Image Based OTP for Data Sharing In Cloud Using Accountability Method

[1]Janardhana D R, [2] Sunil B N

Assistant Professor
Department of ISE,
Sahyadri College of Engineering and Management, Mangalore, India

***Abstract*— Cloud computing is widely precise as momentous modernizations in computer technology. Cloud computing refers to the liberation of computing resources over the Internet on an as needed basis. With the evolution of cloud computing, Data security becomes very important. Cloud computing is an aggressive option to wide-ranging distributed data sharing method. The key component of cloud service is that client's information is commonly prepared remotely on obscure machines that clients can't oversee. To address this issue, in this paper an image based one time password is used with accountability method. The proposed method provides Third party authority to audit contents an also enforce strong backend protection in terms of image based one-time password. It enables the third party authority to keep track of uploaded files in cloud by assigning one time password to each file.**

Index Terms*— cloud computing; data sharing; accountability; image based OTP; Third Party Authority (TPA); AES algorithm*)

I. INTRODUCTION

Cloud Computing is a quickest developing innovation in utilized as a part of Test and improvement, huge information expository, File stockpiling, Disaster recuperation, Backup and information sharing. The distinctive sort of administrations gave by the cloud is exceptionally savvy. The client information is put away in cloud in which the area of information is obscure to the client. In the advancing of cloud computing benefits, the issue of information security is a standout among the most critical issues to be illuminated [1]. The information put away in cloud ought to be secure and just approved client can get to information.

Problem statement: This paper addresses the subsequent problems. How to share owner data in cloud using secure method, which vital to ensure individuals' security on cloud in opposition to unnecessary and illegal access of their secret data. Here image based one time password is used to protect data stored in cloud. Only authenticated user can get image based one time password to access data stored in cloud.

For giving cloud benefits, the touchy information of all information proprietors ought to be put away in the cloud host. As of now, the information insurance and the individual security ought to be ensured. The cloud supplier ought to offer confirmation to these information and private data in host database against all gets to of the unapproved insiders or the malignant pariahs.

II. RELATED WORK

This segment we will discuss the different methods of data sharing in cloud that has been already proposed. P.Varalakshmi, A.R.Shajina, V.Selin soniya [2] proposed the SMOADS model gives a secured information sharing proposition through the one of a kind element chief thought, which diminishes hacking plausibility with no accident in execution. The information trade convention for sharing information was proposed by Marwan Sabbouh in which they prestented the information exchange convention object model, writing framework, uniform indexing of information, and diagram demonstrating of the DIP information [3].

Nupoor M. Yawale and V. B. Gadichha proposed a novel in which the errands of permitting an outsider examiner (TPA), for the benefit of the cloud customer, approve the unwavering quality of the dynamic information put away in the cloud. TPA can play out different examining errands at the same time. Here they concentrated on RC5 Encryption Algorithm for put away information in cloud, and the came about scrambled technique is secure and simple to utilize [4].

Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan proposed the SeDaSC system, which is a cloud storage security plan for gathering information. The proposed strategy gives information confidentiality, secure information imparting to out re-encryption, access control for pernicious insiders, and forward and in reverse access control [5].

An imaginative methodology for consequently logging plan and image encryption strategy that gives security to information in the cloud alongside an inspecting component was proposed by Swapnil Dattatraya Taru [6]. They utilized Object oriented approach to deal with ensure the information utilizing Jar document and improved tumultuous picture encryption technique. They enhanced the effectiveness of CIA system by utilizing scrambled logged records, disorder picture encryption procedure and utilization of container document.

Seung-Hyun Seo, Mohamed NabeelXiaoyu Ding, Elisa Bertino proposed the principal mCL-PKE plan without matching operations and gave its official security. Their mCL-PKE tackles the key escrow issue and denial issue. Utilizing the mCLPKE plan as a key building square, they proposed an enhanced way to deal with safely share delicate information openly mists. Their methodology underpins prompt repudiation and guarantees the secrecy of the information put away in an open cloud while upholding the entrance control approaches of the information proprietor. Their exploratory results demonstrate the effectiveness of fundamental mCL-PKE plot and enhanced methodology for the general population cloud [11].

