Self-destruction of data at rest in cloud

Mr. P R Kuber Gupta[1], Dr. Gangothri[2]
[1] *MCA Scholar, School of CS & IT, Dept of MCA, Jain (Deemed-to-be) University, Bengaluru*
[2] *School of CS & IT, Dept of MCA, Jain (Deemed-to-be) University, Bengaluru*

***Abstract* - Data being an important asset for an organization, individual or community preserving integrity of data is an important task to be achieved. Data can be stored either on premises or off premises. Here on premises refers to data storage in workstations, terminals etc. off premises refers to data stored in cloud. Data that is residing on or off premises should be deleted once our use with it is finished. This can be achieved by deleting data manually but destroying data manually is not efficient process because this might create ambiguity for admin who is managing data. And when storing data in cloud we have to pay even for the data that we are not using, this issue can be resolved by configuring self-destruction of data. The main motto of this concept is that data will be destroyed on its own without human intervention depending on the time to live that is the amount of time that the data should be available. This can reduce administration overhead and can increase the integrity of data.**

***Index Terms* - Data, on premises, off premises, workstations, terminals, cloud, time to live, self-destruction, administration overhead, integrity of data.**

I.INTRODUCTION

Data refers to facts and figures that can be used to create business strategy or can be used to create value to the business. Data goes into archive state once that particular data is out of use. Sensitive data disclosure can lead to loss of organization's reputation, leakage of project details to competitors etc. To overcome this issue, we have proposed a model that destructs data on its own based on the time to live (TTL) constraint. The proposed model contains two attributes that is admin and general user access. General user is given access to upload files into the cloud and during this process he/she is required to set TTL to the concerned file that is user has to set expiry time to the particular data they are uploading. Once data reaches the threshold period of existence it gets deleted from the database automatically this preserves data from being accessed by unauthorized users. If at all data is deleted without its use is over, users can request admin to recover data. If admin feels the request is legitimate, he/she approves data recovery process and data is available to access again.

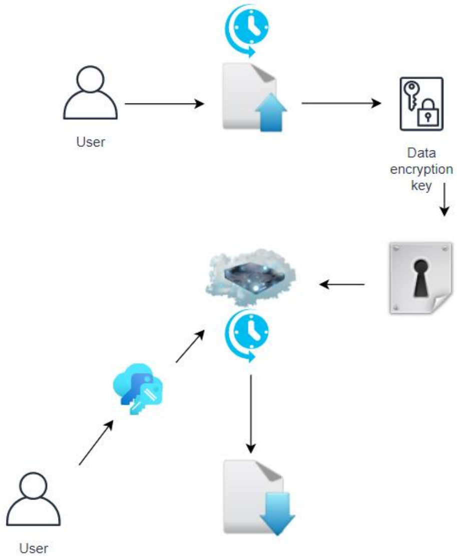


Fig 1: Architecture

II.LITERATURE REVIEW

Though there are many techniques for data destruction only few works efficiently. Every technique / algorithm doesn't delete data, algorithms like vanish, safe vanish, fade, se das doesn't delete data. However, these techniques destroy only keys associated with that particular data but algorithms like self- destruction of data, in gmail, retro grade storage deletes data and secures privacy.

The technique used in this paper is better but can't be declared as best for data destruction (self-data destruction). Since, cloud sky secures data by converting plain text to cipher text using ABE-Attribute based encryption (Asymmetric key approach) but doesn't destruct data but ensures the destruction of keys.

Using retrograde storage destruction technique is good but the problem persists when data is not recoverable using this method. This can lead to serious chaos when conducting forensic investigation on data storage and also during accidental deletion of data.

SafeVanish is a view of broadening the length scope of the key offers and applying the public-key cryptosystem, to duplicate the bouncing assault cost, including capacity prerequisite and the organization data transfer capacity, and to dodge the sniffing assault.

To tackle the issues of the current overwriting techniques, we proposed another information obliteration strategy based on the calculation of information collapsing in this paper. The calculation of information collapsing doesn't have to produce the information succession for overwriting in advance, and the hours of information collapsing can be changed by various necessities. With the calculation of information collapsing, the vulnerability of the "moderate position" and the length of information bring more trouble for information recuperation. Inside a specific scope of the size of documents, it can lessen the time required for overwriting.

III.PROBLEM STATEMENT

Cloud offers unlimited storage and hence users who upload files in cloud has this tendency to forget to delete the files even after completing the task. This can cause serious data disclosure issue anytime in future.

