International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

Identity Broadcast Virtual Proxy for Centralized Cloud Server

Roshitha P P[1],Sneha T Subramanian[2], T Sivakumar[3]
Computer science and Engineering, Anna university, Coimbatore
[1] PG Student, Maharaja Institute of Technology, Coimbatore,
[2] PG Student, Maharaja Institute of Technology, Coimbatore,
[2] M.E.(CSE), Professor, Maharaja Institute of Technology, Coimbatore.

Abstract: **Cloud computing is emerged as a data interactive model in which users can store their data in an online cloud server. Online storing and retrieving data in third party's cloud system causes serious conflict over data security and data confidentiality during the data transactions. A secured distributed storage system is formulated using a secured threshold proxy re-encryption server that integrates with a decentralized erasure code.**

Keywords: Proxy Re-Encryption, Erasure Code, Splitting Technique

I.INTRODUCTION

A cloud storage consist of a collection of storage servers. In cloud storage, users can remotely store their data and use the applications and services from the shared pool. Storing data in a cloud system causes concern over data security. I propose a threshold proxy re-encryption scheme for secured data forwarding using erasure code. Multiple users can interact with the storage system. The distributed storage system supports secure and robust data storage and retrieval. The proxy re-encryption scheme supports encoding operations along with a key over encrypted messages and done forwarding operations. Cloud storage supports privacy preserving public auditing. A third party auditor can be used to check the integrity of outsourced data.

A) SYSTEM DETAILS

a) Existing System

Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. During early years, the Network-Attached Storage (NAS) and the Network File System (NFS) provide extra storage devices over the network such that a user can access the storage devices via network connection. Afterward, many improvements on scalability, robustness, efficiency, and security were proposed.

Disadvantages of existing system

- General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data.
- Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.
- Data robustness is a major requirement for storage systems.

b) Proposed System

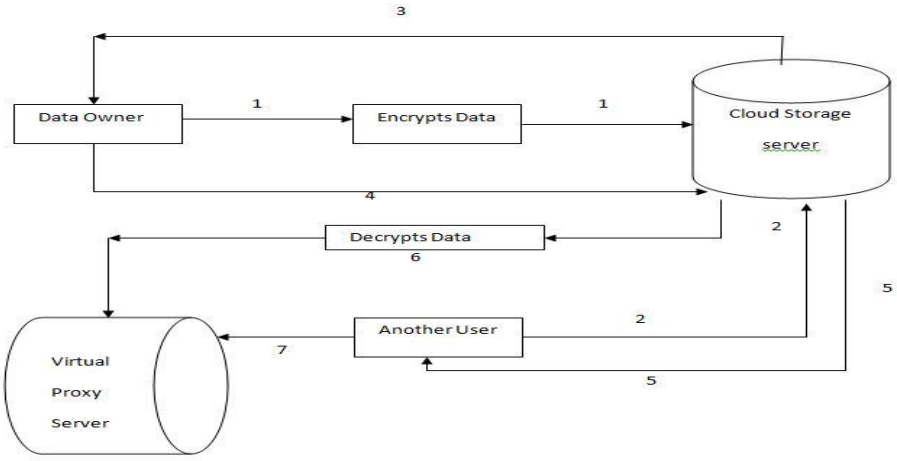
The proposed system propose a protocol based threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated.By using the threshold proxy re-encryption scheme,a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure is formulated.Storing data in a third party's cloud system causes serious concern on data confidentiality. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages.When he wants to use a message, he needs to retrieve the codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys.

