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
1571-0661/

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

the security requirements of distributed systems.

Zeng *et al* [17] have presented an approach for a formal verification of a secure dynamic information flow within the federated cloud system. A model is developed in a way that allows capturing security roles, i.e. BellLaPadula model and cloud security; then Petri nets are used to analyse the correctness of this type of system. Our approach adopts Watson's multi-level security model [13] and has some similarity to the research of [17], in the sense that both studies used the BellLaPadula security model. Nevertheless, our approach is concerned with the performance analysis of a secure model, unlike the [17] which is more about security and correctness analysis using Petri nets.

3 Multi-Level Security Model

As discussed above, an approach for partitioning workflows over clouds has been introduced by Watson [13] based on a multi-level security model which extends the Bell-LaPadula security model. Applications are structured as workflows partitioned based on the sensitivity (i.e. privacy requirement) of data. A security level is assigned to each service and data that are consumed and produced by services. Also, the cloud that will accommodate the data and services is assigned a security level. Thus the security level is used to ensure the security of transferring data and services between the clouds (the source and the destination). For example, where patient data will be processed through four services, read, anonymise, analyse and write, the analyse action may require a lower level of access than read as it acts only on anonymous data.

A tool has been developed by [13] to automatically generate the valid deployment options, which comply with the aforementioned security conditions. The tool will rank the deployment options based on the calculation of the cost, taking into consideration: data storage, CPU and data transfer. However, this cost calculation takes no account of load or availability of resources which would normally be a major consideration for any performance analysis. Figure 1 illustrates the valid deployment options 1 to 4, where the colours red and green are used to indicate the private and the public clouds respectively. For more details about the multi-level security model, we refer the interested reader to [13].

4 The Model

In this section we will investigate the behaviour of two valid deployment options models (*options 1* and *option 4*), as they belong to different deployment classes (public and private). In our previous work [8] we did not model any data transfer costs. Clearly, this can be achieved by adding some network delays between actions being undertaken in different locations. We have made an assumption of using the data transfer delay as an independent action, and there is no pooling for servers, i.e. we do not consider contention for network access and therefore the transfer duration does not depend on how many data transfer actions happen at the same time. This

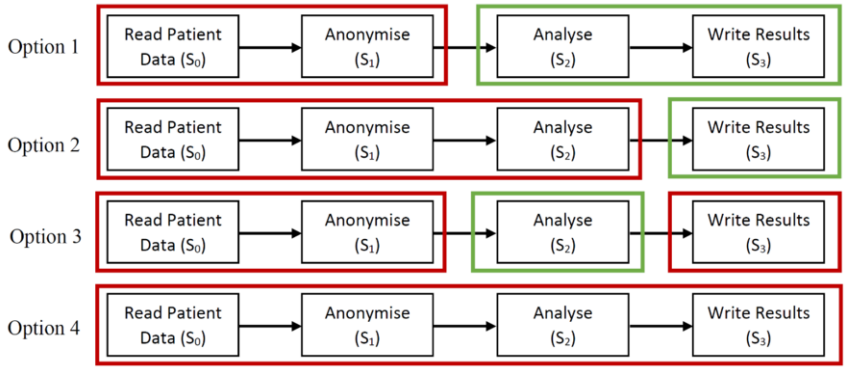

Fig. 1. Valid deployment options, where boxes red and green referring to private and public clouds respectively [13]

assumprion is likely to be reasonable for internal transfers, i.e. within the public or private cloud, but may not be valid for large data transfers between domains with limited router or firewall capacity, or where additional authentication is required in order to perform the data transfer.

The following is the PEPA model of *option 1* (public cloud) where *transferData* action is added to the model:

$$
\begin{aligned}
Service_0 &\stackrel{def}{=} (readData, r).Service_1 \\
Service_1 &\stackrel{def}{=} (anonymise, s).Service_2 \\
Service_2 &\stackrel{def}{=} (transferData, d).Service_3 \\
Service_3 &\stackrel{def}{=} (analyse, t).Service_4 \\
Service_4 &\stackrel{def}{=} (writeResult, w).Service_0 \\
Private &\stackrel{def}{=} (readData, r).Private + (anonymise, s).Private \\
Public &\stackrel{def}{=} (analyse, t).Public + (writeResult, w).Public \\
System &\stackrel{def}{=} Service_0[N] \underset{L}{\bowtie} Private \parallel Public[M1]
\end{aligned}
$$

