International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

DECISIVE RE-ENCRYPTION STRATEGY FOR EFFECTUAL ATTRIBUTE BASED APPROACH IN THE CLOUD COMPUTING

Peddi Tharun Reddy[1], Narsimha Banothu[2]

[1]pursuing M.Tech (CSE), [2]working as an Associate Professor,
Dept. Of Computer Science And Engineering,
Holymary Institute of Technology & Science (HITS), Ranga Reddy(India)

ABSTRACT

Distributed storage get to control is essential for the security of outsourced information, where Attribute-based Encryption (ABE) is viewed as a standout amongst the most encouraging innovations. Flow inquires about principally concentrate on decentralized ABE, a variation of multi-expert ABE plot, on the grounds that traditional ABE plans rely on upon a solitary expert to issue mystery keys for all of clients, which is exceptionally unfeasible in a huge scale cloud. A decentralized ABE plan ought not depend on a focal specialist furthermore, can take out the requirement for synergistic calculation. In any case, developing such an effective and functional decentralized ABE conspire remains a testing research issue. In this think about, we outline another decentralized ciphertext-strategy attribute based encryption get to control conspire for distributed storage frameworks. Firstly, our plan dosage not requires any focal expert and worldwide coordination among various specialists. At that point, it bolsters any LSSS get to structure and along these lines can encode information in wording of any boolean equation. What's more, we likewise use Proxy Reencryption system to conquer the client repudiation issue in decentralized ABE plans, in this way making our plan more down to earth. Our security and execution examination illustrate the exhibited plan's security quality and effectiveness in wording of adaptability and calculation.

I. INTRODUCTION

Cloud computing has been widely concerned, and continually developed [1–3]. Cloud storage is an important service paradigm of cloud computing, by which data owners can host their data to the cloud at any time, in any place. It has attracted much attention and interest from both academia and industry. However, it also has at least three challenges that must be addressed before widely adopted. First of all, data security much be guaranteed. When data are stored and processed in public clouds, where commercial cloud storage service providers may give data access to unauthorized users for profit gain. Secondly, since an access structure as a building block is employed to control different users from accessing the shared resource in the cloud, it is important that the access structure can express a more complicated access policy. Last but not least, a practical cloud storage system must provide user revocation mechanism. The data owner can revoke any customer from accessing the shared resource again, if the purchased service is expired or the customer has malicious behavior.

To address the aforementioned problems, various techniques have been proposed. ABE as a special primitive is regarded as one of the most suitable technologies for access control in cloud storage systems. There are two forms of ABE [4]: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CPABE-CPABE). Especially, CP-ABE provides a scalable mechanism of encrypting data such that an encrypter specifies a set of attributes that a decryptor need to possess them to decrypt the ciphertext. This mechanism effectively eliminates the dependence on the cloud to prevent unauthorized access.

In most existing ABE schemes [4–7], there is only one authority which is responsible to issue secret keys for every user in a system. However, in many applications, it is necessary for a system that there exist multiple authorities simultaneously, each of which manages the attributes within its own domain or organization independently. For instance, a party might want to share medical data only with a user who has the attribute of ”Doctor” issued by a medical organization and the attribute ”Researcher” issued by the administrators of a clinical trial. Another benefit of multi-authorities in a system is that it can protect users’ privacy to a certain extent. Since each authority only issues secret key components which it is in charge of, even if the authority knows parts of the user’s attributes, it is not enough to figure out the user’s identity.

