Journal of Nonlinear Analysis and Optimization

Vol. 16, Issue. 1: 2025

ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications

Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

Enhancing Security in Decentralized Cloud Storage Systems

K. UDAY KIRAN[1], A.SUNEEL[2]

#1 Assistant Professor Department of Master of Computer Applications

#2 Pursuing M.C.A in QIS COLLEGE OF ENGINEERING & TECHNOLOGY

Vengamukkapalem(V),Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract

Decentralized Cloud Storage services represent a promising opportunity for a different cloud market, meeting the supply and demand for IT resources of an extensive community of users. The dynamic and independent nature of the resulting infrastructure introduces security concerns that can represent a slowing factor towards the realization of such an opportunity, otherwise clearly appealing and promising for the expected economic benefits. In this paper, we present an approach enabling resource owners to effectively protect and securely delete their resources while relying on decentralized cloud services for their storage. Our solution combines All-Or-Nothing-Transform for strong resource protection, and carefully designed strategies for slicing resources and for their decentralized allocation in the storage network. We address both availability and security guarantees, jointly considering them in our model and enabling resource owners to control their setting.

Introduction

A clear recent trend in information technology is the rent by many users and enterprises of the storage/computation services from other parties. With cloud technology, what was in the past managed autonomously now sees the involvement of servers, often in an unknown location, immediately reachable wherever an Internet connection is present. Today the use of these Internet services typically assumes the presence of a Cloud Service Provider (CSP) managing the service. There are a number of factors that explain the current status. In general, the procurement and management of IT resources exhibit significant scale economies, and large-scale CSPs can provide services at costs that are less than those incurred by smaller players. Still, many users have an excess of computational, storage, and network capacity in the systems they own and they would be interested in offering these resources to other users in exchange of a rent payment. In the classical behavior of markets, the existence of an infrastructure that supports the meeting of supply and demand for IT services would lead to a significant opportunity for the creation of economic value from the use of otherwise under-utilized resources.

This change of landscape is witnessed by the increasing attention of the research and development community toward the realization of Decentralized Cloud Storage (DCS) services, characterized by the availability of multiple nodes that can be used to store resources in a decentralized manner. In such services, individual resources are fragmented in shards allocated (with replication to provide availability guarantees) to different nodes. Access to a resource requires retrieving all its shards. The main characteristics of a DCS is the cooperative and dynamic structure formed by independent nodes (providing a multi-authority storage network) that can join the service and offer storage space, typically in exchange of some reward. This evolution has been facilitated by blockchain-based technologies providing an effective low-friction electronic payment system supporting the remuneration for the use of the service. On platforms such as Storj [1], SAFE Network Vault [2], [3], IPFS [4], and Sia [5], users can rent out their unused storage and bandwidth to offer a service to other users of the network, who pay for this service with a network crypto-currency [6].

However, if security concerns and perception of (or actual) loss of control have been an issue and slowing factor for centralized clouds, they are even more so for a decentralized cloud storage, where the dynamic and independent nature of the network may hint to a further decrease of control of the owners on where and how their resources are managed. Indeed, in centralized cloud systems, the CSP is generally assumed to be honest-but-curious and is then trusted to perform all the operations requested by authorized users (e.g., delete a file when requested by the owner) [7]. The CSP is discouraged to behave maliciously, since this would clearly impact its reputation. On the contrary, the nodes of a decentralized system may behave maliciously when their misbehavior can provide economic benefits without impacting reputation (e.g., sell the content of deleted files). Client-side encryption typically assumed in DCSs provides a first crucial layer of protection, but it leaves resources exposed to threats, especially in the long term. For instance, resources are still vulnerable in case the encryption key is exposed, or in case of malicious nodes not deleting their shards upon the owner's request to try reconstructing the resource in its entirety.

