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 2, February 2017

Survey on Group Data Sharing With Fine Grained Attribute Based and Secure Data Storage in Cloud Computing

Raosaheb S Wakchaure, Prof. G.S. Deokate

M.E. Student, Department of Computer Engineering, SPCOE, Otur., Pune, Maharashtra, India

Professor, Department of Computer Engineering, SPCOE, Otur., Pune, Maharashtra, India

ABSTRACT: These days Data sharing, support, its security are significant difficulties in worldwide world. Client in the data sharing system transfer their document with the encryption utilizing private key. This property is particularly critical to any expansive scale data sharing system, as any client release the key data then it will get to be distinctly troublesome for the data owner to look after security of the data. In this system give a solid and effective instantiate of plan, demonstrate its security and give a usage to demonstrate its common sense. There are bunches of challenges for data owner to share their data on servers or cloud. There are diverse answers for take care of these issues. For an endeavor, the data stored is gigantic and it is valuable. All undertakings are performed through systems. Consequently, it turns out to be imperative to have the secured utilization of data. In cloud figuring, the most critical worries of security are data security and protection. And furthermore adaptable and versatile, fine grained get to control must be kept up in the cloud systems. For get to control, being one of the great research points, many plans have been proposed and executed. There are strategy based plans have been proposed. In this paper, we will investigate different plans for encryption that comprise of Attribute based encryption (ABE) and its sorts KPABE, CPABE.These procedures are particularly basic to deal with key shared by the data owner. This system will acquaint how with lessen weight of data owner, validate the individuals who have the entrance to the data on cloud. DH calculation is utilized by the TTP to produce the key also, that key will get share to client and in addition the owner. The TTP module gets encoded record F utilizing AES Algorithm from the data owner. It stores key in its database which will be utilized amid the element operations and to decide the duping party in the system (CSP or Owner). Trusted Third Party sends record to Cloud Service provider to store data on cloud.

KEYWORDS: Cloud,Group Key,Secure Data,ABE,CPABE,TTP,Encryption,Deffie Helman,

I. INTRODUCTION

Cloud computing has quickly turned into a generally received worldview for conveying administrations over the web. In this way cloud specialist organization must give the trust and security, as there is important and touchy data in expansive sum stored on the clouds. For securing the secrecy of the stored data, the data must be scrambled before uploading to the cloud by utilizing some cryptographic calculations. In this paper we going to talk about attribute based encryption plot what's more, its categories. Sahai and Waters proposed Fluffy Identity Based Encryption [9] in 2005,and this paper proposed the principal idea of the attribute based encryption conspire through open key cryptography. Fuzzy Identity Based Encryption in which ways of life as an arrangement of elucidating attributes. Fluffy IBE can be utilized for an application that we call attribute based encryption. In this plan in which every client is recognized by an arrangement of attributes, and some capacity of this attributes is utilized to decide unscrambling capacity for each ciphertext. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute based systems [6]in2006. This paper gave an implementation of the ABE encryption system with more intricate get to strategy with (AND, OR door) in light of [9]. This work likewise exhibited distinctive uses of attribute based encryption conspires and tended to a few pragmatic thoughts, for example, key renouncement a d streamlining. Notwithstanding, this work is expelled after the proposition of KP ABE and CP ABE, which is more adaptable and proficient. In 2006, Goyal et al. proposed a key strategy attribute based encryption (KP ABE) conspire [3]. Fine grained get to control give d by KP ABE as contrasted and established model. In 2007 Bethencourt et al. proposed a cipher text strategy attribute based (CP ABE) conspire [1]. Data owner just trusts the key backer as CP ABE conspire addresses the issue of KP ABE. Both KP ABE and CP ABE can uphold general get to approaches that can be portrayed by a monotone get to structure. Besides, Muller proposed an appropriated attribute based encryption plot in 2008; Yu e. proposed a fine grained data get to control encryption conspire ; Tang proposed a Verifiable attribute based encryption plot .Ostrovsky et al. proposed an improved ABE plot which underpins non monotone get to structures[8].

