RESEARCH ARTICLE OPEN ACCESS

Aggregate Secured Key Cryptosystem on cloud with Dynamic Data Sharing

Yateesh Kumar D G*, Dr. Thippeswamy G R**, Prajwal R***,
Prashanth C K****, Subramaniyam R*****
*(Department CSE, DBIT, VTU, Bengaluru
yateeshkumar142@gmail.com,
prajwal.praju7783@gmail.com,
prashanthck321@gmail.com,
rsubhisubha02@gmail.com)
**(Professor, Department CSE, DBIT, VTU, Bengaluru
thippeswamygowda@gmail.com)

----------------------------------*************************----------------------------

Abstract:

Cloud application be the next peer groupof architecture in the IT enterprisetechnologies based on self-serviced, ubiquitous network access, resource pool, resource elasticity and transferrable risk. Cloud is one of the primarycharacteristic of new computing model, where entireinformation is to be centralized, based on the user perception to both individual user and IT enterprise,so that design and describe, how to store and access the data within the cloud.For elasticand on demandtechniques are utilized to achieve Dynamic data sharing in cloud, so in this paper, we developed attributebased encryption (ABE)techniques, so that user can keep track of very high sensitive data on confidentiality against untrusted servers.

***Key words* — Security, TPA, Privacy, Cryptosystem, Cloud Security**

--------------------------------*************************--------------------

I. INTRODUCTION

Cloud application be the next peer group of architecture in the IT enterprised technologies based on self-serviced, ubiquitous network access, resource pool, resource elasticity and transferrable risk.Cloud is one of the new computing model for centralized data, based on user perspective towardsIT enterprises, manipulate the data remotedly in a cloud, here cloud provides the flexible, and secure manner to bring the applications so benefited more over cloud has many benefits with geographical self-sufficientlocations, prevention of resources like, expenditure on hardware, software, personnel maintenance, and so on.

Cloud application will provide many advantages than other traditional applications than ever, but regarding on security perspectives new challenges evolved based on outsourced data. Basically cloud service provider in an application is a separate administrative entity, where data manipulation is essentiallygive up the owner's data control.

II. LITERATURE SURVEY

Attribute-based Encryption (ABE) technique to be consideredfor trustworthy cryptographical tools,where itsecurecontrol on owner's data to be stored in cloud.

Threshold multi-authority CP-ABE access control scheme (TMACS) is utilizedfor public cloud, where multiple authority can have enabledtogether to alterand used unique attributes. TMACS, build a hybrid model, in which it fulfils the develop the attributes approaching from various authorities to achieve security [1].

Cipher text updation in bidirectional re-encryption method augmented to analysis and investigation in security perceptiveness will shows how to verify and adopt security vulnerabilities [2].

AnonyControl is a security technique to secure bilinear data transaction, i.e. AnonyControl is a unidentified partial uniquenessdata (attributes) toreveal each ability [3].

CiphertextPolicy Attributebased Encryption (CP-ABE) is most versatile technologytocontrol the access of data in cloud, i.e. provides direct access control policies to data owners. The designing of CP-ABE scheme is very significant andwell-organized data access control for multiple authorized cloud system [4].

Data sharing is a multiple owner approach, whereuser can preserve the data and specify the confidentialityin cloud for challenged issues [5].

III. SYSTEM ARCHITECTURE

The proposed architecture is distributed into 4 main modules they are: owner, end user, TPA, cloud server.Data owners are the one who uploads the security based files along with a filename and encrypts it and saves it. Later the end user has to register/login into his/her portal and ask for the particular file downloading secret key with data owner name and file name. The request is then sent to TPA (Third party auditors) and there TPA's generate the secret key and once that is done user will get the secret key and then only he/she can download the file.

