Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

ENSURING THE PRESERVATION OF ASSETS IN FEDERATED FILEHOSTING

K.Shekhar, Assistant Professor CSE, Vaagdevi College of Engineering (Autonomous), India
A.Deepika, UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India
B.Shravya, UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India Saba Uzma, UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India Lubna Shereen, UG Student, CSE, Vaagdevi College of Engineering (Autonomous), India

ABSTRACT

Federated file hosting leverages a distributed approach, enabling multiple organizations or entities to pool their storage resources and collectively manage an extensive repository of files. However, this decentralized nature introduces complexities in ensuring the long-term preservation of these digital assets. In the context of federated environments, preserving assets encompasses not only safeguarding against data loss but also maintaining accessibility, authenticity, and reliability over time.This research proposes a comprehensive framework for ensuring the preservation of assets in federated file hosting ecosystems. The framework combines technological strategies, governance policies, and collaborative practices to address multifaceted preservation challenges. Key components include data redundancy mechanisms to mitigate against loss, cryptographic techniques for ensuring authenticity, access controls to manage data integrity, and versioning strategies for maintaining historical context.In conclusion, this research contributes to the evolving landscape of data preservation by offering a tailored approach for ensuring the preservation of digital assets within federated file hosting environments. By addressing the multifaceted challenges of data loss, authenticity, accessibility, and reliability, the proposed framework provides a comprehensive strategy to sustain the value and utility of shared assets in federated ecosystems.

Index :
distributed approach, accessibility, authenticity, and reliability, cryptographic techniques, comprehensive strategy.

1. INTRODUCTION

In today's digital landscape, the exponential growth of data and the increasing demand for collaborative platforms have catalyzed the evolution of file hosting services. Among these services, federated file hosting has emerged as a promising solution that capitalizes on the distributed nature of data storage. Federated systems allow multiple organizations [1],[2], institutions, or entities to collaboratively manage and share a common repository of files. This collaborative approach offers benefits such as resource optimization, enhanced data accessibility, and improved scalability.

However, as federated file hosting gains traction, a critical challenge arises: the preservation of digital assets within such dynamic and decentralized ecosystems. Unlike traditional centralized models, federated environments involve a diverse range of stakeholders with varying priorities, access patterns, and governance structures[4]. Ensuring the long-term preservation of assets— ranging from documents and media files to critical data—within these multifaceted federated systems demands a comprehensive strategy that encompasses technical, governance, and collaborative aspects.

This project focuses on the pivotal task of preserving assets in federated file hosting, where multiple participants collectively manage a shared pool of resources[3]. The goal is to develop a framework that ensures the continuous integrity, authenticity, and accessibility of assets while navigating the challenges posed by distribution, collaboration, and varying levels of control.The following sections[5]-[7] will delve into the intricacies of this challenge and outline the proposed framework designed to tackle the multifaceted aspects of preserving assets within the context of

federated file hosting. By addressing technical strategies, collaborative approaches, and governance mechanisms, this project aims to contribute to the sustainable management and preservation of digital assets in the era of federated data ecosystems.

2. LITERATURE SURVEY

Decentralized cloud storage systems have gained popularity due to their potential for improved data privacy, availability, and resilience. However, ensuring the security of resources within such systems presents unique challenges. This literature survey explores[8] various approaches and strategies for securing resources in decentralized cloud storage environments.

The survey begins with an overview of the fundamental concepts related to decentralized cloud storage, including the benefits and challenges associated with decentralization. It also highlights the critical importance of resource security in these systems.

The main body of the survey comprises a comprehensive review of research articles, studies, and projects that have addressed resource security in decentralized cloud storage. Each work's methodologies, cryptographic[9] techniques, access control mechanisms, and security models are examined in detail. Additionally, the survey analyzes the reported security performance and resilience of these approaches.

The survey evaluates the strengths and weaknesses of different security strategies within the context of decentralized cloud storage, considering factors such as scalability, performance overhead, and resistance to various security threats.

In addition to summarizing existing research, this survey identifies emerging trends and challenges in the field of securing resources in decentralized cloud storage [9]. This includes adapting security models to evolving threats, addressing scalability issues, and ensuring compliance with data protection regulations.

In conclusion, this literature survey provides a comprehensive overview of the various methods and techniques used to secure resources in decentralized cloud storage. It serves as a valuable resource for researchers, practitioners, and organizations seeking effective strategies to protect data andresources in decentralized cloud environments[10].

Decentralized cloud storage systems have emerged as a promising solution for data storage and sharing, offering enhanced privacy and availability. However, ensuring the security of resources in these decentralized environments is of paramount importance. This literature survey [11] delves into the diverse strategies and methodologies employed to secure resources in decentralized cloud storage.

The survey commences with a thorough introduction to decentralized cloud storage, elucidating the key advantages and challenges associated with this paradigm shift. Emphasis is placed on the critical role of resource security within these systems.

