IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

Sensitive Information Storage in Cloud

G.Asha Jyothi[1],Mr. M.Y.Sekharam[2]

M.Tech Scholar, Department of Computer Science & Engineering, AKRG College of Engineering & Technology, Nallajerla, West Godavari, Andhra Pradesh[1]

Assistant Professor, Department of Computer Science & Engineering, AKRG College of Engineering & Technology, Nallajerla, West Godavari, Andhra Pradesh[2]

Abstract: Users can transfer their data to the cloud remotely with cloud storage services, and conduct data sharing with others. Remote data integrity auditing is proposed to ensure that data stored in the cloud is essential. Some can cloud storage systems, such as the electronic health records system, can contain some confidential information in the cloud file When sharing a cloud file, the confidential information will not be revealed to anyone. Encrypting the entire shared file will conceal confidential information, but would make this shared file impossible for anyone to use. Whether to know data sharing in remote data integrity auditing with confidential information shielding has not been discussed up to now. To fix this issue, we are proposing a remote data integrity auditing scheme that performs data sharing with confidential hiding information in this project. Under this scheme, a sanitizer is used to sanitize the data blocks that refer to the file's confidential information and convert the signatures of these data blocks into valid ones for the sanitized file.Such signatures are used for checking the validity of the sanitized file during the validity auditing process. As a result, our scheme allows the file stored in the cloud to be exchanged and used by others provided that the confidential information is secret, while remote data integrity audits can still be conducted effectively

Keywords: Big Data, Proxy Re-encryption, Storage Path, Cloud Storage, Sensitive Data.

I. INTRODUCTION

New companies are entities newly created that are competing for existence. Typically, these elements are presented, based on splendid thoughts and grow to succeed. Such wonders are stated in the speculations concerning administration, partnership, and industry. Notwithstanding that, an unmistakable image of these substances is not available. This paper attempts to conceptualize the wondersStart, and appreciate the difficulties they face. The paper ends in the wake of discussing the process of life and the difficulties Few thoughts to finish. This paper seeks a reasonable proportion of new business execution, and then clarifies this metric by different business process metrics. WITH Touchy Knowledge Creation,It's an daunting weight for clients to tostore the sheer measure of local knowledge. This means a increasing number of organizations and people want to store their information in the cloud. Whatever happens, the information stored in the cloud may be adulterated or lost due to the inevitable code glitches, hardware problems and human errors in the cloud.

CLOUD storage can provide users with efficient and on request data storage services[1]. Using the cloud service , customers can outsource their data to the cloud without spending major hardware maintenance costs even in realistic situations, which is not user-friendly. Furthermore, the hardware token containing the private key can also be lost. Through losing your password or equipment. The consumer will no longer be able to create the authenticator for any new data block until the password is forgotten or the hardware token is lost. The auditing of data integrity won't work as normal.

Consequently, discovering a method for conducting data integrity auditing without storing the private key is quite important and appealing. A feasible approach is to use biometric data as the private key, such as fingerprint and iris scanning[16, 17]. Being a part of the human body, biometric data can uniquely connect person and private key. Sadly, biometric data are calculated with unavoidable noise at each point and can not be reliably reproduced[18] because certain variables can influence the biometric data changes. For example, each person's finger will produce a different image of fingerprints each time due to strain, moisture, angle of view, dirt, different sensors, and so on. The biometric data therefore cannot be used directly therefore as the private key to generate authenticators in data integrity auditing.

The contribution of this paper can be summed up as follows: We are performing the first work on how to use biometric data as a fuzzy private key to perform data integrity auditing, and are suggesting a new method called data integrity auditing without private key storage. A customer of such a scheme uses biometric data to verify his identity, as his fuzzy private key.. The data integrity audit can be conducted on condition that there is no hardware token to store the private key. We further formalize the Data Integrity Auditing Scheme definition for safe cloud storage without the need to store the private key. We create a practical data integrity audit scheme without storing private key for secure cloud storage.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 8, August 2020
DOI 10.17148/IJARCCE.2020.9808

In our scheme, two fuzzy private keys (biometric data) are extracted from the user in the phase of registration and the phase of signature generation. We respectively use these two fuzzy private keys to generate two linear sketches that contain coding and error correction processes. In order to confirm the user's identity, we compare these two fuzzy private keys by removing the "noise" from two sketches. If the two biometric data are sufficiently close, we can confirm that they are extracted from the same user; otherwise, from different users.

How to design a signature satisfying both the compatibility with the linear sketch and the block less verifiability is a key challenge for realizing data integrity auditing without private key storage. In order to overcome this challenge, we design a new signature scheme named as MBLSS by modifying the BLS short signature based on the idea of fuzzy signature. We give the security analysis and justify the performance via concrete implementations. The results show that the proposed scheme is secure and efficient

II. LITERATURE REVIEW

Many related works are present in the literature on cloud data storage and retrieval methods (Cong et al. 2012, Henry et al. 2014, Libin et al. 2014, Jun Li et al. 2013, Abraham et al. 2011, Arshdeep et al. 2012). Among them, Wang et al. (2011), developed a new method for guarantying data integrity in cloud data storage. In their work, they support only the data dynamic operations for effective data manipulation. For to accomplishing efficient data dynamics of data storage, they used the Merkle Hash Tree construction model.

Cong et al. (2013), proposed a cloud security model that allows the users to perform auditing on the cloud storage. After auditing, the results are used to check the correctness of storage. In addition, it also concurrently reduces data error within the server. Their design also supports safe and effective dynamic data manipulation operations. They have also achieved the data integrity as well as data availability in cloud storage. Their work reduces the various attacks such as data modification server, colluding and access vitiation types of attacks.

Hsiao et al. (2012), proposed a distributed secured data storage system including the retrieval process into cloud database using the re- encryption techniques. Their scheme supports the encryption and forwarding techniques with integrated encryption process, encoding information and its forwarding.

There are many works that discuss about cloud data storage and retrieval methods. Wang et al. (2013), proposed a secured data storage technique which recommends for public auditability of cloud database system storage so that the user can use a third party auditing mechanism to maintain data integrity.

Ayad et al. (2013) proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the cloud service provider. Their scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Junbeom et al. (2013) proposed an attribute based data sharing scheme to enforce a fine-grained data access control by exploiting the characteristic of the data sharing system. Huaqun et al. (2013) designed an efficient pairing-based PPDP protocol for providing security in data communications oncloud.

Yan et al. (2012), devised a new data possession technique in order to guarantee integrity and security. Yang et al. (2012), proposed a model in which they supported the reduction of maintenance costs and also provided a secured way of data updation and deletion of user's data. They have designed and implemented a technique called File Assured Deletion (FADE) which achieves access control policies which are file creation, file updation and filedeletion. Kan et al. (2013) proposed a new protocol for privacy preserving audit for cloud data storage. Even though this model reduces a considerable amount of cost and provides data security, it takes a lot of time for dynamically auditing the data stored in the cloud database. Jian et al. (2015) proposed a public auditing scheme for regenerating-code-based cloud storage system. In their model, they provided various levels of privileges based on users.

Cheng-Kang et al. (2014), proposed a new method to explain the process of sharing data with other users in a secure, efficient and flexible manner in cloud data storage. They have implemented a public-key cryptosystem to produce same size input cipher texts so that an effective delegation of decryption rights for cipher texts is possible on user request. Using the cryptosystems which makes use of cryptography aggregate key mechanism, they have shown the method to compress the secret keys. This helps to store data in a secure manner. By this approach, the hierarchical key management process can only reduce spaces in the case that all users having the key share the same set of privileges. This system has the limitation of usage of the model to only limited cipher texts classes. Wei Li et al. (2016) proposed a new threshold and attribute based encryption scheme called for providing effective storage in public cloud with access control. Their experimental results show that their scheme is robust and secure.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 8, August 2020
DOI 10.17148/IJARCCE.2020.9808

Lan et al. (2013), proposed a Role Based Encryption (RBE) model that combined the cryptographic algorithms with Role Based Access Control technique. Based on this scheme, they have presented a secured RBE which is based on hybrid cloud storage planning that gives an organization the control to securely store the data in the public cloud and also maintain the confidential information of the organization in a privatecloud.

