Security Audit on Cloud data Storage

[1]Heyshanthinipandiyakumari S, [2] Dr. B. Rajalakshmi, [3]Bindu V S

[1]Assistant Professor, [2]Professor, [3]M.Tech Student,
[1,2]New Horizon College of Engineering, Bangalore, India
[3]Department of Computer Science and Engineering,

Abstract: Cloud computing provides on-demand and online services for to store the data and to provide network related services. The data in the cloud must be secured enough as it's a source of information to all the data owners. Using cloud storage users can remotely store their data enjoy the on demand high quality applications and services from a united pool of computing resources, without burden to data storage and maintenance. To securely maintain, the data encryption and decryption mechanisms are being carried out. Even though the data is being hacked, to avoid this we introduce a third party authentication scheme. Where its role is to authenticate the user and to provide permission at every task he performs. The secured cloud storage processing with public auditing is being carried and data privacy is attained. The data in cloud is made backup and is being checkup with its backup while it's being accessed. In case if the data is hacked even then the data present in backup is given. The identification and encryption of data is done using RSA algorithm. Efficient auditing plays a crucial role in securing the cloud environment. Users no longer have physical control of the outsourced data makes the data integrity protection in cloud computing a formidable task.

***IndexTerms* - cloud computing, data auditing, network security and third party authentication.**

I. INTRODUCTION

Cloud computing is mainly based for allowing worldwide, convenient , on-line network service access for to combine all the computing resources like several networks, accessible servers, storage data and application. Which can be examined with little effort and can be brought up to the service level interactions. If one wants to start his own company he has to accommodate several resources, servers, man power, credentials, place of execution etc., but cloud makes all this to run in one environment by providing its services. Hence it provides many services like platform as a service, infrastructure as a service and software as a service. Where different services are delivered to an organization's computers and device through the internet [5]. Cloud computing plays a major role in the field of information technology of storing and managing the resources even carrying of the application related task. However there are still some problems that the end user is having regarding the deployment of application on the cloud. To solve these issues many ways were proposed and the security to each of them also played an important role in managing the cloud [7]. Data security is one of the most weighty hurdle in its adoption to itself with the environment which has several issued regarding its privacy maintains, trust on the work, compliance and legal matters. Therefore, one of the important goal here is to maintain security and integrity of that data stored in the cloud because of the critical natural of cloud computing and large amount of complex data it carries. The users concerns for security should be rectified first to make cloud environment trust worthy. Only then all do believe and use of it increases at faster rate.

The problems associated with data that resides in cloud are privacy for the data, protection of data, data availability, data positioning, and secure transfer of data. Other problems that affect the data in the cloud are with loss of data, intruders malfunctioning, Threats to the data, improper functionality of services, are the security challenges of the cloud. Data resides longer time on the cloud. The data in the cloud cannot be accessed directly by the end user instead a service provider plays a major role in servicing the end user when requested. To this to happen in a proper fashion ever time the integrity of data is also maintained. The data loss must not occur and even it must not be modified by any malicious user [2]. The cloud computing service providers must maintain the integrity, consistency of the data. Private and confidential data must be secured. As the data access is only given to the authorized user. The confidentiality is maintained by access control strategies of cloud. The data confidentiality to the end user is given out by building the trust and increasing the reliability, fault tolerance of the system. To keep track and maintain all these parameters new implementations should be brought out. Finally if these are achieved new enhanced advancements are done in the field of cloud technological computing. To believe that the data is secured many cryptographic technique are followed. This is the only reason that all people of different fields like business, banking, information technology, health, government and others do trust this platform to store their data on the cloud. The data related to the end users are kept in confidential and ensures privacy. As cloud has huge amount of data it is been made dynamic in nature. The system must be adoptable even when storage exceeds its capacity which means it's scalable in nature [1].