The core of the survey encompasses an extensive review of research papers, projects, and studies that have tackled resource security in decentralized cloud storage[12],[13],[14]. Each work's approaches, cryptographic techniques, access control mechanisms, and security evaluations are meticulously examined. Additionally, the survey scrutinizes the reported security performances and resistance levels against a spectrum of security threats.

The survey provides a critical assessment of the merits and limitations of distinct security strategies within the decentralized cloud storage context. It takes into account various factors, including scalability, performance overhead, and adaptability to evolving security threats.

Furthermore, this literature survey[15] identifies emerging trends and confronts the challenges in the realm of resource security in decentralized cloud storage, including the need for innovative security models, scalability solutions, and compliance with data privacy regulations.

In conclusion, this comprehensive literature survey serves as a valuable repository of knowledge, offering insights into the multifaceted methods and techniques for safeguarding resources in

decentralized cloud storage. Researchers, practitioners, and organizations will find it an indispensable resource for enhancing the security of their decentralized storage environments.

Decentralized cloud storage has emerged as a promising solution for data storage and sharing, offering advantages in terms of privacy, availability, and fault tolerance. However, ensuring the security of resources within decentralized cloud storage environments is a complex endeavor[16]. This literature survey provides an in-depth exploration of the various strategies and techniques employed to secure resources in these decentralized settings.

The survey initiates with a comprehensive introduction to decentralized cloud storage, outlining its potential benefits and challenges. Particular attention is given to the significance of resource security within this context.

The primary focus of the survey is a meticulous review of research papers, projects, and studies that have addressed resource security in decentralized cloud storage[17]-[18]. Each work's methodologies, cryptographic approaches, access control mechanisms, and security evaluations are rigorously examined. Additionally, the survey analyzes reported security performances and the resilience of these methods against diverse security threats.

The survey critically evaluates the strengths and limitations of different security strategies within decentralized cloud storage, [19], [20] taking into account factors such as scalability, performance impact, and adaptability to evolving security threats.

Furthermore, this literature survey identifies emerging trends and confronts the challenges in the field of resource security in decentralized cloud storage, including the need for innovative security models, scalable solutions, and compliance with evolving data protection regulations.

In conclusion, this comprehensive literature survey serves as an invaluable resource for researchers, practitioners, and organizations seeking to enhance the security of resources in decentralized cloud storage environments[21]. It provides a detailed overview of various methods and techniques to protect data and resources within this evolving landscape.

3. PROBLEM STATEMENT

Protection of the encryption key is therefore not sufficient in DCS scenarios, as it remains exposed to the threats above[23]. A general security principle is to rely on more than one layer of defense. In this paper, we propose an additional and orthogonal layer of protection, which is able to mitigate these risks.

On the positive side, however, we note that the decentralized nature of DCS systems also increases the reliability of the service, as the involvement of a collection of independent parties reduces the risk that a single malfunction can limit the accessibility to the stored resources. In addition to this, the independent structure characterizing DCS systems [22] - if coupled with effective resource protection and careful allocation to nodes in the network - makes them promising for actually strengthening security guarantees for owners relying on the decentralized network for storing their data.

LIMATATON OF DRAW BACKS

While decentralizing resources we are losing security.Availability and protection responding to currently open problems of emerging DCS scenarios

4. PROPOSED SYSTEM

The proposed solution also enables the resource owners to securely delete their resources when needed, even when some of the nodes in the DCS misbehave. Second, we investigate different strategies for slicing and distributing resources across the decentralized network, and analyze their characteristics in terms of availability and security guarantees. Third, we provide a modeling of the problem enabling owners to control the granularity of slicing and the diversification of allocation to ensure the aimed

availability and security guarantees. We demonstrate the effectiveness of the proposed model by conducting several experiments on an implementation based on an available DCSsystem. Our solution provides an effective approach for protecting data in decentralized cloudstorage and ensures both availability and protection responding to currently open problems of emerging DCS scenarios, including secure deletion[23]. In fact, common secret sharing solutions (e.g., Shamir [8]), while considering apparently similar requirements are not applicable in scenarios where the whole resource content (and not simply the encryption key) needs protection, because of their storage and network costs (e.g., each share in Shamir's method has the same size as the whole data that has to be protected).

ADVANTAGE OF SYSTEM

Our solution provides an effective approach for protecting data in decentralized cloud storage.

5. IMPLEMENTATION

5.1 CSP

In this application csp is a module, csp can login directly with username and password. After download csp can perform some actions like view data owner and authorize, view data users andauthorize and also can view all files.

5.2 DataOwner

Here data owner should register and should authorized by the cloud then only the owner can login with the application after his successful login he can perform some actions like uploadfile, view files,view file requests.

5.3 Data User

Here data user should register and should authorized by the cloud then only the user can login with the application after his successful login he can perform some actions like view profiles, search file, request status.

