IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 05-11

"Secure File Hosting System on Cloud using Cryptography" India.

1. Ashwini A. Bagde 4. Kajol V. Jaunjal
2. Trushali P. Pardhi 5. Chetan H. Hande
3. Prajakta P. Selokar 6. Gaurav P. Mahakalkar

Department of Computer Science & Engineering , Tulsiramji Gaikwad & Patil College of Engineering & Technology Roshani Talmamle Head, Department of Computer Science & Engineering

Abstract: *Cloud computing is a computing technology or information technology architecture used by organization or individuals. It launches data storage and interactive paradigm with some advantages like on-demand self-services, ubiquitous network access. Due to popularity of cloud services, security and privacy becomes major issue. There is the issue of legitimate responsibility for information (If a client stores some information in the cloud, can the cloud supplier benefit from it?). Numerous Terms of Service assentions are quiet on the topic of proprietorship. Physical control of the PC hardware (private cloud) is more secure than having the gear off site and under another person's control (open cloud). This conveys awesome motivation to open distributed computing administration suppliers to organize building and keeping up solid administration of secure administration. This paper addresses design of proposed system.*

I. Introduction

Cloud Computing

Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud servic

es. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage. An example is introduced to identify the main motivation. In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. Thereinto, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

Objectives:

1. To develop a web based application that will provide user with file sharing options.
2. To provide data security with AES.
3. To provide time stamping to users based on time limit.
4. Saving cloud storage space with data compression.
5. Providing user with mail services for faster notifications.

II. Proposed Methodology

Problem Statement:

1. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc.

2. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks.
3. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability.

Proposed Architecture:
The proposed work is planned to be carried out in the following manner.

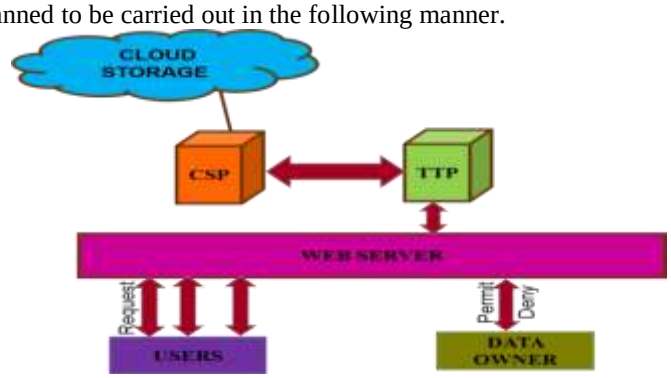

Figure 1 : System Architecture

However, most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions.

Here the secured system and data owner can decide whether the user can access the system or not. Access permission is totally depend on data owner. Access request itself cannot reveal the user's privacy.

III. Architectural Block Diagram of Proposed System

Activity diagrams are graphical representations of workflows of stepwise activities and action with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i.e. workflows). Activity diagrams show the overall flow of control.

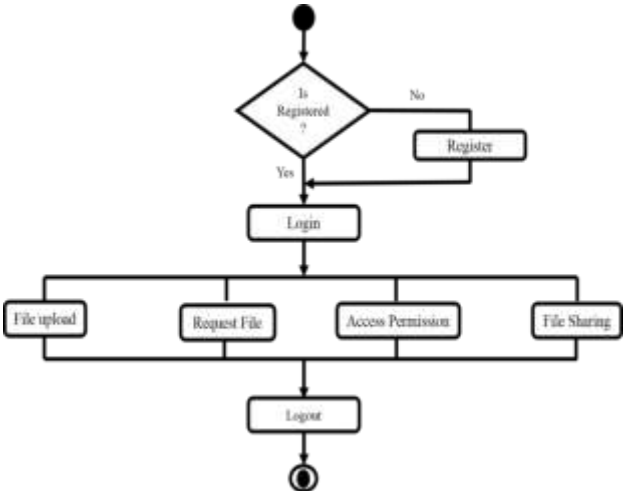

Figure 2 : Architectural Block Diagram of Project Flow

IV. Description About Each Block And Connectivity Between Each Block

4.1 Registration

In this module an owner has to upload its files in a cloud server, he/she should register first. And a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

Fig.(a): Login Page

This is the home page of the system. Using the login screen user can login to the system and if not register user can then click on the register button to open the registration form.

Fig.(b): Registration Form

Using this form user can register into the system, User need to upload a valid image as profile picture and proper email id. The system generates a random password and sends it to user mail id for email id verification.

4.4 Login

If the user is already registered then he/she can directly login to the system by using Email id and password and then user main page get opened.

Fig.(a): User Main Page

After login, user main page is opened on screen.

Fig.(b): Forgot Password

Using this form user can generate a new password for provided email id. The system generates a new password for the given mail id and then sends it to user email id.

4.4.3 File Upload

In this module Owner uploads the file(along with meta data) into database. The uploaded file was in encrypted form, only registered user can decrypt it.

