iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40999

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Multi Cloud Data Hosting with SIC Architecture

Amit V. Munde[1], Dr. Pranjali P. Deshmukh[2]
[1, 2]*Information Technology Department, Sant Gadge Baba Amravati University*

Abstract: ***Data hosting on cloud decreases cost of IT maintenance and data reliability get enhance. Nowadays, customers can store their data on single cloud, which has some drawbacks. First is vendor lock in problem and second is security on cloud. The solution to this problem is to store the data on different cloud server without redundancy using encryption algorithm. Customers do not want to lose their sensitive data on cloud. Another issue of cloud computing is data thievery should be overcome to supply higher service. Multi-cloud environment has ability to scale back security risks. To avoid security risk we offer framework.***
Keywords: Cloud computing, cloud storage, data hosting, data intrusion, multi-cloud, single cloud.

I. INTRODUCTION

Cloud computing can be a virtualized resources that allows user to gain access in web base environment on demand. in a cloud computing environment, people and businesses work with applications and data hold on and/or maintained on shared machines in a internet environment instead of physically situated within the home of a user or as company [2] environment. More and more enter-prices and organizations are hosting all or part of their data into the cloud, in order to reduce the IT maintenance cost and enhance the data reliability [3], [4], [5].

In multi cloud data Storage, data and information are shared with external users, so cloud computing users need to avoid vital information from attackers or malicious business executive is of essential importance. Users are responsible for protecting operating system and cloud providers must provide protection for user's data. Resources within the cloud are accessed through the net, oftentimes even though the cloud supplier concentrates on security within the cloud infrastructure; the information continues to be transmitted to the users through networks which may be insecure. So the basic motivation behind this is-

1) To use SIC Secure-Inter-Cloud Architecture. It is three-tier architecture. There is one CSP i.e. Cloud Service Provider.
2) This is the main central server which keeps the data about clients. Clients/users do not have any idea about where exactly the data/files have been stored.
3) Data is stored in cloud server. The servers may reside in different physical locations. The CSP decides the servers for data storage depending upon available spaces.
4) This implementation uses load balancing algorithms for making the decision, on which server we should actually store the data. The CSP will also keep track about the files stored on each server. The cloud servers will only store the data, but they will not have any records about the user accounts, their passwords or encryption and decryption keys. [7].

II. PROPOSED DESIGN

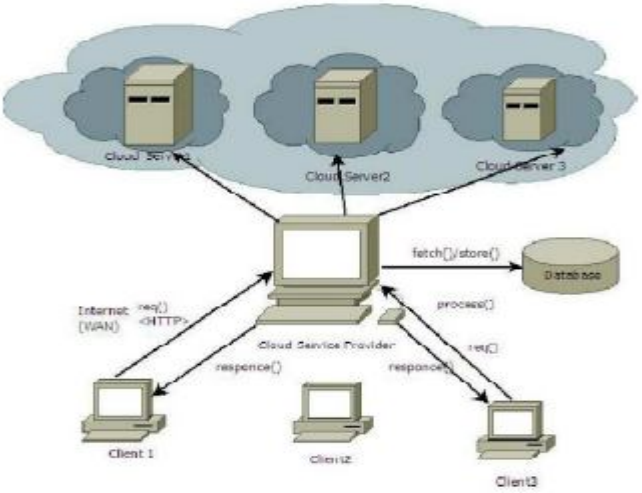


Fig.1 SIC Architecture

SIC - Secure Inter-Cloud Architecture. The proposed architecture is the 3 tier architecture. There is one CSP in architecture i.e. cloud service provider. This is main server which keeps the client's data. Any cloud service user can be represented by client in figure . Clients/users do not have any idea about where exactly the data/files has been stored. Data is stored in cloud server. The servers may located in different physical locations. The CSP decides the servers for storage of data depending upon available spaces. The CSP will also keep watch on the files stored on each server. The cloud servers will only store the data, but they will not have any records about the user accounts, their passwords or encryption and decryption keys.

