International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 07, July-2019

An Efficient Mechanism to Provide Secrecy and Integrity of Sensitive Data in Cloud

M.V.S.Mahalakshmi[1], Sripada Rama Sree[2]

[1] *Department of Computer Science and Engineering, Aditya EngineeringCollege, Surampalem, JNTUK,A.P,*
[2]*Professor, Department of Computer Science and Engineering, Aditya Engineering College, Surampalem,JNTUK,A.P,*

Abstract: Cloud computing is a fast growing technology which is a form of Internet based computing that offers shared computing processing resources which provide storage as the service to users on demand. Due to the storage of data at cloud server, the integrity of data which is stored at the cloud server is the basic consideration of the users, because there is a chance that the data stored at cloud server can be modified, attacked or damaged by the attackers. In order to avoid this, the proposed mechanism implements privacy-preserving public auditing scheme for regenerating code-based cloud storage. In this scheme TPA is used to maintain integrity of the data and proxy is used to regenerate data blocks on corrupted servers during the repair process.

Keywords: TPA, Proxy, Regenerating code, privacy-preserving, cloud storage.

I. INTRODUCTION

Cloud computing is stated as availability of computer resources, particularly computation power and data storage on demand. Cloud computing is everywhere because users can access system using a web browser at any location via the internet. As per NIST the definition of cloud computing is described as "It is a way for enabling convenient, ubiquitous, on-demand network access to a shared pool of the configurable computing resources (e.g. servers, services, storage, networks etc.,) which rapidly provisioned and also released with the minimum management support"[1]. The Services that mainly offered by Cloud computing providers as per NIST are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2].

Services of cloud:

1) Software as a Service (SaaS):

SaaS model offer users to get access to the databases and application software. In this model, Cloud service provider handles the platform and infrastructure that helps to run the required applications. Application software provided by Saas is as pay per use to the end users. In this, the required application software can be installed and operated at cloud by cloud service providers and the cloud users will use the application software such that there is no need to install the application software on our device. (E.g. Google Applications, Sales force).

2) Platform as a Service (Paas):

PaaS is used to provide software as well as hardware equipments for the developers such that they can create, run and test the required applications. Google Apps Engine, Windows Azure are some examples of Paas.

3) Infrastructure as a Service (Iaas):
IaaS offers cloud computing infrastructure in virtual environment. The customers can access the resources like storage, operating system etc (e.g. Amazon Web Service, Microsoft Azure).

Cloud Computing Characteristics:

- On-demand self service is defined as the computer system services like applications, email, server service etc will be available without the requirement of human communication with the cloud provider. Cloud providers include Amazon Web Services, IBM, and Google etc.
- Resource pooling can be stated as computational resources which are combined together to offer services to many end users. In resource pooling, the resources which are used are network bandwidth, storage, processing and memory etc.
- Rapid elasticity is defined as the resources that can be rapidly as well as elastically provisioned. In this, appending the resources can be done by scaling up the systems and this scaling can be manual or automatic.
- Measured service is defined as the usage of cloud resources that need to be measured. Cloud computing service uses a meter system that helps to manage and optimize the resource usage which means that if one user uses more resources then that user need to pay more.

II. RELATED WORK

In 2007, Ateniese [3] has proposed Provable of Data Possession model(PDP). In this model, for auditing the data which is outsourced, homomorphic verifiable tag is used. However this PDP model is only applicable to the static data of a file and it does not provide dynamic data operations. Wang [4] proposed a protocol which provides data dynamics and public auditing by utilizing the HLA scheme which is based on BLS together with the Merkle Hash Tree. In this, proposed protocol gains the integrity of data, still this protocol failed in gaining the confidentiality of the data which is stored at cloud. Meenakshi[5] proposed a model that uses TPA for auditing the stored data of cloud users with the help of Merkle Hash Tree (MHT) algorithm. This protocol provides data dynamics, but it is unsuccessful to achieve data confidentiality which is stored at cloud server. Kaliski and Juels[6] proposed a protocol called Proof Of Retrievability(POR) that can be used for analyzing the integrity and availability of data that is outsourced. This model uses error-correcting code method as well as spot-checking method to assure the possession and retrievability of data on remote nodes. But limited number of queries can only handle in this scheme and also it does not gain public auditability. An improved POR Scheme is proposed by Waters and Shacham [7]. In this Public auditable scheme is achieved with the help of secure BLS signatures. However, this scheme does not support Privacy preserving.

