© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Smart Cloud Security Back-up System for High Recurrent Data in Cloud Storage

M. Swarnamala, M. Pajany
IFET College of Engineering, IFET Nagar, Gangarampalayam, Valavanur Post, Villupuram, Tamil Nadu, India

ABSTRACT

Now days, Cloud Computing plays an important role. We can archive and retrieve a data from the cloud. In this paper we propose a smart data backup plan using Threshold value techniques with Advance Encryption Standard (AES) algorithm. Data Migration is also one of the techniques in cloud storage. We are proposing a procedure which allows Owner to store their data onto the cloud, as soon as the file is stored at the first cloud storage (Drop Box) it gets encrypted using AES. Then, User can search the file using key. Using Threshold value, user can view the file up to the value; the file can be automatically back-up into cloud storage. This method focuses on the security concept for the backup files stored at cloud storage using AES encryption algorithm. It's also focuses on the storage space concept, to reduce numerous storage spaces in cloud.

Keywords : Encryption, Decryption, Recurrent Usage, Cloud Storage, Automatically Back-up.

I. INTRODUCTION

Cloud can be used as a public cloud, private cloud or hybrid cloud. In public cloud services can be offered over the internet and clouds Provide owners and operate in it. In private cloud, the infrastructure is dedicated to a particular organization and not shared with other organization. The usage of both public and private cloud is called hybrid cloud. Cloud computing has many challenges when data owners and data users are involves, and the data is stored in the offsite location. This paper introduces back up the high frequency usage data file. Using AES algorithm, encrypt the data files on owner side and upload into cloud account. The high recurrent usage data files will back up automatically in cloud using threshold values.

Objective

Our project aim is to reduce the storage space and provide more security for backup the frequent data files in cloud storage.

II. METHODS AND MATERIAL

A. Related Works

a) Tanay Kulkarni et. al., proposed a smart remote data backup plan using Seed Block Algorithm (SBA) with Advance Encryption Standard (AES) algorithm.

b) Neetesh Gupta et. al., proposed backup and restore data in Android Smartphone as it uses RLE compression technique it saves time, space to store and improve performance.

Table 1. Comparison between Various Cloud Data Online Back-Up

Types of Cloud Online Backup	Advantage	Disadvantage
Crash plan	• No File Size Limit • Unlimited Plan(s) • No Bandwidth Throttling • File Encryption (448-bit)	• Mirror Image Backup • Offline Backup Option(s) • Offline Restore Option(s)
Back blaze	• Unlimited Plan(s) • No Bandwidth Throttling • Bandwidth Control (Advanced)	• File Encryption (448-bit) • Mirror Image Backup
Mozy	• Native 64-bit Software • File Encryption (256-bit) • Offline Backup Option(s)	• Unlimited Plan(s) Local Backup Option(s)
Carbonite	• No Bandwidth Throttling • File Encryption (448-bit) • Mirror Image Backup	• Bandwidth Control (Advanced) • Local Backup Option(s)
SOS	• Native 64-bit Software • File Encryption (256-bit)	• Offline Backup Option(s) • Idle Backup Option
Live drive	• Unlimited Plan(s) • File Encryption (256-bit)	• Native 64-bit Software • Offline Restore Option(s)

B. Problem Identification From Existing System

In existing data shared between owner and user very securely. But all data's will be stored, important data's and unimportant data's stored in cloud get overloading problem. In cloud storage data Backup is not working properly, so some important data get missing. Backup data has been taken for all files, so we have to allocate more storage space.

C. Proposed System

In this proposed work, the files could manage by using atomization techniques helps to back up the data files. Backup data files based on the recurrent usage of a specific time i.e. (3 time per week). Other than that unused files could be remains our own PC and cloud. The data migration methodology plays a vital role on the atomized cloud storage mechanism.

D. Advantages

Data migration techniques is very user to for efficiently taking backup files. Once the data are eventually atomized in timely manner, Auto Backup data has been taken based user frequency views. So we can avoid overloading problem and also avoid numerous storage space.

E. Module Description

1. Encryption

The encryption method is used in this work with AES (Advanced Encrypted Standard). While uploading the file, the first encryption will be done; the second is when storing the data into drop box cloud account.

2. File Transfer Protocol (FTP):

File transfer protocol (FTP) is used to transfer the data files between drop box cloud account and computer. This protocol is used to store and receive the data.

3. Timely Manner Automatic Backup

In Time Manner Backup, its work is set a time period for take a backup file but in that time period the user must access that file in a threshold set value. For example we set a time period one week and threshold value Three then the user must access that particular cloud file three time in between a time period of One week then only the Data Migration method takes a backup file and store in a database.

4. Decryption

This method is given by the cloud service provider. The data can be decrypted using online tool. Legal user can download the method using their registered account. Web application is used in their work to decrypt the key.

F. Advanced Encrypted Standard (AES) Algorithm

The algorithm of AES (Advanced Encrypted Standard) is used in this work to secure the data which is stored in the cloud. This algorithm use 256 bit auto generated secret key. The generation of key is single encryption. The existing system used 12 rounds to encrypt and decrypt the data, but in this work, 1 round is used for encryption.

