ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Privacy Preserving Mechanism for Data Integrity on Shared Data in the Cloud

Mohammad Rafath Ullah
M.Tech Student,
Lords Institute of Engineering and Technology
Himayathsagar, Hyderabad, Telangana, India.
email id: rafath526@gmail.com

T. Manohar
Associate Professor,
Lords Institute of Engineering and Technology
Himayathsagar, Hyderabad, Telangana, India.
email id: telugumanohar@gmail.com

ABSTRACT: ***Cloud computing is an emerging scenario in today's world. With the advent of new technologies new challenges associated with them to emerge, as in cloud computing. Cloud computing is faced by challenging issues like data security, data integrity, data duplication, authentication and authorization. Providing data integrity is a tricky task in cloud computing. the intricacy faced by the user at the time of storage management and storage maintenance can be reduced by cloud based data outsourcing in which a hassle free platform for data storage is provided which is of considerable low-cost, is scalable and is location-independent. To guarantee data integrity audit service are vital, audit services plays a significant role to ensure the integrity and accessibility of outsourced data and to achieve digital forensics and reliability on cloud computing.***

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data— while preserving identity privacy — remains to be an open challenge. In this paper, we propose the first privacy-preserving mechanism that allows data integrity on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.

KEYWORDS—cloud computing, data integrity in cloud Security, Cloud storage, Interactive proof system, Audit service streaming.

1. INTRODUCTION

With the new advent in technology, the traditional information systems are getting an easy substitute in the form of cold computing. Cloud computing is a rapidly growing and fast evolving technique. Cloud computing provides a scalable environment for budding amounts of data and that work is carried out on various applications and services by means of on-demand self-services. One of the fundamental characteristic of this paradigm shifting is that data are being centralized and outsourced into clouds. The outsourced storage service provides a comparably low-cost, scalable, location-independent platform for managing clients' data. Hence storage management and storage maintenance are taken care of by cloud storage service (CSS). Whereas clouds are quite susceptible to crashes or attacks or failures which could be irreparable, irretrievable, irreversible. It could incur huge loss of important and useful data.

The main reasons for these risks is that the cloud infrastructures are much more powerful and reliable than personal computing devices However, they are still vulnerable to security threats both from outside and inside the cloud (Armbrust et al., 2010); for the benefits of their possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users (Tchifilionova, 2011); furthermore, the dispute occasionally suffers from the lack of trust on CSP. Consequently, their behaviors may not be known by the cloud users, even if this dispute may result from the users' own improper operations (Ko et al., 2011).

Therefore, it is necessary for cloud service providers to offer an efficient audit service to check the integrity and availability of the stored data (Yavuz and Ning, 2009).

Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature schemes (Hsiaoet al., 2009; Yumerefendi and Chase, 2007), cannot work on the outsourced data without a local copy of data. More so ever, it is not a convenient solution for data validation. As might require downloading them which might be expensive especially for large-size files. Moreover, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users (Armbrust et al., 2010). Therefore, it is critical to realize public audit ability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds(Yan Zhu 2012).

2. CLOUD COMPUTING: OVERVIEW, ISSUES, AND CHALLENGES

Cloud computing one of the latest promising technology trends today, for its potential to be a "unsettling" technology. The goal of this section is to address the unique challenges and data integrity threats of cloud computing for practical application and utilization of Cloud Computing.

The data storage and computing are not in the local computer and server but in the amount of computer distributed in the internet in the cloud computing. The cloud computing move the tasks which are implemented in the personal computer and private data center into the larger computing center which are shared with total user and distributed in the internet. It compose applications out of loosely coupled services and one service failure will not disrupt other services.

The cloud computing system can be divided into two sections: the front end and the back end. They connect to each other through the internet. The front end is user who use the service provided by the back end which is the cloud section of the system. The cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals.

If the environment is built correctly, virtual servers will not be affected by the loss of a host. Hosts may be removed and introduced almost at will to accommodate maintenance. The virtual servers in the cloud computing system can be scaled out easily and if the administrators check out that the resources supporting a virtual server are being taxed too much in the real environment and they can modify the amount of resources allocated to that virtual server. The user need not computing and storage resource and don't provide the application in the cloud computing. The resource and server can be provided by the cloud computing. The cloud computing can be classified into private cloud, public cloud and hybrid cloud based upon the difference of service object. The hybrid cloud is the composition of two or more clouds and bounded by standard or proprietary technology. Hybrid clouds combine character of both public and private clouds.