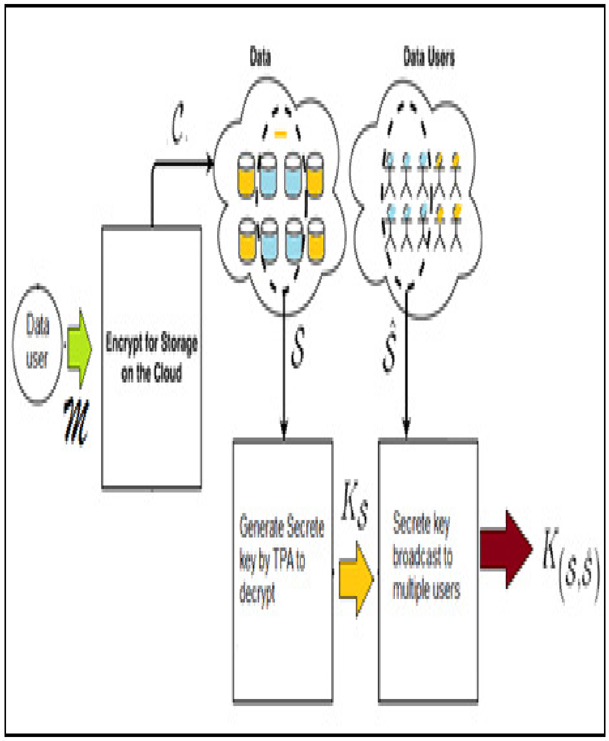

Data
Data Users
C
S
Ŝ
Data user
m
Encrypt for Storage on the Cloud
Generate Secrete key by TPA to decrypt
Ks
Secrete key broadcast to multiple users
K(S,Ŝ)

Fig 1: System Architecture

The proper data flow between TPA, Data owner, e ed architect verifies the request and generates the secret key. Once the SK (Secret Key) is generated, then the end user can enter the secret key and download the file that was being requested.

File Upload

In Cloud application storage of data might be the important service, where data is alter, retrieve and updated the services remotely via internet, i.e.Cloud services can permit the end users to store very important files via internet, so the end users can access and uploadany information in its geographic locations.

Cloud Server:

Cloud service provider (CSP) is to offer considerable data storage space and computational property for cloud servers, it is working very similar to the physical servers.

Third Party Auditor's (TPA) Request:

TPA is a checker tool, it function towards on Private auditing and Public auditing, i.e. Private auditing can accomplish higher level security services, where as public auditing permit any users can access the cloud services, not only specific user.

