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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Attribute Based Access to Scalable Media

Lokesh Khubalkar[1], Mrutyunjay Meshram[2], Narendra Rewatkar[3], Swapnil Mahant[4],

Prof. Neha Zade[5]

Final Year B.E. Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, India[1,2,3,4].

Assistant Professor, Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, India[5].

ABSTRACT: In this paper Attribute-Based access to the media in the cloud where it uses cipher-text policy Attribute-Based Encryption (CP-ABE) technique to create an access control structure by using the algorithms. In the access policy the attributes are used to encrypt the data and a secret key consisting of user attributes to decrypt the data and is used as an access policy in order to restrict the access of the user. This requires flexible and accessible cryptographic key management to support difficult access policies. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one Cipher text such that only the users whose attributes satisfy the access policy can decrypt the Cipher text.

I.INTRODUCTION

The data owners encrypt the data using this user attributes and then upload the file to the cloud. The user whenever wanted to download the file should decrypt the file only if its attributes get satisfied. Hence for a particular shared data among the multiple users we need to encrypt the data with every user's public key which is predefine in program in order to provide security hence an ordinary encryption is unsatisfactory. Instead if the cipher text consists of the set of attributes then by using the key and access policy we can decrypt the data i.e. the key works only when the attributes in the cipher text satisfies the access policy. The Multi-message Cipher text Policy Attribute-Based Encryption (MCP-ABE) technique and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers attributes (e.g., Department, Year) rather than an explicit list of the consumers names. However in order to design an access policy mechanism there are many challenges to overcome some of them are (1)user can upload any kind of document file.(2) any can give any number of attributes and hence two or more users may have same attributes. (3) Any individual may grand any kind of access to any number of users. This approach allows the user to implement the access control on their data directly in content sharing service rather than through a central administrator. In order to provide a complex access policy mechanism we need flexible and scalable cryptographic key management algorithms. To overcome these disadvantages we are using attribute based encryption .hence we employee CPABE (cipher text policy – attribute based encryption) technique as a remedy to the abovementioned problem in CP-ABE the recipient can decrypt the data only when the user attribute satisfy the access policy and this can be seen as one-to-many public key encryption and the data owner provides access to many users. CP-ABE scheme is similar to the KP-ABE (key policy attribute-based encryption).In key policy attribute based scheme the access policy is built-in the users secret key where as in CP-ABE (cipher text policy attribute based encryption) the access policy is switched into the encrypted data andtheattributes are linked with the public key of the user in order to decrypt the data. If the attribute set in the users secret key satisfies the access policy present in the encrypted data then the data will be decrypted.

II. RELATED WORK

The traditional access control architectures usually assume the data owner and the servers storing the data are in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor responsible for defining

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

and enforcing access control policies. This assumption, however, no Longer holds in cloud computing since the data owner. Furthermore, we observe that there are also cases in which cloud users themselves are content providers. They publish data on cloud servers for sharing and need fine grained data access control in terms of which user (data consumer) has the access privilege to which types of data. In contend-based access control, individuals are explicitly authorized to access collections of records matching certain criteria. We refer to these as collections as content slices. This approach supports individuals who do not have precisely defined roles, such as contractors or medical researchers. Cloud-based multimedia content sharing is one of the most significant services in cloud-based multimedia systems. In some security and privacy issues of multimedia services are proposed by exploring the multimedia-oriented mobile social network. The relationship between the user identification and resource in content sharing applications is dynamic.

Modules
1) Registration
2) Attribute oriented access control
3) DES function
4) Cipher-text policy attribute-based encryption

Modules Description Registration In this module normal registration for the multiple users. There are multiple owners, multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Attribute oriented access control in this Module, supports fine-grained access control policies and dynamic group membership by using CP-ABE scheme.KP-ABE (Key Policy Attribute based Encryption) to enforce access policies based on data attributes.DESfunction in this Module, usually for security or data management purposes..
Cipher-text policy attribute-based encryption in this Module, every user's personal set of attributes while every cipher text is associated with an access policy. A user successfully decrypts a cipher text only if her set of attributes satisfies the access policy specified in the cipher text. We briefly describe the CP-ABE. We will extend this CP-ABE scheme to MCP-ABE scheme and use the latter in our access control scheme.

