The Need and Impact of Fault Tolerance in Cloud Storage

Balaji.S [1] Shobana. M[2]

[1]Faculty,Department of Computer science, D.B.Jain College

[2] Research Scholar, Department of Computer science, D.B.Jain College

Abstract

Cloud computing has been extremely embraced as several organizations take into account some style of cloud strategy that can applied to their business method. Cloud computing offers varied services with none initial investment in servers, storages or network. Because of theexponential growth of cloud computing, the necessity for fault tolerance may be a key investigation factor in cloud and researchers focus more on fault tolerance due to its complexity. Fault tolerance is the ability of a system to continuously perform its functionality in spite of any sudden hardware or software failure. The major advantage of using fault tolerance in cloud includes failure recovery, lower costs, and improve performance criteria. Researchers have come up with new methods to search out the advantages and barriers of fault tolerance systems in cloud computing. This paper discusses about the need of fault tolerance methods in cloud computing.

Keywords: Cloud Storage, Reliability,Replication, Data Recovery, Fault tolerance.

1. Introduction

Cloud computing plays a necessaryrole in providing computing services to businesses of different sizes. It is a distributed computing environment that provides various resources as a service to the user on demand. The main advantage of cloud is that the user can focus on the core business activities rather than worry about the maintenance of the system or application. The features of cloud such as availability of heterogeneous resources, dynamic resource provisioning, pay-as-you-go model make it a reliable platform for users to run their applications on cloud.

The cloud storage is one of the cloud services. Low cost and high availability are the key conditions to allure the customers into storage cloud. The complex and variable nature of cloud storage service not only enhances the service capabilities of computing resources to users, but also weakens the user's ability to manage and treat service resources and their problems. The facilities of the cloud increase rapidly and the security threats and challenges growing exponentially.

Large scale storage systems for cloud storage services are composed of heterogeneous storage devices with significantly different failure rates. Cloud while hosting user's applications is also responsible for storing and maintaining client's data. This data is critical and if there is loss or damage to the data, it can lead to severe calamity. Data loss is very critical to an

organization as it may result in revenue loss and business loss. Hence, cloud should provide proper fault tolerance mechanisms so that even if fault occurs the system can recover from it in a short amount of time with minimal or no damage to the applications hosted in the cloud and also to the data stored.

A fault tolerance technique enables a system to continue performing even if not fully operational at least at a minimal capacity rather than shutting down fully when failure occurs [1]. Fault tolerance mechanisms leads to failure recovery, lower cost and improvement of performance metrics.Traditional cloud storage systems adopt redundancy, e.g. erasure codes and replication, to reconstruct data when drive failure occurs, which is called as reactive fault tolerance.

2. Literature support

There are many outages have occurred in cloud provider's systems. For instance, Apple iCloud experienced an outage during which various services such as email, game center, and iTunes were impacted. Users were unable to access the affected services due to a failure in authentication.

M.A. Aman and E.K.Cetinkaya (2017) work include a cloud security system that addresses the performance of cloud based backup services. This system focuses three dimensional services to the backup data. The services include selection of encryption intensity, safe du- plication and querying on encrypted data. The user has a facility to select the strength of encryption standard of their files.

W Jiang *et al.* [2] work has pointed out that the failure factors affecting cloud storage include disk failure, physical interconnection failure, protocol failure and performance failure. Among them, 20% to 55% of storage system failures are caused by disk failure. However, the classification of cloud storage failure factors is crossover.

YanbingJiang*et al*. work includes Balanced Data Redistribution (BDR) scheme to accelerate the scaling process which can be applied on XOR based Triple Disk Failure Tolerant array(3DFTS) in 2016. This scheme distributes the data uniformly and reduces the scaling I/O by 77.45 percentage and increasing the scaling processing of 3DFTS by 4.17. This BDR achieves the balanced data distribution, minimal data migration ratio and parity modification ratio.

Hong Liu *et al.*(2015) introduced a Shared Authority based Privacy-preserving Authentication protocol (SAPA). This protocol prevents to access if the user compromise the security privacy issues of other user data and includes shared access authority is achieved by anonymous access request matching mechanisms with security and privacy considerations.

A survey on FTCC techniques is presented in [3]. The paper discussed and described the techniques, the tools used, the policies and the research obstacles. The paper classified the techniques into proactive and reactive based techniques. Checkpoint and replication are considered as reactive techniques while s-guard is determined as a proactive technique.

Proactive and reactive FT techniques are presented in [4]. Reactive techniques start to work after an error occurred and has a negative impact on the system. However, proactive fault tolerance predicts the error before it occurs or affects the system. Fault Tolerance Manager (FTM) and Message Passing Interface (MPI) are the examples used to demonstrate the reactive FT technique. Self-healing and preemptive migration examples are used to illustrate the proactive FT techniques.

3. Fault Tolerance Techniques

3.1 The Need for Fault Tolerance in CloudComputing

Previously, high performance was considered as the main criteria in the design of data centers. In today's scenario, with the development of cloud computing-based data storage centers and demand for the use of cloud services, failure is common in today's data centers, which can be attributed partly to the large scales of data stored. Since the scale data raises, access to them gets more complicated, so that different levels of access may be required for each application or each data item. The main intend of fault tolerance is to achieve robustness and dependability in every system.

There are several techniques used to implement Fault Tolerance Technique in Cloud Computing (FTCC). FT techniques are classified into two main categories or policies. They are Reactive Fault Tolerance (RFT) and Proactive Fault Tolerance (PFT) as shown in Figure 1.

RFT techniques attempt to continue the service through recovery technique. A few techniques that are classified as reactive policy are given below:

- **Check pointing-** It is a structured fault tolerance technique for long running and large applications. In this plot after doing each and every change in the system a check point is done. If a task fails, instead of starting it from the beginning the job can be restarted from the recent check point.
- **Replication-** It is one of the most notable fault tolerance techniques in storage centers that have been extensively used in online service systems. Replication means nothing but cloning or duplication. For successful execution and optimal results various tasks are replicated. Replication is performed on different resources. It can be implemented through HA- Proxy, Hadoop and AmazonEC2.
- **Migration-** Due to some reason a job may not be executed completely by a particular machine. In such scenario the task can be migrated to another machine. Job migration can be implemented by HA-Proxy.
- **S-Guard** – It is based on rollback recovery and can be implemented in Hadoop, Amazon EC2.
- **Retry** - It is the easiest technique where the failed task is retried and implement on the same resource.
- **Task Resubmission**-In this case if a failed task is detected, at run time the same task is resubmitted either to the same or different resource for execution.

- **User defined exception handling**- In this technique the user defines procedure for a failed task.
- **Workflow**-Even if any failure occurs in the task the workflow will continue its processing.
- **Software Rejuvenation-** This proactive fault tolerance technique restarts the system with a clean state of software.
- **Self-Healing** -This one of the critical technique where a huge task is divided into parts for better performance. It can automatically handle failure of application and its instance that is running on various virtual machines.
- **Preemptive migration**-The application is thoroughly monitored and analyzed so that preemptive measure can be taken. This is based on feedback control loop technique.

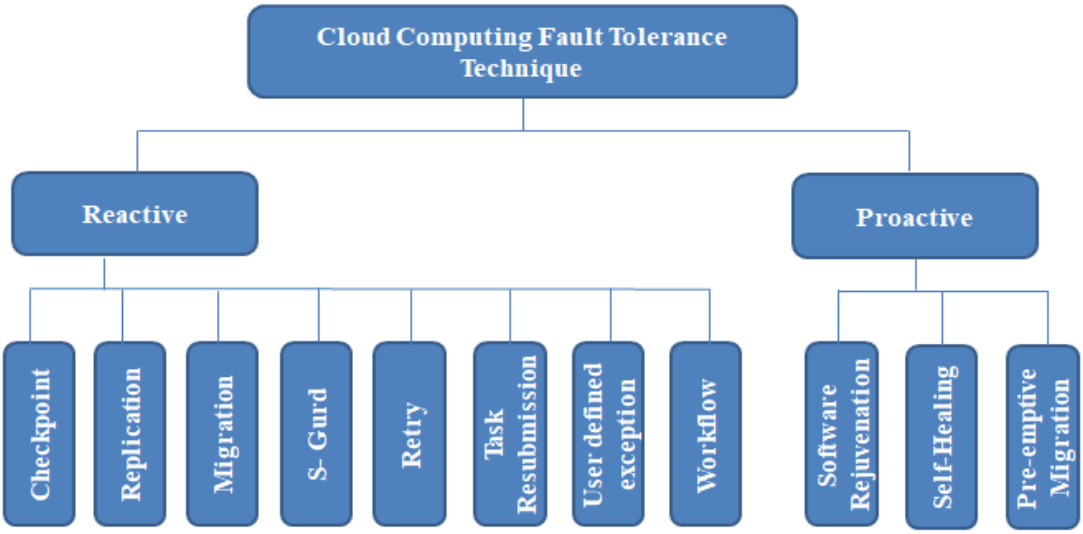

Figure 1. Fault tolerance techniques in cloud computing.

3.2 Fault Tolerance Models in Cloud Computing

Fault tolerance models in cloud computing can be classified into three types as per the fault tolerance technique mentioned until currently. They are as follows

- Checkpoint based fault tolerance
- Replication base fault tolerance
- Models based on multiple techniques

Checkpoint based fault tolerance-

It consists of three major types: coordinated checkpointing, uncoordinated checkpointing, and Communication Induced Checkpointing (CIC) [5]. CIC is an equal cost checkpointing scheme with variable checkpoint interval.

Checkpoint based fault tolerance for cloud computing uses Another Union File System (AUFS) so as to differentiate read-only properties from read and write parts in VM image. Another model with a union file system is given in [6] that use time storing VM checkpoints.

Replication based fault tolerance-

Most of the cloud computing environments have predefined hardware redundancy primarily based fault tolerance as the response time is a crucial parameter replication based FTCC that differs in handling faults.

A systematic replication scheme is proposed in [7]. This scheme transparently tolerates crash failures and provides high performance, high availability, generality, transparency and seamless failure recovery. The major drawback of this model is the latency. The network buffering causes performance overhead it requires additional hardware. Despite of being a significant model it is not recommendable for application that are sensitive to network delay or latency.Niagara is a middleware that is proposed in [8] that provides low latency and high availability.

Replication based models that are used to tolerate byzantine failures are the Byzantine Fault Tolerance(BFT). A framework for byzantine fault tolerance is proposed in [9] which tolerates faults in particular: crash, behaviors, and arbitrary. The same message algorithm that was used in Practical Byzantine Fault Tolerance(PBFT) has been used in this framework but they vary in the number of replicas. A Hybrid Quorum (HQ) protocol for BFT is presented in [10]. It switches between BFT and quorum-based protocol -i.e. Query/Update (Q/U) - according to the failure occurrence. Adaptive Fault Tolerance model in Real time Cloud Computing (AFTRC) is proposed [11]. AFTRC offers both backward and forward recovery.

Models based on multiple techniques-

Candy: This model is based on high availability modelling framework.

Vega Warden: An efficient model that has been constructed for virtual cluster based cloud computing environment to control two major problems such as usability and security that appear as a result of sharing infrastructure.

Magic Cube: A Highly reliable and low redundancy storage architecture for cloud computing.

Fault Tolerance Manager: This model is proposed to overcome the limitations of available methodologies of the on-demand services. In this method the user can specify and apply the required level of fault tolerance without a prior knowledge about its implementation. FTM architecture can be viewed as a collection of many web services components with specific purpose.

4. Conclusion

This paper studied an outline of the available fault tolerance techniques and models that may be applied in cloud computing service. Cloud providers can choose the any suitable technique or model that satisfies their requirements. Fault-tolerance methods work when a fault enters the boundary of a system. The fault-tolerance methods are used to predict the fault and perform an appropriate action, even before the faults actually occur.

In the present scenario, there are tolerance error models that introduce different fault-tolerance mechanisms to improve the system. However, there are still challenges that need to be considered for any framework or model. There are weaknesses that cannot complete all aspects of the faults. Thus, it is possible to overcome the weaknesses of all previous models. Fault tolerance in cloud computing is still an active research area therefore; this work can be a reference for researchers and developers in this field

5.References

[1] Zeeshan Amin, Nisha Sethi, Harshpreet Singh, "Review on Fault Tolerance Techniques in Cloud Computing", International Journal of Computer Applications (0975 – 8887), Volume 116 – No. 18, April 2015

[2] Jiang W, Hu C, Zhou Y, et al. Are Disks the Dominant Contributor for Storage Failures? A Comprehensive Study of Storage Subsystem Failure Characteristics[C]// Usenix Conference on File & Storage Technologies. 2008.

[3] Tsidulko, J. (December 2014). The 10 biggest cloud outages of 2014.CRN.The Channel Company. Retrieved April 5th 2014 from http://www.crn.com/slide-shows/cloud/300075204/the-10-biggest-cloud-outages-of-2014.htm?itc= refresh

[4] Kaur, J., &Kinger, S. (2014). Analysis of different techniques used for fault tolerance. (IJCSIT)International Journal of Computer Science and Information Technologies, 5(3), 4086-4090.

[5] Kumar, S., & Kumar, P. (2010). Hierarchical Non-blocking coordinated CHECKPOINTING algorithms for mobile distributed computing. International Journal of Computer Science and Security (IJCSS), 3(6).

[6] Vallee, G., Naughton, T., Ong, H., & Scott, S. (October 2006). Checkpoint/restart of virtual machines based on xen. High Availability and Performance Computing Workshop (HAPCW 2006).

[7] Cully, B., et al. (2008). Remus: High availability via asynchronous virtual machine replication.Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation.

[8] Imran, A., Gias, A. U., Rahman, R., Seal, A., Rahman, T., Ishraque, F., &Sakib, K. (2013). Cloud-niagara: A high availability and low overhead fault tolerance middleware for the cloud. Proceedings of 16th International Conference Computer and Information Technology (ICCIT)

(271-276).

[9] Zhang, Y., Zheng, Z., &Lyu, M. R. (July 2011). BFT cloud: A byzantine fault tolerance framework for voluntary-resource cloud computing. Proceedings of 2011 IEEE International Conference on Cloud Computing (CLOUD) (pp. 444-451). IEEE.

[10] Cowling, J., Myers, D., Liskov, B., Rodrigues, R., &Shrira, L. (November2006). HQ replication: A hybrid quorum protocol for Byzantine fault tolerance. Proceedings of the 7th Symposium on Operating Systems Design and Implementation (pp. 177-190). USENIX Association.

[11] Malik, S., &Huet, F. (July 2011). Adaptive fault tolerance in real time cloud computing. Proceedings of 2011 IEEE World Congress on Services (SERVICES) (pp.280, 287).

[12] B. S. Taheri, M. G. Arani and M. Maeen, "ACCFLA: Access Control in Cloud Federation using Learning Automata", International Journal of Computer Applications, vol. 107, no. 6, (2014), pp. 30-40.

[13] Garg, A., & Sachin, B. (2015). An autonomic approach for fault tolerance using scaling, replication and monitoring in cloud computing. 2015 IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE) (pp. 129-134). IEEE.

[14] Jhawar, R., Piuri, V., &Santambrogio, M. (2012). Fault tolerance management in cloud computing: A system-level perspective. Systems Journal, IEEE, 7(2), 288-297.

[15] Mohammed, B., Mariam, K.,, Irfan-Ullah, A., &Kabiru, M. M. (2016). Optimising fault tolerance in real-time cloud computing IAAS environment. Proceedings of 2016 IEEE 4th International Conferenceon Future Internet of Things and Cloud (FiCloud) (pp. 363-370). IEEE.

[16] F. Shieh, M. G. Arani and M. Shamsi, "De-duplication Approaches in Cloud Computing Environment: A Survey", International Journal of Computer Applications, vol. 120, no. 13, (2015), pp. 6-10.

[17] J. Evans, "Fault Tolerance in Hadoop for Work Migration", (2011).

[18] M. A. Aman and E.K.Cetinkaya (2017) Towards Cloud Security Improvement with Encryption Intensity Selection, Design of Reliable Communication Networks, 13 International Conferences, Munich, Germany,2017.

[19] Seyyed Mansur Hosseini and Mostafa GhobaeiArani, “Fault-Tolerance Techniques in Cloud Storage: A Survey”, International Journal of Database Theory and Application, Vol.8, No.4 (2015), pp.183-190, 2015.

[20] Carlos André Batista de Carvalho, Miguel Frank- lin De Castro and Rossana Maria De Castro An- drade(2017) Secure Cloud Storage Service for Detection of Security Violations, Cluster, Cloud and Grid computing,17 IEEE /ACM International Conference,Madrid, Spain, 2017.