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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Novel Verifiable Multi-Authority Secret Sharing Method in Cloud Storage

V.Aravind Kumar[1], M.Dharani Kumar [2]

M. Tech Student, Dept of CSE, P.V.K.K Institute of Technology, Ananthapuramu, Affiliated to JNTUA, India[1]

Assistant Professor, Dept of CSE, P.V.K.K Institute of Technology, Ananthapuramu, Affiliated to JNTUA, India[2]

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. 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 ke y 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

DOI: 10.15680/IJIRCCE.2017. 0506111

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

Wei Li, et al. [1] in access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multi -authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-authority scheme with this scheme, construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Hong, et al. [2] demonstrated that, with the component CUK a revoked user can transform the newly encrypted ciphertext to a previous version, which can be further decrypted with his/her revoked old-version secret keys.

Jung, et al. [3] proposed a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. The proposed scheme was able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The scheme was tolerant against authority compromise, and compromising of up to (N −2) authorities did not bring the whole system down. Author provides detailed about security and feasibility of the scheme. Also implements the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

Yang, et al. [4] proposed a revocable multi -authority CP-ABE scheme, where efficient and secures revocation method introduced to solve the attribute revocation problem in the system. Attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security and forward security. This scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority no t the server. Even if the server is not semi-trusted in some scenarios, this scheme can still guarantee the backward security. Then, apply
proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

Liu, et al. [5] to achieve secure data sharing for dynamic groups in the cloud, combined the group signature and dynamic broadcast encryption techniques. This scheme describes the details of Mona including system initialization, user registration, user revocation, file generation, file deletion, file access and traceability. Also this scheme provides security to Mona in terms of access control, data confidentiality, anonymity and traceability.

III. EXISTING SYSTEM

Attribute-based totally Encryption (ABE) is appeared as one of the maximum suitable schemes to conduct information get entry to manage in public clouds for it may guarantee facts owners' direct manage over their information and offer a fine-grained get right of entry to manipulate provider. Till now, there are many ABE schemes proposed, which can be divided into categories: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based totally Encryption (CP-ABE).
In KP-ABE schemes, decrypt keys are associated with get entry to structures at the same time as ciphertexts are best labeled with special attribute units. On the opposite, in CP-ABE schemes, facts proprietors can outline an get admission to policy for each report based on customers' attributes, that can assure proprietors' greater direct manipulate over their information. Therefore, in comparison with KP-ABE, CP-ABE is a desired desire for designing get admission to control for public cloud storage.

DISADVANTAGES OF EXISTING SYSTEM:

In maximum existing CP-ABE schemes there's most effective one authority responsible for characteristic control and key distribution. This most effective-one-authority situation can bring a unmarried-factor bottleneck on each safety and performance.

Once the authority is compromised, an adversary can effortlessly attain the only-one-authority's master key, then he/she will be able to generate personal keys of any attribute subset to decrypt the precise encrypted records.

Moreover, as soon as the simplest-one-authority is crashed, the device absolutely cannot paintings well.

Although some multi-authority CP-ABE schemes have been proposed, they nevertheless can't address the trouble of unmarried-factor bottleneck on each security and performance noted above.

The adversary can reap personal keys of precise attributes by compromising specific one or extra authorities.

IV. PROPOSED SYSTEM

In this paper, we suggest a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to address the unmarried-point bottleneck on each safety and overall performance in maximum current schemes.

In TMACS, a couple of authorities mutually control the whole characteristic set but no person has full control of any precise characteristic. Since in CP-ABE schemes, there's usually a secret key (SK) used to generate characteristic non-public keys, we introduce (t; n) threshold secret sharing into our scheme to proportion the secret key amongst authorities.

In TMACS, we redefine the name of the game key inside the conventional CP-ABE schemes as grasp key. The introduction of (t; n) threshold mystery sharing ensures that the grasp key cannot be received by means of any authority alone.

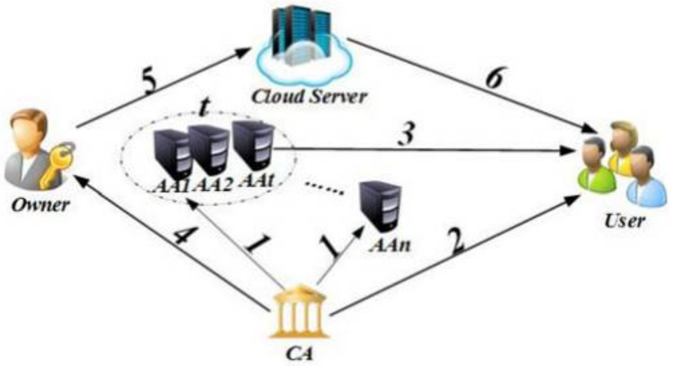
ADVANTAGES OF PROPOSED SYSTEM:

TMACS isn't best verifiable comfortable whilst less than t government are compromised, however additionally strong while no less than t government are alive within the machine.

