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. 4, Issue 12, December 2016

A Survey on Large Data Access with Efficient Attributes Access Policy in Cloud Computing

Minal Hadawale, Prof. Arti Mohanpurakar

M.E. Student, Department of Computer Engineering, D.Y.Patil School of Engineering and Technology, Lohegaon, Pune, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering., D.Y.Patil school of Engineering and Technology, Lohegaon, Pune, Maharashtra, India

ABSTRACT: In cloud computing environment, there are many users of cloud. They stores there data and accessing of large data stored on cloud. But this users face some of major issue causing loss of data in cloud and facing a problem in authority and privacy of users. Cipher text-Policy Attribute based Encryption (CP-ABE) is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of file and upload encrypted file with encrypted attribute with, key provided by attribute authority. Cloud consumers want to download any file so it only allow data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the cipher text in plaintext form, which may also leak some private information about end-users. Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected, these issues are modify in this scheme to provide more security. In this scheme attribute authority assign public key to user while uploading files on cloud and also files secret key and private key to data consumer are used while uploading and downloading respectively .

KEYWORDS: Big Data, Access Control ,CP-ABE , Privacy-preserving Policy, Encrypted Index.

I. INTRODUCTION

In the era of massive information, an enormous quantity of information is generated quickly from numerous sources (e.g. good phones, sensors, machines, social networks etc.). Towards these massive information, standard pc systems don't seem to be competent to store and method these information[1]. Owing to the versatile and elastic computing resources, cloud computing could be a natural suitable storing and process massive information. With cloud computing, end-users store their information into the cloud, and consider the cloud server to share their information to alternative users (data consumers). So as to solely share end-user's information to licensed users, it's necessary to style access management mechanisms in step with the necessities of end-users. Once outsourcing information into the cloud[2], end-users lose the physical management of their information. Moreover, cloud service suppliers don't seem to be fully-trusted by end-users that build the access management tougher [3]. For instance, if the standard access management mechanisms square measure applied, the cloud server becomes decide to gauge the access policy and build access call. Thus, end-users might worry that the cloud server might build wrong access call on purpose or accidentally, and disclose their information to some unauthorized users. So as to change end-users to manage the access of their own information, some attribute-based access management schemes square measure projected by investment attribute-based encoding. In attribute-based access management, end-users first outline access policies for his or her information and code the information underneath these access policies. Solely the users whose attributes will satisfy the access policy square measure eligible to decode the information[4].

In an efficient and fine-grained massive information access management scheme with privacy-preserving policy. Specifically, we tend to hide the total attribute (rather than solely its values) within the access policies. However, once the attributes square measure hidden, not solely the unauthorized users however additionally the licensed users cannot grasp that attributes square measure concerned within the access policy, that makes the secret writing a difficult downside. To help information secret writing, we tend to additionally style a completely unique Attribute Bloom Filter

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. 4, Issue 12, December 2016

to gauge whether or not AND attribute is within the access policy and find the precise position within the access policy if it's within the access policy[5]. Security analysis and performance analysis show that scheme will preserve the privacy from any LSSS access policy while not using abundant overhead.

II. SCOPE

Scope of system is to provide services to cloud user by implementing an efficient and fine grained big data access control scheme . This system implements model of hiding whole attribute in its access policy rather than hiding only its value. So users can not know attributes of files.

III. LITERATURE SURVEY

In Cipher text policy attribute base encryption scheme provides an efficient scheme for encrypting files and assign attribute access policy to file while uploading file on cloud but this cause problem while uploading files with attribute access policy. Its attributes are not fully encrypted, while uploading only its name is encrypted but value of attributes remain unencrypted. [1]
If unauthorized user gets this value then he may get file and access that file so security concern arises. Also data owner having more direct control on access policy and it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. [2]
In this scheme file is upload on cloud without entering any keywords of file. File upload on cloud only with attribute access policy for access of file. While cloud consumer want to download file from cloud then consumer enter only attributes and user get resulted file. This resulted file contains many files matching attributes but this is not exact matching result.[5]
Also this file are once upload, remain for long time on cloud, this cause wastage of space on cloud and cloud consumers get this file as a result each and every time and this file is of no use after long time. File uploading on cloud are in encrypted format so many difficulty occur searching over an encrypted data.[4]
The cloud server is not fully trusted authority, if users sensitive data or files remain for long time on cloud then file are not secure.[3]

