Single key Based Secure Data sharing in Cloud

[1]Mr.B.V.Satish Babu Asst. Professor,[2]p.Tejaswani,[3]m.Sirisha,[4]b.Poornima

[1,2,3,4]*Department of Computer Science Engineering,*
[1,2,3,4]*Andhra Loyola Institute of Engineering and Technology, Vijayawada*

Abstrac—*Sharing of data is a general handiness property in storage cloud. In this paper, we show how to provide security, viably, and adaptably for data that has to be shared to others in distributed storage. In our application number of files is encrypted before uploading in to cloud storage. Another user who wants to access the shared files in cloud uses the single secret key which was send to his email. This single secure key is used to decrypt the files before they are downloaded*.

Keywords—*Cloud stockpiling, information sharing, KAC-based encryption, persistent encryption*

I. INTRODUTION

Storage clouds are getting predominance starting late. In huge business, there is a climb mainstream for sending data out to manage, that helps the key organization of corporate confidential data. It is moreover seen as a middle advancement apart of various online communities for individual security applications.

Nowadays, it is not hard to implement with the desire of complimentary records for accumulation, archive distribution or conceivably accessing from remote, in the limit measure greater than 25 GB .Along with the present remote advancement, customers can get to the greater part of records along with messages using wireless at any point in the world.

Including data security, a standard solution to cope with certification and depend on upon the server to materialize numerous approval (e.g., [1]), infers the sudden advantage uplifting that reveal complete data. In the form of shared inhabitance appropriated registering condition, things end up being shockingly more unpleasant.

Data originated from different clients are to encouraged in discrete virtual computing system (VMs) yet depend up on physical machine. Important data in a target virtual machine can be manipulated and stolen by starting another virtual.

According to reports, there are lots of changes in crypto based security arrangements which allow an evaluator to check and avail of archives for the advantage of data owner without leaking anything about the data [3], or without piggybacking off the data proprietor's identity [4] downloading the encoded data about the limit, then send it to others for the purpose of sharing, be that as it may it loses the estimation of circulated stockpiling. Customers may have the ability to get to benefits of offering data to others.

Regardless, of choosing a compelling and secure method to deal with share partial data in sharing is not all immaterial. Underneath we will take storage cloud "Drop box" for security.

II. LITERATURE SURVEY

Benaloh showed that encryption method is at first propose for transmitting many number of keys in convey circumstance. This kind of advancement is essential along with this we rapidly review its plan for derivation of keys. The acceptance of these keys for a course of different actions (which is a combination of all possible figure content models) is according to the accompanying [1].

A composite model of modulus is selected where entity **p** and entity **q** are two far reaching unpredictable prime numbers. An efficient secret key is selected unpredictably. Each type of class is correlated with a specific prime number. All of the prime numbers can be used set in overall public structure parameter. A strong size(S) key for set can be conveyed.

For those persons who have been allocated the get to rights for S' can be delivered. In any way, it is expected for the symmetric key cryptographic system setting. The substance provider needs to get the relating secret key to encode data which is not sensible for a few applications. Since technique is used to make a riddle regard instead of several open/puzzle keys, it is fuzzy to find how to implement this idea for the purpose of open encryption of key plot.

As a result, we observe the arrangements that help to endeavor to reduce the key size for fulfilling concept in symmetric-key encryption, e.g.,

[4]. Regardless, sharing which is unscrambling power should not be considered as stress in these arrangements. Identity-based encryption (IBE) is a type of open key encryption where overall (pk)public key of a customer can be used as a character string assigned to customer).

Identity based encryption that holds an expert riddle key which issues a secret secure key to every customer in regards and relative customer character. The actual key provider can make use of overall public key parameter and customer character to scramble the given message. The receiver can unravel the message by his riddle key.

Guoet al. endeavored to produce identity based encryption with key accumulation. In their arrangements, KAC is restricted as in all generated keys has to be originate from distinct sources. In the mean while there is an availability of exponential number of entity identities and henceforth confidential keys, that only a polynomial generated based number of them can be amassed .This in a general sense fabricates the costs of securing and transmitting figure works, which is unreasonable all around, for instance, shared conveyed stockpiling.

As another method to deal with, we have to implement hashing methods to string meaning of the chipper class, besides, keep hash method again and again until we have a prime number is gotten as a result of the hash based work. We decided to determine, our arrangements incorporate reliable figure content size.