As the resources are becoming dynamic, scalable and virtualized, the data has to be more secured in cloud. Therefore, auditing is taking more attention for increased complexity of cloud resources for the researches today. The auditing method makes storing and sharing of data easier in cloud. Various cloud computing types include public, private, hybrid and community based clouds used for data and application on the network resources and various security policies. Data stored, processing and movement of data outside the controls of an organization poses an inherent risk and making it vulnerable to various attacks [3]. Privacy preserving is an important issue in business because the user who is accessing the cloud files may changes the contents of the original file which may lead to legal consequences in future. Therefore, security is the biggest concern when it comes to cloud computing environment. The main challenge here is to deal with the security and privacy concerns of business thinking of adopting it. Hacking the cloud system and network infrastructure would affect many business clients as well as their profit which seriously need to be thought.

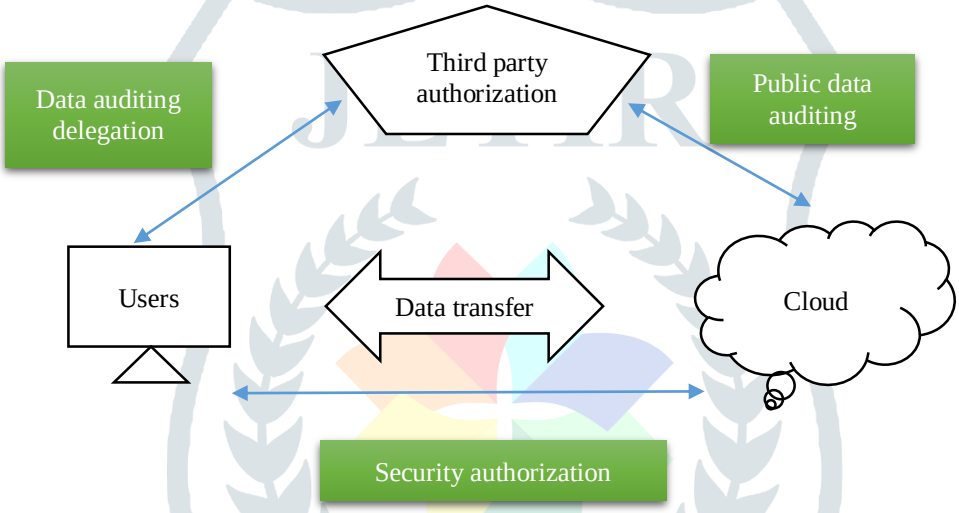
II. RELATED WORK

To secure the cloud system a storage auditing with privacy preserving protocol has been built. The auditing system in cloud has many requirements of the user, services of the cloud to meet the auditing requirements of the user and technical approach for security auditing. The problems that are involved in security auditing are mainly infrastructure security and data security issues. The data security provides privacy preserving protocol for auditing [4]. This is the public auditing system. Where the infrastructure security provides technology related auditing. This schemes have audits done by external source to audit outsource data in cloud. The goal here is to preserve the privacy of the user data in public cloud. The scheme has external auditor to audit outsourced data in could. The main goal is to achieve privacy preserving public auditing system for cloud data storage. This public auditing scheme allows third party authority to check the correctness of data that resided in cloud [6].

The data storage security for the public audit is a dynamic data operation for block insertion. Cloud computing supports an efficient public auditing for holomorphic authentication. This scheme provides batch auditing for multiple tasks by using third party authentication. This batch processing for multiple task is used for file authentication. This supports public auditability and data dynamic operations. Integrity of outsourced data is checked using privacy preserving audit service. This achieves public auditability and dynamic data operations. The privacy preserving public auditing system is used to carry out public auditability on cloud information.

III. SYSTEM DESIGN

Cloud system model comprises of four entities namely client, auditor, hacker and cloud server. The architecture of the proposed system is given in the below diagram.



1. The Client [Data owner] – data owners are the end users who store their data on the cloud.
2. Cloud storage provider [CSP] — Cloud storage provider maintains Cloud storage service which is having a large space for storage of data. They provides data storage service and has lot amount of storage space.
3. Data Receiver – the person who gets the data sent by the data owner.
4. Third party auditor or TPA — TPA is an auditor who verifies the user's data. It monitors outsourced data under the assignment of data owner.
5. Hacker- The hacker or the third party intruder stores multiple user processes and transaction into the index table. The user processes and administrator process transactions are indicated in this phase.