II. RELATED WORK

The writing overview that containing investigation of various schemes accessible in Attribute Based encryption(ABE).That are KP ABE,CPABE,Attribute based Encryption Scheme with Non Monotonic Access Structures , ABE and MABE.Also incorporate preferred standpoint ,detriment and an examination table of each scheme based on fine grained get to control,efficiency,computational overhead and collusion safe. Attribute based encryption (ABE): An attribute based encryption scheme presented by Sahai also, Waters in 2005 and the objective is to give security and get to control. Attribute based encryption (ABE) is an open key based one to numerous encryption that permits clients to scramble and unscramble data based on client attributes. In which the secret key of a user and the cipher text are reliant upon attributes (e.g. the nation she lives, or the sort of memberships he has). In such a system, the decoding of a cipher text is conceivable just if the arrangement of attributes of the client key matches the attributes of the cipher text. Decoding is just conceivable when the quantity of coordinating is no less than a limit esteem d Collusion resistance is critical security highlight of Attribute Based Encryption .An enemy that holds various keys ought to just have the capacity to get to data if no less than one individual key stipends access.The issue with attribute based encryption (ABE) scheme is that data owner needs to utilize each approved client's open key to scramble data.The use of this scheme is limited in the genuine condition because it utilize the entrance of monotonic attributes to control client's entrance in the system. Key Policy Attribute Based Encryption(KP ABE) It is the adjusted type of established model of ABE. Clients are doled out with a get to tree structure over the data attributes. Limit doors are the hubs of the get to tree. The attributes are related by leaf hubs. To mirror the get to tree Structure the mystery key of the client is defined. Figure writings are marked with sets of attributes and private keys are related with monotonic get to structures that control which ciphertexts a client can decrypt.Key Policy Attribute Based Encryption (KPABE) scheme is intended for one to numerous interchanges. It enhances the impediment of KPABE that the encoded data can't pick who can unscramble. It can bolster the get to control in the genuine condition. Furthermore, the client's private key is in this scheme, a mix of an arrangement of attributes, so anser just utilize this arrangement of attributes to fulfill the get to structure in the encoded data. Disadvantages of the most existing CP ABE schemes are still not satisfying the endeavor prerequisites of get to control which require significant flexibility and proficiency. CPABE has impediments as far as determining strategies and overseeing client attributes. In a CP ABE scheme, decoding keys just bolster client attributes that are composed consistently as a solitary set, so the clients can just utilize every conceivable blend of attributes in a solitary set issued in their keys to fulfill policies.After that ciphertext policy attribute setbasedencryption (CP ASBE or ASBE for short) is presented by Bobba, Waters et al [7]. ASBE is an expanded type of CP ABE. it sorts out client attributes into a recursive set based structure and permits clients to force dynamic limitations on how those attributes might be consolidated to fulfill a policy. The CP ASBE comprises of recursive arrangement of attributes. The test in developing a CP ASBE scheme is inselectively permitting clients to join attributes from various sets inside a given key. There is test for keeping clients from joining attributes from numerous keys.

III. PROPOSED SYSTEM

Every user's group secret key is unique in relation to others and bound together with his private key related with traits. To decrease users' calculation loads, we present two cloud service providers named encryption cloud service supplier (E-CSP) and ecryption-cloud service supplier (D-CSP). The obligation of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decoding operation.

