

Dynamic Storage Cost Optimization for Cloud Data Users

N.S. Usha, Associate Professor, S.A Engineering College, Chennai,
Tamil Nadu, India

Dept. of Computer Science Engineering, S.A Engineering College,
Chennai, Tamil Nadu, India

Abstract

Distributed storage Providers (CSPs) offer geologically information stores furnishing a few stockpiling classes with various costs. A significant issue looking by cloud clients is the way to abuse these capacity classes to serve an application with a period changing responsibility on its articles at least expense. This expense comprises private expense (i.e., capacity, Put and Get expenses) and potential movement cost. To address this issue, the first propose the ideal disconnected calculation that uses dynamic and direct programming strategies with the suspicion of accessible careful information on responsibility on objects. Because of the great time intricacy of this calculation and its prerequisite for deduced information, we propose two online calculations that make a compromise between private and movement costs and powerfully select capacity classes across Cloud Storage Providers. The important internet calculation is deterministic with no need for any information on responsibility and causes closeto

2 multiple times of the base expense acquired by the ideal disconnected calculation, where is the proportion of the private expense in the most costly information store to the least expensive one in one or the other organization or capacity cost. The next internet calculation is randomized that influences the "Receding Horizon

Control" procedure with the misuse of accessible future responsibility data for w time allotments. This calculation brings about all things considered 1 + w times the ideal expense.

1. Introduction

The item responsibility is controlled by how frequently it is perused (i.e., Get access rate) and composed (i.e., Put admittance rate). The Get access rate for the item transferred to an informal community is regularly high in the early life of the article and such article is supposed to be understood concentrated and in problem area status. Interestingly, over the long haul, the Get access pace of the article is diminished and it moves to the cool spot status where it is considered as capacity serious. A comparative pattern occurs for the Put responsibility of the item; that is, the Put admittance

rate diminishes as time advances. Subsequently, such applications use more organization than capacity in the early life of the article, and over the long haul, they utilize the capacity more than network.

2. Related works

Author Dr.C.Cartiban et al., in 2017 proposed "Analysis Database Confidentiality in the Cloud" and also finding opportunities for cloud architecture design for reporting into the data release system. Security is a major challenge in adapting a database to the cloud. The main purpose of the architecture is multi-user key distribution schemes, and it

also works under various assumptions of threat models[1]. Cost is also an issue for a cloud database. The main problem faced by this literature is that cloud security is an issue in which confidentiality, integrity, and authentication are key areas. Lack of responsibility leads to many conflicts between service providers and users. The location of data plays an important role in the security of cloud computing.

Author Ning Cao et al., in 2017 proposed the "Analysis for privacy-preserving multi-keyword ranked search over encrypted cloud data" data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings[2]. The problem faced is the potentially large number of data-on-demand users and

the huge number of external documents with data in the cloud, this problem is particularly challenging because it is extremely difficult to meet the performance, usability, and scalability requirements as well

Author Qingji Zheng et al., in 2014 proposed the "Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data" suggested that data owners often transfer your data to the cloud[3]. Since the cloud cannot be completely trusted, the outsourced data must be encrypted. However, this raises several questions, such as: How should the data owner provide the data users with search capabilities? How can authorized data users search for encrypted data outsourced to the data owner? The solution allows a data user whose credentials satisfy the data owner's access control policies to(i)

search for data outsourced to encrypted data owner data, (ii) submit tedious searches to the cloud, and (iii) check if searches are in progress. Formally define safety per WABKS requirements and describe the design that satisfiesthem.

Author Zhihua Xia et al., in 2014 proposed "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data" that with the growing popularity of cloud computing, more and more data owners are looking to transfer their data to cloud servers for greater convenience and lower data management costs[4]. However, sensitive data must be encrypted before outsourcing privacy requirements, making data use such as keyword-based document search obsolete. A secure multi-keyword ranked search scheme over

encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents.

Author Wenjing Lu et al., in 2014 proposed "Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud" encryption before outsourcing as a fundamental solution for protecting the privacy of user data in an unreliable cloud server environment[5]. In this document, we will focus on a different, but a more complex scenario in which an outsourced dataset can be provided by multiple owners and searchable by multiple users. We present the first Attribute-Based Keyword Search Scheme with Effective User Verification (ABKS-UR), which provides

scalable granular search authorization.

Author Qian Wang et al., in 2009 proposed "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance" suggested that distributed data storage is gaining popularity for efficient and reliable data management in wireless sensor networks (WSN). But distributed architecture also makes it difficult to build highly reliable systems[6]. Based on the principle of secret sharing and erasure coding, we first propose a hybrid scheme for creating and allocating shared resources to achieve reliable and fault-tolerant storage of the original data by providing redundancy for the original data components¹. The proposed scheme allows individual sensors in one version of the protocol to simultaneously check all

relevant data fragments in the absence of initial data.

Author Binanda Sengupta et al., in 2018 proposed, secure distributed cloud storage schemes provide reliable and permanent storage of this data on multiple servers[7]. We propose the idea of creating such a scheme for static data by encoding blocks of data (using error-correcting codes) and then attaching authentication information (tags) to these encoded blocks. We've identified some issues by expanding this idea to add-only data placement. Moreover, the client does not need to download any data (or parity) blocks to update the tags of the changed parity blocks residing on the servers.

Author Priyanka Maharu Salunke et al., in

2018 proposed Cloud services provide users with greater convenience to use cloud-based applications on-demand without considering the constraints of on-premises infrastructure[8]. During data access, different users can be in a collaborative relationship, and thus sharing data becomes essential to achieve productive benefits, propose a privacy-preserving authentication protocol (SAPA) based on shared authority to solve the above privacy issue for cloud storage.

Author Hong Liu et al., at 2014 proposed "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing" an interactive data paradigm for realizing user data remotely stored on a cloud-based online server[9]. Cloud services provide users with greater

convenience to use cloud-based applications on-demand without considering the constraints of on-premises infrastructure. The Universal Layout Model (UC) is designed to prove that SAPA is theoretically correct. The modern client security issue of cloud server anxiety to require elective clients for indirect sharing is the drawback in this document.

Author Huaqun Wang et al., at 2014 proposed "On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multi-cloud Storage" building an efficient PDP scheme for multi-cloud storage[10]. They investigated the existence of multiple CSPs for jointly storing and serving customer data. This means that an attacker can receive a reward without saving customer data. It is important to clarify the

scientific fact to develop a safer and more practical CPDP scheme.

Author Yuehai Xu et al., at 2012 proposed "Workload Analysis of a Large-Scale Key-Value Store" Key-value stores are a vital component of many scale-out businesses, including social media, online retail, and risk analysis [11]. They are receiving increased attention from the research community to improve their performance, scalability, reliability, cost, and power consumption. Designing and Implementing Any Storage or Caching the system must be optimized for its workload to be efficient.

Author Doug Beaver et al., at 2014 proposed "Finding a needle in Haystack: Facebook's photo storage" this document

describes Haystack, an object storage system optimized for the Facebook Photos app[12]. Facebook currently stores over 260 billion images, which means over 20 petabytes of data. The problem faced here is each image is stored in its file, a huge amount of metadata is generated at the storage layer due to namespace directories and files.

Author Yu Wu et al., at 2014 proposed "Scaling Social Media Applications into Geo-Distributed Clouds" The federation of geo-distributed cloud services is a trend in cloud computing that, spanning multiple data centers in different geographic locations, can provide a cloud platform with much greater capacity [13]. The issue is the system can recommend videos for users based on parameters such as user location, video types, metadata(tags),

popular searches, etc.
Specific Sample Social
Media Application –
YouTube.

Author Mohammad A. Salahuddin et al., at 2015 proposed "Social Network Analysis Inspired Content Placement with QoS in Cloud-based Content Delivery Networks" Content placement (CP) problem in cloud-based content delivery networks (CDN) exploits resource elasticity to create cost-effective CDNs that guarantee QoS [14]. To the best of our knowledge, this is the first model and heuristic of its kind that is timely and provides a fundamental pre-allocation framework for the future of online and dynamic resource provisioning for CCDN.

Author James Broberg in 2009 proposed "Metacdn Harnessing 'StorageClouds'

for high-performance content delivery" Akamai and Mirror Image are hosting web server clusters in multiple geographic locations to improve responsiveness and localization of the content they host to end-users[15]. However, the prices for their services are not affordable for all but the largest corporate clients.

3. Proposed system

To tackle the minimization of cost problem and to get the required cloud space problem, cloud users are required to answer two questions: (i) which storage class from which CSP should host the object and (ii) when the object should probably be migrated from a storage class to another owned by a similar or different CSPs.

None of these studies investigated the trade-off between network and storage costs to optimize the cost of

replication and migration data across multiple CSPs.