Advantages of proposed system

- The paper focus on designing a cloud storage system for robustness, confidentiality, and functionality.
- A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers.
- Provide one time data access based on Time/Date protocol.
- Secured threshold proxy re-encryption server provide more security and helps in access enhancement/restriction.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

II. SYSTEM ARCHITECTURE



1. Data owner Store the original data in to the cloud storage server. The data will encrypt and stored in the cloud storage server.
2. Any can view the uploaded data. But the data will be in the encrypted format. Another user can only view the file name of the data. And another user will send request to the cloud server to view the data.
3. Cloud server will forward the request from the user to the data owner.
4. Data owner wants to accept the request from the cloud server.
5. Cloud server will forward a de encrypted key to the user.
6. Simultaneously cloud server will create a virtual server and decrypts the data from the cloud storage server.
7. User can enter the de encrypted key to the proxy server to view the original data. The key will be valid for one time only.
8. After the data view from the proxy server, the virtual data will be deleted automatically.

A) Modules

- Cloud Formation
- Data Owner
- Construction of secure cloud storage
- Proxy re-encryption
- Secure data Forwarding over cloud

Cloud formation

The public cloud environment is the IaaS/PaaS Infrastructure that we rent from Linux (IaaS) or Microsoft (PaaS).Both are enabled for web hosting. The SaaS stack will run under our own equipment which would make it private. The paper implementing a web services for the output purpose as well as the environment will be shown in actual while hosting the application. The SaaS can be fully utilized in cloud environment as IaaS/PaaS.

Data Owner

The data owner have the control over information to access, create, modify, derive benefit from, sell or remove data. Data ownership is act of having legal rights and complete control over data. The data owner can create a login and upload their files in the cloud storage.

Construction of secure cloud storage

A personalized cloud store server for both big data and secured erasure code. The storage server will be unique which is distributed into much system for easy access of data.

Proxy Re-Encryption

Decentralized erasure codes are sparse and having reduced communication, storage and comtputation cost. Assume that there are n storage nodes with limited memory and k<n sources generating the data. A data collector who appear in the network for accessing data is needed to query any k storage nodes, to retrieve the data.

Secure data forwarding over cloud

Proxy re-encryption schemes are cryptosystems which allow third-parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. . It allows a message recipient (key holder) to generate a re-encryption key based on his secret key and the key of the delegated user. This re-encryption key is used by the proxy as input to the re-encryption function, which is executed by the proxy to translate cipher texts to the delegated user's key

B) Algorithm used

Rijndael, the length of both the block to be encrypted and the encryption key are not fixed. They can be independently specified to 128, 192 or 256 bits. The number of rounds varies according to the key length. It can be equal to 10, 12 and 14 when the key length is 128bits, 192 bits and 256 bits, respectively. The basic components of Rijndael are simple mathematical, logical, and table lookup operations.Rijndael is considered to be the fastest algorithm in terms of the critical path between plaintext and cipher text.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

Steps involved

1. Key Selection: The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block is 8bits long (8*16=128 bits).
2. Generation of Multiple keys: The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a onetime process; these expanded keys can be used for future communications any number of times till they change their initial key value.
3. Encryption: Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: SubBytes, ShiftRows, MixColumns and AddRoundKey.
4. Decryption: The decryption process is similar as encryption, but we use Inverse SubByte Transformation.

