IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Self-Destruction System for Recycling Space in Cloud Storage

[1]Shankar Gadhve, [2]Ashwini Khobragade, [3]Sneha Lendekar, [4]Toshika Darwade, [5]Abhishek Telange

[1]Assistant Professor, [2,3,4,5]UG Students, Department of Information Technology, Nagpur Institute of Technology, Nagpur, Maharashtra, India.

Abstract :- Mostly there are storage platforms which works on dedicated and this one is also the storage structure which works on cloud application implementation, but the problem is that these applications does not introduced a self-automated deletion of unused uploaded data which ultimately impact on storage capacity. So as per the problem statement one thing we are developing that it will be a highly secured cloud database that will be work as a storage device for integrated with cloud to store local files and media's and mainly follows the self-deleting automated technology which releases the storage space acquired by unused files without user intervention.

Index Terms— Dedicated cloud storage structure, Self-automated deletion technology, storing local files into cloud storage, RSA encryption algorithm, module one – login registration, module two portal design, module three – encryption, module four – self-automated deletion, enabling storage integrity.

I. INTRODUCTION

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. Cloud may be limited to a single organization or be available to many organization. Cloud poses privacy concern because the service provider can access the data that in in the cloud at any time. Many cloud providers can share information with third parties if necessary for purpose of law and order without a warrant. Solution to privacy include policy and legislation as well as end users choice for how data is stored. With the development of Cloud computing and popularization of mobile Internet, Cloud services are becoming more and more important for people's life. As people rely more and more on the Internet and Cloud technology, security of their privacy takes more and more risks. The term Cloud Computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The storage of data and application on remote server, and accessing them via internet.

Cloud security is the protection of data stored online from theft, leakage and deletion. Methods of providing cloud security include firewalls, virtual private networks (VPN), and avoiding public internet connection. Cloud security also will be providing an important feature of recycling of the space, as the data will be deleted within some particular duration of time and the space of that deleted data can be easily reused by the user. The cloud computing provides rich benefits to the cloud clients such as costless services, elasticity of resources, easy access through internet etc. The cloud computing has enormous benefits, cloud users are unwillingly to place their confidential data or sensitive data, it includes personal health records, emails and government sensitive files. So, the Cloud Service Provider has to promise to ensure the data security over the stored data of the cloud clients by using the methods like firewalls,virtualization, deletion of the data after some particular duration of time and reusing of the space on the cloud.

II. LITERATURE SURVEY

[1]. MS Jayaprabha , Dr A R Nadira Banu Kamal. "A Secure Data Self-Destructing Scheme In Cloud Computing". [IJANA]

In this paper authors, introducing A Secure Data Self Destruction Scheme in Cloud Computing Environment using KP-TSABE. The KP-TSABE is able to solve some importante security problem by supporting user-defined authorization period and by providing fine-grained access control during the period So that the sensitive data will be securely self-destructed after a user-specified expiration time.

[2].Shankar Gadhve, Deveshree Naidu. "Self-Destruction System for Protecting Data Privacy in Cloud Storage". [IJEESE]

In this paper authors, presenting a system that meets with the challenge through integration of active storage techniques. It mainly aims at securing the user valuable data's privacy through integration of active storage techniques.

[3]Cong Wang, Sherman S.M. Chow, Kui Ren and Wenjing Lou. "Privacy-Preserving Public Auditing for Secure Cloud Storage". [IJERGS]

In this paper authors, propose a privacy-preserving public auditing system for data storage security in cloud computing. It mainly focuses on securing the data content stored on the cloud server .Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

[4]. Lingfang Zeng, Dan Feng, Shibin Chen and Qir.gsong Wei. A Self-Destructing Data System Based on Active Storage Framework. [IEEE]

This paper introduced a new approach for protecting data privacy from attackers who retroactively obtain, through legal or other means, a user's stored data and private decryption keys. All data and their copies become destructed or unreadable after the user-specified time using novel integration of cryptographic technique. The system will help to provide researchers with further valuable experience to storage system designs for cloud services.

III. PROBLEM DEFINATION

Personal data stored in the cloud may contain account numbers, passwords, notes, and other important information that could be used and misused by a miscreant, a competitor, or a court of law. These data are cached copied, and archived by cloud service providers often without user's authorization and control. The people used the data which is shared in environment at that time the security is major problem so the sensitive data may not be in secure position.

A typical problem with encryption scheme is that it is impractical because of huge amount communication overheads over the cloud access patterns. Cloud does not provide a huge amount of data storage space. The space on the cloud cannot be reused by the again and again. Not much security is provided to the data stored in the cloud. The issues related to the cloud data storage such as data breaches, data thefts and unavailability of cloud data.