Protection of the encryption key is therefore not sufficient in DCS scenarios, as it remains exposed to the threats above. 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 - 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.

owners to securely store their resources in DCS services, to share them with other users, while still being able to securely delete them. Our contribution is threefold. First, leveraging the protection guarantees offered by All-Or-Nothing-Transform (AONT), we devise an approach to carefully control resource slicing and allocation to nodes in the network, with the goal of ensuring both availability (i.e., retrieval of all slices to reconstruct the resource) and security (i.e., protection against malicious parties jointly collecting all the slices composing a resource). 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 DCS system. Our solution provides an effective approach for protecting data in decentralized cloud storage and ensures both availability and protection responding to currently open problems of emerging DCS scenarios, including secure deletion. 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).

Literature Survey

1. FileDES: A Secure Scalable and Succinct Decentralized Encrypted Storage Network

- **Authors**: Minghui Xu, Jiahao Zhang, Hechuan Guo, Xiuzhen Cheng, Dongxiao Yu, Qin Hu, Yijun Li, Yipu Wu
- **Merits**: Introduces a scalable Proof of Encrypted Storage (PoES) algorithm resilient to Sybil and Generation attacks; employs rollup-based batch verification for efficient auditing.
- **Demerits**: Focuses primarily on scalability and efficiency; does not extensively address user access control or data sharing mechanisms.
- **Reference**: arXivarXiv+1arXiv+1Kalima Blockchain

2. Haina Storage: A Decentralized Secure Storage Framework Based on Improved Blockchain Structure

- **Authors**: Zijian Zhou, Caimei Wang, Xiaoheng Deng, Jianhao Lu, Qilue Wen, Chen Zhang, Hong Li
- **Merits**: Proposes a Bi-direction Circular Linked Chain Structure (BCLCS) and a Proof of Resources (PoR) decision model to enhance storage capacity and efficiency.
- **Demerits**: The complexity of the proposed structures may introduce implementation challenges and overhead.
- **Reference**: arXivarXiv

3. Securing Dynamic Distributed Storage Systems against Eavesdropping and Adversarial Attacks

- **Authors**: Sameer Pawar, Salim El Rouayheb, Kannan Ramchandran
- **Merits**: Addresses security in dynamic environments with node failures; provides upper bounds on information storage safety.
- **Demerits**: The focus on theoretical bounds may limit practical applicability in real-world systems.
- **Reference**: arXivarXiv

4. Towards Privacy-assured and Lightweight On-chain Auditing of Decentralized Storage

- **Authors**: Yuefeng Du, Huayi Duan, Anxin Zhou, Cong Wang, Man Ho Au, Qian Wang
- **Merits**: Introduces a lightweight auditing solution using homomorphic linear authenticators and sigma protocols for privacy-preserving verification.

- **Demerits**: The reliance on blockchain for auditing may lead to scalability issues as the number of users grows.
- **Reference**: arXivarXiv

5. Blockchain Technology for Cloud Storage: A Systematic Literature Review

- **Authors**: Rui Zhang, Rui Xue, Ling Liu
- **Merits**: Provides a comprehensive review of blockchain applications in cloud storage, highlighting security and privacy enhancements.
- **Demerits**: The review is broad and may lack in-depth analysis of specific implementations or case studies.
- **Reference**: ACM Digital Library

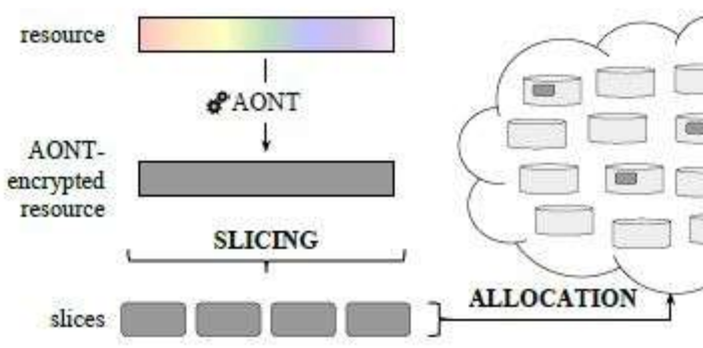
6. Blockchain-based Decentralized Architecture for Cloud Storage System

- **Authors**: Not specified
- **Merits**: Proposes a blockchain-based architecture incorporating access control and integrity checking mechanisms for enhanced security.
- **Demerits**: The paper lacks detailed performance evaluations and comparisons with existing systems.
- **Reference**: ACM Digital LibraryACM Digital Library

7. Decentralized Cloud Storage Using Blockchain

- **Authors**: G. Richa Shalom, Ganesh Rohit Nirogi
- **Merits**: Utilizes IPFS for file storage and blockchain for metadata management, ensuring data integrity and security.
- **Demerits**: The system's reliance on IPFS and blockchain may introduce latency and scalability challenges.
- **Reference**: IJRASET

System Architecture:



MODULES**:**

1. Csp
2. Data owner
3. Data user

Module Description

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 and authorize and also can view all files.

