A. Sahai and B. Waters, ``Fuzzy identity-based encryption," in *Advances in CryptologyEUROCRYPT* (Lecture Notes in Computer Science),vol. 3494. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457_473.

[10] V. Goyal, O. Pandey, A. Sahai, and Bowater's, ``Attribute-based encryption for _ne-grained access control of encrypted data," in *Proc. 13th ACMConf.Compute. Common.Secure. (CCS)*, Oct./Nov. 2006, pp. 89_98.

[11] J. Hur and D. K. Noh, ``Attribute-based access control with efficientabrogation in data outsourcing systems," *IEEE Trans. Parallel DistributedSyst.*, vol. 22, no. 7, pp. 1214_1221, Nov. 2011.

[12] J. Lai, R. H. Deng, C. Guan, and J.Weng, ``Attribute-based encryption with variable outsourced decryption," *IEEE Trans. Inf. Forensics Security*,vol. 8, no. 8, pp. 1343_1354, Aug. 2013.

[13] K. Yang, X. Jia, and K. Ren, ``Attribute-based _ne-grained access controlwith efficient abrogation in cloud storage systems," in *Proc. 8th ACMSIGSAC Symp. Inf., Compute.Common.Secure. (ASIACCS)*, New York, NY,USA, 2013, pp. 523_528.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, ``Attribute based data sharing withattribute abrogation," in *Proc. 5th ACM Symp. Inf., Compute Common. Secure (ASIACCS)*, New York, NY, USA, 2010, pp. 261_270.

[15] J. Bethencourt, A. Sahai, and B. Waters, ``Ciphertext-policy attributebasedencryption," in *Proc. IEEE Symp.Secure. Privacy (SP)*, May 2007,pp. 321_334.

[16] L. Cheung and C. Newport, ``provably securecipher text policy ABE,"in*Proc. 14th ACM Conf. Compute. Commun.Secur. (CCS)*, Oct. 2007,pp. 456_465.

[17] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan,``CP-ABE with constant-size keys for lightweight devices," *IEEE Trans.Inf. Forensics Security*, vol. 9, no. 5, pp. 763_771, May 2014.

[18] J. Li *et al.*, ``Fine-grained data access control systems with user accountability in cloud computing," in *Proc. IEEE 2nd Int. Conf. Cloud Compute.Technol. Sci. (CloudCom)*, Nov./Dec. 2010, pp. 89_96.

[19] R. Ostrovsky, A. Sahai, and B. Waters, ``Attribute-based encryption with on-monotonic access structures," in *Proc. 14th ACM Conf. Compute .Commuication. Secure.(CCS)*, New York, NY, USA, 2007, pp. 195_203.

[20] B. Waters, ``Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. 14th Int. Conf. Pract.Theory Public Key Cryptograph. (PKC)*, vol. 6571.2011, pp. 321_334.

[21] A. Lewko and Bowater's, ``New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Advances in Cryptology*, vol. 7417. Berlin, Heidelberg: Springer-Verilog, 2012,pp. 180_198.

[22] M. Chase, ``Multi-authority attribute based encryption," in *Proc. 4th IACRTheoryCryptograph. Conf. (TCC)*, vol. 4392. Feb. 2007, pp. 515_534