ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A Review on Various Access Controls Policies and It's Limitations over Cloud Storage

C.Veena, Dr. M. Hanumanthappa

Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India

Professor & Chairman, Dept. of Computer Science& Applications, Bangalore University, Bangalore, India

ABSTRACT: Many data owners are motivated to outsource their sensitive data to the cloud in order to avoid local maintenance and to reduce the cost, after outsourcing the sensitive data to the cloud the data owner doesn't have any control on his data if data owner want to define set of policies over his remote data before outsourcing the data he has to be encrypt with set of policies, so Data access control is an effective way to ensure the data security in the cloud, Access control is defined as a policy or procedure that allows, denies or restrict access over cloud storage. Various techniques have been proposed to protect the data contents privacy via access control. The major issues in cloud computing environment are security and access control. To control remote data the data owner has to define an effective access control mechanisms but according to the literature survey some access control mechanisms are defined but they have some limitations so in this paper will reviews on various access controls mechanisms advantages and limitations over cloud storage.

KEYWORDS: ABE, IBE,Fuzzy-IBE, CP-ABE, KP-ABE, Access control

I. INTRODUCTION

Cloud computing offering services through internet so now days many users are attracted to new paradigm of cloud, and they are using cloud as pay-per use, without burden of investment and maintenance then can migrate to cloud, generally in storage as a service cloud consist of three entities like data owner, data user and cloud service provider so here the data owner will upload the data to the cloud but cloud is un trusted so in order to protect his data the data owner should encrypt the data and after encrypting the data he can outsource to the cloud,, now data user can download particular file from cloud but in order to decrypt he has to get the corresponding key from data user. So in this process the data owner has to generate decryption key to every data user but this is difficult process however the data owner can depend on third party for generating key, so we can't trust third party and if the decryption key is disclosure to un authorized users may be data confidentiality will loss, so in order to overcome all these difficulties an efficient access polices should be defined, some of access control mechanisms are Identity Based encryption (IBE), Fuzzy Identity based encryption (Fuzzy-IBE), Attribute based encryption (ABE) , Cipher text policy based encryption (CP-ABE), Key policy based encryption (KP-ABE) , in all these access controls an attribute authority required to manage attributes.

II. RELATED WORK

Identity-based encryption (IBE) in which the owner of a data can indicate an access control by using identity such that only a receiver with matching identity can decrypt it. In this mechanism three entities will involve one is owner who want to outsource his data and second one user who want to download data from cloud and final one key generator. Using IBE the data owner can encrypt the document, in order to encrypt the document the owner required public key for generating public key the owner will depend on PKG (public key generator) for downloading secrete key the user submit identity to Public key generator based on identity the PKG issues private key for user, so after downloading the document from cloud the private key should satisfy with identity then the document will decrypt.
In this process first owner will request to Public key generator for generating public key, the public key generator will take the identities from users and based on owner request he will generate pubic key, after generating the public key the key generator will send key to the owner, after receiving public key from key generator the owner will encrypt the data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

using public key later he can outsource to the cloud. Once user download the file from cloud in order to download he has to get corresponding secrete key from key generator, in order to get secrete key the user has to submit identities based on identities the key generator will generate secrete key.

Fuzzy identity based encryption (Fuzzy-IBE) after IBE; Fuzzy Identity-Based Encryption is proposed in order to overcome IBE limitations, in this process identities are set of descriptive attributes. Here the data owner can define set of identities instead of single identity like IBE scheme, here also the data owner can specify the data access control but he can't revoke the particular user. The system model and process is similar to IBE, only the difference is descriptive attributes other than that everything is similar.

In this Fuzzy-IBE process the owner encrypt the document based on selected user multiple identities, so in order to encrypt the document the owner will get the key from PKG and same way in order to get private the user will submit attributes to PKG. while decrypting document among multiple attribute minimum one attribute should be match.

Attribute based encryption (ABE): in this encryption scheme the data owner is able to describe set of access policies over cloud encrypted data, in this scheme the access policy made with set of attributes of intended user. Using this scheme the owner can achieve one-to-many access policy, on one document with different permission set.

In this process the attribute authority will maintain set of attributes and based on set of attributes the attribute authority will generate public key for owners and private key for users.