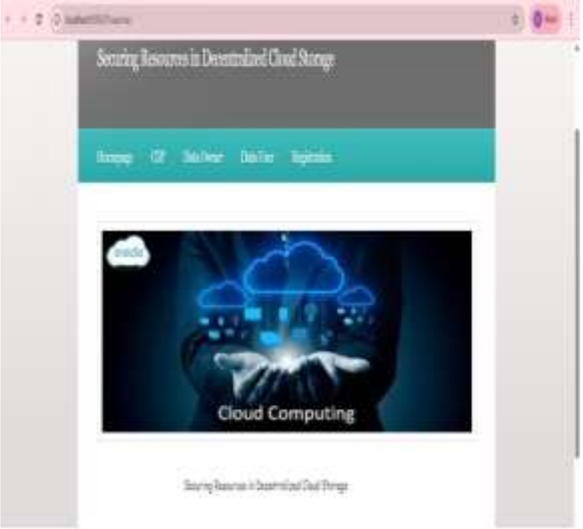
2. **DataOwner**
   Here data owner should register and should authorized by the cloud then only the owner can login with the application after his successful login he can perform some actions like uploadfile, view files, view file requests.
3. **Data User**
   Here data user should register and should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

onclusion And Future Enhancement

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 to control 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 the spatial overhead.

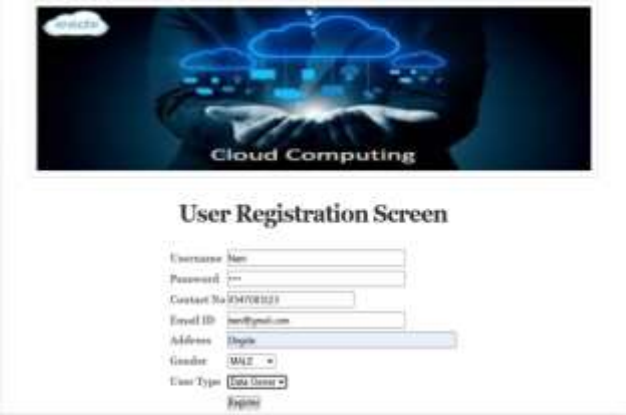
IMPLEMENTATION:

EXECUTION PROCEDURE



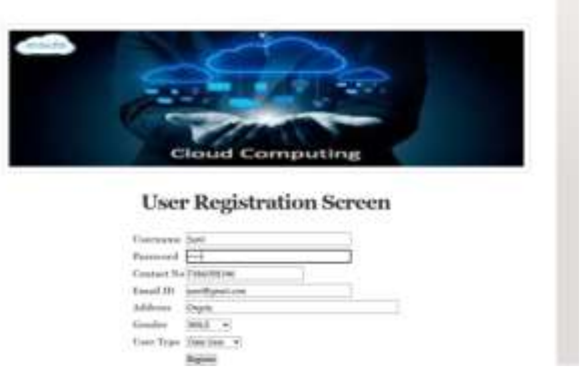
Securing Resources in Decentralized Cloud Storage

Securing Resources in Decentralized Cloud Storage



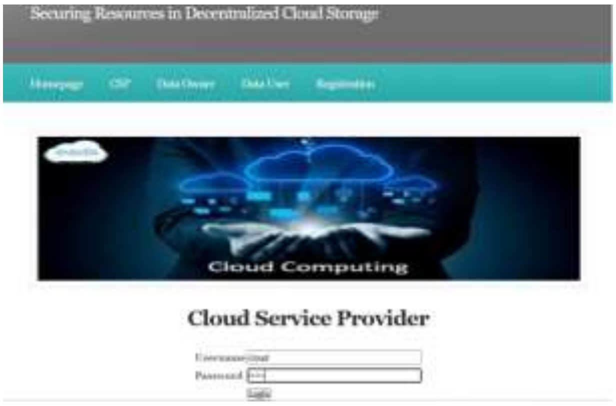
User Registration Screen

Username Nani
Password ***
Contact No [illegible]
Email ID nani@gmail.com
Address Ongole
Gender MALE
User Type Data Owner