1V IMPLEMENTATION

The system is designed and developed to check out the correctness of the data present in the cloud by using TPA. It also promises that no data is leaked to third party authority during the process. It maintains the data stored to be secured and correct. The system proposed contains 5 basic entities, those are data owner who sends the data, cloud which stores the data, third party authority is one who grants the permissions for every activity which is carried on, data receiver who gets the data and hacker is one that changes or modifies the data. Their responsibilities are to split up the file into block and encrypt the blocks using AES algorithm, each block encryption is carried on by SHA-2 hash value. Here we see every data file is broken downed into four equal halves and the encryption mechanism is done. As the data generated is by hash value. It is not possible to decode it. Later on the hashes are combined to generate RSA signature. Which is helpful at the receiver side to decode the data. These block are stored in cloud. Data owner has to get registered before uploading a file. The TPA has to permit the data owner for his activities. The uploaded file is broken and hash is applied on it. Finally generating the encrypted data. Data is transferred to the receiver. Verification processes is carried on where the signature generated by TPA and the one stored in the TPA of that file is which is provided by the data user are compared by the TPA.

In the verification process, the signature generated by TPA and the one stored in the TPA which is provided by the data user are compared by the TPA. If they matches with each other it means that the data is intact and data is not been tampered by any outsider or attacker. If it does not matches then indicates that the data integrity has been affected or tampered. The result for the data integrity check is provided to the data owner.

Data owner is an important part of our proposed system. It performs most of the responsibility related to the data. In the proposed auditing scheme, the data owner first performs login and registration with cloud server and TPA. The new user has to firstly register itself by filling the registration form and be the active member of the system. A message for successful registration will be provided. If a user is already the member of the system then he or she can perform login process. If the user name and password exist in the database, then they will be login successfully for being for being valid users or else they will receive an error message.

Once successfully login, the data owner will select the file he or she want to store on cloud serve. The file selected by him will be split into number of blocks. In order to carry out the splitting of the required file into blocks a file splitter algorithm is used. In this algorithm, we check if the file exist or not. If exist then the file is split in specific size based up on the file size. For example if the file is of size 23kb then it will be split into 20kb and 30kb. Here in the example the size specified to split a file is 20kb. Next, we are using a strong encryption algorithm.

