International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Threshold based Multi-Authority Access Control System in Public Cloud Storage – A Review

Sangita V. Gajare[1], Namdev M. Sawant[2]
[1]*Student, Dept. of Computer Science and Engineering, SKN Sinhgad College of Engineering, Solapur, India*
[2]*Professor, Dept. of Computer Science and Engineering, SKN Sinhgad College of Engineering, Solapur, India*

***Abstract*: Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owner's direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Subsequently, some multi-authority schemes are proposed, in which multiple authorities separately maintain disjoint attribute subsets. However, the single-point bottleneck problem remains unsolved. It is proposed to conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t, n) threshold secret sharing, the master key can be shared among multiple authorities and a legal user can generate his/her secret key by interacting with any authorities. Security and performance analysis will be made when less than t authorities are compromised, also when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.**

***Keywords*: CP-ABE, (t; n) threshold secret sharing, multi-authority, public cloud storage, access control**

1. Introduction

From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Sales force, etc...With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. In earlier cloud computing environment there are lots of data security issues are present like how we can provide the better security to data using new algorithms, how client will communicate with database system and data owner, how authorities will provide the final key to end user, how CA can securely communicate with all parties, and suppose in case any authority will get fail then how we can reduce the single-point bottleneck on both security and performance. These are the issues in current system. We have to investigate the all the obstacles in previous systems and provide a smooth and scalable solution for data security.

This paper conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, in which multiple authorities jointly manage a uniform attribute set. In this system, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that this system is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system.

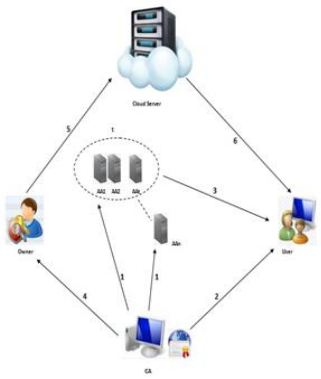

Fig. 1. Framework and Basic Protocol Flow

The basic protocol flow of threshold based multi-authority system is as follows AA registers to CA to gain (aid;aid:cert).(2) User registers to CA to gain (uid; uid:cert).(3) User gains his/her SK from any t out of n AAs.(4) Owners gain PK from CA.(5) Owners upload (CT) to the cloud server.(6) Users download (CT) from the cloud server.

In robust multi-authority public cloud storage systems, there exist five entities:

A. Certificate authority (CA)

In System CA is responsible for the construction of the

system .by setting up system parameters and attribute public key of each attribute in the whole attribute set.CA accepts users and AA's registration requests by assigning a unique uid for each legal user and a unique aid for each AA. CA also decides the parameter t about the threshold of AAs that are involved in user's secret key generation for each time.

B. Attribute authorities (AAs)

Focus on the task of attribute management and key generation. AAs can be the administrators of the application system. All AAs jointly manage the whole attribute set.

C. Data owner

Data owner encrypts his/her file & defines access policy about who can get access to his/her data. Each owner encrypts his/her data with asymmetric encryption algorithm like AES & DES.

D. Data consumer (User)

The data consumer (User) is assigned with a global user identity uid from CA, applies for user secret keys from AAs with user identification. The user can freely get the cipher texts that he/she is interested in from the cloud server. He/ She can decrypt the encrypted data if & only if his/her attribute set satisfied the access policy hidden inside the encrypted data.

E. Cloud server

The cloud server provides a platform for owners storing and sharing their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by user.

2. Literature review

A. Fuzzy identity-based encryption

A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a cipher text encrypted with an identity, ω', if and only if the identities ω and ω' are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, they show that Fuzzy-IBE can be used for a type of application that has termed as "attribute-based encryption" [4].

B. Expressive key policy attribute based encryption with constant-size cipher texts

This paper proposes the first key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant ciphertext size. Towards achieving this goal, it show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP- ABE systems in the selective set model. Then describe a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size cipher- texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

C. Ciphertext-policy attribute-based encryption [9]

In this paper, the author has introduced system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. by using this techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our 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 our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, they provide an implementation of our system and give performance measurements. Author created a system for Ciphertext-Policy Attribute Based Encryption. This system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt.

D. DAC-MACS: Effective data access control for multi-authority cloud storage systems

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to data access control for multi-authority cloud storage systems, due to the in efficiency of decryption and revocation. Author has proposed an effective data access control scheme for multi-authority cloud storage systems, DAC-MACS. They also constructed a new multi-authority CP-ABE scheme, in which the main computation of decryption is outsourced to the server. Also designed an efficient attribute revocation method that can achieve both forward security and backward security. However, in DAC-MACS, all the users' secrets uid are revealed to each AA. If the

revoked user corrupts any AA and some non-revoked users, it can derive the key update key easily and apply it to update its secret key.

E. Attributed-based access control for multi-authority systems in cloud storage

In this paper, they defined a new access control framework for multi-authority systems in cloud storage and proposed an efficient and secure multi-authority access control scheme. They first designed an efficient multi-authority CP-ABE scheme that does not require a global authority and can support any LSSS access structure. Then, they proved that our multi-authority CP-ABE scheme is provably secure in the random oracle model. They also proposed a new technique to solve the attribute revocation problem in multi-authority CP-ABE systems. The analysis and simulation results showed that this proposed access control scheme is scalable and efficient.

3. Conclusion

Threshold multi authority control system (TMACS) provides a fine-grained and non-interactive access control mechanism of encrypted data and has great potential applications in many fields. It expound the emergence and development of ABE schemes. TMACS pay attention to main research directions of ABE, including multi-authority, use/attribute revocation, accountability, and proxy re-encryption. It also construct a hybrid scheme that is more suitable for the real scenario, in which attributes come from different authority sets and multiple authorities in an authority-set jointly maintain a subset of the whole attribute set. This enhanced scheme addresses not only attributes coming from different authorities but also security and system-level robustness.

References

[1] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2010, pp. 62-91.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in Proceedings of the13th ACM conference on Computer and communications security. ACM, 2006.

[3] N. Attrapadung, B. Libert, and E. Panaeu, "Expressive key policy attribute-based encryption with constant-size ciphertexts," in Proceedings of the 14thInternational Conference on Practice and Theory in Public Key Cryptography.Springer, 2011, pp. 90-108.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-basedencryption," in Proceedings of *IEEE Symposium on Security and Privacy*. IEEE, 2007, pp. 321-334.

[5] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2011, pp. 53-70.

[6] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy at-tribute based encryption," in Proceedings of the 35th International Colloquiumon Automata, Languages and Programming. Springer, 2008, pp. 579-591.

[7] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proceedings of the 14th European Symposium on Research in Computer Security. Springer, 2009, pp. 587-604.

[8] T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proceedings of The 32nd *IEEE International Conference on Computer Communications*. IEEE, 2013, pp. 2625-2633.

[9] J.Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, 2013.

[10] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," *IEEE Transactions on Multimedia*, vol. 15, no. 4, pp. 778-788, 2013.