IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

Secure Cloud Search Using Dual Server with Key Encryption

Prof. K S Raghu Kumar[1], Ankith Gowda M[2], Aswin B Prasad[3], Anish A[4], Amruth Kaginakar[5]

Associate Professor, Department of CSE, Don Bosco Institute of Technology, Bangalore, Karnataka, India[1]

U.G. Student, Department of CSE, Don Bosco Institute of Technology, Bangalore, Karnataka, India[2,3,4,5]

ABSTRACT: The efficient, secure search of data in cloud is a difficult issue. Searchable encryption preserves data security and usability while offering a safe way to store data. Scholars have extensively examined key encryption with keyword search, a significant subfield of encryption. Nevertheless, keyword guessers can compromise the majority of conventional PEKS methods. It is anticipated that the ability to withstand keyword guessers will become a crucial feature. IKGA mitigation has long proven ineffective and challenging, and the majority of PEKS methods now in use fall short of security objectives. In response to the aforementioned issues, we provide the concept Secure Cloud Search Using Dual Server with Key Encryption, which enables the authentication and guards by utilizing two uncooperative servers. Next, we give a construction that doesn't involve bilinear pairings. Our system is suited for implementation in real-world applications because to its excellent security and great efficiency.

KEYWORDS: dual servers, authorization, inside keyword guessing attacks, key encryption with keyword search, servers, cloud computing, encryption, and cloud storage.

I. INTRODUCTION

The exponential rise of data has made cloud storage a promising in addition to offering consumers on-demand storage, it makes accessing data easier for users. Sensitive information, such as financial and health records for the organization, may be included in data that is out sourced to servers, raising protection concerns. One common strategy is to decode the data sending it to before the cloud in action to preserve data secrecy. However, the use of decoded data is more challenging, especially when it comes to data retrieval. Songe et al. the first one to introduce the idea of searchable data, on the symetric crypto-system, to achieve searchable feature of decoded data.

The three entities that comprise the framework are the user, the data receivers, and the cloud. Using the public key of the data receiver, the user encrypts the data and each keyword that is extracted from them. The ciphertext is then uploaded to the server. With the keyword or keywords they want to search, the user sends a request to the cloud server. The cloud server checks to see if the keyword corresponding to the trapdoor and the keyword underlying the ciphertext are the same. The decrypted data corresponding to the trapdoor is returned by the server. Regretfully, even with all of their advantages, Boneh's framework-based techniques are largely ineffective against internal keyword guessers. The malicious cloud server typically launches it, and it may divulge personal information about the recipient, such as identification or interests. The ability of the malicious cloud server to access the trapdoor, create ciphertext for any keyword, and repeatedly run the test method makes it feasible. Another aspect is that real-world applications usually contain a small key word. So, the adversary might continue following the preceding stages until he finds the correct keyword. Searchable encryption requires a great deal of security design.

II. RELATED WORK

The topic of the works is how to strengthen the scheme's defenses against keyword guessers assaults. We have just examined one aspect of searchable encryption—public-key with keywords search—in order to keep things simple. 4 polynomial time randomised algorithm make up the first key encryption with keywords search method, which was proposed by Boneh et al. user can search ciphertext in an asymmetric encryption context thanks to their scheme.

The method eliminatee the need for a secured channel by incorporating a key-pair for the server. Next, the SCF-PEKS security model was improved by Rahee et al. and Emmura et al., in different ways. Furthermore, because the keyword is usually not big in practical application, Byunn et al. found that traditional PEKs may be vullnerable to the keyword guesser attack, which can reveal the keyword of a trapdoor by receiver.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

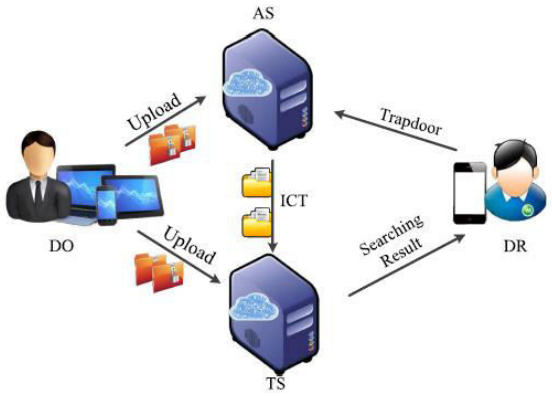
|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

