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 7, July 2017

Secured Access Control Using Two-Way Approach for Cloud Computing Services

Saraswati Gore[1] , Prof. Kalyan. D. Bamane[2]

M.E Student, Department of IT, Alard college of Engg, Murunji, Savitribai Phule Pune University, Pune, India[1].

Prof, Department of IT, D Y Patil college of Engg, Akurdi, Savitribai Phule Pune University, Pune, India[2].

ABSTRACT: Cloud computing is an internet based computing which enables sharing of services. With cloud computing, users can remotely store their data into the cloud and use on-demand high-quality applications. Cloud allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. The advantage of cloud is cost savings. The prime disadvantage is security. We present another Secured Access Control Using Two-Way Approach for Cloud Computing Services to achieving security in distributed cloud storage. In particular, in our proposed access control framework, a property based access control system is executed with the need of both a client secret key and a lightweight security device. As a client can't access the data on the off chance that they don't hold both secrete key and OTP. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). We also apply Cauchy approach for data storage on cloud. In this approach first we divide (fragment) our file and then store each fragments on nodes. When user wants to upload another file then system checks is any fragment is similar to previous fragments. If any similar fragment is found then Cauchy approach assign pointer to new similar fragment instead of storing that fragment. With the help of our system we can achieve maximum security of data in distributed cloud. Likewise, characteristic based control in the framework too enables the cloud server to restrict the access to those clients with the same arrangement of properties while preserving client protection, i.e., the cloud server just realizes that the client satisfies the required predicate, however no clue has on the precise personality of the client.

KEYWORDS: Access control, ASA, Cauchy Approach, Delfi Hellman, Fine-grained, Identity Based Encryption, RSA, Two-factor, Web services.

I. INTRODUCTION

Background:

As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser. A recently proposed access control model called *attribute-based access control* is a good candidate to tackle the first problem. It not only provides anonymous authentication but also further defines access control policies based on different attributes of the requester, environment, or the data object. In an attribute-based access control system, each user has a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer. When we consider the above mentioned second problem on web-based services, it is common that computers may be shared by many users especially in some large enterprises or organizations.

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 7, July 2017

Motivation:

In the existing system each user has a user secret key issued by the authority but the user's secret key is stored inside the personal computer. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares. We propose a Secured Access Control Using Two-Way Approach for Cloud Computing Services to achieving security in distributed cloud storage. As a user cannot access the system if they do not hold both OTP and secrete key. The mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services.

Our system has the following properties:

(1) It can compute some lightweight algorithms.

e.g. hashing and exponentiation.

(2) It is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

Objective and Goal:

- To propose a secured access control using two-way approach web-based cloud computing services.
- To achieve reliability, security, integrity of the data on the cloud.
- To reduced storage space.

II. LITERATURE SURVEY

No	Author Name	Topic Name	Algorithm/Techniques	Output	Year
1	Rashmi 1,Dr.G.Sahoo2, Dr.S.Mehfuz3	Securing Software as a Service Model of Cloud Computing: Issues and Solutions	Survey is performed in this paper: • Data Segregation • Data Access • Web application security • Data breaches • Backup • Identity management and sign-on process	• An attempt to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also endeavors to provide future security research directions	2013
2	Kashif Munir and Prof Dr. Sellapan Palaniappan	Framework for Secure Cloud Computing	• Generic cloud security model	• Identifies security and privacy challenges in cloud computing • Satisfy security and privacy requirements in the clouds and	2013

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 7, July 2017

				protect them against various vulnerabilities	
3	Mr. Ankush Kudale, Dr. Binod Kumar	A Study on Authentication And Access Control For Cloud Computing	• A grid distributed parallel authentication model • SSL • TLS protocols • Stream cipher heuristic code generator models	• Will give you many ideas about different methods and frameworks designed by many researchers	2014
4	Harvinder Singh1, Amandeep Kaur2	Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication	• Use security questions and image based for the login protection in cloud platforms on mobile devices and software systems for computers • Use Unique Identification Number (UIN)	• Supports anonymous authentication and performs decentralized key management • Prevents replay attacks and supports creation, modification and reading data stored in the cloud	2015
5	Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou	k-times attribute-based anonymous access control for cloud computing	• Implementations of Protocol PK0 and PK1	• Allows a user to authenticate himself/herself • Provides k-times limit for anonymous access control	2014
6	J. Bethencourt, A. Sahai, and B. Waters	Ciphertext-policy attribute based encryption	• ciphertext-policy attribute-based encryption (CP-ABE) • Access tree T	• Encrypted data can be kept confidential even if the storage server is untrusted • Methods are secure against collusion attacks	2007
7	D. Boneh, X. Ding, and G. Tsudik	Fine-grained control of security capabilities	• mRSA Key Generation Algorithm • mRSA Signature Algorithm • mRSA Decryption Algorithm • mRSA Key Generation for multiple SEM-s	• Revoking the client's certificate • Revokes the client's ability to perform cryptographic operations such as signature generation and	2004

