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

Double Server Public-Key Encryption with Keyword Search for Secure 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

Accessible encryption Technique is expanding the enthusiasm to ensure the information protection in secure accessible distributed storage. In this task, explore the security of a notable cryptographic crude, specifically, public key encryption with watchword search (PEKS) which is valuable in numerous utilizations of distributed storage. Tragically, it has been demonstrated that the customary PEKS structure experiences an intrinsic frailty called inside watchword speculating assault (KGA) dispatched by the malignant worker. To address this security weakness, we propose another PEKS structure named double worker PEKS (DS-PEKS). As another fundamental commitment, characterize another variation of the smooth projective hash capacities (SPHFs) alluded to as straight and homomorphic SPHF (LH-SPHF). at that point show a conventional development of secure DS-PEKS from LH-SPHF. To represent the plausibility of our new system, it give an effective launch of the overall structure from a Decision Diffie–Hellman-based LH-SPHF and show that it can accomplish the solid protection from inside the KGA.

KEYWORDS: *Encryption, DS-PEKS, LH-SPHF, Cryptographic Primitive*

How to cite this paper: A. Brahma Reddy | K. V. Ranga Rao | V. Vinay Kumar "Double Server Public-Key Encryption with Keyword Search for Secure Cloud Storage" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1560-1567, URL: www.ijtsrd.com/papers/ijtsrd35726.pdf

IJTSRD35726

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network 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.

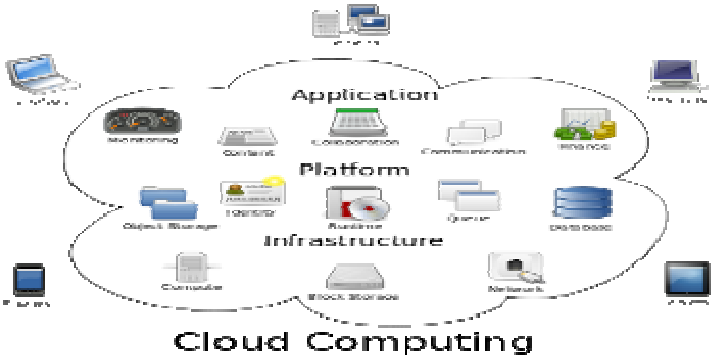

Fig 1: Structure of cloud computing

2. Existing System:

In A Peks System, Using The Receiver's Public Key, The Sender Attaches Some Encrypted Keywords) With The Encrypted Data. The Receiver Then Sends The Trapdoor Of A To-Be- Searched Keyword To The Server For Data Searching. Given The Trapdoor And The Peks Ciphertext, The Server Can Test Whether The Keyword Underlying The Peks Ciphertext Is Equal To The One Selected By The Receiver. If So, The Server Sends The Matching Encrypted Data To The Receiver. Baek Et Al. Proposed A Ew Peks Scheme Without Requiring A Secure Channel, Which Is Referred To As A Secure Channel-Free Peks (Scf-Peks). Rhee Et Al. Later Enhanced Baek Et Al.'S Security Model For Scf-Peks Where The Attacker Is Allowed To Obtain The Relationship Between The Non-Challenge Ciphertexts And The Trapdoor. Byun Et Al.

Introduced The Off-Line Keyword Guessing Attack Against Peks As Keywords Are Chosen From A Much Smaller Space Than Passwords And Users Usually Use Well-Known Keywords For Searching Documents. Despite Of Being Free From Secret Key Distribution, PEKS Schemes Suffer From An Inherent Insecurity Regarding The Trapdoor Keyword Privacy, Namely Inside Keyword Guessing Attack (KGA). The Reason Leading To Such A Security Vulnerability Is That Anyone Who Knows Receiver's Public Key Can Generate The PEKS Ciphertext Of Arbitrary Keyword Himself. Specifically, Given A Trapdoor, The Adversarial Server Can Choose A Guessing Keyword From The Keyword Space And Then Use The Keyword To Generate A PEKS Ciphertext. On One Hand, Although The Server Cannot Exactly Guess The Keyword, It Is Still Able To Know Which Small Set The Underlying Keyword Belongs To And Thus The Keyword Privacy Is Not Well Preserved From The Server. On The Other Hand, Their Scheme Is Impractical As The Receiver Has To Locally Find The Matching Ciphertext By Using The Exact Trapdoor To Filter Out The Non-Matching Ones From The Set Returned From The Server.

3. Proposed System:

The contributions of this project are four-fold. formalize a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to address the security vulnerability of PEKS.A new variant of Smooth Projective Hash Function (SPHF), referred to as linear and homomorphic *SPHF*, is introduced for a generic construction of DS-PEKS. show a generic construction of DS-PEKS using the proposed Lin-Hom SPHF. To illustrate the feasibility of our new framework, an efficient instantiation of our SPHF based on the Diffie- Hellman language is presented in this paper. All the existing schemes require the pairing computation during the generation of PEKS ciphertext and testing and hence are less efficient than our scheme, which does not need any pairing computation. Our scheme is the most efficient in terms of PEKS computation. It is because that our scheme does not include pairing computation. Particularly, the existing scheme requires the most computation cost due to 2 pairing computation per PEKS generation. In our paper it requires another stage for the testing, our computation cost is actually lower than that of any existing scheme as we do not require any pairing computation and all the searching work is handled by the server.