III. **OBJECTIVES**

We utilized image based OTP structure to fulfil taking after destinations:

- Data which is put away in cloud must be utilized by end client who is approved by cloud administration supplier.
- TPA will generate image based OTP corresponding to the files uploaded by data owner and it also provide the file status to data owner
- Log records should be generated as and when data is accessed by the end user and it sent periodically to data owner to inform current utilization of data.
- On the off chance that there is any abuse of information then data owner can have admittance data of an end client.
- Providing Auditing Facilities based on file usage by TPA.

.

IV. **PROPOSED SYSTEM DESIGN**

The image based OTP for data sharing in cloud proposed in this paper conducts automatic generating image based OTP for each file uploaded in cloud. Auditing mechanism is performed by third party authority and it also provides the security to user data which is stored in cloud.

A. Image based OTP

In our proposed system we used images to generate the OTP. The steps to generate image based OTP as follows:

- TPA contains number of images.
- Data owner upload files along with access count.
- TPA randomly select set of images as OTP for each files uploaded by data owner based on access count.
- Each image has unique ID which is used to generate OTP for files uploaded by data owner.
- When end user wants to download files from cloud he should send request for OTP.
- The OTP value entered by end user will sent back to TPA and TPA will compare the OTP value with corresponding image ID by comparing images.
- If it's valid OTP then user will get access to that particular file.

B. Process flow

The general layout is appeared in figure. Data owner who wants to share data in cloud will login with user name and password. Data owner will be authenticated by the cloud service provider. Data owner will upload his files to the cloud. The file path will be encrypted which is uploaded in cloud to provide security for owner data. The third party authority (TPA) will generate image based one time password (OTP) for each file uploaded by data owner. This image based OTP gives more security to owner data. End client validated by CSP who needs to get to information which is available in cloud. End user will send request to TPA to send image based opt for the file to download it. After receiving OTP end user successfully download the file. The flowchart is shown in figure 2.