III. PROPOSED WORK

In this paper, proposed the public auditing scheme for regenerating code based cloud storage. The proposed system is developed to verify correctness of the cloud data using TPA. During this process of auditing it ensures that no data is revealed to TPA. It provides the confidentiality and integrity of stored data. In the proposed scheme four basic entities are considered. They are: Data owner, TPA, Cloud Service Provider and Proxy.

Data Owner:

Data Owner wants to store huge volume of data files at cloud server. Before data stored at cloud server, user need to be registered. Following steps need to perform during data file uploading.

1. Data Owner generates secret key to encrypt the data file that is stored at the cloud.
2. While storing data in cloud, data is encrypted by AES-256 bit algorithm to maintain secrecy.
3. If Data Owner wants to view the file he needs to enter filename And secret key
4. Data Owner downloads the file if necessary.

Third Party Auditor:

TPA is to ensure the correctness of stored data at cloud. TPA should essentially audit the data properly without deriving user's data content. That is it must have no knowledge about the stored data at cloud server so that preserving the privacy of stored data can be achieved.TPA examines the data uploaded at cloud and data owner data to assure the integrity of data.

Cloud Service Provider:

Cloud service provider is used for delivering the services like data storage and has necessary space for data and computing assets.

1. Deals with received data file which is uploaded by data owner.
2. The data uploaded by data owner is stored in three servers.
3. Each server divides the file content into blocks.

Proxy:

A proxy regenerates data block on the failed servers on behalf of data owner during repair procedure of the data.

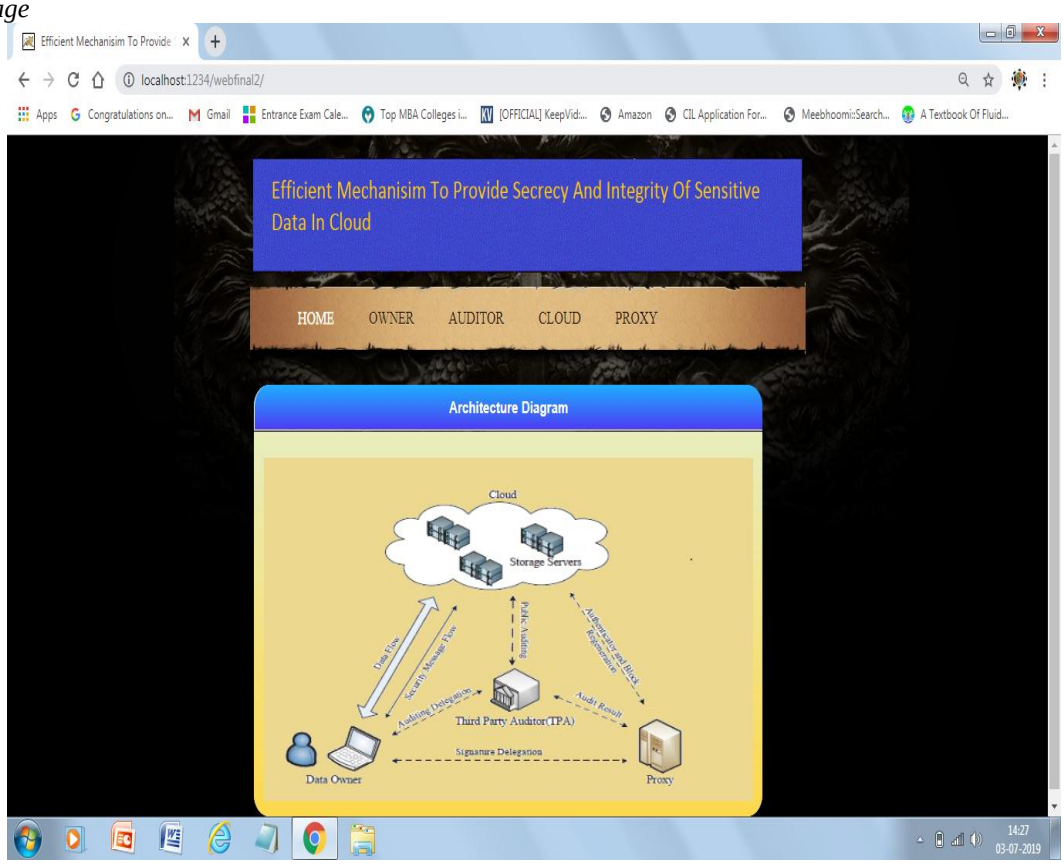
1. Proxy connects with cloud server and repairs the blocks in false server
2. That is proxy regenerates data blocks if the data blocks get damaged.
3. Damaged block is replaced with regenerated data block.

