Chapter 11
Managing Multi-Cloud Data Dependability Faults

Mohammed A. AlZain
Taif University, Saudi Arabia

Alice S. Li
La Trobe University, Australia

Ben Soh
La Trobe University, Australia

Mehedi Masud
Taif University, Saudi Arabia

ABSTRACT

Cloud computing is considered a great paradigm that enables access to large scale, on demand, flexible computing infrastructure. Lower infrastructure cost and better application performance are some of the benefits of utilizing a cloud computing model. With the appearance of the new generation of multi-cloud computing, clients can benefit from a diversity of services. However, data security has become an important requirement for clients when dealing with clouds that may fail due to faults in the software or hardware, or attacks from malicious insiders. Hence, building a highly dependable and reliable cloud system has become a critical research problem. To that end, this chapter investigates and presents the results in relation to that how Byzantine fault tolerance (BFT) and secure cloud data storage and sharing techniques can be deployed to manage multi-cloud data dependability faults.

INTRODUCTION

Cloud computing is considered a great paradigm that enables access to large scale, on demand, flexible computing infrastructure. Lower infrastructure cost and better application performance are some of the benefits of utilizing a cloud computing model. With the appearance of the new generation of multi-cloud computing, clients can benefit from a diversity of services. However, data security has become an important requirement for clients when dealing with clouds that may fail due to faults in the software or hardware,

DOI: 10.4018/978-1-5225-7347-0.ch011

or attacks from malicious insiders (Tiwari and Joshi 2018). . Hence, building a highly dependable and reliable cloud system has become a critical research problem (Williams and Griffin 2018). It means a cloud service provider needs to make sure that two of the dependability requirements are satisfied: (1) its clients' outsourced data are stored securely and, (2) data queries and retrievals are executed correctly (in terms of reliability) and privately (in terms of three security attributes: Confidentiality, Integrity and Availability – CIA) (AlZain, Soh et al. 2013) (AlZain, Soh et al. 2011) (AlZain, Pardede et al. 2012) (AlZain, Soh et al. 2013) (AlZain, Li et al. 2015). Here, we term any data fault as data dependability fault that leads to security beaches and unmet reliability.

On the other hand, it also means businesses are willing to outsource their data to a third party (cloud service provider) only if they trust their data are not accessible and visible to the service provider and other non-authorized parties (Hore, Mehrotra et al. 2004). However, one of the main obstacles here for ensuring multi-cloud data dependability is Byzantine faults.

Byzantine fault tolerance (BFT) has received growing attention from the academic research community but not many systems use it in practice. While a great deal of recent research has focused on comparing the standard practical Byzantine fault tolerance protocol (PBFT) (Castro and Liskov 1999) and improving its performance with the development of Zyzzyva (Kotla, Alvisi et al. 2007) and Aardvark (Clement, Wong et al. 2009), very few studies on the BFT in a multi-cloud computing environment have addressed the detection of Byzantine failure to ensure data dependability within the cloud. In this chapter, we extend the original definition of Byzantine faults (Lamport, Shostak et al. 1982) to include the CIA dimensions (data Confidentiality, data Integrity and service Availability) (AlZain, Pardede et al. 2012), and cloud data intrusion by malicious insiders. Needless to say, data dependability is a major issue whenever users rely on third-party services because of the possibility of Byzantine failure in the cloud. Therefore, building a highly dependable multi-cloud system has become a critical research problem. To that end we enhance our previous investigation on how BFT and, secure cloud data storage and sharing techniques can be deployed to manage multi-cloud data dependability faults (AlZain, Li et al. 2016).

The remainder of this chapter is organized as follows. We first present the related work followed by overviews our conceptualization of multi-cloud data dependability faults as well as fault tolerant state machines. Then we detail three crucial operations in the proposed fault-tolerant architecture, and propose fault-tolerant method in managing multi-cloud data security faults. Subsequently we give a qualitative evaluation of the proposed architecture, and conclude this chapter with our research contribution.

RELATED WORK

As mentioned previously, multi-cloud data dependability faults subsume Byzantine faults that can be caused by malicious attacks or operator errors related to cloud data. Sending inconsistent results from clouds to the clients is considered a Byzantine fault as well (Castro and Liskov 1999).

Much research has been dedicated to Byzantine Fault Tolerance (BFT) since its first introduction (Lamport, Shostak et al. 1982), (Pease, Shostak et al. 1980). Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption (Kuznetsov and Rodrigues 2009) and remains peripheral in distributed systems (Vukolic 2010),(Lamport, Shostak et al. 1982). BFT for Web services as well as distributed systems have received more attention. Zhao (Zhao 2007) presented a framework of BFT for Web services which was based on the PBFT protocol (Castro and Liskov 1999) and ran the system with Byzantine faults in a distributed environment. In addition, Merideth et al. (Merideth,