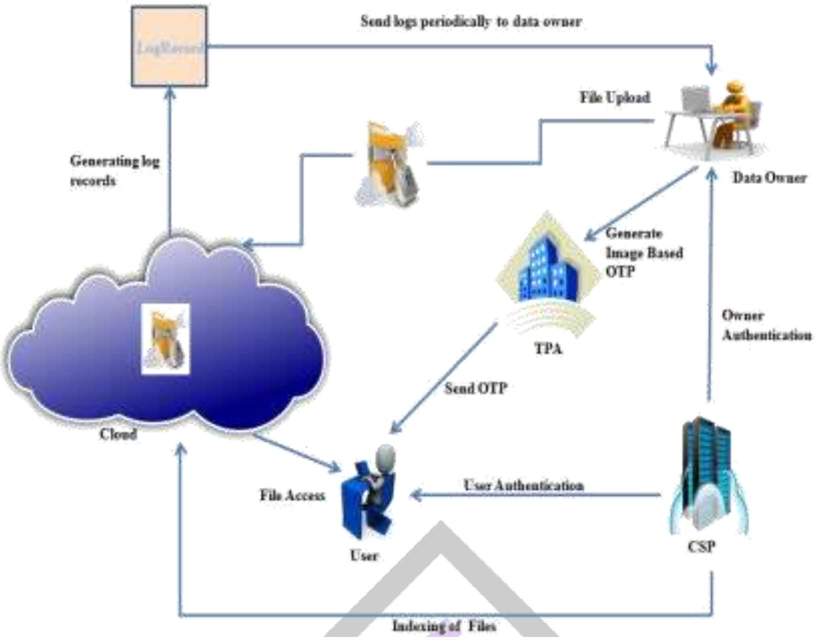

Fig.1. Data sharing system architecture

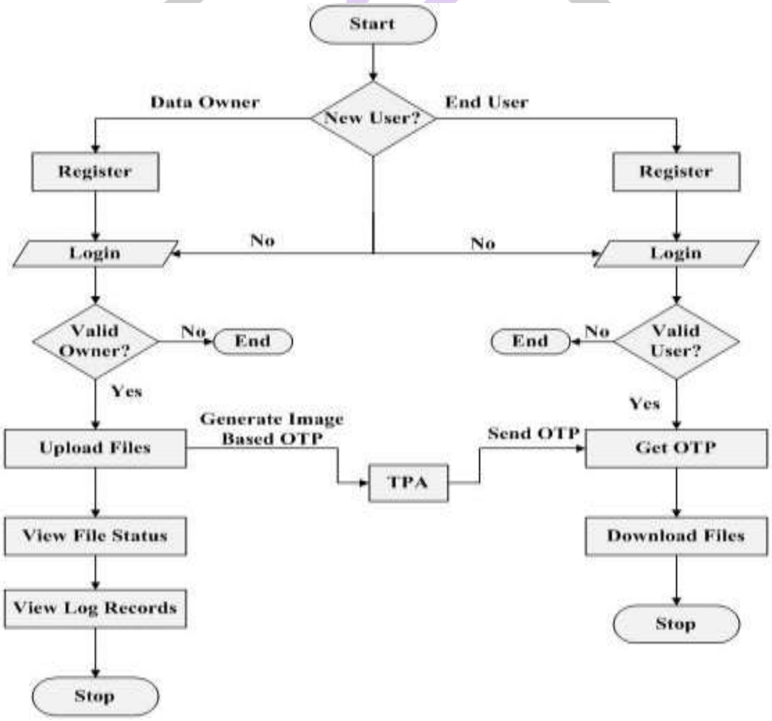

Fig.1. Flow Chart

C. Log Record Generation

At the point when there is any entrance to information present in cloud log record is naturally created. The every log record contains data of the end client in tuple group as takes after:

LR:<Username, File Name , Location, Time>. This Log Record information is periodically sent to the data owner.

D. Algorithm

AES is short form for Advanced Encryption Standard and is a United States encryption standard characterized in Federal Information Processing Standard (FIPS) 192 [7]. This algorithm is used for encryption of file path which is uploaded into cloud by data owner.

AES is a symmetric encryption algorithm managing out information in square of 128 bits. AES is symmetric in light of the fact that the same key is utilized for encryption and the converse change, unscrambling. The main mystery expected to keep for security is the key. AES may design to utilize distinctive key-lengths, the standard characterizes 3 lengths and the resultant calculations are named AES-128, AES-192 and AES-256 individually to determine the length in bits of the key.

V. RESULTS

A. Image based OTP

TPA will generate image based OTP for the files uploaded by data owner using access count. The following graph shows the number of access count against the time in seconds.