It is not always feasible and may lead to inaccurate results, especially in the following cases:

(i) when the prediction methods are deployed to

predict workloads in the future for a long term (e.g., a year)

(ii) for start-up companies that have limited or no history of demand data

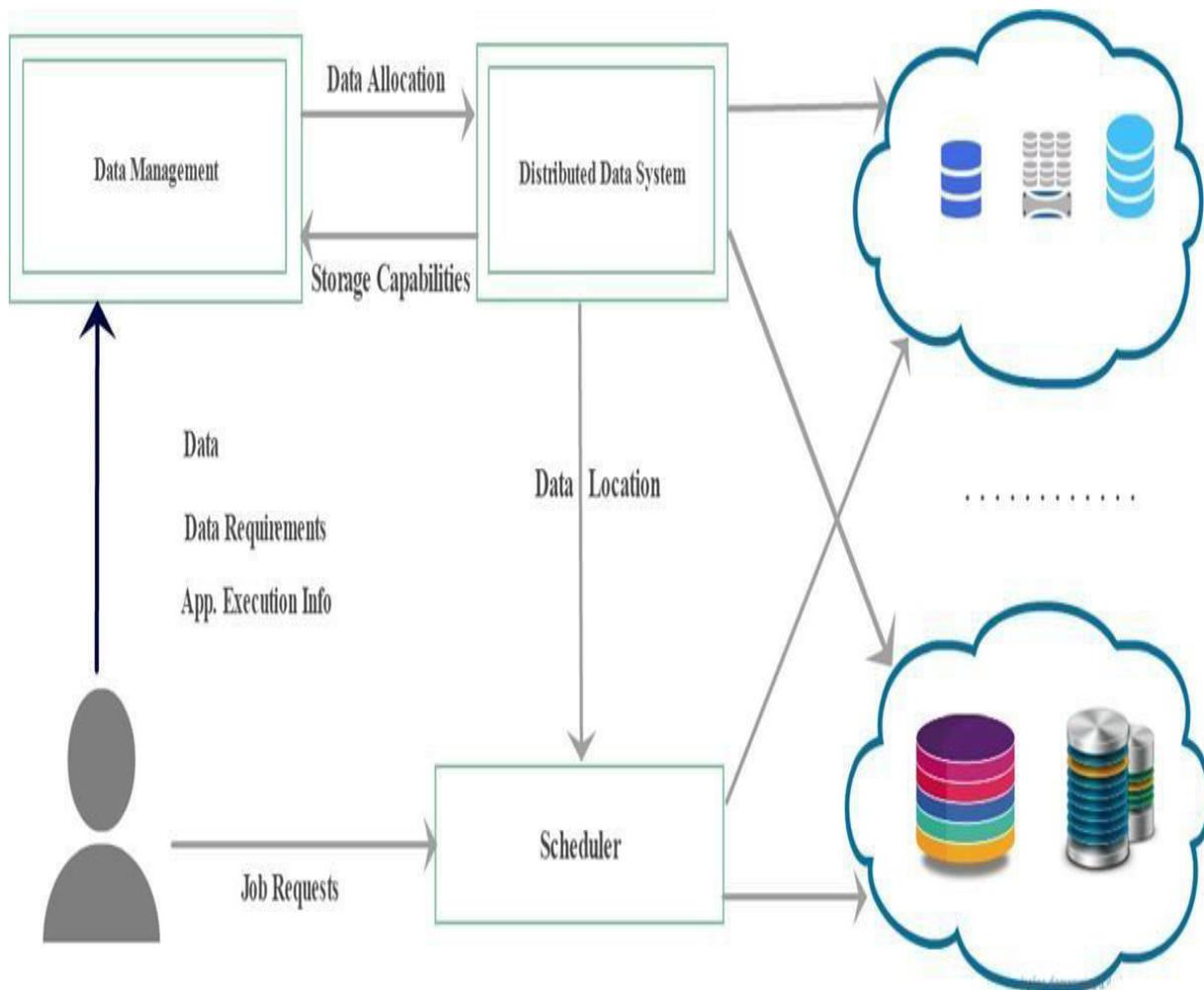


Fig 1. Architecture Diagram

Introduction about related work:

The below table consists of Existing system's literaturesurvey papers of cloud data with improving mechanisms.

4. Comparision of relatedworks

Year	Mechanism	Pros	Cons
2018	Privacy Preserving Data Storage Technique in Cloud Computing	Usability & Accessibility. Users can easily drag and drop the files in cloud storage.	Devour more opportunity to examine the information.
2017	Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data	It motivates to improve flexibility and economic savings	Have limited computation and memory resource
2014	Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data	It is for static data	It is not for dynamic data
2015	A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted CloudData	Deletion and insertion process is done simultaneously	Time cost was high
2014	Protecting Your Right: Attribute-based Keyword Search with	It allows multiple users to encrypt and send	May be not secure against adaptive attacks

	Fine-grained Owner-enforced Search Authorization in the Cloud	data independently	
2009	Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance	It ensures integrity of distributed data shares	Not highly secure and efficient
2018	An Efficient Secure Distributed Cloud Storage for Append-only Data	It enables the servers to update parity blocks by themselves	Time consuming process
2018	Secure Data sharing in Distributed Cloud Environment	The energy is reduced slowly	Intruder's attacks in private data
2014	Shared Authority Based Privacy-preserving authentication Protocol in Cloud Computing	Proposed protocol is attractive for multi users	Difficult to develop the framework.
2014	On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multi cloud Storage	It can pass verification even if stored data is deleted	Problem to design secure and efficient CPDP scheme for integrity verification in multi cloud storage.
2012	Workload Analysis of a Large-Scale Key-Value Store	It has strong locality measures	Requires more memory.
2010	Finding a needle in Haystack: Facebook's photo storage	It increases overall throughput	It brings about an over top number of circle activities due to metadata queries.

2014	Scaling Social Media Applications into Geo-Distributed Clouds.	It predicts future demand	It is ideal for supporting large-scale social media applications with dynamic contents and demands.
2014	Social Network Analysis Inspired Content Placement with QoS in Cloud-based Content Delivery Networks	It minimizes the degree of QoS violations	The CP problem is NP Hard problem.
2018	On Optimizing Replica Migration in Distributed Cloud Storage Systems.	It minimizes replica creation time	Reproduction position frameworks for the most part need to move and make countless information

5. Modules:

CLOUD SERVICE PROVIDER

Cloud Service provider to provide the service to user. User register the details to service provider before send the file. After user registration admin verify the user profile and accept the user request. Admin may be reject the Unauthorized profile details.

USER UPLOAD

After admin verify the user details, User to upload the file to cloud server. While upload the file, files are encrypted and stored in the database and folder. While upload the data are split and store the three server. Because hacker, cannot not hack server data. Because data parts are stored

in three servers. Key gen algorithm used in data upload and encrypted.

FILE CONVERT

While uploading data to server all data are in zip format for reduce the file occupy memory. It uses lossless data compression algorithm (Huffman's algorithm).

AUTHORIZED USERS

Authorized users, these users only to download the file from the others users. These users to send the file request to admin and file owner.

FILE REQUEST

User may be share the our files to another users. Shared users to fetch the file from file owner. Shared user

to send the file request to file owner and automatically same request send to admin. Then Admin verify the server and provide the clearance to provide the key from file owner. After file owner to send the temporary key to shared users. if shared users download the shared file the temporary key automatically expire.

FILE RECOVERY

If user file may be corrupt or may be delete. So if user delete any file from server, user can recover the deleted files from file sever. It is very useful to all cloud users. If user to recover the deleted file, user login and get the deleted files.