To the great of our knowledge, this paper is the primary try to address the singlepoint bottleneck on both protection and performance in CPABE get admission to manage schemes in public cloud garage.

In present access manipulate structures for public cloud storage, there brings a single-point bottleneck on both protection and overall performance towards the single authority for any precise characteristic.

SYSTEM ARCHITECTURE



IMPLEMENTATION

TMACS

The TMACS a couple of authorities jointly control the whole attribute set but nobody has full manage of any precise attribute. In TMACS, a worldwide certificates authority is answerable for the development of the machine, which avoids the greater overhead caused by AAs' negotiation of system parameters. CA is also accountable for the registration of users, which avoids AAs synchronized maintaining a listing of customers. However, CA isn't always involved in AAs' grasp key sharing and users' secret key generation, which avoids CA turning into the security vulnerability and overall performance bottleneck. Design of TMACS is reusing of the grasp key shared among a couple of attribute government. In conventional (t;n) threshold secret sharing, as soon as the secret is reconstructed among multiple members, a person can truly benefit its value. Similarly, in CP-ABE schemes, the best-one-authority knows the grasp key and makes use of it to generate every person's secret key according to a specific characteristic set. In this situation, if the AA is compromised with the aid of an adversary, it turns into the security vulnerability. To avoid this, with the aid of (t;n) threshold secret sharing, the master key cannot be individually reconstructed and gained by way of 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 recommend a strong and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the unmarried-point bottleneck on both safety and performance in most existing schemes. In TMACS, multiple authorities together manipulate the entire attribute set but no one has full control of any unique characteristic. Since in CP-ABE schemes, there's always a secret key (SK) used to generate characteristic non-public keys, we introduce (t;n) threshold mystery sharing into our scheme to percentage the secret key among authorities. In TMACS, we redefine the name of the game key within the traditional CP-ABE schemes as master key. The advent of (t;n) threshold secret sharing ensures that the grasp key cannot be received by any authority by myself. TMACS isn't always only verifiable cozy whilst less than t authorities are compromised, however also strong while no less than t government are alive within the device. To the pleasant of our expertise, this paper is the first try to deal with the single point bottleneck on both safety and overall performance in CPABE get right of entry to control schemes in public cloud storage.

Certificate authority:
The certificate authority is a international depended on entity within the machine this is chargeable for the development of the machine via putting in system parameters and attribute public key (PK) of every characteristic inside the whole characteristic set. CA accepts users and AAs' registration requests by using assigning a unique uid for each criminal consumer and a unique aid for every AA. CA additionally makes a decision the parameter t about the threshold of AAs which are worried in users' mystery key technology for each time. However, CA is not concerned in AAs' master key sharing and users' secret key technology. Therefore, as an example, CA can be authorities corporations or employer departments that are responsible for the registration. Certificate authority is answerable for the development of the system, which avoids the extra overhead because of AAs' negotiation of device parameters. CA is likewise accountable for the registration of customers, which avoids AAs synchronized retaining a listing of customers.

Attribute authorities:
The attribute authorities recognition at the challenge of characteristic management and key generation. Besides, AAs take a part of the responsibility to assemble the device, and they can be the directors or the managers of the utility device. Different from other present multi-authority CP-ABE systems, all AAs mutually manipulate the complete attribute set; however, any person of AAs cannot assign users' mystery keys by myself for the grasp secret's shared by using all AAs. All AAs cooperate with each other to proportion the master key. By this indicates, every AA can gain a chunk of master key shareas its non-public key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it involves generate users' secret key, each AA only ought to generate its

corresponding mystery key independently. The master key shared amongst a couple of characteristic government. In conventional (t;n) threshold secret sharing, once the key's reconstructed among multiple participants, someone can simply gain its price.

VI. CONCLUSION AND FUTURE WORK

In this paper, we advocate a new threshold multi-authority CP-ABE get right of entry to manipulate scheme, named TMACS, in public cloud storage, wherein all AAs together control the complete characteristic set and share the grasp key a. Taking gain of (t; n) threshold mystery sharing, through interacting with any t AAs, a felony user can generate his/her secret key. Thus, TMACS avoids someone AA being a single-point bottleneck on both safety and performance. The analysis outcomes show that our get entry to control scheme is strong and comfortable. We can without difficulty locate appropriate values of (t; n) to make TMACS no longer handiest at ease when much less than t government are compromised, but also robust when no much less than t government are alive within the gadget. Furthermore, primarily based on efficaciously combining the conventional multi-authority scheme with TMACS, we also construct a hybrid scheme this is greater appropriate for the actual state of affairs, wherein attributes come from extraordinary authority-units and a couple of authorities in an authority-set at the same time hold a subset of the whole characteristic set. This improved scheme addresses not handiest attributes coming from different authorities however also safety and machine-degree robustness. How to reasonably pick out the values of (t; n) in concept and layout optimized interplay protocols may be addressed in our future work.

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.

DOI: 10.15680/IJIRCCE.2017. 0506111