ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Study of Different Fault Tolerance Mechanism in Cloud Computing

Pooja R. Kathalkar[1], A.V. Deorankar[2]

M. Tech. Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH), India[1]

Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH), India[2]

ABSTRACT: The advent of Cloud Computing is considered to be the single largest change in Information Technology. This change has stimulated everyone, from individuals to community and the large corporations. Now, the popularity of using Cloud are widely accepted that organizations are moving their traditional information processing systems to Cloud services for storing large volumes of data. One key research challenge in Cloud Computing is to ensure continuous reliability and guaranteed availability of resources provided by it. So there is a need for a robust Fault Tolerant system in Cloud Computing. To better understand Fault Tolerance in Cloud Computing, it is essential to understand the different types of faults. In this paper, we highlight the basic concepts of fault tolerance by understanding the different Fault Tolerance policies like Reactive Fault Tolerance policy and Proactive Fault Tolerance policy and the associated Fault Tolerance techniques used on different types of faults. A study on various fault tolerant methods, algorithms, frameworks etc., has been carried out which are developed and implemented by research experts in this field. This is an area where lot of research is happening and these studies will guide us to build a robust Fault Tolerance technique in Cloud.

KEYWORDS: Cloud Computing, Fault Tolerance, Proactive fault tolerance, Reactive fault tolerance, checkpoint restore

I. INTRODUCTION

With the immense growth of internet and its users, Cloud computing, with its incredible possibilities in ease, Quality of service and on-interest administrations, has turned into a guaranteeing figuring stage for both business and non-business computation customers. It is an adoptable technology as it provides integration of software and resources which are dynamically scalable. Cloud computing is built upon virtualization, distributed computing, utility computing, and more recently networking, web and software services. Individuals and organizations use hardware and software managed by third parties at remote location. Online file storage, social networking sites, webmail, and online business applications are some common cloud services. User can use these services without knowing the underlying hardware and software details.

Cloud computing is made up of several elements. Each element has a purpose which plays specific roles which can be classified as clients, Distributed servers, data centers.

- Clients: These are typically the computers which are used by the end users i.e. the devices which can be used by the end user to manage the information on cloud (laptops, mobile phones, PADs etc.)
- Data center: These are collection of servers where the service is hosted. In order to create number of virtual server on one physical server in data center, virtualization is used.
- Distributed servers: These are servers which are located in different geographical place. It provides better accessibility, security to the user.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Cloud computing demands are increasing day by day as a result of which it is mandatory to provide accurate services in the presence of fault also. Fault tolerance is the procedure of finding faults in the system. Although there is hardware or software failure in the system yet the system should work properly. Fault tolerance has the property that it works gracefully with the system capabilities so that the system can work correctly against the hardware or software failure. In order to obtain robust cloud computing the failures should be handled with care. The considerable use of fault tolerance in cloud computing is to cope up with software and hardware failures, reducing cost and increasing the performance. A more reliable method than checkpointing can be used to cop up with VM failure. The service provider starts a new VM with same features as the failed VM and then it request the customer to deploy its application on this new VM.

Fault Tolerance Mechanism

Metrics for Fault Tolerance in Cloud Computing

The existing fault tolerance technique in cloud computing considers various parameters: throughput, response-time, scalability, performance, availability, usability, reliability, security and associated over-head.

- Throughput–It defines the number of tasks whose execution has been completed. Throughput of a system should be high.
- Response Time- Time taken by an algorithm to respond and its value should be made minimized.
- Scalability– Number of nodes in a system does not affect the fault tolerance capacity of the algorithm.
- Performance– This parameter checks the effectiveness of the system. Performance of the system has to be enhanced at a sensible cost e.g. by allowing acceptable delays the response time can be reduced.
- Availability: Availability of a system is directly proportional to its reliability. It is the possibility that an item is functioning at a given instance of time under defined circumstances.
- Usability: The extent to which a product can be used by a user to achieve goals with effectiveness, efficiency, and satisfaction.
- Reliability: This aspect aims to give correct or acceptable result within a time bounded environment.

Types of Fault Tolerance Mechanism

i)Reactive fault tolerance

Reactive fault tolerance techniques are used to reduce the impact of failures on a system when the failures have actually occurred. Techniques based on this policy are checkpoint/Restart and retry and so on.

- Check pointing/Restart- The failed task is restarted from the recent checkpoint rather than from the beginning. It is an efficient technique for large applications.
- Replication: In order to make the execution succeed, various replicas of task are run on different resources until the whole replicated task is not crashed. HAProxy, Haddop and AmazonEc2 are used for implementing replication
- SGuard:It isbased on rollback recoveryand can be executed in HADOOP, Amazon Ec2.
- Retry: This task level technique is simplest among all. The user resubmits the task on the same cloud resource.
- Task Resubmission:The failed task is submitted again either to the same machine on which it was operating or to some other machine.
- User defined exception handling: Here the user defines the specific action of a task failure for workflows.
- Rescue workflow: It allows the system to keep functioning after failure of any task until it will not be able to proceed without rectifying the fault.

ii) Proactive Fault Tolerance:

- Proactive fault tolerance predicts the faults proactively and replace the suspected components by other working components thus avoiding recovery from faults and errors. Preemptive migration, software rejuvenation etc. follow this policy.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

- Software Rejuvenation-the system is planned for periodic reboots and every time the system starts with a new state.
- Proactive Fault Tolerance using self-healing: Failure of an instance of an application running on multiple virtual machines is controlled automatically.
- Proactive Fault Tolerance using Preemptive Migration: In this technique an application is constantly observed and analyzed. Preemptive migration of a task depends upon feed-back-loop control mechanism.

II. RELATED WORK

Wenbing Zhao et al [1] put forward a Low Latency Fault Tolerance (LLFT) middleware framework for fault tolerance which replicates the processes of applications, using the leader/follower replication approach. This framework is equipped with a LLFT Messaging Protocol which ensures reliable communication between the replicated processes. LLFT Membership Protocol ensures that the entire replicated process group has a consistent view of their membership.

Ravi Jhawar et al point out a method to exploit the virtualisation layer to offer required fault tolerance properties to the applications as an on-demand service. This is done by adding a service layer which acts as a Fault Tolerance Middleware (FTM) providing the required properties to facilitate revamp support to its applications [2]

Sidirglou et al [3] discuss about Assure, an autonomous fault management system in Cloud environment by introducing rescue point technique. However, one potential problem is that there is a chance that one of the major rescue points will be called frequently during normal execution creating higher overhead for server applications.

Shelp [4] is another autonomous FT system proposed by Gang Chen et al which uses checkpointing as FT technique in virtual environment.

Naixue Xiong et al.[5] (2007) Given that networks are dynamic and unexpected, Naixue-Xiong, investigates Failure detector properties with connection to real and programmed fault-tolerant cloud based network systems, in order to discover a general non-manual investigation strategy to self-tune corresponding parameters to fulfill user requirements. Based on this general self-tuning method, they propose a dynamic and programmed Selftuning Failure Detector scheme, called SFD, as an improvement over existing schemes.

Anjali Meshram et al. [6](2013) proposed fault tolerance model for cloud (FTMC). This model accesses the reliability of computing nodes and choses the node for the computation on the basis of reliability. The node can be removed if it does not perform well.

Ravi Jawahar et al. [7](2012): provided a new dimension for applications deployed in a cloud computing infrastructure which can obtain required fault tolerance properties from a third party. The model straightforwardly work fault tolerance solution to user's applications by combining selective fault tolerance mechanisms and discovers the properties of a fault tolerance solution by method of runtime monitoring.

Sagar C Joshi et al [8] (2014) proposed a fault tolerance mechanism to handle server failures by migrating the virtual machines hosted on the failed server to a new location. Virtualization has been applied for data centers giving rise to the concept of virtual Data Centers (VDC) which have virtual Machine (VM) as the basic unit of allocation. Using appropriate resource allocation algorithms, multiple VDCs can be hosted on a physical data center.

Shivam Nagpal et al (2013) proposed a fault tolerant model that takes decisions. Reliability of a node is estimated on the basis of 2 parameters; accuracy and time. If any of the nodes does not achieve the level then backward recovery is performed by the system. This model focuses on adaptive behavior of processing nodes and the nodes are removed or added on the basis of reliability.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Hiep Nuyen[10] (2013) proposes that one of the biggest challenges for diagnosing an abnormal distributed application is to pinpoint the faulty components. Black-Box online fault localization system called F-chain has been presented that can pinpoint faulty components immediately after a performance anomaly is detected. F-chain is presented as: a practical online fault localization system for large scale Iaas clouds. This system does not depend upon prior knowledge i.e. previously seen and unseen anomalies, and is practical for Iaas clouds. To achieve higher pinpointing accuracy, an integrated fault localization scheme has been introduced that consider both fault propagation patterns and inter component dependencies.

III. CONCLUSION

Fault tolerance is an essential aspect of a cloud as most of the applications fail due to occurrence of faults during their execution. Due to fault, the running time of the application increases and resources of the cloud are wasted. So, an efficient technique to cop up with the faults is required in the cloud. All the techniques discussed here are highly efficient in detecting faults and recovering the system from it. Fault tolerance techniques are used to minimize failure impact on the system and application execution by predicting failures and taking an appropriate action before failures actually occur.

REFERENCES

1. W. Zhao, P. M. Melliar-Smith, and L. E. Moser. "Fault tolerance middleware for cloud computing." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 67-74. IEEE, 2010.
2. R. Jhawar, V. Piuri, and M. D. Santambrogio, "Fault tolerance management in IaaS clouds." In Satellite Telecommunications (ESTEL), 2012 IEEE 1st AESS European Conference on, pp. 1-6. IEEE, 2012.
3. S. Sidiroglou, O. Laadan, C. Perez, N. Viennot, J. Nieh, and A. D. Keromytis. "Assure: automatic software self-healing using rescue points." In ACM Sigplan Notices vol. 44, no. 3, pp.37-48, 2009.
4. G. Chen,, H. Jin, D. Zou, B. B. Zhou, W. Qiang, and G. Hu. "SHelp: Automatic Self-healing for Multiple Application Instances in a Virtual Machine Environment." In Cluster Computing (CLUSTER), 2010 IEEE International Conference on, pp. 97-106. IEEE, 2010.
5. Nguyen, H., Shen, Z., Tan, Y., & Gu, X. (2013, July). FChain: Toward black-box online fault localization for cloud systems. In Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on (pp. 21-30). IEEE.
6. Meshram, A. D., Sambare, A. S., & Zade, S. D. (2013). Fault Tolerance Model for Reliable Cloud Computing
7. Jhawar, R., Piuri, V., & Santambrogio, M. (2013). Fault tolerance management in cloud computing: A system-level perspective. Systems Journal, IEEE, 7(2), 288-297.
8. Joshi, S. C., & Sivalingam, K. M. (2014). Fault tolerance mechanisms for virtual data center architectures. Photonic Network Communications, 28(2), 154-164..
9. Zeeshan Amin L, 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
10. Brian, O., Brunschwiler, T., Dill, H., Christ, H., Falsafi, B., Fischer, M., Zollinger, M. (2012). Cloud Computing. White Paper SATW.
11. Amal Ganesh , Dr. M.Sandhya , Dr. Sharmila Shankar, "A Study on Fault Tolerance methods in Cloud Computing", Advance Computing Conference (IACC), 2014 IEEE International.
12. Bertier, M., Marin, O., & Sens, P. (2003, June). Performance analysis of a hierarchical failure detector. In 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 635-635). IEEE Computer Society.