Advantages & Limitations:
1) Advantages
a) The scheme has several benefits that ensure password complexity and security control over the sharable data.
b) The present scheme is also secured against user collusion attacks due to use of attribute-based encryption.
c) We present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery.
2) Limitations
a) In an existing system solution is flexible, but it is high complex.
b) The existing method is to classify users into different roles based on their attributes, assign role keys to users and then encrypt the content using the role keys. However this approach results in high complexity.

III. METHODOLOGY

Cloud computing is an emerging computing paradigm that brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for data management when fine grained data access control is desired, and thus do not scale well. In content sharing applications like social networking media, the mapping between user identity and resource is dynamic, access control methods related to our work can increase the security level against user collusion attacks due to use of attribute-based encryption. So the fundamental policy is to implement a control model where we can provide attributes attached to both users and resources. In content sharing applications,

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

as a mapping between user identity and resource is dynamic, access control methods related to our work can be implemented using the following steps for more secured content sharing. Components in an attribute -based access control scheme includes subjects each specified by a set of attributes, objects and access policies. Attribute Authority (AA), a trusted third party, sets up the system parameters of attribute-based encryption system, and verifies every user's attribute (e.g., group membership, role, and security clearance or authorization information) and issues predefine public key corresponding to the set of attributes of the user. In practice, there could be multiple AAs in a system. For example, a university or corporate may run an AA, and a user may act as an AA for his/her extended family members.

IV. PROPOSED WORK

Here we are providing better security in owner's upload side as well as on the download side. For better security client splitting that single file into nine different blocks and providing a unique identification number for each block.

A.DES function

The Data Encryption Standard (DES) is a symmetric-key method of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same key.

B. Cipher-text policy attribute-based encryption

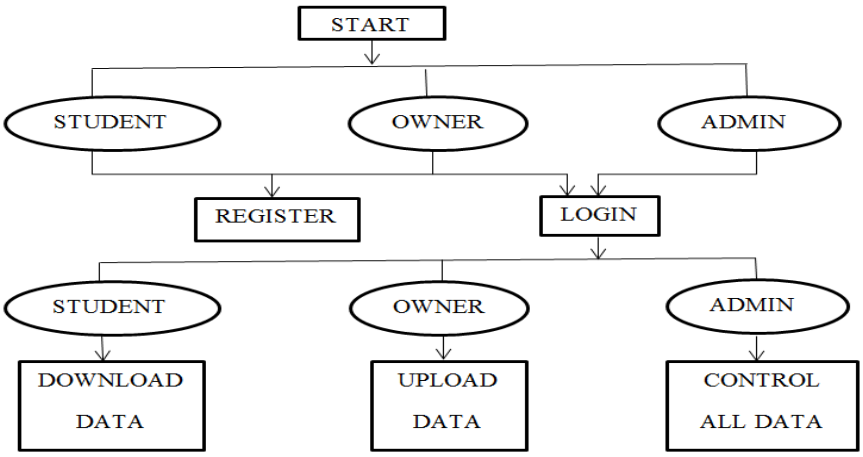
In this Module, every user's is associated with a set of attributes while every cipher text is associated with an access policy. A user successfully decrypts a cipher text only if her set of attributes satisfies the access policy specified in the cipher text.

1) AB-Setup: It is an initialization algorithm run by an Attribute Authority (AA). It takes as input a security and outputs a public key PK.

2) AB-Encrypt: Data owner to encrypt a message according to an access tree.

3) AB-Decrypt: Data consumer in possession of a set of attributes and the key K in order to decrypt the cipher-text CT with an access policy.