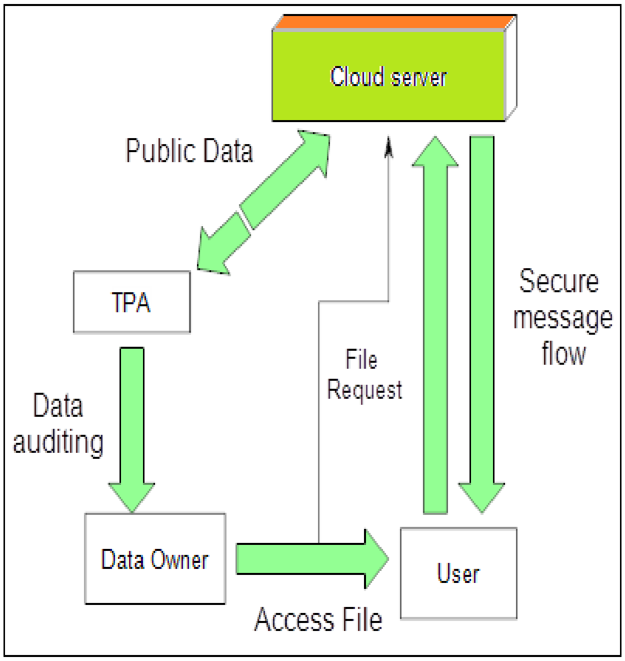


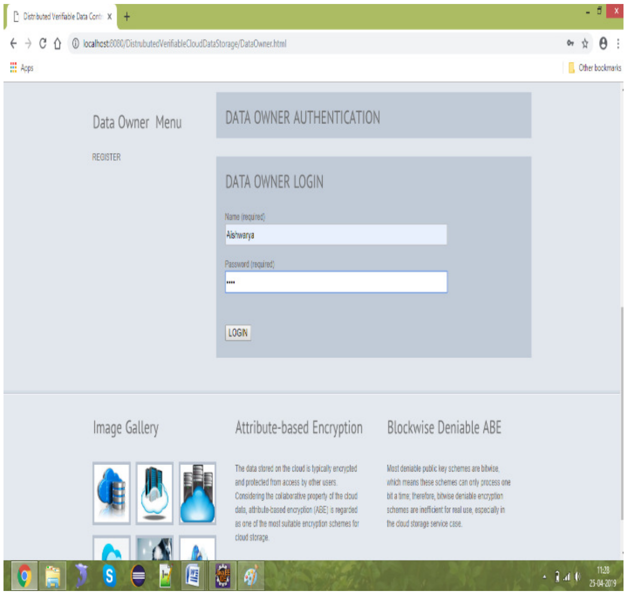
Fig. 2. Data flow diagram

Message Authentication Code (MAC) Request:

Message authentication code is a tiny chunk of information, it is utilize to authenticate theinformation, sometimes the MAC algorithms, is also called ascryptographichash function, where it owns secret key has input which is verify and authenticated by an arbitrary messagelength and executes the outcome. Basically the MAC algorithm keep track of both data integrity and authenticity of messages.

IV. RESULT ANALYSIS

For the execution of proof of concept by the application, below snapshots are executed, where data owner can login with user account credentials, like.


Distributed Verifiable Data Cont
localhost:8080/DistrubutedVerifiableCloudDataStorage/DataOwner.html
Apps
Other bookmarks
Data Owner Menu
REGISTER
DATA OWNER AUTHENTICATION
DATA OWNER LOGIN
LOGIN
Image Gallery
11:28
25-04-2019

Name (required): Aishwarya

Password (required): ••••

Attribute-based Encryption

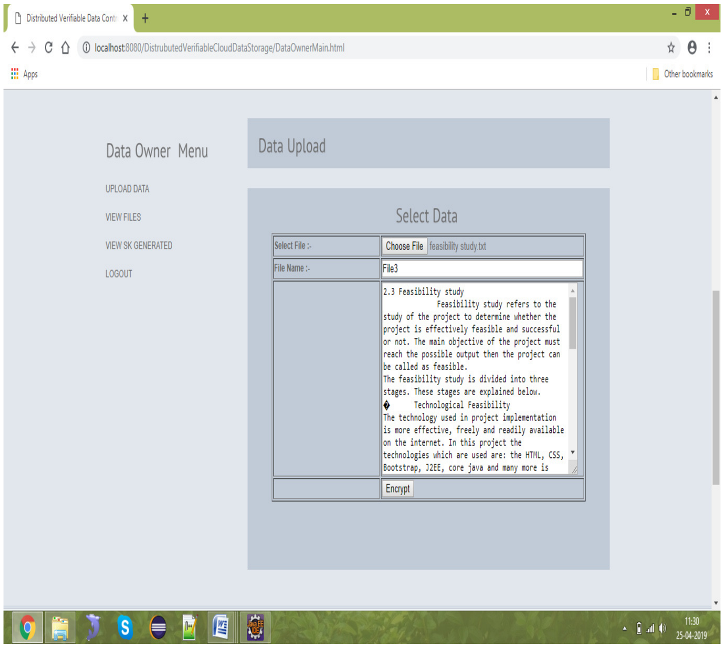
The data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage.

Blockwise Deniable ABE

Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case.

Fig.3 Data owner uploads file page

Here the usercan upload and retrieve the files on the cloud server by requesting for the download key.