III. PRACTICAL RESULT

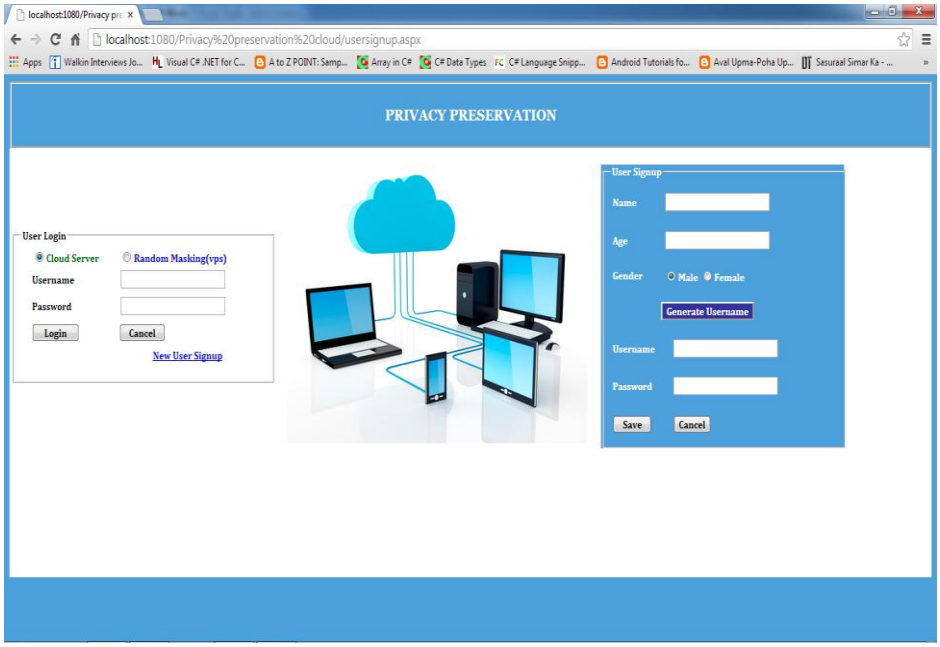


Figure 1: New user sign up

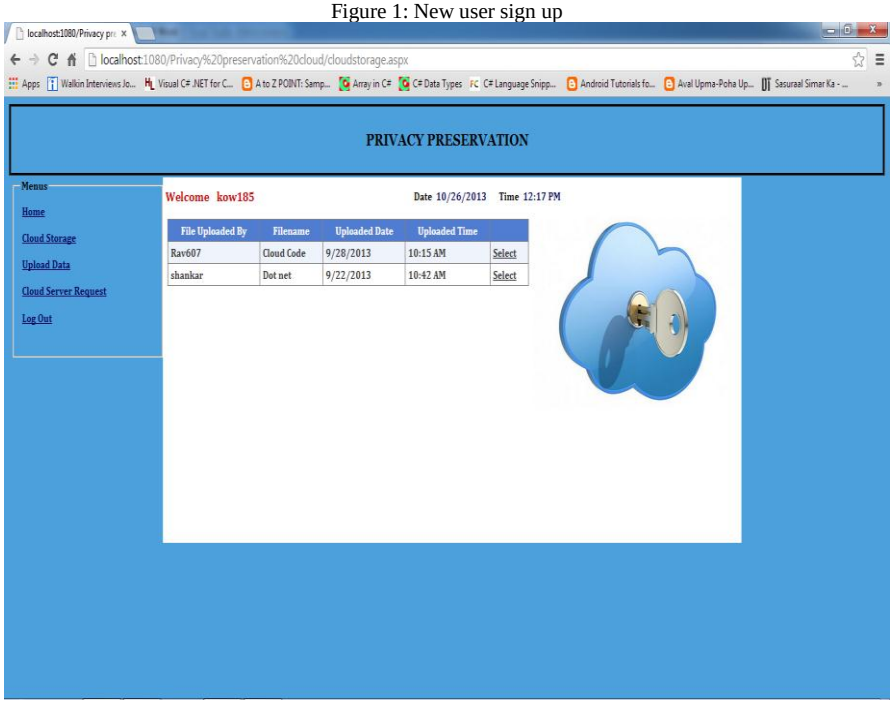


Figure 2 : Cloud storage

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