The private cloud is deployed in the company and the security can be made easily. Private clouds are virtualized cloud data centers inside firewall and it is a private space dedicated to system within a cloud data center. Private cloud refers to internal data centers of a business or other organization not made available to the general public. The cloud system infrastructures are owned by an organization which sells cloud services to the general public or to a large industry company. The public cloud is running in the internet and the security is very complex. Public clouds are virtualized data centers outside of firewall and the service provider makes resources available to consumer on demand over the public Internet. The cloud computing is highly virtualized and standardized infrastructures and it can give more efficient and application management. It has the character of massive scalability and it can deliver more applications to large number of users. Cloud computing allows for flexibility, and capital and operational expenses for resources are only incurred when they are needed. The cloud computing is on-demand service and it give computing capabilities as needed automatically. It can use the service by many machine such as desktop, laptop, PDA and mobile phone. The cloud service model include SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).In the software as a service the consumer use the provided application and don't manage or control the network, servers storage and the application. It can reduce expenses and is easy to use and access everywhere. It share instance of a software application as a service accessible via internet browser or client based role access and sharing rules.

The service provider hosts the software so the user don’t need to install or manage or buy hardware for it.

All they have to do is connect and use it. The examples of SaaS are Flickr, Google Docs, Siri, Amazon and Cloud Drive. In platform as a service the consumer deploys their applications on the cloud computing system and controls their applications but they don't manage servers and storage and delivers a computing platform or solution stack as a service. It share platform for custom software application configuration, development, testing and deployment. The examples of PaaS are Google App Engine, Amazon Web services. In the infrastructure as a service the consumer get access to the infrastructure to deploy their application and system but they don't manage or control the infrastructure and they control the storage and applications. It share managed pool of configurable and scalable resources such as network, middleware, database and storage servers. The examples of IaaS is Amazon Elastic Compute Cloud (EC2). The cloud has the elastic character and resource allocation can get bigger or smaller depending on demand. The cloud also has the scalability and the cloud can scale upward for peak demand and downward for lighter demand There are many cloud computing systems in the market such as Google, Windows, IBM and Amazon. The Google cloud computing systems include GFS (Google File System), Map Reduce and Bitg table.

3. CLOUD INTEGRITY PROBLEM

As the cloud system runs over the internet security issues faced by the internet can also be faced by the cloud system. The cloud systems are quite similar to traditional systems i.e. pc and are vulnerable to special and new security issues. The major concerns about cloud computing are data integrity and privacy. The traditional security problems such as security vulnerabilities, virus and hack attack can also make threats to the cloud system and can lead more serious results because of property of cloud computing.

Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems. The data and business application are stored in the cloud center and the cloud system must protect the resource carefully. Cloud computing is a technology evolution of the widespread adoption of service oriented architecture, virtualization and utility computing over the Internet and it includes the applications, platform and services. If the systems meet the failure, fast recovery of the resource also is a problem.

The cloud systems hide the details of service implementation technology and the management. The user can’t control the progress of deal with the data and the user can’t make sure the data security by themselves. Data moving to any authorized place you need it, in a form that any authorized application can use it, by any authorized user, on any authorized device. Data integrity requires that only authorized users can change the data and Confidentiality means that only authorized users can read data. Cloud computing should provide strong user access control to strengthen the licensing, certification, quarantine and other aspects of data management. In the cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. The users do not know what position the data and do not know which servers are processing the data. The user do not know what network are transmitting the data because the flexibility and scalability of cloud system.

The user can't make sure data privacy operated by the cloud in a confidential way. The cloud system can deploy the cloud center in different area and the data can be stored in different cloud node. The different area has different law so the security management can meet the law risk. Cloud computing service must be improved in legal protection.