The *option 4* PEPA model (private cloud) is same as the above model except for the following changes:

$$
\begin{aligned}
Private &\stackrel{def}{=} (readData, r).Private + (anonymise, s).Private \\
&\quad + (analyse, t).Private + (writeResult, w).Private \\
System &\stackrel{def}{=} Service_0[N] \underset{L}{\bowtie} Private[M2]
\end{aligned}
$$

Where for both options $N = 15$ *to* 2000, $M1 = 5$ *to* 25 and $M2 = 5$ *to* 25. Also the cooperation set $L = \{readData,\ anonymise,\ analyse,\ writeResult\}$. Also, we have used four assumptions for the data transfer delay ($d = 0.001, 0.01, 0.1, 1$), with

the intention to investigate the impact that have on the model overall throughput. Table 1 displays the rates used with the model of *option 1* communications cost.

	Rates				
Assumption	r	s	d	t	w
1	1	0.1	0.001	0.001	1
2	1	0.1	0.01	0.001	1
3	1	0.1	0.1	0.001	1
4	1	0.1	1	0.001	1

Table 1
The rates of the the *option 1* communication cost model

Furthermore, the rates of the *option 4* communication cost model are shown in Table 1, except for the rate d which is set to *1*, hence we assume it is 1000 times faster than the same slow rate that used in the *option 1*.

5 Experiments and Results

In this section the experimental results of the *option 1* and *option 4* communication cost models will be discussed. Two analyses have been used to evaluate the performance of these systems. Continuous time Markov chain (CTMC) analysis gives an exact solution of the models, but suffers from the state space explosion problem when the number of servers or workflows are very large. Thus we also employ a fluid approximation based on ordinary differential equations (ODEs) to provide scalable analysis.

5.1 CTMC analysis

Figure 2 displays the throughput of *option 1* and *option 4* models taking into account the data transfer cost. In the case of the *option 1* model the various rates that are assigned to the action *transferData*, have a noticeable impact on the performance of the model. Under assumption 1, the throughput of the model is low and the system is saturated rapidly at 10 instances of public clouds. However, under assumptions 2, 3 and 4, the throughput is much higher, specifically under assumption 3 and 4 where the throughput is increased significantly. But the assumptions 2, 3 and 4 are saturated at exactly the same point where the system has 15 public cloud instances, due to the liminted number of available servers.

We have assumed that the data transfer delay of the private cloud (*option 4*) will be lower than the public cloud (*option 1*) as it is only involves local communication. Therefore, the rate of *transferData* is assigned a relatively higher value, which consequently has a greater impact on the throughput of the *option 4* model as shown in Figure 2. Whereas the throughput of the *option 4* model is slightly higher than the *option 1* (assumption 3) and identical with the assumption 4. This

is because the behaviour of *option 4* model is limited by the overhead of the *analyse* action, as it has a comparatively slow rate. Obviously, the consideration of the data transfer cost is shown that *option 4* will be a valuable choice as same as the *option 1* public. However, the cost of designing and creating data center for example, and the computational cost will be significantly higher than the *option 1*. Hence, even with the use of a small rate for the *transferData* action in *option 1*, it is still offering a good performance and it is more cost effective when the number of workflow instances and servers are relatively small.

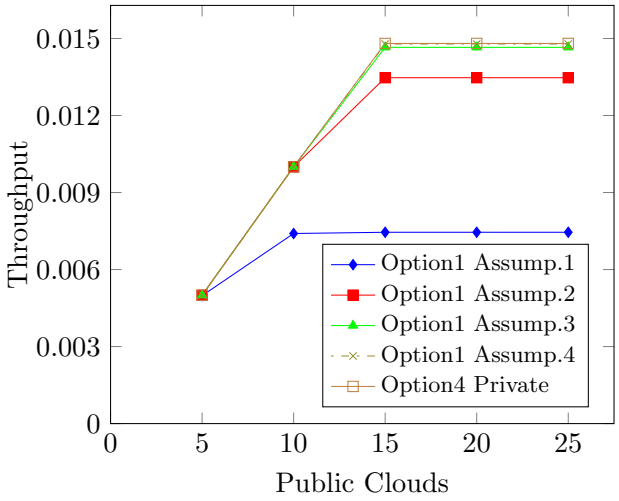

Fig. 2. The communications cost throughput of both *option 1* and *option 4*, using rates of *assumptions 1-4* of Table 1 for *option 1* and the rates $r = 1, s = 0.1, d = 1, t = 0.001$ and $w = 1$ for *option 4*

