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 5, May 2018

Two-Factor Data Security Protection Mechanism for Cloud Storage System

P.P. Dandavate[*], Manas Pandit[**], Ashish Dalbhanjan[**], Vishal Dighe[**]

Department of Computer Engineering, TSSM's PVPIT, Pune University, India

ABSTRACT: In our system, proposed system exhibit another fine-grained two-variable approval (2FA) get the opportunity to control structure for electronic circulated Computing associations .We introduced user cannot access data without a secret key and a light weight security device like a finger print scanner ,and user need both secret key as well as a light weight security device for accessing of any file.If secret key and user thumb match with registered image then user can view file as well download it. admin store file in fragmented format also with its replica. If some of uploaded files fragment data loss then we can get backup of our data from replica .We also introduced, If we want to acess any file in a a particular location and for a particular time then we can do it.from user, security key is stolen or delete from a mail then user can revoke this security key from admin by request. Admin will accept the request and send key on users mail so user can download the file.

KEYWORDS: Two-factor, factor revocability, Fine-grained,security, cloud storage

I. INTRODUCTION

A.BackGround

In our system, we proposed system exhibit another fine-grained two-variable approval (2FA) get to control structure for electronic distributed Computing organizations. Specifically, we proposed system proposed 2FA get to control structure, a property based get to control framework is executed with the need of both a customer secret key and a lightweight security device. new user can't get to the structure in case they don't hold both, the instrument can enhance the security of the system, especially in those circumstances where various customers have a similar PC for online cloud organizations. In a same trademark based control in the structure too enables the cloud server to restrict the access to those customers with a similar proposed system to perform new activity of properties while saving customer insurance, i.e., the cloud server just understands that the customer fulfills the required predicate, however no piece of information has on the exact identity of the user.

B.Motivations:-

1. The new worldview of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web-based cloud services.
2.As sensitive information might be put away in the cloud for sharing reason or advantageous access; and qualified clients may likewise get to the cloud framework for different applications and administrations, user authentication has turned into a basic segment for any cloud framework.
3.A user can revoke a secret key if key is deleted by the user.
4. A user is required to login before utilizing the cloud benefits or getting to the sensitive information put away in the cloud. There are two issues for the traditional record/secret key based framework.
5.First, the traditional account/password-based authentication is not privacy-preserving.
6.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. To solve this problem we proposed two factor access controls.

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 5, May 2018

C. Objective and Scope

1.To provide a high security to data we propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device i.e. Scanner and secret key.
2. When any file is uploaded, that file store on a cloud in a fragmentation format so,data become more secure.
3.If the secret key is deleted by the user,then we can revoke it.
4.Our system provide more data security as compare to other existing system.
5.Scope of our project , provide security with 2 FA using secret key and biometric thumb.
6.we can use application our application for security related systems

II . LITERATURE SURVEY

1.Dynamic credentials and cipher text delegation for attribute-based encryption:
An architecture that ensures the privacy of data stored in cloud storage. The proposed architecture can directly applicable to existing clouds without any modifications or any changes in cloud database. It can be process that connects directly to an encrypted cloud database without an intermediate devices or systems with geographically distributed clients and it also allowed executing independent and operations including those changing the database structure. The proposed system eliminates the limit on scalability, and availability properties of cloud based solutions.

2.A CCA-secure identity-based conditional proxy re-encryption:
In A CCA-secure identity-based conditional proxy re-encryption without random oracles proposed a short and efficient Certificate Based Signature (CBS) scheme to improve level of trust in cloud environment. This scheme was need one group element for public key and the signature size and it reduced the public information to one group elements for each and every user in the cloud environment. This key size is smaller than the PKI based signature scheme because it needs one group element for generation of public key and the another group element is needed for the certificate.

3.Unidirectional chosen-ciphertext secure proxy re-encryption:
At a solitary directional picked ciphertext secure intermediary re-encryption depicted unidirectional intermediary re-encryption plans. This plan is with picked figure content security in the standard model. The two commitment of this proposed framework is fitted a unidirectional expansion of the Canetti– Hohenberger security show and another is the means by which to change the plan to accomplish security. It gives extra properties like as non-intuitive brief assignments.

4. Distributed, concurrent, and independent access to encrypted cloud databases:
In Distributed, concurrent, and independent access to encrypted cloud databases .proposed an approach that overcomes the problem in Attribute-Based Encryption (ABE). In this introduced a cipher text delegation procedure that re-encrypted a cipher text based on the public information and analyzed the problem of revocable in existing Attribute-Based Encryption technique. Based on the analysis it is necessary for first fully secure construction, it modifies an existing Attribute-Based Encryption scheme. Thus this approach was used for revocation on stored data.