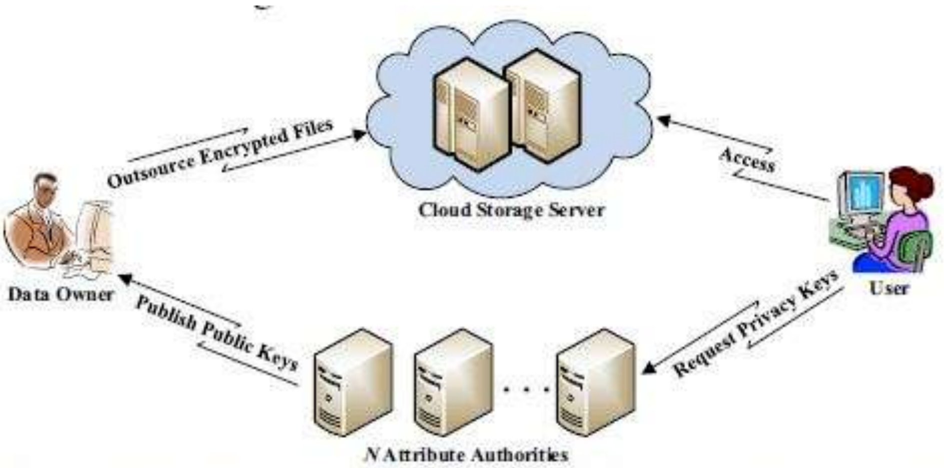

Fig. 1. System model of our decentralized access control scheme

Due to at least the above two reasons, multi-authority ABE has attracted a lot of attention in the research community. The first work to explicitly propose a multi-authority KPABE scheme was by Chase [8]. In the scheme, one of the main challenges is to resist the collusion attack of malicious users. Prior single-authority ABE schemes achieved collusion resistance when the system authority tied together different components of a user’s private key by randomizing it. However, if the multiple authorities can work independently, the scheme would be subject to this attack. Chase [8] overcame this problem by introducing a Global Identifier (GID). All the user’s secret keys from different authorities must be tied to his GID. In order to make the ciphertext be independent of the user’s GID, a central authority must be established to compute a special secret key for the user using his secret key and the other authorities’ secret keys. However, the central authority is too powerful and it can become a vulnerable point for security attacks and the performance bottleneck for large scale systems. The same problem also exists in [9–11]. In subsequent work, some other multi-authority ABE schemes [12, 13] were proposed to remove any central authority. But they require collaborations among multiple authorities to conduct the system, which results in the heavy communication cost and the lack of scalability in large scale systems. Recently, Lekwo and Waters proposed a new multi-authority ABE scheme named decentralizing CP-ABE scheme [14].

II. ATTRIBUTE-BASED ENCRYPTION

Attribute Based Encryption (ABE) was along these lines proposed to have versatile get to control of encoded data utilizing access courses of action and acknowledged attributes associated for private keys and figure messages independently. Attribute based encryption, a substantial bit of ABE systems are produced with pairings while the figuring cost in the translating stage creates close by the measure of the passage approach. ABEs are typically too much expensive for resource constrained front-end customers, which gigantically ruins its valuable notoriety. Encryption requires the data sender to scramble an extra sporadic message and enlist a checksum regard related to two messages; unscrambling requires the untouchable organization to execute the concealed translating computation twice and the data authority to affirm the outsourced estimation with respect to the encoded messages.

III. ADVANCED ENCRYPTION STANDARD

Its miles a web device to encrypt and decrypt text using AES encryption algorithm. You could pick 128, 192 or 256-bit long key length for encryption and decryption. The result of the procedure is downloadable in a textual content file. If you want to encrypt a text put it in the white text region above, set the key of the encryption then push the Encrypt button. The end result of the encryption will seem in base64 encoded to prevent person encoding issues. If you need to decrypt a textual content be sure it is in base64 encoded and is encrypted with AES algorithm! Positioned the encrypted textual content within the white textual content region, set the important thing and push the Decrypt button. whilst you need to encrypt a private text right into a decrypt able format, as an example while you need to ship sensitive data in electronic mail. The decryption of the encrypted textual content it is possible handiest in case you recognise the proper password.AES (acronym of advanced Encryption well-known) is a symmetric encryption algorithm. The set of rules changed into evolved by using Belgian cryptographer Joan Diemen and Vincent Rijmen. AES became designed to be efficient in each hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