In the Figure 3, the population of the model of the communication cost of *option 1* is shown. Whereas we have only depicted the population of two most important services ($Service_2$ and $Service_3$), which respectively representing the *dataTransfer* and *analyse* actions. That is because the behaviour of the model is investigated through varying the rate of these two actions (see Table 1). Obviously, by varying the rate of *transferData* action the model behaviour has changed importantly, where the population of $Service_2$ is noticeably decreased and the saturation point has changed to 15 public cloud instances, i.e. assumptions 2 and 3. On the other hand, it is clear that the *analyse* action is still limiting the model performance where the increase of the rate of $Service_2$ is correspondingly increasing the population of $Service_3$, hence raise the queuing time of the *analyse* actions that waiting to be processed.

As we have assumed that the rates of *option 4* are comparatively fast except the rate of $Service_3$, the population of *option 4* model in Figure 4 exhibiting that the model performance is limited by the rate of *analyse* action, regardless the increase of the number of private clouds instances, which is showing consistency with the population of the same service of the *option 1* (public) that shown in Figure 3. So, the population of $Service_3$ is shown as a flat line (saturated). In spite of the fact that we have varied the rate of transfer data in *option 1* and it has been fixed to

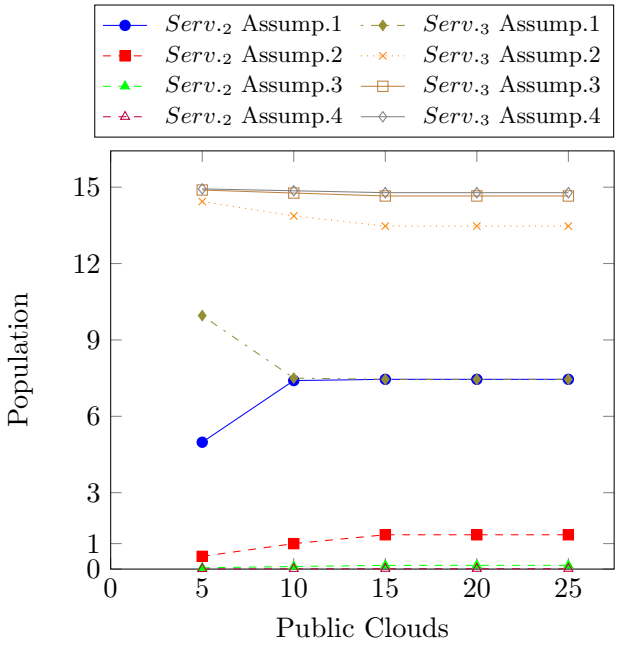

Fig. 3. Population of the communications cost *option 1* model ($Service_2$ and $Service_3$) by using rates of *assumptions 1–4* of Table 1

1 in the *option 4*, the performance of both options, however is exceedingly similar. Consequently, in terms of the cost *option 1* is still presenting better performance. Additionally, for more clarification for the behaviour of $Service_2$, Figure 4 is used with two different scales to show the variation of the $Service_2$, which is unclear without using a small scale for the population of the $Service_2$. Indeed, it is obvious that the number of workflow instances that used in this section is small, where the CTMC allows us to only analyse 15 workflows instances in parallel, therefore, the ODEs analysis will be used to evaluate large systems.

5.2 ODEs analysis

In the following set of experiments the communication cost of the *option 1* and the *option 4* PEPA models have been analysed using the ODEs analysis. Where, the number of workflows has been varied from 20 (Figures 5 – 8) to 2000 (Figures 9 – 12) for both options and the number of public and private clouds have been varied from 5 to 10. The main purpose of using the ODEs is to analyse the system behaviour with a large number of workflows instances, which cannot be processed by CTMC. Figure 5 and Figure 7, are respectively, demonstrating the performance of *option 1* model with 5 and then 10 public cloud instances. It is obvious that the population of $Service_3$ is decreased by only doubling the number of public clouds from 5 to 10, and also, the model in Figure 7 reaches its steady state faster than the Figure 5.