4. PROPOSED SYSTEM

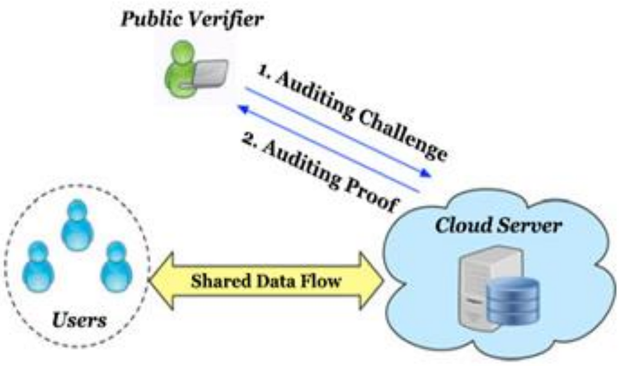
To come up securely and steadily an efficient third party auditor (TPA), the following two essential requirements have to be met:

1) The TPA should without introducing any further on-line difficulty to the cloud user be able efficiently audit the cloud data storage without demanding the local copy of data

2) The auditing process carried third party should not bring in new vulnerabilities towards user data privacy.

In this paper, we consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud.

ARCHITECTURE



Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic groups — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy. To solve the above privacy issue on shared data, we propose a novel privacy-preserving public auditing mechanism. More specifically a public verifier is able to verify the integrity of shared data without retrieving the entire data while the data of the signer on each block in shared data is kept private from the public verifier.

MODULES

1. Cloud Owner
2. Admin
3. Third Party Auditor
4. Data Sharing

Cloud Owner

- **Owner Registration**

In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

- **Owner Login**

In this module, any of the above mentioned person have to login, they should login by giving their email id and password.

Admin

- **Admin Login**

If Admin username and password are mentioned correctly then administrator can access the application .Administrator has all the powers such as it can access the account details of a cloud owner , shared file details , Admin can delete cloud owner ,ca view his/her files stored ..etc

Third party auditor

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- **ThirdPartyAuditor Registration**

In this module, if a third party auditor TPA(maintainer of clouds) wants to do some cloud offer , they should register first. Here we are doing like, this system allows only three cloud service providers.

- **ThirdPartyAuditor Login**

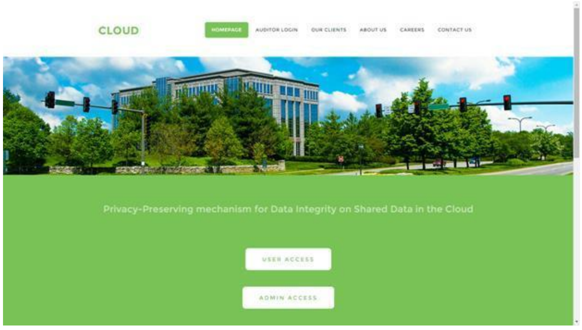
After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud. Here we are providing three TPA for maintaining three different cloud accounts.

- **Data Sharing**

We only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The cloud owner will decide to share data to whom in the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with *dynamic groups* — a new cloud owner can be added into the group and an existing group member can be revoked if illegal access case is found during data sharing against him

SCREENSHOTS

HOME PAGE

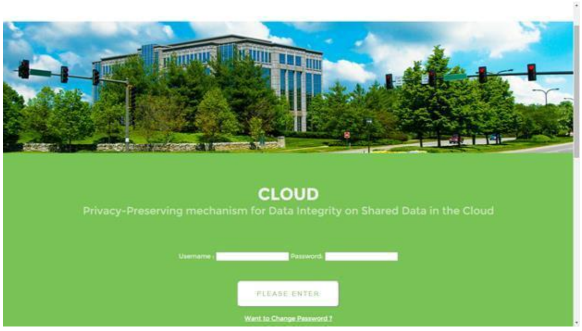


Privacy-Preserving mechanism for Data Integrity on Shared Data in the Cloud

Fig: Home Page

The home page can be seen with two buttons for access to user and admin respectively.