6. EXPECTED OUTCOMES

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

Fig 6.1 Home Page

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

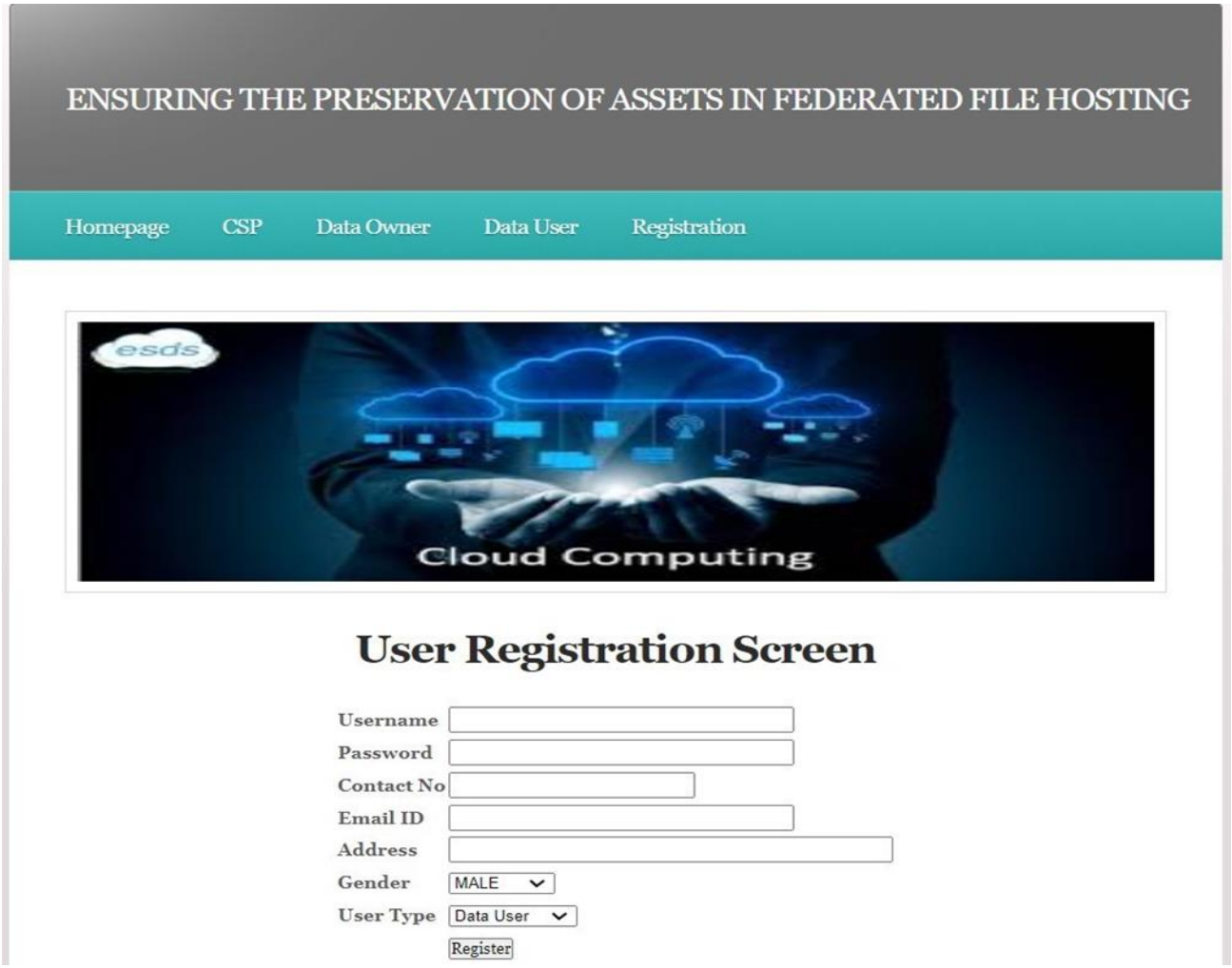

Fig 6.2 Data User Registration Screen

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

Fig 6.3 Data User Login Screen

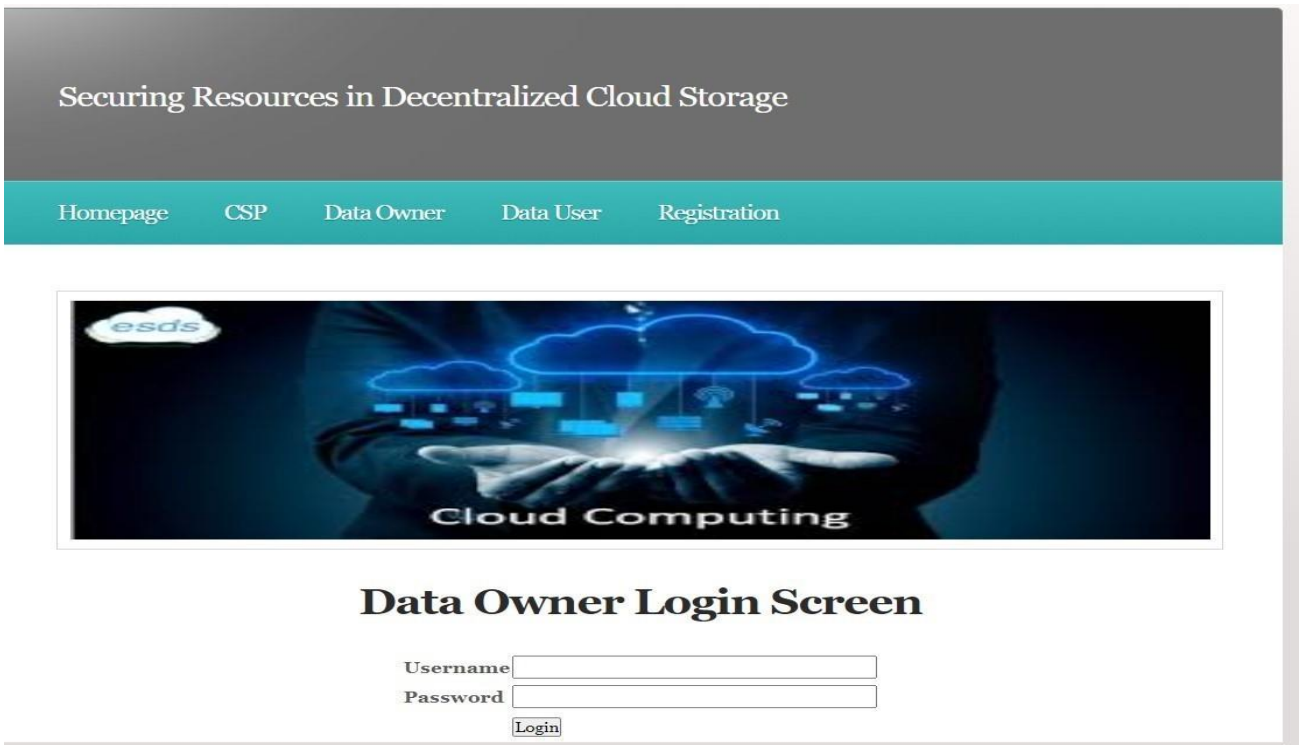

Fig 6.4 Data Owner Login Screen

