International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A 'No Data Center Solution' for Cloud Computing/File Hosting

Srishti Kakkar[1], Nikhil Joshi[2], Rajiv Dahiya[3], Ruchika Doda[4]
[1, 2]*Student, Department of Electronics and Communication Engineering, MVSIT, Sonipat*
[3]*Head of Electronics and Communication Engineering and Electrical Engineering Department, MVSIT, Sonipat*
[4]*Project Guide, Department of Electronics and Communication Engineering, MVSIT, Sonipat*

Abstract: ***Cloud computing or file hosting provides on demand services to its clients. Hosting files of owner or data storage is among one of the primary services provided by cloud computing. Cloud service provider hosts the data/files of data owner on their server and user can access their data from these servers. An independent mechanism is required to make sure that data is correctly hosted in to the cloud storage server. In this paper, we will discuss the technique that is used for secure data storage on cloud or on personal server of the owner. Cloud computing has been envisioned as the next generation architecture of IT enterprise. Cloud computing moves the application software and data bases to the large data centers, where the management of the data and services may not be fully trustworthy. This poses many new security challenges which have not been fully implemented. In this paper, we mainly focus on aspects for providing security for data storage on a personal server, also architecture for data storage that can be accessed from anywhere by owner, key points for proving security for data storage. The objective is to enhance the security issues on the platform of cloud so that data can be securely hosted in the premises of the owner. This can be a affective solution in the long run.***
Keywords: cloud computing, file hosting server, data storage, secure hosting, file server

I. INTRODUCTION

Cloud computing is the combination of many preexisting technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take benefit from all these technologies. Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere through data centers. Data breaching is possible in cloud environment or through a data center, since data from various users and business organizations lie together in cloud. By sending the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Sometimes the Cloud Service Provider (CSP) itself will use/corrupt the data illegally. Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. A simple solution is to keep all the data on your own server and you can access it from anywhere and anytime through your id and password. This approach ensures that the data is not visible to external users and cloud administrators but has the limitation that your server needs to be active for 24 hours. In this paper, we discuss what are the requirements for this file hosting server and how this solution can be achieved.

II. EXISTING SYSTEM

The existing system of file hosting includes cloud storage as one of the primary requisite. We can define cloud storage as storage of the data online in the cloud. A cloud storage system is considered as a distributed data centres, which typically use cloud-computing technologies and offers some kind of interface for storing and accessing data. When storing data on cloud, it appears as if the data is stored in a particular place with specific name.

There are four main types of cloud storage as of now:

1) *Personal Cloud Storage:* It is also known as mobile cloud storage. In this type storage, individual's data is stored in the cloud, and he/she may access the data from anywhere.
2) *Public Cloud Storage:* In Public cloud storage the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data centre. The cloud storage provider fully manages the enterprise's public cloud storage.
3) *Private Cloud Storage:* In Private Cloud Storage the enterprise and cloud storage provider are integrated in the enterprise's data centre. In private cloud storage, the storage provider has infrastructure in the enterprise's data centre that is typically managed

by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

4) Hybrid cloud storage: It is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

In all these storages the data is under the control of some third party and the user doesn't know where his/her data is stored. This can lead to data breaching.

Through this paper we have proposed an idea where the user can host files, websites or any sort of data in his/her own premises or on the personal server and can then access the files or data at anytime and from anywhere.

This will provide secure and efficient hosting on a personal premises for websites and data files so that it can be accessed remotely anytime, anywhere through the medium of internet

III. CHARACTERISTICS OF EXISTING

There are five characteristics of existing system of cloud computing or data hosting. The first one is on-demand self-service, where a consumer of services is provided the needed resources without human intervention and interaction with cloud provider. The second characteristic is broad network access, which means resources can be accessed from anywhere through a standard mechanism by thin or thick client platforms such mobile phone, laptop, and desktop computer. Resource pooling is another characteristic, which means the resources are pooled in order for multitenants to share the resources. In the multi-tenant model, resources are assigned dynamically to a consumer and after the consumer finishes it, it can be assigned to another one to respond to high resource demand. Even if the resources are assigned to customers on demand, they do not know the location of these assigned resources.

