International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage

A. Brahma Reddy[1], K. V. Ranga Rao[2], V. Vinay Kumar[3]

[1]Associate Professor, Department of CSE, Malla Reddy College of Engineering for Women, Telangana, India
[2]Professor & HOD, Department of CSE, Neil Gogte Institute of Technology, Telangana, India
[3]Associate Professor, Department of ECE, Anurag University, Venkatapur, Telangana, India

ABSTRACT

As a significant application in distributed computing, distributed storage offers client adaptable, adaptable and top notch information stockpiling and calculation administrations. A developing number of information proprietors decide to re-appropriate information records to the cloud. Since distributed storage workers are not completely reliable, information proprietors need trustworthy intends to check the ownership for their documents moved operations to far off cloud workers. To address this vital issue, some distant information ownership checking (RDPC) conventions have been introduced. However, many existing plans have weaknesses in effectiveness or information elements. In this paper, we give another productive RDPC convention dependent on homomorphic hash work. The new plan is provably secure against phony assault, supplant assault and replay assault dependent on a run of the mill security model. To help information elements, an activity record table (ORT) is acquainted with track procedure on document blocks. We further give another streamlined execution for the ORT which makes the expense of getting to ORT almost steady. Besides, we make the far reaching execution investigation which shows that our plan has preferences in calculation and correspondence costs. Model usage and examinations show that the plan is plausible for genuine applications.

KEYWORDS: *RDPC protocol, homomorphic hash function, ORT, cloud computing*

How to cite this paper: A. Brahma Reddy | K. V. Ranga Rao | V. Vinay Kumar "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1568-1578, URL: www.ijtsrd.com/papers/ijtsrd35727.pdf

IJTSRD35727

1. INTRODUCTION

Cloud computing is the use of computing resources that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

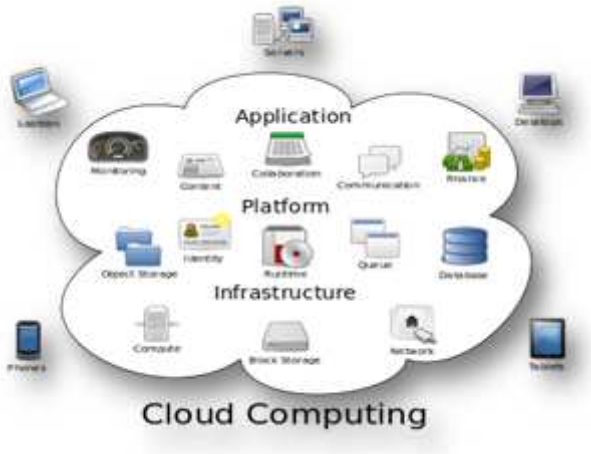


Fig 1: Structure of cloud computing

2. Existing System:

1. The first RDPC was proposed by Deswarte et al. based on RSA hash function. The drawback of this scheme is that it needs to access the entire file blocks for each challenge.

2. In 2007, the provable data possession (PDP) model was presented by Ateniese et al., which used the probabilistic proof technique for remote data integrity checking without accessing the whole file. In addition, they supplied two concrete schemes (S-PDP, E-PDP) based on RSA.
3. Although these two protocols operations had good performance, it's a pity they didn't support dynamic operations. To overcome this shortcoming, in 2008, they presented a dynamic PDP scheme by using symmetric encryption. Nonetheless, this scheme still did not support block insert operation. At the same time, lots of research works devoted to construct fully dynamic PDP protocols. For instance, Sebé et al. provided a RDPC protocol for critical information infrastructures based on the problem to factor large integers, which is easily adapted to support data dynamics.

2.1. Disadvantages Of Existing System:

1. Did not Support Dynamic Operation.
2. Heavy Computation Cost.
3. Insecure against replay attack and deletion attack.
4. These schemes are either insecure or not efficient enough.

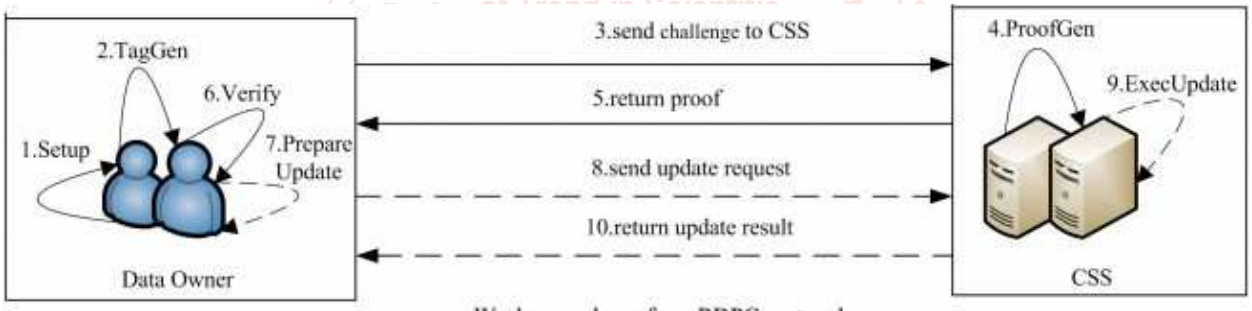
3. Proposed System:

1. We present a novel efficient RDPC scheme with data dynamics. The basic scheme utilizes homomorphic hash function technique, in which the hash value of the sum for two blocks is equal to the product for two hash values of the corresponding blocks
2. We introduce a linear table called ORT to record data operations for supporting data dynamics such as block modification, block insertion and block deletion. To improve the efficiency for accessing ORT, we make use of doubly linked list and array to present an optimized implementation of ORT which reduces the cost to nearly constant level.
3. We prove the presented scheme is secure against forgery attack, replay attack and replace attack based on a typical security model. At last we implement our scheme and make thorough comparison with previous schemes.