Flow Diagram:



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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

V.RESULT ANALYSIS

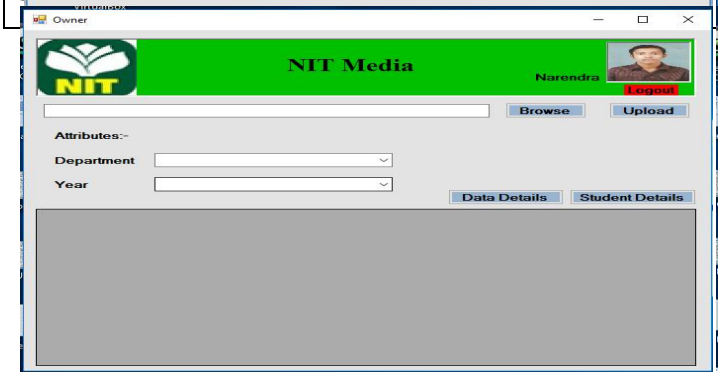
Front Page: In the front page there are three users, from that Admin is predefine. Student and Owner have to register them self through the registration form and also can change their password from forget password form. At the Registration form the Owner and Student have to fill their details like mobile number, email and specially department and year.

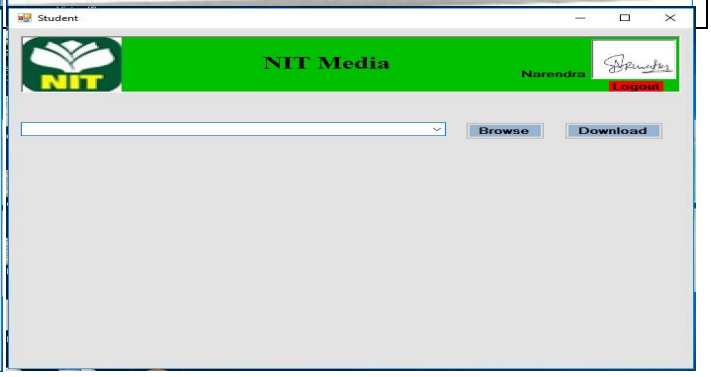
Login Form: For all the users a different login form is open for performing their operations (upload, download and delete). Student and Owner can login by using their provided email id and password which is automatically generated at the time of registration.

Owner Show Data: Owner can browse file, select the attributes and upload file in the database with encrypted form. Owner can also check the uploaded data and student details. Owner has ability to select any type of document file and can send it to the respective department and year. Owner can also change their password and other details by clicking on his profile picture that will generate a form with his details.

FRONT PAGE:

LOGIN FORM:





Student Show Data: Student will browse the file, if its attributes are same as owner provided at the time of file upload then only student can download the file in decrypted form. Only the authorised student can download that file other student can't browse that file. Student can also change their password and other details by clicking on his profile picture that will generate a form with his details.

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

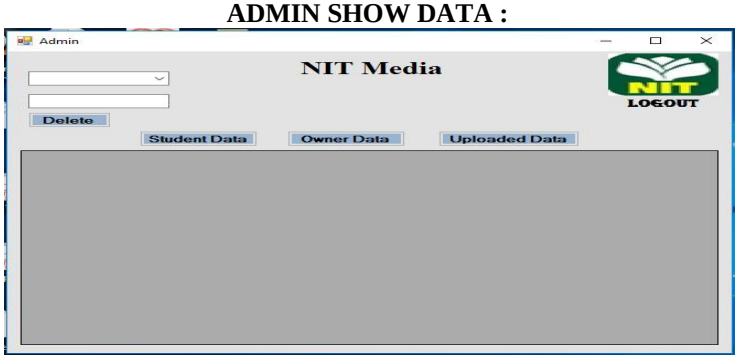
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