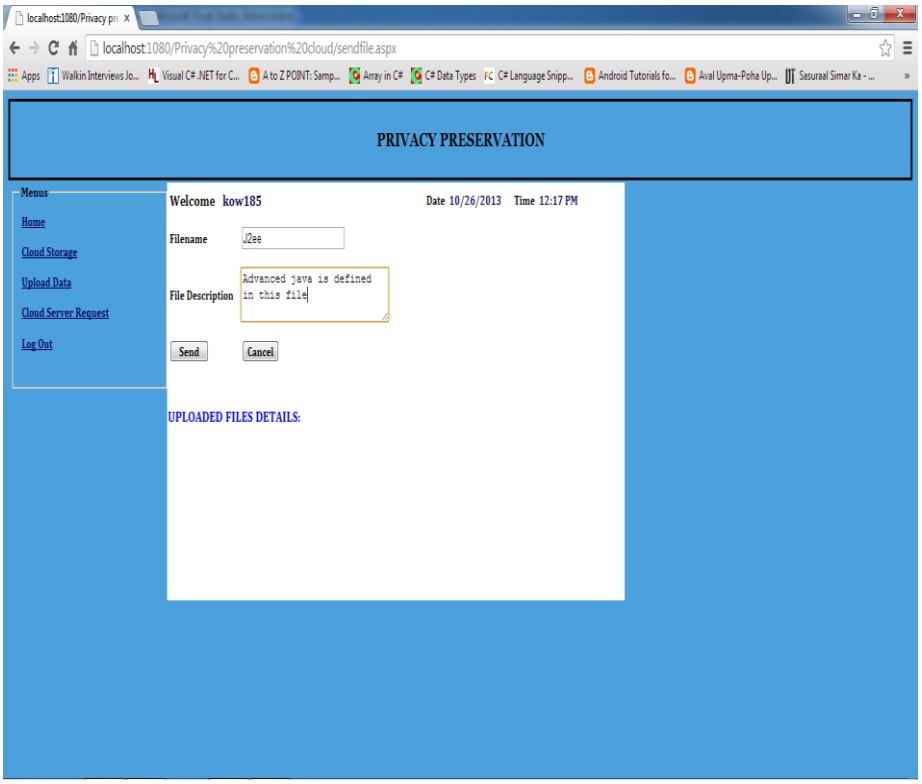


Figure 3: User uploading files in cloud storage

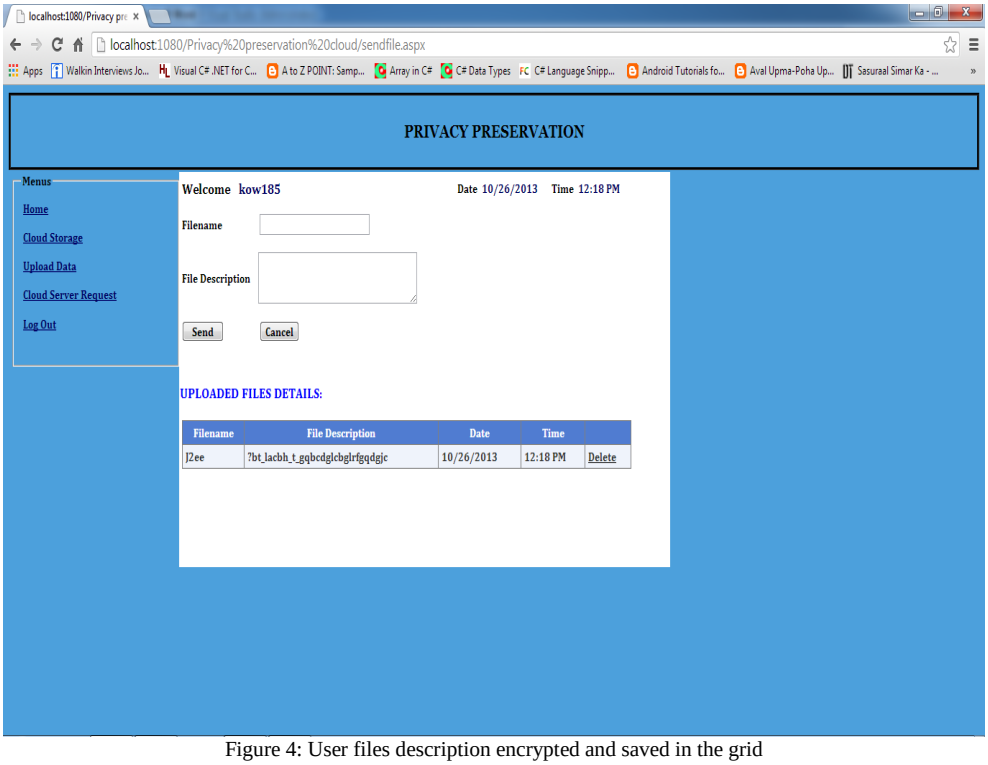


Figure 4: User files description encrypted and saved in the grid