III. RELATED WORK

We present a novel decentralized ciphertext policy attribute-based encryption access control scheme for cloud storage systems. In our scheme, multiple authorities can work independently without any central authority and coordination among them. In order to resist the collusion attack from the users, the GID is employed to tie all the user’s secret keys issued from different authorities, such that the scheme is any number resilient, as we will discuss in detail in Section III. Moveover, our scheme can support any LSSS access structure [7, 17] and so the access policy will be very expressive, which is important especially under the complicated context. With respect to the user revocation, we utilize Proxy Re-encryption technique [18] to improve the efficiency of operations without reducing the security of the access control system. More specifically, we make full use of the cloud to distribute the legitimate users' update keys and be imposed most burden of re-encrypting ciphertext. In contrast to single-authority ABE schemes, this is especially important for multi-authority ABE schemes, because users' attribute keys may come from many different authorities, and the mechanism makes the legitimate users obtaining update keys only in the cloud, thus alleviating the communication overhead.

IV. OBJECTIVE

The utilization of these capacities makes the re-encryption plan to lose the Multi-utilize highlight, which is required as portrayed in this paper. That is, previously a Re-encryption Key produced by rkgen pke () is utilized to re-scramble, no further re-encryptions should be possible to that encoded protest. Notwithstanding, for the motivations behind approval in this paper, this sort of re-encryption just should be done to re-scramble the ensured question under the asking for client open key. What's more, this is done in the last reencryption, which is the one that outcomes in the information being encoded under the client open key. Therefore, re-encryption keys created with the first rkgen() capacity ought to even now be connected for re-encryptions along the approval way, aside from the one influencing the client, which is the last reencryption.

With this approach, the information proprietor utilizes people in general key of the client when characterizing rules in the approval demonstrate. Upon a demand, the information question is re-encoded under the asking for client open key. This client can then unscramble the information by utilizing the comparing private key. Consequently, enter administration brings about overseeing open and private key sets of PKE, which should be possible by method for usually utilized and standard PKI arrangements.

V. PROBLEM DEFINITION

Distributed storage is a vital administration worldview of distributed computing, by which information proprietors can have their information to the cloud whenever, in wherever. It has pulled in much consideration and enthusiasm from both scholarly community and industry. Nonetheless, it additionally has no less than three difficulties that must be tended to before broadly embraced. As a matter of first importance, information security much be ensured. At the point when information are put away and handled out in the open mists, where business distributed storage specialist organizations may give information access to unapproved clients revenue driven pick up.

Furthermore, since a get to structure as a building piece is utilized to control diverse clients from getting to the mutual asset in the cloud, it is essential that the get to structure can express a more entangled get to approach. To wrap things up, a useful distributed storage framework must give client disavowal instrument. The information proprietor can repudiate any client from getting to the mutual asset once more, if the obtained administration is terminated or the client has malignant conduct..

VI. PROPOSED SOLUTION

In this paper, we bring outsourcing calculation into IBE disavowal, and formalize the security meaning of outsourced revocable IBE for the essential time to the pleasant of our aptitude. We underwrite a plan to offload all the key period related operations all through key-issuing and key upgrade, leaving least complex a consistent scope of straightforward operations for PKG and qualified clients to complete provincially. In our plan, as with the motivation, we perceive repudiation by means of redesigning the private keys of the unrevoked clients. however as opposed to that canvases which unimportantly links era with recognizable proof for key innovation/upgrade and requires to re-issue the entire private key for unrevoked clients, we propose a particular intrigue safe key issuing technique: we contract a half and half individual key for every buyer, in which an AND door is worried to interface and bound two sub-segments, to be specific the ID segment and the time segment. At to start with, client is fit for acquire the distinguishing proof issue and a default time component (i.e., for present day term) from PKG as his/her non-open key in key-issuing. A short time later, while in transit to hold unscramble potential, unrevoked clients' needs to occasionally ask for on key substitute for time component to a recently brought element named Key redesign Cloud supplier guarantor. Contrasted and the past compositions, our plan does no longer need to re-inconvenience the whole non-open keys, however essentially need to upgrade a lightweight issue of it at a specific element. We additionally indicate that 1) with the guide of owner, customer craves now not to contact with PKG in key-redesign, in various expressions, PKG is allowed to be disconnected subsequent to sending the renouncement leaning to. 2) No calm channel or client validation is required all through key-supplant amongst individual and data owner.