IV. EXPERIMENTAL RESULTS

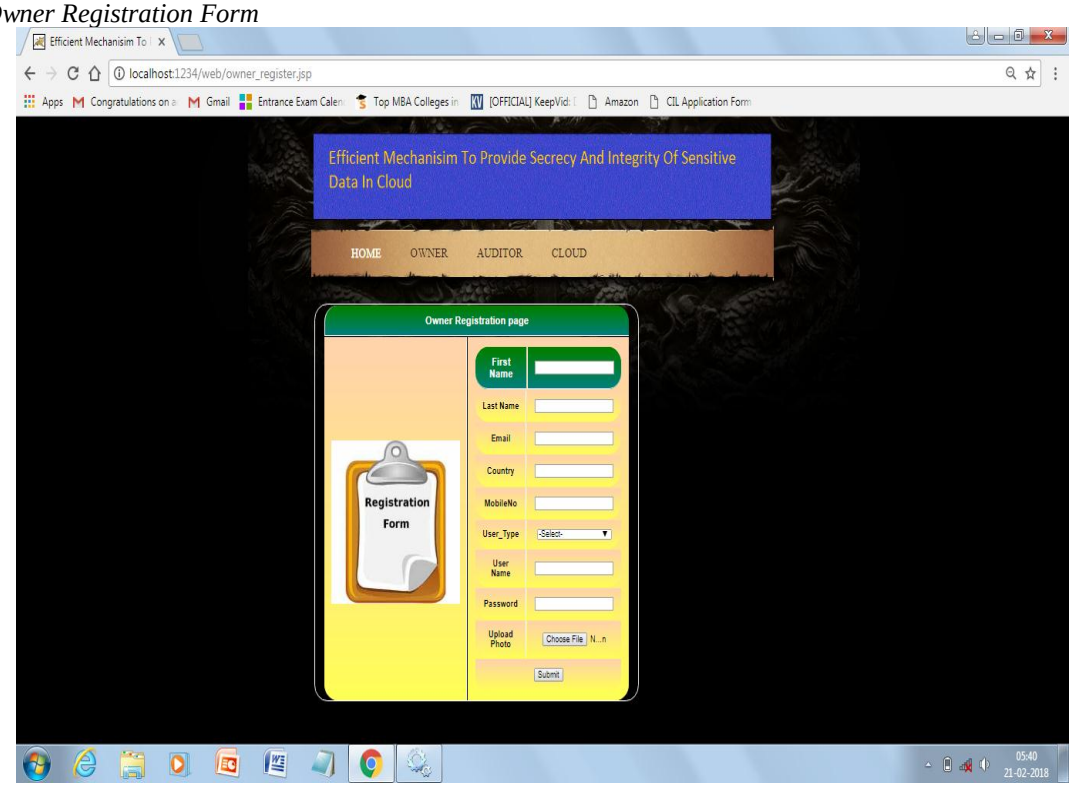
The proposed work is implemented by using java with Drive HQ cloud. With the help of JSP framework the user interface is created and the files uploaded by data owner will be stored in Drive HQ cloud. To encrypt the file the standard encryption algorithm AES is used.