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

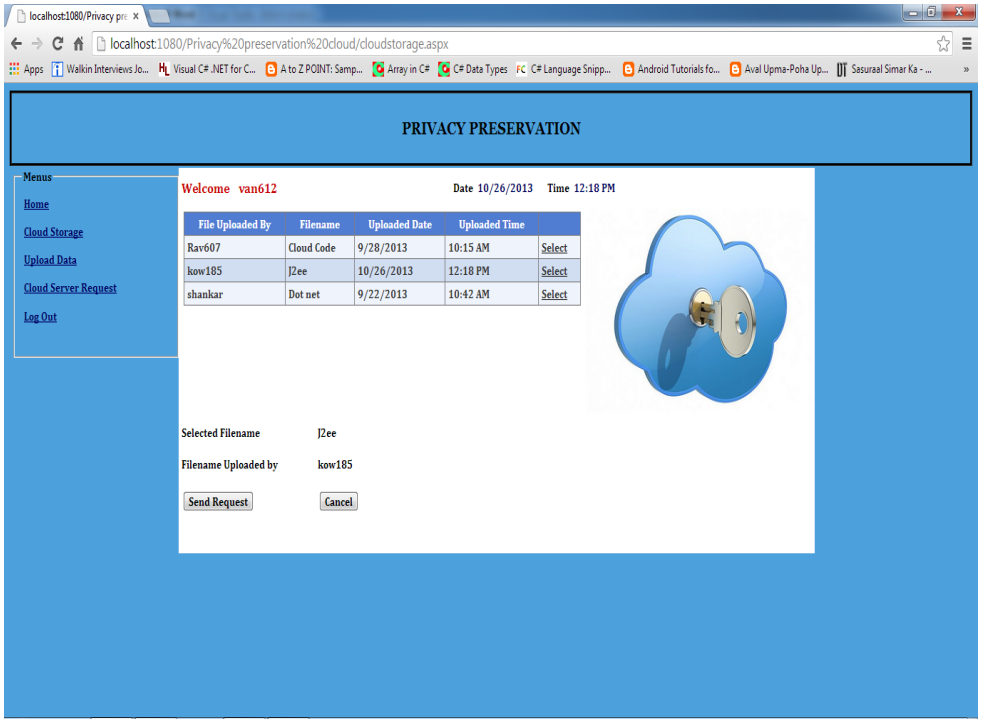


Figure 5 : User 2 sending request for the file to user1

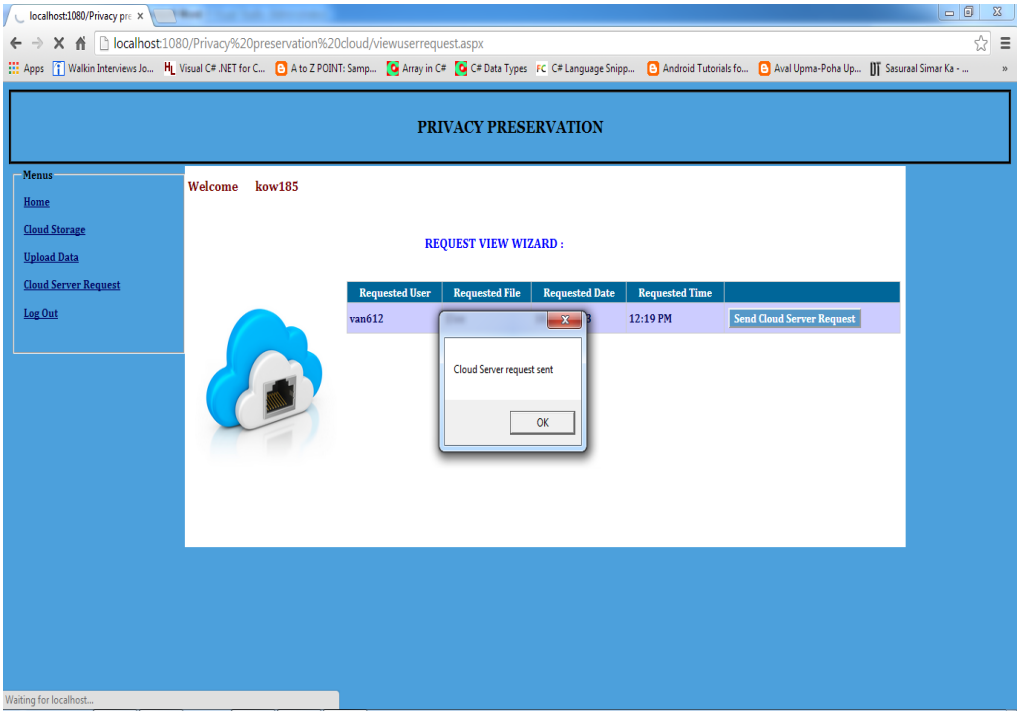