III.SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM:

The Audit Data. When linking auditor Reviews the accounts or reviews key monetary statements for an entity, square findings usually calculate create a report or compile it in a very systematic manner Fashion. Many Remote Information Management Proposals have been proposed. The information proprietor right off the bat needs to generate marks for information obstructs in remote information honesty checking plans before uploading them to the cloud. Such labels are used to show that the cloud has such trustworthy knowledge hinders Study. Then after that, the proprietor of the knowledge passes these hinders to the cloud alongside their corresponding points. For other centralized storage systems , for example, Google Drive, Dropbox, and iCloud, the information put away in the cloud is exchanged periodically among various clients. Specific Data

3.1.1 DISADVANTAGES

- In the existing work, the data correctness is not based on hash code.
- The existing doesn't have more security since it doesn't have sensitive information hiding techniques.

3.2 PROPOSED SYSTEM

❖ The proposed framework explores how to achieve data sharing by remote data integrity auditing with sensitive information hiding, and suggests a new model called identity-based, mutual data integrity auditing with sensitive information hiding for safe cloud storage. The confidential information may be covered in such a system, and the other information can be released. This makes the file saved in It makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected, while the remote data integrity auditing is still able to be efficiently executed.

❖ The proposed system also designs a practical identity-based shared data integrity auditing scheme with sensitive information hiding for secure cloud storage. The data blocks referring to the file's confidential details are sanitized with a sanitizer. Firstly, in our comprehensive scheme, the user blinds the data blocks corresponding to the original file 's personal sensitive information and produces the corresponding signatures, and then sends them to a sanitizer. The sanitizer hygienizes these blocked data in a standard format and It also transforms the corresponding signatures into valid ones for the sanitized file. This method not only realizes the remote data integrity auditing, but also supports the data sharing on the condition that sensitive information is protected in cloud storage. To the best of our knowledge, this is the first scheme with the above functions. Besides, our scheme is based on identity-based cryptography, which simplifies the complex certificate management.

❖ The proposed system gives the security analysis of the proposed scheme, and also justifies the performance by concrete implementations. The result shows that the proposed scheme achieves desirable security and efficiency.

3.2.1 ADVANTAGES

➢ Private Key correctness: to ensure that when the PKG sends a correct private key to the user, this private key can pass the verification of the user.

➢ Auditing correctness: to ensure that when the cloud properly stores the user's sanitized data, the proof it generates can pass the verification of the TPA.

IV IMPLEMENTATION

DATA OWNER

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Upload File with Blocks,View All Upload File with Blocks, Perform Data Integrity Auditing, View Transactions.

CLOUD SERVER

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View and Authorize Users, View and Authorize Owners,View All File's Blocks,View All Transactions,View All Attackers, View Time Delay Results,View Throughput Results

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 8, August 2020
DOI 10.17148/IJARCCE.2020.9808

TPA

In this module, the TPA performs the following operations such as View Metadata Details, View All Transactions,View All Attackers

DATA USER

In this module, the user has to register to cloud and log in and performs the following operations such as Search Data, Download Data.