User Registration Screen

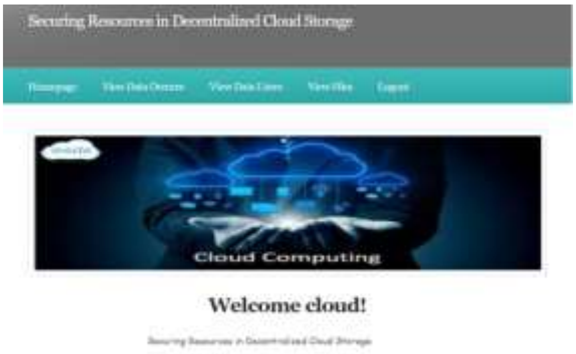
Username Sunil
Password ****
Contact No [illegible]
Email ID sunil@gmail.com
Address Ongole
Gender MALE
User Type Data User



Securing Resources in Decentralized Cloud Storage

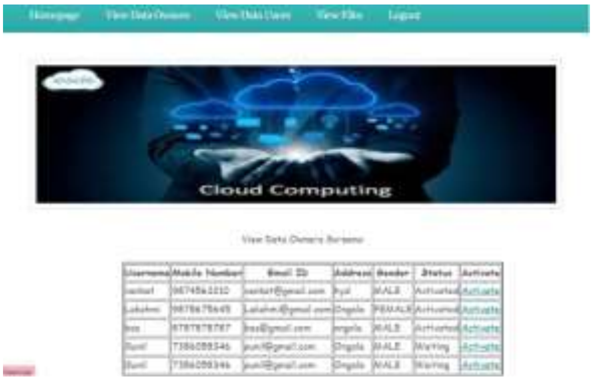
Cloud Service Provider

Username cloud
Password ****



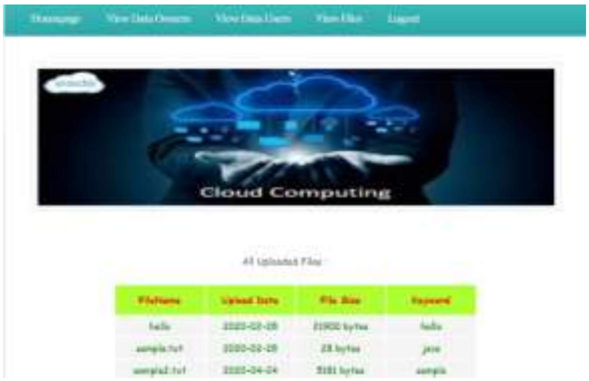
Welcome cloud!

Securing Resources in Decentralized Cloud Storage



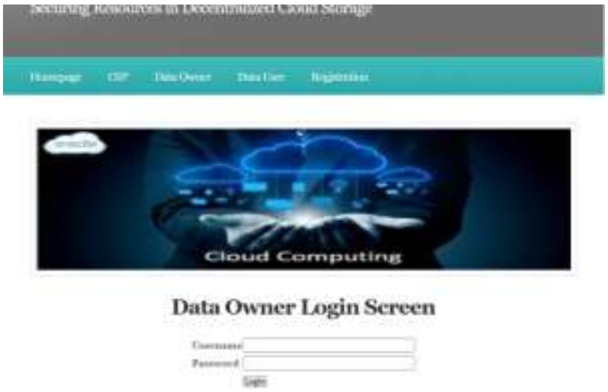
View Data Owners Screens

Username	Mobile Number	Email ID	Address	Gender	Status	Activate
santot	9874561210	santot@gmail.com	hyd	MALE	Activated	Activate
Lakshmi	9878675645	Lakshmi@gmail.com	Ongole	FEMALE	Activated	Activate
bas	8787878787	bas@gmail.com	ongole	MALE	Activated	Activate
Sunil	7386088346	sunil@gmail.com	Ongole	MALE	Waiting	Activate
Sunil	7386088346	sunil@gmail.com	Ongole	MALE	Waiting	Activate