CSP is central server, it must be well configured. Care should be taken for protection of CSP. Cloud service provider acts as an effective bridge between the user and cloud server. Cloud users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

A. Working and Results of Proposed System

The working system implements the concept of multiple clouds and provides data security with RSA algorithm. When user wants to upload the data to system then the data get encrypted with private key. And when user wants to download the data from the system then with help of public key, the data get decrypted and downloaded from the system. Also this system implemented CSP module which will give the guarantee to the client of cloud that their document will be safe on server and if any unauthorized access happen on server then CSP rectify problem very first.

Fig 2 shows login form for user authentication. User can authenticate their self with username and password. Once authentication of user is done this user dashboard get open as shown in Fig. 3 when user clicks on folder the folder get opened and then users are allowed to upload and download the file from folder. When user get authenticate their self, the public and private keys are generated dynamically as shown in Fig. 4. If user wants to upload the file to the server then he/she has to enter the private key to encrypt the file as shown in Fig. 5. And if user wants to download the file from the server then he/she has to enter the public key to decrypt the file as shown in Fig. 6. The encrypted format is shown in Fig 7.

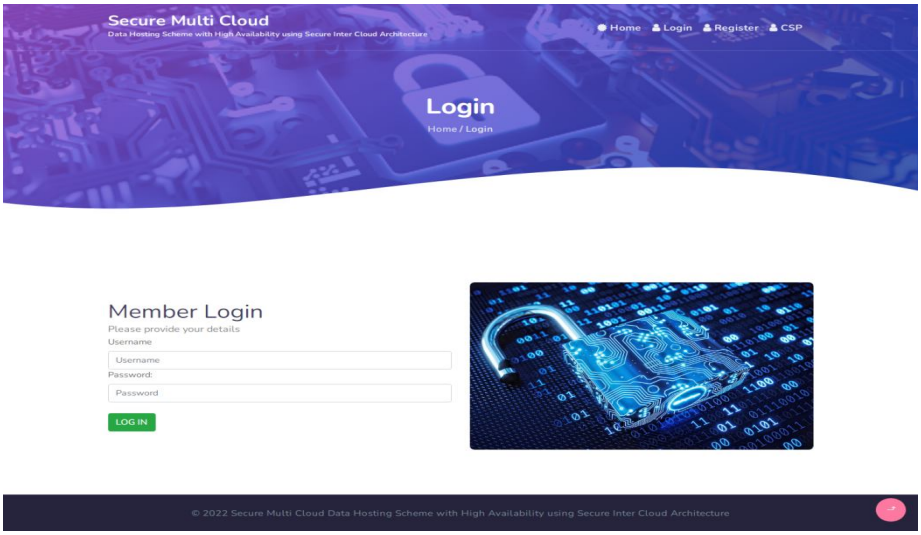


Fig. 2: Login page

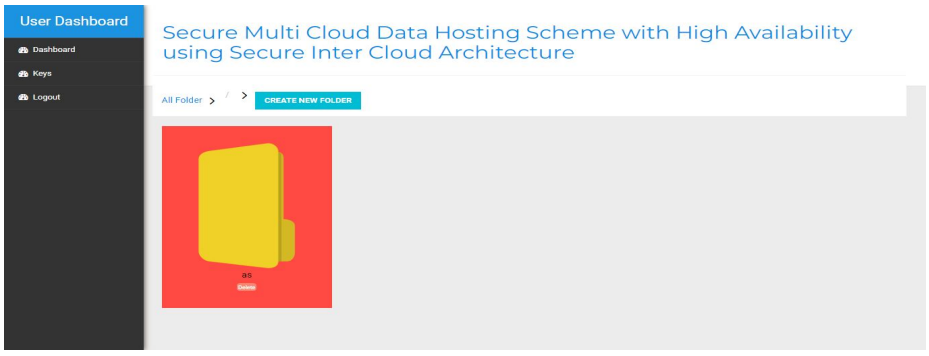


Fig. 3 Dashboard page

Fig. 4 key page

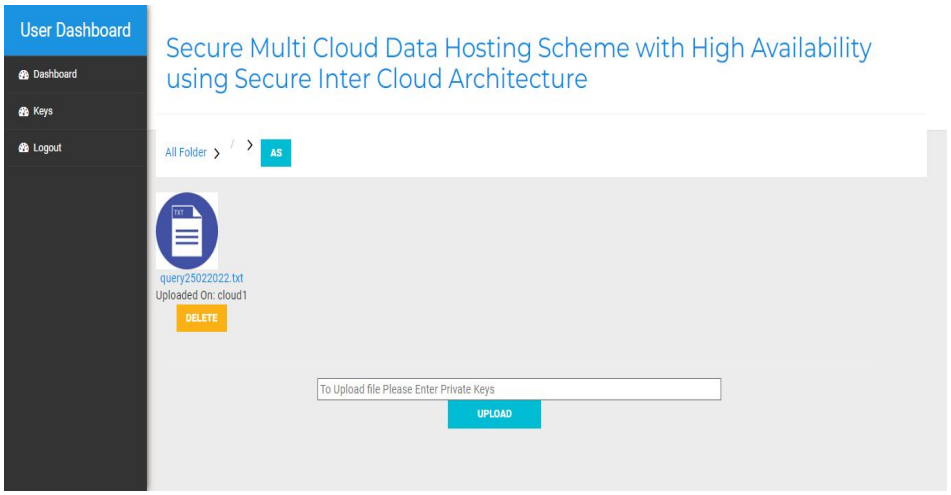


Fig. 5 File which stored in encrypted format.

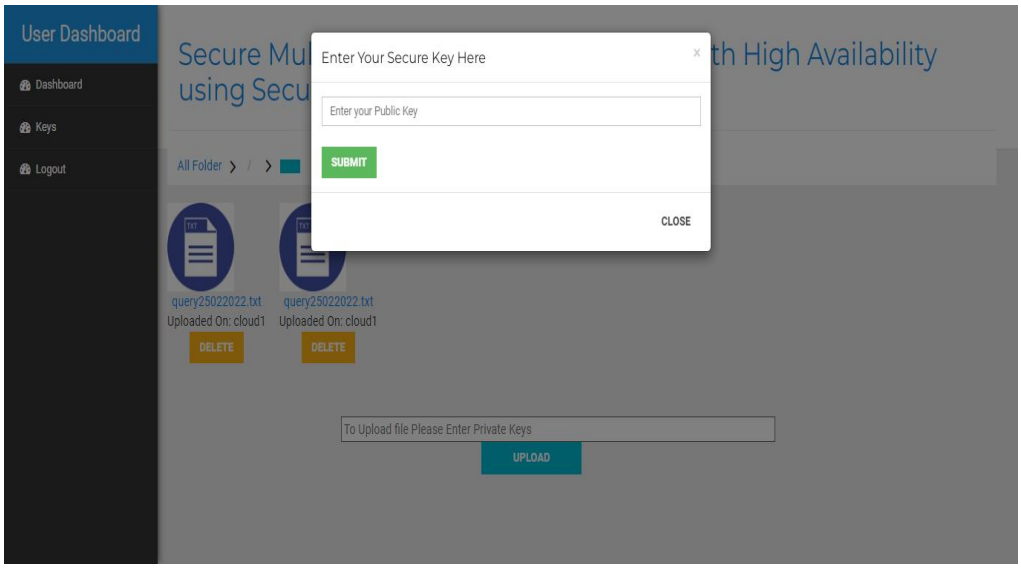


Fig. 6 Download file

Fig. 7 Encrypted Format

At another side of this implementation there is a cloud service provider. Once authentication of cloud service provider is done then they are allowed to see the files and their details uploaded by users on the cloud as shown in Fig. 8. Also CSP have authority to check if the files are safe or not on the server. Fig. 9 shows the status of files.

