ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Secure File Storage using Hybrid Cryptography

Sonukumar[1], Vibhas kale[2], Sanket Sarode[3], Rishikesh Girgaonkar[4], Dr. Srinivas Ambala[5]

UG Student, Department of Computer Engineering, G. H. Raisoni College of Engineering And Management, Wagholi, Pune, India[1, 2, 3, 4]

Professor, Department of Computer Engineering, G. H. Raisoni College of Engineering And Management, Wagholi, Pune, India[5]

ABSTRACT: Cloud computing model allows the customers to access the secured information from the cloud server without the help of using the hardware or the software. For the effective usage of the data from the cloud provider, the data owner encrypts the data and then its ends to the cloud server. To secure the data in the cloud we have dealt through lots of security issues earlier. In this system we have proposed the idea how the data could be made more secured using visual cryptographic techniques. This model not only increases the trust among the users to send their information with full reliability and also helps in the authorization of the users.

KEYWORDS: Cloud Computing, Visual Cryptography, File Backup, Encryption.

I. INTRODUCTION

Security has emerged as the most concerned aspect of cloud computing environment and a prime challenge for the cloud users. The stored data can be retrieved by the user whenever and wherever required. But there is no guarantee that the data stored in the cloud server has not been accessed by any unauthorized user.

The current cloud framework does not allow encrypted data to be stored due to the space and storage cost. Storing secret data in an unencrypted form is vulnerable to external attacks by both illegitimate customers and a Cloud Service Provider (CSP)

Traditional encryption techniques require more computation and storage space. Hence, protecting cloud data with minimal computations is the prime task. Secured Document Sharing Using Visual Cryptography technique proposes an efficient storage scheme in a cloud for storing and retrieving a document file ensures data confidentiality and integrity.

II. REVIEW OF LITERATURE

1. Neha K. Lakde, ``Visual Cryptography Scheme with Authentication Using Shamir Andmk Reddy Techniques", International Refereed Journal of Engineering and Science (IRJES)

In this paper introduced a technique for visual cryptography in which any type of image can be chosen as a password, images then divided and then apply Shamir and M K Reddy encryption and decryption techniques . After decryption system get match with original image then system give result as the user is authenticate otherwise non authenticate. The system introduced in this paper satisfy the needs of authentication. From Implementation. And Results we can say that this system can help in using multiple size and type of images for authentication. Shamir is one of the algorithm to satisfy the needs for authentication. The PNSR value is enhanced by using the system. The time required by the system is lesser then normal system. More the number of authentication parts less is the time required. From all the results we can also say that Shamir is better than MK Reddy which satisfy the needs for authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

2 Anandhi and S. Satthiyaraj, ``Embedded Visual Cryptography Schemes for Secret Images", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.12, December 2012

Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using the tool, thus gets the original image. The proposed Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using the application here sender gets the two or more transparencies of the same image. The application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using the application we can send encrypted images that are in the format of GIF and PNG.

3. Rini K, D. Rajapriya, ``Secure Data Transfer: Based on Steganography and Visual Cryptography", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 5 May 2017, Page No. 21523-21527

Secure data transfer is one of the most important concern with the internet users who are transmitting highly secures information through internet. We have various technologies available to overcome this issue and the main includes the steganographic and visual cryptographic techniques. Using steganography, messages senders can hide their secure data in image, audio or video files. Images are widely used because of its availability as well as there are millions of images are transmitted through internet in each fractions of second, which makes them an excellent cover for secure messages. Steganography got a challenger in the form of steganalysis who can recreate the secure data from the message using various steganalysis techniques. Visual cryptography is another important method which provides 2 way authentication, where the user the needs to get all the shares of the image to complete the required action. In this paper, we have presented a system which uses both the concepts of steganography and visual cryptography to securely transfer data. The secured message is hidden in the image using the steganographic LSB and then the images are partitioned into shares and send separately to the receiver. The receiver needs all the shares to recover the image with hidden message and then the message to be decoded from the image.