All Uploaded Files

FileName	Upload Date	File Size	Keyword
hello	2020-02-28	21900 bytes	hello
sample.txt	2020-02-28	28 bytes	java
sample2.txt	2020-04-04	5181 bytes	sample

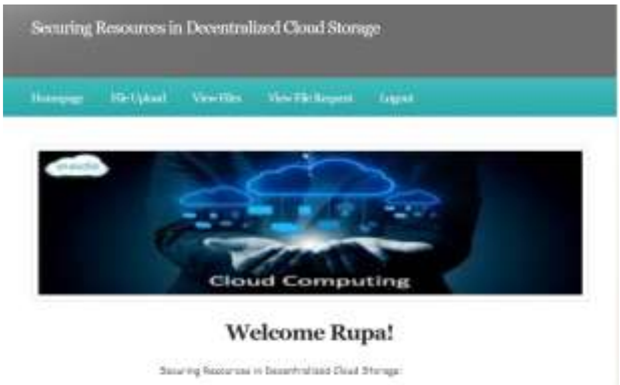


Data Owner Login Screen

Username

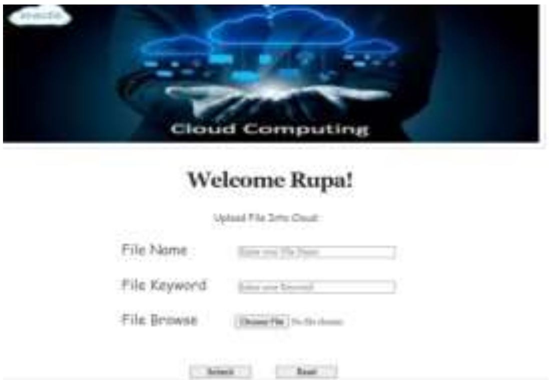
Password

Login



Welcome Rupa!

Securing Resources in Decentralized Cloud Storage



Welcome Rupa!

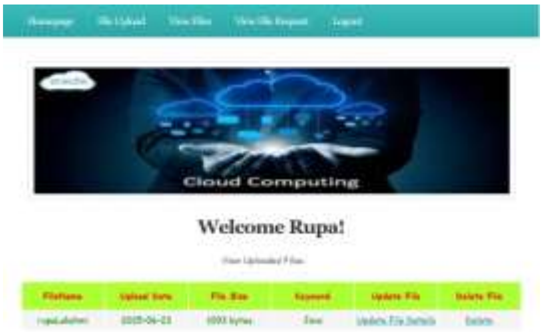
Upload File Into Cloud

File Name Enter your File Name

File Keyword Enter your Keyword

File Browse Choose File No file chosen

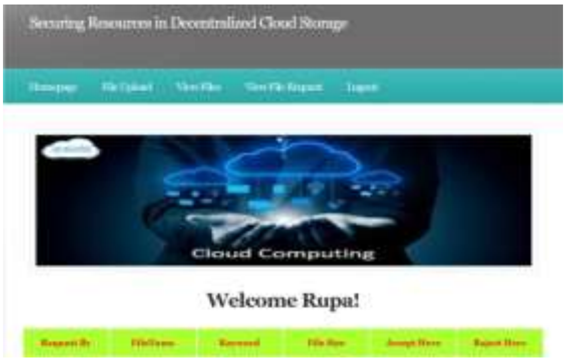
Submit Reset



Welcome Rupa!