Select File :- feasibility study.txt

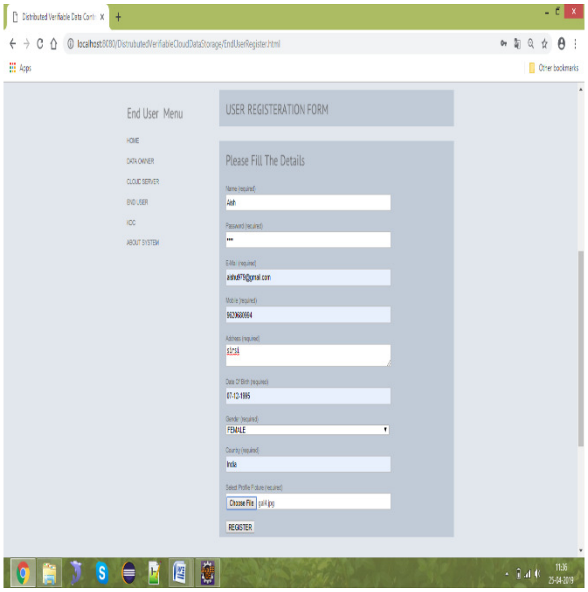
File Name :- File3

```
2.3 Feasibility study
            Feasibility study refers to the
study of the project to determine whether the
project is effectively feasible and successful
or not. The main objective of the project must
reach the possible output then the project can
be called as feasible.
The feasibility study is divided into three
stages. These stages are explained below.
�       Technological Feasibility
The technology used in project implementation
is more effective, freely and readily available
on the internet. In this project the
technologies which are used are: the HTML, CSS,
Bootstrap, J2EE, core java and many more is
```

Fig.4 Encryption of file data page

The file data is uploaded and it is then encrypted and stored successfully.After uploading the file by data owner, if any user wants to retrieve the file, users must register themselves, then only user can login with their user credentials.

.


Distributed Verifiable Data Cont
localhost:8080/DistrubutedVerifiableCloudDataStorage/EndUserRegister.html
Apps
Other bookmarks
End User Menu
HOME
DATA OWNER
CLOUD SERVER
END USER
KDC
ABOUT SYSTEM
Choose File
REGISTER

USER REGISTERATION FORM

Please Fill The Details

Name (required): Aish

Password (required): ***

E-Mail (required): aishu979@gmail.com

Mobile (required): 9620680994

Address (required): sirsi

Date Of Birth (required): 07-12-1995

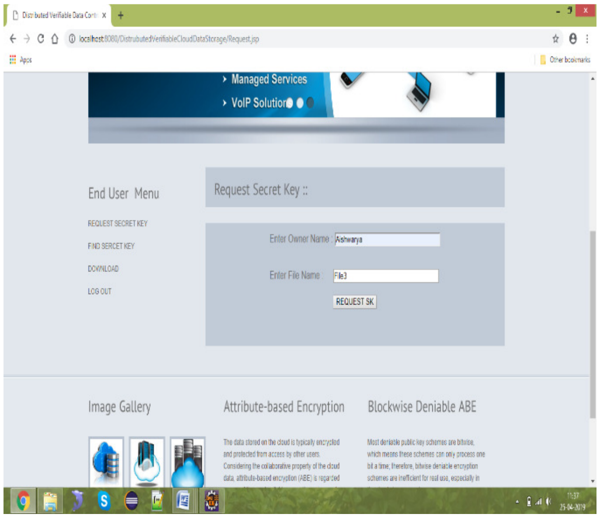
Gender (required): FEMALE

Country (required): India

Select Profile Picture (required): gal4.jpg

Fig.5 End User Requests the Key

Once the end user registers he/she can login to their account credentials, then only user can demandfor the secret key of the particular file by specifying the file name and file owner name.