Drive HQ: In this project, Free cloud server Drive HQ is used .1 GB of storage space is provided by Drive HQ. In Drive HQ cloud storage service system, it easy to upload and download files. This can be done by using Drive HQ file manager, web browser, ftp service etc. From anywhere users can access files. In order to access the services of Drive HQ, it requires signup that consists of username, password and email address. One can use the services only if the given login details are valid.

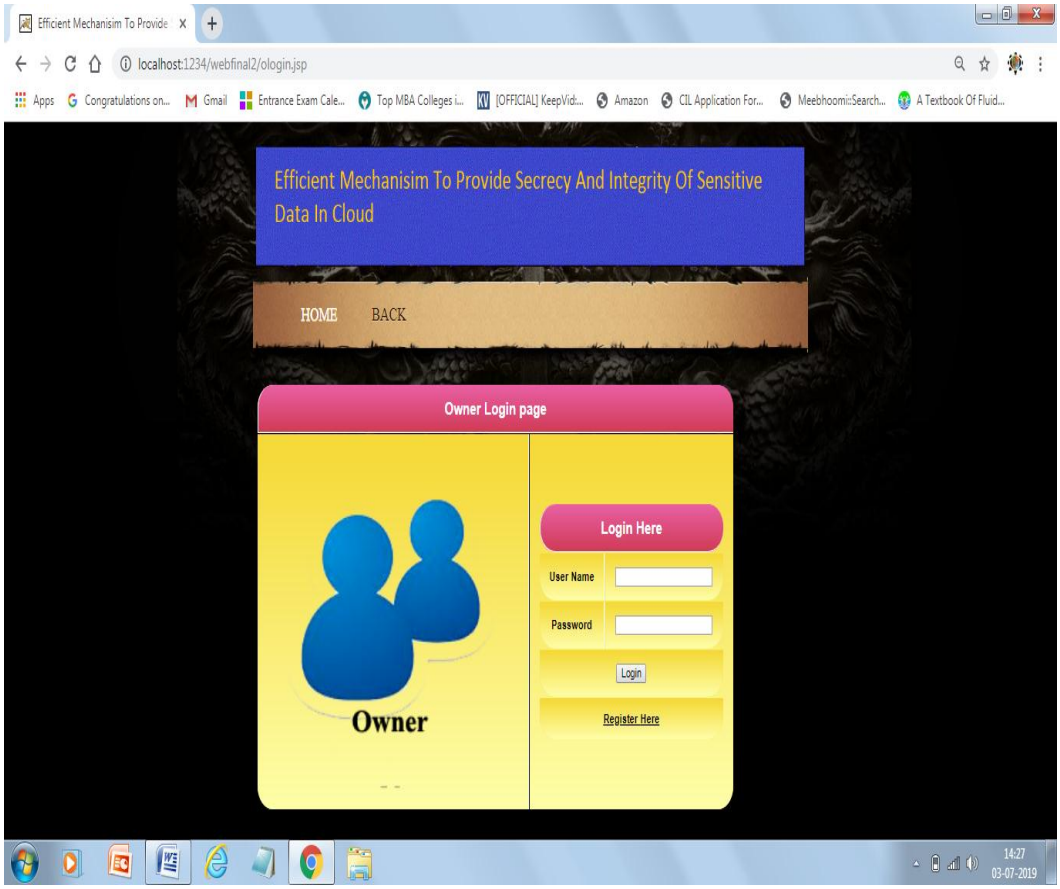
A. Homepage



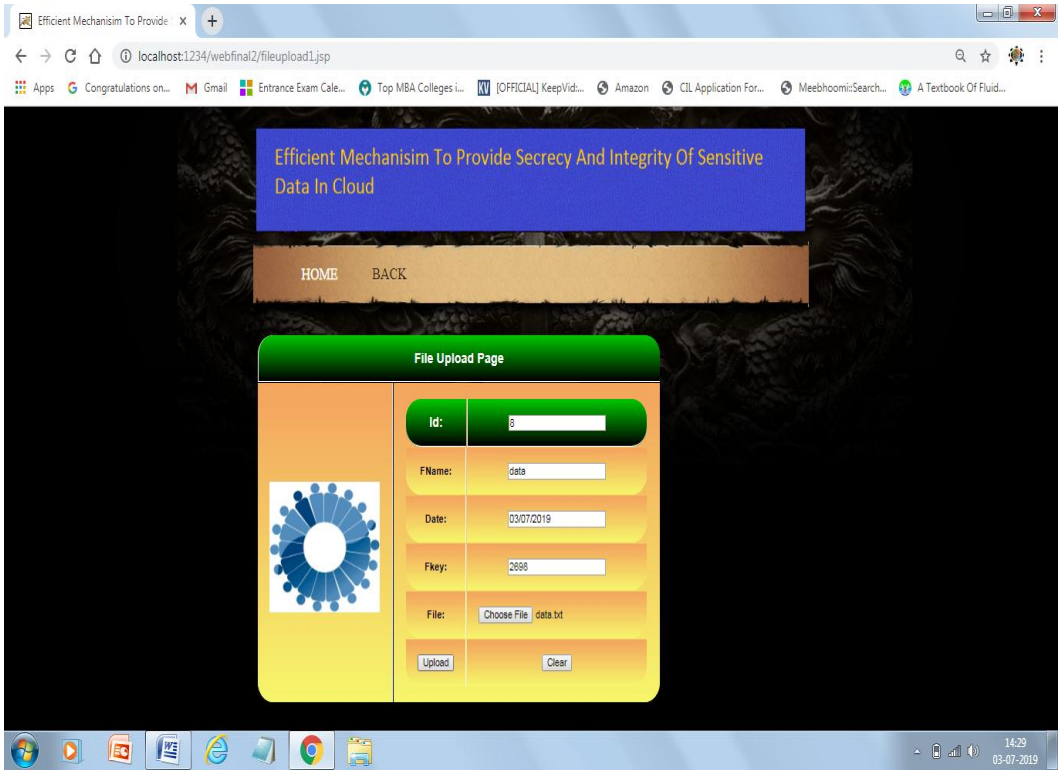
B .Data Owner Registration Form



