Journal of Soft Computing and Decision Support Systems

Hybrid Service for Business Contingency Plan and Recovery Service as a Disaster Recovery Framework for Cloud Computing

Fatemeh Sabbaghi [a,*], Arash Mahboubi [b], Siti Hajar Othman [a]

[a] Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM), Malaysia
[b] Queensland University Technology (QUT), Australia

* Corresponding author email address: mfzsab@gmail.com

Abstract

Cloud computing is the latest effort in delivering computing resources as a service to small and medium sized enterprises. These enterprise organizations require installing and maintaining expensive equipment to keep business up and running at all the times. Naturally this requires building an infrastructure flexible enough to respond to any threat under all circumstances. Any disaster may be considered to be a threat associated with the IT infrastructure in a data center. Disaster can occur either naturally or by humans. This paper is focused on how disaster may be controlled in a cloud computing data center which provides services to an organization and how to keep the organization business running while a disaster strikes. The availability and performance of any service is measured by its overall uptime. Recent recovery techniques that have been developed in cloud computing domain have several advantages and disadvantages. Therefore, researchers should conduct some investigations in this field. A hybrid service which utilize redundancy and fault tolerance techniques for providing more accurate recovery in cloud computing when disaster strikes is proposed in order to overcome these challenges in this paper. This hybrid service integrates the Infrastructure as a Service (IaaS) and Disaster Recovery as another Service (DRaaS). The proposed framework is formed by the integration of five essential types of proven redundancy techniques that have a major impact on the uptime of the services during disaster in cloud data centers. For evaluation of the proposed framework, a survey was conducted through a questionnaire presented to and filled by networking professionals and experts. The outcome of data analysis indicates that redundancy-based disaster recovery framework improves the performance of data center recovery and results in a high level of availability of the restored enterprise when disaster strikes. A total of 59.4 % of survey respondents accepted the fact that this framework reduces more than 70 % of threats associated with disaster.

Keywords: Cloud computing, Disaster recovery, Infrastructure as a Service (IaaS), Disaster Recovery as a Service (DRaaS)

1. Introduction

Cloud Computing is a technology that provides services to the users and access to the resources regardless of geophysical location. It consists of several service models for different types of organizations. These services may consist of private or global services. Cloud computing consists of three major services namely Infrastructure as a Service, Platform as a Service and finally Software as a Service. These services are scalable on consumer demand that can be priced on a pay-per-use basis (Bohm et al., 2010). However, cloud services are demanded in enterprise organization for the last several years (Sriram and Khajeh-Hosseini, 2010). Nevertheless, cloud may consist of several data centers or individual data centers that are dependent on the size of organization. Cloud often leverages massive scale, homogeneity, virtualization, resilient computing, low cost software, geographic distribution, service orientation, and advanced security technologies. The last aspect is composed of four deployment models in cloud computing including Private, Community, Public, and Hybrid Clouds. These resources are provided by service providers and require minimal effort for management. Third party management is also applicable (Mell and Grance, 2011; Susanto et al., 2012; Suganya, 2015).

Most enterprises are equipped with expensive IT infrastructure complex network architectures that keep their business running. These infrastructures required management, maintenance, protection to keep business running and avoiding any business contingency. Due to the fact that data in any circumstances should be available to the customers and partners of the organizations, any single point failure might cause unlimited damage to the business impacts. In other words, there are internal and external threats to hard and soft assets and organizations must provide effective prevention and recovery for their assets. In fact, critical incidents may occur any time either naturally or accidentally. However, one form of these incidents is a disaster. Almost all enterprise organizations take precautions and protect the assets of the organization