The term "trapdoor indistinguishability" was coined by Rhee et al. to ensure data privacy; this means that two trapdoors would be unique from each other even if they shared a keyword. Fang et al. established two important security concepts, but more study that strategy is ineffective in achieving its security goal. The strategy suggested by Guu o et al. features less computing overhead and a shorter cipher text length than the method of. To protect trapdoor privacy, it additionally employs identity based encryption key unlinkability. Jeonng et al. observed that it is very difficult to construct secure PEKs scheme that can withstand within the original framework, and that the previously described methods are vulnerable to the inside Guessers. Xuv et al. proposed the idea key encryption with fuzzy keywords in order to overcome the aforementioned problems. Since numerous keywords may share the same fuzzy trapdoor, the vicious server is unable to determine the precise keyword through it. Additionally, Hang et al. suggested an effective. To stop the inside hostile server from figuring out the keywords in the scheme, the owner is provided key-pair. However, the created trapdoor will remain the same if keywords is left unchanged. Accordingly, the vicios cloud server would be aware of the statistics pertaining to the trapdoor would be able to identify the keywords associated with them. Furthermore, Chen et al.'s techniques employ two cloud servers—one of which have no link with the other—to prevent IKGA. Unfortunately, the fundamental reason why the works are unsafe schemes lack the authentication attribute, which allows the adversary to create a legitimate trapdoor using a keyword which search for decoded data. Nevertheless, in order assist customers in generating the pre-processed keyword, the task necessitates a reliable third party. Additionally, a novel PEKS strategy is suggested in effort to use the permission tokens to thwart the KGA. However, the it calls for more communication over the consumer and the owner.

Furthermore, in contrast to symmetric searchable encryption (SSE), the majority of PEKS schemes necessitate certain computation-intensive processes (such as bilinear pairing and map-to-point hashing), which in real-world applications will represent a significant performance constraint. The work developed a quadratic residues based IBE method (PEKS scheme) to lower the computational cost without requiring the bilinear pairing operation; however, the protocol remains unfeasible. Xu et al. recently used a hidden structure to reduce the amount of computation-intensive processes in the construction of a lightweight searchable public-key encryption. As a result, introducing any new PEKS schemes should be avoided.

III. METHODOLOGY



Defense against inside keyword guessing attacks and efficiency improvement in PEKS schemes. It focuses on public-key encryption with keyword search. The initial PEKS scheme enabled data users to search ciphertext data in asymmetric encryption settings, garnering attention from researchers. Subsequent developments, including SCF-PEKS and its security model enhancements by different teams, eliminated the need for secure channels, advancing the field of searchable encryption.

Encryption: The data owner, who wants to store data in the cloud, first encrypts the data using symmetric key encryption algorithm.

Keyword Trapdoor Generation: When a user wants to search for data containing specific keywords, they generate a keyword trapdoor using their private key and the keyword itself.

Keyword Search: The user transmits the obtained search token to the data storage server. Then data storage server uses the search token and the public key to verify its validity. If valid, it searches the stored encrypted data for entries that match the information embedded within the token.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

Data Retrieval: If the search on the data storage server yields a match, it retrieves the corresponding encrypted data containing the relevant keyword. The user utilizes their private key to decrypt the retrieved data, obtaining the originally encrypted symmetric key.