4. System Architecture:

Figure 2: system architecture

Data Owner: Register with cloud server and login (username must be unique). Send request to Public key generator (PKG) to generate Key on the user name. Browse file and request Public key to encrypt the data, Upload data to cloud service provider. Verify the data from the cloud. Public Key Generator: Receive request from the users to generate the key, Store all keys based on the user names. Check the username and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revoke the user after updating the private key for the corresponding file based on the user). Key Update: Receive all files from the data owner and store all files. Check the data integrity in the cloud and inform to end user about the data integrity. Send request to PKG to update the private key of the user based on the date parameter.

5. RESULTS:

Figure3: home page

Figure 4: User Registration

Figure 5: User login

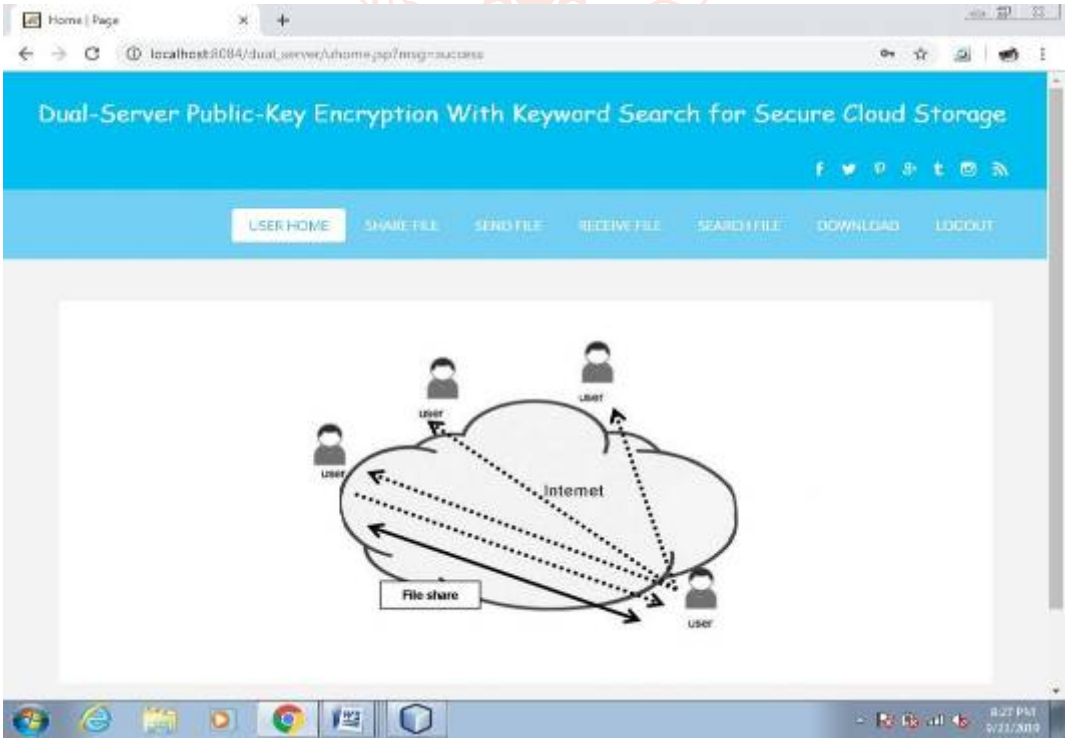

Figure 6: User Home

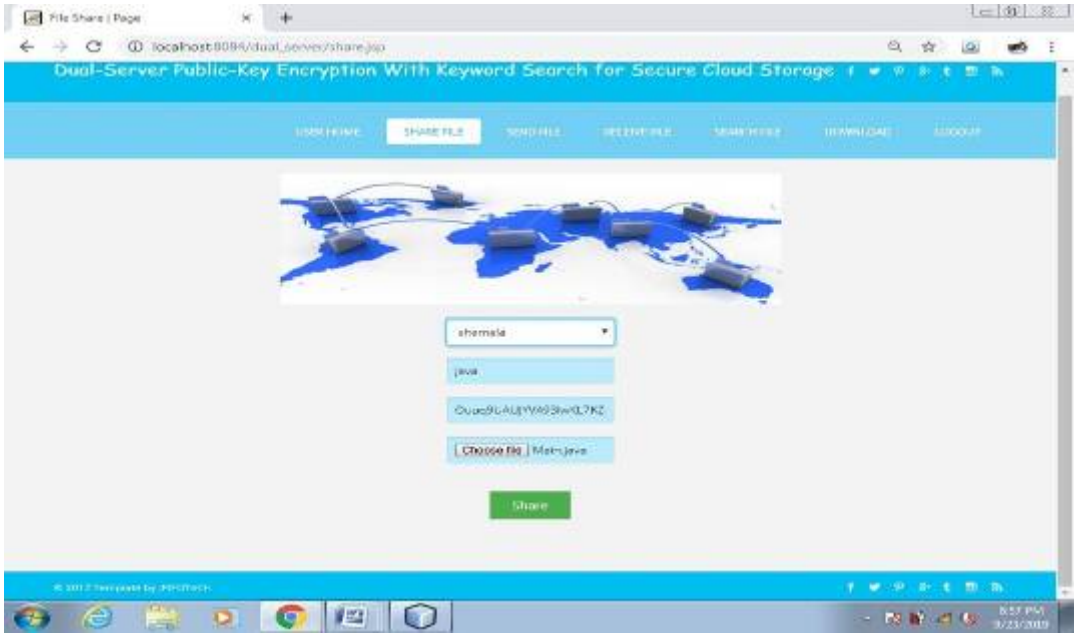

Figure 7: share file

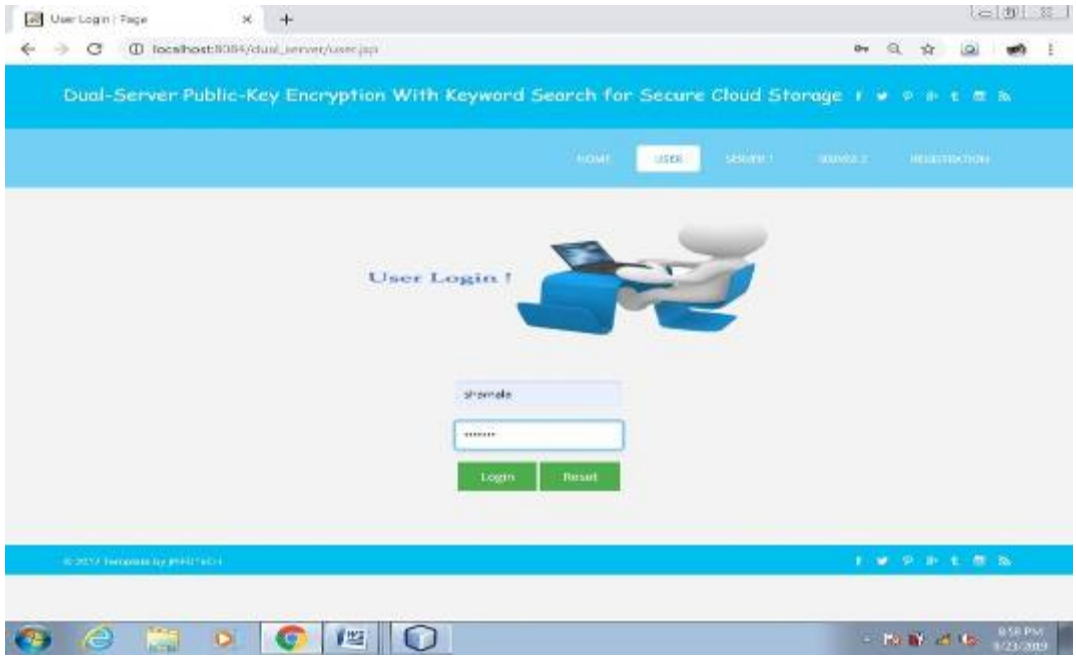

Figure 8: receiver login:

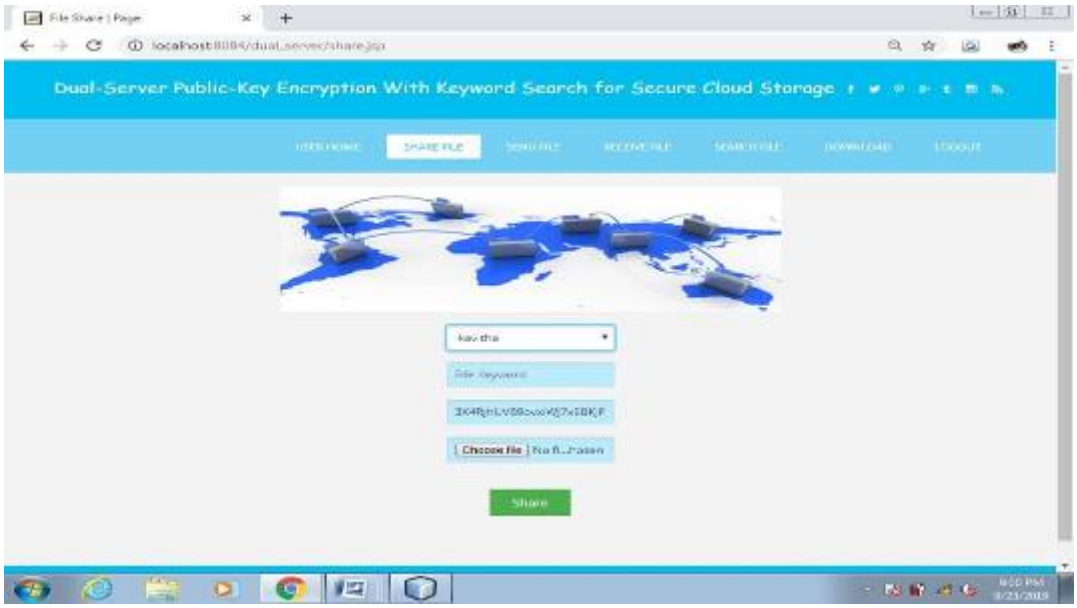

Figure9: Receiver share file

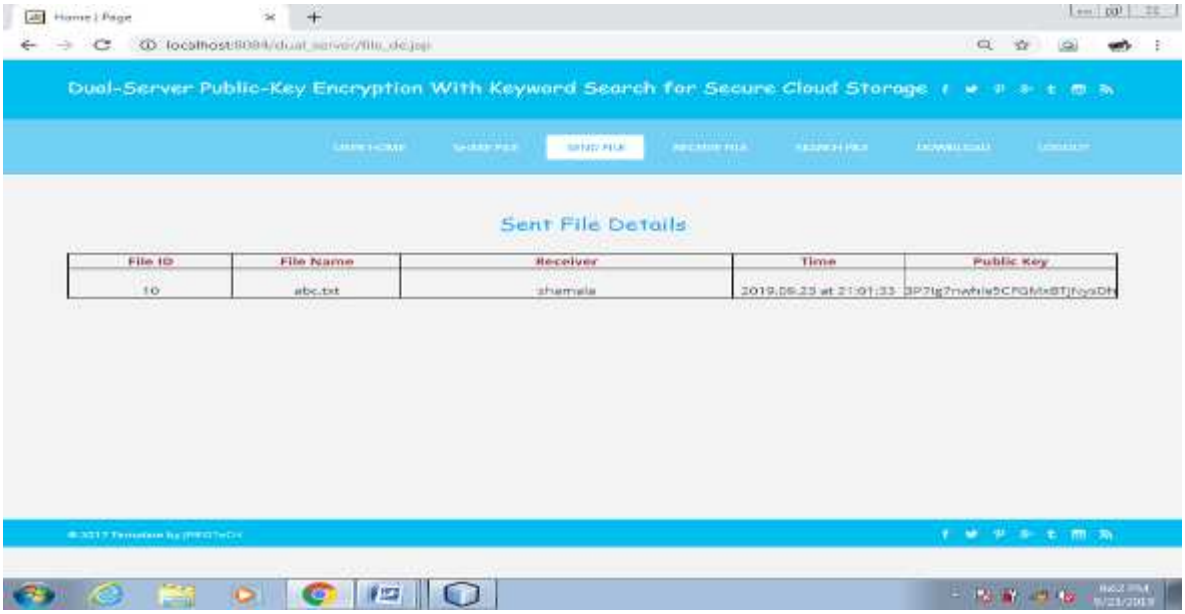

Figure 10: Receiver File Details

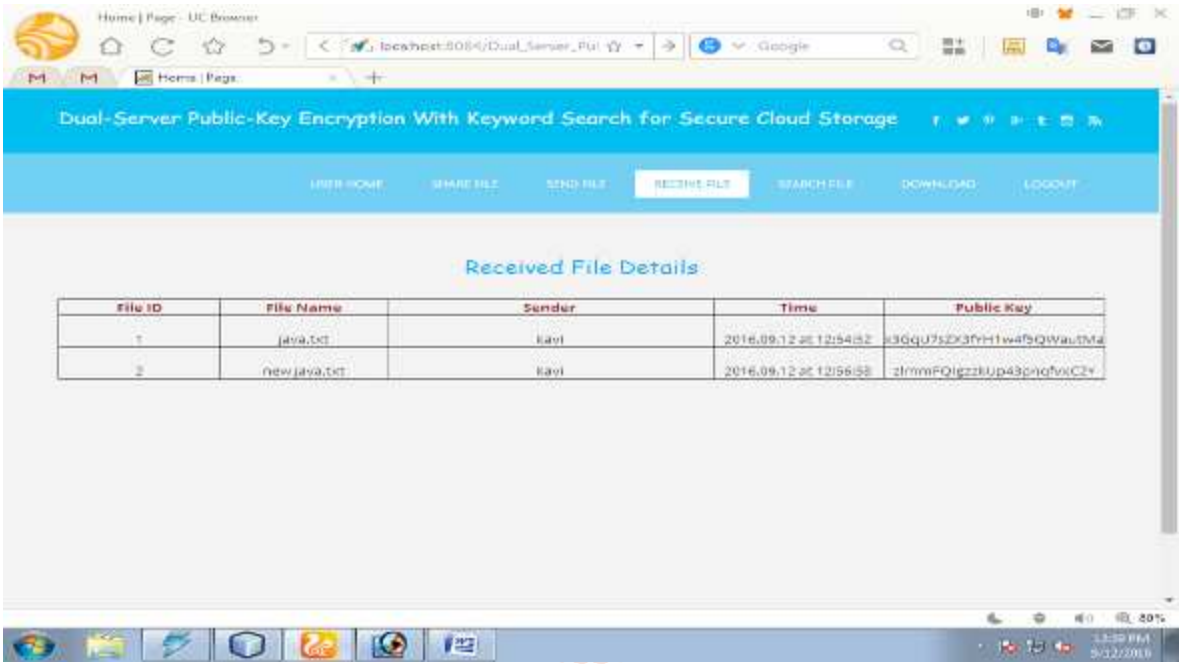

Figure 11: Received files

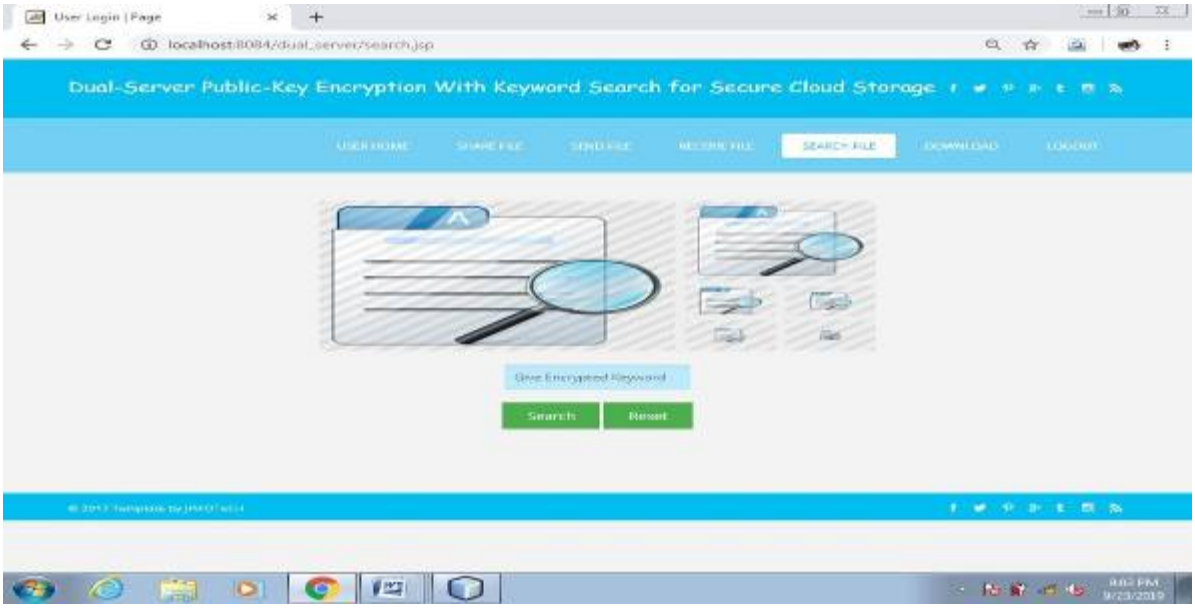

Figure 12: searching File

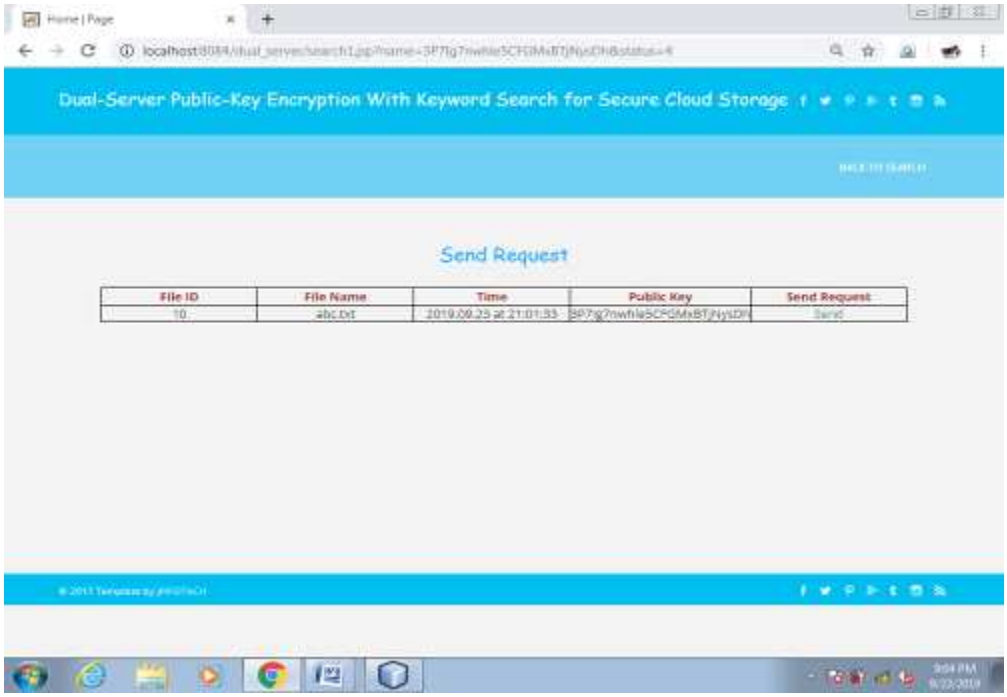

Figure13: send request