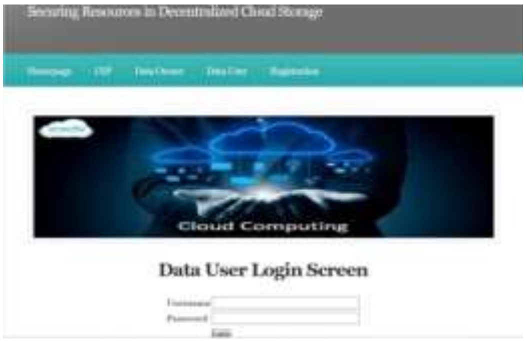
View Uploaded Files

FileName	Upload Date	File Size	Keyword	Update File	Delete File
rupaLakshmi	2025-06-23	1000 bytes	Java	Update File Details	Delete



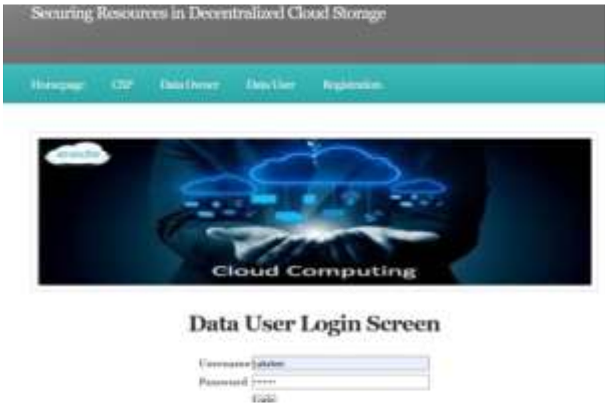
Welcome Rupa!

Request By	FileName	Keyword	File Size	Accept Here	Reject Here



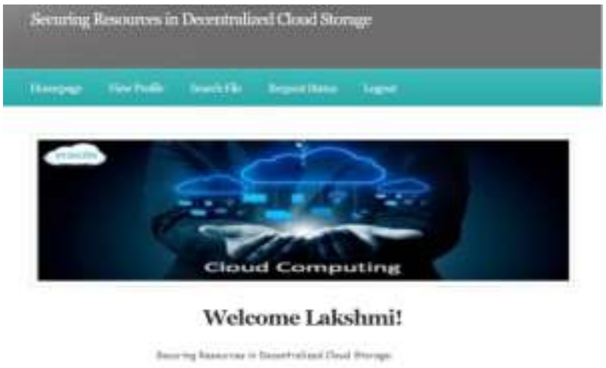
Data User Login Screen

Username
Password
Login



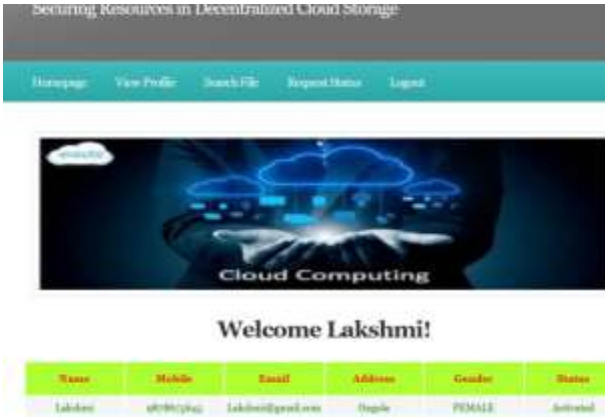
Data User Login Screen

Username lakshmi
Password ••••••
Login



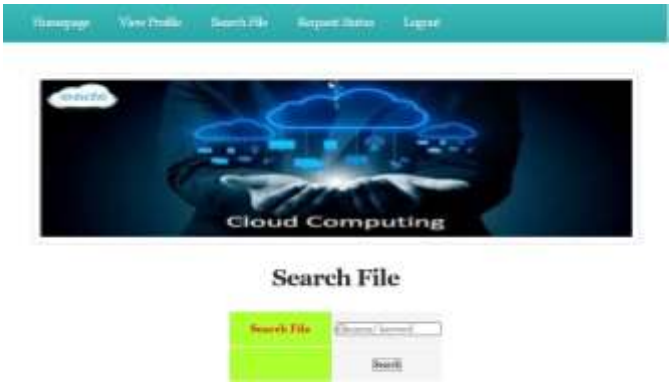
Welcome Lakshmi!