IV. EXPERIMENTAL RESULTS

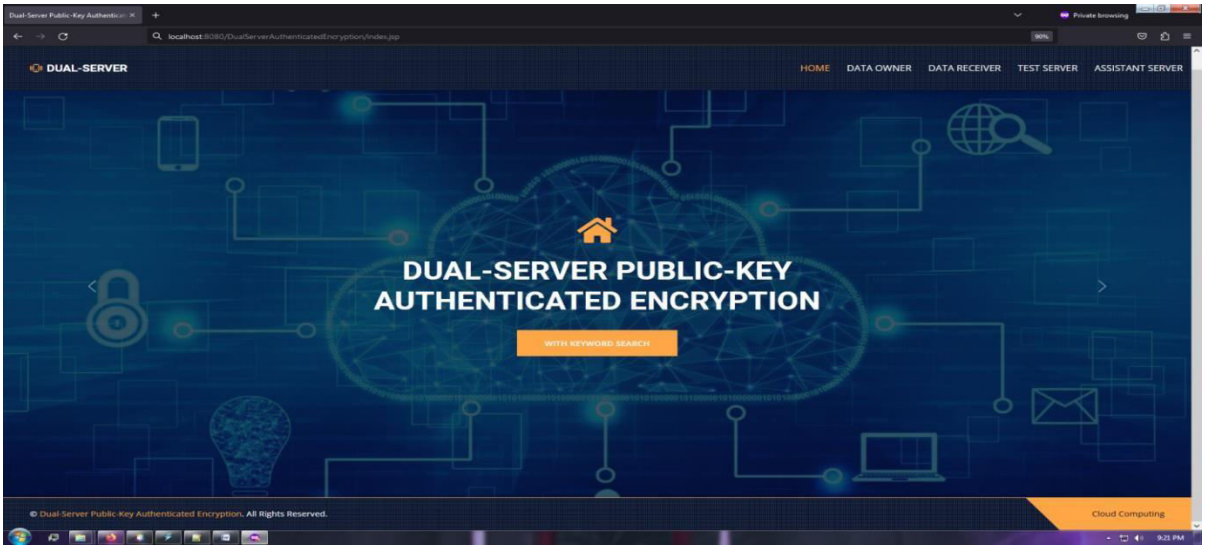


FIG 1 : HOME PAGE

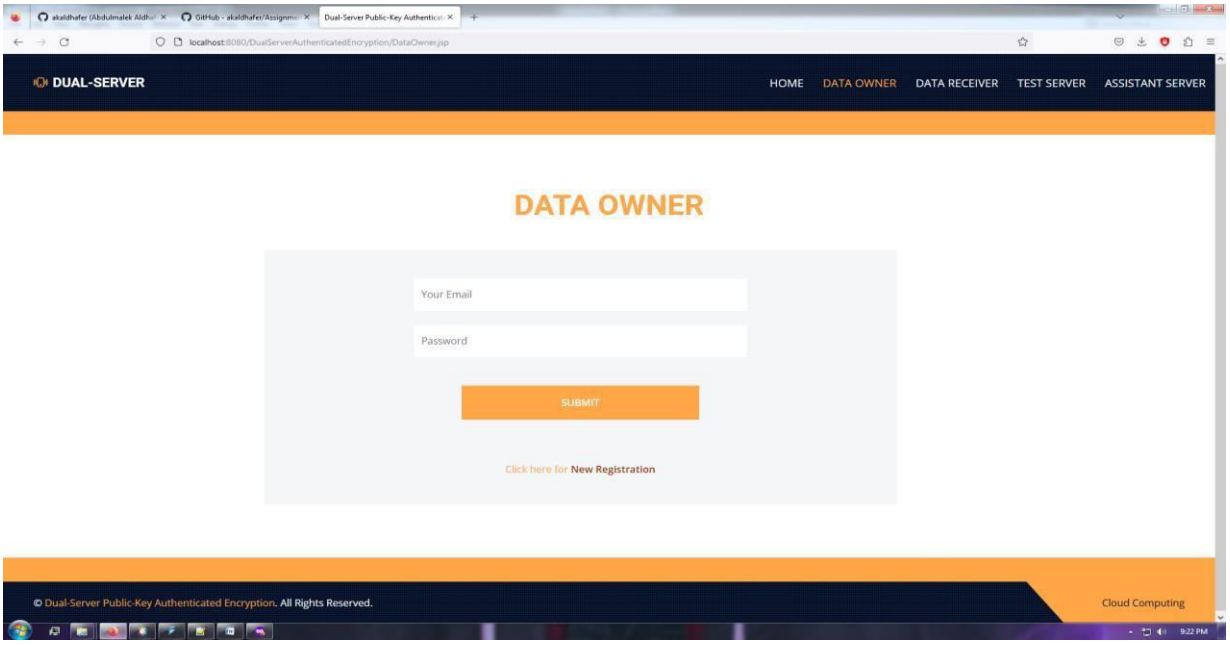


FIG 2 : DATA OWNER

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

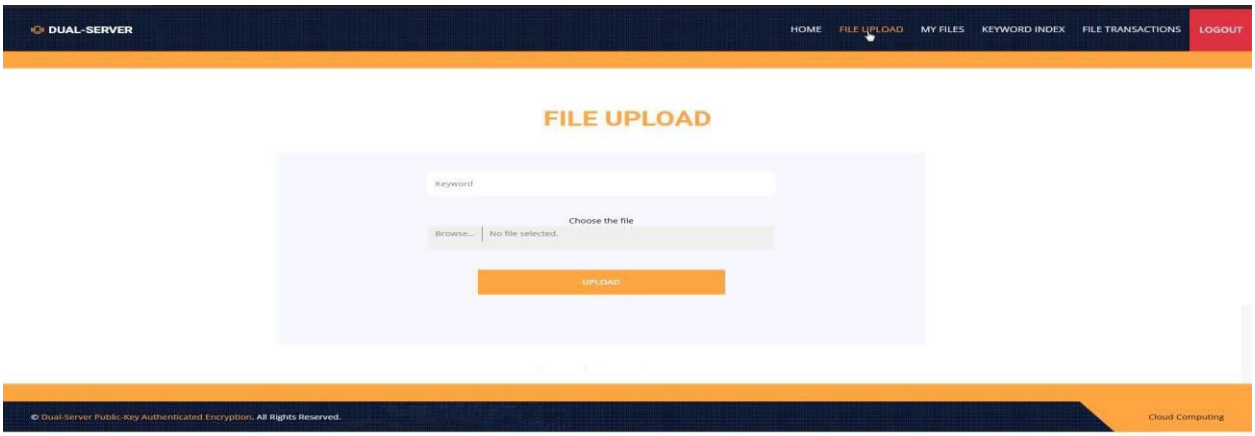


FIG 6.4 : FILE UPLOAD

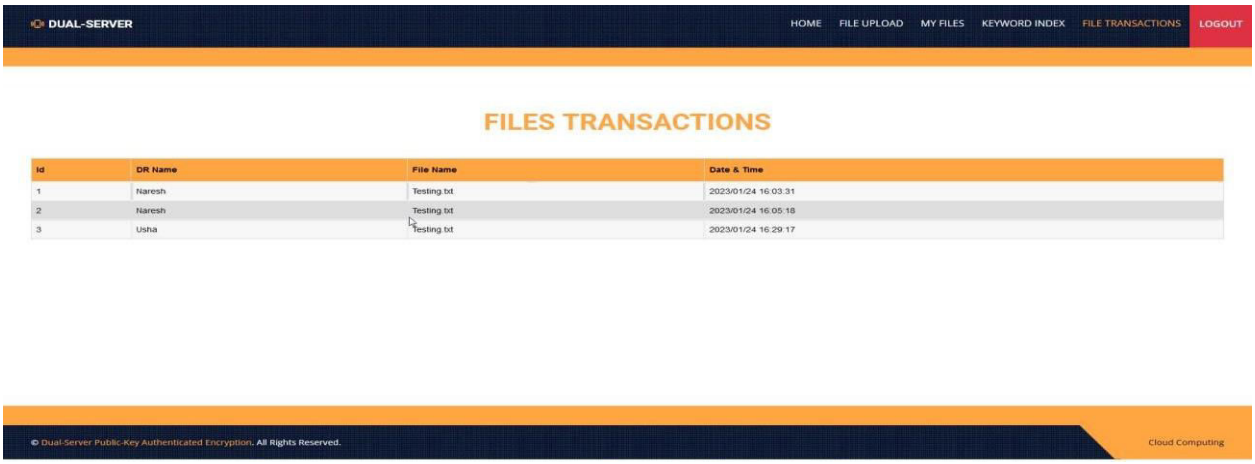


FIG 6.5 FILE TRANSACTIONS

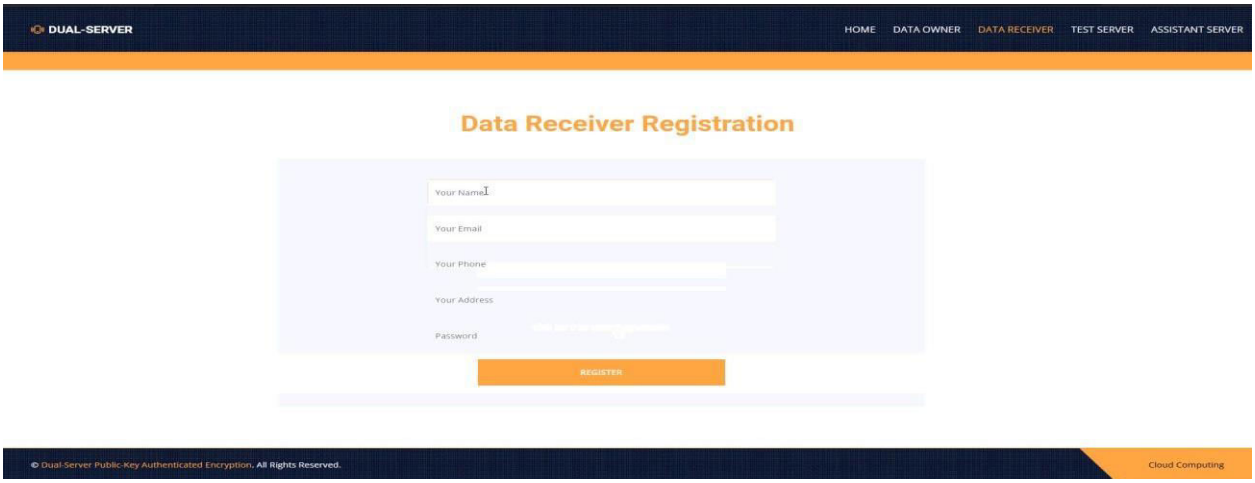


FIG 6.6 : DATA RECEIVER REGESTRATION

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

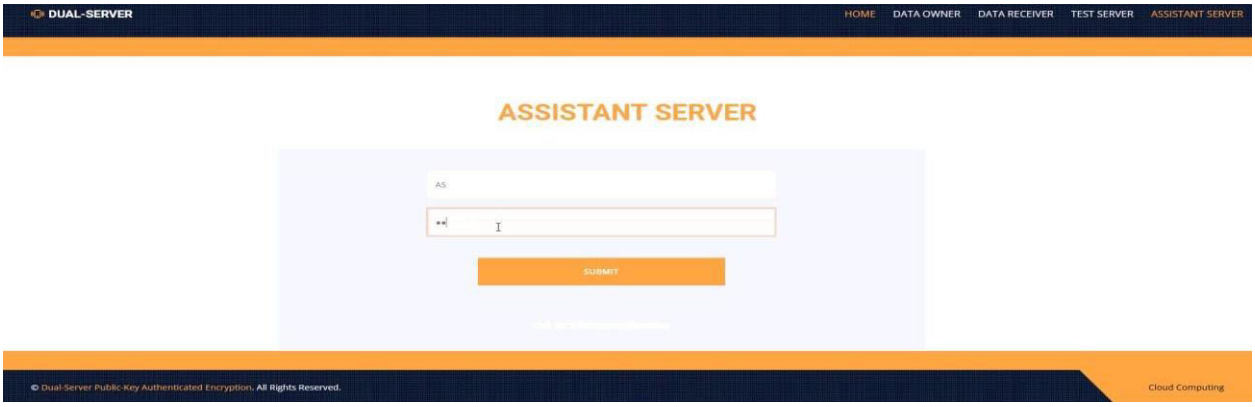


FIG 6.7 : ASSISTANT SERVER

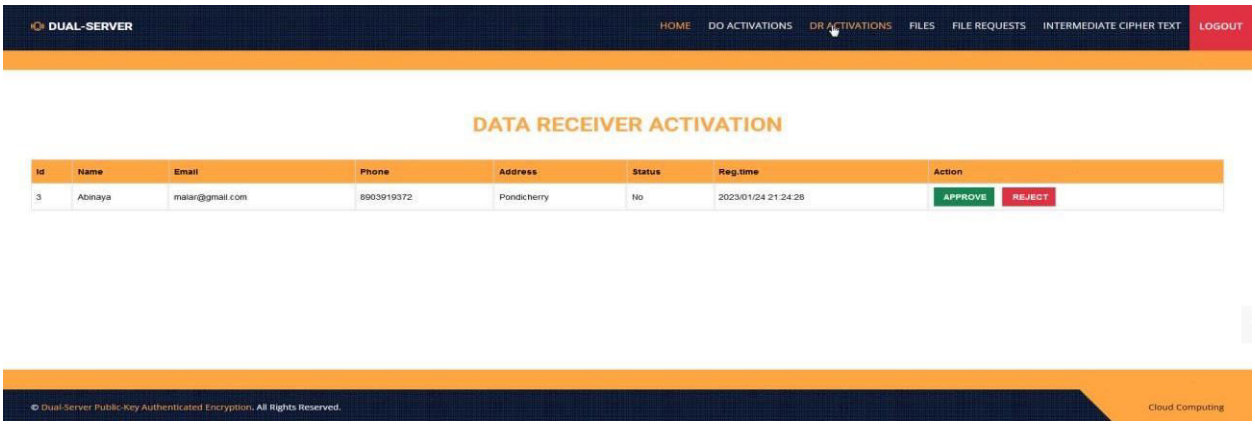


FIG 6.8: DATA RECIVER ACTIVATION

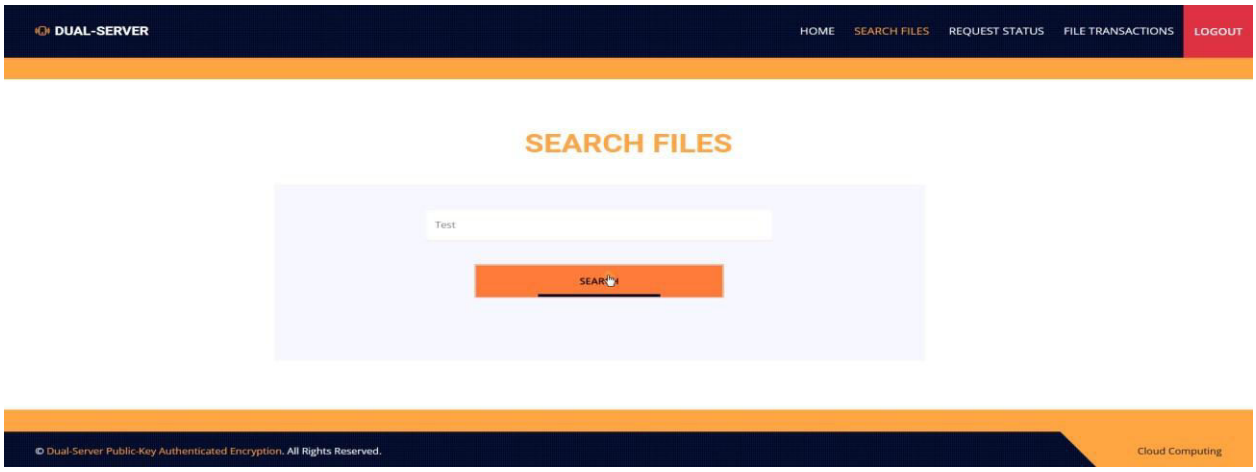


FIG 6.9 : SEARCH FILES