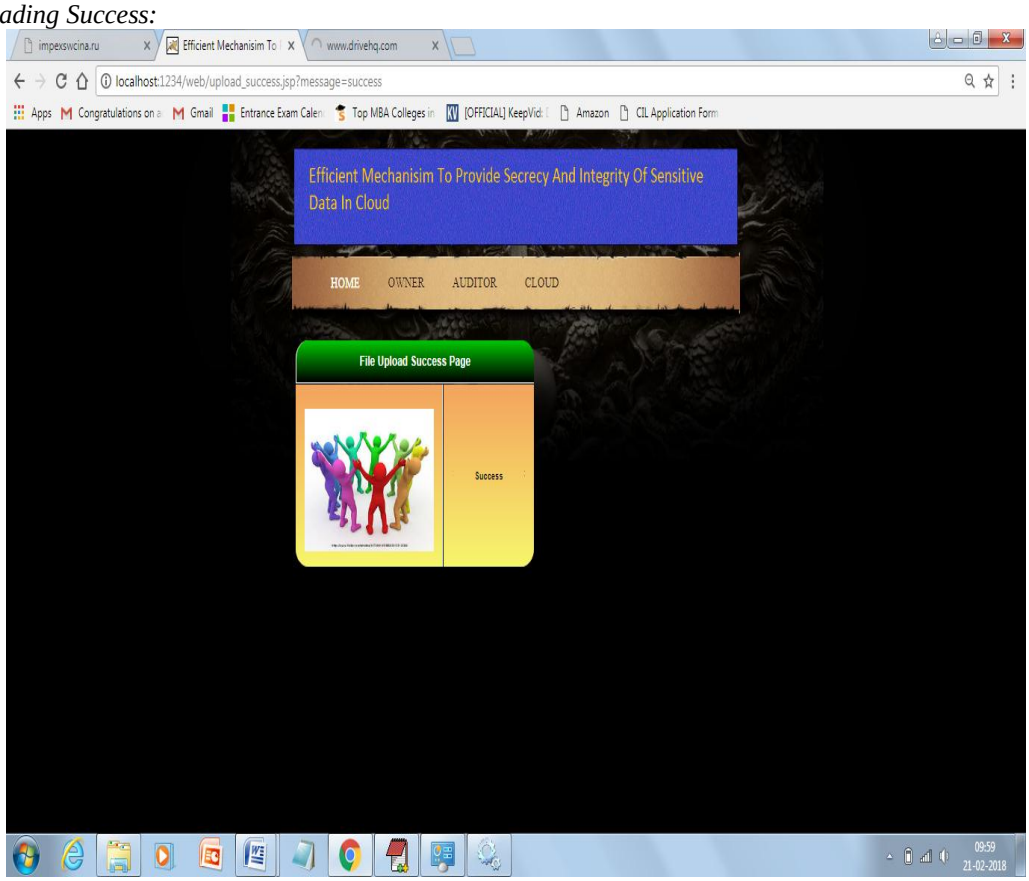
C. Data Owner Login



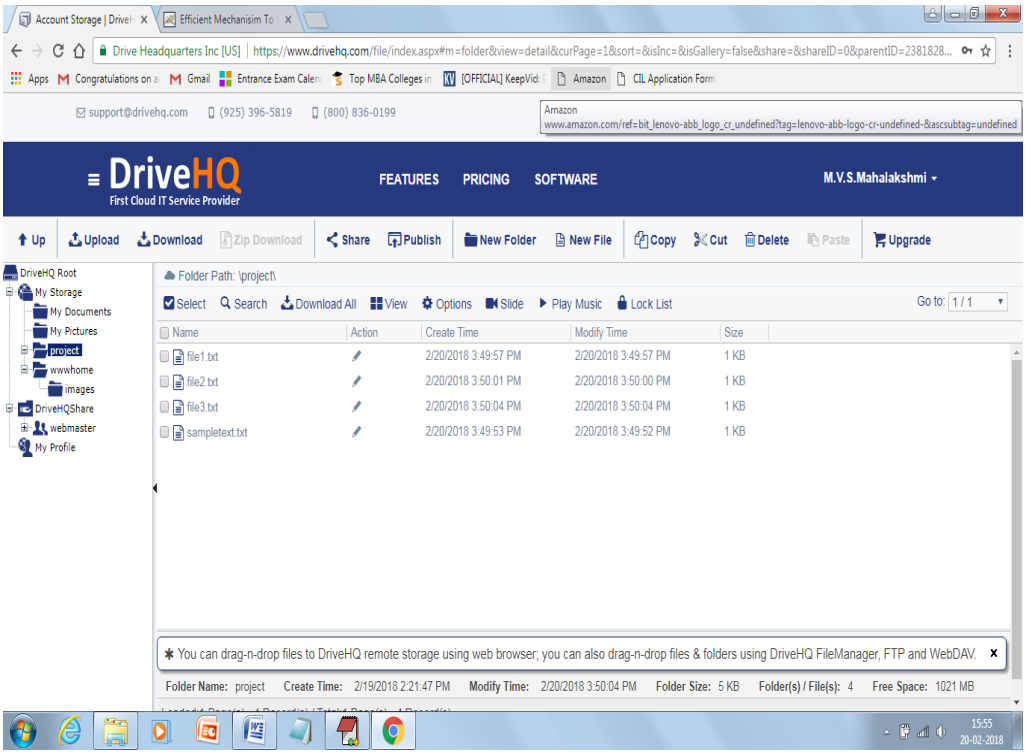
D. File uploading page



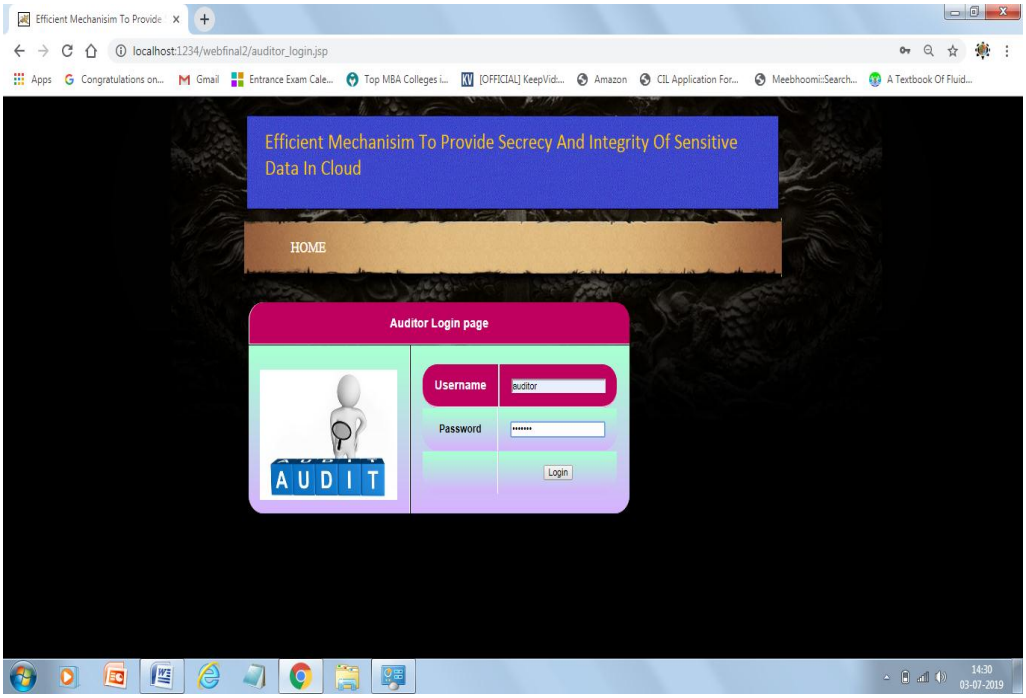
E. File Uploading Success:



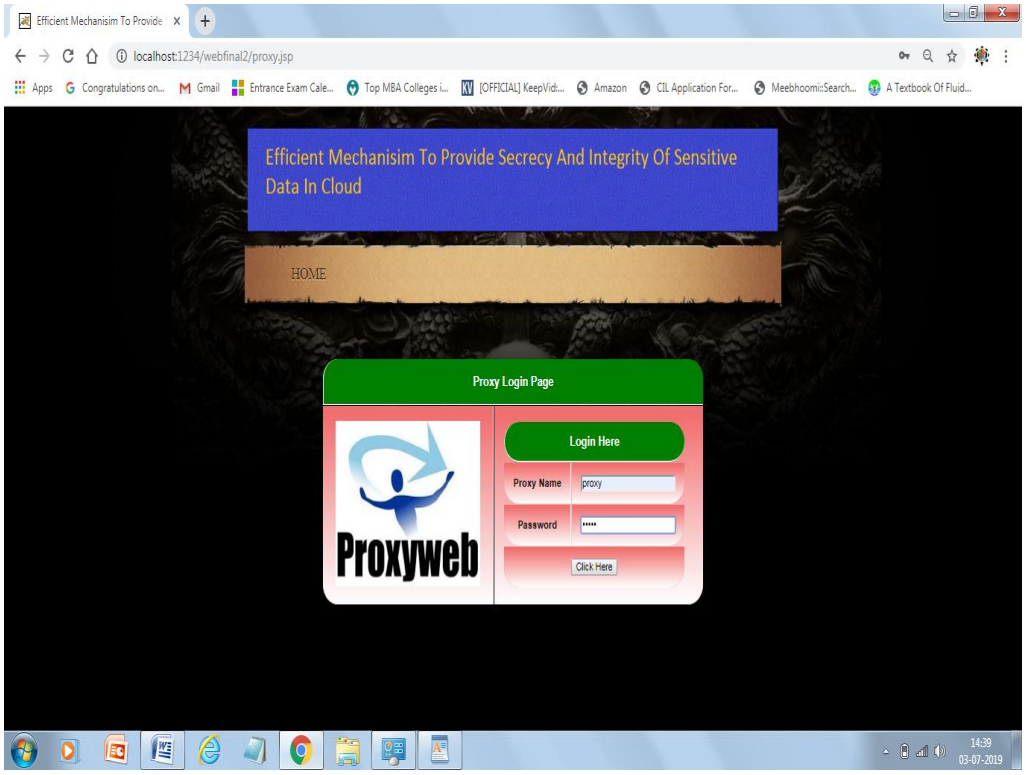
F. Store File in drive hq Cloud



G. Auditor Login page



H: Proxy Login Page



V. CONCLUSION

An efficient mechanism to provide secrecy and integrity of data at cloud is a major concern in the storage systems of cloud even though it comes with attractive benefits. The proposed system uses the concept of privacy-preserving public auditing scheme for regenerating code-based cloud storage by that secrecy and integrity of data can be enhanced. In this scheme, TPA is used to achieve the integrity of the data and to ensure security data should be encrypted by AES-256 bit algorithm and proxy is used to regenerate data block on corrupted servers during the repair process.

VI. ACKNOWLEDGMENT

I would like to express my gratitude to my Guide Dr S Rama Sree, M. Tech, Ph.D, Professor, CSE Department. Her understanding encouragement and personal guidance provided the basis for this paper.

REFERENCES

[1] Tim Grance and Peter Mell, " NIST definition of Cloud Computing," *Communications of the ACM*, vol. 53, no. 6, 2010.
[2] Vaishali Chourey and Tunisha Saxenal "A Survey Paper on Cloud Security Issues and Challenges," 2014 Conference on IT in Industry, Business and Government. (CSIBIG).doi:10.1109/csibig.2014.7056957.
[3] G. Ateniese, R. Curtmola, R. Burns, Z.Peterson, J. Herring, L. Kissner and D. Song, Provable Data Possession at Untrusted Stores, Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 598-609, 2007.
[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public Auditability and data dynamics for storage security in cloud Computing, "*IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5,pp. 847–859, May 2011.
[5] Sudha George and IK Meenakshi ," Cloud Server Storage Security using TPA", International Journal of Advanced Research in Computer Science And Technology (IJARCST) ISSN: 2347-9817, 2014.
[6] B.S. Kaliski and A. Juels, "PORs: Proofs pf Retrievability for Large Files," in *Proc. ACM CCS*, 2007, pp. 584–597.
[7] B. Waters and H. Shacham, "Compact Proofs Of Retrievability", The 14th Annual International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), Vol. 5350, pp. 90-107, Dec. 2008.

AUTHORS PROFILE

M.V.S.Mahalakshmi received the B.Tech Degree in Computer Science& Engineering from Aditya College of Engineering & Technology, affiliated to Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India. Presently working for M. Tech Degree in Computer Science & Engineering at Aditya Engineering College, affiliated to Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India.

Dr. S Rama Sree received M.Tech from Jawaharlal Nehru Technological University, Kakinada and received Ph.D from Jawaharlal Nehru Technological University, Hyderabad. She has teaching experience of 18 years. She is currently working as Professor in CSE Department and Vice Principal at Aditya Engineering College, Surampalem and Andhra Pradesh, India. Her research interest includes Software Engineering, Soft Computing and Cloud Computing. She published more than 30 International Journals and Conferences.