International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

An Efficient Verifiable Multi-Authority Secret Access control scheme in Cloud Storage

M.Sreelakshmi & P.Gangadhara

[1]M.Tech, Dept of CSE,Shri Shirdi Sai Institute of Science and Engineering, Affiliated to JNTUA,Ananthapuramu, AP, India .
sree.lakshmi4u9@gmail.com

[2]AssistantProfessor, Dept of CSE, Shri Shirdi Sai Institute of Science and Engineering, Affiliated to JNTUA,Ananthapuramu,AP, India.
gangadhara115208@gmail.com

Abstract: *Data access control is an efficient way to provide the data security in the cloud but due to data outsourcing over untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Despite many advantages of cloud storage, there still remain various challenging obstacles, among which, privacy and security of users' data have become major issues, especially in public cloud storage Attribute-based Encryption (ABE) technique is regarded as a most trustworthy cryptographic conducting tool to guarantee data owner's direct control on their data in public cloud storage. The previous ABE schemes involve only one authority to maintain the complete attribute set, which can bring a single-point hindrance on both security and performance. Paper proposed the design, an expressive, efficient and revocable decentralized manner data access control scheme for multi-authority cloud storage systems, where there are multiple authorities exist and every authority is able to issue attributes independently.*

I. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures. Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern. To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user. Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over data and provide a fine -grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attribute based Encryption (KP-ABE) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in cipher texts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data whenever its attributes match the access policies. Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud environment. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme is introduced.

II. RELATED WORK

1) "Cryptographic cloud storage,"
AUTHORS: S. Kamara and K. Lauter,
The predominant pursuits of this technique a secure multi-owner data sharing theme. It implies that any person in the cluster will firmly proportion facts with others with the aid of the sector company honest cloud. This theme is prepared to assist dynamic groups. Expeditiously, especially, new granted customers will directly rewrite records documents uploaded before their participation while not contacting with information house owners. User revocation can be really carried out thru a completely particular revocation list at the same time as now not trade the key. Keys of the last users the size and computation overhead of coding are constant and impartial with the quantity of revoked customers. We have a tendency to present a comfy and privacy-preserving access management to customers, that assure any member at some point of a cluster to anonymously make use of the cloud aid. Moreover, the real identities of knowledge residence owners could be disclosed with the aid of the cluster supervisor as soon as disputes occur. We provide rigorous safety evaluation, and perform extensive simulations to illustrate the potency of our subject matter in phrases of garage and computation overhead. Cloud computing offers a value powerful and not pricey resolution for sharing cluster aid among cloud users sharing records AN rather in a very multi-owner manner while holding statistics and identity privacy from an untrusted cloud remains a tough issue, because of the frequent modification of the membership.

2) "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,"
AUTHORS: A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters

In this paper, we present two completely comfortable functional encryption schemes. Our first end result is a fully cozy attribute-primarily based encryption (ABE) scheme. Previous constructions of ABE have been most effective established to be selectively secure. We obtain full protection by way of adapting the dual system encryption technique these days added by means of Waters and previously leveraged to achieve completely comfortable IBE and HIBE structures. The number one mission in making use of dual machine encryption to ABE is the richer shape of keys and ciphertexts. In an IBE or HIBE machine, keys and ciphertexts are both related to the equal kind of simple item: identities. In an ABE device, keys and ciphertexts are related to extra complicated gadgets: attributes and access formulation. We use a singular facts-theoretic argument to conform the dual system encryption methodology to the more complex structure of ABE systems. We construct our gadget in composite order bilinear corporations, wherein the order is a fabricated from three primes. We prove the safety of our machine from three static assumptions. Our ABE scheme supports arbitrary monotone get admission to formulas. Our 2nd result is a completely secure (attribute-hiding) predicate encryption (PE) scheme for inner-product predicates. As for ABE, preceding buildings of such schemes have been best verified to be selectively cozy. Security is verified beneath a non-interactive assumption whose size does now not depend upon the range of queries. The scheme is comparably efficient to present selectively comfy schemes. We additionally gift a completely comfortable hierarchical PE scheme below the identical assumption. The key approach used to achieve these results is an complicated combination of the twin device encryption method.

3) "Secure threshold multiauthority attribute based encryption without a central authority,"
AUTHORS: H. Lin, Z. Cao, X. Liang, and J. Shao

An attribute based encryption scheme (ABE) is a cryptographic primitive in which each user is diagnosed by using a hard and fast of attributes, and a few function of these attributes is used to decide the potential to decrypt each ciphertext. Chase proposed the first multi authority ABE scheme which requires a fully relied on principal authority who has the capability to decrypt every ciphertext inside the machine. This imperative authority might endanger the whole device if it's far corrupted. This paper affords a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a government for the first time. An encrypter can encrypt a message such that a person should only decrypt if he has at the least dk of the given attributes approximately the message for as a minimum t+1,t⩽n/2 sincere authorities of all of the n characteristic government in the proposed scheme. This paper considers a stronger adversary version inside the experience that the corrupted government are allowed to distribute wrong secret keys to the customers. The protection proof is based totally on the secrecy of the underlying dispensed key technology protocol and joint 0 secret sharing protocol and the standard decisional bilinear Diffie–Hellman assumption. The proposed MA-FIBE can be prolonged to the threshold multi authority characteristic based encryption (MA-ABE) scheme, and both key coverage based and ciphertext coverage primarily based MA-ABE schemes without a central authority are provided in this paper. Moreover, several different extensions, inclusive of a proactive massive universe MA-ABE scheme, are also provided in this paper.