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

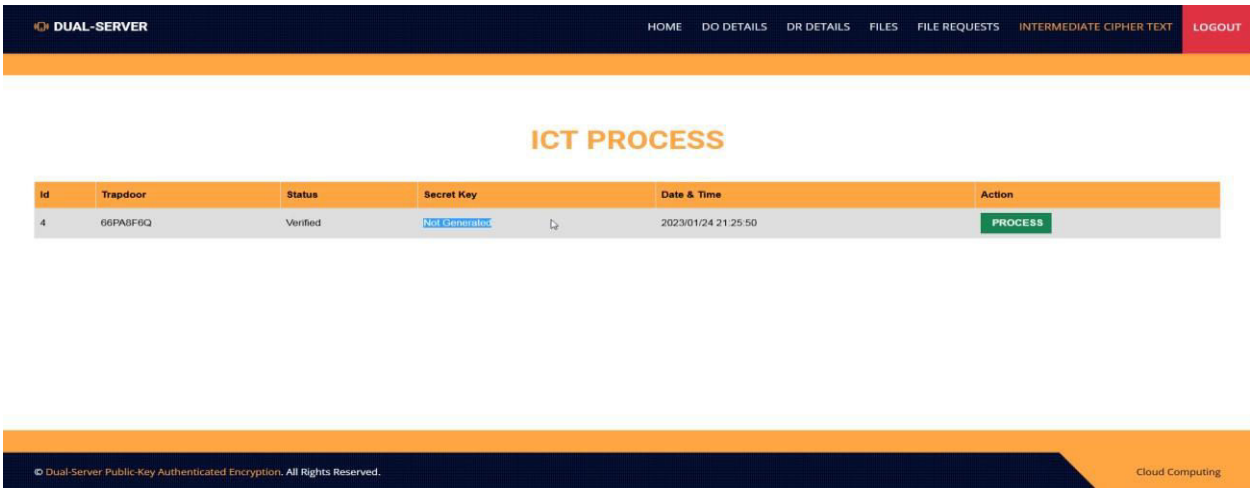


FIG : ICT PROCESS

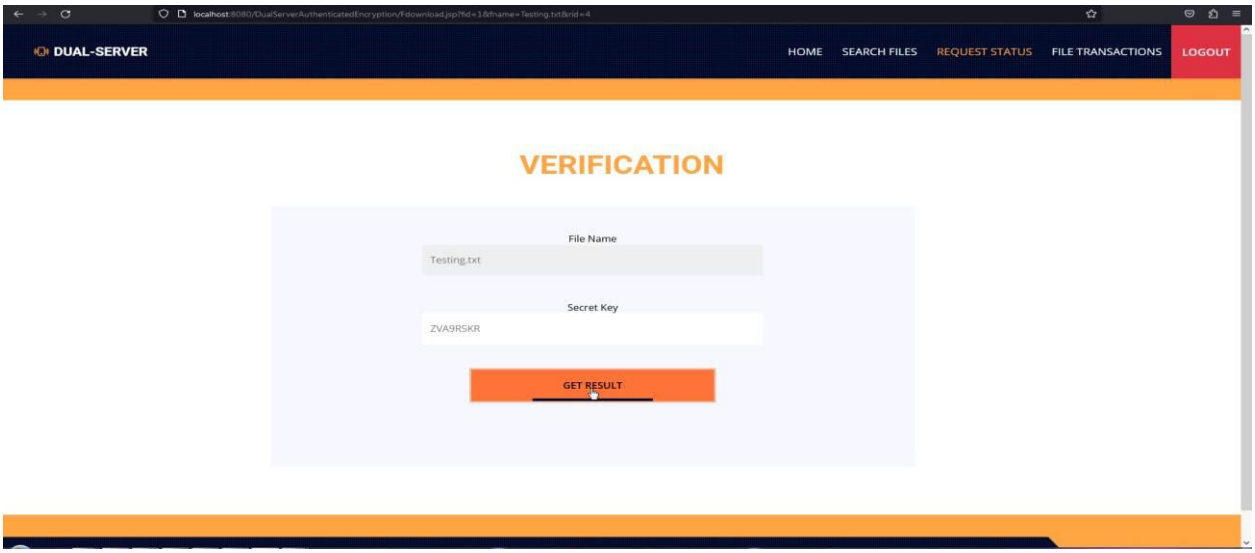


FIG : VERIFICATION FOR FILE ACCES

V. CONCLUSION

As the two properties in this study are incompatible, combining efficiency and protection against IKGA is not straightforward. Here, we've introduced a brand-new plan we call secure cloud search with dual server key encryption. Two non-colluding servers are utilized to prevent IKGA, and a pair of keys should be given to the owner to authenticate the data, among other characteristics. Lastly, we put the suggested system into practice and assessed its effectiveness. The empirical findings we were able