Resource & Availability in Multi-cloud Using Services

Prof. Suhas M. Patil*, Mr. Niraj A. Papde**, Mr. Ketan D. Kamble***

*Department of Computer Engineering, Pune University Pune, India
**Department of Computer Engineering, Pune University Pune, India
***Department of Computer Engineering, Pune University Pune, India

Abstract- Cloud computing reduces costs associated with computing with increase of flexibility and scalability for computer processes because of this cloud computing is counted as one of today's most exciting technologies. As we know that Turbo-c, Microsoft visual studio, Java is software package available in the windows operating system. But one important thing which we should note is there is operating system restriction with these software packages. We can't use some application in Linux operating system. Also another thing is we can't use this software over internet. So there are some OS restrictions and Hardware restrictions with existing system. The solution to this problem is to develop a soft-ware application which should avoid the OS restrictions and Hardware restrictions. It should be usable over the internet. Cloud benefits such as load balancing, better level of the security will help to increase the performance of this application. We are developing a technique thro-ugh cloud computing in which user will handle systems from far distances with the help of centralized server and can access applications as well insert them from client machines, and can store data on data storage area on proxy server.

Index Terms- cloud security, cloud storage, data security, service availability, Web application.

I. INTRODUCTION

Users can use cryptographic methods to protection of the stored data in the cloud. Hashing function is effective solution for data integrity. The loss of availability of service is limitations in cloud computing is done by storing the client data on different servers in cloud. If the data is processed from several clients, then privacy cant ensured by data encryption. Cloud can be attacked by the Third-party

This project is about developing an cloud based software that will provide the users the features similar to that of turbo c, Microsoft visual studio, java. The advantage of deploying it on cloud is that, the user can create, modify and access the documents from anywhere with no need of carrying the documents. The aim of this project is to deploy most commonly used modules of Application (turbo-c, Microsoft visual studio, and java) on Cloud and make it available to all people without any OS restriction or restrictions of Hard disks space and Hardware requirements and with 24*7 availability of application with the help of internet connection.

II. RELATED WORKS

Dealing with the cloud computing for a first time it is important to avoid potential pitfalls and confusion

- The notion of how cloud services are deployed is often used interchangeably with where they are provided, which may cause confusion. like private or public clouds may be described as internal or external cloud, which model may or may not be correct in all cloud model.
- The manner in which cloud services are consumed is often described relative to the location of an organization's management or security perimeter (usually presence of a firewall). It is important where security boundaries lie in terms of cloud computing.

A. Existing System
- Customers make use of methods like encryption and decryption for security of stored data in the cloud.[1]
- Data integrity is achieved by hash function.[1]
- Availability of cloud service is considered as the main limitations in cloud computing and it has been maintain by storing the data on several clouds.
- Different clients process different data, data encryption cannot ensure privacy in the cloud.
- Cloud can be attacked by the Third-party[1]
- Security of data in the cloud model is major concern but this is not achieved by this system, it will only used for data storing. [1]

B. Proposed System
- User guarantee data confidentiality, it does not need code execution in their servers.
- User's data does not affected by loss of availability, loss of corruption of data, loss of privacy, vendor lock-in problem.
- User is able to access application environment which is located on server side.
- Every user can access licensed version software for their work

.

III. GOAL

To develop a system for sharing of software and hardware in cloud from which user can access applications anytime, any-where in secured environment.
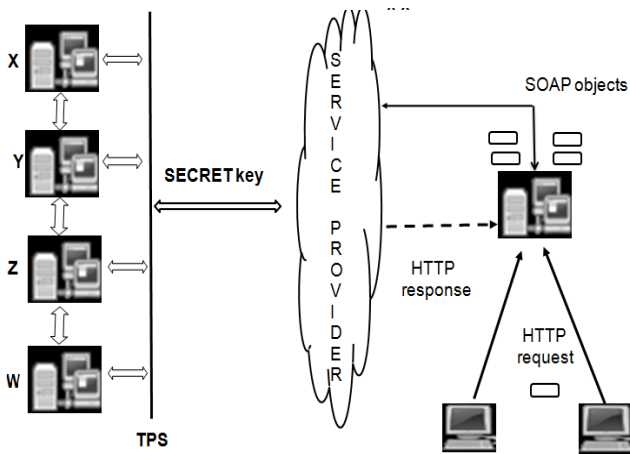
IV.   SYSTEM ARCHITECTURE

Figure .1: System architecture

Fig 1 describes system architecture .Client sends HTTP request to domain server. Domain accept request and send SOAP object to Service provider (Azure ,Amazon, Google etc).Web service which contains Secrete sharing algorithm divide key in no of shadows which are stored on different server via TPS (Transaction process System).X,Y,Z are cloud servers which contains applications. When client request any application after login first secret key is checked after authentication of user application is accessed via HTTP response.

