Eliminating Single Point of Failure and Data Loss in Cloud Computing

Ranjithprabhu .K[1], Sasirega .D[2]

[1]Research Scholar, KG College of Arts and Science (Affiliated to Bharathiar University), Coimbatore 641035, Tamil Nadu, India

[2]Assistant Professor, KG College of Arts and Science (Affiliated to Bharathiar University), Coimbatore 641035, Tamil Nadu, India

Abstract: ***Cloud computing is not without its risks. The fact is that these risks are definitely manageable with some effort taken. Once the issues are resolved, then the remaining process should go on smoothly, thereby providing various benefits for both the cloud provider and the cloud consumer. It is a new era of computing that offers huge benefits including such as reduced time consumption, surplus computing power and scalable computing capabilities. A single point of failure (SPOF) is one of the design issues in cloud computing that is more vulnerable and such failures mitigate the entire system unavailable. This paper elaborates the redundancy techniques to overcome Single point of Failure and data replication with data mapping to prevent data loss in cloud computing.***

Keywords: Single point of failure, SPOF, Cloud security, Redundancy, Data loss

1. Introduction

The resources provided by grid computing are not adequate to use. As a solution for this, Cloud computing comes into existence and offers sufficient resources in a manner that provides on-demand resources[1] to the users as a metered service. It provides new computational power by delivering new computing resources to the locally available computational power. Internet is the key for cloud computing. It is a distributed internet computing [2] for IT and scientific research. The applications in the cloud are accessible through the internet and such applications are stored in large data servers. Data centre comprises of a large amount of data servers used to host cloud services and applications. On the other hand, cloud provides metered service where anyone can obtain computing resources, network storage and other metrics in the basis of "pay per use".

Cloud computing services are indefinitely available across the overall computing arena. Cloud computing includes three primary service models, which are as follows:

- Infrastructure as a service (IaaS): raw computing power, data storage and network bandwidth
- Platform as a service (PaaS): databases, development tools and other components required to support the delivery of custom applications.
- Software as a service (SaaS): applications both general and specialized. General applications include such as word processing, email and spreadsheet and specialized applications includes such as enterprise resource management (ERM) and customer relationship management (CRM).

1.1 Cloud Characteristics:

Cloud has five different characteristics [3] which are essential for cloud deployment and they are listed below.

- On-Demand Self Service: Cloud consumers must be capable of obtaining the cloud services at the infrastructure, platform or application level at any time without requiring any significant assistance.
- Measured Service: It is similar to utility computing where the used resources and obtained services are measured.
- Resource Pooling: It allows multiple users to make use of available physical and virtual resources.
- Rapid Elasticity: It provides flexible computing based on the demand which can expand or contract.
- Broad Network Access: Cloud services can be obtained in any kind network even it can remotely accessed from mobiles, Laptops, PDA's via internet.

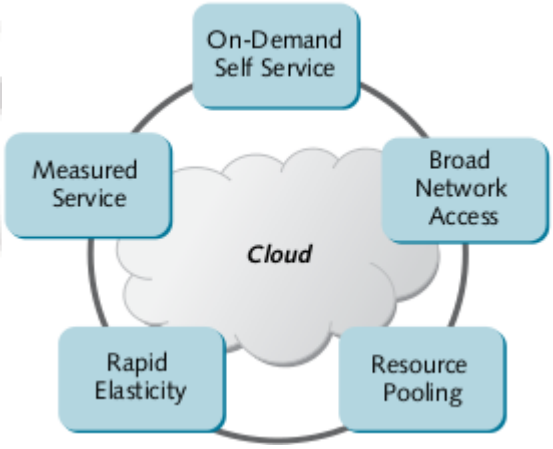

Figure 1: Characteristics of Cloud

1.2 Cloud Deployment Models:

NIST defines four various deployment models [3]: Private cloud, Public cloud, Community cloud, and Hybrid cloud.

- Private Cloud: A private organization running its own cloud infrastructure managed by a third party or its own. The resources are limited to the clients (cloud user) based on their level of access and it has utmost control over the data.
- Public Cloud: A cloud infrastructure is built and made available for anyone on the internet. Various services requested by different customers are rendered by the public cloud. It may provide some its service for free of

cost but not all.

- Community Cloud: A cloud infrastructure is shared by two or more organization that requires similar cloud services. It is managed by the organization or a third party and it may exist in on-premises or off-premises.
- Hybrid Cloud: A cloud infrastructure which essentially a composition of two or more clouds to attain elasticity at the user level.