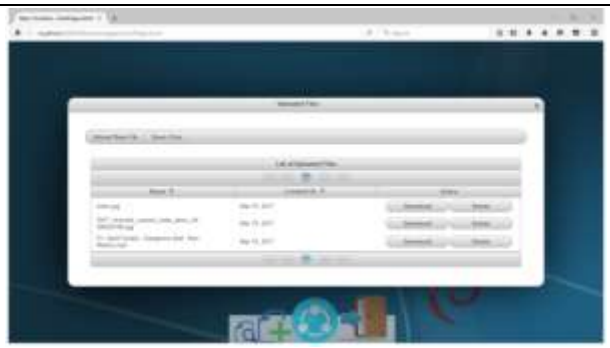

Fig.(a): File upload

Fig.(b): Choose file for upload a file

Fig. 4.4.3: File Uploading Forms

This forms are used to upload and save file to a server. First user need to click on upload file, a dialog appear for file browsing and selection. Once the file is selected user need to click on save file so the file can proceed for further operations.

4.4.4 Request File

In this module, if any registered user want to access the file stored on cloud, and that file is under privacy condition then that user have to request that file first to file owner and wait for approval. After requesting a file, one notification is send to the file owner's Email account.

Fig. 4.4.4(a): Request File Form

Ifany user want to access file, so he/she will first request file to data owner and wait for approval.

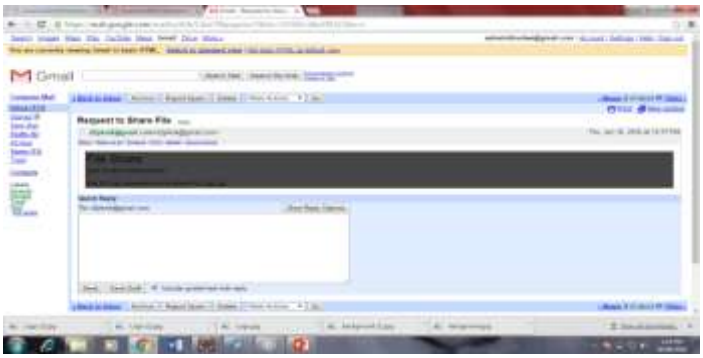

Fig. 4.4.4(b): Mail Notification To The File Owner

4.4.5 Access Permission

Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data. If owner want to share the file, one Email is send to the user who requested the file.

Fig. 4.4.5: Mail Notification to The User

4.4.6. File Sharing

In this module, if the data owner want to share file then he/she is login first then by selecting the file and the user to whom the file to be shared, the owner shares the file.

Fig.(a): File Share Form

Fig.(b): Selection Of File And User

This form is used to share multiple files to the multiple users. First the data owner have to click on share file, the chose the file as well as user to whom the file is to share.

V. Conclusion

Every segment in Cloud framework has its helplessness which may affect the entire Cloud's Computing security. Cloud computing business develops quickly notwithstanding security concerns, so coordinated efforts between Cloud gatherings would aid in overcoming security difficulties and push secure Cloud Computing administrations.

There is the issue of legitimate responsibility for information (If a client stores some information in the cloud, can the cloud supplier benefit from it?). Numerous Terms of Service assentions are quiet on the topic of proprietorship. Physical control of the PC hardware (private cloud) is more secure than having the gear off site and under another person's control (open cloud). This conveys awesome motivation to open distributed computing administration suppliers to organize building and keeping up solid administration of secure administration.

The proposed system provides security using Key Aggregation and AES encryption algorithm. These project servers an alternative to key management systems. The security provided is improvise using a random key generator which uses a key aggregation function. The proposed system can be used in any application which includes data sharing between users (either one to one or many to many) approach.

Reference

[1]. "Cloud Computing Security: From Single To Multi-Clouds" Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

[2]. "Ensuring Data Integrity And Security In Cloud Storage" Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

[3]. "Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage" Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

[4]. C. Cachin, I. Keidar And A. Shraer, "Trusting The Cloud", ACM SIGACT News, 40, 2009, Pp. 81-86. Clavister, "Security in The Cloud", Clavister White Paper, 2008.
[5]. [5] H.Mei, J. Dawei, L. Guoliang And Z. Yuan, "Supporting Database Applications As A Service", ICDE'09:Proc. 25thintl.Conf. On Data Engineering, 2009, Pp. 832-843.
[6]. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez "An Analysis Of Security Issues For Cloud Computing" Hashizume Et Al. Journal Of Internet Services And Applications 2013.
[7]. Sarita Motghare, P.S.Mohod, "Advanced Research in Computer Science". IEEE Transactions On Parallel And Distributed Systems Vol:pp No:99 Year 2014.
[8]. K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore ieee.org/stamp/stamp. jsp?tp=&arnumber=6311398, 2012.
[9]. L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.
[10]. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp .jsp? tp = & arnumber = 6374615, 2012.
[11]. S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.
[12]. S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services:Use Authentication for Social Enhancement of Home Networking,"IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp.1424-1432, 20