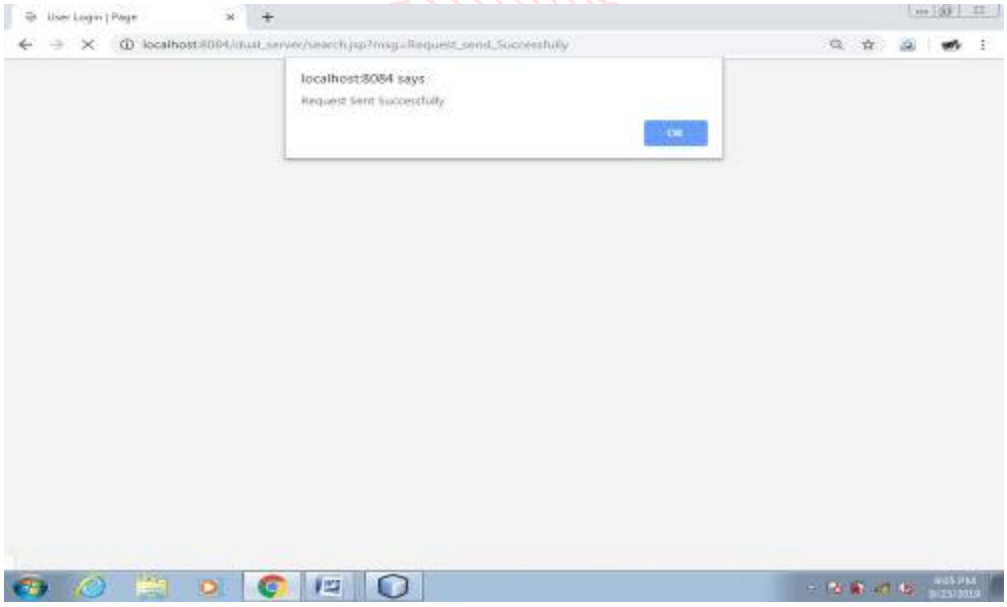

Figure 14: request successful

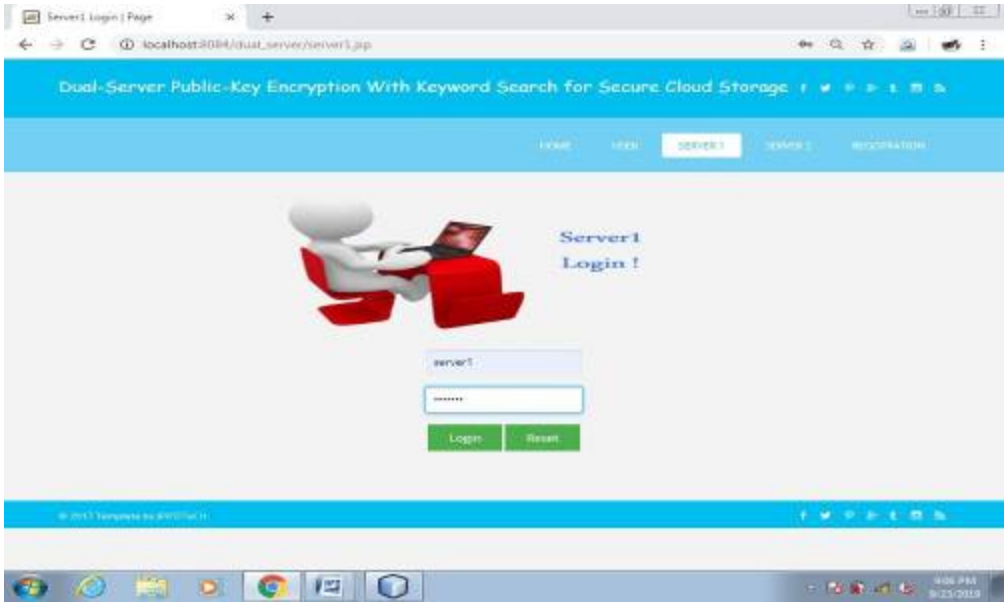

Figure 13: Server login

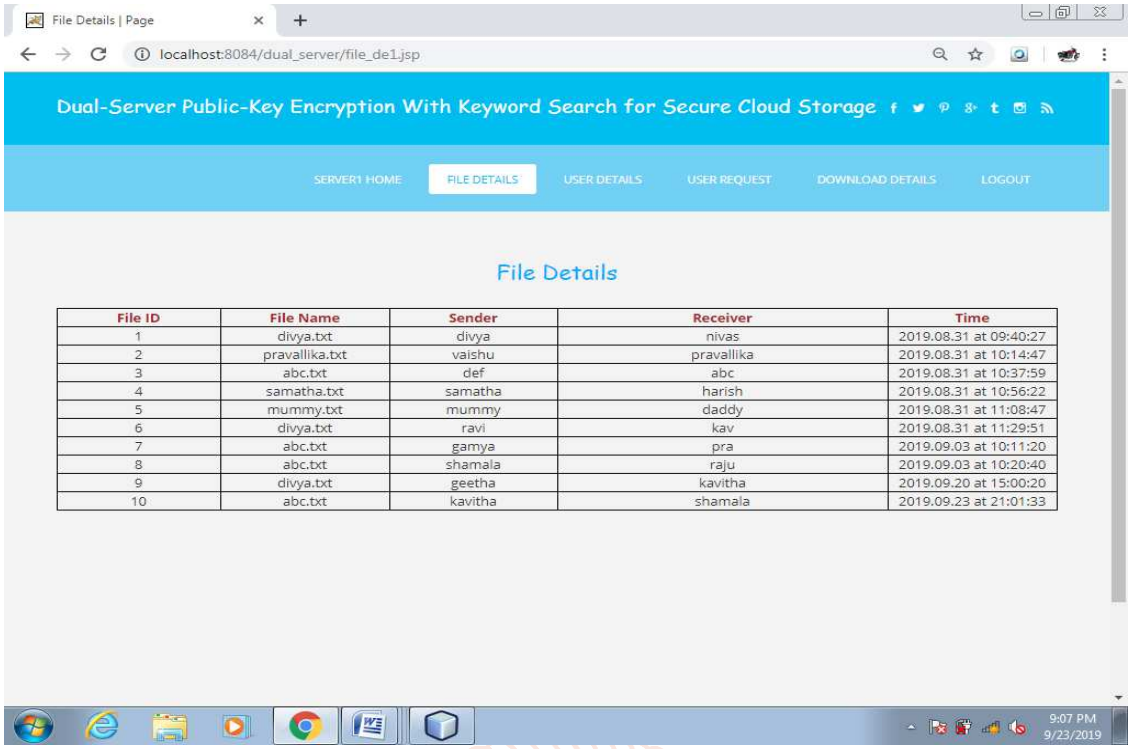

Figure 16: file details

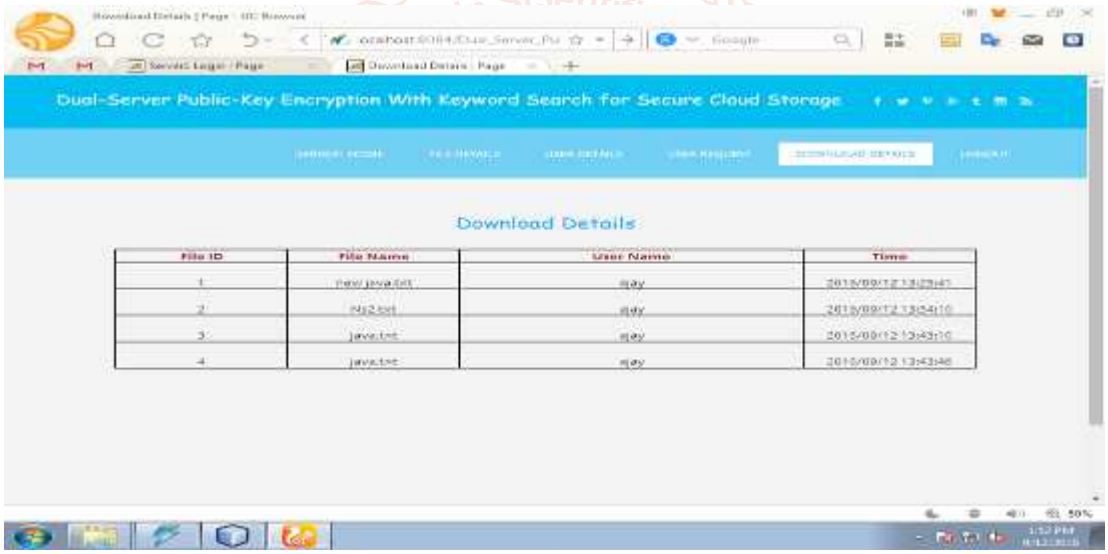

Figure 17: Download details

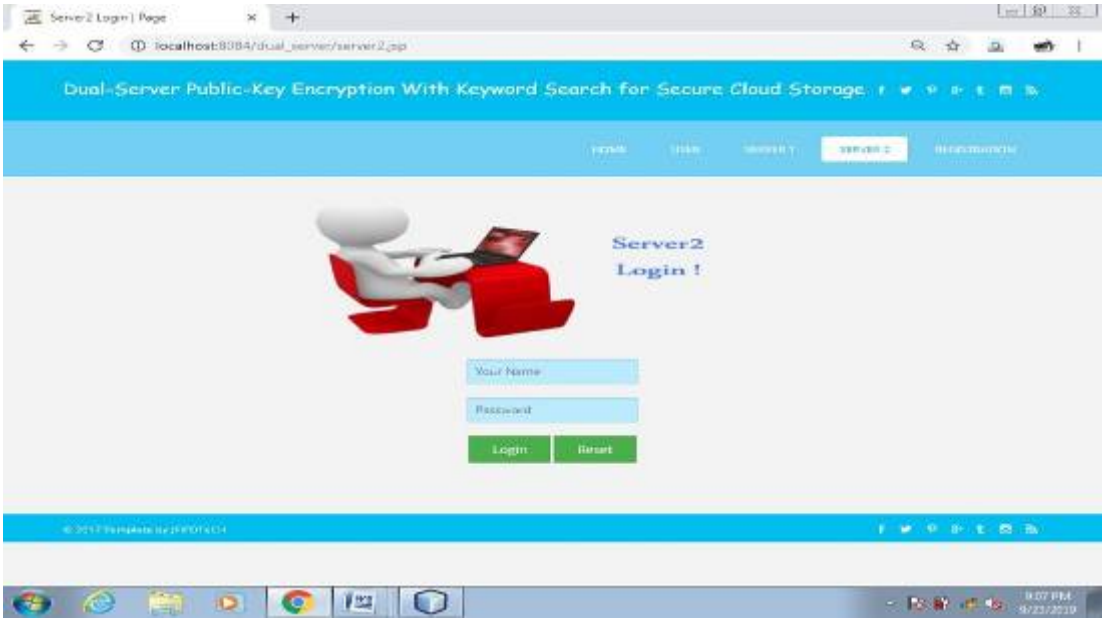

Figure 18: server2 login