5.Certificate-based encryption and the certificate revocation problem:
In Privacy-preserving public auditing for secure cloud storage proposed a solution for problem of efficiently delegating in key revocation and generation in Identity Based Encryption (IBE) scheme. In a proposed realization of RHIBE, it is constructed based on the scheme called Boneh-Boyen HIBE (BB-HIBE) scheme. Any size of cipher text and revocation cost was same for both RHIBE and BB-HIBE schemes. But in RHIBE allows hierarchical structure of entities and selective ID was protected under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

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

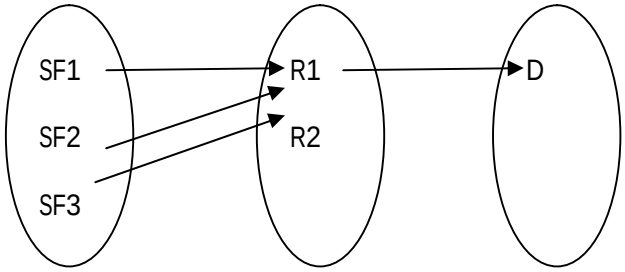
International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

III. MATHEMATICAL MODEL



SF1: Search File:eg Sachin.
SF2: Search File: eg Dhoni
R1: Get accurate result
SF3: Search File:eg salman
R2: Error in the accessing of the system

Set Theory:-

S={s, e, X, Y,Φ}

Where,

s = Start of the program.

1. Log in System
2. Search the name which we want to search.

e = End of the program.

File which is search by user.

X = Input of the program.

Input should be user file name.

Y = Output of the program.

Proper name of file which is store in cloud will match then user can download correct file

X, Y $\in$ U

This module help the admin to upload his file with encryption using AES algorithm. The User to view the uploaded files and downloaded files

Let U be the Set of System.
U= {SF1,SF2,SF3,R1,R2,D}
Where SF1,SF2,SF3,R1,R2 are the elements of the set.
SF1=Search first File
SF2= Search second File
SF3= Search Third File
R1=Get Accurate result
R2= Error in the accessing of the system
D=Download File

Failures:

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

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 5, May 2018

3. Software failure.

Success:

1. We get file which want to search.

2. We get accurate file.

Above mathematical model is NP-Complete.

IV.EXISTING SYSTEM APPROACH

In existing system cloud computing are not great advantages, there are meanwhile also concerns about security and privacy especially for web-based cloud services. 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, authentication of user has become a critical component for any cloud system. the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password-based authentication is not privacy-preserving. Then, it is we known that privacy is an essential feature that must be considered in cloud computing systems. Another system, 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. In existing, Even though the computer may be locked by a password, it can still be possibly guessed or stolen by undetected malwares.

V.PROPOSED SYSTEM APPROACH

In the System, 4 modules are present authority,trustee,user,cloud server.

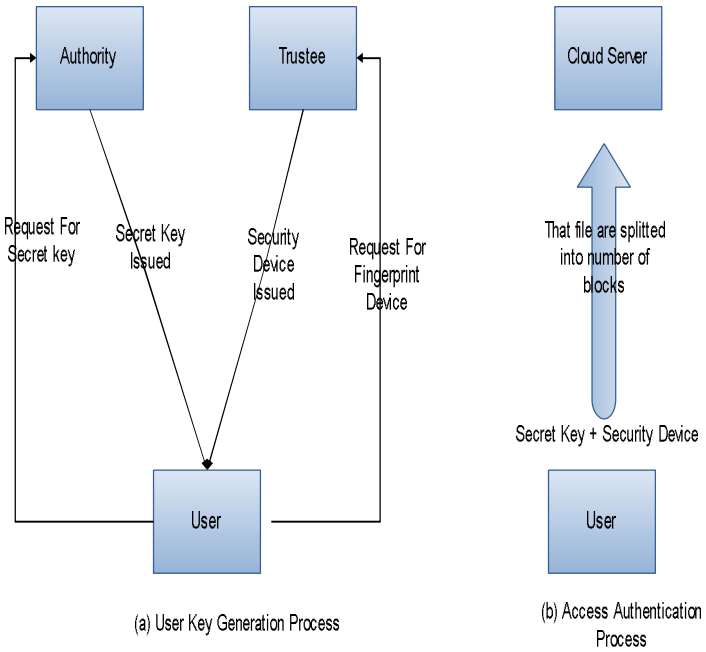


Fig.1 Block Diagram of Proposed System

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 5, May 2018

User : User register to the system with scanning finger print and send the request to activate him. User login to system with first time by OTP and gives scanned image if they matched user logged in to system. User view files and send request for secrete key to admin. When users get secrete key user can download the file by entering secrete key. If secrete key lost then user can again request for key.
Trustee: Trustee login to system and accept the user request for his entry in system.
Admin: Admin login to system and upload file .Admin can view all file details. He gets the request from user for secrete key and send the secrete key to users mail.
Cloud Server:-Store the data on a cloud server.