ADMIN LOGIN PAGE

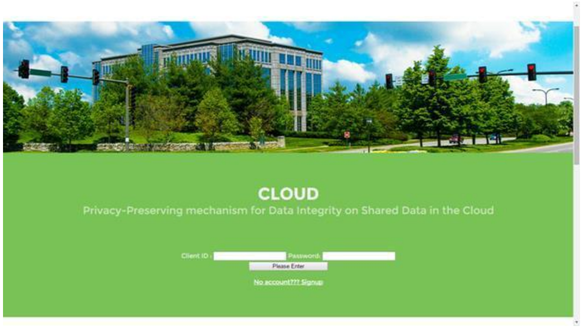


Privacy-Preserving mechanism for Data Integrity on Shared Data in the Cloud

Fig: Admin Login Page

- Admin can log in by clicking on ‘Admin Access’ button.
- Admin needs to enter the username and password. Then he has to click on ‘Please Enter’ button.

CLOUD OWNER LOGIN

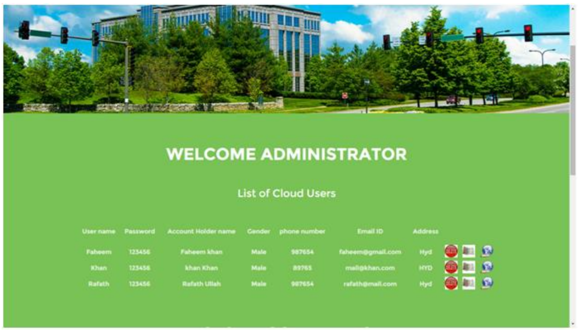


Privacy-Preserving mechanism for Data Integrity on Shared Data in the Cloud

Fig: Cloud Owner Login Page

- Cloud owner can log in by clicking on ‘User Access’ button.
- User needs to enter the clientid and password.
- Then he has to click on ‘Please Enter’ button.

ADMIN WINDOW



WELCOME ADMINISTRATOR

List of Cloud Users

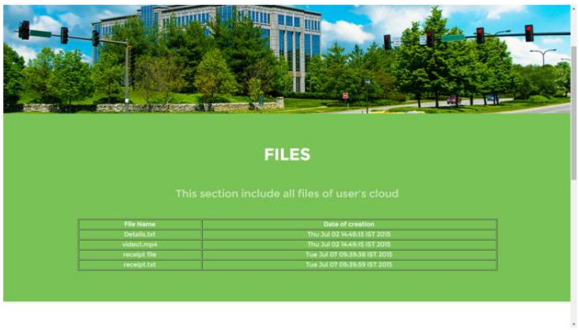
User name	Password	Account Holder name	Gender	phone number	Email ID	Address
Faheem	123456	Faheem khan	Male	987654	faheem@gmail.com	Hyd
Khan	123456	khan Khan	Male	89765	mail@khan.com	HYD
Rafath	123456	Rafath Ullah	Male	987654	rafath@mail.com	Hyd

Fig: Administrator Window

As the Administrator logs in, he/she will be able to view the list of cloud uses. Beside each user you can see 3 icons.

- He can view the file details of the cloud owner
- He can see the list of received files by the cloud owner and
- He can delete the cloud owner.

FILE DETAILS OF CLOUD OWNER



FILES

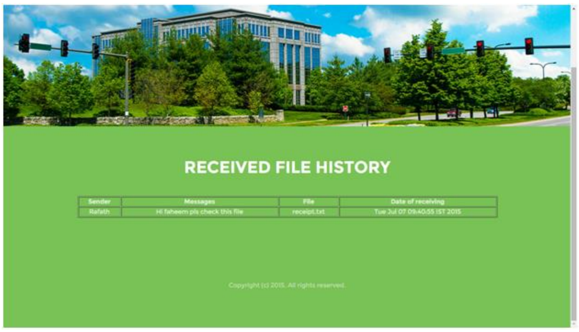
This section include all files of user's cloud

File Name	Date of creation
Details.txt	Thu Jul 02 14:48:13 IST 2015
video1.mp4	Thu Jul 02 14:49:15 IST 2015
receipt file	Tue Jul 07 09:39:38 IST 2015
receipt.txt	Tue Jul 07 09:39:59 IST 2015

Fig: File details of cloud owner as seen by Administrator

- Administrator can view the file details of each cloud owner.
- Information such as file name and the date of creation of each file is shown.