6. Screenshots

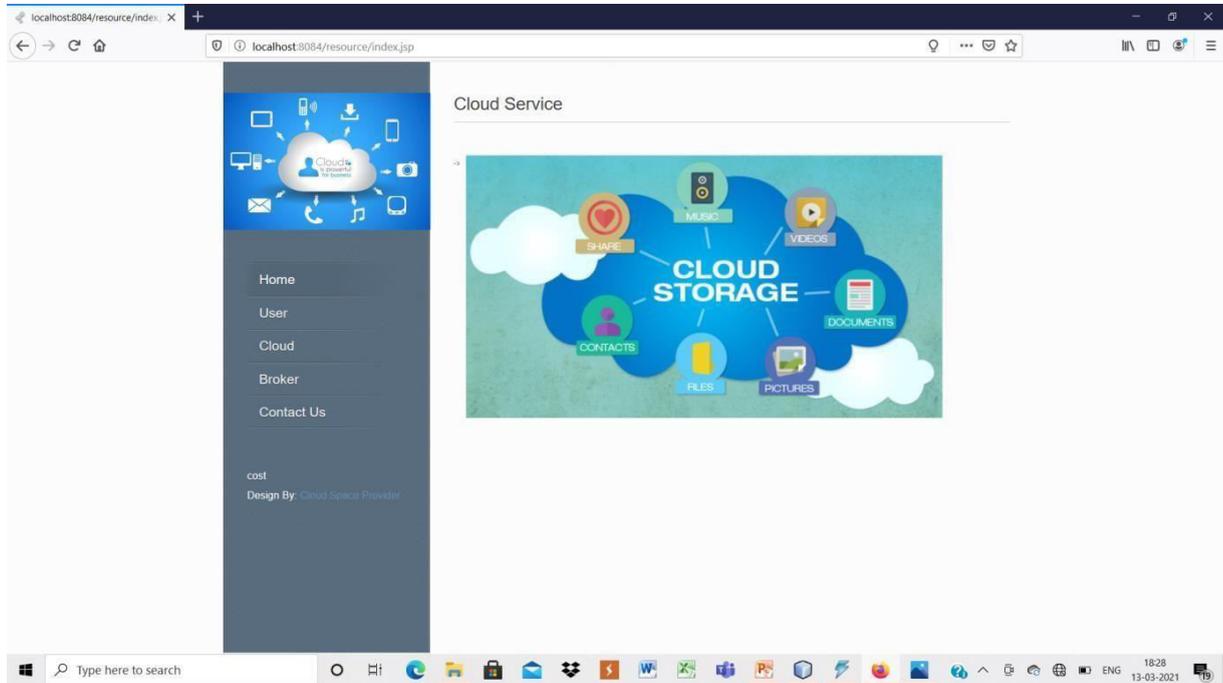


Fig 6.1 Home Page

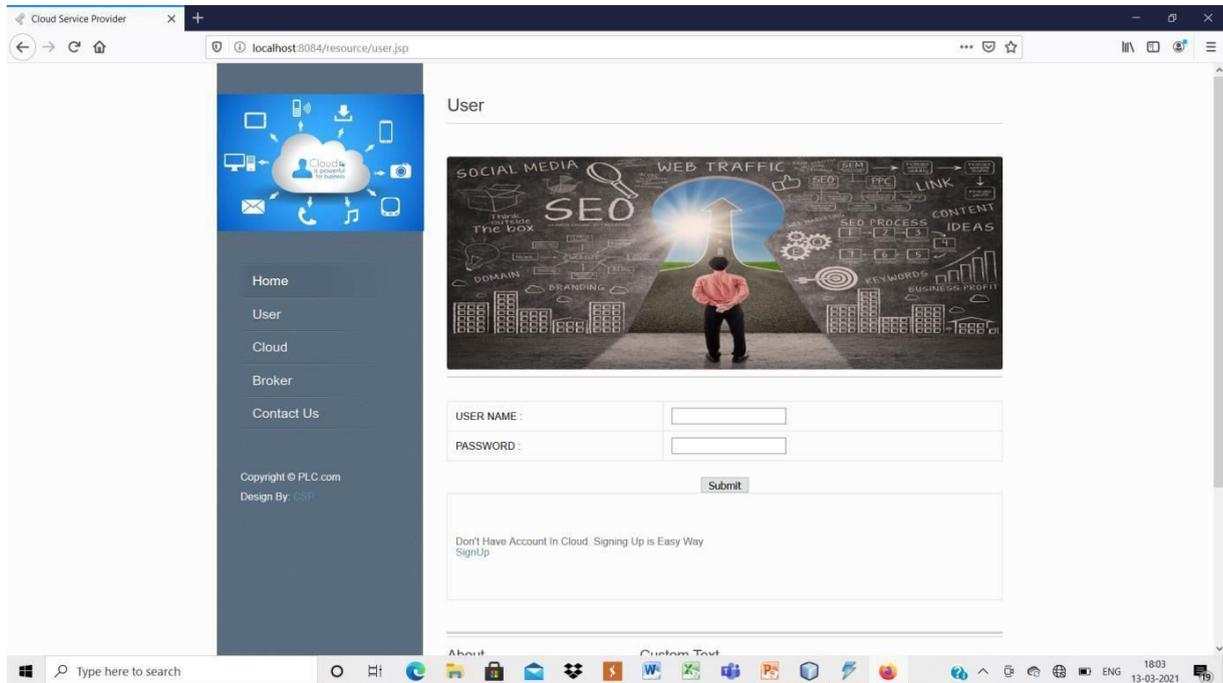


Fig.6.2 User Page

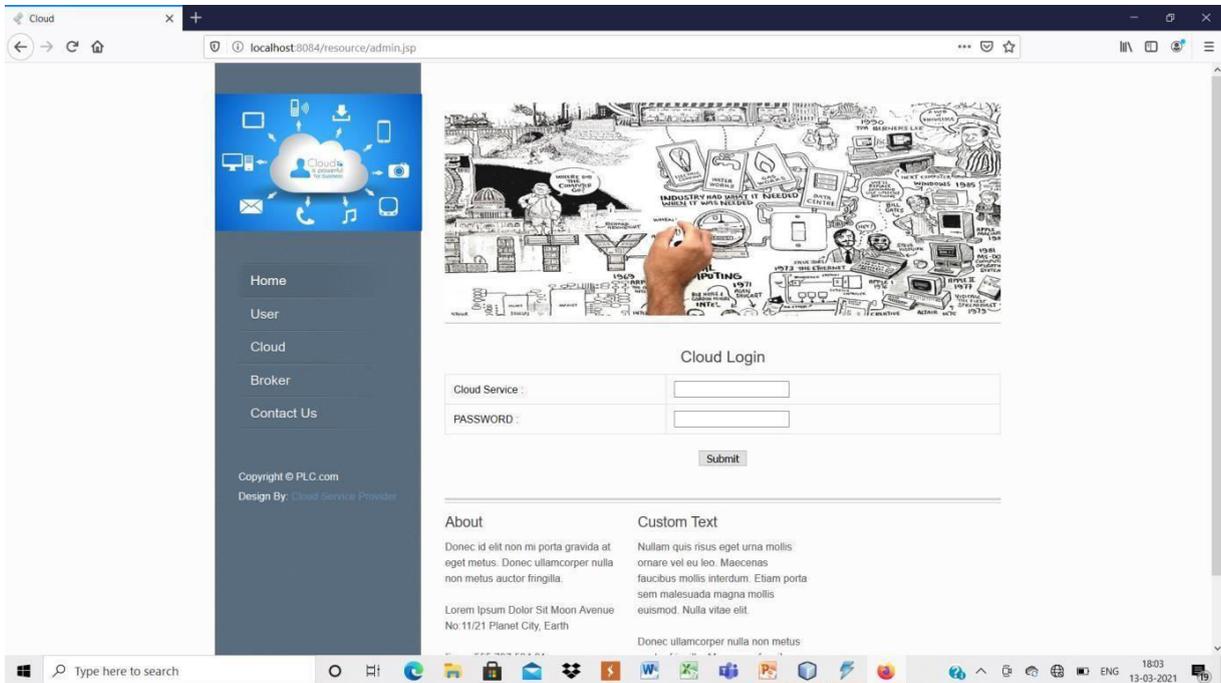


Fig 6.3 Cloud Page

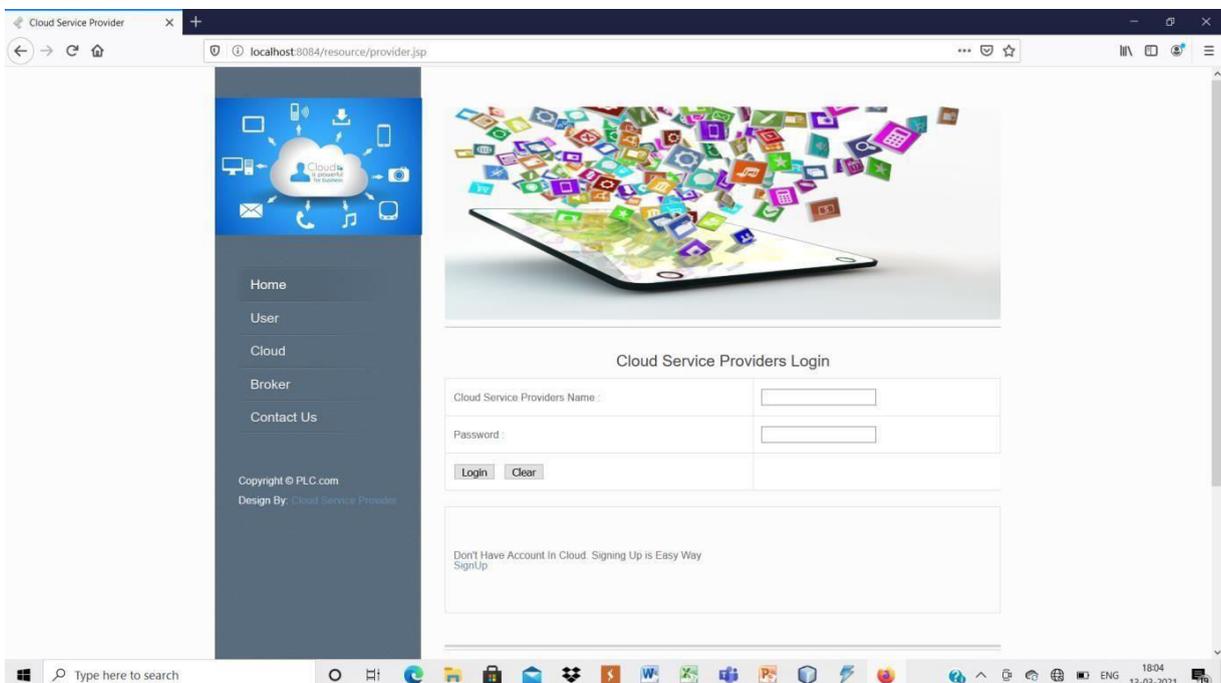


Fig 6.4 Broker Page

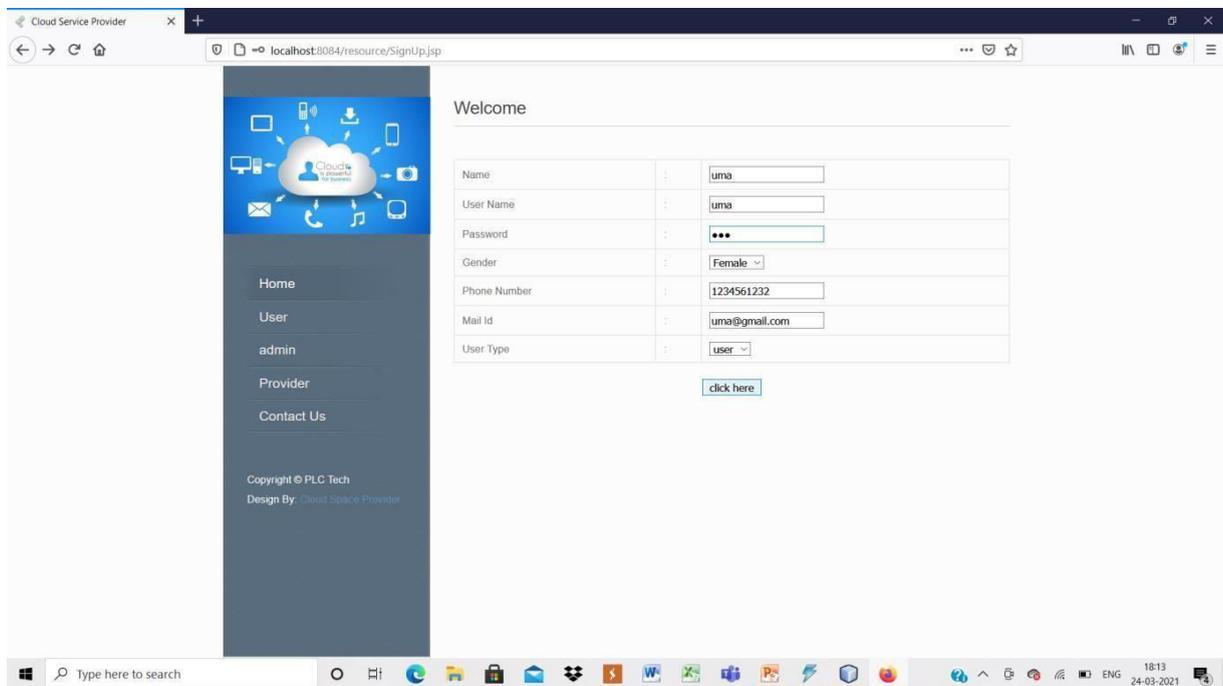


Fig 6.5 User Registration

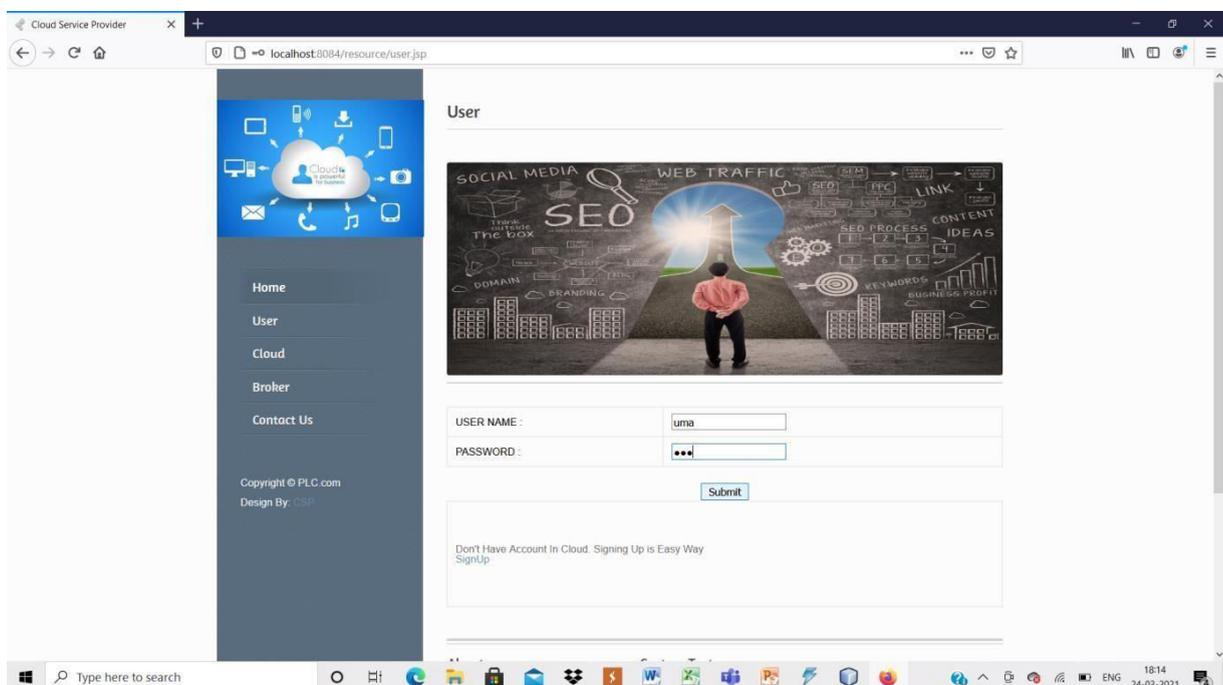


Fig 6.6 User Login

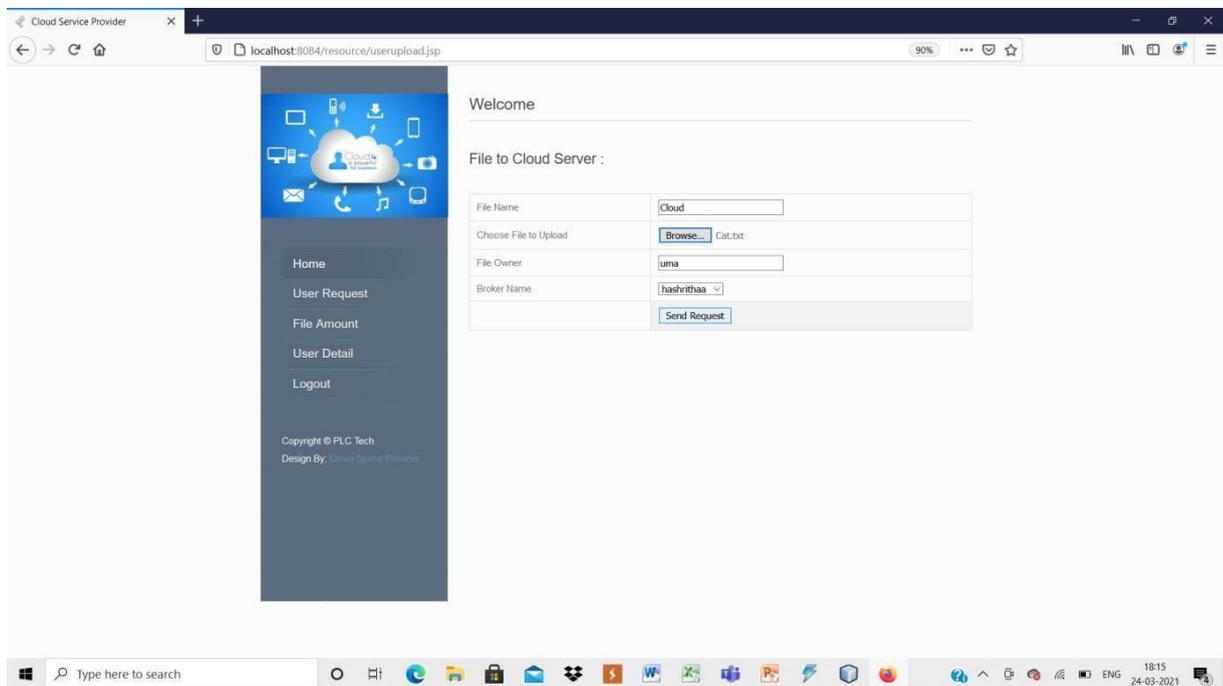


Fig 6.7 Send Request to Broker

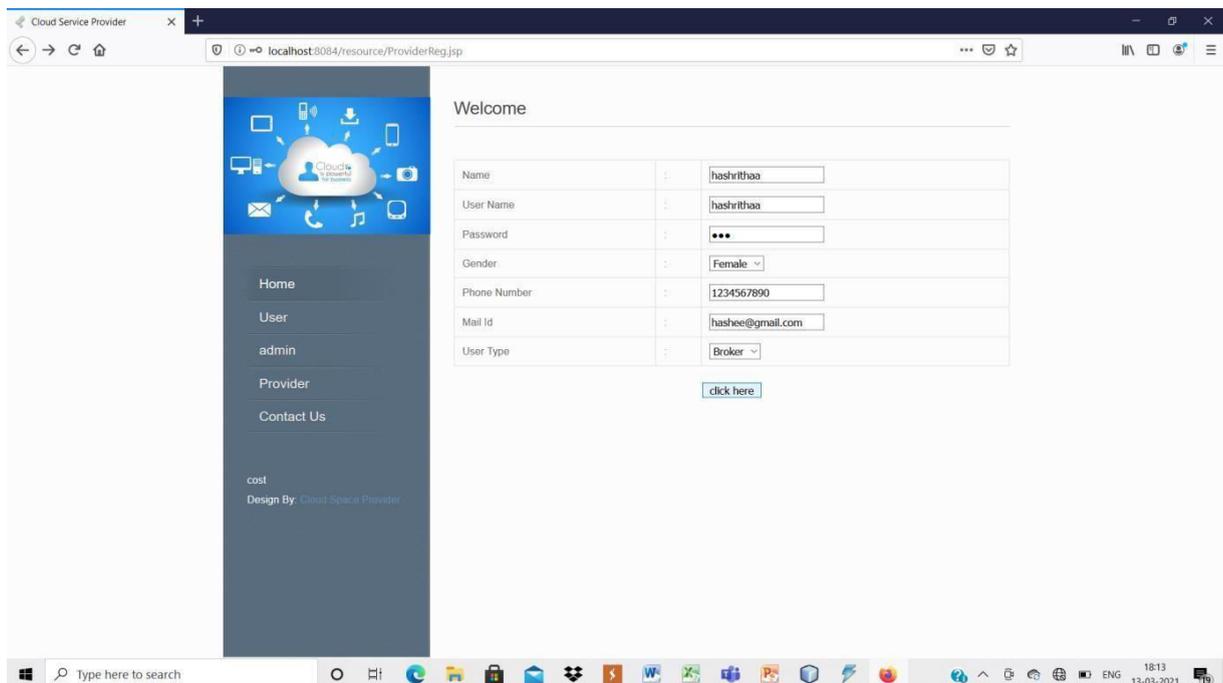


Fig 6.8 Registering for Broker

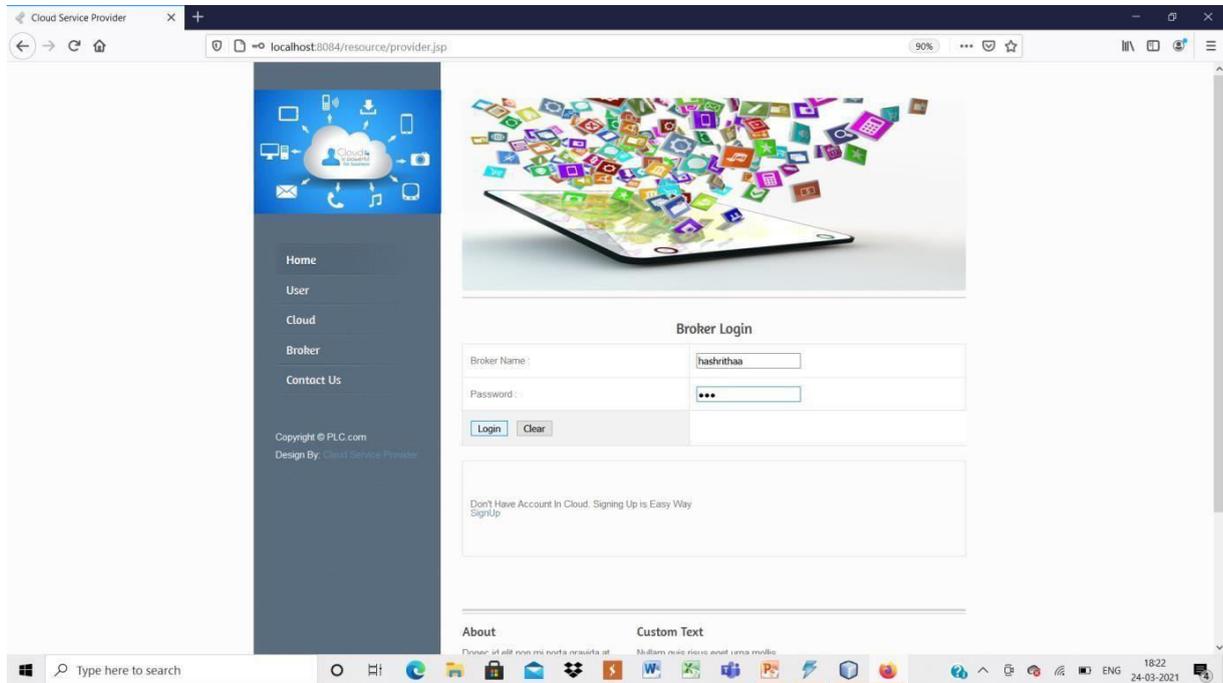


Fig 6.9 Broker Login

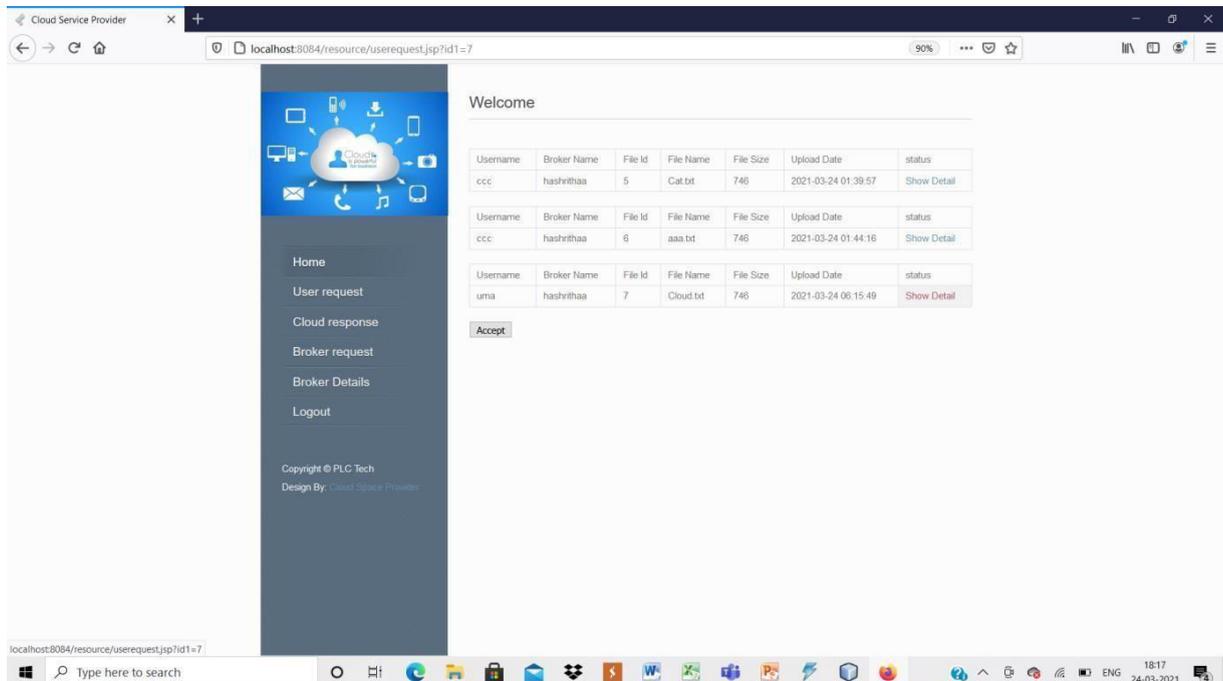


Fig 6.10 Accepting User Request

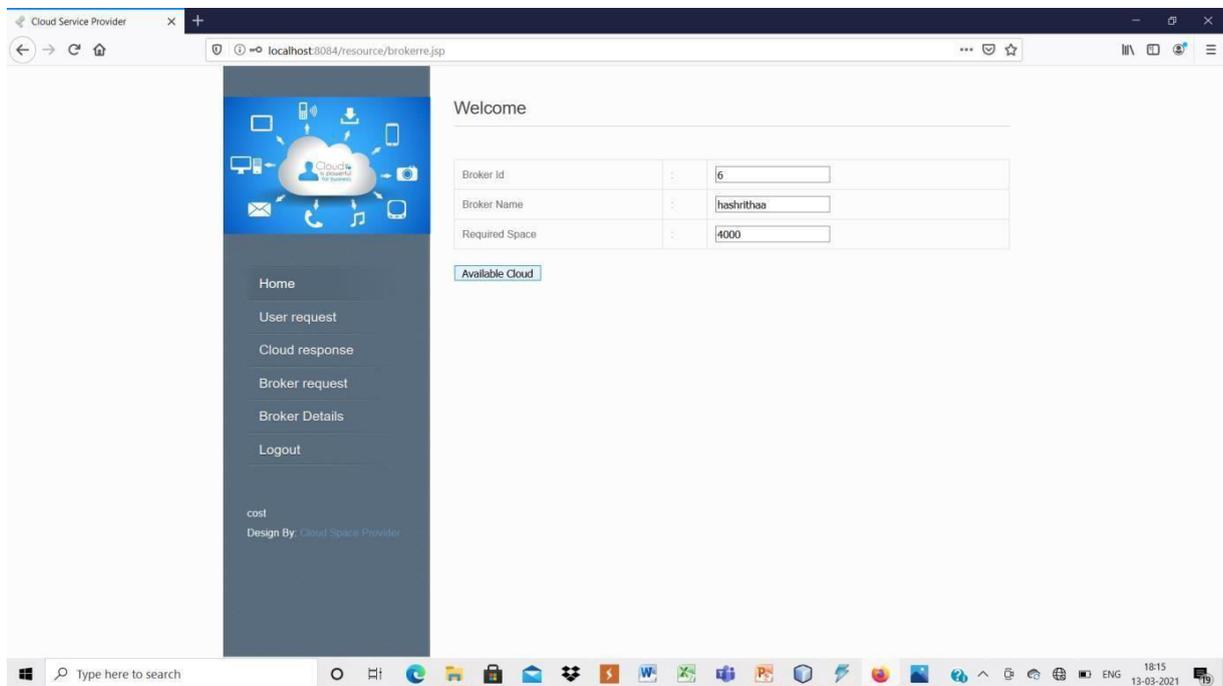


Fig 6.11 Requesting for Space to Cloud

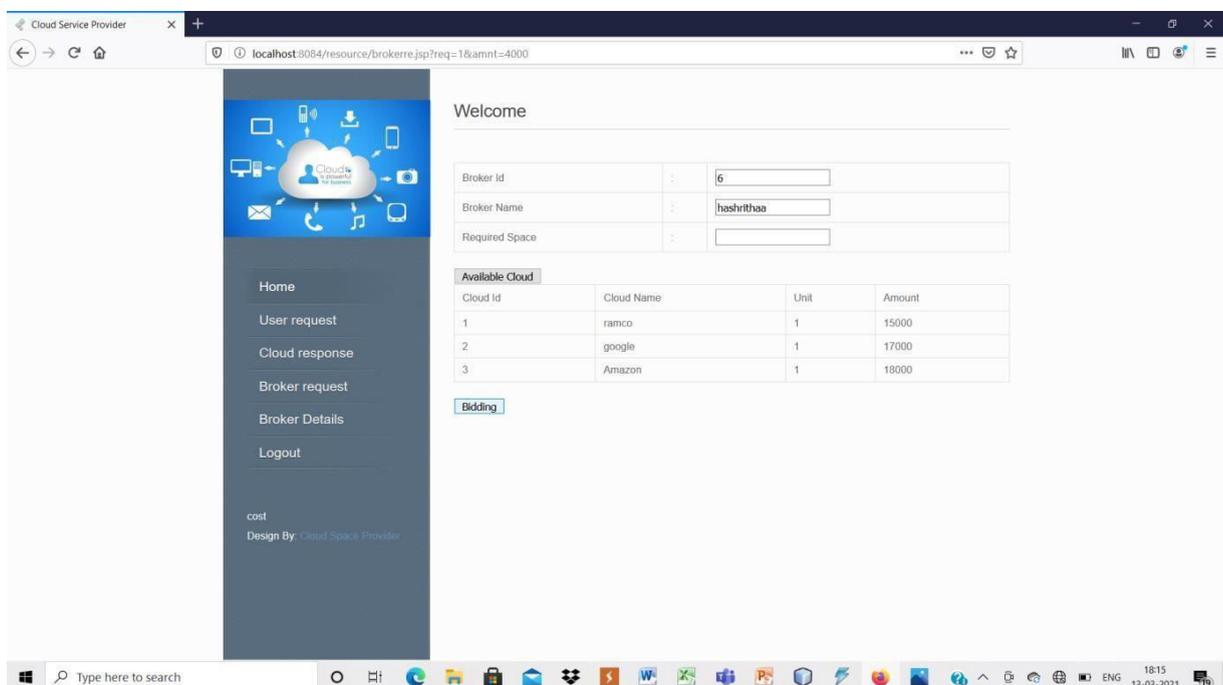


Fig 6.12 Showing Available Cloud

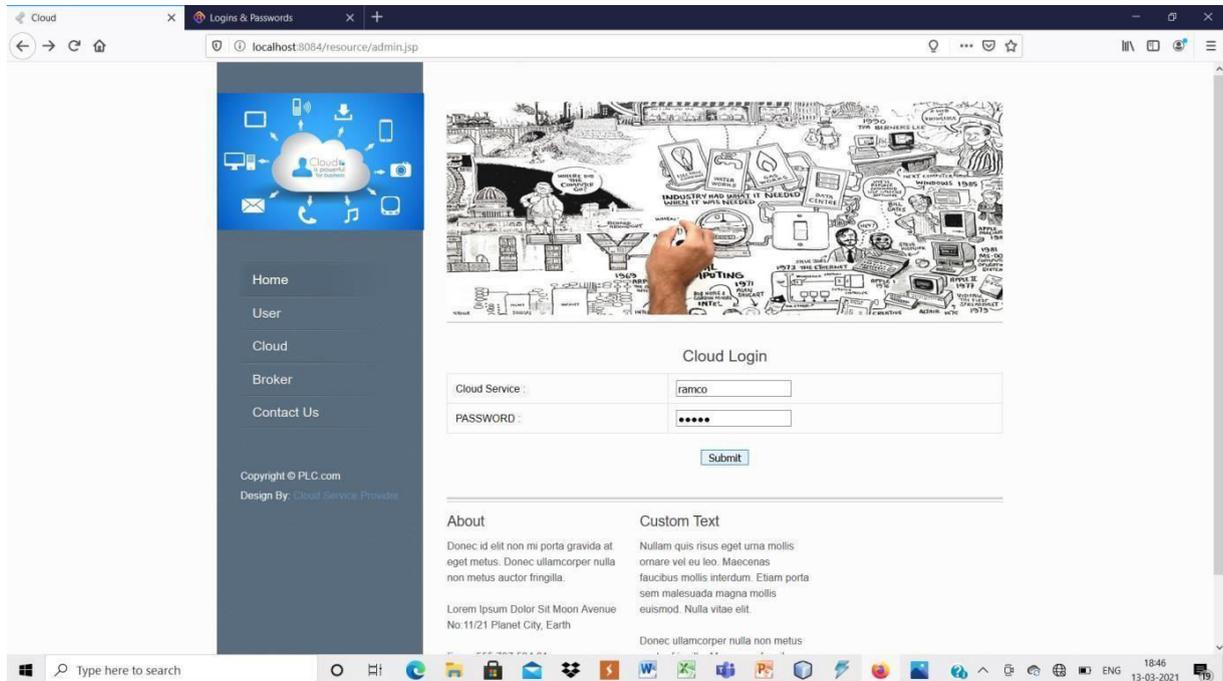


Fig 6.13 Cloud Login

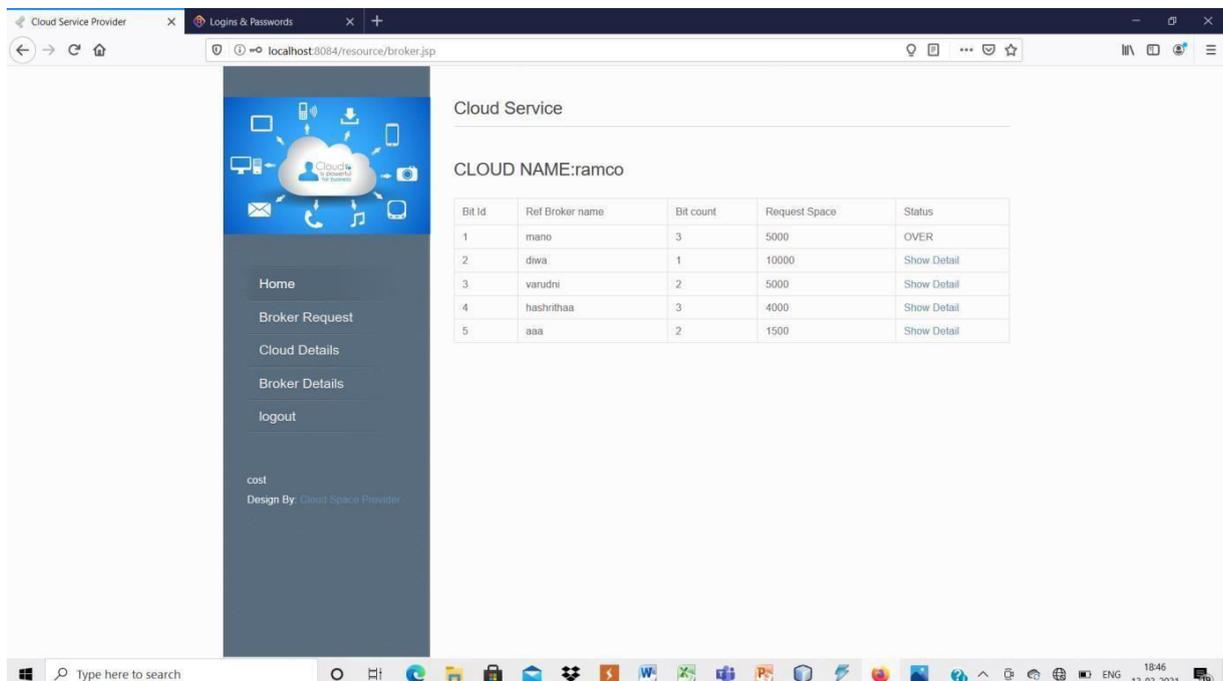


Fig 6.14 List of Broker's Request

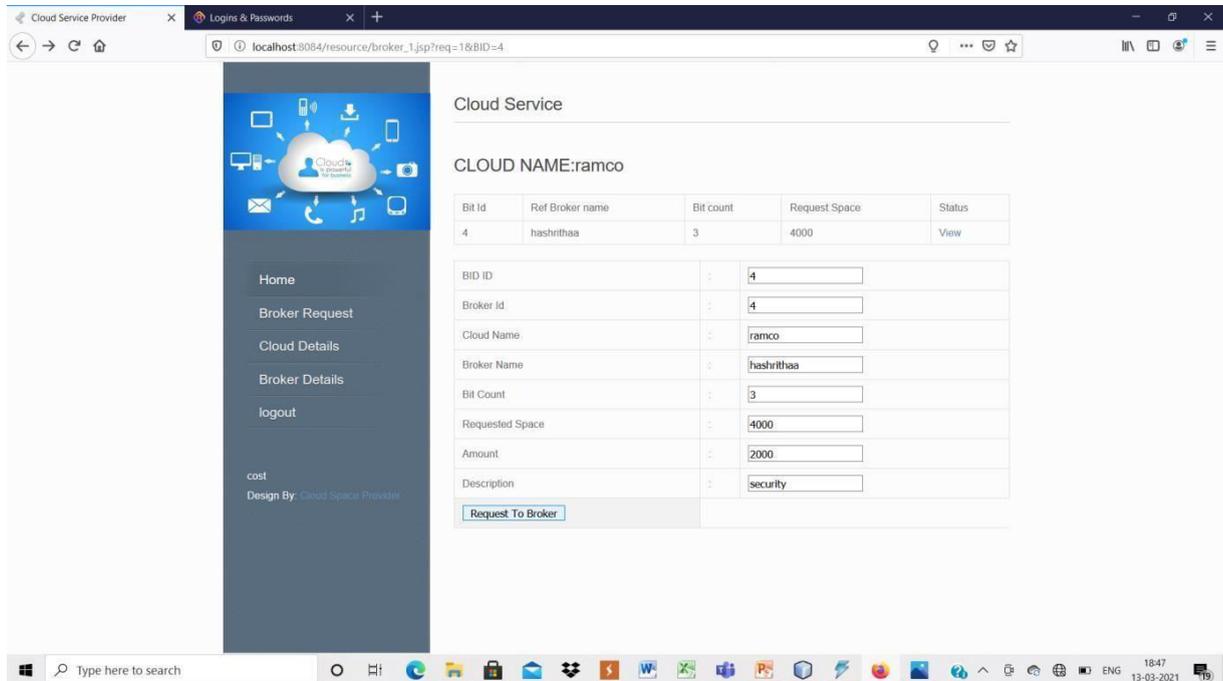


Fig 6.15 Entering the Amount

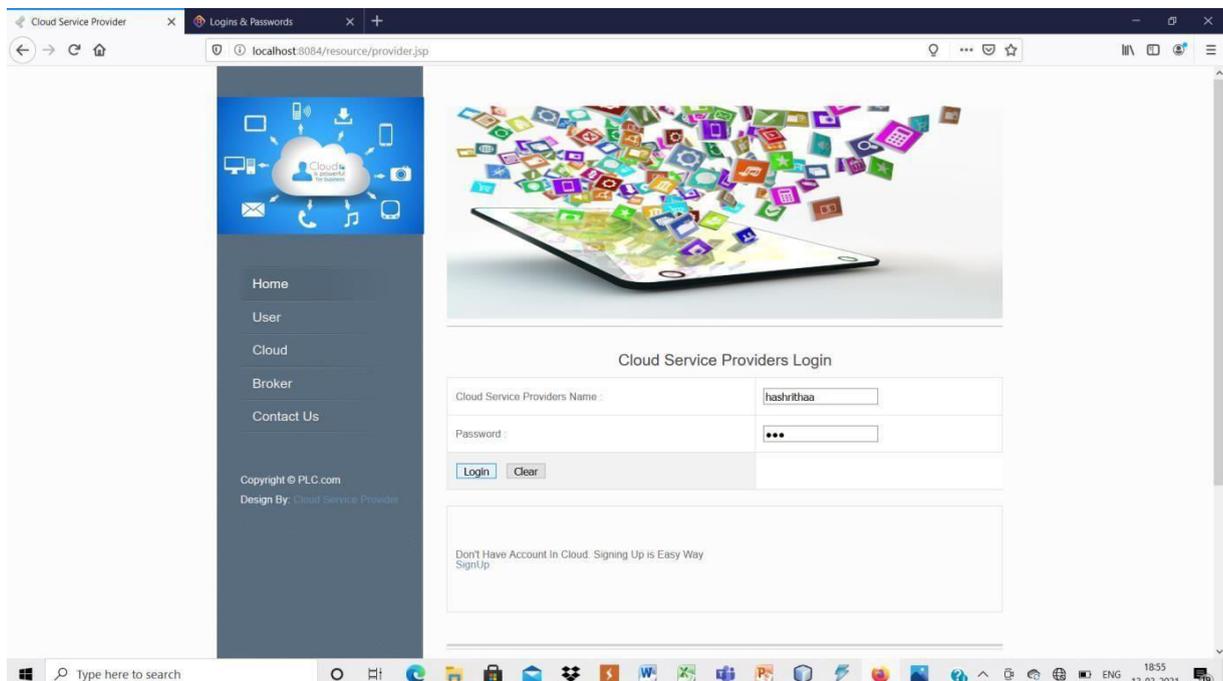


Fig 6.16 CSP Login

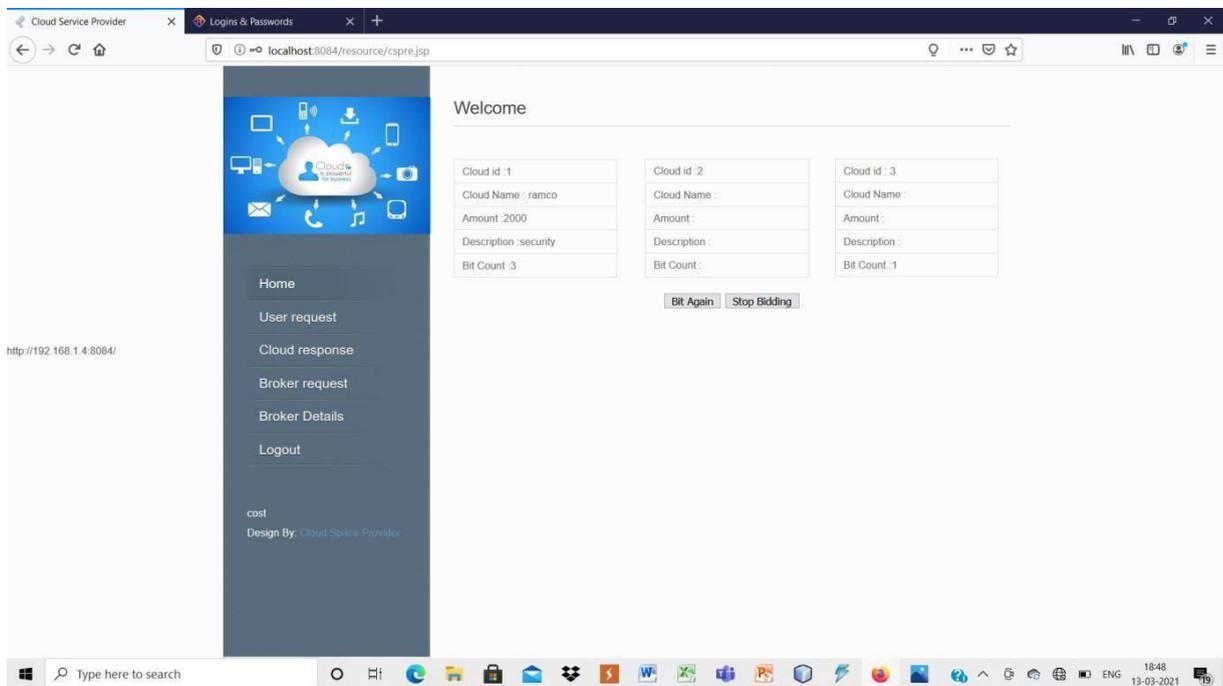


Fig 6.17 Stop Bidding

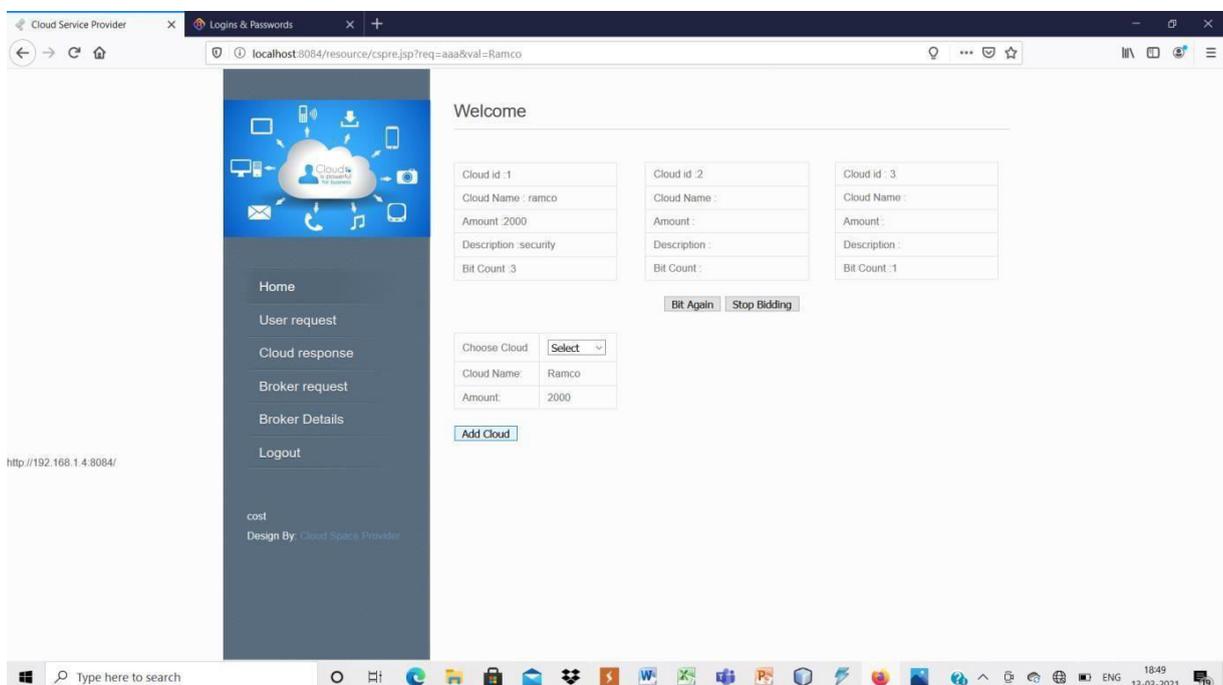


Fig 6.18 Selecting Cloud

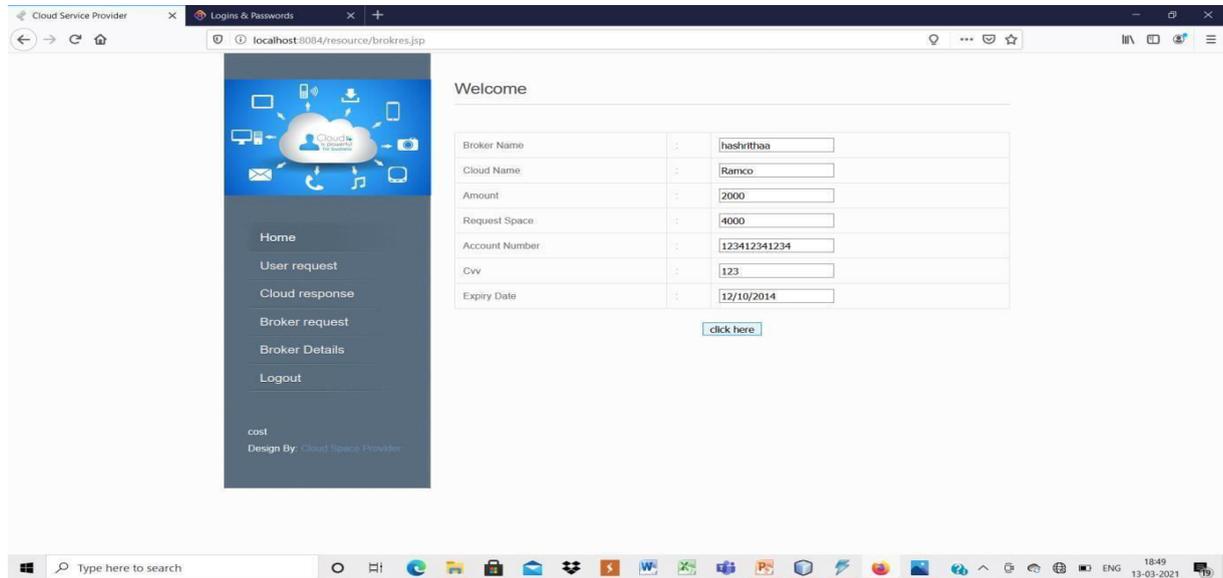


Fig 6.19 Payment

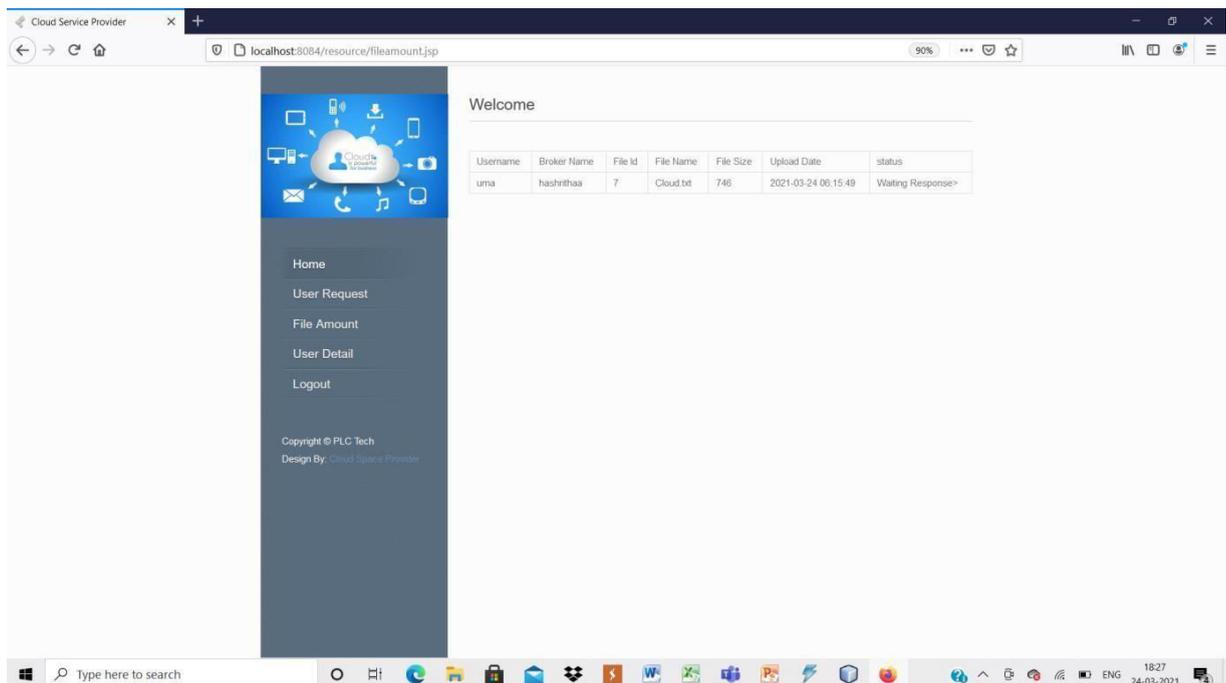


Fig 6.20 Viewing File amount in user login

7. Conclusion