Figure 6: Acknowledgement for cloud server request sent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

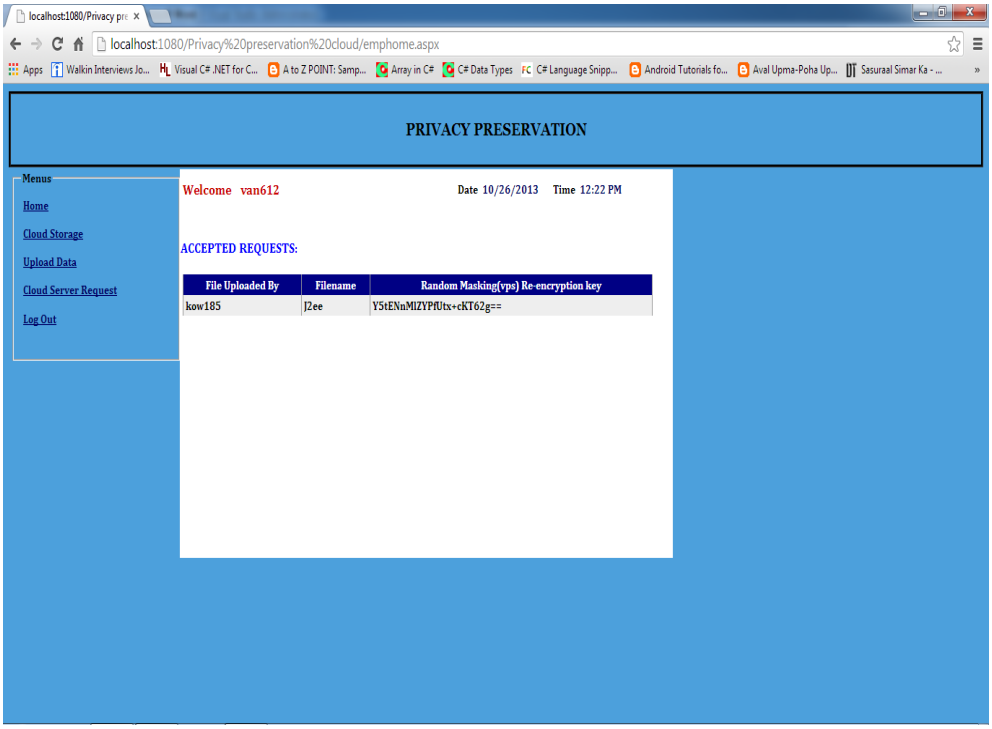


Figure 7: User2 receives the permission for viewing the file along with the proxy key