IV. SURVEY ON CP-ABE TECHNIQUES

In many distributed systems a user ought to solely be able to access knowledge if a user posses a definite set of credentials or attributes. Currently, the sole technique for imposing such policies is to use a trustworthy server to store the info and mediate access management. However, if any server storing the info is compromised, then the confidentiality of the info are compromised. In CPABE we tend to gift a system for realizing complicated access management on encrypted knowledge that we tend to decision Ciphertext-Policy Attribute-Based coding. By victimization our techniques encrypted knowledge are often unbroken confidential although the storage server is untrusted ; what is more, our ways square measure secure against collusion attacks. Previous Attribute-Based coding systems used attributes to explain the encrypted knowledge and designed policies into user's keys; whereas in our system attributes square measure wont to describe a user's credentials, and a celebration encrypting knowledge determines a policy for United Nations agency will decode.
Attribute-based encryption (ABE) is a new approach that include public-key cryptography concept . In public-key cryptography ,by using receiver's public -key, message is encrypted for particular receiver. Attribute based encryption can define set of attribute and by using subset of attributes(Key-policy attribute based encryption -KP-ABE) or policies defined over set of attribute(Ciphertext-policy attribute based encryption-CP-ABE), message can be encrypted.The main issue is, only authorized user can decrypt a ciphertext those who have key for "matching attributes"and that key is received by trusted party only[1].

A user's private key is associated with a set of attributes in ciphertext-Policy attribute-based encryption(CP-ABE) and an access policy is specifies by a ciphertext over a defined universe of attributes within the system. If user's attributes satisfy the policy of the respective ciphertext then user will be able to decrypt ciphertext. Using conjunctions, disjunctions and(k,n)(k, n)-threshold gates policies may be defined over attributes i.e., kk out of nn attributes have to be

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. 4, Issue 12, December 2016

present(there may also be constructions for policies defined as arbitrary circuits and meanwhile with additional negations there may also be non-monotone access policies). For instance, let us assume that the universe of attributes is defined to be {P, Q, R, S}{P, Q, R, S} and user 1 receives a key to attributes {P, Q}{P, Q} and user 2 to attribute {S}{S}. If a ciphertext is encrypted with respect to the policy (P∧R)∨S(P∧R)∨S, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.

V. CONCLUSION

In this paper propose a mechanism for cloud computing. In cloud users upload their files and also access files from cloud .So scheme provides an efficient encryption scheme for security of data stored on cloud and then efficient access policy on data files. In public-key cryptography,by using receiver's public-key, message is encrypted for particular receiver. . If user's attributes satisfy the policy of the respective ciphertext then user will be able to decrypt ciphertext.

REFERENCES

[1] Kan Yang, Qi Han, "An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy" Citation information: DOI 10.1109/JIOT.2016.2571718, IEEE Internet of Things Journal
[2] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.
[3] K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," IEEE Trans. on Multimedia (to appear), February 2016.
[4] B. Waters, "Ciphertext -policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. of PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.
[5] H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. on Dependable and Secure Computing [DOI: 10.1109/ TDSC.2015. 2406704] , 2015.
[6] K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. on Computers, vol. 55, no. 10, pp. 1259–1270, 2006.
[7] J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proc. of ASIACCS'12. ACM, 2012, pp. 18–19.
[8] J. Hur, "Attribute-based secure data sharing with hidden policies in smartgrid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180,2013.
[9] A. Beimel, "Secure schemes for secret sharing and key distribution,"Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel,1996.
[10] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.
[11] Arti Arun Mohanpurkar, Madhuri Satish Joshi, "A Traitor Identification Technique for Numeric Relational Databases with Distortion Minimization and Collusion Avoidance" International Journal of Ambient Computing and Intelligence Volume 7 • Issue 2 • July-December 2016
[12] Arti Mohanpurkar, Madhuri Joshi, " The Effect of the Novel Anti-Collusion Fingerprinting Scheme on the Knowledge from Numeric Databases" International Journal of Scientific & Engineering Research, Volume 6, Issue 12, December-2015 ISSN 2229-5518
[13] Arti Mohanpurkar, Madhuri Joshi, "Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance" International Journal of Computer Applications (0975 – 8887) Volume 130 – No.5, November2015