To limit the expense of information arrangement for time-changing responsibility applications, engineers should ideally abuse the prize distinction among capacity and organization administration across different CSPs.

In future work, we wanted to propose calculations in which the mentioned availabilities of an item regarding the number of nines are additionally thought of.

8. References

- [1] Dr. K. Kartheeban and A Durai Murugam. Privacy Preserving Data Storage Technique in Cloud Computing. IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2018.
- [2] Ning cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems (Volume: 25, Issue: 1, Jan. 2014), 2017.
- [3] Qingji Zheng, Shouhuai Xu and Giuseppe Ateniese. Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 2014.
- [4] Zhihua Xia, Xinhui Wang, Xingming Sun, Qian Wang. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud

- Data. IEEE Transactions on Parallel and Distributed Systems (Volume: 27, Issue: 2, Feb. 1 2016), 2015.
- [5] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou, Hui Li. Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud. IEEE Conference on Computer Communications, 2014.
- [6] Q. Wang, K. Ren, W. Lou, Y. Zhang. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance. IEEE INFOCOM 2009.
- [7] Binanda Sengupta, Nishant Nikam, Sushmita Ruj, Srinivasan Narayanamurthy, Siddhartha Nandi. An Efficient Secure Distributed Cloud Storage for Append-only Data. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.
