Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 337 (2018) 105–117

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Investigating the Cost of Transfer Delay on the Performance of Security in Cloud Computing

Said Naser Said Kamil[1] Nigel Thomas[2]

School of Computing Science
Newcastle University
Newcastle Upon Tyne, UK

Abstract

This study presents a performance evaluation of the deployment of partitioned workflows over hybrid clouds taking into account the cost of transfer data delay. This paper extends previous work on the cost of security in cloud computing based on the multi-level security model. This research aims to provide performance predictions of different deployment options in public and private clouds in terms of the computation and communication costs. The Markovian process algebra PEPA is used to evaluate the models behaviour under different scenarios.

Keywords: Communications Cost, Performance Moddelling, Performance Evaluation, PEPA, Cloud Computing.

1 Introduction

With the growth in data generation and use many organisations tend to outsource their data storage and analysis through the use of cloud computing to decrease the load on their local resources and to reduce the costs of the management and the maintenance. This is because, cloud computing provides numerous advantages such as, scalability, less effort of data management, on demand access, pay as you go [1,3,12]. Nonetheless, confidentiality, integrity and privacy of data are still the main security concerns for both data owners, i.e. individuals and enterprises, and also cloud service providers [4,5,6,16]. As reported in [11], the lack of physical control on data results in a considerable problem regarding the security and the integrity of the data. Consequently, several organisations tend to use federated clouds (mixing

[1] Email: said.kamil@ncl.ac.uk

[2] Email: nigel.thomas@ncl.ac.uk

https://doi.org/10.1016/j.entcs.2018.03.036

public and private) based on the privacy of the deployed data, where the workflows are partitioned and deployed over the clouds.

A number of studies have considered the partitioning of workflows and the deployment over clouds while meeting the security requirements, for instance, [7,13], in order to mitigate the cloud security issues. In [13] a multi-level security model for partitioning workflows and the deployment over federated clouds is introduced. In our previous work [8], a cost model has been created by means of PEPA based on the multi-level security model of [13]. Although, the developed model has explored the costs associated with different security choices, however, we have not considered the communications cost. Therefore, this paper aims to extend our previous models [8] to include the data transfer cost in order to investigate the performance of two different deployment options on public and private clouds with different transfer costs.

This paper is structured as follows. In section 2, some background and related work have been reviewed. Then, we describe briefly the multi-level security model in Section 3. After that, the communications cost PEPA model is presented in Section 4. This is followed by the illustration and discussion of the experimental results in Section 5. The paper is concluded in Section 6 and outline some further works.

2 Background and Related Work

Despite the important features that are associated with the use of federated clouds, for example significantly decreasing the cost of computational support, security breaches can arise through the flow of data between private and public clouds. A methodology for making the access control matrices dynamic is presented by [9], where workflows are modelled using Petri Net and security policies for read and write access have been taken into consideration. Furthermore, in [10] the Bell-LaPadula security conditions, i.e. no read up and no write down, are used to assign different security levels for a formal model specified by means of Petri Nets. Our approach has some similarity to these approaches [9,10] in using a multi-level security model and formal modelling and analysing workflows. However, these approaches are more concentrated on the security aspects such as control access rather than investigating the performance cost of security in cloud computing.

Watson in [13] has presented a multi-level security model for partitioning workflows over hybrid clouds. The model adopts the security conditions of the Bell-LaPadula [2] and extends them to include the cloud computing. The model of [13] generates a collection of valid deployment options based on the sensitivity of data. Furthermore, a tool has been developed by Wen and Watson[15] for dynamic exception handling, which extends the multi-level security model of [13]. The authors indicate that the tool can discover alternative partitions with low-cost paths to deal with exceptions that may occur during run time. Later, Watson and Little [14] have extended the work further to assign security levels to services, data, platforms and networks. Additionally, this study [14] has introduced a methodology for modelling