1V RESULTS

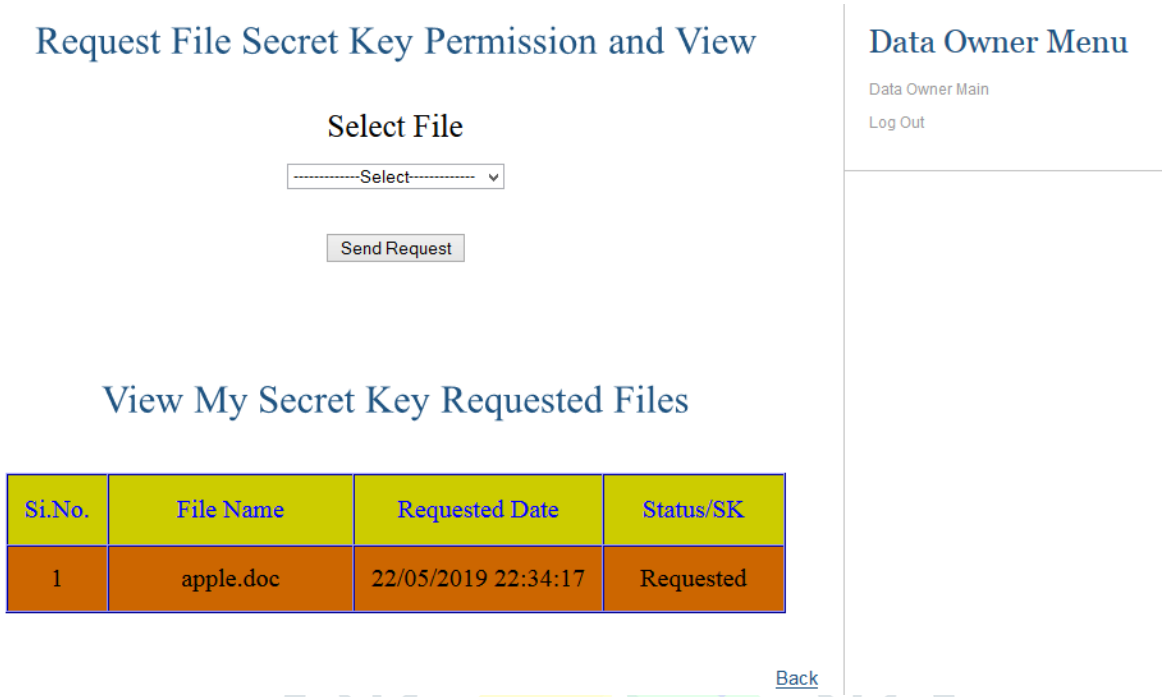


Fig1: Request file Secret key permission and view

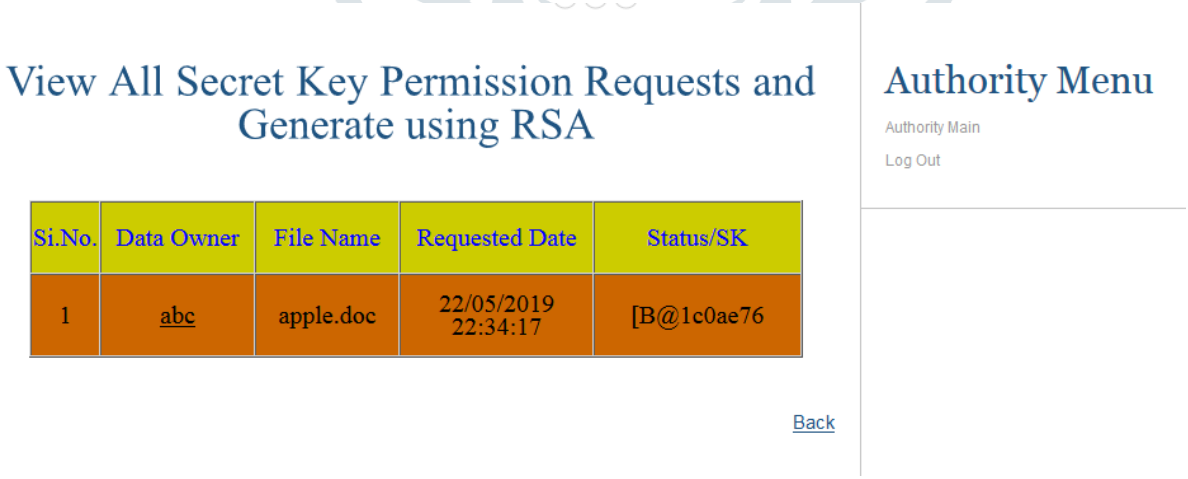


Fig2: View all secret key permission request and generate using RSA

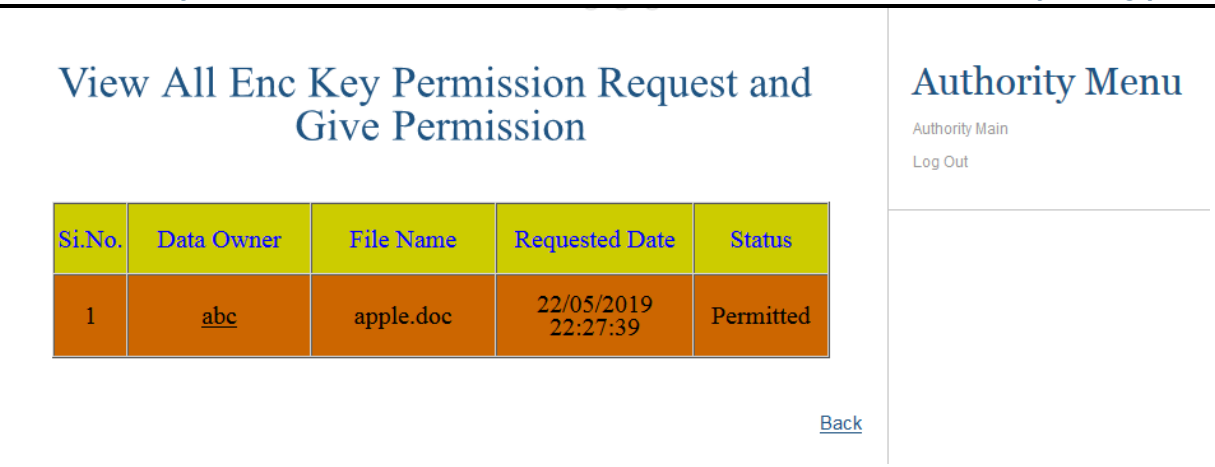