Example: in this scenario the report or document would be encrypted with set of attributes like {"B+", "veena", "Age 35-45"}, and only the users with all of these three attributes in the blood bank can hold the corresponding private keys and thus decrypt the document, while others cannot.

Attribute based encryption (ABE) will categorized into cipher CP-ABE and KP-ABE, so in CP-ABE the encrypted document is associated with a set of attributes of intended users and the private key of user is associated with the access policy. The data owner can defines the set of attributes these are necessary for decrypt the encrypted document. The attribute authority AA who creates user's secret key based on set of user attributes, In KP-ABE a private key is generated with set of attributes and the encrypted document is associated with set of policies.

III. LIMITATIONS

In above all Access control Mechanisms the problems identified as

1. In above discussed control scheme the data owner is depending on key generator (Third party) in order to generate public key and private key.
2. In some situations may be third party might be comprised, and then identities will be exposed to unauthorized users.
3. After outsourcing data to the cloud if any dynamic operations need to be perform on the document, then the document should be re-encrypt and new keys should be re-issue to the corresponding users.
4. If any user want quit from the cloud access or due to dynamic policies the user must be revoked, so in order to revoke the user, the data owner must be re-encrypt the document and re-generate the new keys, after using secure channel the key should be distribute to authorized users.
5. Due to the above limitations, a new access control model should be implemented and the new model should effectively handle the dynamic policies and dynamic operations.

IV. CONCLUSION

By utilizing storage as a service the data owner will distribute or share his sensitive document to line of cloud users among multiple approved users however before outsourcing the document into the cloud storage server the data owner should alter set of access polices over document like users will access the information and illicit users can't access the information and he may also outline access structure over set of users. therefore so as to outline access management and strategy for document totally different access management mechanisms area unit outlined therefore in these papers we tend to taken a review over multiple access controls schemes and their method and limitations.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

REFERENCES

1. Ravi S. Sandhu and Pierangela Samarati "Access Control: Principles and Practice" IEEE Communications Magazine, September 1994.
2. Yingjie Xia, Li Kuang and Mingzhe Zhu "A Hierarchical Access Control Scheme in Cloud using HHECC" Information Technology Journal 9 (8): 1598-1606 , 2010
3. Hazen A.Weber "Role Based Access Control: The NIST solution" San Institute of Info Reading Room, October 3 ,2008.
4. Joon S.Park, Gail-Joon Ahn, Ravi Sandhu "Role-based Access control on the web using LDAP".
5 Abdul Raouf Khan " Access control in cloud computing Environment" ARPN Journal of Engineering and Applied Science,vol 7, No.5 May 2012.
6 Zhu Tiayni, Liu Weidong, Song jiaxing "An Efficient role based access control system for cloud computing" 2011 11th IEEE International Conference on Computer and Information Technology.
7 Xiaohui Li, Jingsha he, Ting Zhang "Negative Authorization in Access Control for Cloud Computing" International Journal of security and its Applications. Vol. 6, No.2 April 2012.
8. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 2007, pp. 321–334.
9. M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.
10. M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

BIOGRAPHY

C.Veena is working as a Asst.Professor in CSE Dept. Holy mary Institute of Technology & Science. She has completed her MCA from S.V.University in 2002. She Completed M.Tech in CSE from JNTU Anantapur in 2013. She is having a total 08 years of teaching experience. Her research area of interest are Cloud Computing, Network security, Data Mining, Etc.

Dr. M. Hanumanthappa is working as a Professor & Chairman Dept of Computer Science& Applications, Bangalore University, Bangalore. His completed his MCA from Bangalore University in 1996. His received his M.Phil & Ph.d in Data Mining from Bangalore University in 2009. His having total 18 years of teaching, Administration & Industry Experience. He adjudicated nearly 50 Ph.d, M.Phil (Computer science thesis of various Universities) and conducted 18 viva voce examinations for Ph.d, M.Phil candidates. He has total research publications:95 out of which international journals 47, International conferences 28, national conferences 17, Monographs 03. His guiding 08 number of ph.d students and Awarded 03 Ph.d. He received Dr.RadhaKrishna GIold Medal award by Global Economics progress and research association in 2012. His area of interest are Data Mining, Cloud computing, Network security.