IV.PROPOSED MODEL

The user while uploading the file to the cloud from the client system by dividing the file in to the blocks, each block will be encrypted with the user's key and also, he can give the time to deletion of the file. The block details of the file will be stored in the server database. If the current time is equal to the deletion time, file will be downloaded to the server and decrypt with the user's key and again encrypt with the Authority's key and upload to the recovery cloud, and delete the all the blocks related to the file from the cloud storage.

The user can recover the file by sending request to the Authority, If the Authority approves the request, file will be download to server and decrypt with the Authority's key and again upload to the previous cloud storage by encrypting the blocks with the user's key, then user can download the file to the client system. Authority can delete the file from the recovery cloud based on some time limit.

Advantages of proposed system:

- Data will be more secure, because file will be stored in the form of blocks.
- Hackers cannot able to find which block related to which file, those details are present in the server database.
- Self-destruction of the file based on the time constraint.

V.REQUIREMENTS

Hardware:

•	Processor	: Pentium IV 2.4 GHz.
•	Hard Disk	: 500 GB.
•	RAM	: 4 GB

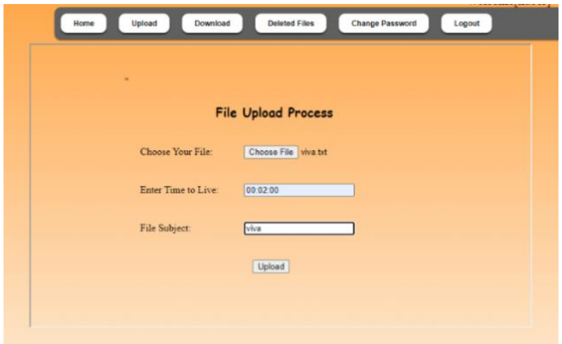
Software:

•	Operating system	:	Windows
•	Coding Language	:	Java
•	Web Technology	:	Servlet, JSP
•	Database	:	My-SQL

VI.ALGORITHM

Self-data destruction algorithm is one among the finest data destruction algorithms that works efficiently. Various other data destruction algorithms like vanish, safe vanish etc. delete encryption keys but when it comes to self-data destruction algorithm it works directly on data rather than encryption keys and deletes data completely.

VII.RESULT ANALYSIS



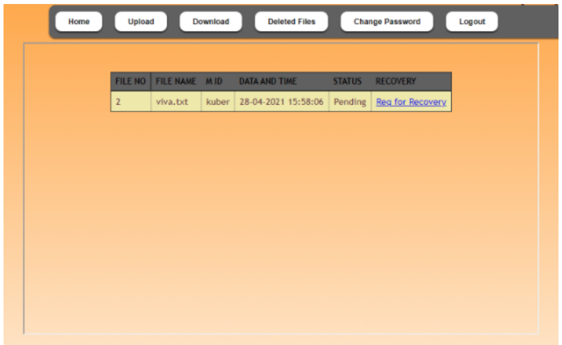
File Upload Process

Choose Your File: viva.txt

Enter Time to Live: 00:02:00

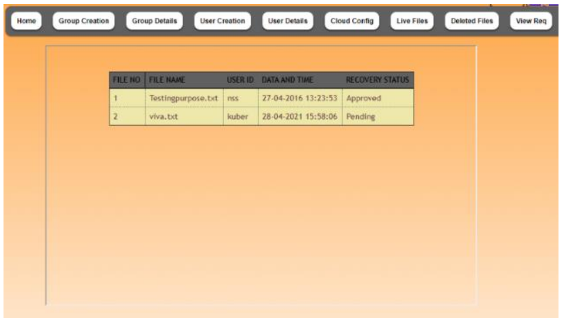
File Subject: viva

Fig 2: file uploaded by user to cloud



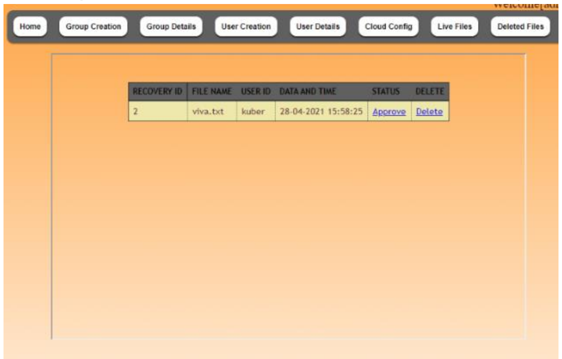
FILE NO	FILE NAME	M ID	DATA AND TIME	STATUS	RECOVERY
2	viva.txt	kuber	28-04-2021 15:58:06	Pending	Req for Recovery