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 7, July 2017

				decryption	
8	J. Camenisch, M. Dubovitskaya, and G. Neven	Oblivious transfer with access control	• Issuer Setup algorithm • Database Setup algorithm • Issue protocol • Transfer protocol	• Present a protocol for anonymous access to a database where the different records have different access control permissions	2009
9	K. Liang, W. Susilo, and J. K. Liu	Privacy-preserving ciphertext multisharing control for big data storage	ciphertext sharing mechanism with the following properties: • Anonymity • Multiple receiver-update • Conditional sharing	• Preserve the anonymity for ciphertext sender/receiver, conditional data sharing and multiple recipient-update	2015
10	J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan	Secure sharing and searching for real-time video data in mobile cloud	• AES encryption • Searchable Symmetric Encryption (SSE) • Ciphertext policy attribute-based encryption (ABE) • Digital signature	• Proposed an infrastructure for secure sharing and searching for real-time video data	
11	Y. Wu, Z. Wei, and R. H. Deng	Attribute-based access to scalable media in cloud-assisted content sharing networks	• Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE)	• Allows a data owner to enforce access control based on attributes of data consumers without explicitly naming the specific data consumers • Supports only one privilege level	2013

IV. SOFTWARE REQUIREMENT SPECIFICATION

User Classes and Characteristics

To design products that satisfy their target users, a deeper understanding is needed of their user characteristics and product properties in development related to unexpected problems that the user's faces every now and then while developing a project. The study will lead to an interaction model that provides an overview of the interaction between user characters and the classes. It discovers both positive and negative patterns in text documents as higher level

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 7, July 2017

features and deploys them over low-level features (terms). In proposed work is designed to implement above software requirement. To implement this design following software requirements and hardware requirements are used.

Software Requirements

- Operating System - Windows XP/7
- Programming Language - Java/J2EE
- Software Version - JDK 1.7 or above
- Tools - Eclipse
- Front End - JSP
- Database - Mysql

Hardware Requirements

- Processor - Pentium IV/Intel I3 core
- Speed - 1.1 GHz
- RAM - 512 MB (min)
- Hard Disk - 20GB
- Keyboard - Standard Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LED Monitor

V. IMPLEMENTATION STATUS

- **Registration and login**
  - User first have to registered with the system and then login with the system
  - At the time of login system must have to check user is authorized person or not
  - After login successful user entered in his/her account and perform other operations
  - Cloud Server and Authority directly perform login without registration with the system
- **Key generation**
  - For uploading file first user choose cloud type and choose file. Then user send request for key to authority
  - Authority is responsible for generating key
- **Fragmentation and duplication checking**
  - At the time of uploading file, system first make fragments of file and then checks one by one fragment is same as another stored fragment or not

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 7, July 2017

- If fragment is duplicate then system assign pointer to that original fragment and original fragment is not stored on cloud to reduce storage space
- If fragment is not duplicate then system stored that particular fragment on cloud

- **Generate OTP**

  - For downloading other users file user must request to system for OTP
  - System creates OTP and sends on users mail account

VI. COMPARISON BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based existing system. First, the traditional account/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It may be easy for hackers to install some spyware to learn the login password from the web-browser. Therefore such systems are not fully secured. In the existing system each user has a user secret key issued by the authority but the user's secret key is stored inside the personal computer. Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares. We propose a Secured Access Control Using Two-Way Approach for Cloud Computing Services to achieving security in distributed cloud storage. As a user cannot access the system if they do not hold both OTP and secrete key. The mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services.

Our system has the following properties:

(1) It can compute some lightweight algorithms.

e.g. hashing and exponentiation.