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

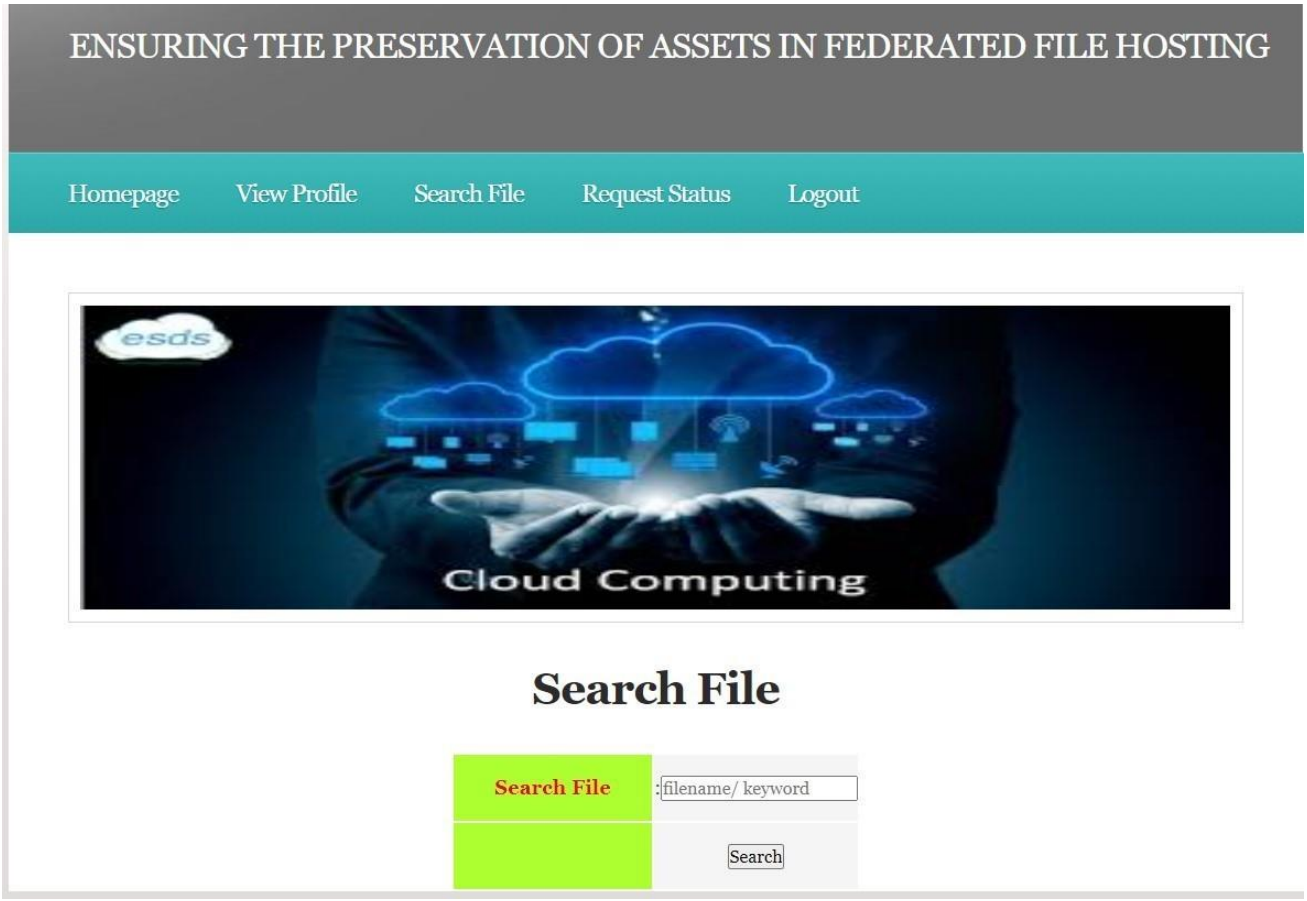

Fig.6.5 Data User Screen to Search File

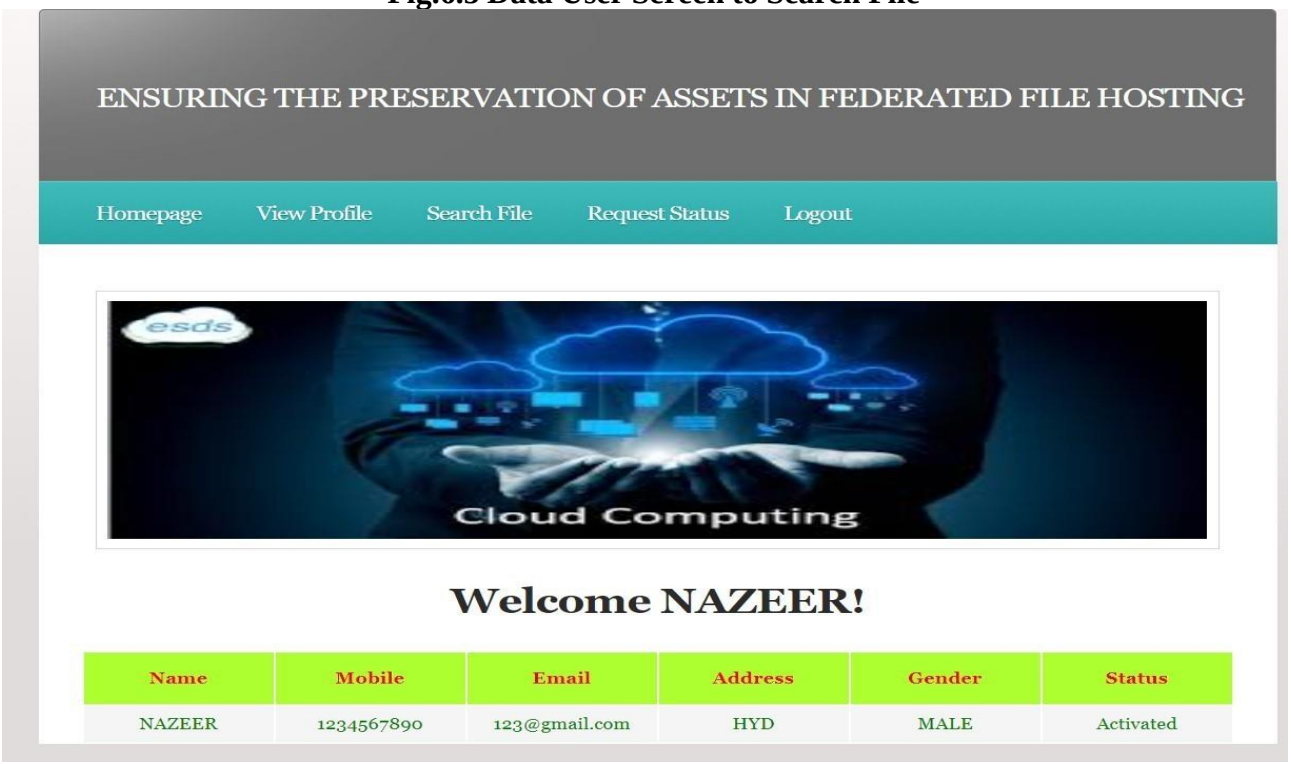

Fig.6.6.Data User Screen after Login

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

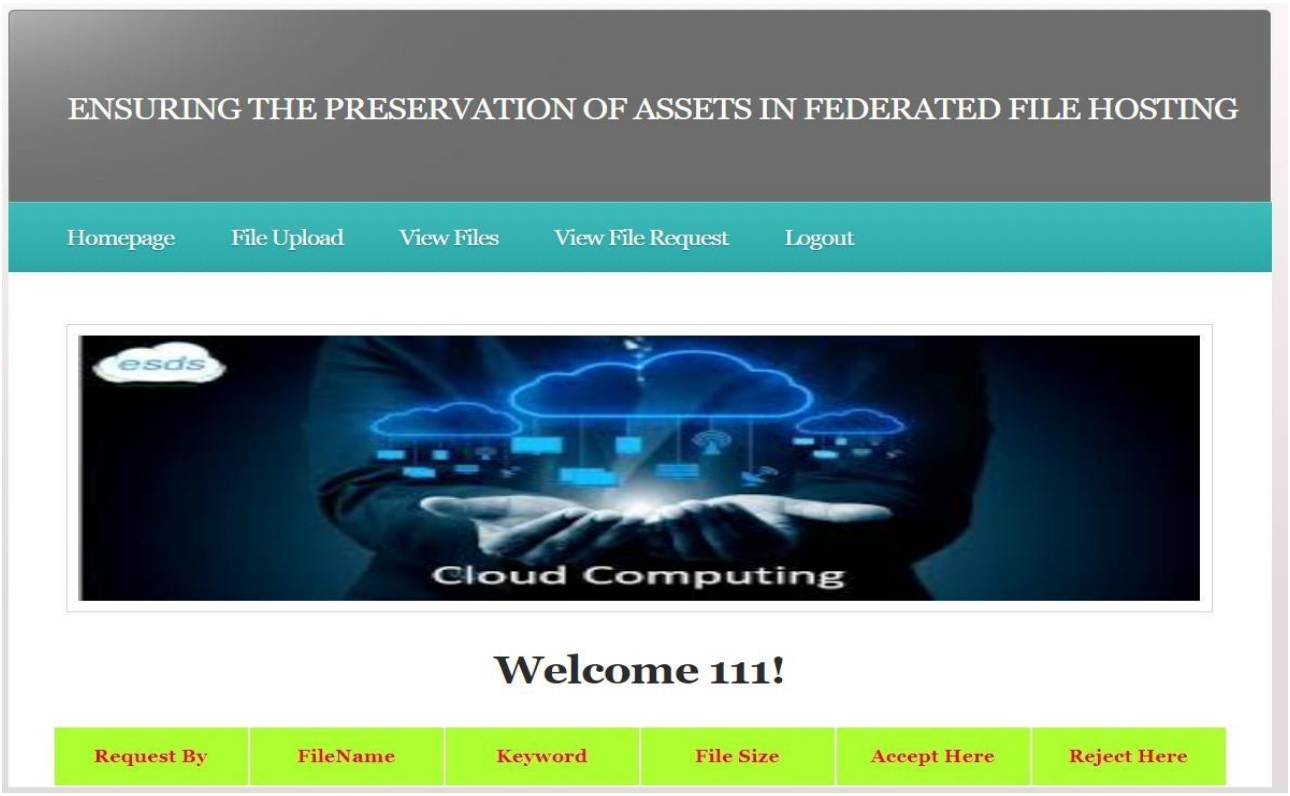

Fig.6.7. Data Owner Screen after View File Request

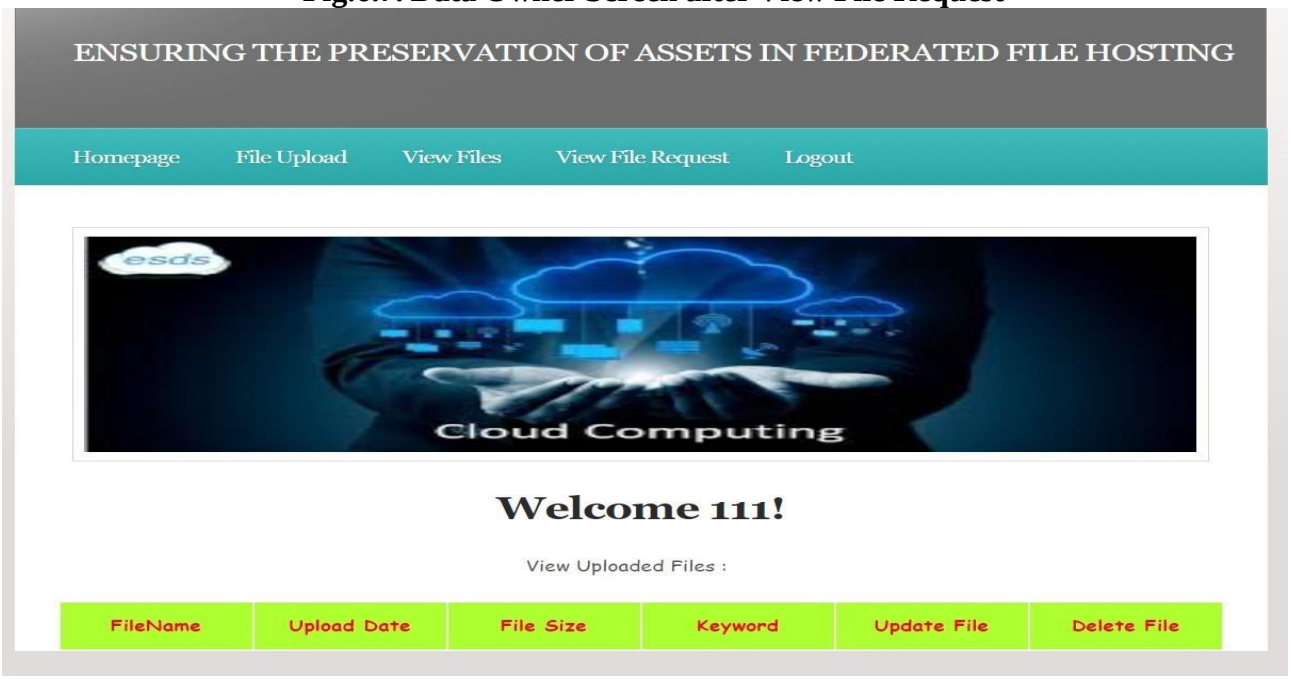