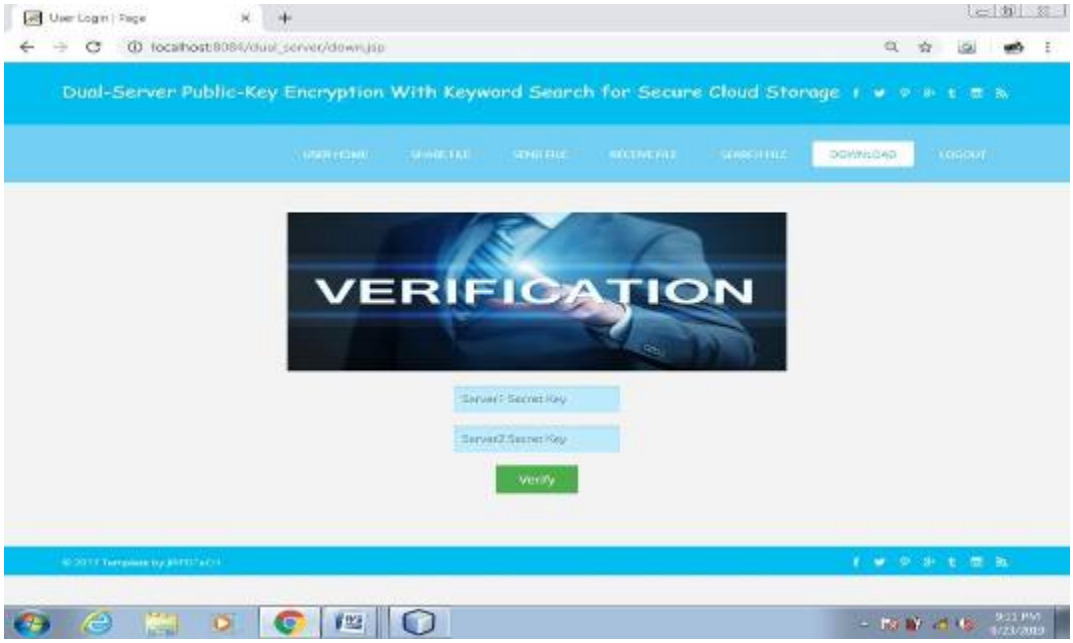

Figure 19: Verification

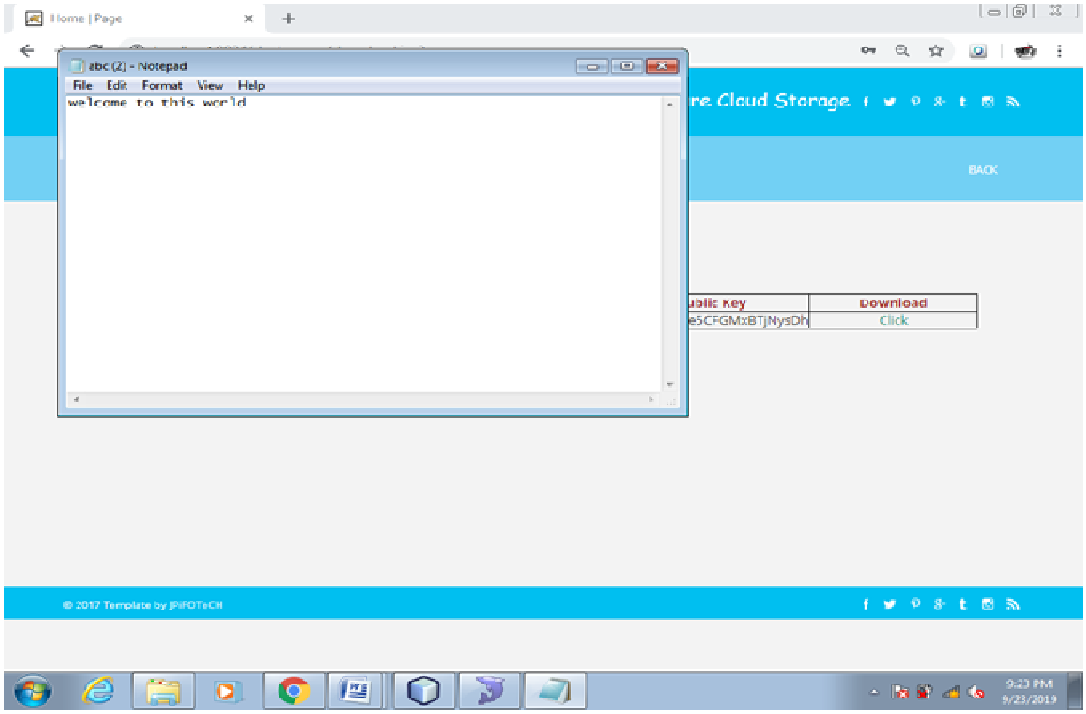

Figure 20: File upload

6. Conclusion:

In this paper, we proposed a new framework, named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS), that can prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DS-PEKS scheme. An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also identified and solved. In the project, which gives secure data from efficient DS-PEKS scheme with dynamic pairings.

7. References:

[1] Josef pieprzyk, Suriadi "A Dual Server for public key encryption with keyword search," in Proc. 20th Australasian Conf. Inf. Secur. Privacy 2017, pp. 59–76.

[2] J. W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in Proc. 3rd VLDB Workshop Secure Data Manage. (SDM), 2017, pp. 75–83.

[3] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015, pp. 59–76.

[4] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44– 55.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006, pp. 79–88.