3.1. Advantages Of Proposed System:

1. Experiment results show that the new scheme has better performance and is practical for real applications.
2. We show the advanced RDPC scheme supporting fully dynamic block operations based on ORT.
3. Minimum Computation Costs.
4. The data owner can perform dynamic operations of the files

4. System Architecture:



Work procedure of our RDPC protocol

5. Results:

Figure 5.1 Home page

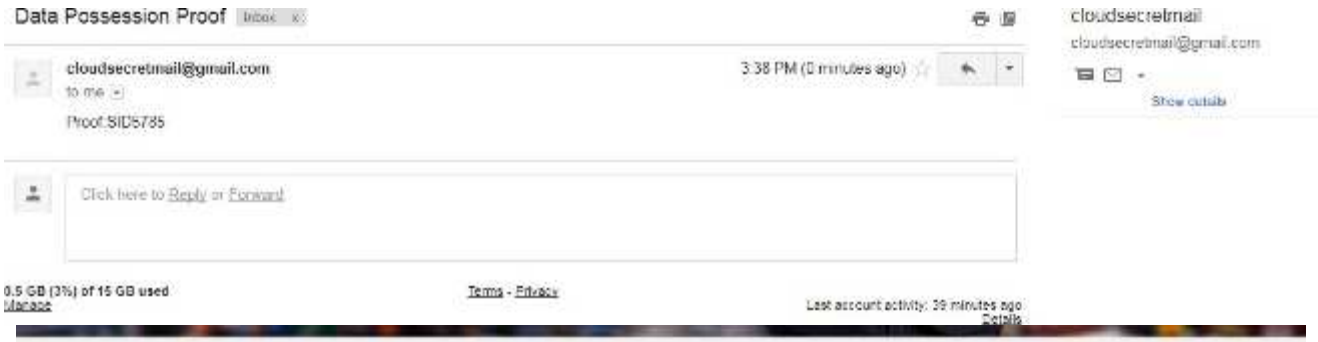


Figure 5.2 Data Owner Registration

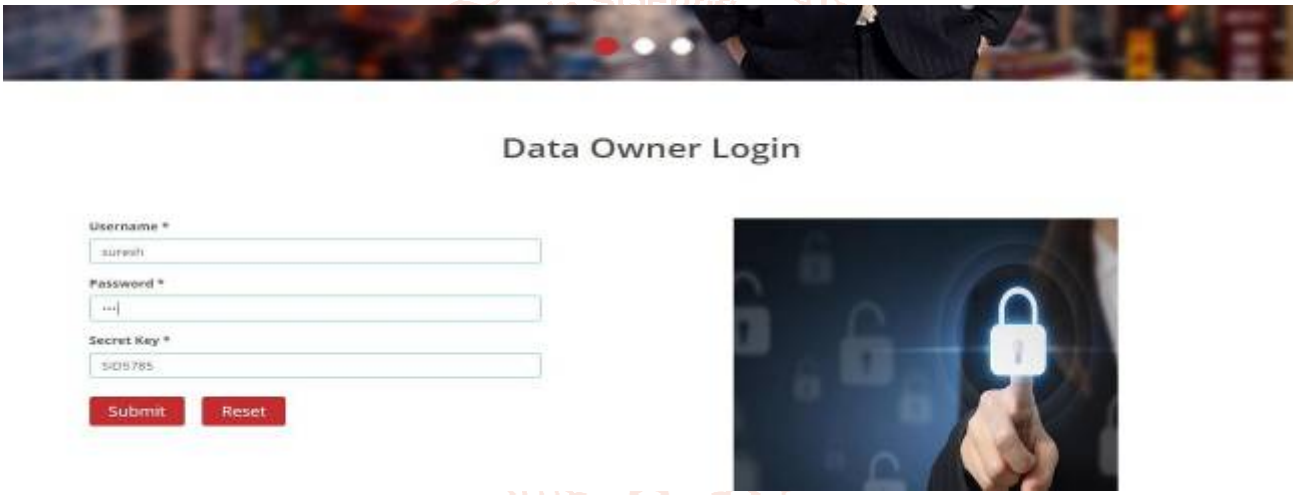


Figure 5.3 Data Owner Login

Figure 5.4 Data Owner Home

Figure 5.5 Upload file and generate keys

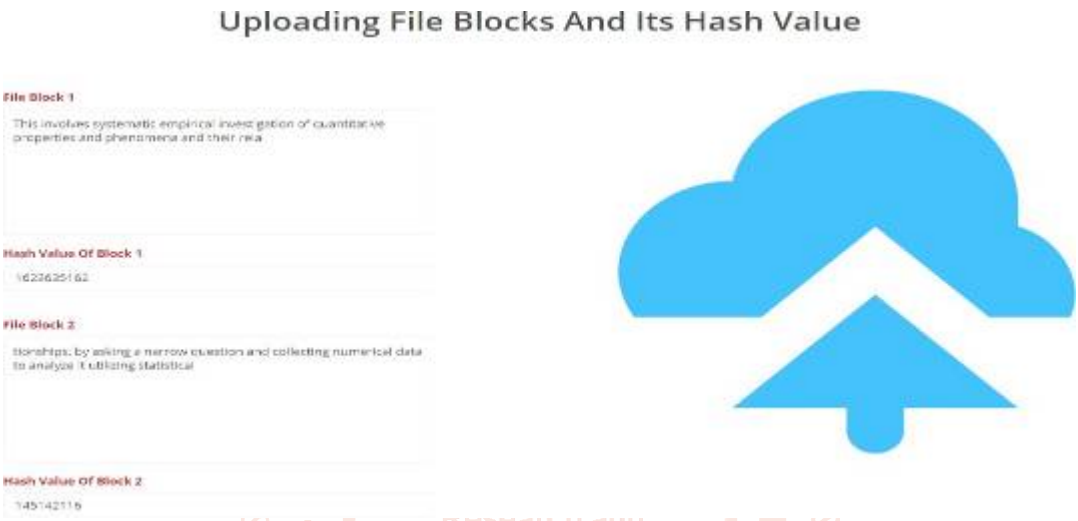


Figure 5.6 Uploading file blocks and its hash value

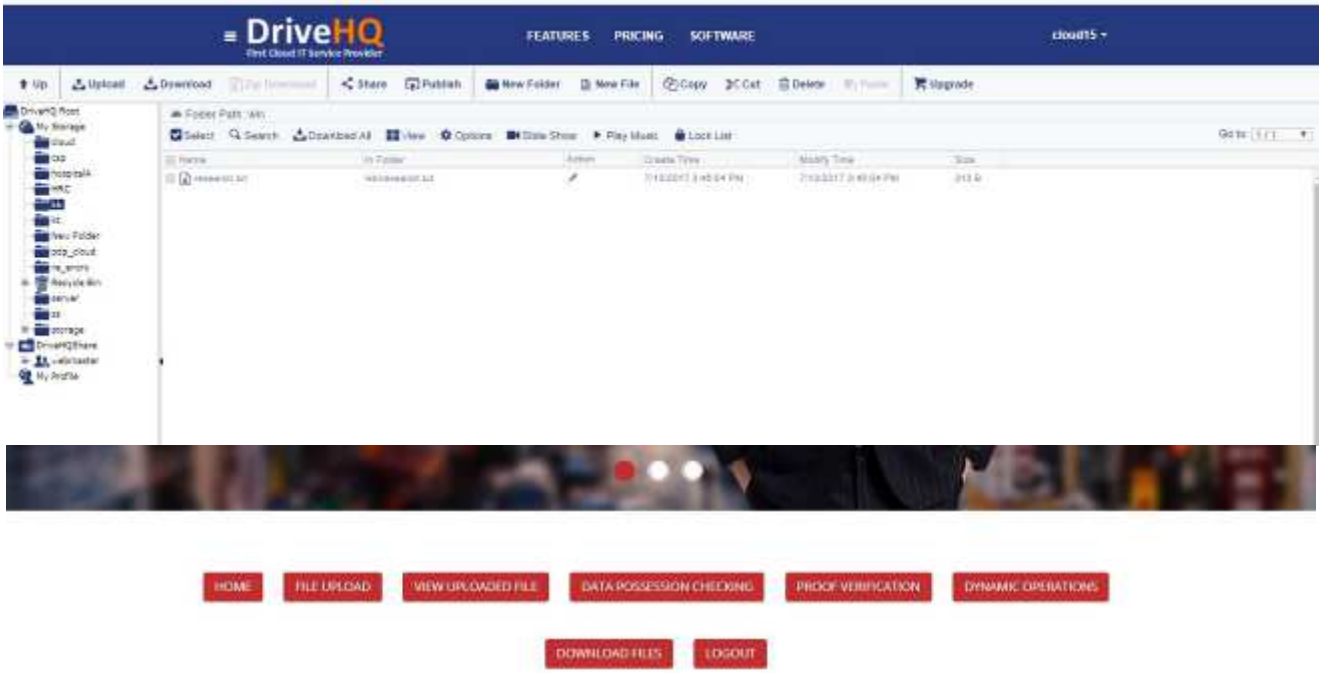


Figure 5.7 View uploaded files

Figure 5.8 Data Possession Challenge

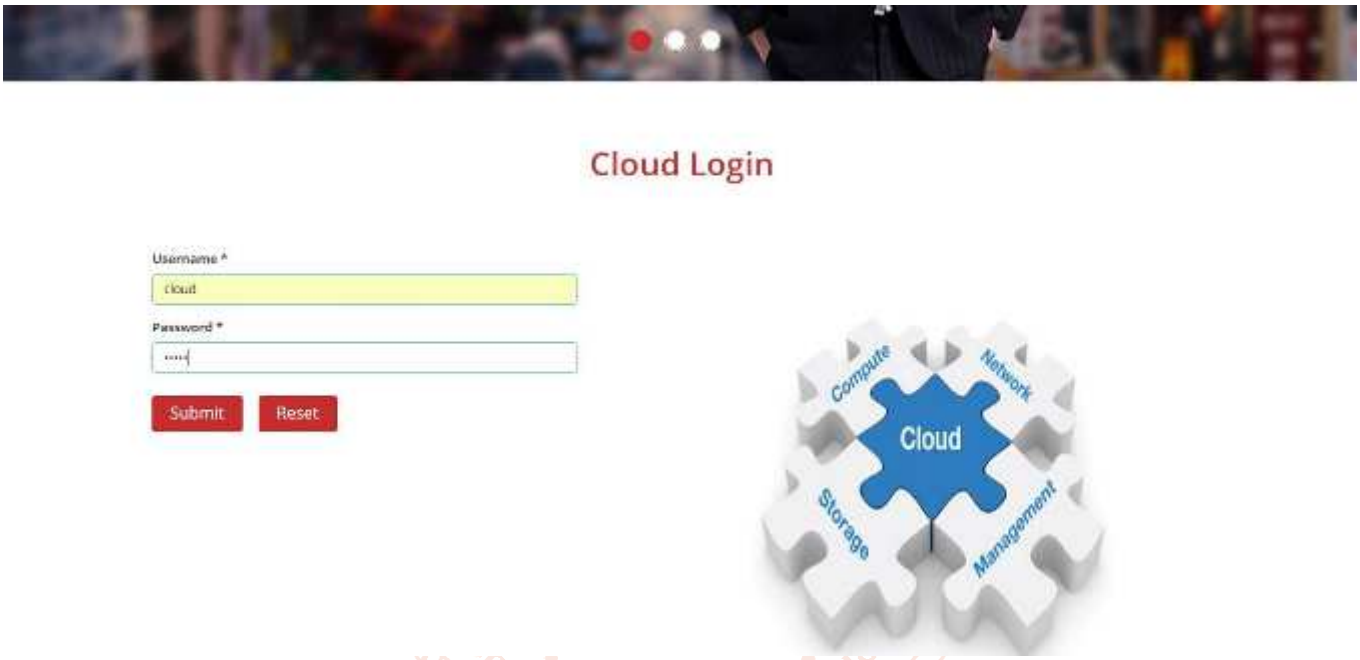


Figure 5.9 Cloud Login

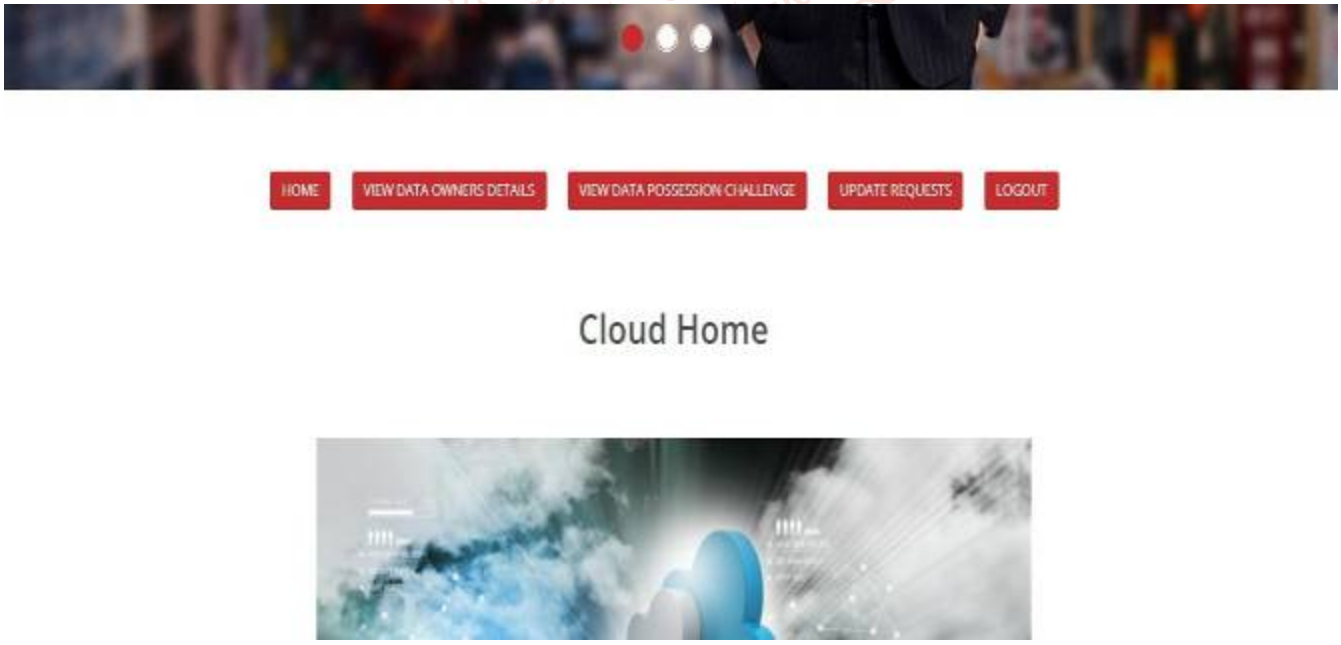


Figure 5.10 Cloud Home

Figure 5.11 Data Owner Details

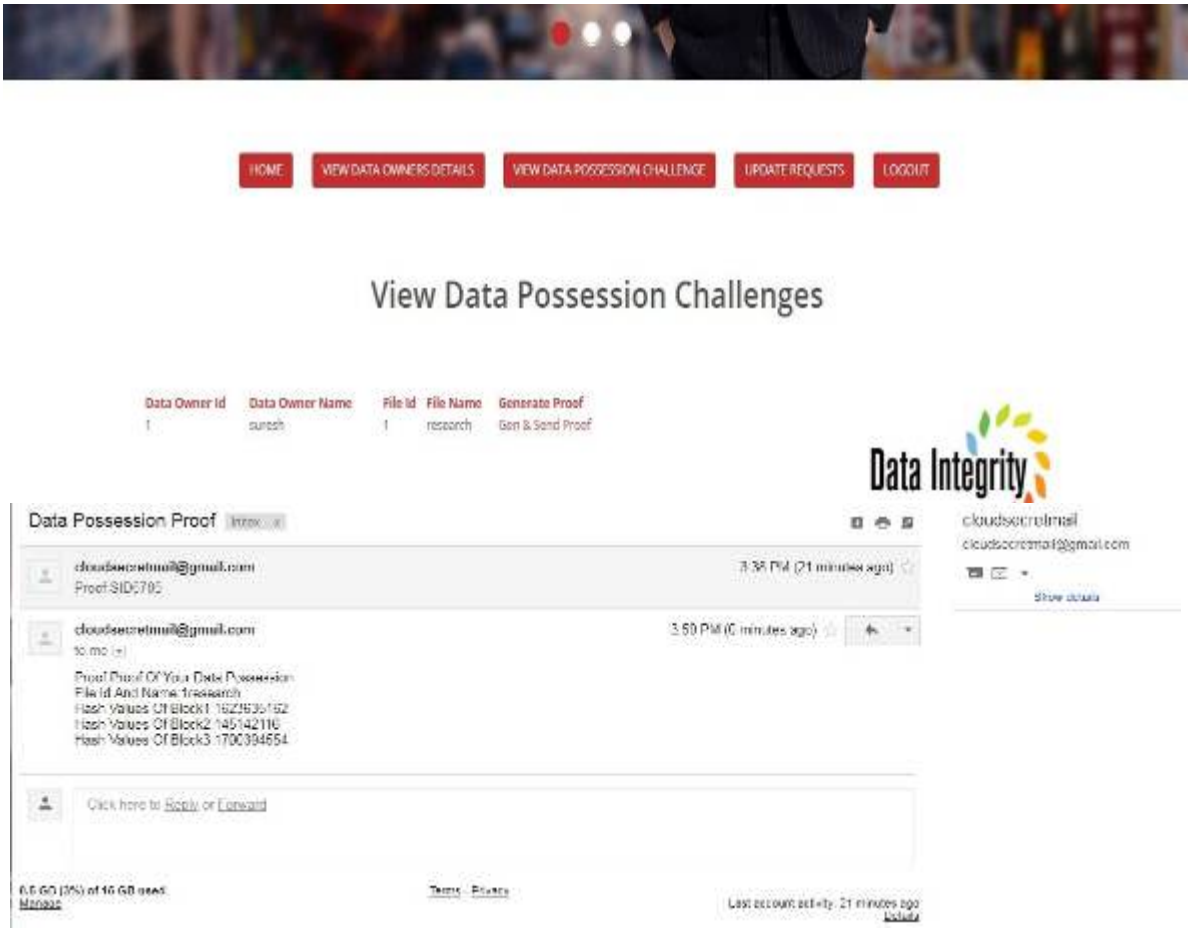


Figure 5.12 View Data Possession Challenges

Figure 5.13 Proof Verification

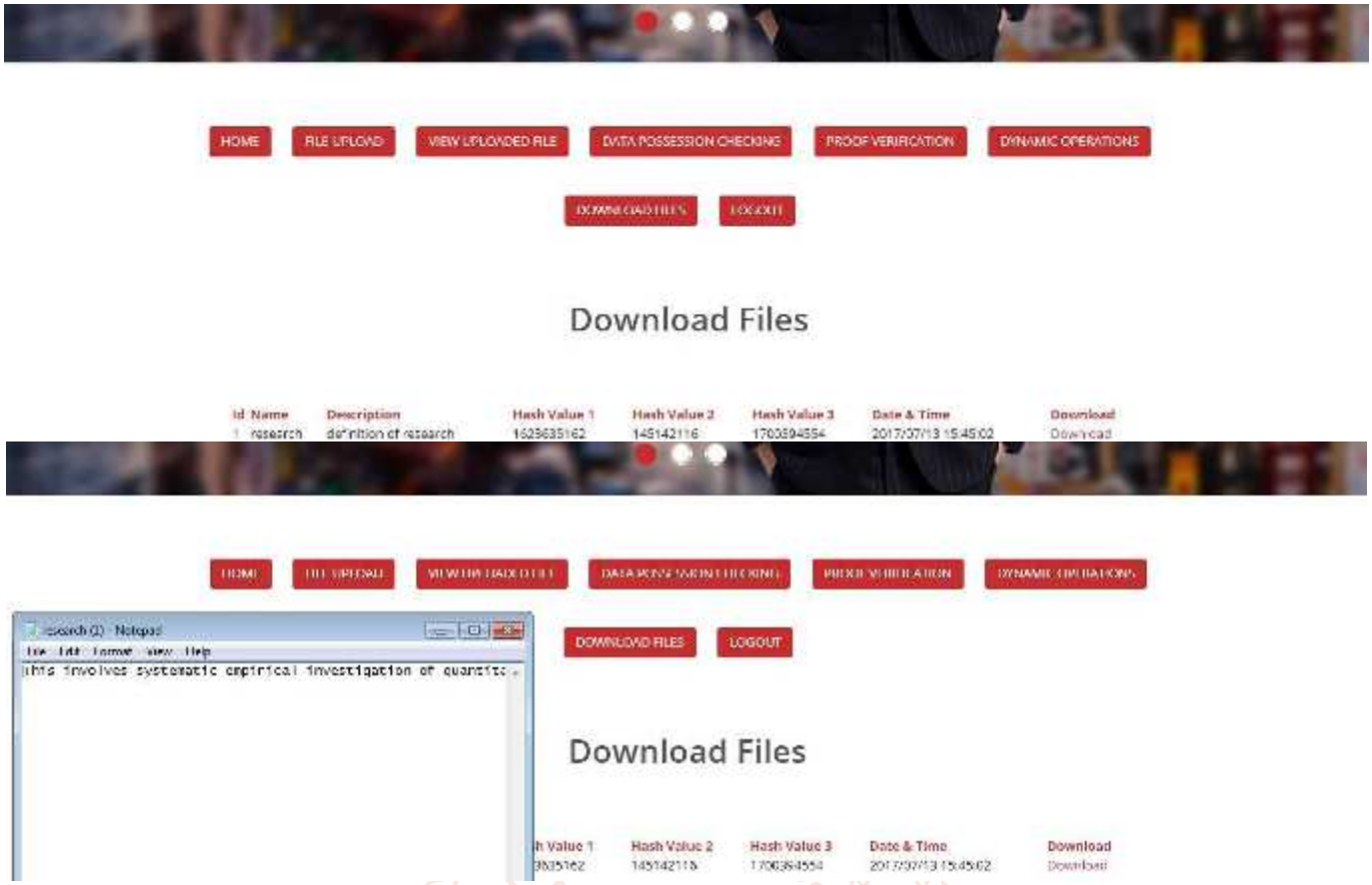


Figure 5.14 Download files

Figure 5.15 Dynamic Operations on Data

Figure 5.16 Insert data in the block

Figure 5.17 Data update request

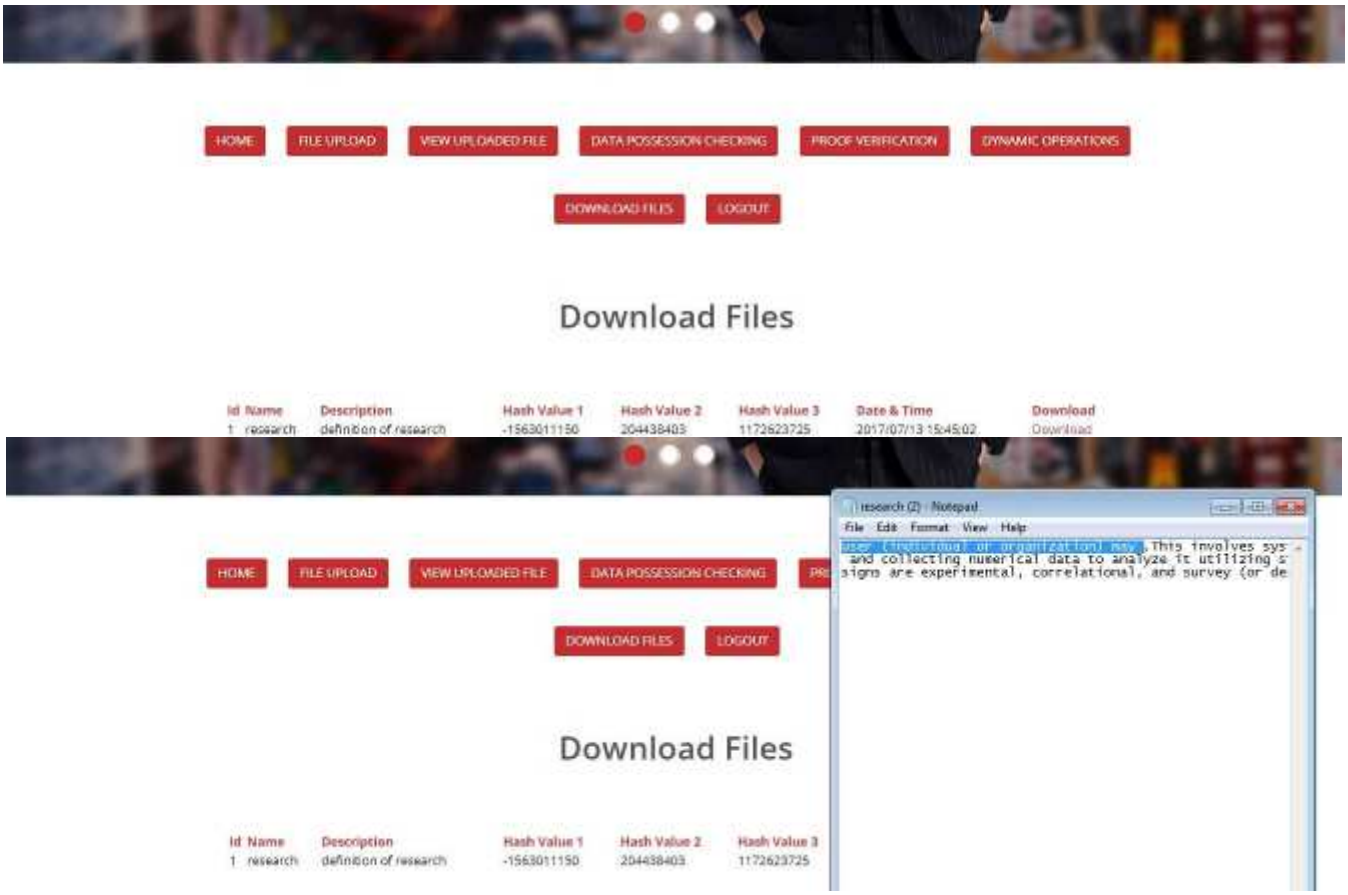


Figure 5.18 Download files

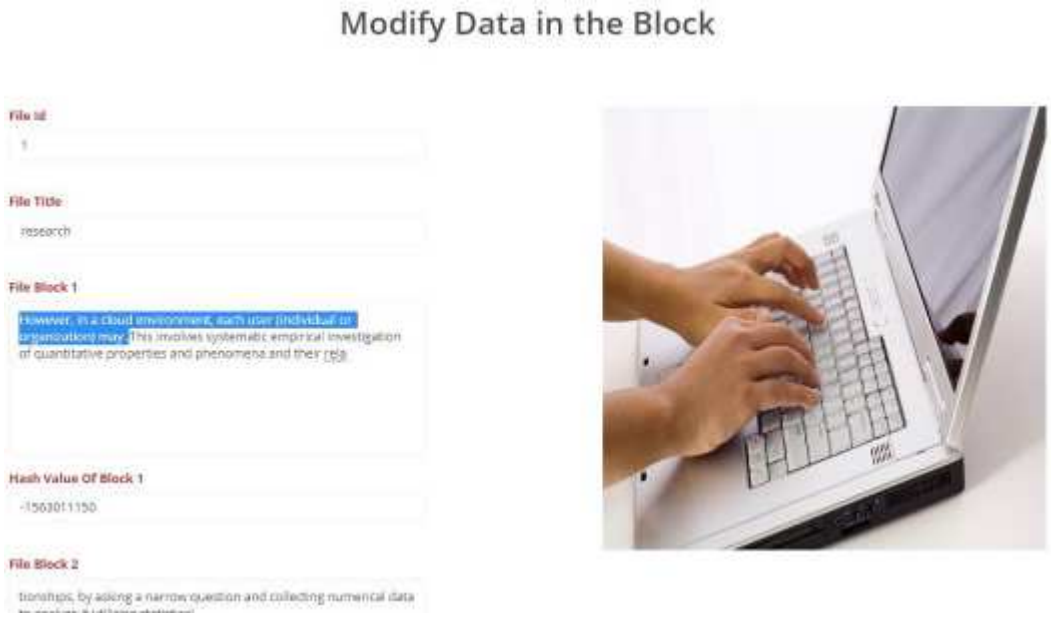


Figure 5.19 Modify Data in the block

Figure 5.20 Data update request

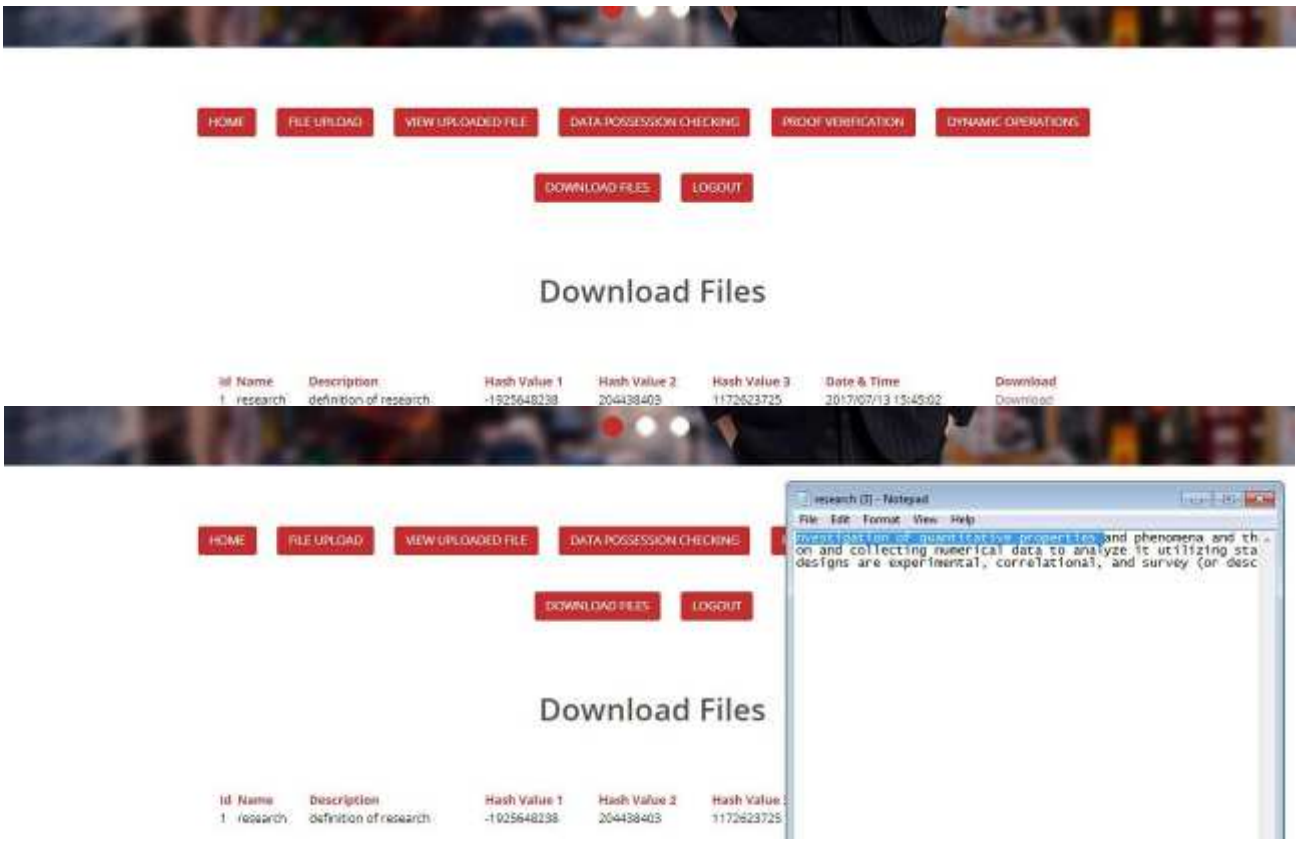


Figure 5.21 Download files

Figure 5.22 View uploaded files

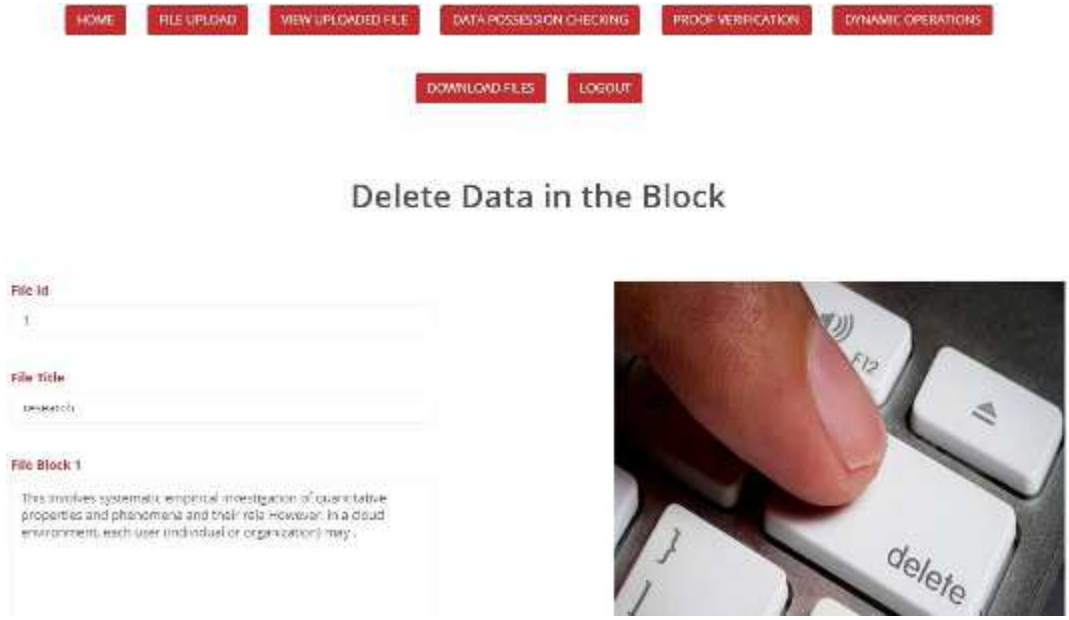


Figure 5.23 Delete data in the block

Figure 5.24 Data update request

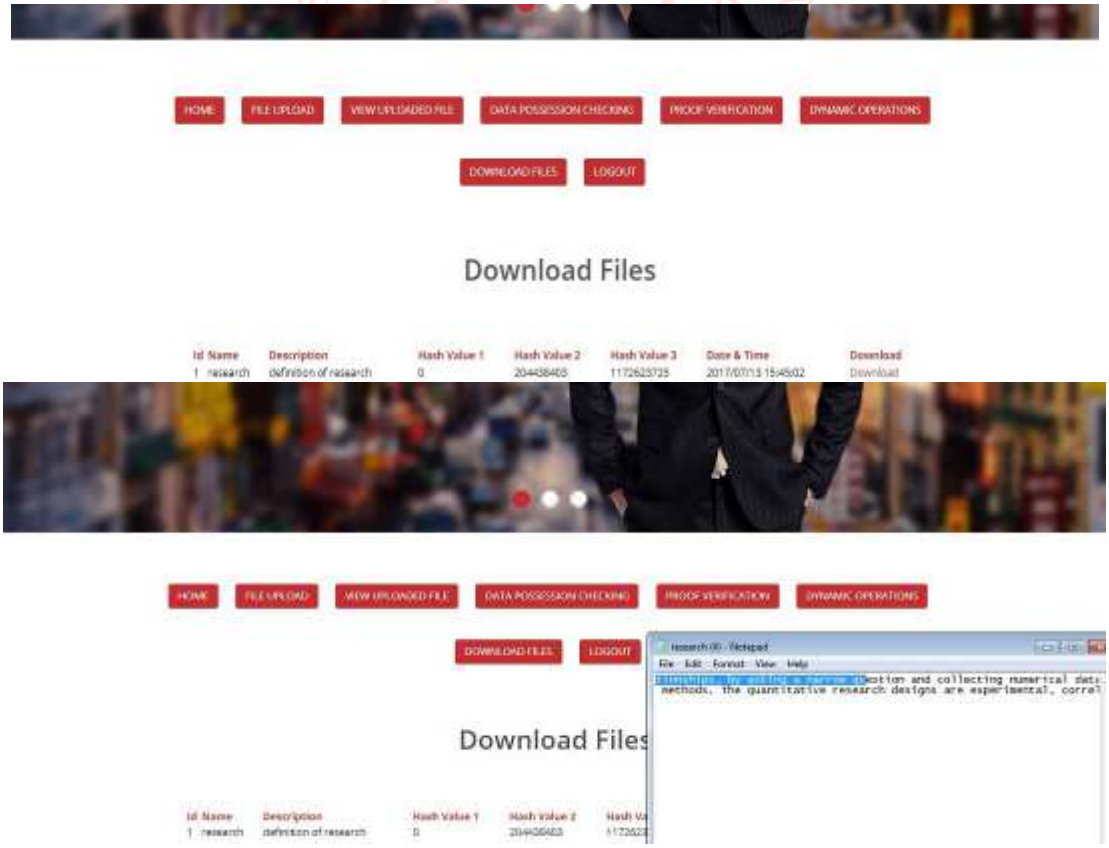


Figure 5.25 Download files

Fig 11.26 View uploaded files

6. Conclusion:

Files outsourced to remote server and propose an efficient secure RDPC protocol with data dynamic. Our scheme employs a homomorphic hash function to verify the integrity for the files stored on remote server, and reduces the storage costs and computation costs of the data owner. We design a new lightweight hybrid data structure to support dynamic operations on blocks which incurs minimum computation costs by decreasing the number of node shifting. Using our new data structure, the data owner can perform insert, modify or delete operation on file blocks with high efficiency. The presented scheme is proved secure in existing security model. We evaluate the performance in term of community cost, computation cost and storage cost. The experiments results indicate that our scheme is practical in cloud storage.

7. References:

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comp. Sy., vol. 25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute- based encryption with keyword search function for cloud storage," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016. 2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," Int. J.Commun. Syst., DOI: 10.1002/dac.2942.

[6] J. G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no.11, pp. 2150-2162, 2012