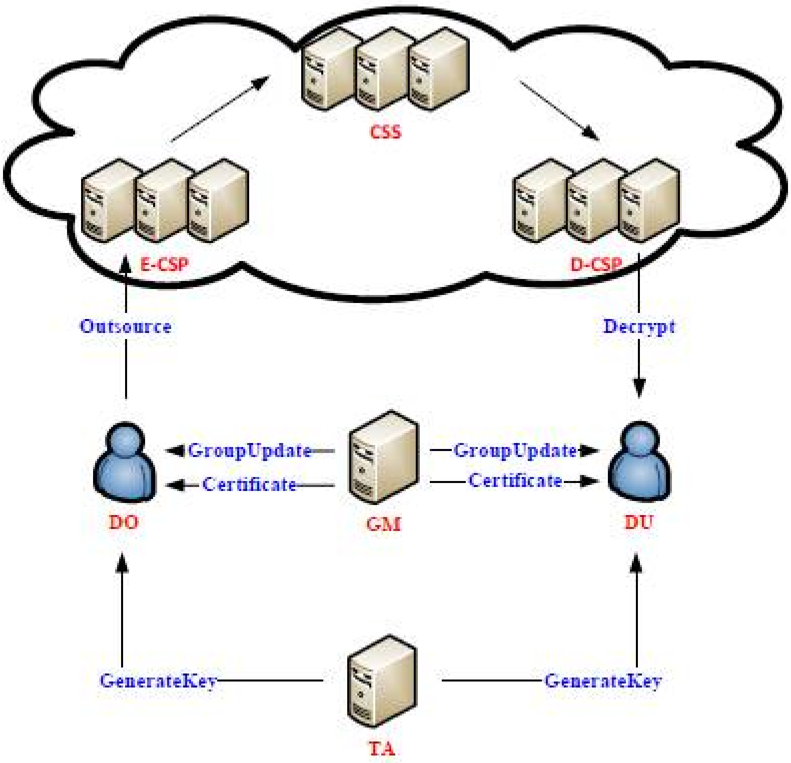

Fig:System Architecture [Ref. 10.1109/TSC.2016.2520932]

IV. CONCLUSION AND FUTURE WORK

This paper clarifies about the usage of cipher text policy attribute based scheme utilizing AES encryption decryption calculation. Where consider CP ABE scheme by tended to the issue of time require for encryption furthermore, decryption overhead and diminish era of complex key.The Proposed work gives simple and easy to and justifiable key structure. As future extension, numerous associations and actualize it on various cloud to scale up the business thought.

V. ACKNOWLEDGEMENT

I dedicate all my works to my esteemed guide and HOD, Prof.G.S.Deokate , whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this paper

REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalable Access Control in Cloud Computing", in IEEE Transactions on information forensics and security, Vol. 7, No. 2, in April 2012.
[2] Schucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," Achieving secure, scalable, and fine grained data access control in cloud computing," in Proc IEEE INFOCOM,2010.
[3] A.Sahai and B.Waters,"Fuzzy Identity Based Encryption," In Proc. Advances in Cryptology Eurocrypt,2005, vol.3494,pp.457473.

[4] S.Muller, S.Katzenbeisser, and C.Eckert," Distributed attribute-based encryption,"in Proc.11th Int.Conf.Information Security and Cryptology, 2008,pp.20-36, Springer.
[5] J.Hur and Dong Kun Noh," Attribute - Based Control with Efficient Revocation in Data Outsourcing systems," IEEE Transactions on Parallel and Distributed Systems,Vol.22, No.7,July 2011.
[6] V.Goyal, O.Pandey, A.Sahai and B.Waters,"Attribute - based encryption for fine - grained acess control of encrypted data," in Proc.ACM Conf.Computer and Communications(ACM CCS), Alexandria,VA,2006.
[7] J.Bethencourt, A. Sahai, an d B.Waters, "Ciphertext - policy attribute based encryption," in Proc.IEEE Symp. Security and Privacy, Oakland, CA,2007.
[8] R.Bobba, H.Khurana and M.Prabhakaran," Attribute - sets: A practically motivated enhanced to attribute - based encryption," in Proc .ESORICS, Saint Malo, France, 2009.
[9] G.Wang, Q.Liu, and J.Wu," Hierarchical attribute -based encryption for fine -grained access control in cloud storage services," in Proc.ACM Conf. Computer and Communication security(ACM CCS), Chica go.IL,2010.
[10] M.Cahse," Multi - authority attribute based encryption," inProc.TCC'07, 2007,pp.51- 534, Springer.