V.   ALGORITHM AVAILABLE FOR CLOUD SECURITY

To reduce the risk in cloud storage model , user can use encryption and decryption for security purpose of the stored data in the cloud [7]. Data integrity by for keeping a short hash use of hash function [9] is a preferred solution . by recalculating hash user will get required key [7].for large database hash tree [9]is used rather than hash function.

A, HAIL (High Availability and Integrity Layer) [6]

Distributed cryptographic system noting but a set of server which available for 24*7 and that the client's stored data is retrievable and integral.

B.RACS (Redundant array of cloud storage)[3]

This employs RAID like technique to implement high-available and storage –efficient data replication on diverse clouds. In cloud use of replication decreases the cost of providers and also gives better fault tolerance. This results into, amount of large database load will be divide among different providers as a result of the Redundant array of cloud storage proxy server .[3]

C. Depsky

Deals with this problem using Byzantine fault tolerance replication to store data on cloud services, allowing data to be retrieved correctly even if some of the clouds corrupt or lost data.

VI.   SECRETE SHARING (SHAMIR'S SECRET SHARING)[5]

In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participants. When shares are combined together then and then only secret can only be reconstructed. Individual key share holder cannot change/access the data.

Goal is to divide some data D (e.g., the safe combination) into n pieces D1, D2….Dn in such a Way that:

- Knowledge of any k or more D pieces which in turns makes D easily computable.
- Knowledge of any k -1 or less pieces will not be sufficient for determination of D.

This scheme is called (k,n) threshold scheme. In case if k=n then all participants are required together to reconstruct the secret. Suppose we want to use (k,n) threshold scheme to share our secret S where k<n.

Choose at random (k-1) coefficients a1, a2, a3ak-1, and let S be The a0

$$f(x)=a_0 + a_1x + a_2x^2 \ldots\ldots +a_{k-1}^{k-1}$$

Construct n points (i,f(i)) where i=1,2..n

Given any subset of k of these pairs, by interpolation user can find the coefficients of the polynomial to evaluate a0=S , which is the required secret.

VII.   ADVANTAGES

- Number of services available by category wise
- It provide secured cloud.
- In system server side program can be access and can be modified as per as your need and teacher can able to comment on it.
- Load balancing will be provide to avoid any system clash and Dividing the traffic between servers, data can be sent and received without major delay Multi cloud computing service availability

- Http and SOAP protocol is used, for two way communication
- Minimum response time required when worker processor is busy i.e. proxy server can reply
- Secret sharing algorithm provide security

VIII. DISADVANTAGES

- The major disadvantage of our project is that any new user or any client will have to first authenticate by the server. It has limited access.
- It will always give access to the application then we are running .exe file in our client machine hence we require good internet connections with high speed.

IX. CONCLUSION

System allows user to access applications, use resources (printer) re-motley .System is available on internet so that user can access service anytime from anywhere,. When any user access any service server will get a notification. Service is available for 24*7.user need not to purchase license software. While developing any system with cloud security must taken in consideration first.System will be developing the cloud computing environment with the safety issues through analyzing a cloud computing framework security needs. Finally conclude a cloud computing model for data security from single to multi-cloud. Cloud computing, while still evolving in all its iterations, can offer IT a powerful alternative for efficient application, infrastructure, and platform delivery. If it is implemented on practical basis it will be very efficient for user.

REFERENCES

[1] Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom "Cloud Computing Security: From Single to Multi-Clouds", *45th Hawaii International Conference on System Sciences*,2012

[2] A. Bessani, M. Correia, B. Quaresma, F. Andre and P. Sousa "DepSky: dependable and secure storage in a cloud-of-clouds ", *EuroSys'11:Proc. 6thConf. on Computer systems*, 2011, pp. 31-46.

[3] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", *SoCC'10:Proc. 1st ACM symposium on Cloud computing*, 2010, pp. 229-240.

[4] Zhou Wei, Guillaume Pierre, Chi-Hung Chi "CloudTPS:Scalable Transactions for Web Applications in the Cloud", *IEEEtransactions on services computing, special issue on cloud computing*, 2011

[5] http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

[6] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. *16th ACM Conf. on Computer and communications security*, 2009, pp.187-198.

[7] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", *ACM SIGACT News*, 40, 2009, pp. 81-86.

[8] R.C. Merkle, "Protocols for public key cryptosystems", *IEEE Symposium on Security and Privacy*, 1980, pp. 122-134.

[9] CongWang, Kui Ren, and JiaWang " Secure and Practical Outsourcing of Linear Programming in CloudComputing ", *IEEE transactions on cloud computing april* 10-15, 2011

AUTHORS

First Author– Prof. Suhas M. Patil,
patil.suhas85@yahoo.com
Second Author – Mr. NirajA.Papde,
BE,KJCOEMR,Pune,niraj143143gmail.com
Third Author – Mr. KetanD.Kamble,
BE,KJCOEMR,Pune,ketankable3894@gmail.com

Correspondence Author -Mr. Vishal B.Gadilkar,
BE,KJCOEMR,Pune,vg11717@gmail.com