Multi-Cloud Data Management using Shamir’s Secret Sharing and Quantum Byzantine Agreement Schemes

Mohammed A. AlZain, College of Computers and Information Technology, Taif University, Ta’if, Saudi Arabia

Alice S. Li, La Trobe Business School, La Trobe University, Bundoora, Australia

Ben Soh, Department of Computer Science and Information Technology, La Trobe University, Bundoora, Australia

Eric Pardede, Department of Computer Science and Information Technology, La Trobe University, Bundoora, Australia

ABSTRACT

Cloud computing is a phenomenal distributed computing paradigm that provides flexible, low-cost on-demand data management to businesses. However, this so-called outsourcing of computing resources causes business data security and privacy concerns. Although various methods have been proposed to deal with these concerns, none of these relates to multi-clouds. This paper presents a practical data management model in a public and private multi-cloud environment. The proposed model BFT-MCDB incorporates Shamir’s Secret Sharing approach and Quantum Byzantine Agreement protocol to improve trustworthiness and security of business data storage, without compromising performance. The performance evaluation is carried out using a cloud computing simulator called CloudSim. The experimental results show significantly better performance in terms of data storage and data retrieval compared to other common cloud cryptographic based models. The performance evaluation based on CloudSim experiments demonstrates the feasibility of the proposed multi-cloud data management model.

Keywords: Multi-Cloud Data Management, Quantum Byzantine Agreement, Shamir’s Secret Sharing

1. INTRODUCTION

Cloud computing has increased rapidly in many organizations. In recent years, there has been a move towards the concept of “multi-clouds” (Bertino et al., 2009; BNA, 2009). This is because a “single cloud” such as Amazon Cloud (2010) has its potential single-point-of-failure problems
when there are no standbys (Al Zain et al., 2012). In this paper, our focus is on a multi-cloud environment consisting of private and/or public clouds. It is noteworthy that multi-clouds are different from federated (hybrid) clouds, in that in a multi-cloud environment a cohort of clouds with the same domain are centrally controlled by a manager in the domain.

As data and information are shared with a third party, cloud computing users want to avoid an untrusted cloud provider, even more so in a multi-cloud environment. Security risks are clearly considered to be a crucial matter in a cloud computing environment due to the valuable information stored for users in the cloud (Liu et al., 2014, Wang et al., 2015, Wei et al., 2014). Cloud providers thus need to address privacy and security issues as a matter of high and urgent priority if they wish to attract more businesses.

This paper begins with a general discussion of issues related to the data security management of cloud computing. We then present a proposed multi-cloud data management model called Byzantine Fault Tolerance Multi-Clouds Database (BFT-MCDB). Our proposed BFT-MCDB model incorporates the Quantum Byzantine Agreement protocol (Lamport et al., 1982) and Shamir’s Secret Sharing approach (Johnson, 1988) to secure business data storage in a multi-cloud environment. We compare our proposed multi-cloud data management model with other common cloud cryptographic models using the CloudSim simulator (Garg and Buyya, 2011).

The remainder of this paper is organized as follows. Section 2 presents a brief background of the cloud computing techniques, while Section 3 presents our proposed multi-cloud data management model. Section 4 discusses the evaluation, analysis and implementation methods of our proposed approach. Section 5 concludes the paper with suggestions for future work.

2. BACKGROUND

Our proposed multi-cloud data management model uses Shamir’s Secret Sharing approach and a Quantum Byzantine Agreement protocol. We briefly describe below the background of these two crucial schemes to ensure data Confidentiality, Integrity and Availability (CIA).

2.1. Shamir’s Secret Sharing Approach

Agrawal et al. (2009) introduces Shamir’s secret sharing algorithm (1979) as a solution to the privacy issue. The algorithm proposes dividing the data $D$ into $(n)$ pieces $(D_1, ..., D_n)$ in such a way that knowledge of any $k$ or more of $D_i$ pieces makes the value of $D$ known. Therefore, a complete knowledge of $(k - 1)$ pieces reveals no information about $D$. $k$ should be less than $n$ to keep the value of shares un-constructible and ensure that the adversary cannot access $k$ data pieces. Shamir’s method theoretically secures information.

In addition, by using a $(k,n)$ threshold scheme with $n = 2k - 1$, In Agrawal et al. (2009), it is shown that a strong key management scheme can be achieved. The goal is to take a distributed approach to secure DaaS (Data as a Service), having the best of both worlds in the use of a secret-sharing approach and also multiple service platforms. With this approach, we can address both privacy-preserving querying and the data security of outsourced data.

2.2. Quantum Byzantine Agreement Protocol

The Quantum Byzantine Agreement protocol is an essential part of ensuring reliable distributed computing that the cloud computing falls into. Under this protocol, an agreement is reached if two conditions are satisfied. IC1: All non-faulty processors agree on the same value. IC2: If the
Productivity and Innovation in Services: The Multidisciplinary Perspective
Offered by Service Science
Aleksandar Ivanovic and Leonora Fuxman (2012). *Service Science Research, Strategy and Innovation: Dynamic Knowledge Management Methods* (pp. 170-183). www.igi-global.com/chapter/productivity-innovation-services/61875?camid=4v1a

Trust and Reputation in Digital Environments: A Judicial Inkling on E-Governance and M-Governance