Fig 3: file deleted automatically after TTL



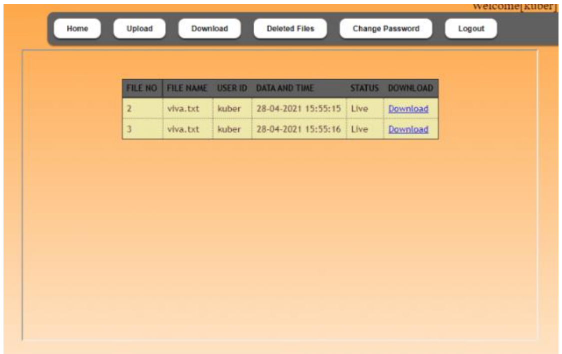
FILE NO	FILE NAME	USER ID	DATA AND TIME	RECOVERY STATUS
1	Testingpurpose.txt	nss	27-04-2016 13:23:53	Approved
2	viva.txt	kuber	28-04-2021 15:58:06	Pending

Fig 4: request sent to admin for file recovery



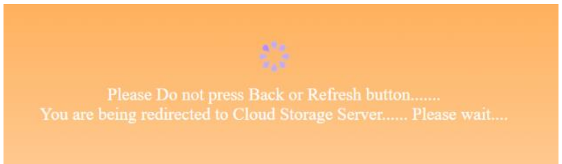
RECOVERY ID	FILE NAME	USER ID	DATA AND TIME	STATUS	DELETE
2	viva.txt	kuber	28-04-2021 15:58:25	Approve	Delete

Fig 5: admin granting access for file recovery operation



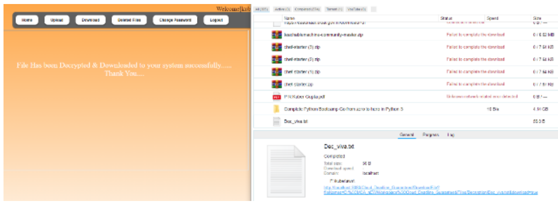
FILE NO	FILE NAME	USER ID	DATA AND TIME	STATUS	DOWNLOAD
2	viva.txt	kuber	28-04-2021 15:55:15	Live	Download
3	viva.txt	kuber	28-04-2021 15:55:16	Live	Download

Fig 6: file available to download



Please Do not press Back or Refresh button.......
You are being redirected to Cloud Storage Server...... Please wait....

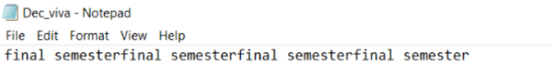
Fig 7: file downloading from cloud server



File Has been Decrypted & Downloaded to your system successfully......
Thank You.....

Dec_viva.txt
Completed
Total size: 56 B
Domain: localhost

Fig 8: file downloaded successfully



```
final semesterfinal semesterfinal semesterfinal semester
```

Fig 9: file is available to access

VIII.CONCLUSION

Data is one of the important assets for any organization and securing it from unauthorized access or vandalizers is a great task to achieve and to delete unwanted data with no manual intervention it is better to use some automated model that destructs data. The developed model destructs data based on the time that user has set during data upload interval into cloud. Data disappears once it meets time to live.

REFERENCES

[1] Cloud Based Deduplication and Self-Data Destruction Authors: Ankush R. Deshmukh, Prof. R. V. Mante, Dr. P. N. Chatur

[2] A Review on Self Destructing Data:Solution for Privacy Risks in OSNs Authors: Reshmie T S, Daniel madan raja S

[3] Secure Self-Destruction of Shared Data in Multi-CloudIoT Authors: Farida Ali Guechi, Ramdane Maamri

[4] An Efficient Retrograde Storage for Self-Destructing Messages on Frequently Colliding Hash Table Authors: Yan Zhu, Shuai Yang, Guohua Gan, Xiao He

[5] The Five Levels of Data Destruction: A Paradigm for Introducing Data Recovery in a Computer Science Course Authors: Dr. Gary Cantrell, Professor Joan

[6] Secure Data Storage in Cloud using Cryptographic Algorithms Authors: Nagasai Lohitha Kodumru, Supriya M

[7] SEDAS – Self Destruction Data System Authors: Maruthavani E, Chandra Prabha T, Sakthivel Murugan T, Hemalatha M, Manikandan D

[8] A Secure Document Self-destruction Scheme: An ABE Approach Authors: Jinbo Xiong, Zhiqiang Yao, Jianfeng Ma, Ximeng Liu, Qi Li

[9] SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy Authors: Lingfang Zeng, Zhan Shi, Shengjie Xu, Dan Feng

[10] Data folding: A new data soft destruction algorithm Authors: Xiaolong Xu, Peipei Gong, Jia Xu