Fig.6.8.View File of Data Owner Screen

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

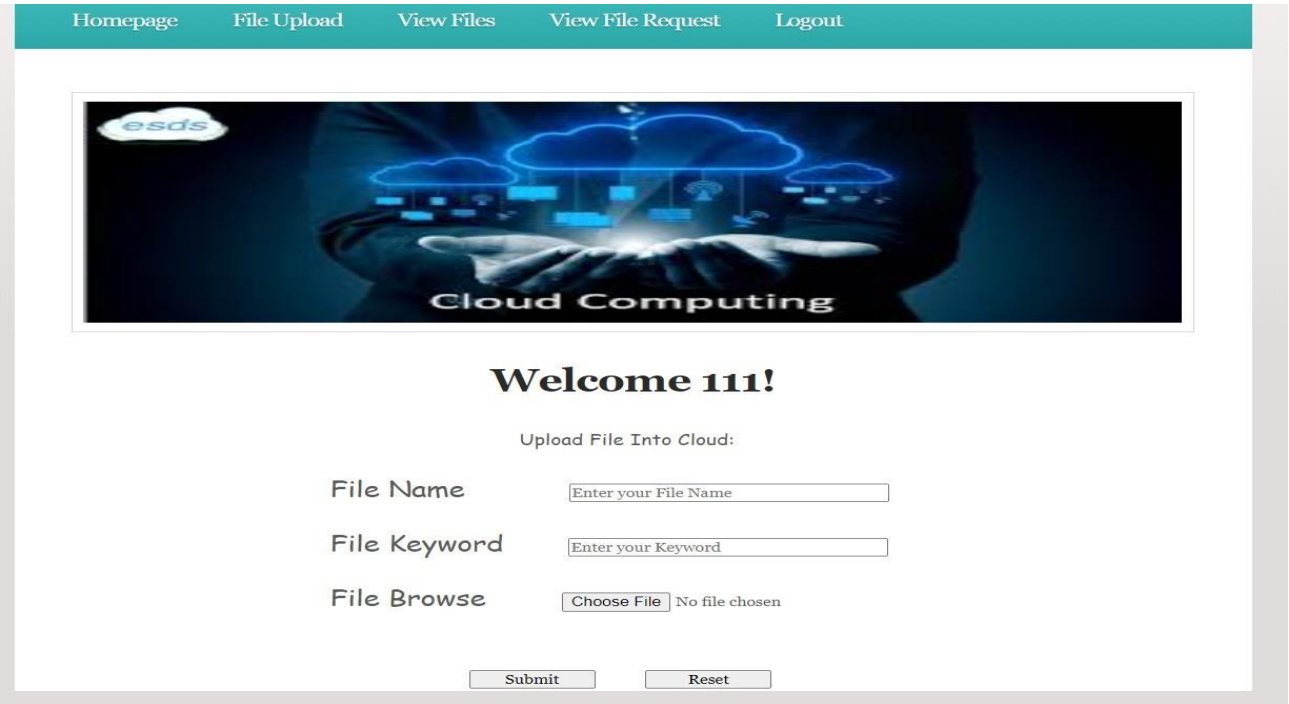

Fig.6.9 File upload of Data Owner Screen

7. CONCLUSION & FUTURE SCOPE

We presented an approach for providing effective secure protection to resources in decentralized cloud storage services. Our approach enables resource owners to protect their resources and to control their decentralized allocation to different nodes in the network. We investigated different strategies for splitting and distributing resources, analyzing their characteristics in terms of availability and security guarantees. We also provided a modeling of the problem enabling owners tocontrol the granularity of slicing and diversification of allocation to ensure aimed availability and security guarantees. Enabling effective control for resource owners, our solution helps in removing natural reluctance due to security concerns and moves a step forward in the realization of novel services effectively benefiting from technological evolution. Our work leaves room for extensions, such as the consideration of error correcting codes and information dispersal algorithms to reduce thespatial overhead.