(2) It is tamper resistant, i.e., it is assumed that no one can break into it to get the secret information stored inside.

VII. ALGORITHM FOR RELEVANT FEATURE DISCOVERY

- **File Fragmentation Algorithm:**

1. If file is to be split go to step 2 else merge the fragments of the file and go to step 8
2. Input source path, destination path
3. Size = size of source file
4. Fs = Fragment Size
5. NoF = number of fragments
6. Fs = Size/Nof
7. We get fragments with merge option
8. End

- **Secrete Key Generation Algorithm:**

```
Random r=new Random();
//pass identity to generate key
 String s=new String(Base64.encodeBase64(KeyGenerator.generateString
```

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 7, July 2017

```
                        (r,"useremail",16).getBytes()));
 String key=KeyGenerator.generateString(r,s,16);

  public class KeyGenerator {
     //setup process
     //public static final String publickey="0023542123qwersa";
     // public static final int publickeyLength=16;
     //extract key process according userid
public static String generateString(Random rng, String characters, int length)
    {
    System.out.println("String:"+characters);
    char[] text = new char[length];  //array size is 16
    for (int i = 0; i < length; i++)
    {
       text[i] = characters.charAt(rng.nextInt(characters.length()));
    }
   // System.out.println("text is:"+ new String(text));
    return new String(text);
    }
}
```

- **AES Encryption Algorithm**

Input: Key 128 bit and Data

Output: CipherText

Step1: Declare initVector=”RandomInitVector”
//This is 16 byte IV to generate the random key.

Step2: Create the objects
IvParameterSpec iv = new IvParameterSpec(initVector.getBytes("UTF-8"));
//UTF-8 is use to convert plaintext bytes into string
SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("UTF8"),"AES");
//SecretKeySpec class specifies a secret key

Step3: Create the objects
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
// cipher class provides the functionality of a cryptographic cipher for encryption
//CBC-cipher block chaining i.e algorithm mode

Step4:
cipher.init(Cipher.ENCRYPT_MODE, skeySpec, iv);
byte[] encrypted = cipher.doFinal(value.getBytes());
//doFinal(byte[] input)-Encrypts data in a single-part operation, or finishes a multiple-part operation.

Step5:
Base64.encodeBase64String(encrypted));
//encodeBase64String(byte[] binaryData)-Encodes binary data using the base64 algorithm

Step6: End
// End the process.

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 7, July 2017

- **OTP Generation Algorithm:**

```
public class CreateToken {

char[] characterSet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789".toCharArray();
        int length=10;
        String Result=null;
        public String  Create_Token_Method(){


          Random random1 = new SecureRandom();
            char[] result = new char[length];
            for (int i = 0; i < result.length; i++) {
               // picks a random index out of character set > random character
               int randomCharIndex = random1.nextInt(characterSet.length);
               result[i] = characterSet[randomCharIndex];
            }
            Result=new String(result);
            System.out.println ("resultttttttttt"+ Result);
         return Result;

}
```

- **AES Decryption Algorithm**

Input: Key 128 bit and CipherText

Output: PlainText

Step1: Declare initVector=”RandomInitVector”
//This is 16 byte IV to generate the random key.

Step2: Create the objects

```
IvParameterSpec iv = new IvParameterSpec(initVector.getBytes("UTF-8"));
//UTF-8 is use to convert plaintext bytes into string

SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("UTF8"),"AES");
//SecretKeySpec class specifies a secret key
```

Step3: Create the objects

```
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
// cipher class provides the functionality of a cryptographic cipher for decryption
//CBC-cipher block chaining i.e algorithm mode
```

Step4:

```
cipher.init(Cipher.DECRYPT_MODE, skeySpec, iv);
byte[] encrypted = cipher.doFinal(value.getBytes());
// doFinal(byte[] input)- decrypts data in a single-part  operation, or finishes a multiple-part operation.
```

Step5:

```
Base64.decodeBase64String(encrypted));
//encodeBase64String(byte[] binaryData)-Decodes cipher text using the base64 algorithm
```