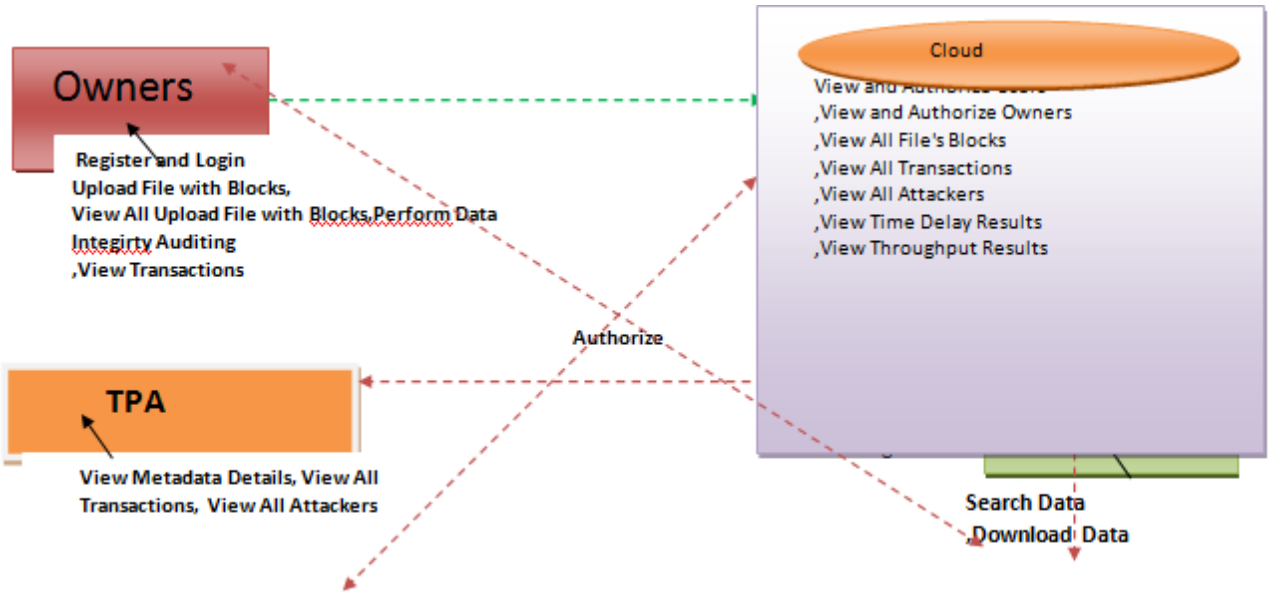

FIG 1:- PROPOSED ARCHITURE

V EXPERIMENTAL RESULT

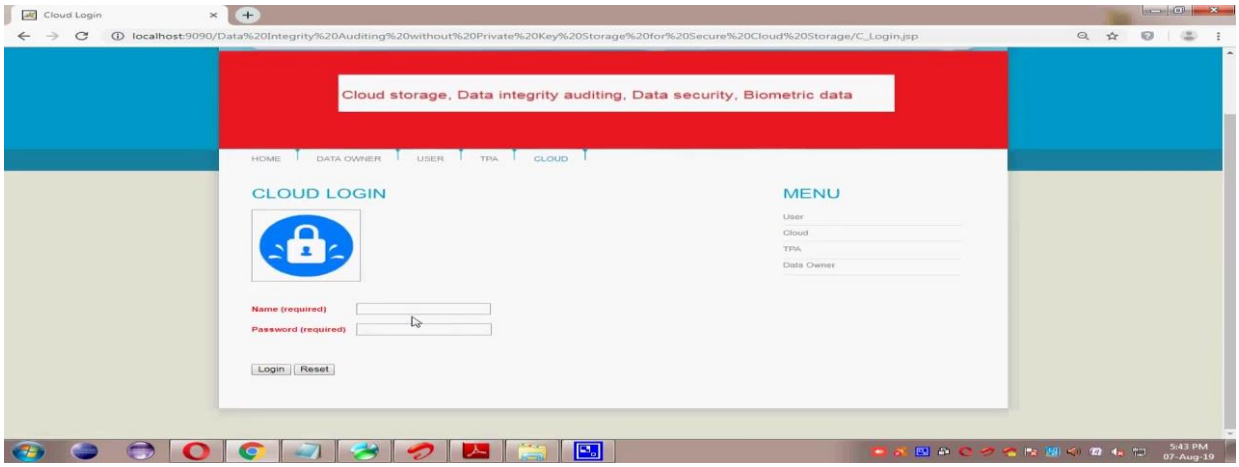

FIG 2 :Cloud login

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

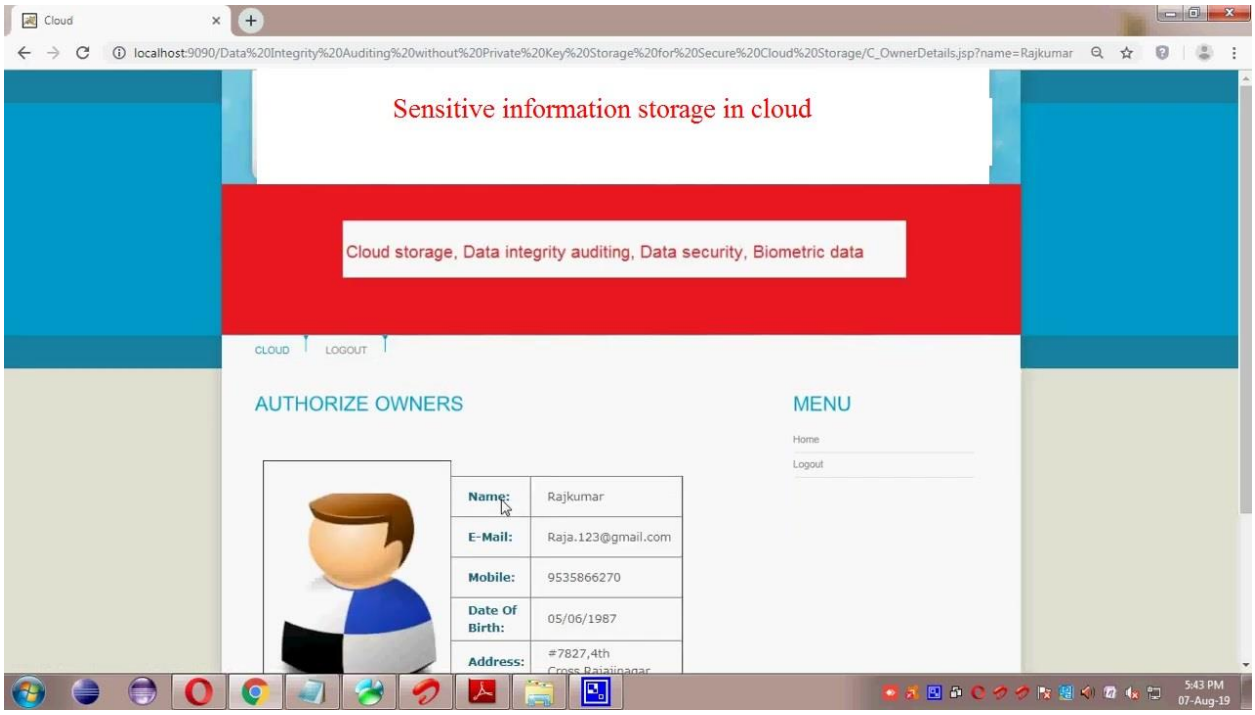

FIG 3:-Home page of cloud

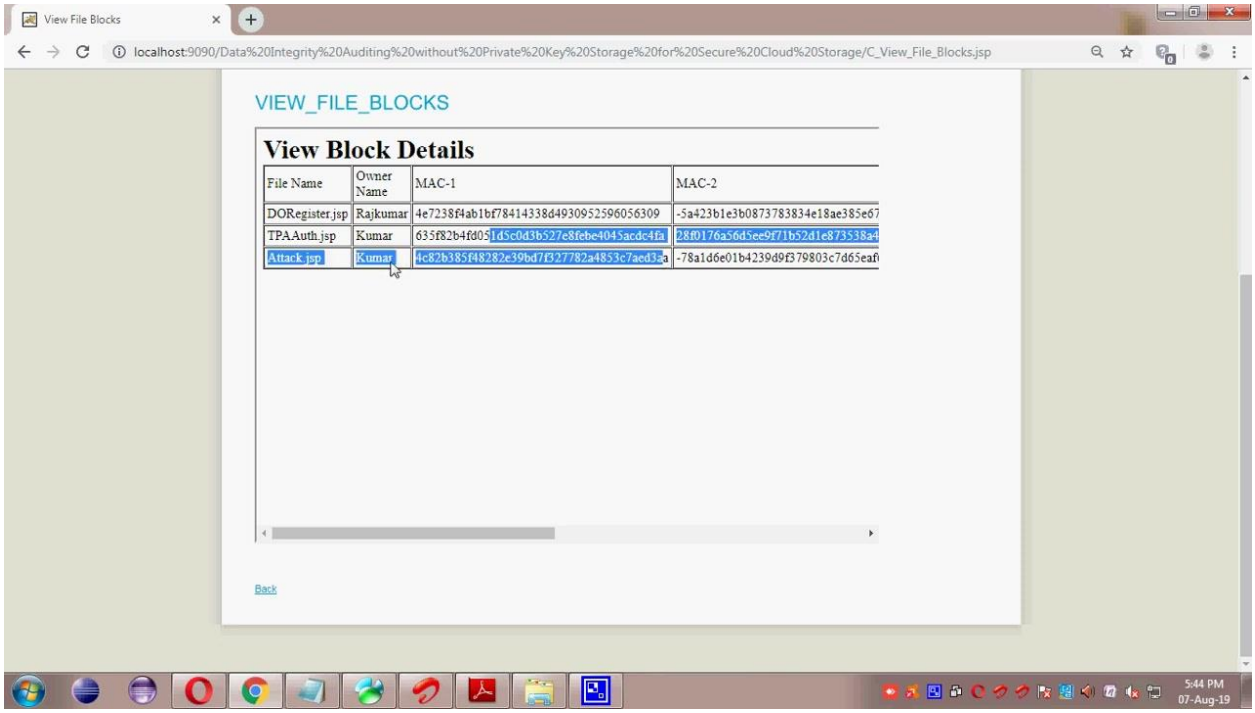

FIG 4 :- File blocks stores in cloud

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

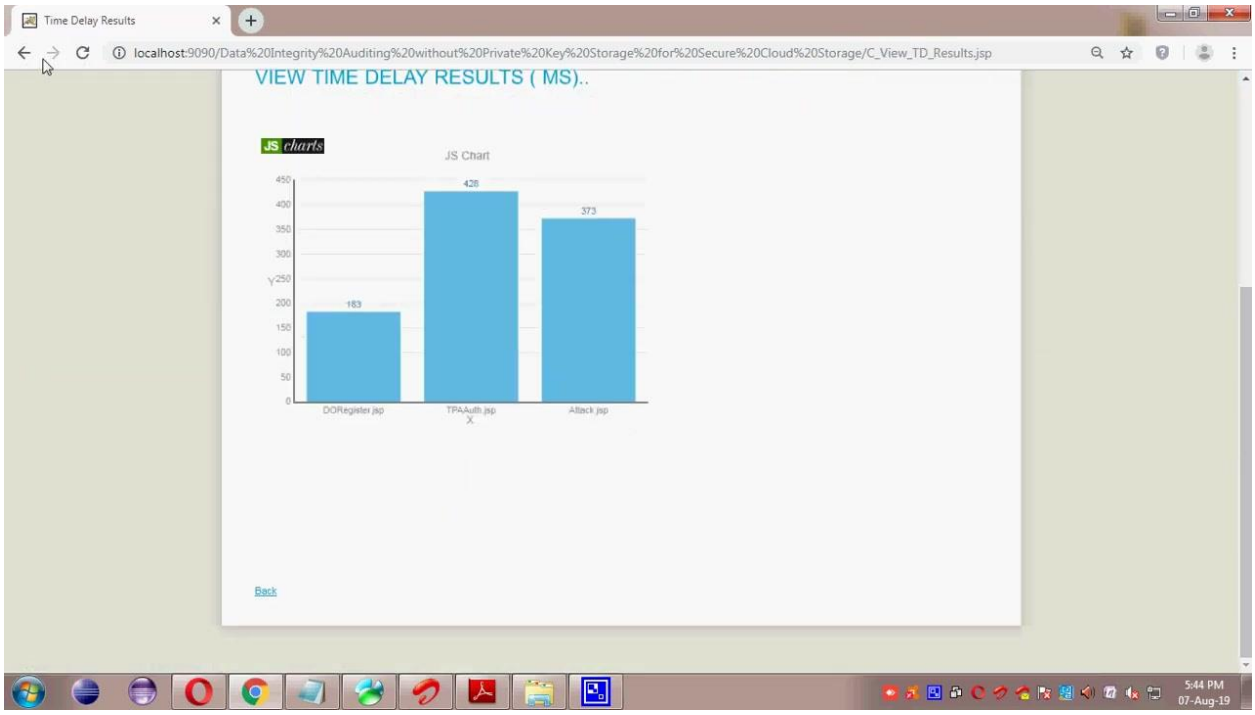

FIG 5 :-Time delay results for file sharing

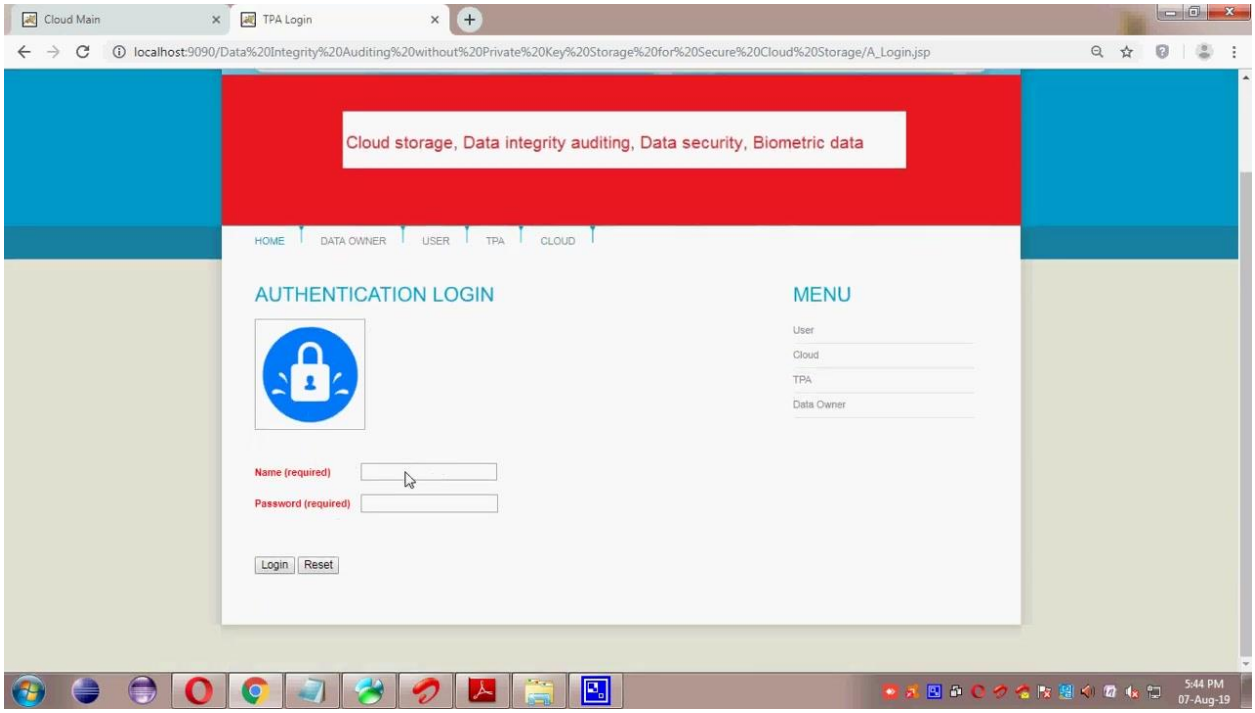

FIG 6:- Authentication login

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

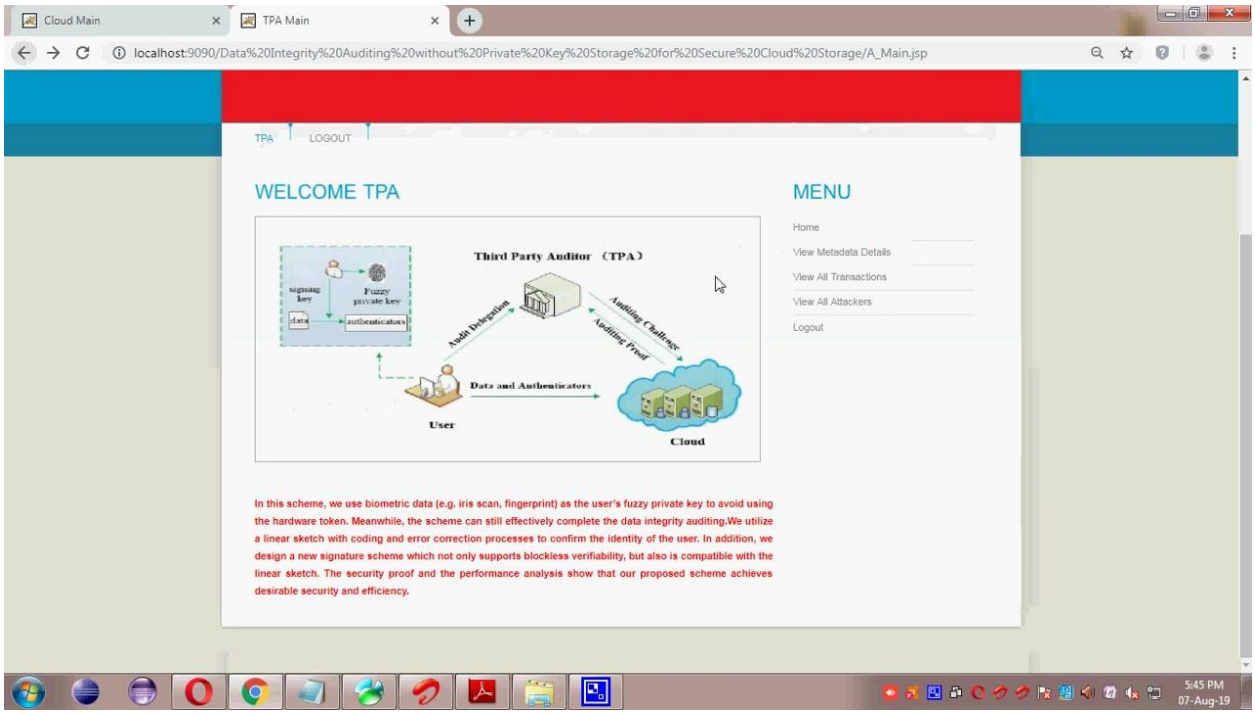

FIG 7 :-Tpa home page

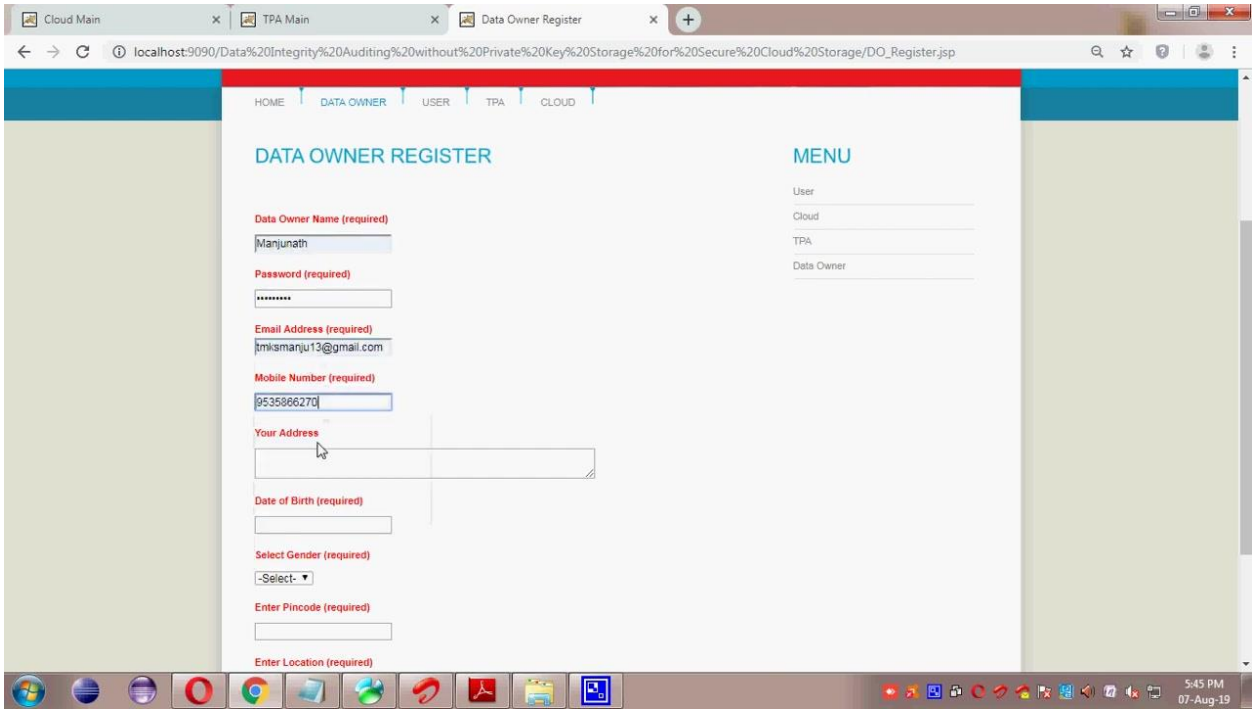

FIG 8 :-Data owner registration

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

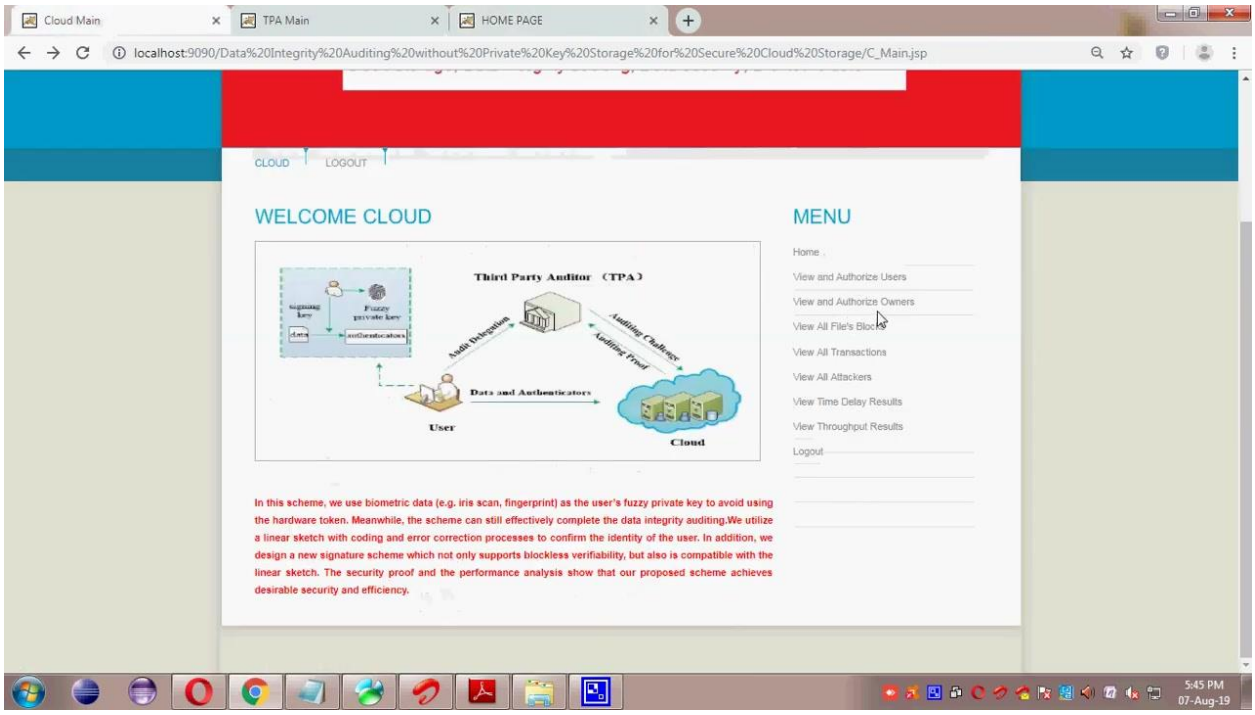

FIG 9 :-Cloud home page

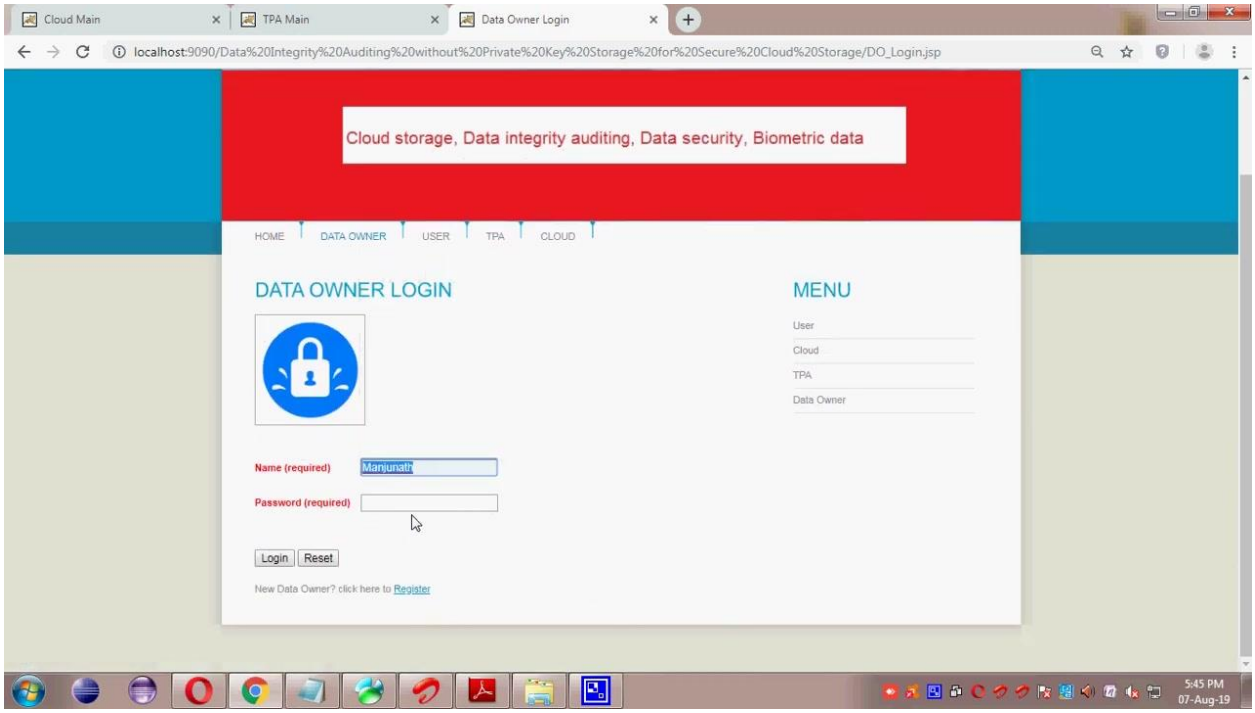

FIG 10 :-Data owner login

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

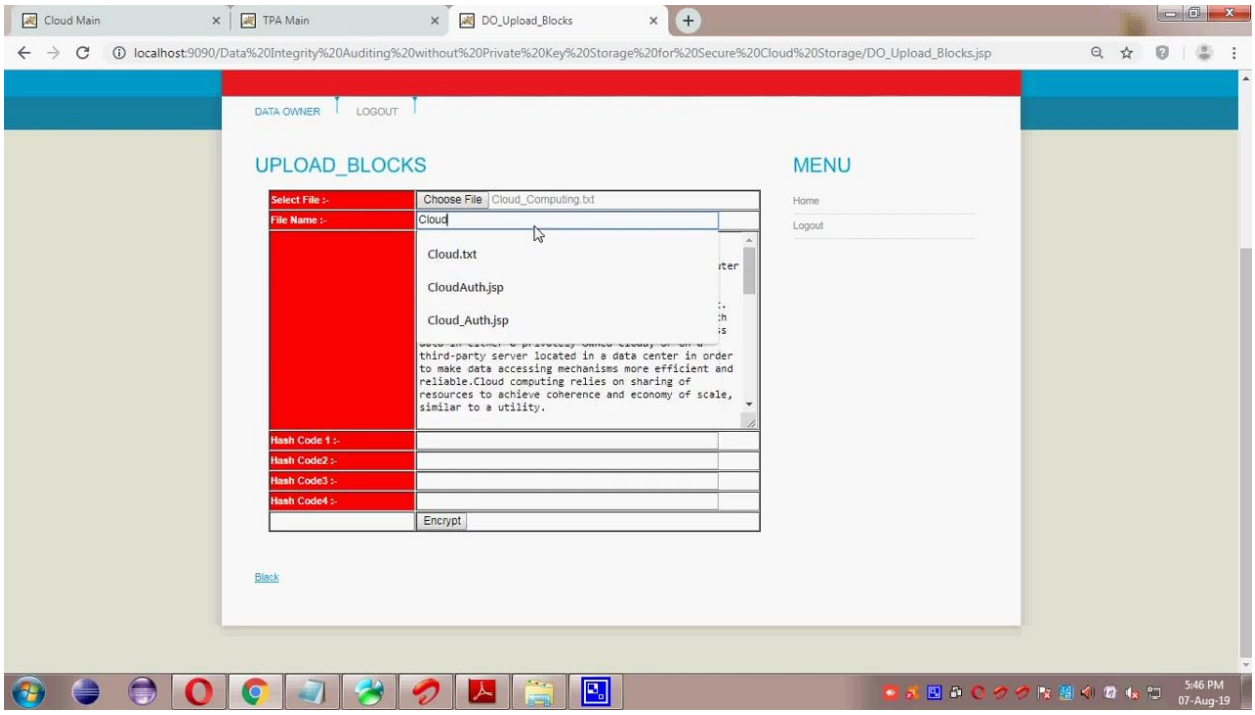