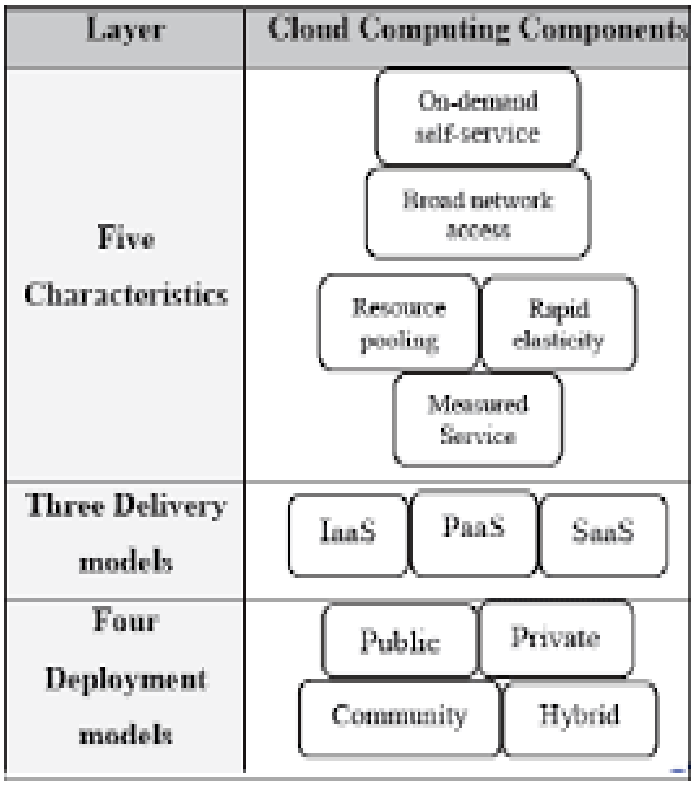

Fig 1 Cloud environment architecture

Sometimes they know the location at a high-level abstraction, such as country, state, and data centre. Storage, processing, memory, and network are the kind of resources that are assigned. Rapid elasticity is another characteristic, which means that resources are dynamically increased when needed and decreased when there is no need. Also, one of characteristics that a consumer needs is measured service in order to know how much is consumed.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

IV. PROPOSED SYSTEM

The data flow diagram of the proposed system is given below.

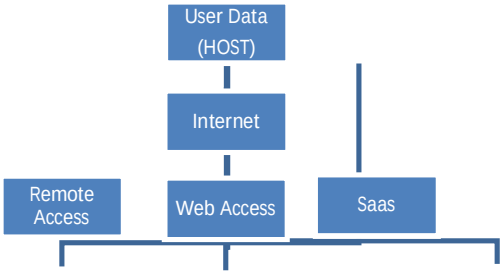

Fig 2 Data flow Diagram

This system ensures the security of data unlike the existing system, as we use the the machine of the data holder as the host for remote access of data.
As Compared to legacy that is being currently used this system is more feasible in terms of valuation for a long term although running cost might be a bit on higher side during initial stages but in the long run its much feasible.

A. Speed of data transfer from host is expected to touch around 10mbps which would be a big improvement over current speed of 4mbps
B. Bandwidth is expected to be increased
C. Storage would be enhanced with hands in hand of SSD RAM

The purpose of the project is to provide secure and efficient hosting on a personal premises for websites and data files so that it can be accessed remotely anytime, anywhere through the medium of internet.
We get to learn about the unique fusion of cloud and networking platform integrated with website designing and development.

V. WORKING OF THE SYSTEM

1) *Front End*– It uses the complex web designing for User interface and payment gateways so as to complete the registration process for hosting
2) *Back End*- It uses networking for the integration of equipment that serves the hosting also it uses the virtualized concept of vendor neutral cloud computing so that data can be accessed from anywhere at anytime and finally it requires internet access 24X7 so as to keep server online.

The only hardware required will be computer with a high speed RAM.
When the user selects the storage space and the domain, he/she will be directed to payment page according to the package selected. Once the payment is done, the user will be provided with a SDK file that needs to be installed on the computer or machine that the user needs to make the server. After this the user will be provided with a login id and password that can be used to access the data stored on that system from anywhere and anytime. The codes for this system has been written using integrated development environment so that the SDK files can run on all operating systems.

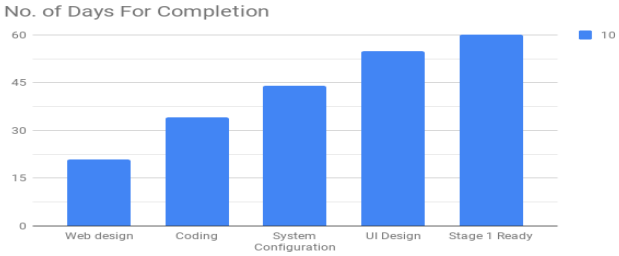

Fig 3 Gantt Chart of the system

VI. CONCLUSION

File hosting or cloud computing enables users to store their data in remote storage location. But data security is the major threat here. Due to this many organizations are not willing to move into cloud environment. To overcome this, confidentiality, integrity, availability should be encapsulated in a system. This system provides them all of this and the data is hosted in the owner's environment. No third party is involved here. The machine of the user becomes the server for hosting files, websites or any sort of data and the data can be accessed from anywhere using login id and password.

The future scope of this project will be good in terms of long run. Though initial cost will be a bit high during initial stages but in the long run it will be feasible.

REFERENCES

[1] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, "Data Confidentiality and Integrity Verification usingUser Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel,

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom, "Cloud computing security: From single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

[8] E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[10] E. M. Mohamed, H. S. Abdelkader, and S. ElEtriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.

[11] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), 2010. IEEE, 2010, pp. 1–7.

[12] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011, pp. 245–249.