Fig3: View all encryption key permission request and give permission

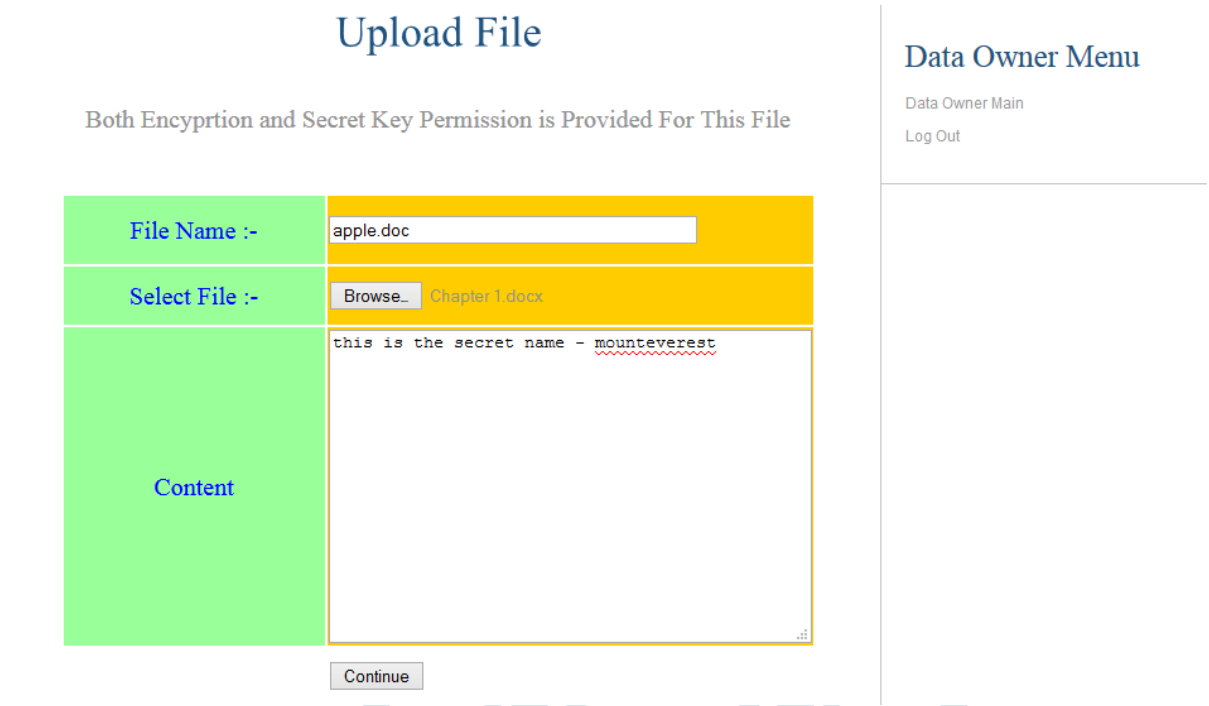


Fig 4: upload file

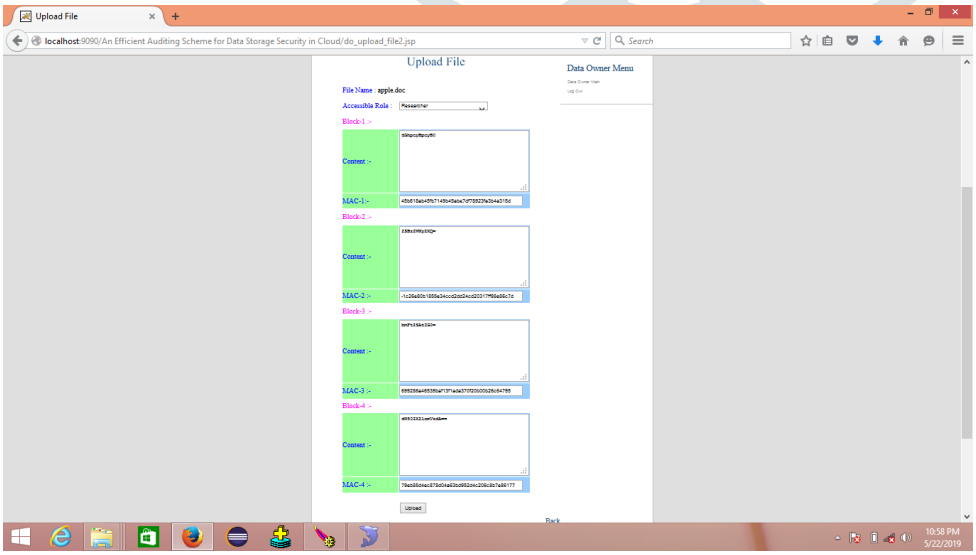


Fig5: Block encryption using RSA

Request Decrypt Key from AA and View Response

Data Receiver Menu

Data Receiver Main

Log Out

Si.No.	File Name	File Size	Status/Response
1	mango	35	Send Request

Back

Fig6: Request decrypt key from AA and view response

View Decrypt Key Requsest from User and Give Permission

Authority Menu

Authority Main

Log Out

Si.No.	Data User	File Name	Requested Date	Status
1	xyz	mango	22/05/2019 23:36:21	Permitted