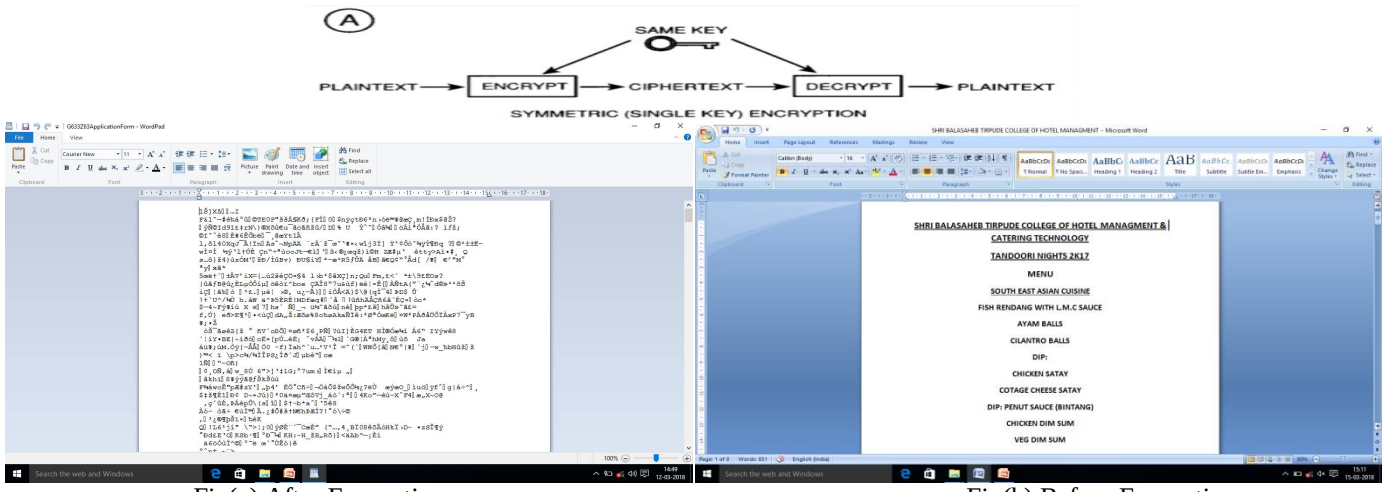
Vol. 7, Issue 3, March 2018

ADMIN SHOW DATA :



Admin Show Data: Admin is a predefine user which can control and monitor all the operations. Admin can also maintain database. Admin has authority to check all the uploaded, Owners and Students data. Admin can maintain that data (ex. Delete).

OUTPUT



Fig(a).After Encryption Fig(b).Before Encryption

VI. CONCLUSION& FUTURE SCOPE

Conclusion:
This paper we implemented an encryption algorithm with better security. MCP-ABE scheme is use as access policy, the attributes are used to encrypt the data and a secret key consisting of user attributes to decrypt the data.
Future Scope:

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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

- In future online based system can implemented with improved features.
- Notification service can be included to send alerts of news feed to users.

REFERENCES

(1) Yongdong Wu, Zhuo Wei, and Robert H. Deng *"Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks"*- IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013.
(2) Priya A. Kamble,Pragati Patil *"Attribute-Based Access To Multimedia In Cloud-Assisted Online Content Sharing"*-IEEE Volume 5,Issue 10 October-2015.
(3) V Benzoic, D Sock, R Steinhardt, and V. I. Val- lanai, *"Multiauthority Attribute-based Encryption with honest-but-curious central Authority"* International Journal of Computer Mathematics, vol. 89, pp. 3, 2012.
(4)International Journal & Magazine of Engineering, Technology, "Management and Research *A Peer Reviewed Open Access''*International Journal ISSN No: 2348-4845 Volume No: 2 (2015), Issue No: 6 June 2015.
(5) Maheswara rao.N 1, Sk.N.Rehmathunnisa2, Scalable Media in *"Cloud-assisted Content Sharing with Attribute-based Access Networks"*, IJCSIET-ISSUE5-VOLUME3-SERIES1.
(6) Venkatesh prasad.Kalluri et al, International Journal of Computer Science and Information Technologies, *"CIPHER-Text Policy Attribute Based Access to Cloud"*, Vol. 5 (3), 2014, 2796-2799.
(7)Authorized licensed use limited to: Univ of Calif Los Angeles *"Cipher text-Policy Attribute-Based Encryption* "July 27, 2009.
(8)Hash-based Digital Signature Schemes, October 29, 2008.
(9) International Journal of Computer Trends and Technology (IJCTT) – volume 15 number ISSN: 2231-2803 3 – Sep 2014.
(10) International Journal of Advances in Applied Science and Engineering (IJAEAS) ISSN (P):2348-1811; ISSN (E): 2348-182X Vol-1, 152-159Iss.-4 September 2014.
(11) International Journal of Advanced Technology and Innovative Research Volume. 06, IssueNo.06, Pages: 543-548 September-2014.
(12) International Journal of Scientific Engineering and Technology Research Volume.03, IssueNo.35, Pages: 7086-7091 November-2014.