Request Secret Key ::

Enter Owner Name : Aishwarya

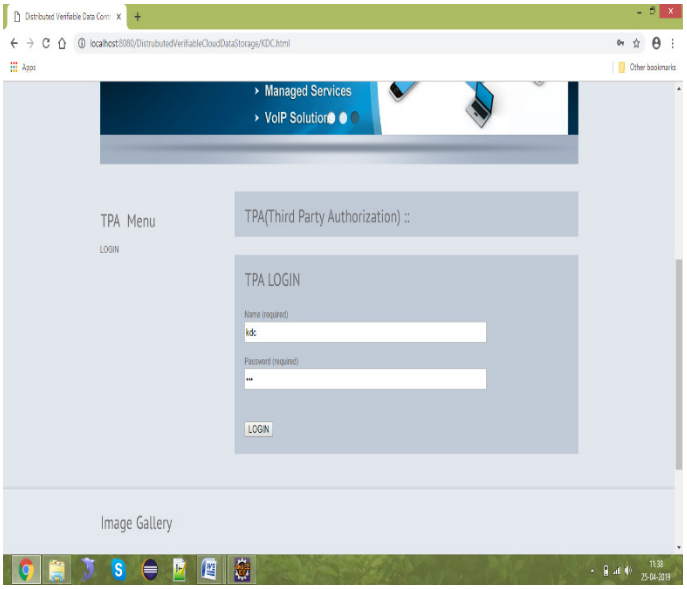
Enter File Name : File3

The data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded

Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in

Fig.6 Request Sent To Third Party Auditor

Once the end user presses the button “REQUEST SK” the request is sent to TPA (Third party auditors).Third party auditors login to generate the secret key.


Distributed Verifiable Data Cont
localhost:8080/DistrubutedVerifiableCloudDataStorage/KDC.html
Apps
Other bookmarks
Managed Services
VoIP Solutions
TPA Menu
LOGIN
LOGIN
Image Gallery

TPA(Third Party Authorization) ::

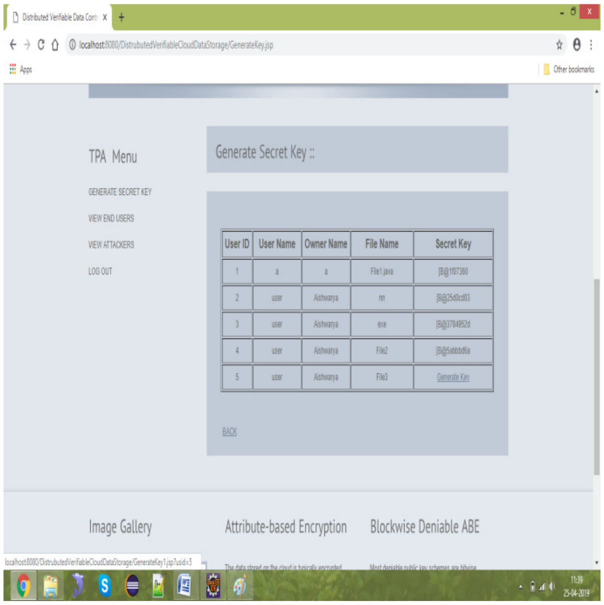
TPA LOGIN

Name (required): kdc

Password (required): ***

Fig.7 Third Party Auditors Generates SK

Once the user will receives the request from particular user, the applicationwithin the TPA will generates secret key to that specific user.


Distributed Verifiable Data Cont
localhost:8080/DistrubutedVerifiableCloudDataStorage/GenerateKey.jsp
Apps
Other bookmarks
TPA Menu
GENERATE SECRET KEY
VIEW END USERS
VIEW ATTACKERS
LOG OUT
BACK
Image Gallery
Attribute-based Encryption
Blockwise Deniable ABE

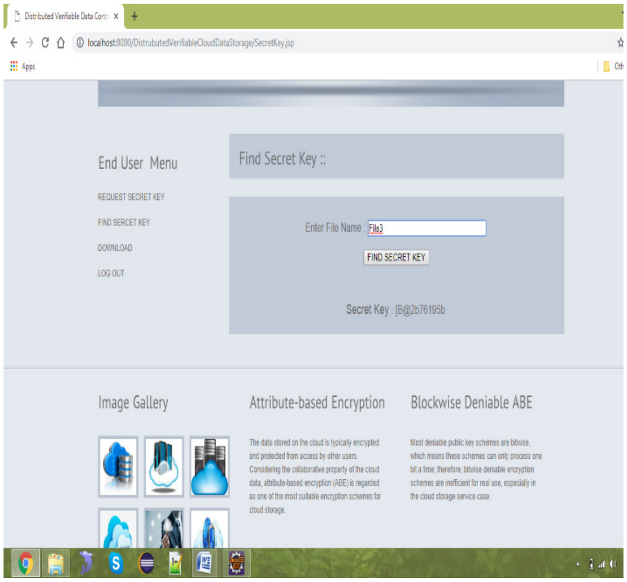
Generate Secret Key ::

User ID	User Name	Owner Name	File Name	Secret Key
1	a	a	File1.java	[B@1f07360
2	user	Aishwarya	nn	[B@25d0cd03
3	user	Aishwarya	exe	[B@3784952d
4	user	Aishwarya	File2	[B@5abbbd6a
5	user	Aishwarya	File3	Generate Key

Fig.8 End user finds the Secret key

Here we can see that the key is generated whereas in the previous screenshot we can see there is no key generated foe File3. But in the next picture we can clearly observe the difference.

Once again the user has to login and then click on find secret key where he/she has to specify the file name that was requested and get the secret key.



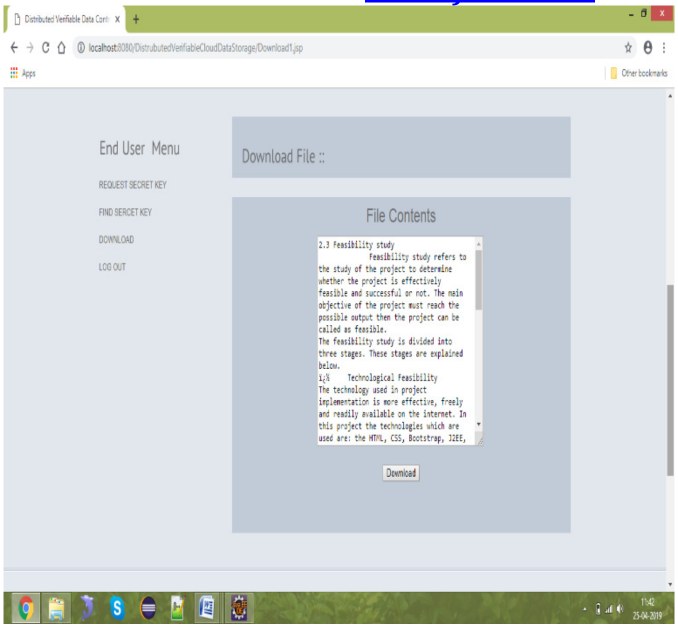
Enter File Name : File3

Secret Key : [B@2b76195b

The data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage.

Most deniable public key schemes are bitwise, which means these schemes can only process one bit a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case.

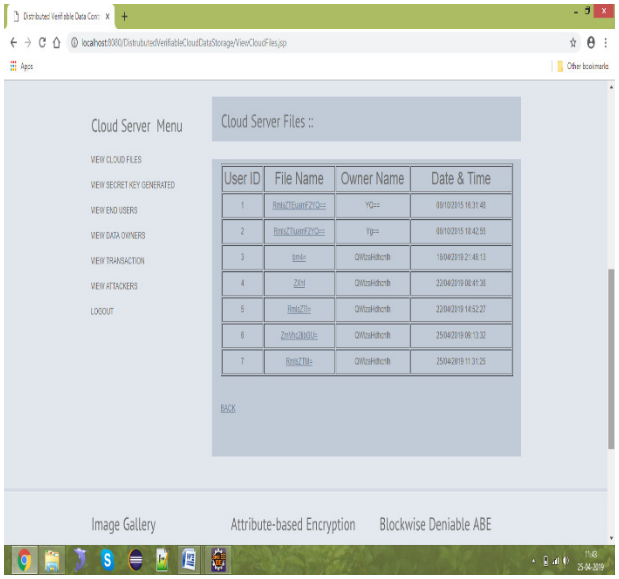
Fig.9 End User Successfully Downloads file



```
2.3 Feasibility study
              Feasibility study refers to
the study of the project to determine
whether the project is effectively
feasible and successful or not. The main
objective of the project must reach the
possible output then the project can be
called as feasible.
The feasibility study is divided into
three stages. These stages are explained
below.
ï¿½     Technological Feasibility
The technology used in project
implementation is more effective, freely
and readily available on the internet. In
this project the technologies which are
used are: the HTML, CSS, Bootstrap, J2EE,
```

Fig.10 End User acts as Attacker

In the application, if either the file name or secret key is entered by the user is wrong, it sure that the user will be treated as attacker then that user account credentials will be stored in TPA, cloud server.



User ID	File Name	Owner Name	Date & Time
1	RmlsZTEuamF2YQ==	YQ==	06/10/2015 16:31:48
2	RmlsZTIuamF2YQ==	Yg==	06/10/2015 18:42:55
3	bm4=	QWlzaHdhcnlh	16/04/2019 21:46:13
4	ZXI1	QWlzaHdhcnlh	22/04/2019 08:41:38
5	RmlsZTI=	QWlzaHdhcnlh	22/04/2019 14:52:27
6	ZmVhc2libGU=	QWlzaHdhcnlh	25/04/2019 09:13:32
7	RmlsZTM=	QWlzaHdhcnlh	25/04/2019 11:31:25

Fig.11 options of Cloud server files

V. CONCLUSION

Proposed a Provable Secure Key Aggregate Cryptosystem carry out proficient attribute revocation for multiple authorized cloud system, where it get rid of decryption operating costby the users based on attribute sets. In the encryption of messages, the data security technique is being used, it is shared by the users in the cloud. The outcome of theProvable Secure Key Aggregate Cryptosystem the data access and decryption is verified by secured and verifiable by TPA. So Provable Secure Key Aggregate Cryptosystem is a favorable techniqueany cloud based online application systems.

REFERENCES

[1]. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, “TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage”, *IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2015.*

[2]. Jianan Hong, Kaiping Xue and Wei Li, “Comments on “DAC-MACS: Effective Data Access Control for Multi-authority Cloud Storage Systems”/Security Analysis of Attribute Revocation in Multi-authority Data Access Control for Cloud Storage Systems”, *IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2015.*

[3]. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, “Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption”, *IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2015.*

[4]. Kan Yang and Xiaohua Jia, “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage”, *IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.*

[5] K. Kumar and Y.-H. Lu, “Cloud computing for mobile users: Can offloading computation save energy?” Computer, no. 4, pp. 51–56, 2010.

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom, “Cloud computing security: From single to multi-clouds,” in System Science (HICSS), 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] G. V. Kapse1 et al, “Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption”, *IOSR Journal of Computer Engineering,National Conference on Recent Trends in Computer Science and Information Technology (*NCRTCSIT-2016), pp 53-59.

[8] E. Aguiar, Y. Zhang, and M. Blanton, “An overview of issues and recent developments in cloud computing and storage security,” in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., “Cloud computing security auditing,” in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[10] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Informatics and Systems (INFOS), 8th International Conference on. IEEE, 2012, pp. CC– 12.