III. EXISTING SYSTEM

In KP-ABE schemes, decrypt keys are associated with access structures while ciphertexts are only labeled with special attribute sets. On the contrary, in CP-ABE schemes, data owners can define an access policy for each file based on users' attributes, which can guarantee owners' more direct control over their data. Therefore, compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage.

DISADVANTAGES OF EXISTING SYSTEM:

In existing CP-ABE schemes there is only one authority responsible for attribute management and key distribution. This only-one-authority scenario can bring a single-point bottleneck on both security and performance. Once the authority is compromised, an adversary can easily obtain the only-one-authority's master key, then he/she can generate private keys of any attribute subset to decrypt the specific encrypted data.

Moreover, once the only-one-authority is crashed, the system completely cannot work well. Although some multi-authority CP-ABE schemes have been proposed, they still cannot deal with the problem of single-point bottleneck on both security and performance mentioned above. The adversary can obtain private keys of specific attributes by compromising specific one or more authorities.

Crash or offline of a specific authority will make that private keys of all attributes in attribute subset maintained by this authority cannot be generated and distributed, which will still influence the whole system's effective operation.

IV. PROPOSED SYSTEM

- ❖ In this paper, we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, TMACS, to overcome the single-point bottleneck on both security and performance in most existing schemes.

- ❖ In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities.

- In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t; n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone.

ADVANTAGES OF PROPOSED SYSTEM:

- TMACS 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.
- By introducing the combining of (t; n) threshold secret sharing and multi-authority CP-ABE scheme, we propose and realize a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set.
- Furthermore, by efficiently combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

SYSTEM ARCHITECTURE

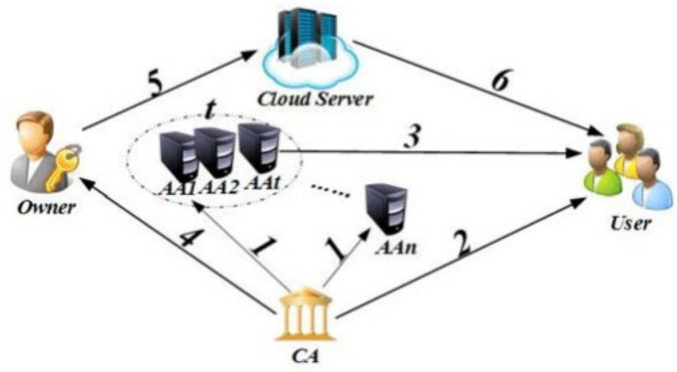

Fig. 1. Framework and basic protocol flow

IMPLEMENTATION

TMACS

The TMACS multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In TMACS, a global certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users. However, CA is not involved in AAs' master key sharing and users' secret key generation, which avoids CA becoming the security vulnerability and performance bottleneck. Design of TMACS is reusing of the master key shared among multiple attribute authorities.

In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value. Similarly, in CP-ABE schemes, the only-one-authority knows the master key and uses it to generate each user's secret key according to a specific attribute set. In this case, if the AA is compromised by an adversary, it will become the security vulnerability. To avoid this, by means of (t;n) threshold secret sharing, the master key cannot be individually reconstructed and gained by any entity in TMACS.hat the master key a is actually secure. By this means, we solve the problem of reusing of the master key.

Data Access Control Scheme:

We propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t;n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t;n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone. TMACS 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. To the best of our knowledge, this paper is the first try to address the singlepoint bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

Certificate authority:

The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs' 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 users' secret key generation for each time. However, CA is not involved in AAs' master key sharing and users' secret key generation. Therefore, for example, CA can be government organizations or enterprise departments which are responsible for the registration. Certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users.

Attribute authorities:

The attribute authorities focus on the task of attribute management and key generation. Besides, AAs take part of the responsibility to construct the system, and they can be the administrators or the managers of the application system. Different from other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set; however, any one of AAs cannot assign users' secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. By this means, each AA can gain a piece of master key share as its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it comes to generate users' secret key, each AA only should generate its corresponding secret key independently. The master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value.

VI. CONCLUSION AND FUTURE WORK

In this paper, a new threshold multi-authority CP-ABE get right of entry to manipulate scheme TMACS is proposed. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key.

TMACS 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. This scheme avoids a single-point bottle neck on both security and performance

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Instit. Standards Technol., vol. 53, no. 6, p. 50, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. 14th Financial Cryptography Data Security, 2010, pp. 136–149.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan.-Feb. 2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 457–473.

[5] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. 14th ACM Conf. Comput. Commun. Security, 2014, pp. 195–203.

[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 62–91.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[8] N. Attrapadung, B. Libert, and E. Panafieu, “Expressive keypolicy attribute-based encryption with constant-size ciphertexts,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 90–108.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute- based encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[10] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 53–70.