2. Single Point of Failure in Cloud Computing

In cloud computing, the single point of failure happens in both hardware and software layout. Single point of failure is a possible risk that affects the systems reliability and availability. SPOF occurs in cloud posed by the flaw in design, architecture or implementation. In a data center, SPOF makes the entire system unavailable to the users. As well as when data is transmitted by multi-tenant through a single point from multi servers, there occur bottleneck [4] problem.

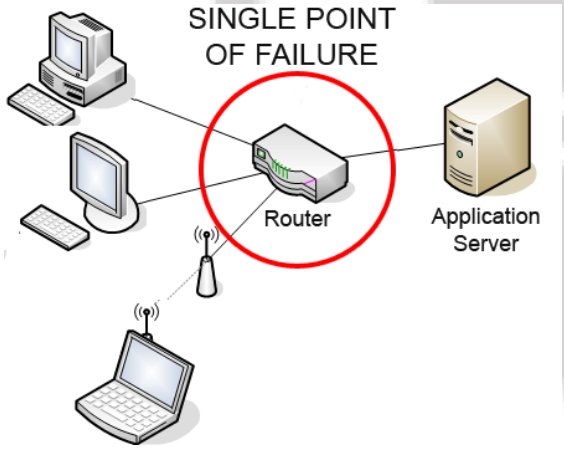

Figure 2: Single Point of Failure

Consider a data center where all the applications run depends upon a single application server. When the single application server fails, then the applications become inaccessible to the clients. Consider the same scenario where multiple servers connected through a single switch or a router in the data center. In such cases, failure of that single switch or a router makes none of the servers available to the users. When more clients access the multi-servers through the single switch or a router in the network, then the bottleneck issue also arises.

In the month April 2011, Amazon's EC2 [5] cloud suffered several day outages resulting in loss of availability of its service and loss of data due to single point of failure. This took down the data of several high profiles sites including Reddit (over 36 hours), Foursquares, Hootsuite and Quora (48 hours). So, it is very essential to eliminate the SPOFs in the architecture of cloud to maintain the availability of cloud services [6].

3. Eliminating SPOFs in Cloud Computing

Redundancy and High-availability clusters are the key factors to avoid SPOFs. Both logical redundancy and physical redundancy is needed to be achieved. High-availability clusters minimize the outages (99.99% availability) of the system components included in the cloud. When a system component fails, then immediately another component should take part the role of the failed component. Such as like Multi switches connected to Multi servers where the failure of a switch should not affect the system, another switch should take the role to maintain the availability of the system.

3.1 Logical redundancy

Software flaws can render outages by themselves to the software architecture [6]. Multiple application server will avoid the software flaw and eliminate SPOFs in the cloud architecture. The cloud service providers should have the scale and resources to identify, address, isolate, and prevent the software flaws. Cyber-attacks of software's need to be defended in a much more professional way like multi-factor authentication[7] to prevent and make the impact of cyber-attacks by logical redundancy.

3.2 Physical redundancy

Physical redundancy can be achieved with high-availability clusters. It will avoid the SPOFs and as well as the Bottleneck problem. None of the hardware or software should rely on a single hardware at any instance. Clusters are collection of servers connected through network components in data centres. It is essential to mitigate the server as highly available in the cloud by enhancing the physical architecture with multiple routers and switches. The data centre architect should ensure the physical redundancy in such a way by avoiding single way communication between the cloud components of the system.