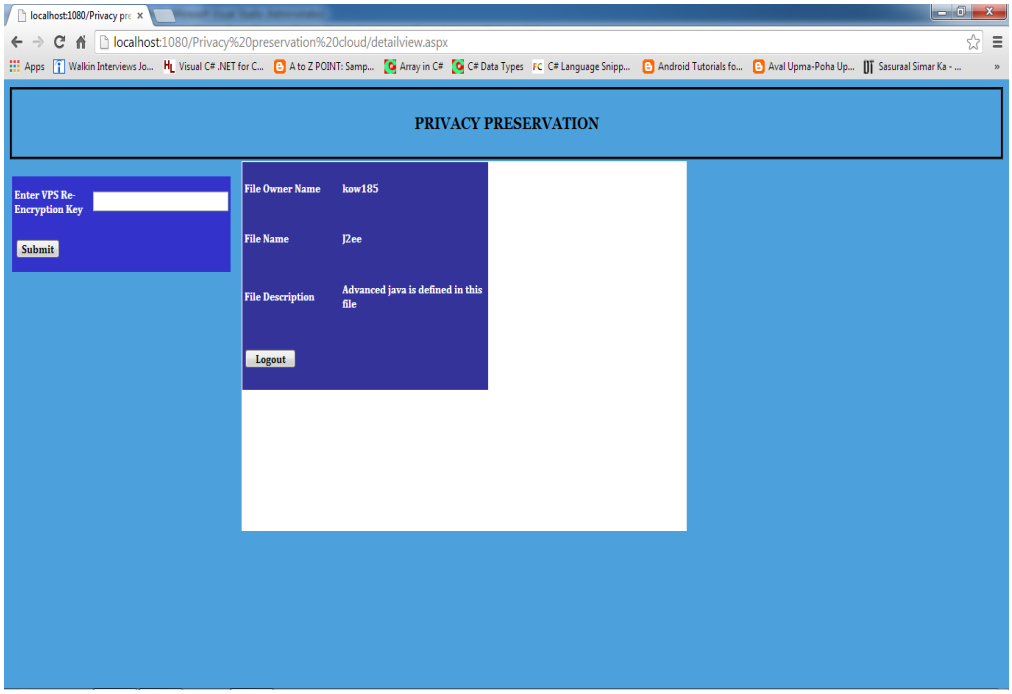


Figure 8:User views the encrypted file description in decrypted form

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

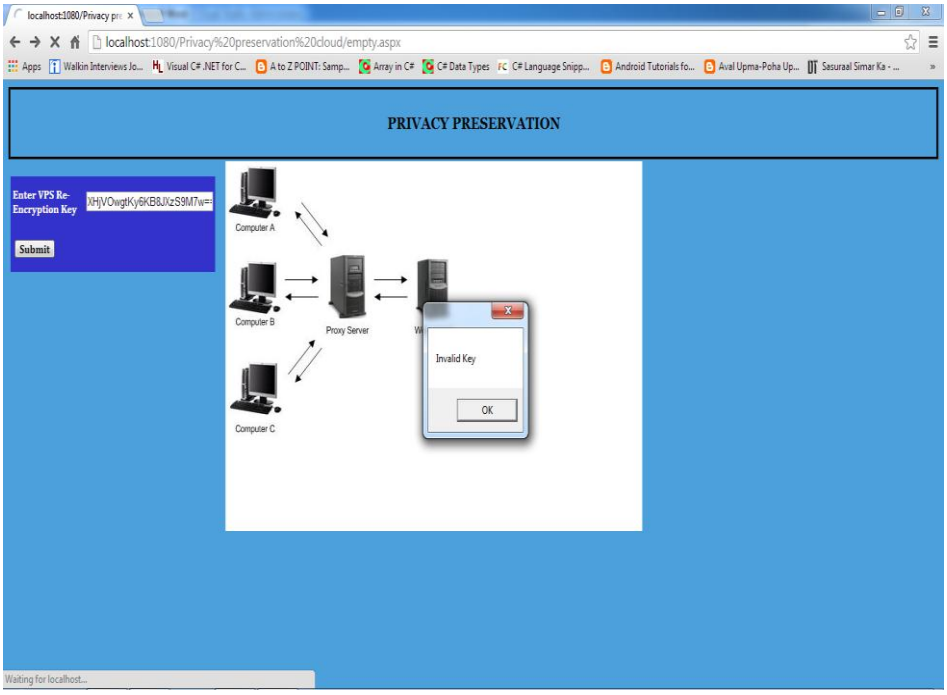


Figure 9:User cannot access the file once the key is used

IV. FUTURE WORK

In future work,the proxy server can be enhanced for more secured data transfer. The proxy refers to a layer-7 application on the OSI reference model. Another way of proxying is through layer-3 which is known as Network Address Translation.