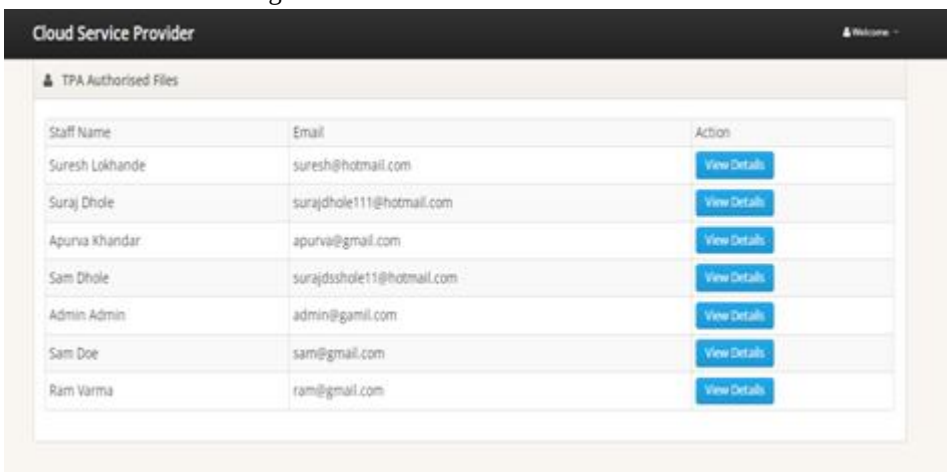


Fig. 8 Authorized Files

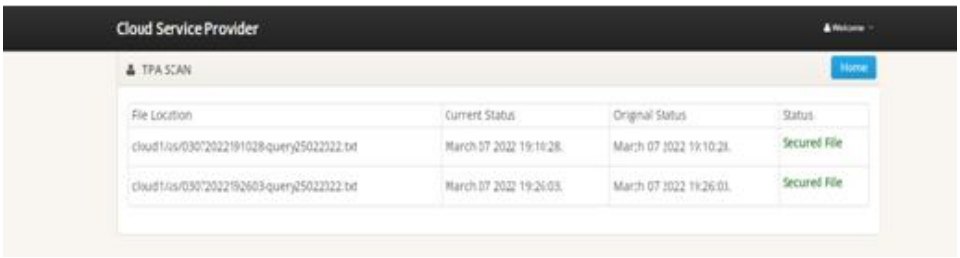


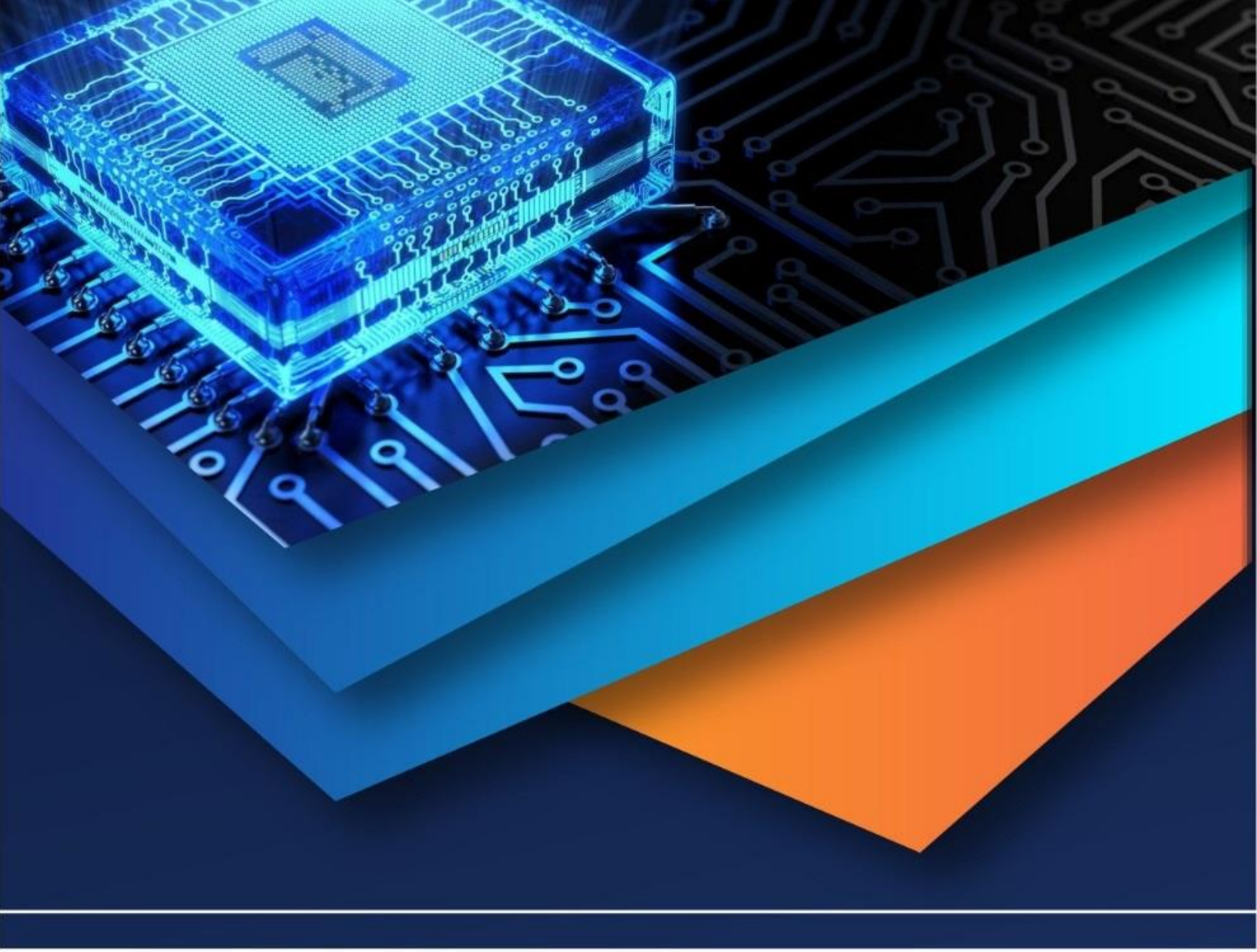
Fig. 9 File Status

III.CONCLUSION

We are here proposed a secure multi-cloud architecture in cloud computing, which provide secure environment to customer to store and retrieve information or data securely and without access failure and within minimal time. We are going to provide secure data by using encryption and by storing data on multiple cloud servers. The sensitive user account information will also secure on different centre server which will help in securing the data from attacks.

REFERENCES

[1] Kim-Kwang Raymond Choo ,Cloud computing: Challenges and future directions.
[2] S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, A. Wolman, and H. Bhogan. Volley: Automated Data Placement for GeoDistributed Cloud Services. In USENIX Symposium on Networked Systems Design and Implementation (NSDI), April 2010.
[3] Gartner: Top 10 cloud storage providers. [Online]. Available: http://www.networkworld.com/news/2013/010313-gartnercloudstorage-265459.html?page=1, 2013.