Step6: End

```
// End the process.
```

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 7, July 2017

VIII. SYSTEM ARCHITECTURE

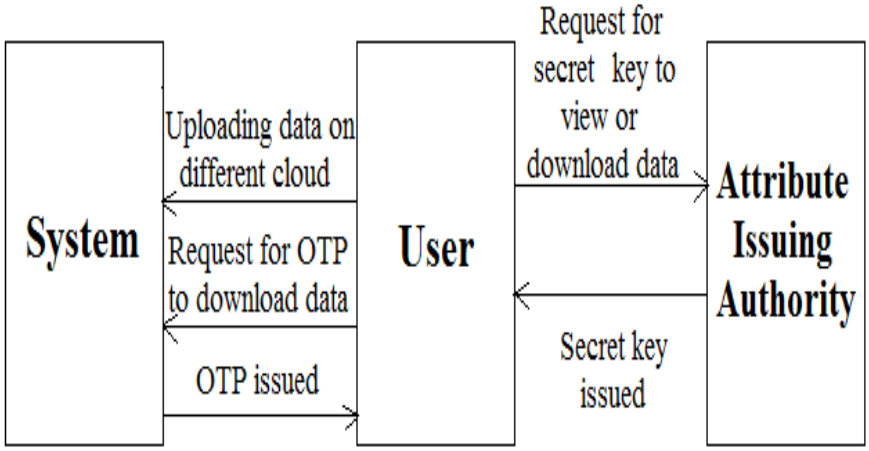

Figure 1: System Architecture

In our system we use two important parameter for downloading the file i.e. OTP and secret key. Client can't access the data on the off chance that they don't hold both secrete key and OTP. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). We also apply Cauchy approach for data storage on cloud. In this approach first we divide (fragment) our file and then store each fragments on nodes. When user wants to upload another file then system checks is any fragment is similar to previous fragments. If any similar fragment is found then Cauchy approach assign pointer to new similar fragment instead of storing that fragment.

The above diagram represents our system architecture. User has choice to select any cloud i.e. public cloud or private cloud for data uploading (storing). At the time of uploading we encrypt file by using Identity Based Encryption (IBE) algorithm and then we fragment file. Then we use Cauchy approach for checking same fragment is already stored or not to reduce storage space on cloud. When user wants to view data then he/she must need to get a secrete key and when user wants to download data from cloud then he/she must need to get a secrete key and OTP.

IX. MATHEMATICAL MODEL

The following terms shows in detail working of project.
S={s, e, X, Y,}

Where,

s = Start of the program.
1. Log in with webpage.
2. Load Files on cloud.

e = End of the program.
User can download file.

X = Input of the program.

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 7, July 2017

Input should be File which is uploaded by user.

Y = Output of the program.
User can download file if and only if user have both OTP and secrete key.

X, Y U

Let U be the Set of System.

U= {Client, OTP, Sk,}
Where, Client, F, R, T are the elements of the set.

Client = User
OTP = One Time Password
OTP is generated by system and required to user for downloading file.
Sk = Secret key
Sk is generated by system and required to user for view or downloading file.

= Failures and Success conditions.

Failures:
1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

Success:
1. Search the required information from available in Datasets.
2. User gets result very fast according to their needs.

X. TEST CASES

The following table shows the test cases of the Secured Access Control Using Two-Way Approach for Cloud Computing Services. It shows the expected result and actual result.

Test Case Id	Name	Purpose of Test	Expected Result	Actual Result	Status Pass or Fail
1	User login	To check whether user can access to system or not using valid and invalid credential	User only login with valid credential	User only login with valid credential, for invalid user it is throwing error	Pass
2	File selection	To check whether file	File must be	File is selected	Pass

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 7, July 2017

		which contains data is selected or not	selected	successfully and users go to next page	
3	Send request for upload key	To check whether upload key request is send successfully or not	Request must be send to authority	Request send successfully to authority	Pass
4	Send request for download key	To check whether download key request is send successfully or not	Request must be send to authority	Request send successfully to authority	Pass
5	Send request for OTP	To check whether OTP request id send or not	OTP request must be send and OTP comes on users mobile number	OTP request send successfully and then OTP comes on users mobile number	Pass
6	Other file download	To check whether other files are downloaded or not after entering valid OTP and key	Files must be downloaded	Files downloaded successfully	Pass

Table 1: Test Cases

XI. EXPERIMENTAL SET UP AND RESULT TABLE

- **Result Table**

Sr. No.	File Length (Bytes)	Time (ms)
1	1702193	902
2	1116625	422
3	64	238

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 7, July 2017

4	1702193	841
5	1702193	918
6	61	185
7	19474	1138

Table 2: File Downloading Time

Above table shows that how much time required for merging all fragments related to that file and downloads that particular file. We take file length i.e. size in bytes and time is in milliseconds (ms).