RECEIVED FILES BY CLOUD OWNER



RECEIVED FILE HISTORY

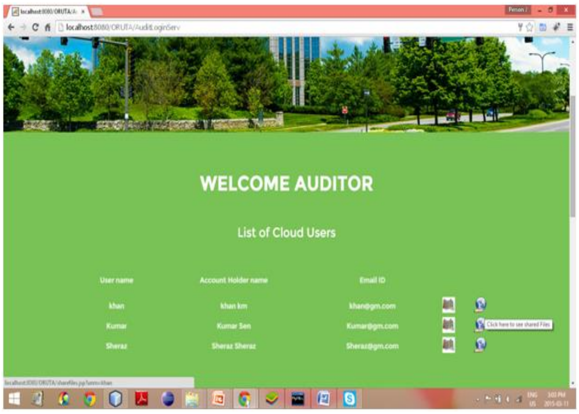
Sender	Messages	File	Date of receiving
Rafath	Hi faheem pls check this file	receipt.txt	Tue Jul 07 09:40:55 IST 2015

Copyright (c) 2015. All rights reserved.

Fig: Received File History of cloud owner as seen by Administrator

- Administrator can view the received file history of each cloud owner.
- All the files received by each cloud owner will be shown.
- Information such as sender, messages, file name and the date of receiving of each file is shown.

AUDITOR WINDOW



WELCOME AUDITOR

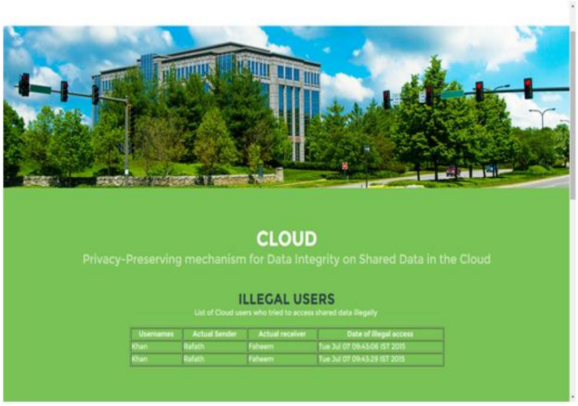
List of Cloud Users

User name	Account Holder name	Email ID
khan	khan km	khan@gm.com
Kumar	Kumar Sen	Kumar@gm.com
Sheraz	Sheraz Sheraz	Sheraz@gm.com

Fig: Auditor Window

- After the Auditor logs in by clicking on 'Auditor Login' from the home page, he will see the details of each Cloud Owners.
- The details such as User Name, Account Holder name and Email Id is shown. Beside each row, two icons can be seen.
- One is to see the file details of the cloud owner and the other is to see the information about the received files by the cloud owner.

AUDITOR ILLEGAL USER ACCESS VIEW



CLOUD

Privacy-Preserving mechanism for Data Integrity on Shared Data in the Cloud

ILLEGAL USERS

List of Cloud users who tried to access shared data illegally

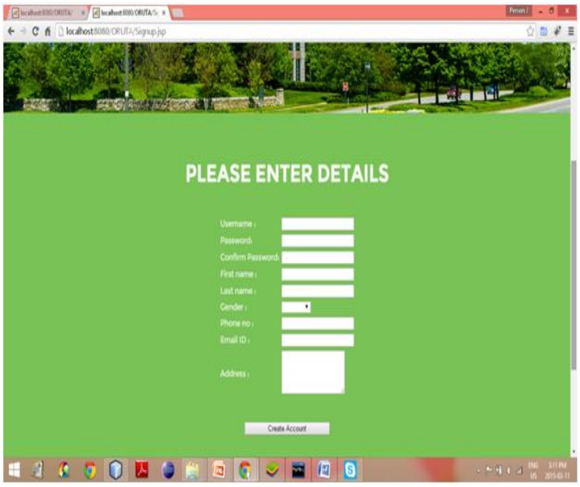
Usernames	Actual Sender	Actual receiver	Date of illegal access
Khan	Rafath	Faheem	Tue Jul 07 09:43:06 IST 2015
Khan	Rafath	Faheem	Tue Jul 07 09:43:29 IST 2015

Fig: Auditor Illegal User Access View

- After the auditor logs in, he can see a tab to see the list of illegal users.

