e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707161 |

Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage

Dhanyashree S[*1], Praveen K S[*2]

Student, Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India. [*1]

Associate Professor, Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[*2]

ABSTRACT : Distributed storage has turned into an essential industry in far off information the executives administration yet in addition draws in safe concerns, where the most ideal that anyone could hope to find approach for forestalling information exposure is encipher. amid them the civic answer encipher amid catchphrase explore (PKSE) is viewed as a promising procedure, because patrons can effectively look through over scrambled information records. That is, a client initially creates a hunt token when to inquiry information documents, the computing grid utilizes the pursuit token to continue the question over encoded information records. Nonetheless, a grim assault is heave when PKSE gather shade. Officially talking, the confuse attendant can gain proficiency with the data of a recently added scrambled information record containing the watchword that recently questioned by utilizing the pursuit tokens it has gotten, and can additionally find the protection data. To resolve this question, we offer a advance locked civic type accessible encipher conspire, in which a obscure server can't get familiar with any data about a recently added scrambled information record containing the catchphrase that recently questioned. To all the more likely comprehend the plan guideline, we present a system for building forward secure civic key accessible encipher plans in view of quality based accessible encipher. At long last, the analyses show our plan is effective.

KEYWORDS:

- Forward Security
- Public Key Encryption
- Keyword Search
- Cloud Storage
- Encryption Scheme
- Data Privacy
- Ciphertext

I. INTRODUCTION

Traditional symmetric searchable encipher techniques have a significant processing cost while searching for data, since the complexity increase with the number of files in the database. Limited functionality , existing methods often only handle simple single keyword searches, not Boolean or fuzzy queries.

The current symmetric searchable encipher techniques are subject to leakage –abuse attacks, which can disclose a client's query privacy even with minor leaks. The existing civic key searchable encipher technology is vulnerable to a variety of assaults when applied in the cloud for preserving potentially resulting in privacy breaches.

II. LITERATURE SURVEY

The chance of civic key open encipher was presented by Boneh et al. which performs better stood out from symmetric accessible encipher in information sharing.

Abdalla et al. present a standard development to encourage the best method for getting civic key open encipher from bewildering character based encipher.

To really try not to utilize conflicting prophets Khader et al. give a game plan considering kresilient character based encipher, which can be exhibited to be secure in the standard model yet ought to expect how much dangerous clients is more unpretentious than a predefined respect.

To beat the block of utilizing areas of strength for a by giving the server a civic key and mystery key pair, Baek et al. plan a game plan without a safeguarded channel, and from there on be relaxed to against adaptively enemies by Emura et al.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

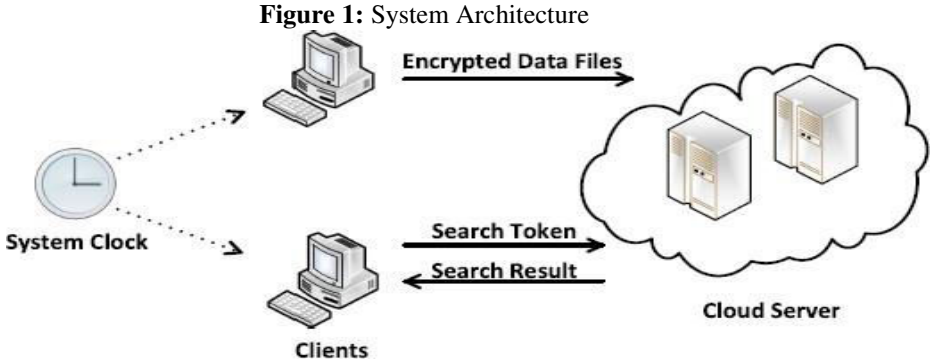
| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707161 |

Kamara et al. Give an arrangement that can capably add mixed data records to the informational assortment by utilizing tree-based information structure, and further update its pursuit suitability. While most plans can keep up with just the chief single watchword search Money et al. use a blended changed record to grasp the central plan that can cycle Boolean solicitations which is reached an other clients model.

III. SYSTEM DESIGN

Figure 1: System Architecture



IV. RESULTS AND OUTCOMES

Enhanced Security:

- **Forward Security**: FS-PEKS ensures that if a private key is compromised at any point in time, it does not affect the security of past encrypted data. This is achieved by updating the private key periodically without affecting the corresponding public key or previously generated ciphertexts.
- **Keyword Search**: The scheme allows for secure keyword search over encrypted data. Users can generate trapdoors for keywords to search over the encrypted data without revealing the keywords or the data to the cloud provider.

Privacy Protection:

- **Data Privacy**: Encrypted data remains confidential, and only authorized users can perform searches and access the data.
- **Search Privacy**: The cloud provider learns nothing about the actual keywords being searched or the content of the documents, preserving user privacy.