Figure 6 and Figure 8, depict the transient behaviour of *option 4*, which shows that the fast rate of the *transferData* action on private clouds has made the perfor-

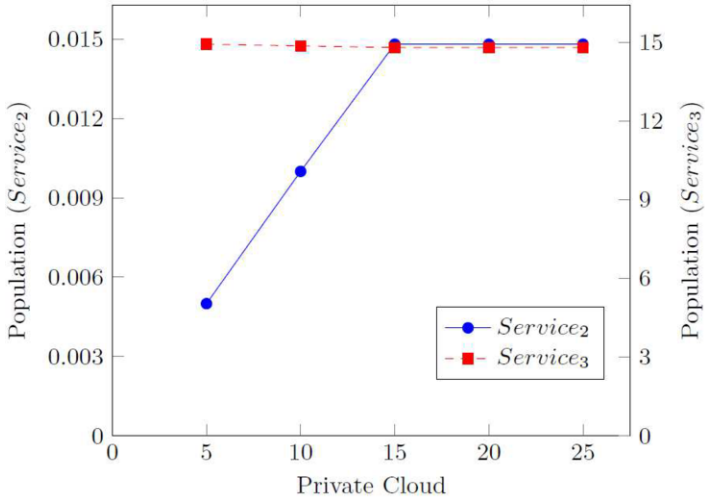

Fig. 4. Population of the communications cost *option 4* model $Service_2$ and $Service_3$

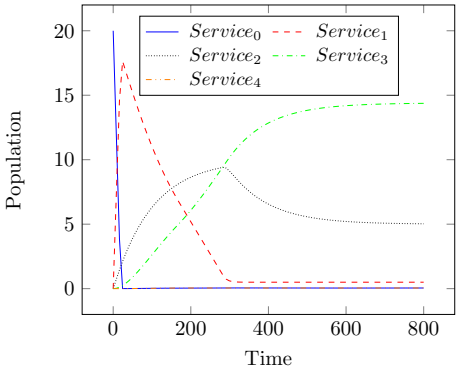

Fig. 5. ODEs of Communication Cost Option 1 model, using assump. 2 of Table 1, $t = 0.01$, $M1 = 5$ and $N = 20$

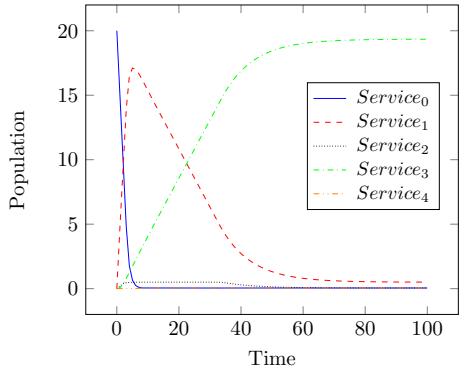

Fig. 6. ODEs of Communication Cost Option 4 model, r=w=1, s=0.1, $d = 1$, $t = 0.01$, $M2 = 5$ and $N = 20$

mance noticeably better than the *option 1* with a slow rate of the *transferData*, i.e. $d = 0.01$. The model reaches its steady state in a much shorter time in comparison with the *option 1*. Doubling the private clouds instances to be 10 (Figure 8) makes the model much faster to perform 20 workflows simultaneously. Nevertheless, it is obvious that the performance of the *option 4* model is limited by the $Service_3$.

Figures 9 – 12 show the performance of *option 1* and *option 4* models for 2000 workflows under ODE analysis. The comparison between these two options (*1* and *4*) shows that *option 1* takes more time to reach the steady state, because it is significantly affected by the slow rate of the *transferData* action, where the most population concentrates at $Service_3$ (*analyse*) action, as seen in Figure 9. Moreover, it is worth noting that doubling the number of public clouds to be 10 in Figure 11 initially shifts the bottleneck of the system to the $Service_2$ (*anonymise*) action and the steady state is reached very rapidly; which is not the case for the option 4 (Figure 12). In the *option 1* making the rate of *anaymise* faster, e.g. $s = 1$, the