III. RESULTS AND DISCUSSION

A. Architecture

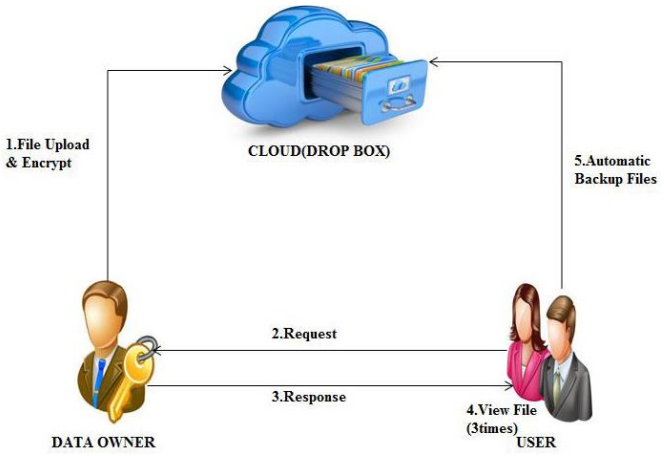


Figure 1. Architecture diagram for Backup the High Frequency usage data files.

In this Fig1. first step to encrypt the data files using AES (Advanced Encryption Standard) algorithm and then upload the data files in Drop Box cloud account. In Second Step, when the user request to data owner for view the upload data files. In Third step, Data owner response the user request to view the data files. In Fourth step, a User can view the files three times. In Fifth step, the viewed data files are automatically back up into drop box cloud storage.

B. Sample Implementation

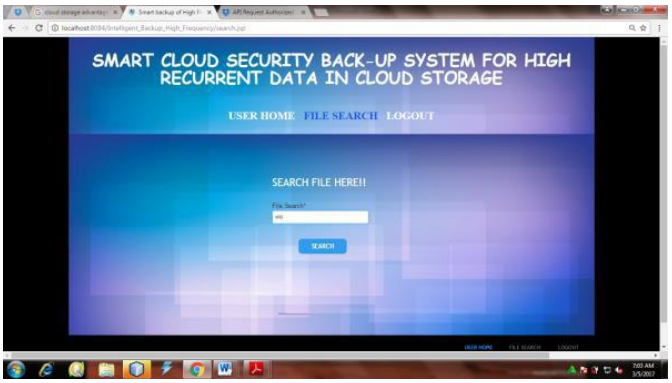
Step 1 : Owner Login

Step 2 : Upload File Using Encryption Key

Step 3 : Upload File Details

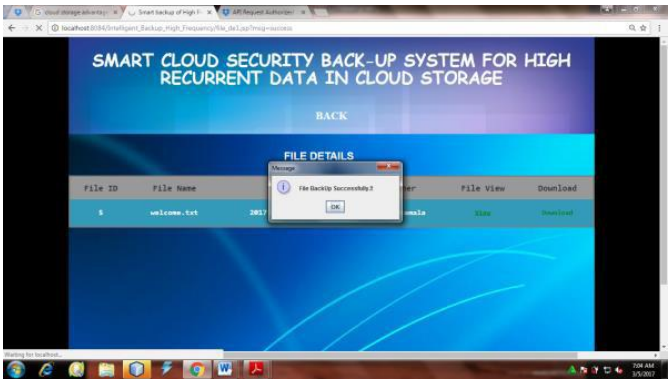
Step 4 : User Login

Step 5 : File Search Using Key



Step 6 : File View (3 Times)

Step 7 : Automatic File Back-Up Successfully



Step 8 : Back-Up File

IV. CONCLUSION

The High Recurrent usage data will be automatically backed up in cloud storage. The first method encryption will do in data owner side and another method is data files will transfer in cloud. While using AES algorithm to encrypt and decrypt the files. The data user can back up the high recurrent data using threshold values. Data Migration method will take a backup files and store in database. This process will be more secure, and reduce storage space in cloud.

V. REFERENCES

[1]. P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., 2009.

[2]. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609.

[3]. Ateniese G, Pietro R.D, Mancini L.V, and Tsudik G, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New York, NY, USA: ACM, 2008, pp.1-10.

[4]. Bowers K.D, Juels A, and Oprea A, "Proofs of retrievability: Theory and implementation," Cryptology ePrint Archive, Report 2008/175, 2008.

[5]. Juels A and Kaliski B.S, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.

[6]. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions On Cloud Computing, Year 2013.

[7]. Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham ,Mirza Aamir Mehmood "Implementation of Eap with RSA for Enhancing The Security of Cloud Computing," International Journal of Basic and Applied Sciences, 2012, pp. 177-183.

[8]. Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," 44th Hawaii International Conference on System Sciences 2011.

[9]. C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security , E. Al-Shaer, S. Jha, and A. D.Keromytis, Eds. ACM, 2009, pp. 213–222.

[10]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.

[11]. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM. IEEE, 2010, pp. 525–533.

[12]. J. Walker, M. Kounavis, S. Gueron and G.Graunke "Recent Contribution to Cryptographic Hash Functions," Intel Technology Journal, vol-13, issue-2, 2009, pp-80-95.

[13]. S.M. Bellovin, E.K. Rescorla," Deploying a New Hash Function," presented at first NIST Workshop", 2005. Available at http://www.csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentatio ns/Bellovin.new-hash.pdf.

[14]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in SAC , W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.