Efficient Key Management:

- **Key Updates**: Periodic key updates are handled efficiently, ensuring minimal computational overhead and maintaining the integrity of the encryption scheme.

Performance:

- **Search Efficiency**: FS-PEKS schemes are designed to allow efficient search operations, with the complexity of the search process being manageable and suitable for practical applications.
- **Scalability**: The scheme is scalable, supporting large datasets and a high number of search queries without significant performance degradation.

Outcome of the Detection:

Improved Data Security in Cloud Storage:

- FS-PEKS provides a robust solution for securing sensitive data in outsourced cloud environments, making it a viable option for industries where data privacy and security are critical, such as healthcare, finance, and government.

User Trust and Adoption:

- Enhanced security features and privacy protections can increase user trust in cloud storage services, potentially leading to higher adoption rates among security-conscious organizations and individuals.

Compliance with Regulations:

- FS-PEKS can help organizations comply with data protection regulations and standards, such as GDPR and HIPAA, by ensuring the confidentiality and integrity of stored data.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707161 |

Reduced Risk of Data Breaches:

- By ensuring that past data remains secure even if a private key is compromised, FS-PEKS reduces the risk and impact of data breaches, thereby enhancing the overall security posture of the organization.

Operational Efficiency:

- The efficient key management and search capabilities of FS-PEKS contribute to smoother operations and reduced administrative burden, particularly in environments with large volumes of data and frequent access requirements

Snapshots:

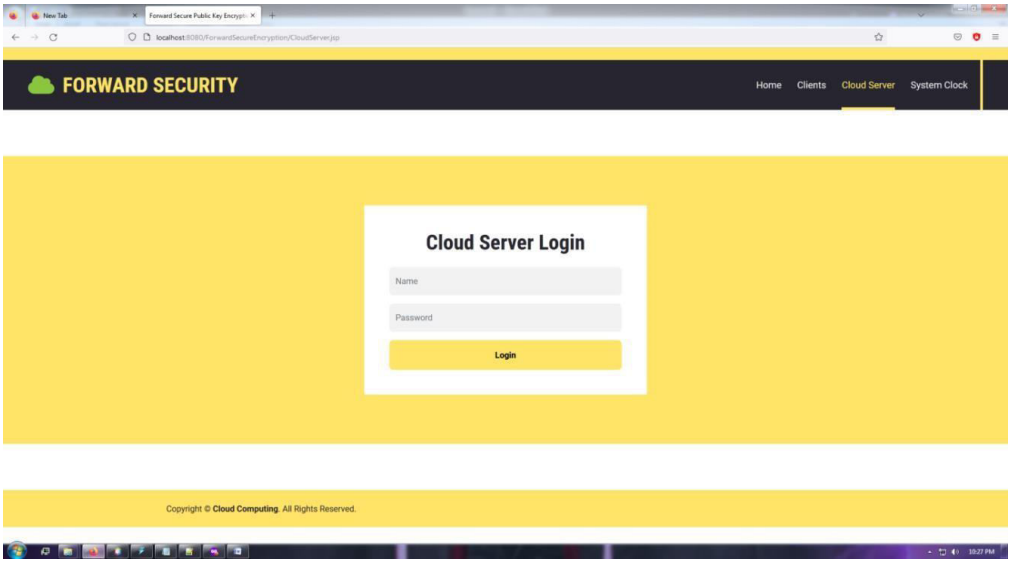


Figure 1: Cloud Server Login

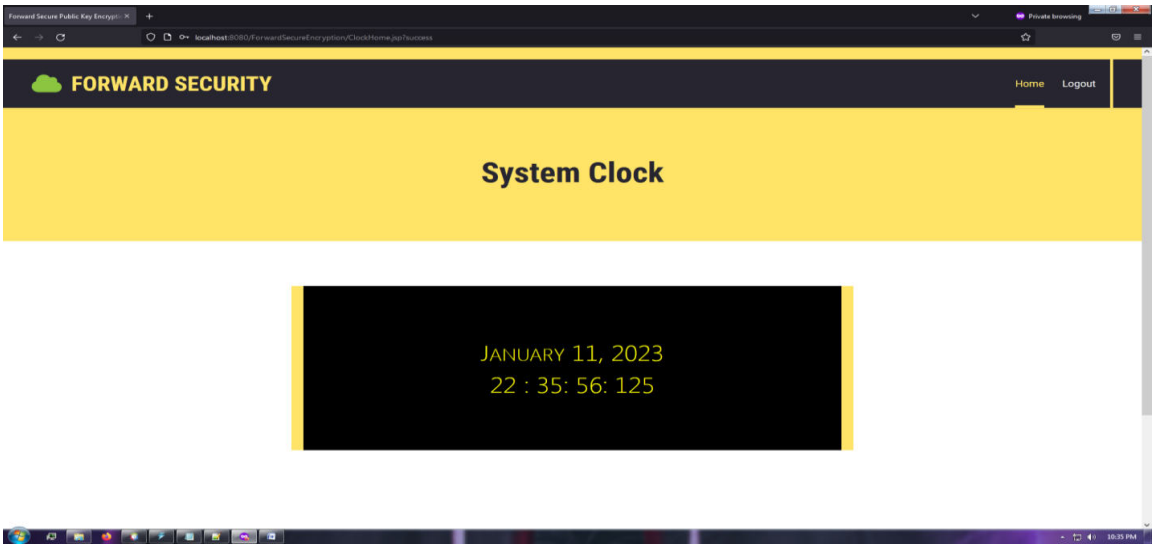


Figure 2: System Login

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707161 |

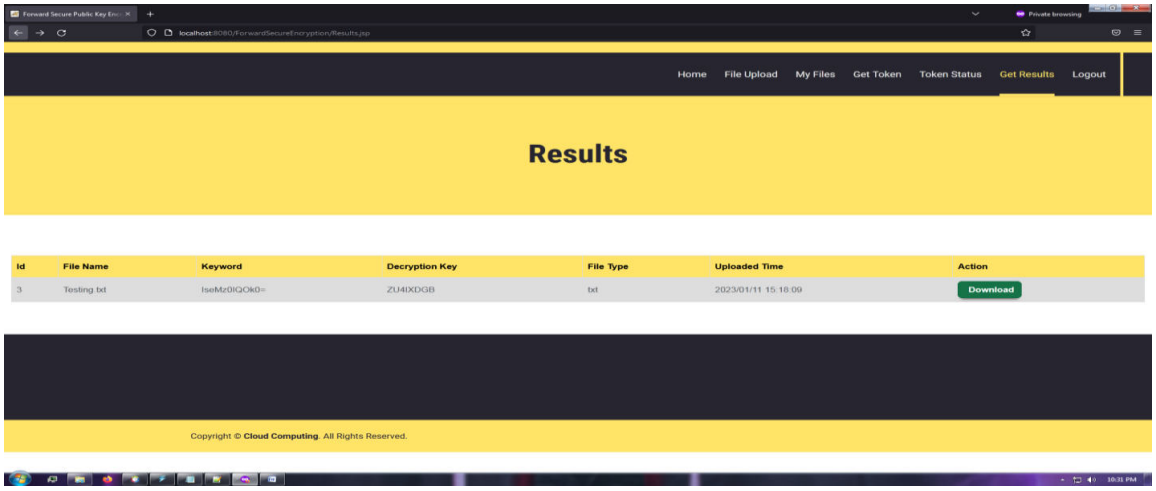


Figure 3: Result

V. CONCLUSION

In this paper, we center around the forward safe for civic key accessible encipher and that proposes another extra encoded information record can't be looked through by the pursuit tokens made before the blended information chronicle. This safe is frantically expected for the civic key open encipher plans conveyed in circled limit and can basically decrease the protection data spilled to a computing grid. As a reaction we propose a huge plan considering the 0-Encipher and 1-Encipher approach and give its safe confirmation further we similarly encourage the most effective method for getting a forward secure civic key open encipher conspire from a brand name based open encipher plot by presenting a common structure. Final we arrangement primers to address the savvy instinct of our proposed plot concerning encipher token age and search.

REFERENCES

[1] Q. Waang, M. Du, X. Chen, Y. Chen, P. Zhou, X. Chen, andX. Huang, “Privacy-preserving collaborative model learning: Thecase of word vector training,” IEEE Trans. Know. Data Eng.,vol. 30, no. 12, pp. 2381–2393, Dec. 2018.
[2] J. Cui, J. Zhang, H. Zhong, and Y. Xu, “SPACF: A secure privacy preserving authentication scheme for VANET with cuckoo filter, ”IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10283– 10295,Nov. 2017.
[3] H. Zhong, W. Zhu, Y. Xu, and J. Cui, “Multi-authority attribute based encipher access control scheme with policy hidden for cloud storage,” Soft Compute., vol. 22, no. 1, pp. 243–251, 2018.
[4] D. X.Song, D.A. Wagner, and A.Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Safe Privacy,2000, pp. 44–55.
[5] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky,“Searchable symmetric encipher: Improved definitions and efficient constructions,” in Proc. ACM Conf. Comput. Commun. Safe,2006, pp. 79–88.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com