Security methods in the standard model can be soft IBE [10], one easy single insignificant confidential key can unscramble figure compositions mixed under various identities that is closed in a particular metric method, any way it is not for a self-decisive course of action of elements and thus it is not possible to arrange with our idea of key based accumulation.

III. PROPOSED SYSTEM

To arrange a gainful open key encryption plot which supports versatile assignment by using any number of subset of the figure compositions are decode capable by a predictable size of unscramble key (delivered by the proprietor of the ace puzzle key[1]."

We deal with this problem by including a remarkable kind of open key based encryption in which we call them as key-add up to cryptosystem. In this method, customers scramble a selected message under an open key, and additionally by using an identifier of figure called class.

That infers actual figure compositions are additionally orchestrated into unmistakable classes. The key owner holds a important element called expert secure key.

This key can be making used to think secure keys for different chipper classes? More basically, the isolated key will have an aggregate key which is consider traditionalist key for a lone class; however adds up to the drive of various such secure keys, i.e., the unscrambling control under any subset of figure substance classes.

With our answer, Alice sends to Bob ,a single aggregate secure key by methods for a protected email. We can then download the mixed photos from Alice's account of Dropbox space and after that utilization this total key us used to unscramble these scrambled photographs. It is more secure.

Decrypting of key is sent by means of a protected channel and kept mystery. It is a productive open key encryption plot which underpins adaptable delegation.

With our solution we encrypt all the files before uploading in the drop box, another user who wants to download file enters the single secret key which was send to email then files are view in decrypted manner.

Different sizes of cipher text open key, Alice master public key, what's more, total key in our KAC plans are all of steady based measure. Past outcomes may be used to accomplish a comparative property including a steady constant size of decoding key, yet the different classes has a need to adjust to some specific predefined in different levels of relationship. Our work is easily adaptable and limitation can be is wiped out, and no extraordinary relation is required that exist between systems. The detail and other related works can be found.

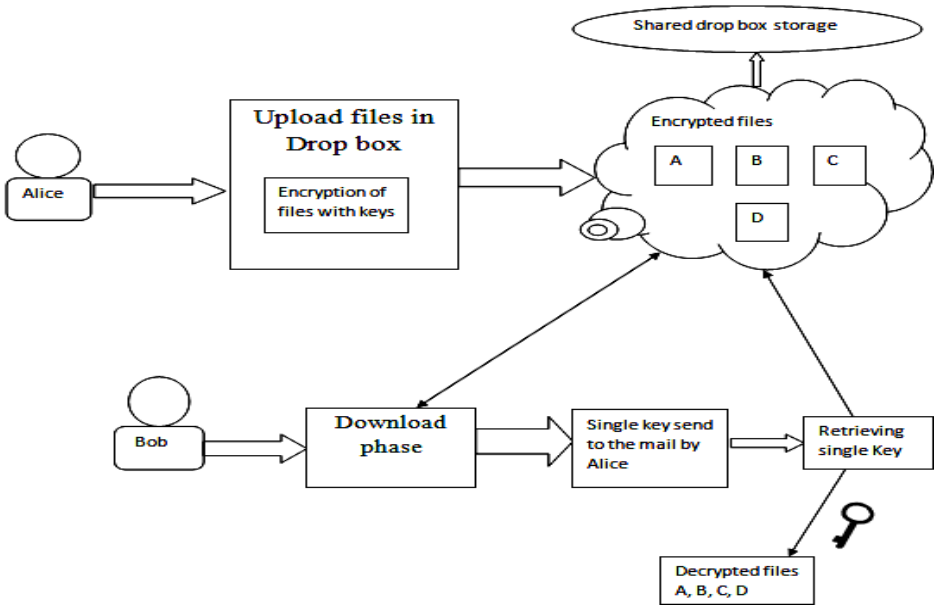


Fig 1: Frame work of the proposed system

Here we propose a method called KAC plan (Figure 1) with possible various security of levels and augmentations in this paper. All included developments can be demonstrated to secure in the proper standard model.

For example Alice is one of user in drop box she wants to upload her files in drop box but she did not relay with the security method given by the drop box. So she wants to convert all files in to cipher before starting of uploading. So she encrypted her files with her own distinct keys and then uploaded in drop box. Bob is also one of the users in drop box he wants to download some of files of Alice. By clicking on download button a single key is sent to mail by Alice he retrieves the single key and then decrypts the files which he has chosen.

IV. RELATED WORK

The PHP module executes the script, which then passes on the result as HTML back to your program, which you see on the screen. Here is an essential PHP layout which outlines the technique.