to gather indicate that it can implemented in real-world scenarios. The Secure Cloud Search Using Dual Server with Key Encryption technique is introduced here. Using two non-colluding servers to thwart Inside Keyword Guessable Attacks (IKGA) and provide improved security is one of its primary characteristics. To add to the scheme's resilience, owner is also provided with set of key for data authentication.

Overall, the presented DPAESR scheme offers a powerful solution for protecting data confidentiality and privacy in cloud storage and other related scenarios. Its ability to counter IKGA, efficient performance, and robust security properties make it a promising addition to the field of searchable encryption. As technology continues to advance, In the proposed scheme may find widespread application and contribute significantly to ensuring secure data management and retrieval in various real-world scenarios.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305359 |

REFERENCES

[1] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," IEEE Syst. J., vol. 12, no. 1, pp. 64–73, Mar. 2018.
[2] D. He, N. Kumar, M. K. Khan, L. Wang, and S. Jian, "Efficient privacy-aware authentication scheme for mobile cloud computing services," IEEE Syst. J., vol. 12, no. 2, pp. 1621–1631, Jun. 2018.
[3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.
[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 506–522.
[5] P. Xu,H. Jin,Q.Wu, andW.Wang, "Public-key encryptionwith fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.
[6] 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. Australasian Conf. Inf. Security Privacy, 2015, pp. 59–76.
[7] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Inf. Sci., vol. 403, pp. 1–14, 2017.
[8] D. Wang, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," Inf. Sci., vol. 321, pp. 162–178, 2015.
[9] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," IEEE Trans. Dependable Secure Comput., 2018.
[10] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl., 2008, pp. 1249–1259.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details