- Illegal users are those users who have tried to access the file owned by a cloud owner that was shared for some other user.

CLOUD OWNER REGISTRATION



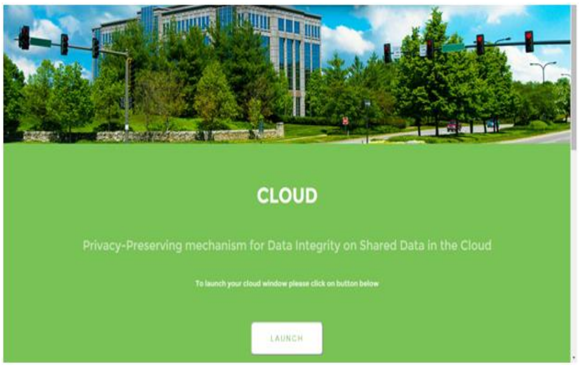
PLEASE ENTER DETAILS

Username :
Password :
Confirm Password :
First name :
Last name :
Gender :
Phone no :
Email ID :
Address :

Fig: Cloud Owner Registration

- Cloud Owner has to register first before trying to log into the system.
- The details such as username, password, first name, last name, gender, phone number, email id and addresses are to be entered.
- After the Cloud Owner successfully creates an account, he can log into the system by entering his username and password.

CLOUD OWNER WINDOW ACCESS



CLOUD

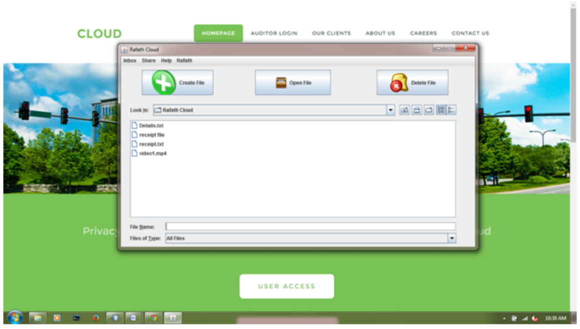
Privacy-Preserving mechanism for Data Integrity on Shared Data in the Cloud

To launch your cloud window please click on button below

Fig: Cloud Owner Window Access

- As the Cloud Owner successfully logs into the system with his/her username and password, he/she will see a 'Launch' button.
- Clicking on 'Launch' button will show the Cloud Owner window.

CLOUD OWNER WINDOW



Look In: Rafath Cloud

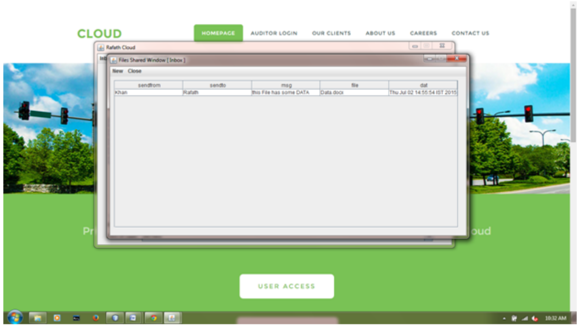
Details.txt
receipt file
receipt.txt
video1.mp4

File Name:
Files of Type: All Files

Fig: Cloud Owner Window

- After the Cloud Owner successfully logs into the system and clicks on 'Launch' button, he will see the Cloud Owner Window.
- The window shows the list of files associated with the Cloud Owner.
- Through this window the Cloud Owner can create the file, open the file and delete the file.
- Apart from this he can see the inbox and also share his files with other Cloud Owners.

INBOX OF CLOUD OWNER

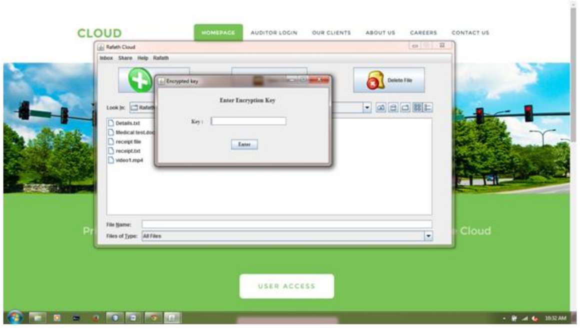


sendfrom	sendto	msg	file	dat
Khan	Rafath	this File has some DATA	Data.docx	Thu Jul 02 14:55:54 IST 2015

Fig: Inbox of Cloud Owner.