FIG 11 :-Uploading the files in encrypted format of blocks

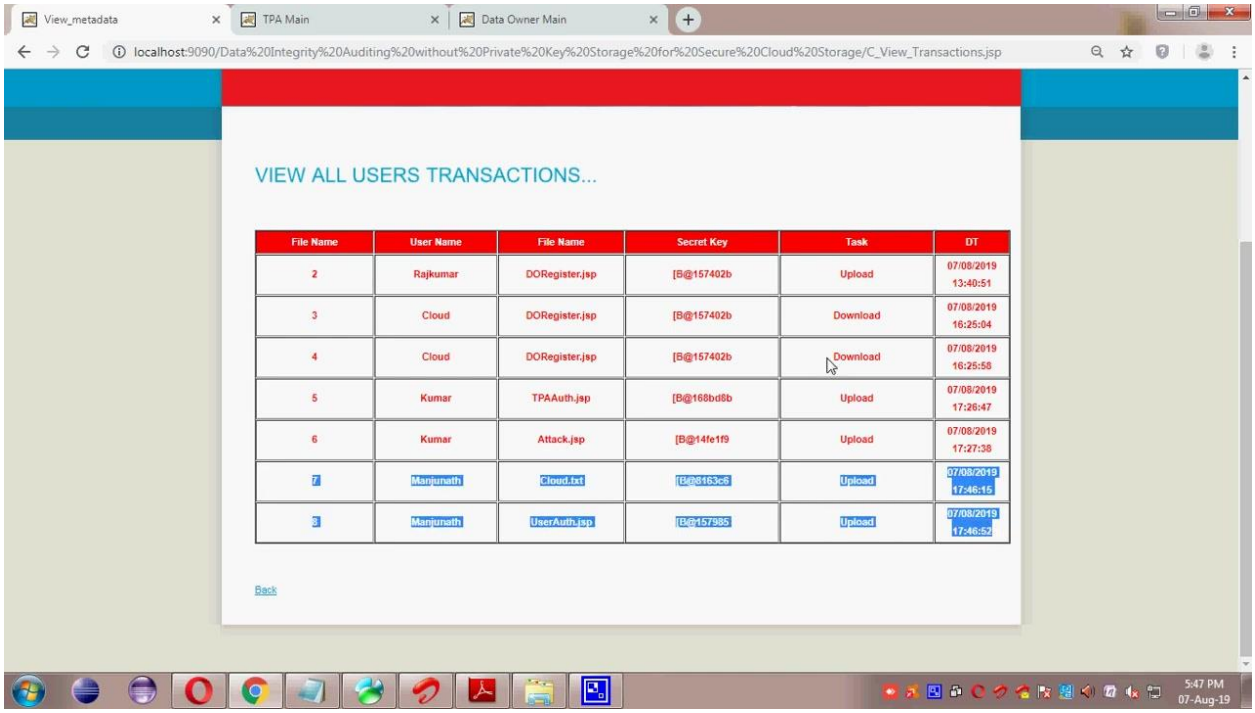

FIG 12:- User transaction report like upload and download

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

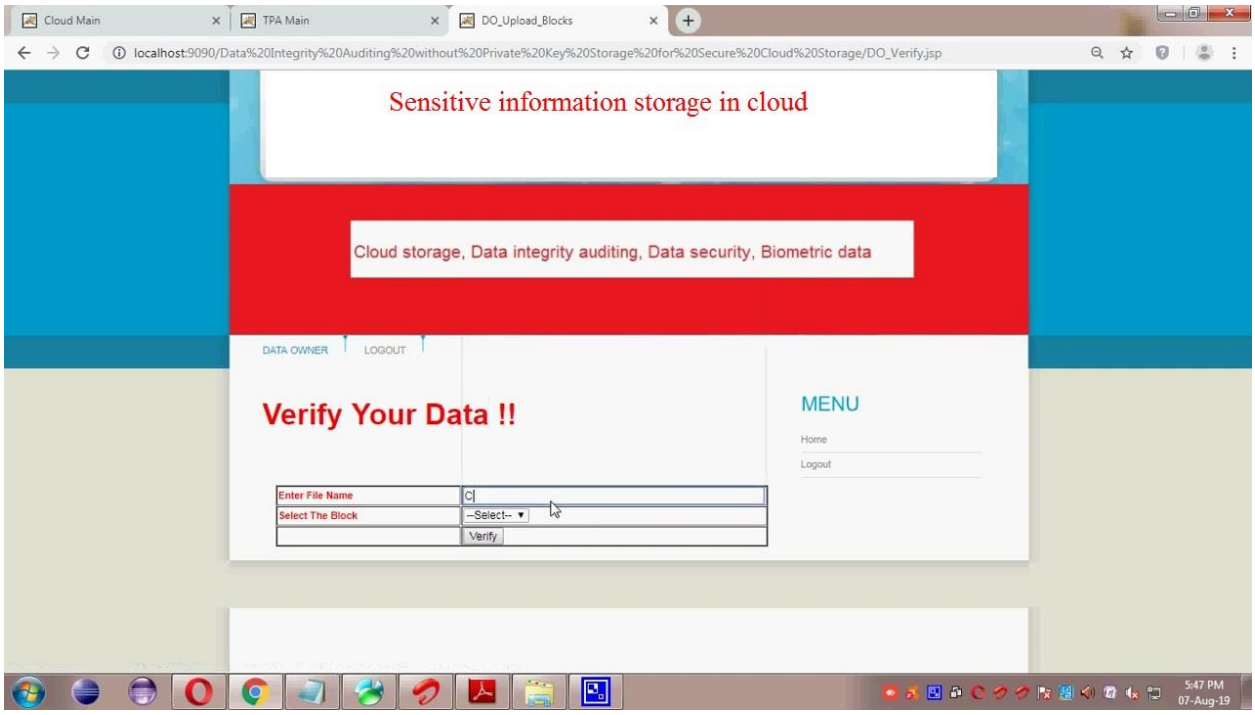

FIG 13:- Verifying the data wich is uploaded for each block

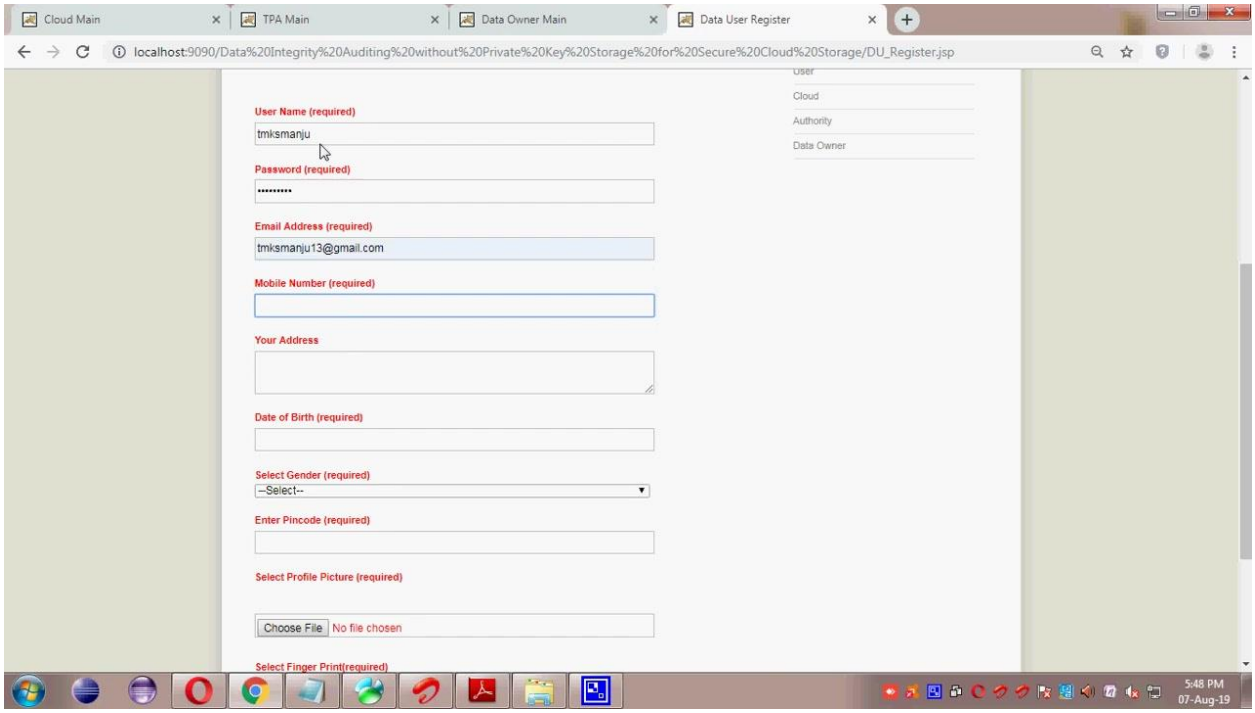

FIG 14 :- User registration

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

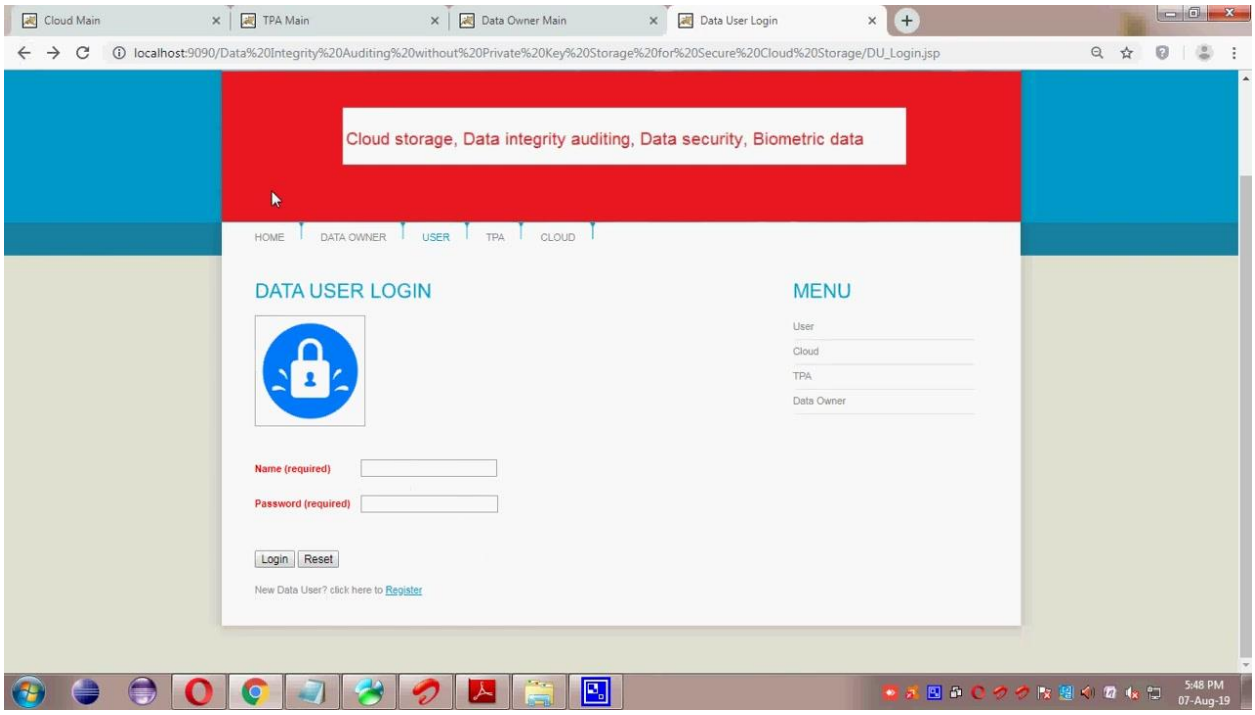

FIG 20 :-User login

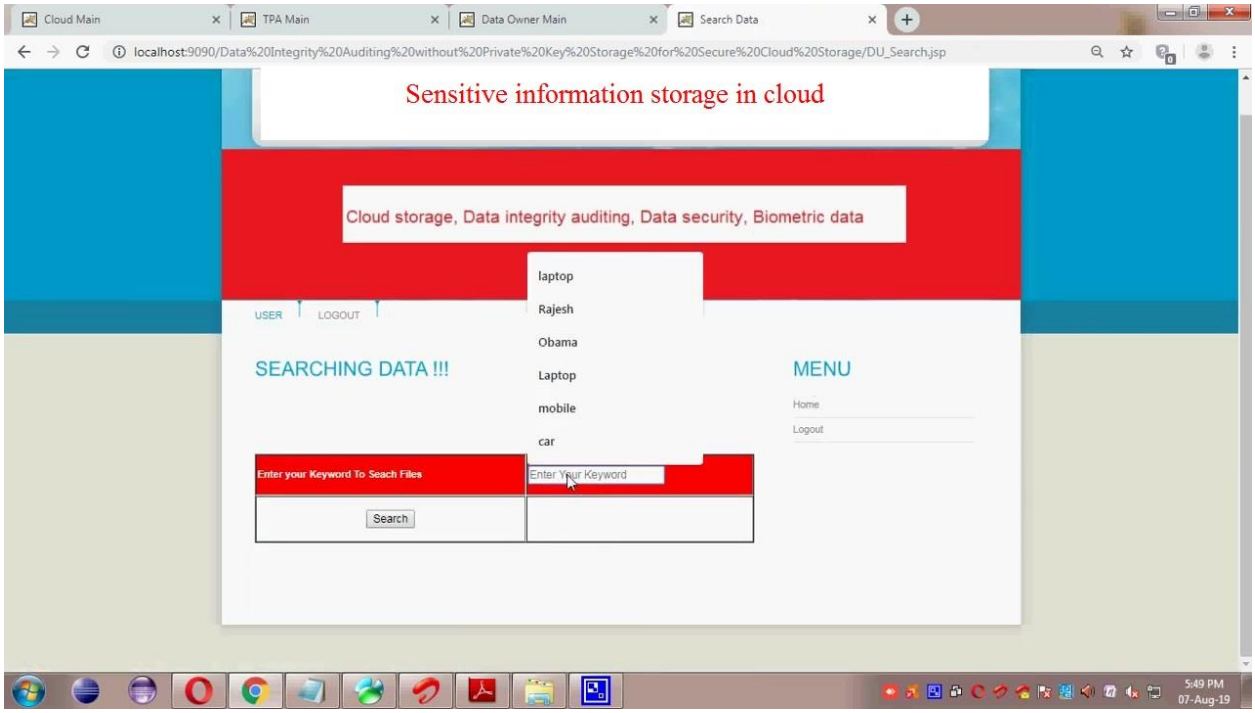

FIG 15 :- Searching the file to download

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 8, August 2020

DOI 10.17148/IJARCCE.2020.9808

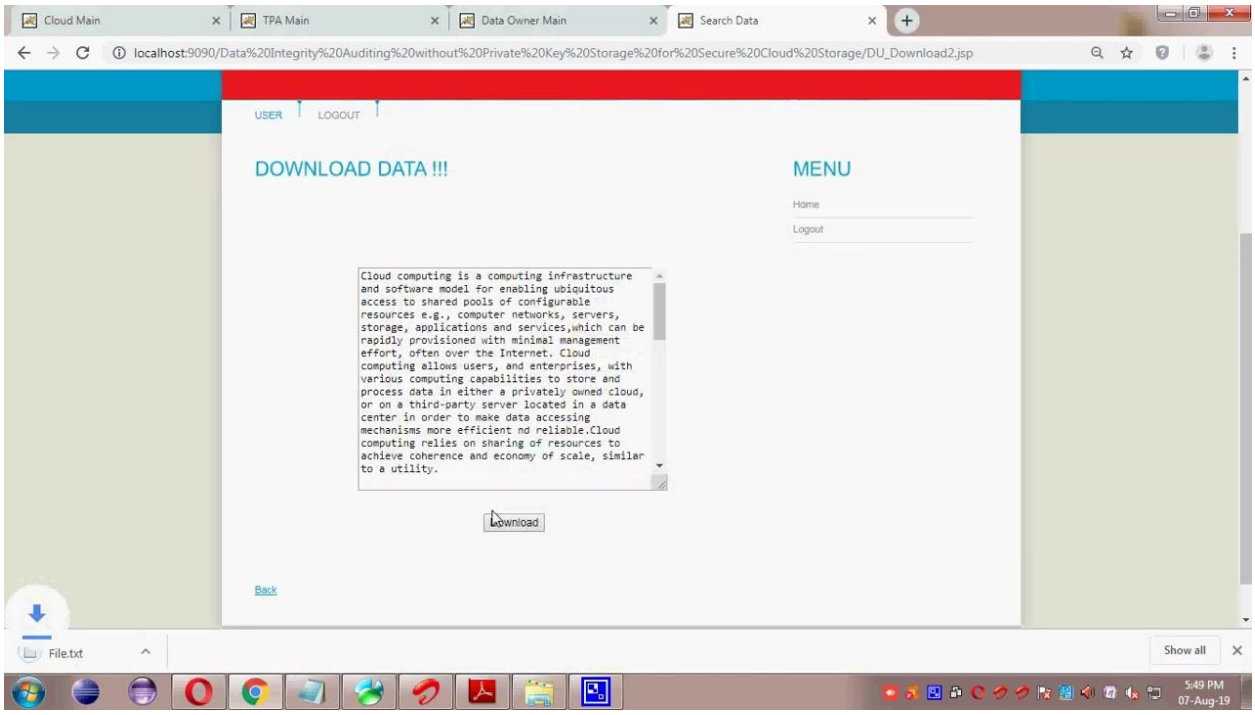

FIG 16 :- Downloading the data after decryption process

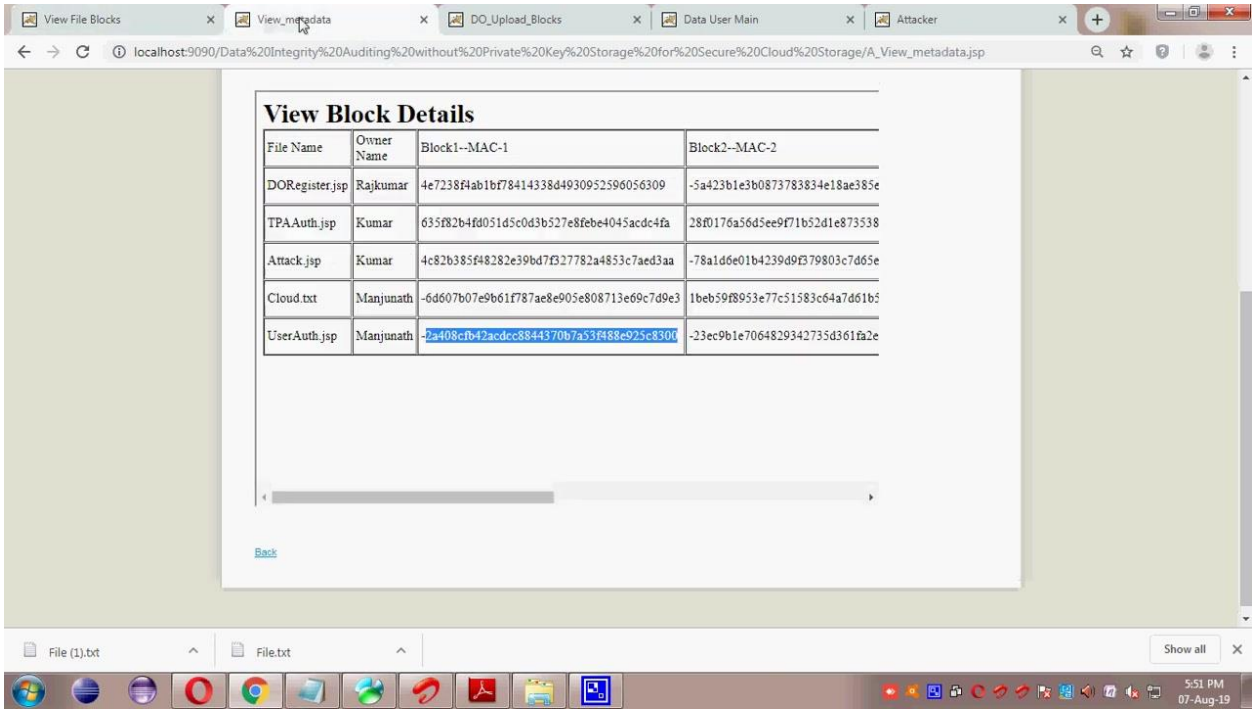

FIG 17 :-Viewing the files blocks stored in cloud server

VI CONCLUSION