IV. PROPOSED APPROACH

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burdein of local data storage and maintainance. Self-destructing data mainly aims at protecting the user data's privacy. All the data and their copies becomes destructed or unreadable after a user specified time, without any user intervention. Our cloud drive is going to provide an important feature rather than that other clouds drives have i.e. deletion of the data.

The stored on the cloud with be provided security so that one can access your data without the user's permission. For storing your data on the cloud, the user needs to have a different user id and password. The space on the cloud can be reused by the user , as the data stored on the cloud will be deleted after some particular duration of time , but unless and until the user grants the permission to delete the data the data will not be deleted and that space of the deleted data can be reused by the user.

A. Admin Module:-

The admin module will provide an access to the users. The user will be the admin deciding who grant to access the system. This module will be handled by an Admin who has a valid user id and password.

1. Register & login
2. View registered list
3. Grant the access permission
4. Send the conformation mail to the user
5. Log Out

B. Login and Registration Module:-

1. The new user has to create a profile
2. This is done by registration.
3. A user id and password are submitted by the user.
4. The user can login successfully, only if user id and password are entered correctly.
5. Once the valid user enters into the system, user can use the function of the system.

C. File Uploading:-

1. When a user upload a file in cloud the user perform encryption using a triggering parameter generated by Shamir algorithm through MD5.
2. Once the files have been uploaded on the cloud storage, the data will be on cloud.

D. File Downloading:-

1. Any authenticated user who has proper permission can download data stored in the data storage system.
2. And hence the file is downloaded successfully.

E. Integration of cloud server:-

1. After the user uploads the files or data the system will integrate with the cloud Server.
2. Hence it will enable the storage of local files directly into the cloud.

F. Manually Deletion:-

1. If the user wants to delete the data, it can be easily deleted.
2. The data will be deleted from the cloud storage, as the user on itself will be deleting that data.

G. Automatic Deletion:-

1. Deletion of file is depending on the triggering parameter, Triggering parameter is a time-to-live property.
2. The triggering parameter is decided by the user.
3. The user will specify the survival time and data will be deleted from the cloud environment, once the survival time is over.

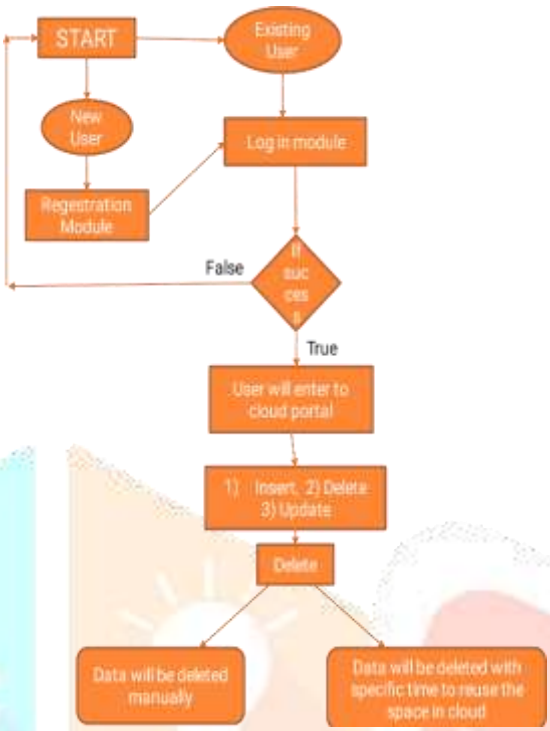

Fig. 4.1 The Flow of cloud storage system

V. PRESENT WORK

The project is developed by using cloud infrastructure, where you don't have to spend huge amounts of money on purchasing and maintaing equipment. One of the major concern of every business, regardless of size and industry, is the security of its data. Our system provides security feature that guarantee that data is securely stored and handled. It allows mobile access to corporate data via smartphones and devices, which is a great way to ensure that no one is ever left out of the loop. Sensitive data is vital to any company. You never know what can happen if a document gets into the wrong hands, you can easily decide which users have what level of access to what data. We are providing an, another feature that is triggering parameter. As it names suggests, you can setup a timer configuration to automatically schedule your function to run. So here we have provide a triggering parameter which will automatically delete the data after a user specified time duration.

We are having only one type of admin who has the authority to manage functions of the system. The admin module will provide an access to the users. The user will be the admin deciding who grant to access the system.

Fig. 5.1. User List- Admin Dashboard

Fig. 5.2. User Conformation-Admin Dashboard

- Fig. 5.1 consist of Admin Dashboard where admin can view the registered user list and their information.
- Fig. 5.2 consist of Admin Dashboard where admin can grant the permission to the user by sending a conformation mail after that the user can easily access their account.

