International Journal of Computing and Applications | **ISSN: 0973-5704**
Volume 13, Number 1, (January-June 2018), pp 91-99

SURVEY PAPER ON FAULT PREDICTION AND MITIGATION IN CLOUD COMPUTING

Vidhi Sutaria[1]

[1]*Department of Computer Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India.*
Email Id:vidhisutaria19031994@gmail.com

Abstract: Cloud computing provides on-demand service in computing engineering. This technology provides integration of software and resources which provide dynamic scalability in nature. These systems are beneficial, but there is also disadvantage is there. If the system is a fail, then it does not provide its functionality. So the solution is that it provides fault prediction and mitigation. It provides the capacity to the system to react smoothly when the system has failed or any unexpected hardware or software failure in the organization. This paper mentioned a better reason of fault prediction and mitigation methods, techniques and tools used for fault prediction and mitigation in cloud computing . In this paper mentioned, the techniques of fault Prediction and mitigation and implementation of fault prediction and mitigation into a simulator.

Index Terms: Cloud computing, Fault prediction, Fault Mitigation, Proactive, Reactive, Hardware fault, Software Fault.

1. INTRODUCTION

A. Cloud Computing

Cloud computing is another innovation is range of vast scale appropriated processing which expands upon on the possibility of virtualization, network computing, utility registering, to execute an administration arranged foundation for diminishing IT dormancy for the client for giving incredible adaptability and aggregate cost of bill and all above on-request administrations to a common plenty of figuring resources[1].

B. Fault Prediction and Mitigation

Fault Tolerance is the procedure of finding faults and failures in a system. If a fracture occurs or there is a hardware failure or software failure, then also the system should work properly. Failures should be handled in an active way for reliable Cloud Computing. It will also give availability and Robustness against the system hardware and software failure into the system.

C. Benefits to Implemented Fault Prediction and Mitigation System

Fault prediction and mitigation intend to accomplish power and constancy in any system. It has two types of techniques: proactive and reactive. The Proactive method can define as to remove the error before it actually comes. The Reactive method can define as to reduce the failure or recover the fault when it actually arrives [1].

2. TYPES OF FAULT

The inability of a system to do its required task caused by an anomalous state or bug in one or more than one parts of a system. Faults are the hypothesized or adjudged cause of an error the main cause which causes an error.[2].

Software Fault: Most of the fault-tolerant strategies have focused towards structuring systems that can recover themselves from the faults that usually occur in hardware modules, this involves splitting a computing system into modules. So if a particular module gets failed, another module can continue its functioning[3].

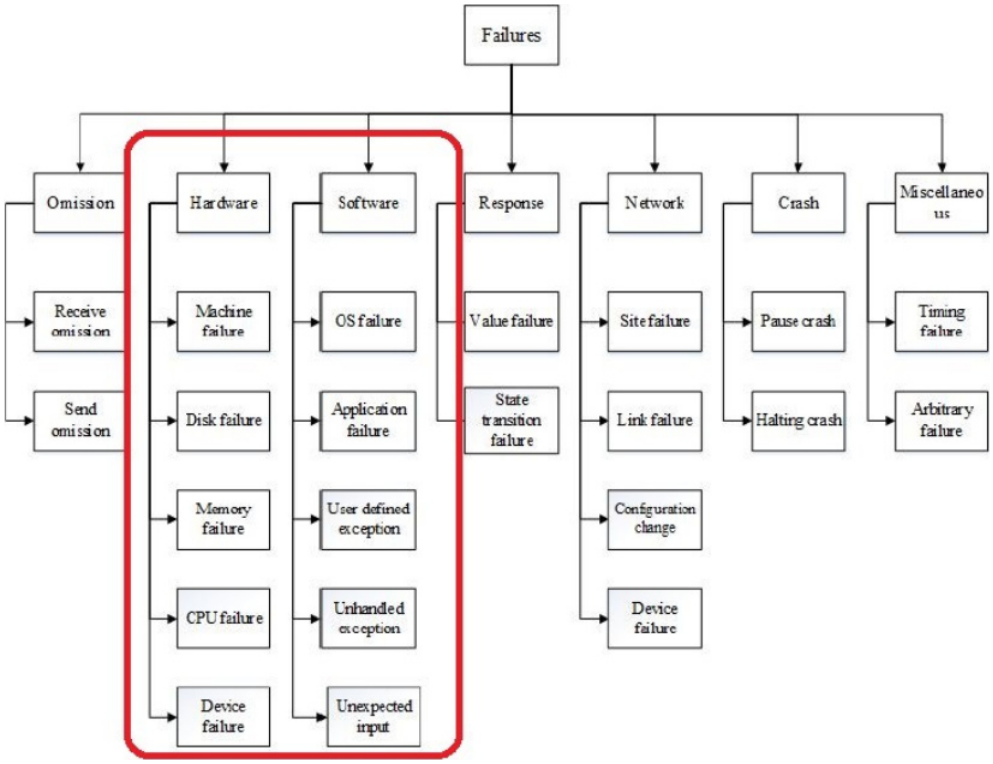

Figure 1: Types of fault[2]

It is similar to hardware approach but here more consideration is on tolerating faults at the software level. For achieving this various static and dynamic redundancy approaches are used[3].

A. Fault Prediction and Mitigation Techniques in Cloud Computing

Proactive Fault Tolerance: This method of is to avoid extra effort for recovering the failed tasks, nodes, by predicting the fault in before and replace them with other working parts. Proactive fault tolerance systems are able to fulfill the time constraints set by the real time systems[4].

Reactive Fault Tolerance: When an actual fault occurs in the system, then this method help to reduce the impact of failures on the running system. These techniques provide good fault tolerant solution for general computing application, but a problem with this technique is that it can not fulfill the time constraints set by real time computing systems[4].

B. Types of Proactive Fault Tolerance

Software Rejuvenation: Programming Rejuvenation is the technique in which an application is promptly ended and afterward restarted as a spotless state. There are different restoration interim and the application is restarted at each interim with a clean inward state. In this method, intermittent reboots are planned for the framework[5].

Using Self Healing: When multiple components of a single system are running on different multiple VM and when a fault occurs by using self-healing the failure of different application instances can be handled automatically[5].

Using Preemptive Migration: By using this technique, the parts of a system running on a computing node that is about to fail are migrated to different nodes. By using preemptive migration the application is migrated to a different node before actual fault occurs[5].

C. Types of Reactive Fault Tolerance

Check pointing/Restart: This method used When doing task scheduling, the check- points are inserted to identify fault incidence. These techniques take less computation and less time as a result of the task is restarted at the previously checked point. There is no ought to restart the full task[5].

Replication: Replication is a very effective technique in fault tolerance. In this, there are various replicas of any application or task on different resources. When any fault occurs in the system then execution continues to succeed until all replicated tasks are destroyed[5].

Job Migration: When due to resource failure or machine failure any task fails then the task is shifted on another virtual machine where it continues its execution of process[5].

Sguard: It requires less registering investment to ordinary process time and accessible more assets free. It is depended on rollback recovery. It takes less time to normal process and makes a lot of resources out there[5].

Retry: In this method first of all the unsuccessful task is re-executed on the same resource from starting. If the task continues to fail on different executing points, then to get rid of the additional overhead the average execution time is computed. A threshold value is set to limit the number of retries of the failed job on the same machine[5].

Task Resubmission: Task resubmission means that when any task fails then it is recommitted either to the same machine or a different one.[5]. User defined exception handling:

When any task/job fails then the user gives the efficient treatment to that failed jobs for work flow. In exception, handling user can write code into the try, catch and finally block to throws exception and it handles the exception[5]. Rescue workflow :

This technique permits the work stream to proceed regardless of the possibility that the undertaking comes up short until it gets to be difficult to push ahead without cooking the fizzled task. It permits the framework to continue working after the disappointment of any assignment until it won't have the capacity to continue without correcting the shortcoming[5].

3. MODELS AND TECHNIQUES OF FAULT PREDICTION AND MITIGATION

A. Comparison Among Various Model

AFTRC a proposed show for ongoing distributed computing it is relies on upon the constant framework and it gives advantage as the figuring limit, adaptable, and virtualized for a continuous framework. LLFT is a given model which conveys a low dormancy, adaptation to non-critical failure (LLFT) middleware for giving adaptation to internal failure to dispersed applications sent inside the distributed computing environment as an administration offered by the proprietors of the cloud. FTWS is a given model which gives a replication and resubmission and assemble work process planning calculation for giving adaptation to non-critical failure by utilizing the need of the assignments. FTM is a model which is conquer the constraint of existing strategies for the on-request service[6]. It is use To accomplish the unwavering quality and strength in adaptation to internal failure show. Treat show gives the accessibility demonstrating structure, which develops a semi-naturally complete accessibility display for framework particular. The Vega-superintendent is work for virtual group to beat the 2 issues: ease of use and security. FT-Cloud utilizes the segment conjuring structure and recurrence for recognizing the component. Magi-Cube a very tried and true and low excess stockpiling design for distributed computing.

B. Various Fault Prediction and Mitigation Techniques

In the given section it describes various existing tools and technology. Table 1 describes various fault tolerance models and Table 2 describes various tools used to implement existing techniques. Table 2 compares these tools based on their Fault tolerance techniques, system, Programming framework and application, Different fault tolerance techniques. HAProxy is used for server fail over in the cloud. ASSURE presents protect focuses for taking care of software engineer foreseen disappointments. Hadoop is utilized for information escalated applications, yet can in like manner be utilized to actualize adaptation to internal failure systems in a cloud situation. Amazon Elastic Compute Cloud (EC2) gives a virtual registering environment to run applications. This table portrays the different adaptation to internal failure instruments and examination among them. By this, we can identify

Table 1
Various Fault Tolerance Models[7]

Model Name	*Protection against type of fault*	*Applied procedure for tolerance the fault*
AFTRC	Reliability	1. Delete node, depending on their reliability 2. Back word recovery with the help of check pointing
LLFT	Crash-cost, trimming	Fault Replication.
FTWS	Dead line of work flow	Replication and resubmission of jobs
FTM	Reliability, availability, on demand inspection and repair	Replication user's application and in the case of replica failure use algorithm like gossip based protocol.
CANDY	Availability	1. It assembles the model components generated from IBD and STM according to allocation notation. 2. Then activity SNR is synchronized to system SRN by identifying the relationship between action in activity SNR and state transition in system SRN.
VEGA-WARDEN	Usability, security, scaling	Two layer authentication and standard technical solution for the application.
FT-CLOUD	Reliability, crash and value fault	1. Significant component is defined based on the ranking. 2. Optimal ft technique is deter- mined.
MAGI-CUBE	Performance, reliability, low storage cost	1. Source file is encoded in then splits to deliver as a cluster. 2. The file recovery procedure is triggered is the original file is lost.

Table 2
Tools Used To Implement Existing Fault Tolerance Techniques

Fault Tolerance Techniques	*System*	*Programming Framework*	*Environment*	*Fault Detected*	*Application Type*
Self Healing, Job Migration, Replication	HAProxy	Java	Virtual Machine	Process/node	Load balancing Fault Tolerance
Check pointing	SHelp	SQL,JAVA	Virtual Machine	Application Failure	Fault tolerance
Check pointing, Retry, Self Healing	Assure	JAVA	Virtual Machine	Host, Network Failure	Fault tolerance
Job Migration, Replication	Hadoop, Sguard, Resc	Java, HTML, CSS	Cloud Environment	Application/node failures	Data intensive
Replication, Sguard, Task Resubmission	AmazonEC2	Amazon Machine Image, Amazon Map	Cloud Environment	Application/node failures	Load balancing, fault tolerance

the performance of the various fault tolerance platform and among them, it can be classified that which is gives better performance. It can be an analysis that these tools are classified the some of the techniques among all the techniques. Which is identify the some of fault among all the hardware as well as software fault. So it can be better to implement programming framework which provides us to identify maximum fault into the system and recover that fault and system give better performance.

4. RELATED WORK

Alain Tchana and Laurent Broto introduced Approaches which is describe the fault prediction and mitigation techniques in autonomic repair technique[4]. In this, describe this with experiments and results where fault tolerance techniques are executed in an autonomic cloud environment[4]. The first strategy depicted in leaving solely the obligation of FT administration to one cloud client or supplier; the second one portray in sharing the duty between the two cloud client[4]. The method that is used two strategies is feasible for repairing a flawed application. The first is a stateless application which Repair blame in restarting the flawed server on the same VM. The second strategy is state-full servers as the MySQL database[4]. Tools that are used Open Nebula, Microsoft Windows Azure platform, HA-Proxy. VM fault can be improved by the check pointing which consists in storing only the difference between successive VM states[4].

Deepali Mittal, and Ms. Neha Agarwal designed model in that described Fault Tolerance is the process of finding faults and failures in a system[8]. In that proposed Dependability Assessment Algorithm and Decision Mechanism Algorithm. To develop this algorithm used virtual Machine. In the present scenario, a number of models are there which provide a different method to improve the system. Yet at the same time, there are a number of issues which requires some sympathy toward each edge work. In this, a few vulnerabilities none of them can give by the every single expected part of faults[8].

Pankaj Deep Kaur and Kanu Priya defined Fault Tolerance Techniques and Architectures for fault tolerance[3]. It presents, in brief, the need and matrices for performing fault prediction and mitigation in the cloud. It gives an outline of the prevalent architectures and the existing techniques for that have been analyzed and compared[3]. It has focused on various existing fault tolerant techniques, architectures for the cloud environment and concluded that there is a necessity of a more effectual and reliable technique which is cheaper than the prevailing techniques[3]. It describes Reactive and Proactive fault tolerance and used SHelp, HA-Proxy, Hadoop, AmazonEc2. More Future research works can explore on MPI architecture in order to present a reliable and less costly technique for fault-tolerance. To achieve reliability, future work can be documented by the implementation of the fault tolerant techniques over a cloud supported simulator or cloud tested[3].

Himanshu Agarwal and Anju Sharma have proposed Fault Tolerance Techniques it describes that better understanding of fault tolerance techniques which are used according to their policies and tool also describes the comprehensive taxonomy of faults, errors, and failures[2]. The usage of taxonomy and survey results are not only used to identify the similarities but also to identify the areas requiring for future research[2]. Fault prediction and mitigation is a property of a system to work properly if the system has failed. It plays a major role in providing availability and reliability of services to the user. It describes various fault tolerance techniques for proactive and reactive methods which may cause failure of machines in cloud infrastructure[2].

Mehdi Nazari Cheraghlou and Ahmad Khadem-Zadeh described fault tolerance architecture in cloud computing[9]. In this described that, techniques for making a limit of Fault Tolerance in Cloud, arrangements of the usage of these strategies are expressed, the distinctive existing models for that lastly, they are thought about in term so of the kind of approaches in the engineering and the strategy for blame forecast and alleviation [9]. AFTRC and PLR models have completely in view of receptive adaptation to non-critical failure technique. In any case, they are distinctive in blame forecast stage. AFTRC has utilized do their forecast technique while PLR has put forth a concentrated effort identification strategy. In blame

recuperation stage, they both go about as framework recuperation[9]. They defined fault tolerance techniques for proactive and reactive methods and for that they implemented it using Map Reduce. It was watched that the depicted models profited from adaptation to internal failure strategies in various ways. The specialists are prescribed to furnish new stage with higher adaptation to internal failure in future[9].

Prasenjit Kumar Patra and Harshpreet Singh introduced fault Tolerance Techniques[1]. It has been classifying that to give a superior comprehension of blame recoup methods utilized for as a part of cloud situations with some effectively characterized model and look at them[1]. It described the fault parameter and described its various parameters, techniques, methods, tools and compare them with each others[1]. They implemented proactive and reactive methods in SHelp, HA-Proxy, Hadoop, AmazonEc2 platform. But there are a number of problems which need some important for every model. So it is assumed to remove all the problems in existing models and try to remove all that problems and make a robust model which will cover all fault detection and recover aspects[1].

Harpreet Kaur and Amritpal Kaur described a Survey which is described to study different types of failure and different techniques for handling them[10]. By taking a correct action before or after the failure arrived, the system can be predicate fault within it and recover the fault [10]. In that discusses the need for fault prediction and mitigation by its different techniques for implementing fault recover in simulator[10].

S. Suguna and K. Devi proposed VMFT: In that Proposed the Virtual machine adaptation to internal failure (VMFT)[11]. In this procedure, the machine endures the disappointment of VM in view of reliability. It gives high unwavering quality, accessibility and decreases the procedure when it is registered on the VM[11]. The characterized VMFT procedure endures the blame in view of the dependability of the figuring hubs. It gives high unwavering quality and accessibility of assets to the end client[11]. It implemented Virtual Machine fault tolerance in CloudSim Simulator. but in the future better efficient algorithm can be implemented for virtual machine fault tolerance[11].

Priority Scheduling Algorithm in Cloud Computing for fault introduced by Seema Bawa and Nimisha Singla[12]. In this, it portrays new need booking calculation with adaptation to non-critical failure. The calculation first calendars the assignments as indicated by need and after that reallocated undertakings from fizzled server to another server as it gives the adaptation to internal failure property furthermore the give better result. This calculation gives preferred execution over another calculation[12]. The Priority scheduling algorithm implemented on Cloud Sim simulator. There is need of more vitality effective calculations later on and also vitality utilization calculation required. This calculation can be further enhanced by acquainting dynamic nature with its need task usefulness[12].

Dilip Kr Baruah and Lakshmi P. Saikia described Fault recover is the functionality that provides a system to continue work properly if there is fault occur[13]. The fault should be recover effectively so its provide robustness in the system[13]. Recent research includes the already done fault recover techniques to RAID disks where information is stored across various disks to improve bandwidth and data can be recollected if a disk fails[13]. In this describes an analysis of different Algorithm for fault tolerance. Adaptation to internal failure techniques are required to end up distinctly progressively imperative in VLSI gadgets to recoup expanding clamor issues and enhance by enduring imperfections that are happened to on vast and complex chips[13].

A. Problem Statement

Given by the literature survey, we can conclude about the various failures techniques and their suggested methods and tools that are used for the fault tolerance. By this method and techniques we are supposed to by-forget the error type and solve that error with it mitigation techniques. So Our proposed study is related to predicting the fault into the corresponding system or application in the cloud and buffet that error into two categories if it is hardware error or software error. And this we can perform with the HTTP status error code. And after identifying the error we are supposed to recover it with the mitigation techniques or event tree analysis. So with this we can predict the error

and make a system robust even if the error comes. Proposed system design and fault tree analysis is mentioned in the next section. By the fault tree and event tree analysis we done prediction and mitigation along with the error code and its methods. By proposed system design it can describe the various types of software fault and hardware fault and techniques for mitigation that particular fault. It also predefined mitigation technique for every specific error code. So, the fault can be predict by the reactive fault tolerance methods and it can be mitigated by the among mention any one of them technique. So it can be prediction before the fault is occur and recover by the mitigation techniques. So given solution is perform and analysis and experimented and give result on simulator and defined appropriate solution for the fault prediction and mitigation.

5. PROPOSED SYSTEM DESIGN

For fault prediction and mitigation we proposed system design. Which is described fault prediction and mitigation in the system. Which first of all identify the fault and predict the fault using Fault Tree Analysis (FTA). According to that, it will identify by the error code if it is hardware fault or software fault. After identifying the reason behind the system failed it will mitigate the fault to recover the system fault. For that system take action according to the Event Tree Analysis (ETA). So, by collaborate FTA with ETA it will predict the system fault, identify the reason behind it and recover the system fault.

In given figures, it describes fault prediction and mitigation various techniques. For fault prediction, it defined various types of fault among them one of the faults can be predicted by the fault tree analysis and after one of them fault and reason behind it can predict by the system after that it can mitigate the particular fault according to the mitigation techniques. By this way, the system can predict the fault and mitigate that fault according to the appropriate action using event tree analysis.

By this way, the system can recover the fault by predicting the fault and mitigate the fault. thus the system can be work properly even if the fault occurs in the system.

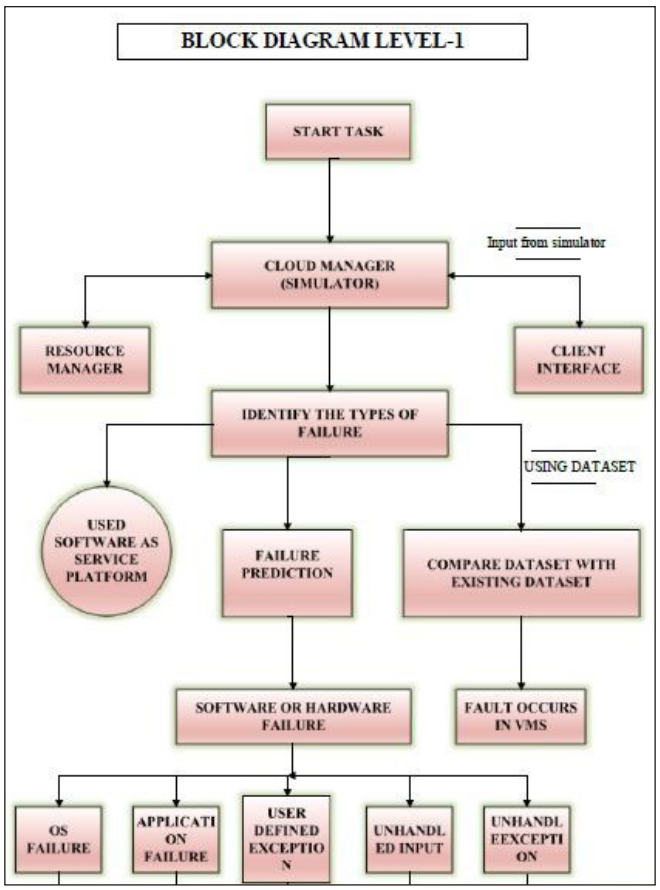

Figure 2: System Design for Fault Prediction

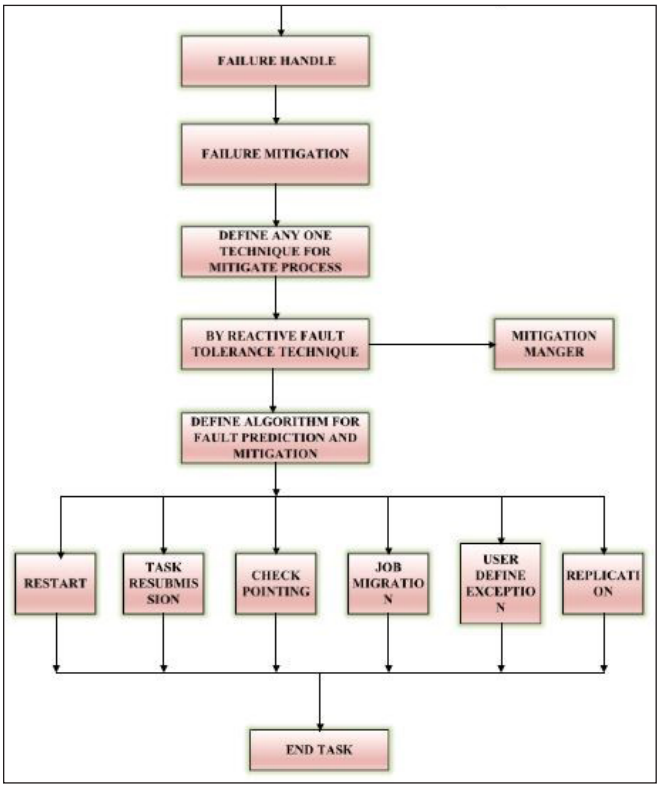

Figure 3: System Design For Fault mitigation

A. Software Failures Codes

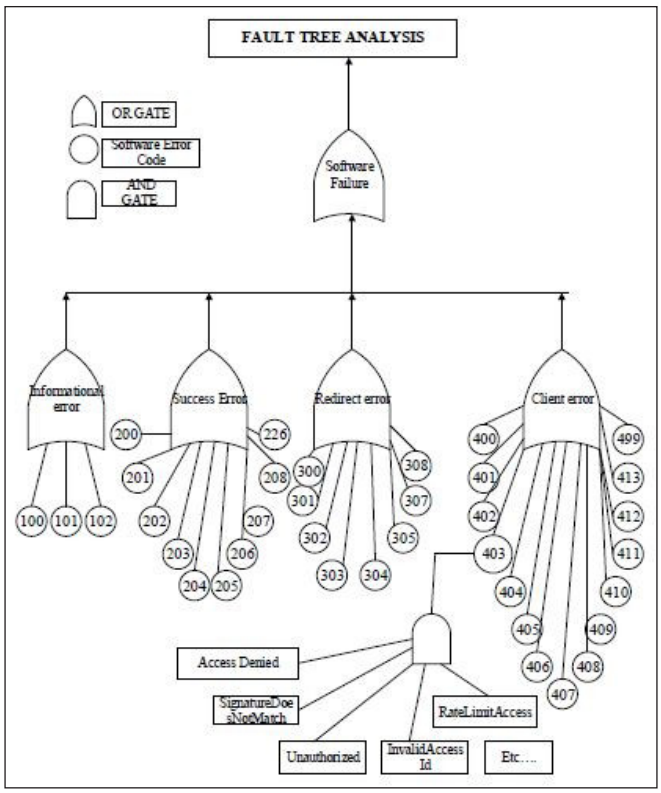

Figure 4: Software Failure codes

B. Hardware Failures Codes

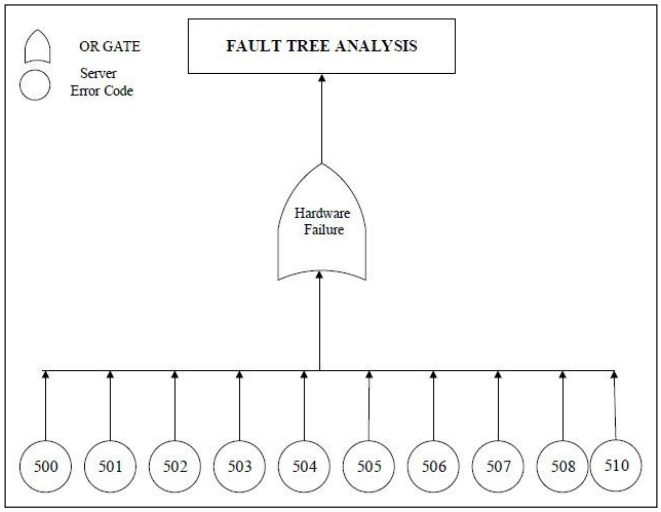

Figure 5: Hardware Failure codes

In the given figures it describes hardware and software failure HTTP codes. By that, we can identify the particular one failure and reason behind it. By that code, we can predict the particular failure into the system and take action according to that fault. There is one particular HTTP code for each and every error if it is hardware error or it is a software error. By this HTTP code, we can by forget the particular error among all the other errors. By this, we can identify the error and reason behind it.

6. CONCLUSION

Fault prediction and mitigation used to provide system availability and robustness when system have hardware or software fault. This literature review focused on the various fault prediction and mitigation techniques and tools used for implementing it and compare this technique and provide the best solution for fault prediction and mitigation.

7. FUTURE WORK

To implement task scheduling using FCFS and if the faulty task arrives then predict the fault, if it is hardware or software failure. Take action for preventing the system from particular fault. Identifying the other failures apart from hardware and software as omission, network, response, crash, and mitigating their effects. Find techniques for recover that fault and make the system robust.

References

[1] P.K. Patra, H. Singh, and G. Singh, "Fault tolerance techniques and comparative implementation in cloud computing," International Journal of Computer Applications, Vol. 64, No. 14, 2013.

[2] H. Agarwal and A. Sharma, "A comprehensive survey of fault tolerance techniques in cloud computing," pp. 408–413, 2015.

[3] P.D. Kaur and K. Priya, "Fault tolerance techniques and architectures in cloud computing-a comparative analysis," pp. 1090–1095, 2015.

[4] A. Tchana, L. Broto, and D. Hagimont, "Approaches to cloud computing fault tolerance," pp. 1–6, 2012.

[5] R. Jhawar, V. Piuri, and M. Santambrogio, "Fault tolerance management in cloud computing: A system-level perspective," IEEE Systems Journal, Vol. 7, No. 2, pp. 288–297, 2013.

[6] A. Ganesh, M. Sandhya, and S. Shankar, "A study on fault tolerance methods in cloud computing," pp. 844–849, 2014.

[7] A. Bala and I. Chana, "Fault tolerance-challenges, techniques and implementation in cloud computing," IJCSI International Journal of Computer Science Issues, Vol. 9, No. 1, pp. 1694–0814, 2012.

[8] D. Mittal and N. Agarwal, "A review paper on fault tolerance in cloud computing," pp. 31–34, 2015.

[9] M.N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "A survey of fault tolerance architecture in cloud computing," Journal of Network and Computer Applications, Vol. 61, pp. 81–92, 2016.

[10] A.K. Harpreet Kaur, "A survey on fault tolerance techniques in cloud computing," International Journal of Science, Engineering and Technology, 2015.

[11] D.o. C.V.E.C.K.S. Suguna, K. Devi, "Vmft: Virtual machine fault tolerance in cloud computing," International Journal of Innovation and Scientific Research, 2016.

[12] N. Singla and S. Bawa, "Priority scheduling algorithm with fault tolerance in cloud computing," International Journal, Vol. 3, No. 12, 2013.

[13] P.R.S.D.o. C.S.E.A.d. T.U.G.I. Dilip Kr Baruah, Lakshmi P. Saikia, "A review on fault tolerance techniques and algorithms in cloud computing environment," International Journal of Advanced Research in Computer Science and Software Engineering, May-2015.