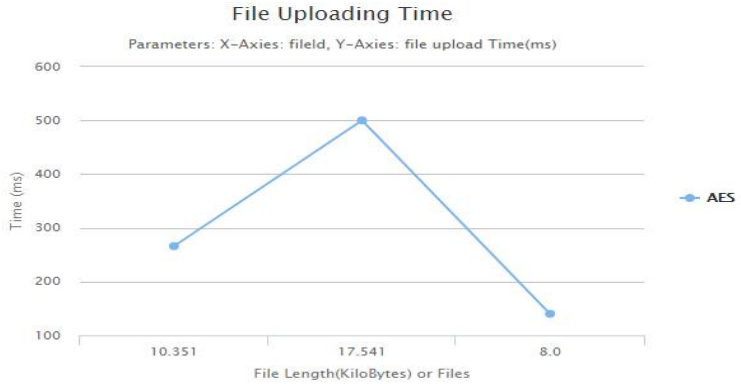
VI. SYSTEM ANALYSIS

In our experimental setup, In table 1,find out different file upload and time required for time for uploading that file. In our experimental setup, in our system first is uploading file size and time for that file.

Sr.No	File Size(Kb)	Time(ms)
1	10351	226
2	17541	500
3	8500	140

Table1: File Uploading Time and Size

From above data, In graph 1,we can see file size of 1 is 10351 kb is required time uploading is 226 ms, and file size of 2 is 1751 kb is required time uploading is 500ms



In our experimental setup, In table 2,find out different file download and time required for time for uploading that file. In our experimental setup, in our system first is uploading file size and time for that file and so on.

Sr.No	File Size(Kb)	Time(Sec)
1	10351	22
2	25000	30
3	8000	10

Table1: File downloading Time and Size

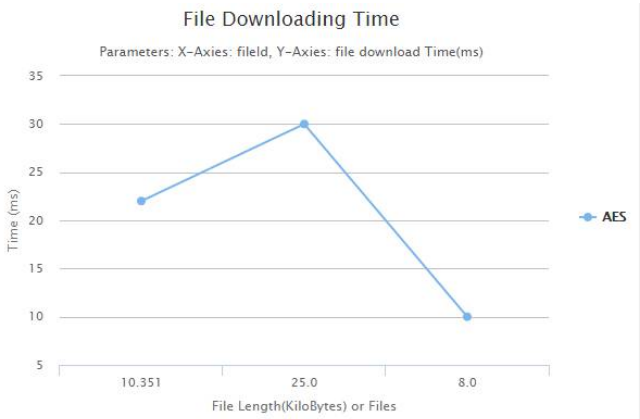
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

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 5, May 2018



From above data, In graph 2,we can see file size of 1 is 10351 kb is required time uploading is 22 second, and file size of 2 is 25000 kb is required time uploading is 30 sec. and so on.

VII. CONCLUTION

In a cloud computing security of data is more important point. We propose a fine-grained two-factor access control protocol for web-based cloud computing services, using a lightweight security device like finger print scanner and secret key.For a registration of we provide biometric thumb and otp.after proper validation user can acess any file on a cloud.We also provide downloading of any file two level security like thumb scanner and secret key.so we provide more security to our data,File can store on cloud in a fragmentation format.User can revoke the secret key .so we maintain our system more secure and reliable.

ACKNOWLEDGMENT

This work is supported in two factor data security and protection mechanism in cloud services system of any state in india. Authors are thankful to Faculty of Engineering and Technology (FET), SavitribaiPhule Pune University,Pune for providing the facility to carry out the research work.

REFERENCES

[1] A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and cipher text delegation for attribute-based encryption. In: Advances in Cryptology–CRYPTO 2012. Springer Berlin Heidelberg. 2012; 199-217.
[2] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles," in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–
246.
[3] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," IEEE Trans. Inf. Theory, vol. 57, no. 3, pp. 1786–1802, Mar. 2011.
[4] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent, and independent access to encrypted cloud databases," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437–446, Feb. 2014.
[5] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Proc. Int. Conf. Theory Appl. Cryptographic Techn. 2003, pp. 272–293.