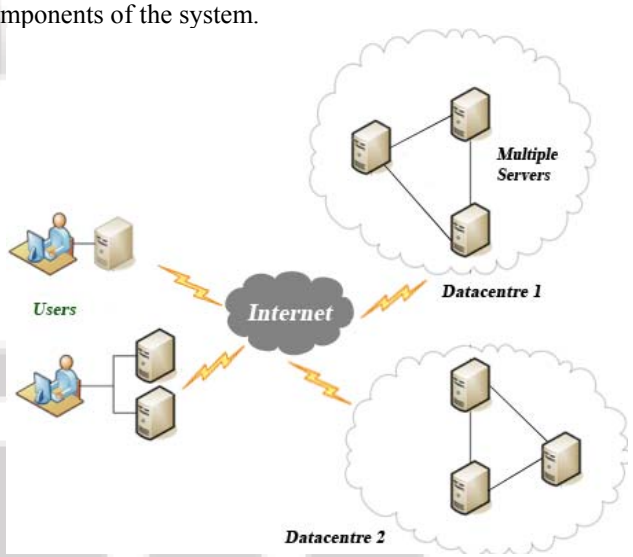

Figure 3: Multiple Servers in Multiple regions to eliminate SPOFs

4. Avoiding Data loss

When a single server holds all the data of a user or an application, then a crash or power failure of that particular server leads to data loss. The entire data in the particular server will be unavailable to clients. The data loss can be avoided through data replication (i.e., copy of the data stored in multiple servers in multiple sites).

4.1 Data Replication

Data replication ensures the availability of data to the user by replicating the data in multiple servers. Replication distinguishes between a primary copy and one or more secondary copies. All operations are performed on the primary copy and if a primary copy is not available then a secondary copy from another server is treated as primary copy. Changes to the primary copy needs to be captured and applied to the secondary copies of the data to maintain the integrity of the data.

Random replication approach being used in data centers to prevent data loss. But it will not be efficient in the case of simultaneous node failures due to cluster-wide power outages. Instead of that Copyset Replication can be used. Copyset replication, a novel general purpose replication technique that significantly reduces the frequency of data loss events [8]. Data should be replicated in multiple servers in various data centres. Natural disaster can occur anywhere in the world at any time. So, cloud service providers should offer redundant data centres to ensure the availability of their services. Though a data centre failed, instantly another data centre should take its responsibility and it should provide the services.

4.2 Data Mapping

Cloud computing service providers are often set-up with several redundant data centres to avoid the outages. In that case, clients should be able to locate the corresponding server for accessing the data. It is complex for the client to access the data. The client node has to check all the servers in order to retrieve or manipulate the data. So, the data should be replicated in multiple servers and the location of the data should be stored in a table. Both replicated and primary data path need to be stored. It is essential to duplicate the data mapping table too. It allows fetch the data rapidly for the clients.

5. Conclusion

Cloud consumer always expects maximum availability of resources from the cloud service provider. High-availability increases the reputation of the cloud service provider and brings more consumers. The availability of the cloud services can be set on high profile by eliminating the Single point of Failure in the cloud architecture. SPOFs can be eliminated with the above mentioned redundancy techniques. Data loss in cloud storage can be avoided with Copyset replication and data mapping provides rapid access to the data for the cloud consumers. It enforces high performance and consistent data access for the cloud users.

References

[1] Rafique.K, Tareen A.W, Saeed.M, Jingzhu Wu, Qureshi S.S. "*Cloud computing economics opportunities and challenges*". 4th IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), 2011.
[2] Marios D.Dikaiakos, Pankaj Mehra, Athena Vakali. "*Cloud Computing: Distributed Internet Computing for IT and Scientific Research"*. IEEE Computer Society, 2009, 135:10-13.
[3] *Chris Harding "Cloud Computing for Business* - The *Open Group* Guide". A Publication of: The *Open Group*.
[4] Kibe.S , Uehara.M , Yamagiwa.M. "*Evaluation of Bottlenecks in an Educational Cloud Environment*", 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2011
[5] Amazon Web Services, *http://aws.amazon.com*
[6] Dr. M.A.C. Dekker *"Critical Cloud Computing - A CIIP perspective on cloud computing services Version 1.0"*, December 2012 .
[7] Banyal. R. K, Jain. P , Jain. V. K. *"Multi-factor Authentication Framework for Cloud Computing"*. 5th International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), 2013.
[8] Asaf Cidon, Stephen Rumble, Ryan Stutsman, Sachin Katti, John Ousterhout and Mendel Rosenblum "*Copysets: Reducing the Frequency of Data Loss in Cloud Storage* ", Proceedings of the 2013 USENIX conference on Annual Technical Conference.

Author Profile

Ranjithprabhu. K completed M.Sc. degree in Software Systems under Bharathiar University in the year 2013. Presently doing M.E. Computer Science & Engineering under Anna University in full time and M.Phil. Computer Science in part time under Bharathiar University.

Sasirega. D received M.C.A. degree in Computer Applications and M.Phil. degree in Computer Science under Bharathiar University in the year 2004 and 2008 respectively. Presently working as Assistant Professor, Department of Computer Science in KG College of Arts and Science (affiliated to Bharathiar University).