Securing Resources in Decentralized Cloud Storage



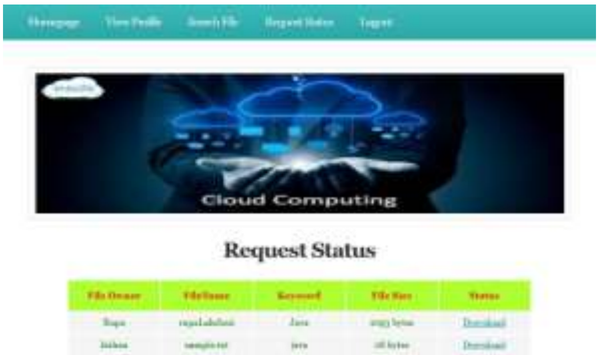
Welcome Lakshmi!

Name	Mobile	Email	Address	Gender	Status
Lakshmi	[illegible]	Lakshmi@gmail.com	Ongole	FEMALE	Activated



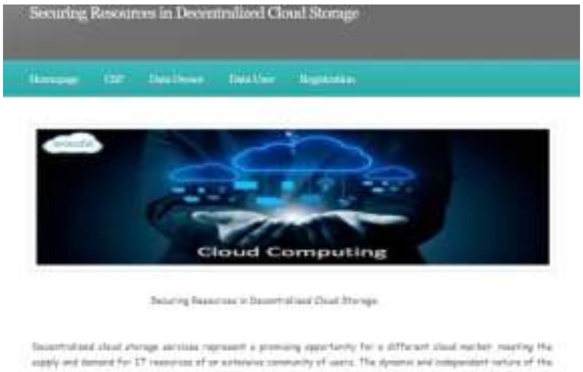
Search File

Search File
filename / keyword
Search



Request Status

File Owner	FileName	Keyword	File Size	Status
Rupa	rupalakshmi	Java	[illegible] bytes	Download
lakhmi	sample.txt	java	18 bytes	Download



Securing Resources in Decentralized Cloud Storage

Decentralized cloud storage services represent a promising opportunity for a different cloud market, meeting the supply and demand for IT resources of an extensive community of users. The dynamic and independent nature of the

Future Enhancement

As decentralized cloud storage continues to gain traction due to its advantages in data ownership, resilience, and cost-effectiveness, ensuring the security of stored resources remains a critical challenge. Future enhancements in this field are expected to focus on advanced cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, to protect data confidentiality and integrity without compromising usability. The integration of decentralized identity (DID) systems and blockchain-based access controls will enable more secure and transparent authentication mechanisms. Moreover, post-quantum cryptography will be essential to safeguard against future quantum computing threats. Artificial intelligence can also play a pivotal role in real-time threat detection and anomaly analysis, while secure multi-party computation (SMPC) and threshold cryptography can facilitate confidential collaboration and reduce the risk of single-point failures. Finally, immutable audit trails and smart contracts can enforce compliance, data sovereignty, and user-defined access policies across jurisdictions. These advancements collectively aim to build a robust, scalable, and secure decentralized storage ecosystem for the future.

Reference

[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 cloudstorage 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 vaultnetwork,” 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 overencrypted data in the database-service-provider model,” in Proc. of ACMSIGMOD, 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 arraysof 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 andintegrity layer for cloud storage,” in Proc. of ACM CCS, Chicago, IL,USA, November 2009.

[14] ——, “Proofs of retrievability: Theory and implementation,” in Proc. ofACM CCSW, Chicago, IL, USA, November 2009.

[15] M. Albanese, S. Jajodia, R. Jhawar, and V. Piuri, “Dependable andresilient cloud computing,” in Proc. of IEEE SOSE, Oxford, UK, March2016.

[16] A. Aldribi, I. Traore, and G. Letourneau, “Cloud slicing a new architecturefor 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 clustersin the

cloud," in Proc. of IEEE CloudCom, Singapore, December 2014.

[18] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, "Privacyrisk, 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 performancein 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: Towardstorage-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 publishingsystem based on document entanglements," in Proc. of ACM CCS,Philadelphia, PA, USA, November 2001.

Authors:

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning,Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

A. SUNEEL[2] is an MCA Scholar, Dept. of MCA, In QIS College of Engineering & Technology, Ongole. His areas of interest are Machine Learning, Deep Learning.