4. K. Brindha, N. Jeyanthi, ``Secured Document Sharing Using Visual Cryptography in Cloud Data Storage"

Security has emerged as the most concerned aspect of cloud computing environment and a prime challenge for the cloud users. The stored data can be retrieved by the user whenever and wherever required. But there is no guarantee that the data stored in the cloud server has not been accessed by any unauthorized user. The current cloud framework does not allow encrypted data to be stored due to the space and storage cost. Storing secret data in an unencrypted form is vulnerable to external attacks by both illegitimate customers and a Cloud Service Provider (CSP). Traditional encryption techniques require more computation and storage space. Hence, protecting cloud data with minimal computations is the prime task. Secured Document Sharing Using Visual Cryptography (SDSUVC) technique proposes an efficient storage scheme in a cloud for storing and retrieving a document file without any mathematical computations and also ensures data confidentiality and integrity.

III. EXISTING SYSTEM

In the existing system visual cryptography is used where they take original image and perform encryption on it that is divide that secret image into two shares and transfer over the network and for data extraction data decryption is used in that these shares are combined together to retrieve actual data. Many of the existing schemes in Visual cryptography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

result in size of shares growing very large, depending on the image type and size. Typically, as the contrast improves, the share size also increases quite dramatically. This increases the image processing time to overall increase in the complexity of the schemes. It reduces the overall potential for the practical application of VC.

IV. SYSTEM ARCHITECTURE

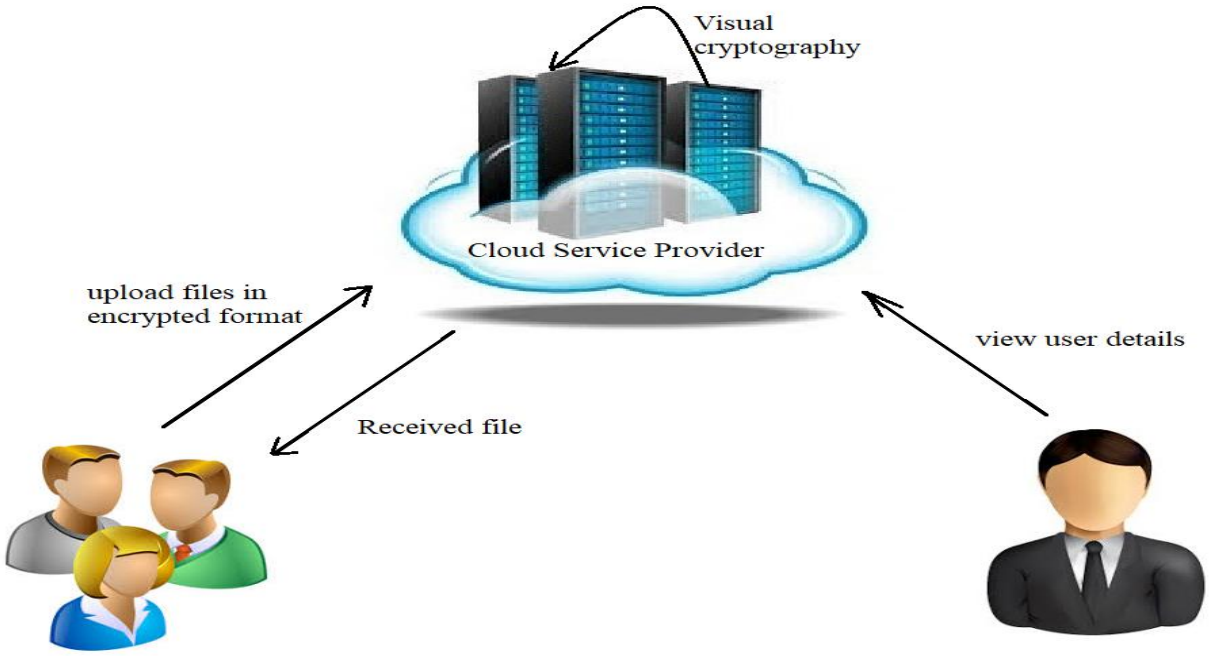

Fig. 1. Propose System Architecture

- Admin: admin can view how many user register to the system.
- User: first user register to the system then user upload his/her files on cloud in encrypted format.

- Visual Cryptography: Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields

V. ALGORITHM

AES Algorithm

1. KeyExpansions
   For each round AES requires a separate 128-bit round key block plus one more.
2. InitialRound
   AddRoundKey—with a block of the round key, each byte of the state is combined using bitwise xor.
3. Rounds
- SubBytes—in this step each byte is replaced with another byte.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

- ShiftRows— for a certain number of steps, the last three rows of the state are shifted cyclically.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

1. Final Round (no MixColumns)

- SubBytes
- ShiftRows

AddRoundKey.

MD5 Algorithm

Computation of the MD5 digest value is performed in separate stages that process each 512-bit block of data along with the value computed in the preceding stage:

1. The first stage begins with the message digest values initialized using consecutive hexadecimal numerical values.

2. Each stage includes four message digest passes which manipulate values in the current data block and values processed from the previous block.

3. The final value computed from the last block becomes the MD5 digest for that block.

Visual Cryptography

- Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

- Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields.

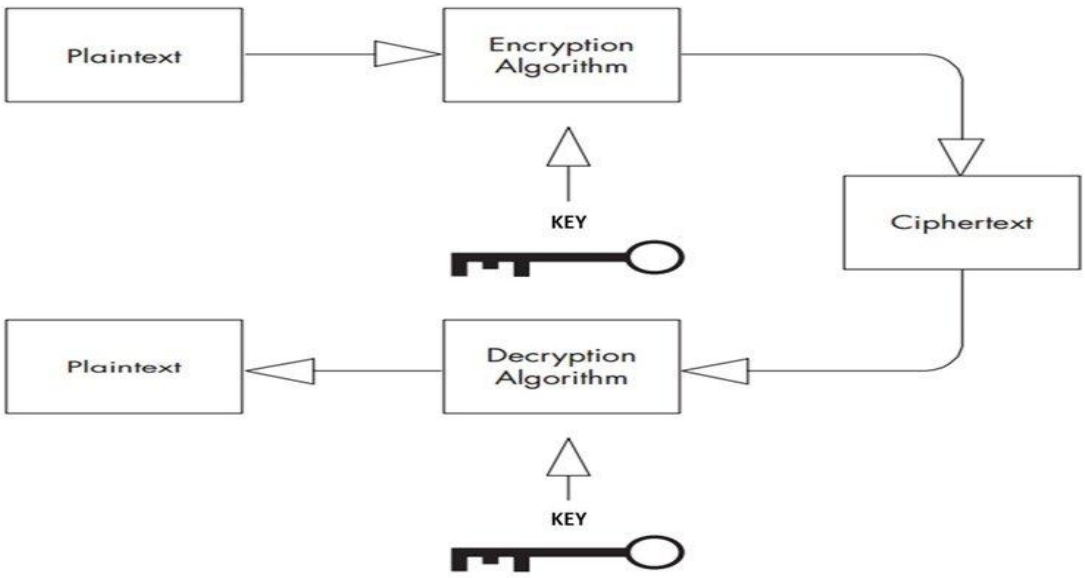

Fig: Visual Cryptography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

VI. RESULT

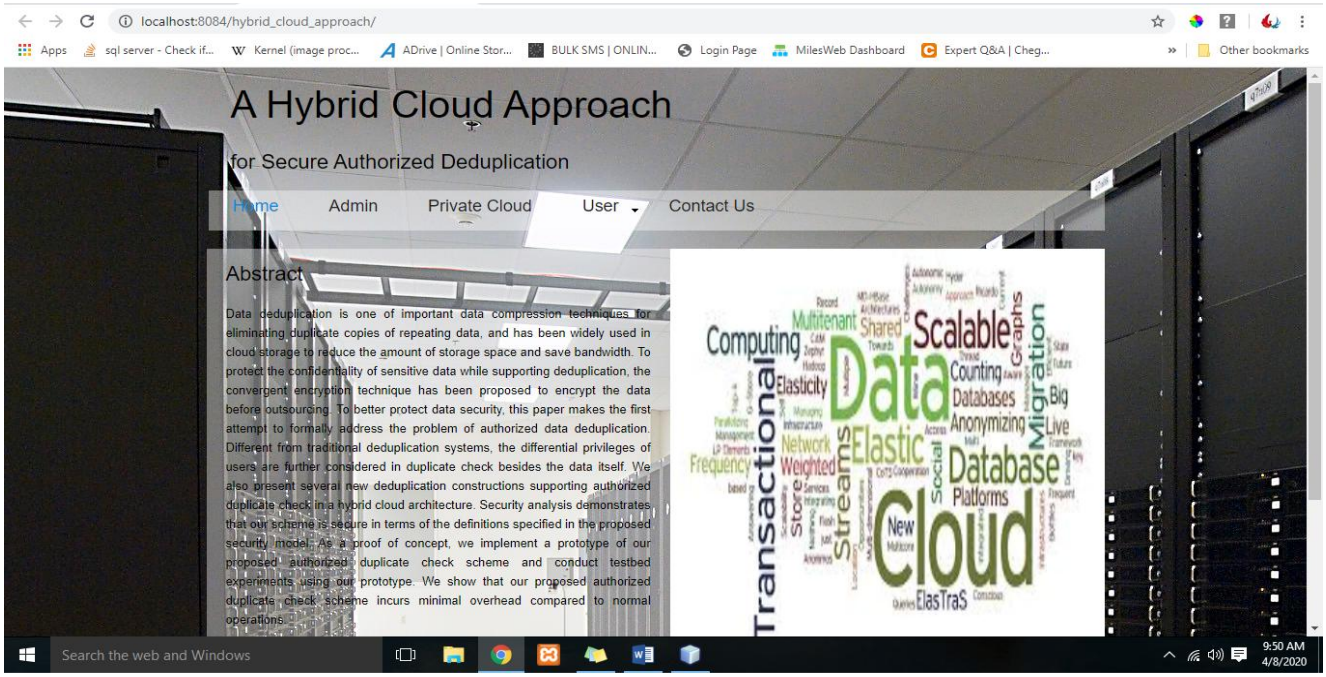

Fig. Home Page

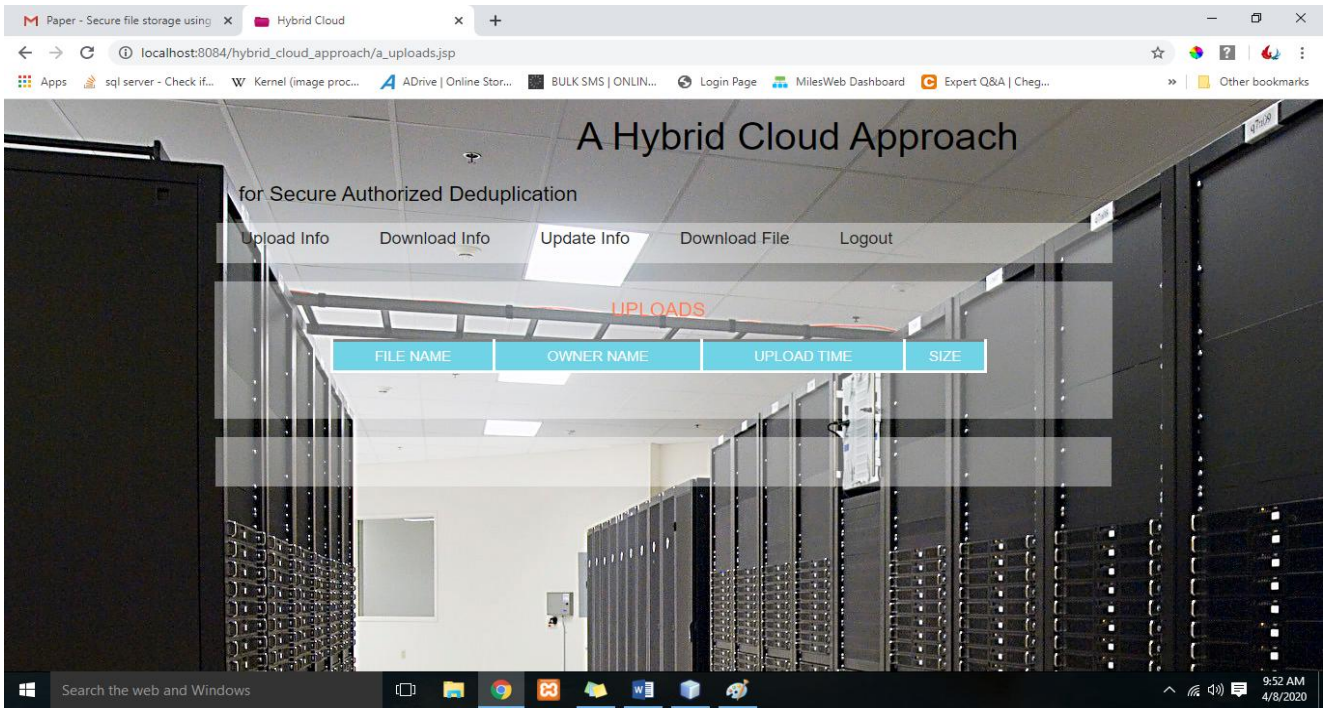

Fig: Admin Menu

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

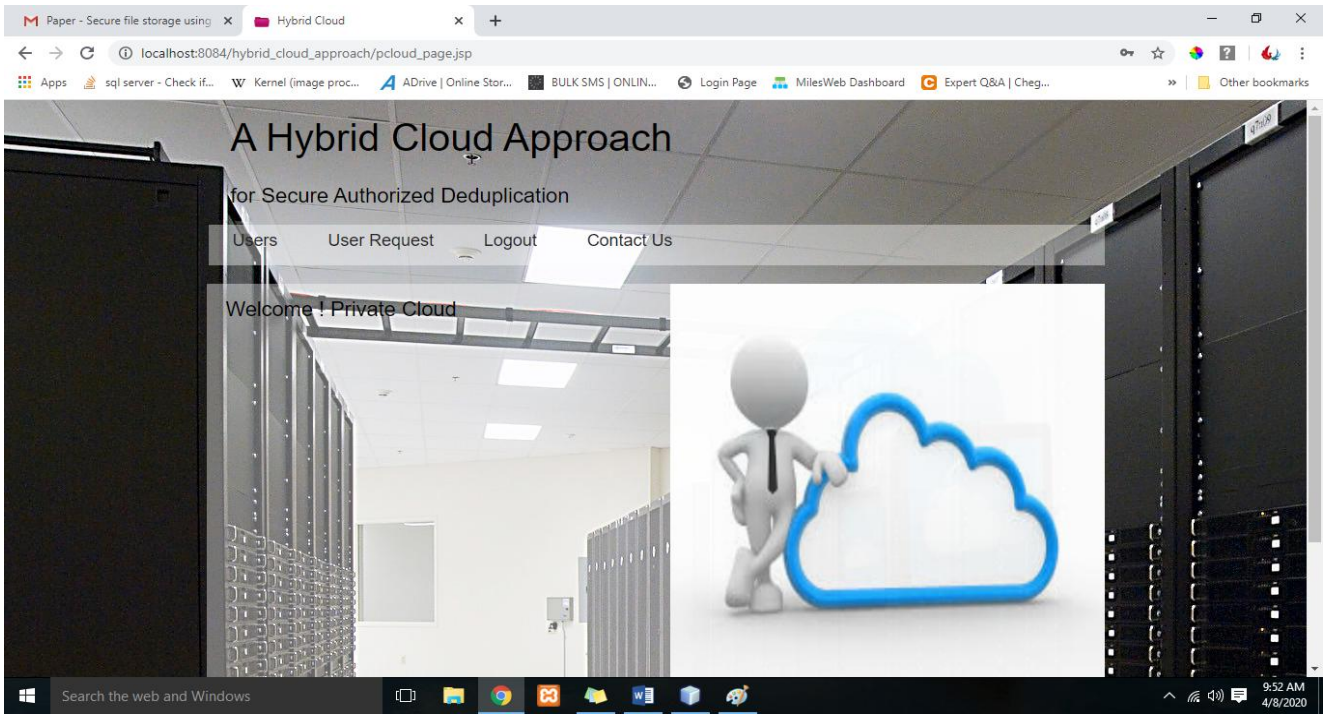

Fig: Private Cloud Menu

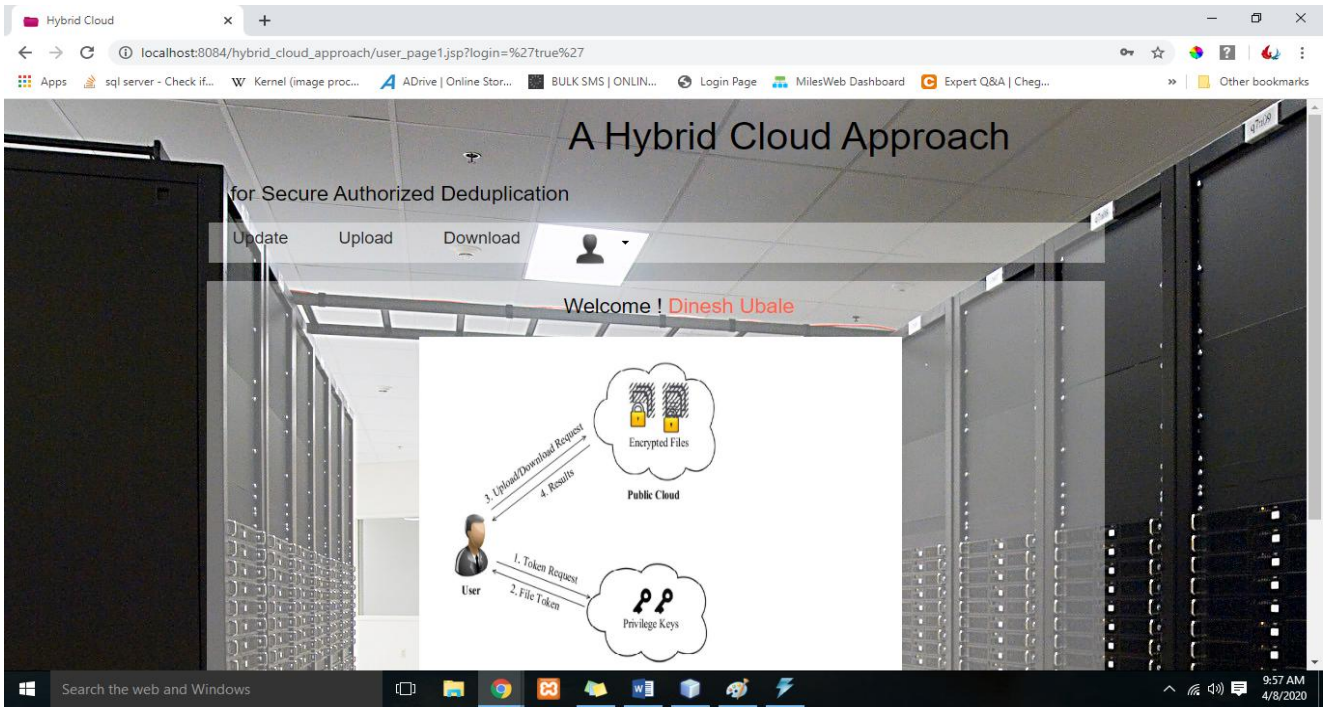

Fig: User Menu

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

VII. APPLICATIONS

1. Banking
2. E-voting
3. Integrity in Storage
4. Authentication of Identity
5. Credentialing Systems

VIII. BENEFITS

1. Data User and data owner easily upload file and download.
2. To store information in secure format.

XI. CONCLUSION

The proposed system designed to provide a secure data and a trustworthy cloud computing system. To ensure the correctness of client data in cloud data storage, the proposed method encrypts data and stores it in cloud and user is allowed for modification of data. Through data security and performance analysis, it shows that work is highly efficient and avoid unauthorized users from accessing the data.

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Advancesin Cryptography (EUROCRYPT'94), 1995, vol. 950, LNCS, pp. 1–12.
2. R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam. Electron., Commun., Comput. Sci.,vol. 82, pp. 2172–2177, Oct. 1999.
3. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit.Lett., vol. 25, pp. 481–494, Mar. 2004.
4. S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally optimal contrast, and no expansion, "J. Vis. Commun. Image Represent. , vol. 21, pp. 900–916, Nov.2010.