The future scope of ensuring the preservation of assets in federated file hosting lies in the convergence of advanced security measures, interoperability enhancements, decentralized storage solutions, AI-driven asset management, immutable data storage, regulatory compliance tools, and scalability/performance optimization. By implementing stronger encryption methods and security measures, improving interoperability between platforms, leveraging decentralized technologies like blockchain, employing AI for automated asset management, ensuring immutable data storage, developing regulatory compliance tools, and optimizing scalability and performance, organizations can address challenges in preserving assets across federated file hosting systems while ensuring data integrity, accessibility, and compliance with evolving regulations. These advancements will enable organizations to securely store and manage digital assets, safeguarding them against unauthorized access, tampering, and data loss while ensuring long-term preservation and accessibility.

8. REFERENCES

[1]S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, P. Hutchins, C. Pollard, and V. Buterin, “Storj: a peer-to-peer cloud storage network (v2.0),” https://storj.io/storjv2.pdf, Storj

Labs Inc., Tech. Rep., 2016.
[2]D. Irvine, “Maidsafe distributed file system,” MaidSafe, Tech. Rep., 2010.
[3]G. Paul, F. Hutchison, and J. Irvine, “Security of the maidsafe vault network,” in Wireless World Research Forum Meeting 32, Marrakesh, Morocco, May 2014.
[4]J. Benet, “IPFS-content addressed, versioned, P2P file system,” Protocol Labs, Tech. Rep., 2014.
[5]D. Vorick and L. Champine, “Sia: Simple decentralized storage,” https: //sia.tech/sia.pdf, Nebulous Inc., Tech. Rep., 2014.
[6]C. Patterson, “Distributed content delivery and cloud storage,” https: //www.smithandcrown.com/distributed-content-delivery-cloud-storage/, Smith and Crown, Tech. Rep., 2017.
[7]H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, “Executing SQL over encrypted data in the database-service-provider model,” in Proc. of ACM SIGMOD, Madison, Wisconsin, June 2002.
[8]A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, September/December 1979.
[9]E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, “Mix&Slice: Efficient access revocation in the cloud,” in Proc. of ACM CCS, Vienna, Austria, October 2016.
[10] N. Lambert and B. Bollen, “The SAFE network - a new, decentralised internet,” http://docs.maidsafe.net/Whitepapers/pdf/TheSafeNetwork.pdf, MaidSafe, Tech. Rep., 2014.
[11] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.
[12] D. A. Patterson, G. Gibson, and R. H. Katz, “A case for redundant arrays of inexpensive disks (RAID),” ACM SIGMOD Records, vol. 17, no. 3, pp. 109–116, Jun. 1988.
[13] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” in Proc. of ACM CCS, Chicago, IL, USA, November 2009.
[14] ——, “Proofs of retrievability: Theory and implementation,” in Proc. Of ACM CCSW, Chicago, IL, USA, November 2009.
[15] M. Albanese, S. Jajodia, R. Jhawar, and V. Piuri, “Dependable and resilient cloud computing,” in Proc. of IEEE SOSE, Oxford, UK, March 2016.
[16] A. Aldribi, I. Traore, and G. Letourneau, “Cloud slicing a new architecture for cloud security monitoring,” in Proc. of IEEE PACRIM, Victoria, Canada, August 2015.
[17] D. Nu˜nez, I. Agudo, and J. Lopez, “Delegated access for hadoop clusters in the cloud,” in Proc. of IEEE CloudCom, Singapore, December 2014.
[18] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, “Privacy risk, security, accountability in the cloud,” in Proc. of IEEECloudCom, Bristol, UK, December 2013.
[19] J. K. Resch and J. S. Plank, “AONT-RS: blending security and performance in dispersed storage systems,” in Proc of FAST, San Jose, CA, USA, February 2011.
[20] M. Li, C. Qin, P. P. C. Lee, and J. Li, “Convergent dispersal: Toward storage-efficient security in a cloud-of-clouds,” in Proc. of HotStorage, Philadelphia, PA, USA, June 2014.
[21] M. Li, C. Qin, and P. P. C. Lee, “CDStore: Toward reliable, secure, and cost-efficient cloud storage via convergent dispersal,” in Proc. Of USENIX ATC, Santa Clara, CA, USA, July 2015.
[22] A. Bessani, M. Correia, B. Quaresma, F. Andr´e, and P. Sousa, “DepSky: Dependable and secure storage in a cloud-of-clouds,” ACM TOS, vol. 9, no. 4, pp. 12:1–12:33, 2013.
[23] M. Waldman and D. Mazieres, “Tangler: a censorship-resistant publishing system based on document entanglements,” in Proc. of ACM CCS, Philadelphia, PA, USA, November 2001.