VII. ADVANTAGES

1. Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.
2. ABE with algorithmic specification reduces the overhead of decryption mechanisms that are mostly felt by the resource constrained systems.
3. Since the algorithmic specification is to be specified by the destination itself here the need of the third party because the use of third party may sometimes lead to data leakage.

VIII. CONCLUSION

In this paper, we have displayed a novel decentralized CPABE get to control conspire for distributed storage frameworks, which is both effective and secure. Our plan does not require any focal expert and coordination among different specialists, therefore wiping out the weight of substantial correspondence and the deferral of community calculation. The plan depends on CP-ABE and can bolster any LSSS get to structure. Also, we upgrade the plan by advancing an on request client renouncement conspire. Along these lines, our get to control plan is more down to earth. We demonstrate the plan's security and show its proficiency through tests.

IX. FEATURE ENHANCEMENT

This project is totally based on generating the key and searching the different files. Based on these facilities we can develop the new technique for key generation. Such as we can use OTP like key generation technique and which is send to the mobile by message application. Now a day we are using emailing system to send the private key and outsourced key to user. This messaging facility is an advanced technique for previous system as well as current working system. In the second way we can put a new advanced searching technology which is implementing in case of Google API. That means when we are searching something it will display related data at the same time only.

REFERENCES

[1] Hadoop, http://hadoop.apache.org/.

[2] Storm, http://storm-project.net/.

[3] Y. Gao, H. Ma, H. Zhang, X. Kong, and W. Wei, "Concurrency optimized task scheduling for workflows in cloud," in 2013 IEEE Sixth International Conference on Cloud Computing (CLOUD). IEEE, 2013, pp. 709–716.

[4] 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. ACM, 2006, pp. 89–98.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in IEEE Symposium on Security and Privacy–SP'07. IEEE, 2007, pp. 321–334.

[6] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456–465.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography– PKC 2011. Springer, 2011, pp. 53–70.

[8] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Springer, 2007, pp. 515–534.

[9] S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," in Information Security and Cryptology–ICISC 2008. Springer, 2009, pp. 20–36.

[10] "On multi-authority ciphertext-policy attribute-based encryption," Bulletin of the Korean Mathematical Society, vol. 46, no. 4, pp. 803–819, 2009.

[11] Z. Liu, Z. Cao, Q. Huang, D. S. Wong, and T. H. Yuen, "Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles," in Computer Security–ESORICS 2011. Springer, 2011, pp. 278–297.

[12] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," in Progress in Cryptology-INDOCRYPT 2008. Springer, 2008, pp. 426–436.

[13] M. Chase and S. S. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 121–130.

[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 568–588.

[15] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 11, 2012.

[16] A. Ge, J. Zhang, R. Zhang, C. Ma, and Z. Zhang, "Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme," IEEE Transactions on Parallel and Distributed Systems, pp. 1–3, 2012.

[17] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[18] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology–EUROCRYPT'98. Springer, 1998, pp. 127–144.

[19] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: management of access control evolution on outsourced data,” in Proceedings of the 33rd international conference on Very large data bases. VLDB endowment, 2007, pp. 123–134.

[20] C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in IEEE INFOCOM 2011. IEEE, 2011, pp. 820–828.

AUTHOR DETAILS

PEDDI THARUN REDDY

Pursuing M.Tech (CSE) in Holymary Institute of Technology & Science (HITS), *Bogaram (V), Keesara (M), Ranga Reddy (D), Hyderabad*-501301, Telangana.

NARSIMHA BANOTHU

Working as Asst. Professor (CSE) in Holymary Institute of Technology & Science (HITS), *Bogaram (V), Keesara (M), Ranga Reddy (D), Hyderabad*-501301, Telangana.