- **Result Graph**

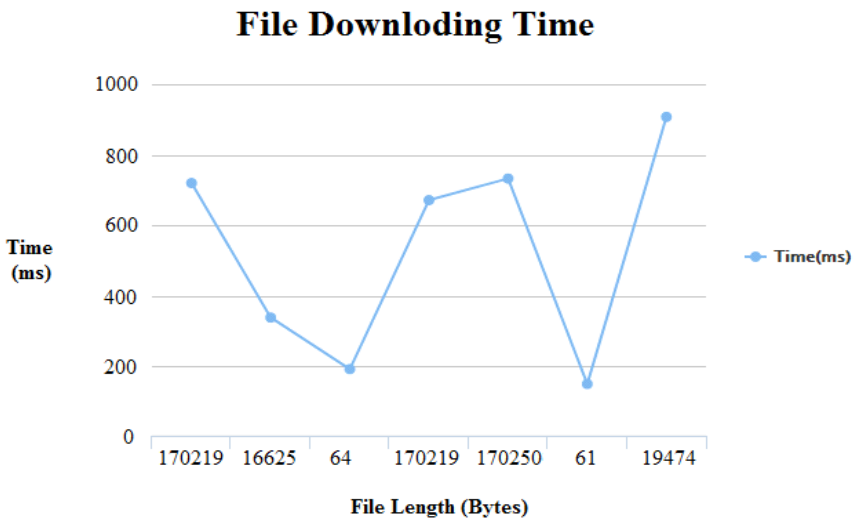

Figure 2: Result Graph of File Downloading Time

The above Figure 2 shows that the File Downloading Time of proposed system. As can be seen in Figure 2 x-axis represent File Length in Bytes and y-axis represents time in milliseconds (ms). Figure 10.1 shows that how much time is required for merging all fragments and download the particular file .The above graph shows how much system need time when user want to download any file.

XII. CONCLUSION

We proposed the Secured Access Control Using Two-Way Approach for Cloud Computing Services to achieving security in distributed cloud storage. Based on the characteristic based access control system, the proposed two-way access control framework has been recognized to not just give power the cloud server to limit the way-in to those clients with the same arrangement of properties additionally save client protection. Moreover, we use Identity Based Encryption (IBE) algorithm to encrypt user data or file. IBE is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). We also apply Cauchy approach for data storage on cloud. With the help of Cauchy approach we save storage (memory) space. Point by point security examination demonstrates that the

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 7, July 2017

proposed access control framework accomplishes the coveted security prerequisites. We leave as future work to assist enhances the productivity while keeping every single pleasing part of the framework.

REFERENCES

1. Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", IJCCSA, Vol.3, No.4, August 2013.
2. Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING", IJCCSA, Vol.3, No.2, April 2013.
3. Mr. Ankush Kudale, Dr. Binod Kumar," A STUDY ON AUTHENTICATION AND ACCESS CONTROL FOR CLOUD COMPUTING", Vol. 1(2), July 2014 (ISSN: 2321-8088).
4. Harvinder Singh1, Amandeep Kaur2," Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication", Volume 4 Issue 11, November 2015.
5. Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou,"k-times attribute-based anonymous access control for cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.
6. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp.Secur. Privacy, May 2007, pp. 321–334.
7. D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
8. D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004.
9. J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.
10. J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in Proc. 16th ACM Conf. Comput.Commun.Secur.(CCS), Chicago, IL, USA, Nov. 2009, pp. 131–140.
11. J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.
12. K. Liang, W. Susilo, and J. K. Liu, "Privacy-preserving ciphertext multisharing control for big data storage," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.
13. J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, and B. Srinivasan, "Secure sharing and searching for real-time video data in mobile cloud," *IEEE Netw.*, vol. 29, no. 2, pp. 46–50, Mar./Apr. 2015.
14. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 743–754, Apr. 2012.
15. Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," *IEEE Trans Multimedia*, vol. 15, no. 4, pp. 778–788, Jun. 2013.