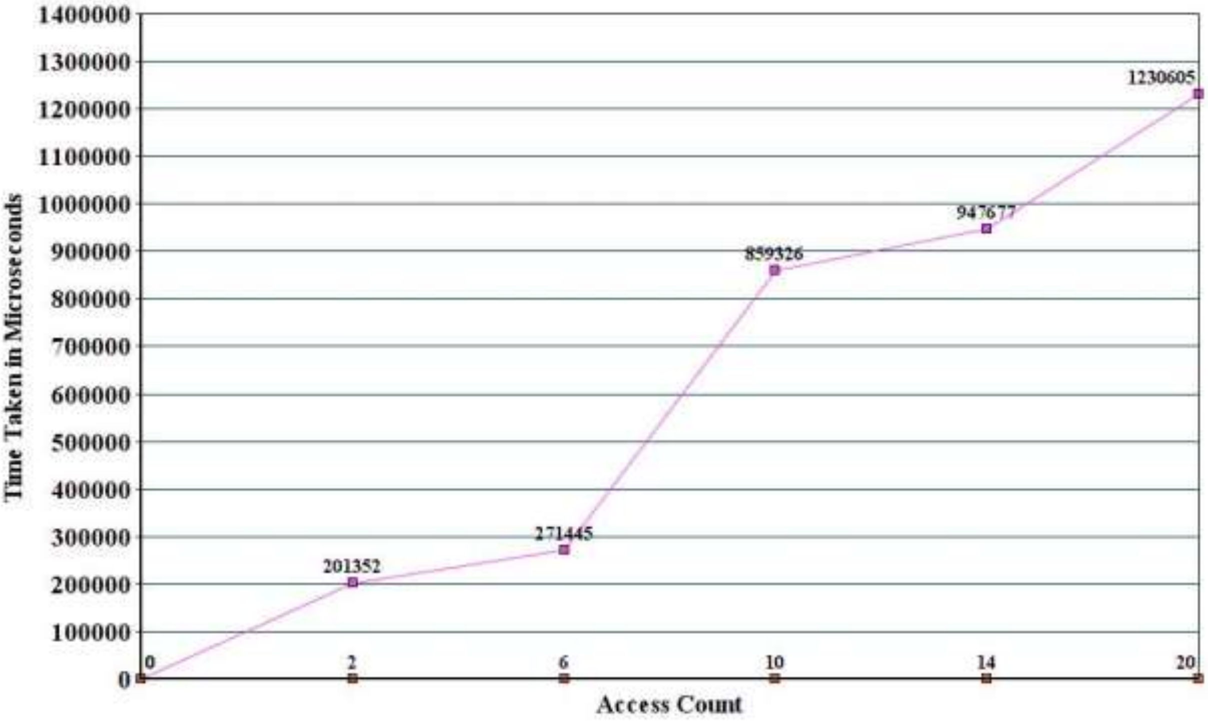

Fig.3. Time consumption for Image based OTP generation

B. Encryption Algorithm Analysis

In our proposed system we used AES algorithm. AES algorithm thought to be one of the best encryption algorithm. The beneath table demonstrates the correlation between various encryption algorithm.

Table 1. Encryption algorithm comparison

Factors	AES	Triple DES	DES	RC2
Key Length	128,192, or 256 bits	(K1,K2 and K3) 168 bits (K1 and K2 is same) 112 bits	56 bits	8-128 bits in step of 8 bits; default 64 bits
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric algorithm
Block Size	128,192, or 256 bits	64 bits	64 bits	64 bits
Security	Secure	Insecure	Inadequate	Vulnerable

VI.CONCLUSION AND FUTURE WORK

In this paper we proposed a novel methodology utilizing image based OTP for information sharing which gives security to information in the cloud alongside responsibility by TPA. It is essential to secure client information on the cloud against surplus and unlawful access of their private information. Since images are utilized to produce OTP, it is more admired contrasted with other OTP techniques. This paper presents effective instrument, which performs programmed approval of clients and makes log records of every information access by the client. Information proprietor ought not stress over information transferred on cloud utilizing this technique and information utilization is translucent.

REFERENCES

[1] Ching-Nung Yang, Jia-Bin Lai “Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing” 2013 International Symposium on Biometrics and Security Technologies

[2] P.Varalakshmi, A.R.Shajina, V.Selin soniya "SMOADS - Secured Multi-Owner Attribute based Data Sharing in Cloud Computing" 2013 Fifth
International Conference on Advanced Computing (ICoAC)

[3] Marwan Sabbouh, Kenneth McCracken, Geoff Cooney "Data Sharing for Cloud Computing Platforms" 2014 IEEE International Congress on Big Data

[4] Miss. Nupoor M. Yawale , Prof. V. B. Gadichha "Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm" international Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 11, November 2013

[5] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Albert Y. Zomaya "SeDaSC: Secure Data Sharing in Clouds" EEE SYSTEMS JOURNAL, 2015

[6] Swapnil Dattatraya Taru, Prof. Vikas B. Maral "Secure Data Sharing in Cloud for Distributed Accountability using Patchy Image Encryption" International Journal of Advance Research in Computer Science and Management Studies Volume 2,Issue 12, December 2014

[7] M.Pitchaiah, Philemon Daniel, Praveen "Implementation of Advanced Encryption Standard Algorithm" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012

[8] Yuchuan Luo, Ming Xu, Shaojing Fu, Dongsheng Wang, Junquan Deng "Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation" 2015 IEEE Trustcom/BigDataSE/ISPA

[9] Yanjiang Yang, Youcheng Zhang "A Generic Scheme for Secure Data Sharing in Cloud" 2011 International Conference on Parallel Processing Workshops

[10] Renuka Goyal, Navjot Sidhu "Third Party Auditor: An Integrity Checking Technique for Client Data Security in Cloud Computing" (IJCSIT)
International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014

[11] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, Elisa Bertino "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING , 2013

[12] Ashish Bhagat, Ravi Kant Sahu "Cloud Data Security while using Third Party Auditor" International Journal of Computer Applications (0975 – 8887) Volume 70– No.16, May 2013

[13] Milind Mathur, Ayush Kesarwani "COMPARISON BETWEEN DES , 3DES , RC2 , RC6 , BLOWFISH AND AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013