Data storage scheme distributed allows the user to outsource the file to untrusted proxy servers. A special type of distributed data storage scheme is to define stable distributed data storage scheme based on it. Where the identity recognizes users and is able to connect without the accepted public key needing to validate. In this project we proposed an identity-based data integrity audit scheme for secure cloud storage, which enables data sharing with sensitive hiding of information. Under our scheme, the file stored in the cloud can be shared and used by anyone as long as sensitive information about the file is protected. The remote data integrity analysis can therefore still be successfully carried out.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 8, August 2020
DOI 10.17148/IJARCCE.2020.9808

Future Enhancement

Our future enhancement for safe distributed data storage based on identification is to allow users to migrate pdf files and to differentiate sheets. Future work will involve advancement such as uploading file File, encrypted format videos for convenience of the user.

REFERENCES

[1] H. Dewan and R. C. Hansdah, "A survey of cloud storage facilities," in 2011 IEEE World Congress on Services, July 2011, pp. 224–231.
[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.
[3] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security,vol. 10, no. 3, pp. 485–497, March 2015.
[4] N. Garg and S. Bawa, "Rits-mht: Relative indexed and time stamped merkle hash tree based data auditing protocol for cloud computing," Journal of Network &Computer Applications, vol. 84, pp. 1–13, 2017.
[5] H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE Transactions on Cloud Computing, vol. 13, no. 9, pp. 1–14,2014.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp.1703–1713, Jul. 2014.
[7] B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," in International Conference on Applied Cryptographyand Network Security, 2012, pp. 507–525.
[8] B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing for shared cloud data supporting group dynamics," in 2013 IEEE International Conference onCommunications (ICC), June 2013, pp. 1946–1950.
[9] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.
[10] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.