- Inbox of the Cloud Owner shows all the files that were shared with the Cloud Owner.

ENCRYPTION KEY TO ACCESS NEW FILE



Enter Encryption Key

Key :

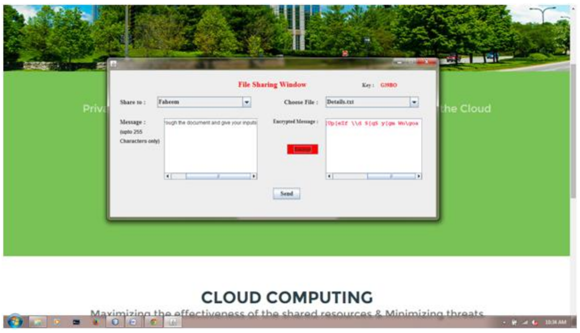
Enter

Fig: Encryption Key to access new file.

- When a Cloud Owner wants to see a new file that has been shared with him/her, then he needs to click on 'New' from his/her inbox.

- He will see a popup asking to enter the encryption key. On successfully entering the encryption key, the Cloud Owner will see the file that has been shared with him/her.

CLOUD OWNER SHARE FILE WINDOW


Send
CLOUD COMPUTING
Maximizing the effectiveness of the shared resources & Minimizing threats

File Sharing Window

Key : G39BO

Share to : Faheem

Choose File : Details.txt

Message : (upto 255 Characters only) rough the document and give your inputs

Encrypted Message : |Op|eZf \\d $[q$ y[qm Wn\goa

Fig: Cloud Owner Share File Window

- Cloud Owner can share the files present in his/her cloud by clicking on 'share' menu.

- On clicking 'share' menu, he will see a window through which he can select the User to whom he want to share the file.

5. CONCLUSION

On the one hand Cloud Computing offers some implausible benefits like unlimited storage, scalability, elasticity, platform independent, low-cost and reliability. access to quick processing power and the ability to easily share and process information, on the other hand though, it does have several issues, and most of which are security related. Cloud systems must overcome many short comings before in order to be widely accepted. Several security issues currently affect cloud systems, however, there may be many undetermined, unstipulated, unspecified and undiscovered security issues.

Therefore there is still a need for optimal solutions if cloud systems are to be widely adopted. Data integrity these problems hinder the development of cloud computing and the security issue is the core problem. In this paper, discussed the construction of an efficient audit service for data integrity in clouds. We proposed an interactive audit protocol to implement the audit service based on a third party auditor.in this the TPA issues a periodic verification to scrutinize outsourced data . for this the security of TPA has to be maintained This approach greatly reduces the workload on the storage servers, while still achieves the detection of servers' misbehavior with a high probability.

REFERENCES

[1] SOFTWARE ENGINEERING – A PRCTITIONER'S APPROACH by Roger S.Pressman

[2] The Complete Reference to Java Seventh Edition. By Patrick Naughton and Herbert Schildt.

[3] Object Oriented Programming through JAVA by P Radha Krishna.

[4] Understanding OOP with Java, updated edition, T.Budd, Pearson education.

[5] Grady Booch,James Rumbaugh, Ivar

Jacobson: The Unified Modeling Language User Guide, Pearson Education.

[6] Atul Kahate: Object Oriented Analysis & Design, The McGraw-Hill Companies.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[8] R. L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2001, pp. 552– 565.

[9] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” in Proc. In-ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416– 432.

[10] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2008, pp. 90– 107.

[11] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, “Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds,” in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 534–542.

[13] D. Boneh, B. Lynn, and H. Shacham, “Short Signature from the Weil Pairing,” in Proc. International Conference on the Theory an Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 514–532.

[14] D. Boneh and D. M. Freeman, “Homomorphic Signatures for Polynomial Functions,” in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2011, pp. 149–168.

[15] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, “Practical Short Signature Batch Verification,” in Proc. RSA Con-ference, the Cryptographers’ Track (CT-RSA). Springer-Verlag, 2009, pp. 309–324.