[4] Z. Li, C. Jin, T. Xu, C. Wilson, Y. Liu, L. Cheng, Y. Liu, Y. Dai, and Z.- L. Zhang, ―Towards network-level efficiency for cloud storage services,‖ in Proc. ACM SIGCOMM Internet Meas. Conf., pp. 115–128, 2014.
[5] Z. Li, C. Wilson, Z. Jiang, Y. Liu, B. Y. Zhao, C. Jin, Z.-L. Zhang, and Y. Dai, ―Efficient batched synchronization in dropbox-like cloud storage services,in Proc.ACM/IFIP/USENIX 14th Int. Middleware Conf., pp. 307–32, 2013.
[6] Ubuntu One File Services. [Online]. Available :http://blog.canonical.com/2014/04/02/shutting-down-ubuntuonefile-services/, 2014.
[7] Kalyani.M.Borse1, Ankita G. Deshpande, Ashlesha A. Deshpande, Ms.Juily.S.Hardas , "SECURITY IN MULTI-CLOUD DATA STORAGE WITH SIC ARCHITECTURE" ,Student, Computer Engineering Department, GES R.H.S.COE, Maharashtra, India
[8] M.A. AlZain and E. Pardede, ‖Using Multi Shares for Ensuring Privacy in Database-asa-Service‖, 44th Hawaii Intl. Conf. on System Sciences (HICSS), pp. 1-9, 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY