International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

PAPER ID: 11A16F

A REVIEW ON THE TOOLS AND TECHNIQUES FOR EFFECTIVE FAILURE DETECTION AND PREDICTION IN CLOUD COMPUTING

Saleh M. Alqahtani [1*], Hamza Arishi [1*]

[1] *College of Computing and Informatics, Saudi Electronic University, SAUDI ARABIA.*

ARTICLEINFO

Article history:
Received 02 May 2020
Received in revised form 03 September 2020
Accepted 15 September 2020
Available online 24 September 2020

Keywords:
Cloud service; Proactive fault tolerance; Reactive fault tolerance; Cloud computing threat; Cloud computing risks; Cloud computing vulnerabilities, Cloud fault detection.

ABSTRACT

Cloud Computing is a model that supports services and computer resources like computing power, storage, and bandwidth to deliver IT services in the organization. With the increasing usage of the Internet and mobile devices, cloud computing has also become a widely adopted model of delivering services through the Internet. Cloud computing is a combination of self-service and automatic computing. The main problem is the complexity of detecting a fault in a cloud-based system due to its large-scale integration and dynamic nature of the cloud. In this paper, we discuss cloud computing in the light of failure detection and prevention to build a reliable cloud-based system that can detect and prevent failures before exploitation.

Disciplinary: Computer and Information Sciences, Digital Business Management and Service.

1 INTRODUCTION

Recently, Cloud Computing has become an essential keyword in the field of Information Technology. Cloud computing is the reality of the dream called "Computing as Utility" as it has massive potential in the current market to revolutionize the IT sector. The term "Cloud Computing" has two keywords where "Cloud" stands for "Internet" and "Computing" stand for "Processing and memory." So, "Cloud Computing" is the term created by the concept of "Computing Power Accessible Virtually from anywhere."

Many business organizations adopted cloud computing to bring competitive advantages compared to their peers to grab more market share by providing better services to their customers. However, like other information technology processes, it also has some drawbacks as well. As the cloud computing concept is entirely based on networking, any network failure can disrupt the total system laming business productivity (Suryateja, 2018). It became easier to hijack one's data as

*Corresponding author (S.M. Alqahtania, H.Arishi). sm.alqahtani@seu.edu.sa, a.hamzah@seu.edu.sa

everybody uses the cloud to store their personal information to get rid of physical storage devices and for virtual accessibility of their data. It has become essential to make a cloud system fully secure and make some tools and techniques to detect faults before collapsing the system.

It is a big concern for the cloud service provider companies to detect and prevent any failures in their cloud computing system. However, it is critical to recognize a fault before a collapse, but understanding the nature of faults is essential to prevent such faults in the future. These faults can provide unavailable resources and make the web applications and web servers down for a long time, leading business losses to the service providers. An example could understand that when Amazon was down for only 45 minutes due to an unexpected error in the system, it led to about 45 million dollar loss to Amazon (Tchernykh et al., 2019). As the cloud hardware and software continuously changed, the fault detection mechanism needs to realize fundamental differences between normal cloud variation and real-time failures. Discussion of tools, techniques, and strategies for effective failure detection and prediction in cloud computing is something to look forward to through the study.

Cloud computing is widely adopted in business organizations and for personal uses due to the internet's rapid growth in recent years. This study aims to find out some tools and techniques to detect and prevent cloud computing faults. Based on the aims of this study, the following objective has set:

- To investigate the vulnerabilities present in cloud computing.
- To evaluate fault tolerance and fault taxonomy in cloud computing.
- To evaluate some tools and techniques to detect and to prevent a fault in a cloud-based system.
- This research work aims to answer the following questions:
- What is the importance of fault detection and prevention in cloud computing?
- How can the faults be detected before the system collapses?

2 METHODOLOGY

In this research, the applied research method is used to conduct the study, with gathered data relevant research papers related to failure detection and prevention in cloud computing outsourced through web-based tools like Google Scholar, PubMed Central, Prismatic, Scopus, etc. According to (Moges & Abebe 2019), applied research is best for this study with aims to find tools and techniques for effective failure detection and prediction of failure in a cloud computing system and find out vulnerabilities present in cloud services design.

3 CLOUD COMPUTING REVIEW

Adaptation of cloud-based technologies is growing daily in the construction of IT infrastructure for business, academic, government organizations, and people as data storage and processing. Though the cloud-based computing systems have many advantages, it also has some drawbacks in the form of security, reliability, and the performance of both computing and communication. In this study's literature section, the drawbacks present in cloud computing, recognition of faults, and some tools and techniques to prevent those faults will be discussed.

3.1 VULNERABILITIES PRESENT IN CLOUD COMPUTING

The vulnerability is the weakness of a system that hackers can access (Dwivedi & Dev, 2018; Shihab, 2020). A primary concern about cloud computing is security and privacy related to securing data and monitoring the use of data by the cloud service provider. Some of the weaknesses present in

cloud computing discussed below:

- Data Breaches: When sensitive or confidential data related to a person or an organization is accessed, copied, or transmitted unethically, the situation is called a data breach. In 2017, the data breach resulted in over 1.4 billion losses of records. It is a fatal risk in cloud computing, taking the number one position in the list of cloud computing vulnerabilities. The causes of this severe problem can be human error, targeted attacks by some hackers, application vulnerabilities, and lack of security measures.
- Data Loss: Natural disasters like floods, earthquakes, and human errors like accidentally deleted files and malware infection can cause the unavailability of data resulting in data loss. Precaution should be taken to avoid data loss by taking backup of the existing data into multiple locations as required data can be accessed without any hassle.
- Malicious Insiders: Insider threat is one of the most dangerous threats in cloud computing. An insider in the form of the formal employee, system administrator, business partner, or third party vendor can use confidential information that causes enormous losses to the service provider. An example, it can be said that due to a recent data breach in Sage, investors lost millions of dollars as the stock price of the company dropped by 4.3%.
- Denial of Service: In this type of attack, a legitimate user cannot access their data or application due to the attack, originating from one source machine.
- Account Hijacking: In cloud computing services, there is a severe risk of account hijacking. Account hijacking is a process of accessing one's account credentials without legitimate users' permission using unlawful practices. Fraud by phishing is one of the most popular types of account hijacking to access one's data for personal gain.
- Unprotected IoT Devices: Recent technological advancements in communication software brought us a term called "Internet of Things," where many devices can communicate with each other to serve the user's needs. As IoT devices have created massive automation, configuration, and patching, one error can cause multiple problems to generate millions of attack vectors. Weak network security can also lead to severe problems as IoT devices are connected through a network to communicate between them.
- Ransomware: Ransomware is a malware that locks the victim's computer files by creating encryption on the victim's files and other resources. In 2016, the FBI commented that 4000 ransomware attacks happened in a day with an increase of 300% from previous years. In 2017, the world saw the WannaCry ransomware's menace that disabled the data in many companies and government agencies.

3.2 TOOLS AND TECHNIQUES FOR FAILURE DETECTION IN CLOUD COMPUTING

Cloud computing is an essential technique for providing demanded services to users at a low cost. To project the correct result despite faulty components, fault tolerance and reliability have great importance (Amin et al., 2015). Demand for fault tolerance is increasing rapidly to achieve reliability in real-time computing. The fault tolerance technique is used to detect a fault and predict them before the fault occurs. The necessity of fault tolerance is to achieve reliability in real-time computing. The fault tolerance technique used in cloud computing considered with various parameters such as

- Throughput: The throughput defines the number of completed tasks, and it should be high for a cloud system.

*Corresponding author (S.M. Alqahtania, H.Arishi). sm.alqahtani@seu.edu.sa, a.hamzah@seu.edu.sa Volume 11 No.16 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID:11A16F http://TUENGR.COM/V11B/11A16F.pdf DOI: 10.14456/ITJEMAST.2020.315

- Response Time: Response time measured by the time taken to respond by an algorithm. The minimum value is preferred for response time.
- Scalability: Fault tolerance capacity should not be affected by some nodes of the algorithm.
- Performance: This parameter checks the effectiveness of a system. The performance of a system can improve by reducing the response time of the system.
- Availability: The reliability of that system can measure the availability of a system. An item's functioning at any given instance of time can tell as the availability of that system.
- Usability: A product that can use to what extent to complete goals effectually is called usability.

There are two types of fault tolerance techniques, namely a) Reactive fault tolerance and b) Proactive fault tolerance (see Figure 1).

Reactive Fault Tolerance: This type of fault tolerance technique is used after the possible occurrence of failures on a system—some of the techniques used in this policy listed below.

- Checkpoint/ Restart: Checkpoint is a process of restarting a failed task from the recent checkpoint rather than from the beginning. For large applications, it is a great technique.
- Replication: Various replicas of the task are run simultaneously on different resources for successful execution until the replicated task has not crashed. Significant components that are used for replication implementation are HAProxy, Hadoop, and AmazonEc2.
- SGuard: SGuard, which is based on rollback recovery, can execute in HADOOP, AmazonEc2.
- Retry: The task level's most straightforward technique is retry, allowing the user to resubmit the task on the same cloud resource.
- Task Resubmission: To resubmit the same task on the same operating machine or another machine is called task resubmission.
- User-Defined Exception Handling: The user defines specific actions of a task failure for workflows.
- Rescue Workflow: After any task's failure, it allows the system to continue until the fault is rectified.

Proactive Fault Tolerance: To predict the faults proactively and to replace the suspected components with working components is called proactive fault tolerance to avoid recovery from faults and errors. Some of the components that follow this policy are

- Software Rejuvenation: It is a periodic reboot process that starts as a fresh new state every time.
- Proactive Fault Tolerance using self-healing: Process of automatic control of failures at any instance occurred in an application.
- Proactive Fault Tolerance using Pre-emptive Migration: Observing and analyzing an application to prevent failure is the primary procedure of this technique depending upon the feedback-loop control mechanism.

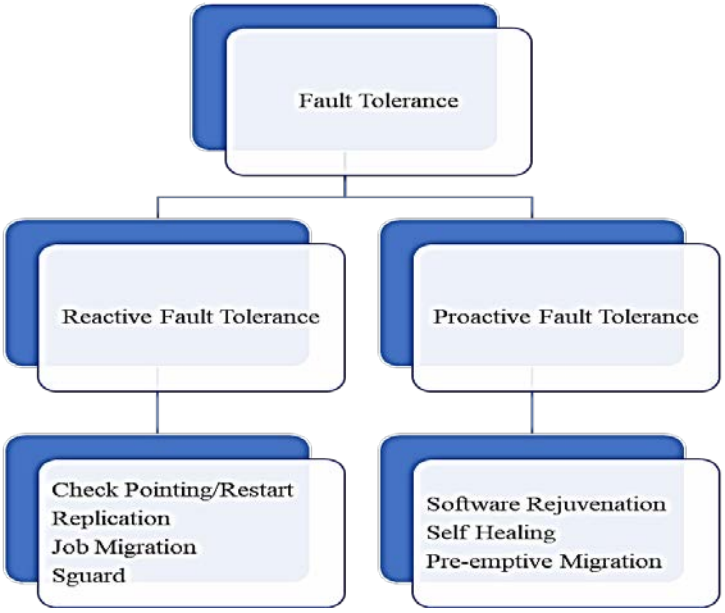

Figure 1: Fault Tolerance (modified from Amin et al. (2015)).

3.3 A CONCEPTUAL MODEL FOR RELIABLE CLOUD COMPUTING SERVICE

The concept of reliable cloud computing services can be understood from the above picture in which cloud computing structure has created with some layers that offer better management of cloud computing resources to make it more reliable (Gill & Buyya, 2018). Three main components in this architecture discussed below:

- Cloud Users: This layer's function is to receive user requests defined by required services in SLA to handle the incoming user requests by the workload manager. After handling those interactive or batch style requests, they are transferred to the middleware to provide the resources.
- Middleware: Middle and the leading layer of the conceptual model divided into subcomponents like accounting and billing, workload manager, resources provisional, resource monitor, and security manager.
- Information related to cloud services expenses, ownership cost, and user budget are kelp stored in accounting and billing modules.
- Workloads coming from the application are managed by the workload manager to execute them successfully with good Quality of Services (QoS) and transfer them to resource provisional.
- SLA manager, VM manager, and Fault manager are three parts of resource provisional. The official contract between user and cloud service provider managed by the SLA manager, maintaining required QoS. By using physical machines or VMs depending upon the availability of VMs, the VM manager facilitates and schedules the cloud resources to execute workloads base on required QoS. The fault manager's function is to detect the faults and probable causes to correct them and keep the system on track. Fault managers also find potential threats that can cause damage to the system in the future.
- The job of resource monitor is to monitor the required QoS for incoming workloads for keeping a continuous record of activities of the underlying infrastructure to make the services available.

*Corresponding author (S.M. Alqahtania, H.Arishi). sm.alqahtani@seu.edu.sa, a.hamzah@seu.edu.sa Volume 11 No.16 ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8 Paper ID:11A16F http://TUENGR.COM/V11B/11A16F.pdf DOI: 10.14456/ITJEMAST.2020.315

- The security manager has deployed virtual network security policies to secure a) data transmission between cloud users and providers and b) migration between workload and Virtual Machines of different data centers.
- Physical Infrastructure: Cloud data centers consisting of processors, network cards, storage devices, and disk drivers included in this layer to execute cloud workloads.

3.4 ADAPTIVE FAILURE DETECTION SYSTEM FOR CLOUD COMPUTING SYSTEMS

A Reconfigurable Distributed Virtual Machine (RDVM) influenced by virtual technologies is proposed to create a reliable cloud computing system that can simplify the failure-aware cloud management system. To build RDVM, Adaptive Failure Detection (AFD) is a crucial component. This RDVM infrastructure is built using a couple of virtual machines that run on top of physical servers in a cloud system (Talia, 2019). Different execution states of cloud services are incorporated within every virtual machine to run the client application. VMs are the basic unit of an RDVM infrastructure. Multiples VMs are hosted by each cloud server to multiply the resources of the underlying physical server. A thin layer called Virtual Machine Monitor (VMM or Hypervisor) manages hardware and export uniform interface to upper guest operating systems.

4 DISCUSSION

The primary data was collected by conducting interviews of five top officials working in the cloud services providing company as managers for sharing their experiences about the failure detection and prevention in the cloud-based system before the actual occurrence of any failure. The secondary data has been accumulated from different journals, research papers, and books written by various cloud computing authors.

It has been found by this study that through the cloud computing system is gaining popularity in the market for new businesses and start-ups, it does have some vulnerability present at the core level of the design architecture of cloud computing. Those weaknesses present in the cloud-based system make it prone to frequent failures, and the system collapses, affecting the business productivity of a cloud service provider company. Various researchers have proposed some tools and techniques to combat the failures before executing any fatal error. However, those tools and techniques' efficiency is limited, as any human error can destroy overall system effectiveness. As the cloud computing system designed with many layers incorporated in it, any fault on one of these layers can make the total system feeble. Cyber-attacks to a cloud-based system to hijack one's data are also dangerous in a cloud computing system. As participants, managers emphasized the security issues they faced during their daily activities due to cyber-attacks performed by hackers in ransomware and malware attacks for their gain.

By analyzing secondary data gathered from various journals and research papers, it has found that there are two types of fault tolerance methods are used in a cloud-based system to prevent failure. They are reactive fault tolerance and proactive fault tolerance methods. The adaptive Failure Detection system is also beneficial for detecting and preventing failures and understanding the causes that create a system's failure. As data is stored and migrated in, many data centers in a cloud-based system, unencrypted data can create severe privacy concerns resulting in loss of confidential data. It has been found that due to a data breach in the cloud-based system, investors in Sage lost millions of dollars as stock prices collapsed 4.3%. American intelligence organization FBI also emphasized that cyber-attacks have increased due to the rapid adaptation of the cloud computing system in businesses

and organizations. That is why proper tools and techniques are essential to detect a failure and prevent it before it occurs. By analyzing data, many researchers are working towards finding a concrete solution for early detection and future prevention of failures that take place within a cloud-based system to ensure uninterrupted cloud services to users by cloud service provider companies.

5 CONCLUSION

From this study, we can say that cloud computing's popularity proliferates as cloud-based services enable users to get rid of physical storage devices and enable businesses to increase their efficiency in the current competitive market scenarios. It is evident that in the future, most business organizations like finance, energy, and transport healthcare will adopt cloud-based services in their primary business operations. Though there may be an enormous number of benefits of cloud computing is available, it cannot be denied that the cloud-based system has vulnerabilities in its core architecture as well. In this study, we have emphasized on the weaknesses that make a cloud system prone to failure is also described. Cloud-based systems are more prone to cyber-attacks as it can be exploited easily by trained hackers to hijack someone's personal and confidential data. Data breaches and cyber-attacks in the form of a ransomware attack, Denial of Service (DoS) attack, and malware attacks are widespread in the cloud-based system. Therefore, to protect users' privacy, cloud service provider companies need to improve their system's data security. To detect and prevent failure in the cloud computing systems, fault tolerance technique is elaborated in this study, in which two types of fault tolerance methods that are Reactive Fault Tolerance and the Proactive Fault Tolerance technique have been briefly explained. Also, components of a conceptual model of reliable cloud computing services are explained and illustrated with a block diagram's help. Another technique for failure detection, the Adaptive Failure Detection (AFD) Technique, which is the main component of Reconfigurable Distributed Virtual Machine (RDVM), is also described and illustrated by a block diagram. To conduct this study applied research method used and qualitative research design has followed. Necessary primary data for this study has been collected by interacting with five executives, who were working in cloud service provider companies as a manager and by analyzing their interviews essential data points have noted and the secondary data collected from various research journals and books written by many prominent authors in this field.

By analyzing the facts about cloud computing failures, further research should be done to improve security for protecting users' confidential data, and more effective tools and techniques should be introduced for better failure detection. It also recommended that the causes of any faults should adequately be examined so that any future faults can be avoided. Though this study explained facts related to tools and techniques for failure detection in cloud computing properly, the future scope is available for further research to improve research outcomes.

6 ACKNOWLEDGMENT

The authors would like to thank Dr. Dinesh Mavaluru, College of Computing and Informatics, Saudi Electronic University, Saudi Arabia, for his guidance during this research work.

7 AVAILABILITY OF DATA AND MATERIAL

Information can be made available by contacting the corresponding author.

*Corresponding author (S.M. Alqahtania, H.Arishi). sm.alqahtani@seu.edu.sa, a.hamzah@seu.edu.sa

8 REFERENCES

Amin, Z., Singh, H., & Sethi, N. (2015). Review on fault tolerance techniques in cloud computing. *International Journal of Computer Applications*, *116*(18).

Dwivedi, U., & Dev, H. (2018). A Review on Fault Tolerance Techniques and Algorithms in Green Cloud Computing. *Journal of Computational and Theoretical Nanoscience*, *15*(9-10), 2689-2700.

Gao, W., Alqahtani, A. S., Mubarakali, A., & Mavaluru, D. (2019). Developing an innovative soft computing scheme for prediction of air overpressure resulting from mine blasting using GMDH optimized by GA. *Engineering with Computers*, 1-8.

Gill, S. S., & Buyya, R. (2018). Failure management for reliable cloud computing: A taxonomy, model, and future directions. *Computing in Science & Engineering*.

Moges, F. F., & Abebe, S. L. (2019). Energy-aware VM placement algorithms for the OpenStack Neat consolidation framework. *Journal of Cloud Computing*, *8*(1), 2.

Pannu, H. S., Liu, J., Guan, Q., & Fu, S. (2012). AFD: Adaptive failure detection system for cloud computing infrastructures. In *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)* (pp. 71-80). IEEE.

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). Research methodology. arXiv preprint physics/0601009.

Shihab, L. A. (2020). Technological Tools for Data Security in the Treatment of Data Reliability in Big Data Environments. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, *11*(9), 11A9M, 1-13.

Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: A review. *International Journal of Computer Sciences and Engineering*, *6*(3), 297-302.

Talia, D. (2019). A view of programming scalable data analysis: from clouds to exascale. *Journal of Cloud Computing*, *8*(1), 4.

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581.

Saleh M. Alqahtan is a Lecturer at the Department of Information technology at Saudi Electronic University, Saudi Arabia. His research interests lie in the area of Data Science, e-Commerce, and Cybersecurity.

Hamza Arishi is a Lecturer at the Department of Information technology at Saudi Electronic University, Saudi Arabia. He received a Master's degree from Gannon University. His research interests span both Data Mining and Machine Learning. Much of his work has been on improving the Understanding, Design, and performance of Sentiment Analysis and Machine Learning, mainly through the Application of Data Mining, Statistics, and Performance Evaluation.