First we need to create an account in Drop box by giving username and password and then login to the drop box account. we need to create an app in Drop box API for implementing our application by the URL . " https://www.dropbox.com/developers/apps"and then click on create an app it displays choose an API it displays two apps that is Drop box API and Drop box Business API in that we need to choose Drop box API since our application is based on storing of files. We need to give name to the app which we create.

When we click on create an app it displays app key and secret key which is most essential part in our application, we need to store app key and secret key for generating a "single secret key".

For storing of registration details we can use XAMPP server or WAMPP server in our application we choose XAMPP server.

The main goal in our application is to provide security to data or files which are stored in cloud. For achieving this we are encrypting files or data with distinct keys before uploading files in Drop box, and then retrieving the same files with a single secure key.

We need to create tables for storing the registration details. Login to the Homepage using (local host/dropboxapi /Home.php) and It displays the synopsis of project in "Homepage" [Output1]. Click on to the "Login" button it displays username and password and at the bottom it displays new Registration.

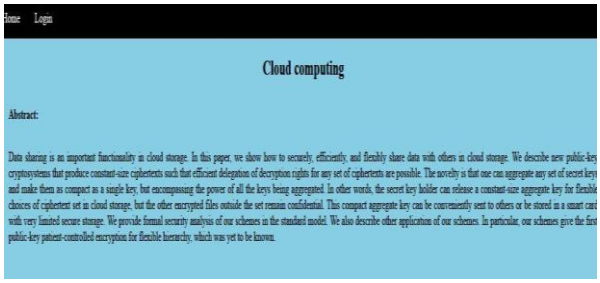
User need to "Register" with their details and then login it displays welcome along with their Email-id. The page contains three buttons they are "upload and download and Logout".

If user needs to upload their files or images they need to click on "Upload" button it displays list of files present in your PC [Output2]. Select the File and click on "Submit" button it again asks for "Do you really want to upload the file" if yes click on submit it displays file uploaded successfully.

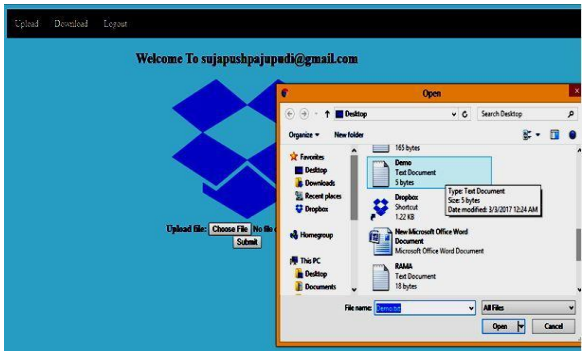
The file has been uploaded in the encrypted Form. In drop box and it displays a popup message in drop box [Output3].If the user wants to download the files then click on "Download" button it displays all the uploaded files in your drop box and then select the multiple files to download [Output4] and click on download button it asks the key which have been send to the Email-id for downloading of selected files.

Enter the key and click on submit button if the enter key is correct then it displays a message downloaded successfully if not it displays a message wrong key. The files which are been downloaded is in the decrypted form [Output5].

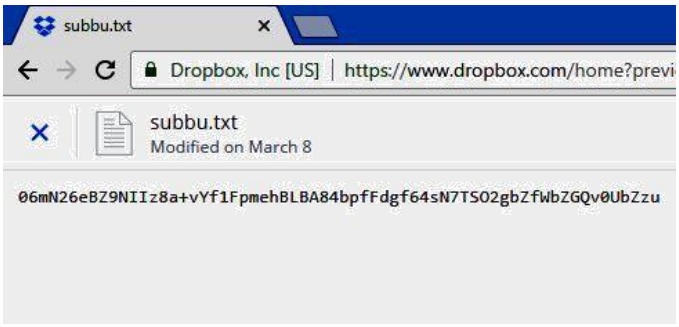
V. RESULTS



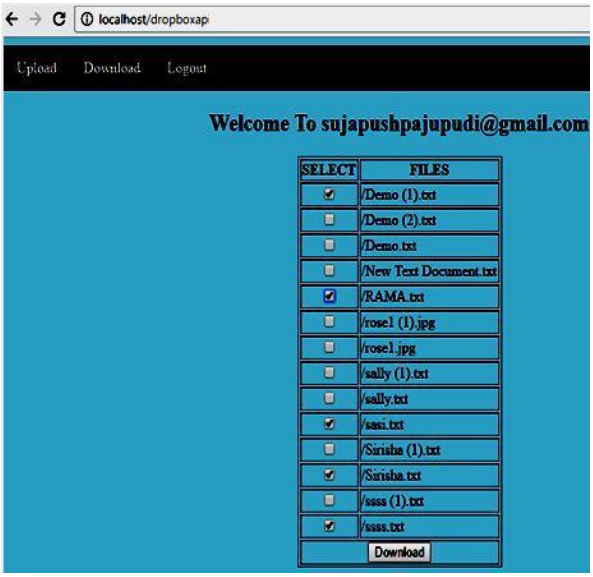
Output1: Homepage to login



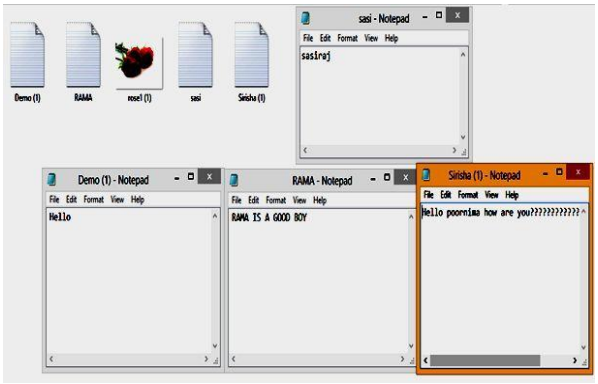
Output2: Uploading of files in drop box



Output3: After uploading file is in Encrypted format



Output4:select of files for download



Output5:selected files downloaded in decrypted format

VI. CONCLUSION AND FUTURE WORK

The most effective method to ensure clients' information protection is a focal question of distributed storage. With more numerical gadgets, cryptographic arrangements are getting more versatile and as often as possible incorporate diverse keys for alone application. In this paper, we consider how to "pack" mystery enters in broad daylight key cryptosystems which bolster assignment of mystery keys for various figure content classes in distributed storage. Notwithstanding which one among the power set of classes, the delegate can essentially get an aggregate key of un faltering size.

An impediment in our work is the predefined bound of the quantity of most extreme figure content classes. In appropriated stockpiling, the amount of figure messages when in doubt grows rapidly. So we have to sufficiently spare figure content classes for the future extension. Else, we have to grow people in general key as we portrayed in Section in spite of the fact that the parameter can be downloaded with figure writings, it would be better if its size is free of the most extreme number of figure content classes. On the other hand, when one bears the relegated enters in a wireless without using remarkable trusted in gear, the key is induce to spillage, delineating a spillage solid cryptosystem yet allows beneficial and versatile key assignment is moreover a charming heading.

VII. 7. REFERENCES

[1] S.S.M. Chow, Y.J. He,L.C.K. Hui, and S.-M. Yiu, "SPICE

[2] Simple Privacy-Preserving Identity-Management for Cloud Environment,"Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

[3] L. Hardesty, Secure Computers Aren't so Secure. http://www.physorg.com/news176107396.html, 2009.

[4] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[5] S.Palani, E.Sujith, Poun Kumar.V "Scalable Data Sharing in Cloud Storage using Key Aggregate Cryptosystems". **IJCTT** V22(3):140-146, April 2015. ISSN:2231-2803.

VIII. VIDEO AND WEB REFERENCES

[6]https://www.youtube.com/watch?v=wfb6h9JyhBY

[7]https://www.w3schools.com/php/php_looping_for.asp

[8]https://php.net/manual/en/function.file

[9]https://www.dropbox.com/developersv1/core/start/php

[10]https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.html

[11]http://monkeylogic.com/whole-file-encryptiondecryption- with-php/

[12] https://www.youtube.com/watch?v=J2-neLr7MXM

B.V.Satish,currently working as an assistant professor in "Andhra Loyola institute of Engineering and technology". His areas of interests include cloud computing, Big data analysis, Image processing, IOT, Distributed systems (DS), Network & Computer programming, server programming

Ms. P.Tejaswani currently pursuing B.Tech degree in Computer Science and Engineering at Andhra Loyola Institute of Engineering And Technology (ALIET). Her research interest include cloud computing.

Ms.M.Sirisha currently pursuing B.Tech degree in Computer Science and Engineering at Andhra Loyola Institute of Engineering And Technology (ALIET). Her research interest include cloud computing.

Ms. B.Poornima currently pursuing B.Tech degree in Computer Science and Engineering at Andhra Loyola Institute of Engineering And Technology (ALIET). Her research interest include cloud computing.