Back

Fig 7: View decrypt key request from user and give permission

Request Secret Key from AA and View Response

Data Receiver Menu

Data Receiver Main

Log Out

Si.No.	File Name	File Size	Status/Response
1	mango	35	Send Request

Back

Fig8: Request secret key from AA and view response

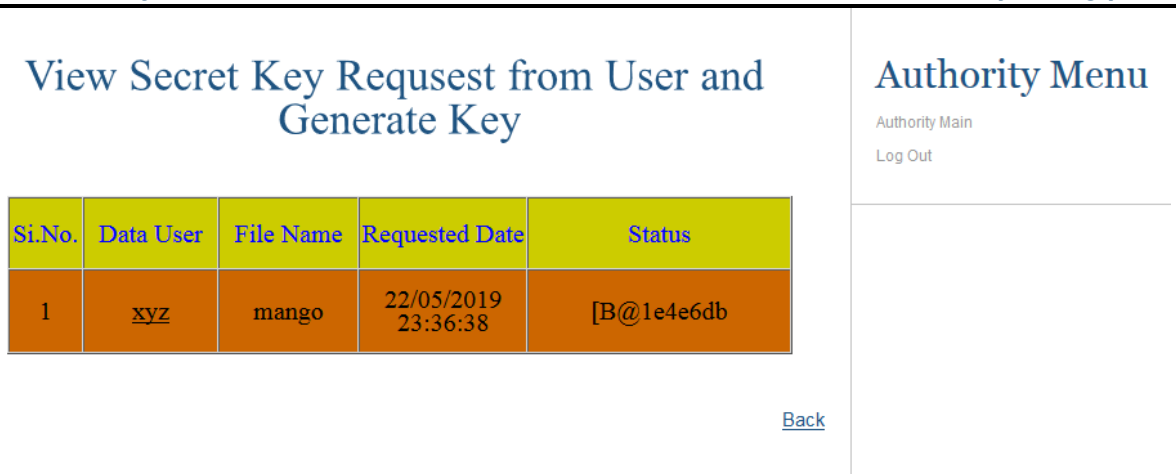


Fig 9: View secret key request from user and generate key

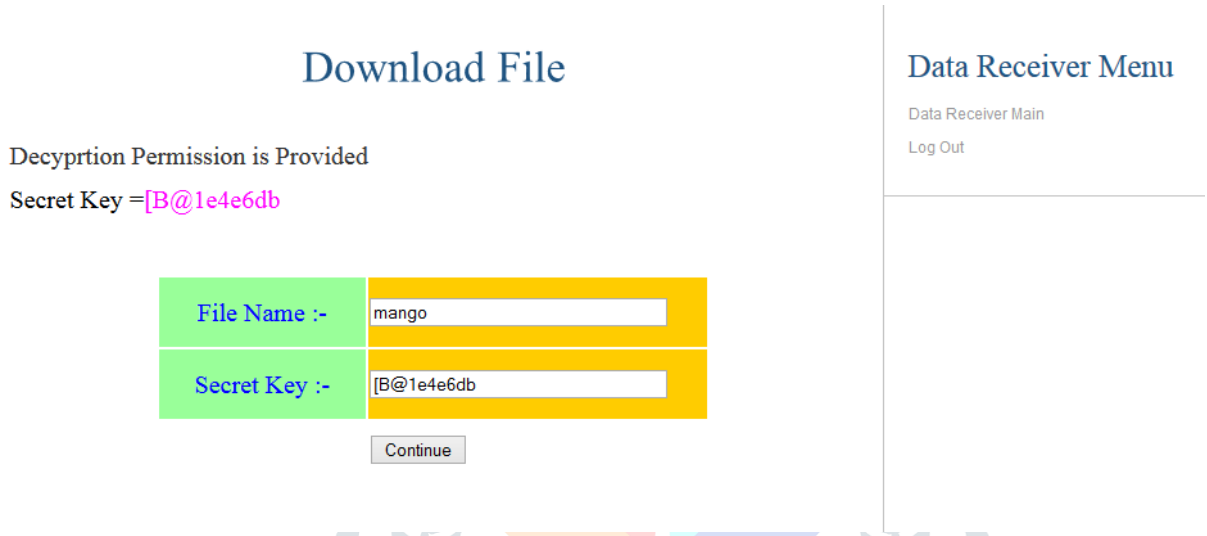


Fig 10: Download file

CONCLUSION

The data in cloud is secured and privacy is maintained. Data is split into parts and then stored in the encrypted format in the cloud storage, thus maintaining the confidentiality of data. The integrity is verified by TPA on request of the client by verifying both the signatures. It only check whether the stored data is tampered or not informs about it to the user. An attempt is made to overcome the limitations of the existing auditing scheme. All the modules in the system are implemented to develop an effective auditing scheme. The public auditing system is presented which provides a privacy preserving auditing protocol. The scheme supports a special auditor to audit the user's data in the cloud without accessing the actual data contents.

REFERENCES

[1] Dr B Rajalakshmi, Ravishankar, Heyshanthinipandiyakumari S , Srujani J, "A Comparision of Load Balancing Approaches in Cloud: ELOB" IJSRCSAMS Vol 7, 2018.

[2] M. Nazir, N. Bshardwaj, R.K. Chawda, R.G. Mishra, "Cloud computing: Reviews, Surveys, Tools, Techniques and Applications – An open-access ebook by HCTL open" ISBN-13.

[3] K. Ruth Ramya, T. Sasidhar, D. Naga Malleshwari &M.T.V.S. Rahul, "A review on security aspects of data storagein cloud computing", International Jounal of AppliedEngineering Research, Vol 10, No 5, 2015.

[4] Hassan Rasheed, "Data and Infrastructure security auditingin cloud computing environments", International Journal of Information Management, 2014.

[5] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacypreservingpublic auditing for data storage security in cloud computing", IEEE INFOCOM 2010.

[6] M.Venkatesh, M.R. Sumalatha and C. Selvakumar, "Improving public Auditability, data possession in data storage security for cloud computing", IEEE, 2012.

[7] C.Wang & K.Ren, "Toward publicly auditable secure cloud data storage services", 2010, IEEE Network