VI. RESULT AND DISCUSSION

Snapshot of designed system is given below which shows interface of various modules of system along with their functionalities.

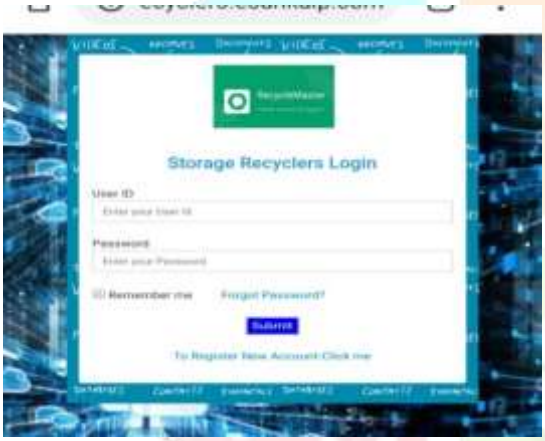

Fig. 6.1 Login Page

Fig. 6.2 registration page

- Fig. 6.1 consist of login page. The user can login successfully, only if user id and password are entered correctly. Once the valid user enters into the system, user can use the function of the system.
- Fig. 6.2 consist of registration page. If the students haven't registered they can register by clicking on the Create an Account. All the details will be stored in the database and after registration user can log in into system by entering the user I'd and Password.

Fig. 6.3 Uploaded Files

Fig. 6.4 Triggering Parameter

- Fig. 6.3 One of feature of the system in which the uploaded file list can be viewed. User can also preview and download the data.
- Fig. 6.4 consist of our another feature that is automatic deletion in which a pop up alert will be generating as per the user specified time.

VII. CONCLUSION

We introduced a new method of protecting data from cloud environment. The Active storage module with the integration of own Cloud Storage is used to store the data on cloud and delete the data from the cloud. In this approach there is no need to put any encryption and decryption method to encrypt the data.

This will be the ultimate storage portal for saving their files, folders, and all the other media files. System will generate a "local time" stamp for each and every uploaded file that will be a help for automatic deletion function. The system will rely on purely cloud storage environment, so that there is no physical device storage space needed.

VIII. FUTURE SCOPE

- In future the experimentations can be carried out by using different types of advanced algorithm for Encryption.
- Implementing the compression of the file size before uploading file in order to reduce the usage of cloud storage.

REFERENCES

[1]. MS Jayaprabha , Dr A R Nadira Banu Kamal. "A Secure Data Self-Destructing Scheme In Cloud Computing", (2017)
[2]. Shankar Gadhve, Deveshree Naidu. "Self-Destruction System for Protecting Data Privacy in Cloud Storage", (2015)
[3]. Cong Wang, Sherman S.M. Chow, Kui Ren and Wenjing Lou. "Privacy-Preserving Public Auditing for Secure Cloud Storage", (2015)
[4]. Lingfang Zeng, Dan Feng, Shibin Chen and Qir.gsong Wei. A Self-Destructing Data System Based on Active Storage Framework, (2013)
[5]. Jamshed, First Information Report (F.I.R.): A Critical Study, (2016)
[6]. T. M. Zaharchuk, Study of Police Management Information Systems, (2016)
[7].Douglas Kunda, Rights of Victims in the Indian Criminal Justice System. (2016)
[8]. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, Vanish: Increasing data privacy with self-destructing data, (2009)
[9]. A. Shamir, How to share a secret, (2007)
[10]. L. Qin and D. Feng, Active storage framework for object-based storage device, (2006)
[11]. Y. Zhang and D. Feng, An active storage system for high perfor- mance computing, (2006)
[12]. Rao, C., Rodi, P., Palande, A., & Bhusari, SEDAS: A Self-Destructing Data System Based on Shamir's Secret Sharing Algorithm, (2015)
[13]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, (2006)
[14]. J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, A full lifecycle privacy protection scheme for sensitive data in cloud computing, (2005)
[15]. G. Wang, F. Yue, and Q. Liu, A secure self-destructing scheme for electronic data, (2013)
[16]. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, (2010)
[17]. S. W. Son, S. Lang, P. Carns, R. Ross, R. Thakur, B. Ozisikyilmaz, W.-K. Liao, and A. Choudhary, Enabling active storage on parallel I/O software stacks, (2010)
[18]. A. Devulapalli, I. T. Murugandi, D. Xu, and P. Wyckoff, Design of an intelligent object-based storage device, (2009)
[19]. T. M. John, A. T. Ramani, and J. A. Chandy, Active storage using object-based devices, (2008)