- [8] Priyanka Maharu Salunke, Vishal. V. Mahale. Secure Data sharing in Distributed Cloud Environment, 2018.
- [9] Hong Liu, Huansheng Ning, Qingxu Xiong, and Laurence T. Yang. Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing. IEEE Transactions on Parallel and Distributed Systems (Volume: 26, Issue: 1, Jan. 2015), 2014.
- [10] Huaqun Wang and Yuqing Zhang. On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage. IEEE Transactions on Parallel and Distributed Systems

(Volume: 25, Issue: 1, Jan. 2014).

[11] Berk Atikoglu, Yuehai Xu. Workload Analysis of a Large-Scale Key-Value Store. ACM SIGMETRICS Performance Evaluation Review, June2012.

[12] Doug Beaver, Sanjeev Kumar, Harry C. Li, Jason Sobel. Finding a needle in haystack: Facebook's photo storage," in Proceedings of the 9th USENIX Conference on Operating, Systems Design and Implementation, ser. OSDI'10. Berkeley, CA, USA:USENIX Association,2010.

[13] Yu Wu, ChuanWu, Bo Li, Linqun Zhang. Scaling socialmedia

applications into geo distributed clouds," IEEE/ACM Trans. Netw., vol. 23, June2015.

[14] Mohammad A. Salahuddin, Halima Elbiaze, Wessam Ajib and Roch Glith. Social Network Analysis Inspired Content Placement with QoS in Cloud Based Content Delivery Networks. ,2015.

[15] James Broberga, Rajkumar Buyyaa, Zahir Tarib. MetaCDN Harnessing 'Storage Clouds' for high performance content delivery. Journal of Network and Computer Applications Volume 32, Issue 5, September2009.