[11] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp.1931–1940, Aug 2017.
[12] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Identity-based remote data possession checking in public clouds," IET Information Security, vol. 8, no. 2, pp.114–121, March 2014.
[13] H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on InformationForensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.
[14] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacypreserving authenticators for cloud storage," Future Generation Computer Systems, vol. 76, no. Supplement C, pp. 136 – 145, 2017.
[15] C. Ellison and B. Schneier, "Ten risks of pki: What you're not being told about public key infrastructure," vol. 16, no. 1, 12 2000.
[16] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp.4–20, Jan 2004.
[17] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar 2003.
[18] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in cryptology—EUROCRYPT 2005, ser. Lecture Notes in Comput. Sci. Springer, Berlin,2005, vol. 3494, pp. 457–473.
[19] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACMConference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.
[20] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievabilityfor large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.
[21] H. Shacham and B. Waters, "Compact proofs of retrievability,"J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul.2013.
[22] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S.Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in ACM Symposium onApplied Computing, 2011, pp. 1550–1557. [23] M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," Information Sciences, vol. 380, pp. 101–116, 2017.
[24] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for data storage security incloud computing," in 2010 Proceedings IEEE INFOCOM,March 2010, pp. 1–9.
[25] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-preserving public auditing protocol for lowperformance end devices in cloud," IEEE Transactionson Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, Nov 2016.