- Layer 7 virtual proxy servers can be used.
- Output can be shown using some medical domain for real time implementation.
- EC2 Cloud server can be implemented.
- Key character length can be increased for more security
- HTTPS can be implemented.
- Network Address Translation (NAT) can be implemented
- Big data concepts can be included in case of huge number of data transaction.

V. CONCLUSION

The paper proposes cloud storage system consists of storage servers and key server. A threshold proxy re-encryption scheme is integrated with erasure code over exponents. The encryption scheme supports encoding, forwarding and partial decryption operations. Each storage server independently performs encoding and re-encryption. Each key server independently perform partial decryption. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks. Our key servers act as access nodes for providing a front-end layer such as a traditional file system interface. Splitting technique is used to provide secured data forwarding over cloud.

REFERENCES

[1] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, (2007)"Provable Data Possession at Untrusted Stores,"Proc. 14th ACM Conf. Computer and Comm. Security (CCS), pp. 598-609.

[2] Ateniese G, BensonK, and Hohenberger S,(2009) "Key-Private Proxy Re-Encryption, "Proc. Topics in Cryptology (CT-RSA),pp. 279-294.

[3] Ateniese G, Fu K, Green M, and Hohenberger S, (2006)"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,"ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30.

[4] Ateniese G, Mancini L.V ,Pietro R,D and Tsudik G,(2008) "Scalable and Efficient Provable Data Possession,"Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm),pp. 1-10.

[5] Blaze M, Bleumer G, and Strauss M,(1998) "Divertible Protocols and Atomic Proxy Cryptography,"Proc. Int'l Conf. Theory and Applica-tion of Cryptographic Techniques (EUROCRYPT),pp. 127-144.

[6] Bhagwan R, Cheng Y.C, Savage S, Tati K and Voelker G.M, (2004) "Total Recall: System Support for Automated Availability Management,"Proc. First Symp. Networked Systems Design and Implementation (NSDI),pp. 337-350.

[7] Cao Z, Shao J,(2009) "CCA-Secure Proxy Re-Encryption without Pairings,"Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC),pp. 357-376.

[8] Dimakis A.G, Prabhakaran V, and Ramchandran,(2005) "Ubiqui-tous Access to Distributed Data in Large-Scale Sensor Net-works through Decentralized Erasure Codes,"Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN),pp. 111-117.

[9] Dimakis A.G, Prabhakaran V, and Ramchandran K,(June,2006) "Decen-tralized Erasure Codes for Distributed Networked Storage,"IEEE Trans. Information Theory,vol. 52, no. 6 pp. 2809-2816.

[10] Mambo M and Okamoto E,(1997) "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences,vol. E80-A, no. 1, pp. 54-63.

[11] TangQ,(2008) "Type-Based Proxy Re-Encryption and Its Construction," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT),pp. 130-144.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 05, May - 2017

Roshitha P P, B. Tech (CSE), Pursuing M. E (Computer Science and Engineering) in Maharaja Institute of Technology. Have keen interest in the Cloud Computing, Networking and Mobile Computing, worked as a guest lecturer for 1 year.

Sneha. T. Subramanian,,B.Tech(CSE),Pursuing M.E(Computer Science and Engineering) in Maharaja Institute of Technology. Have keen interest in the Cloud Computing, Networking and Mobile Computing, worked as a guest lecturer for 1.5 year.

Prof. T. Sivakumar, ME (CSE), He had 10 years of experience in teaching industry. His areas of interest are data mining and data source. Participated in various international and national level conference, seminars/webinars and workshops.