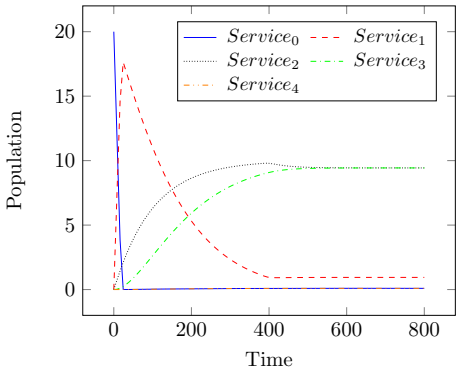

Fig. 7. ODEs of Communication Cost Option 1 model, using assump. 2 from Table 1, $t = 0.01, M1 = 10$ and $N = 20$

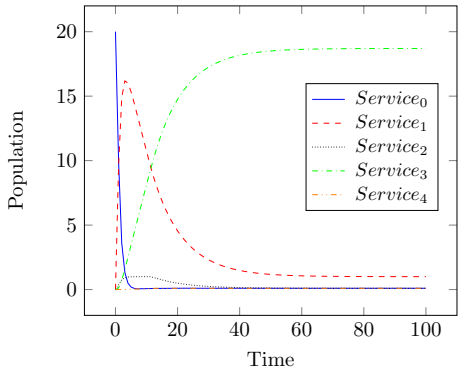

Fig. 8. ODEs of Communication Cost Option 4 model, *r=w=1, s=0.1, d = 1, t = 0.01, M2 = 10* and *N = 20*

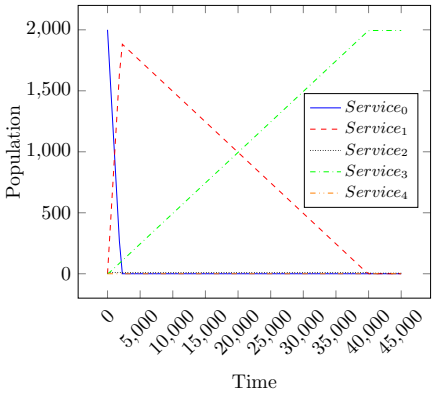

Fig. 9. ODEs of Communication Cost Option 1 model, using assump. 2 from Table 1, $t = 0.01, M1 = 5$ and $N = 2000$

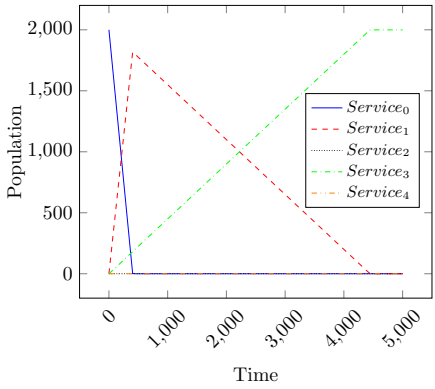

Fig. 10. ODEs of Communication Cost Option 4 model, *r=w=1, s=0.1, d = 1, t = 0.01, M2 = 5* and *N = 2000*

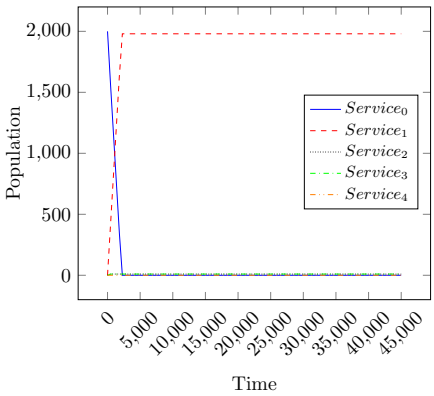

Fig. 11. ODEs of Communication Cost Option 1 model, using assump. 2 from Table 1, $t = 0.01, M1 = 10$ and $N = 2000$

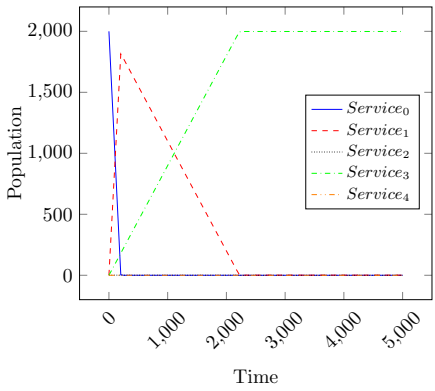

Fig. 12. ODEs of Communication Cost Option 4 model, *r=w=1, s=0.1, d = 1, t = 0.01, M2 = 10* and *N = 2000*

bottleneck moves back to $Service_3$.

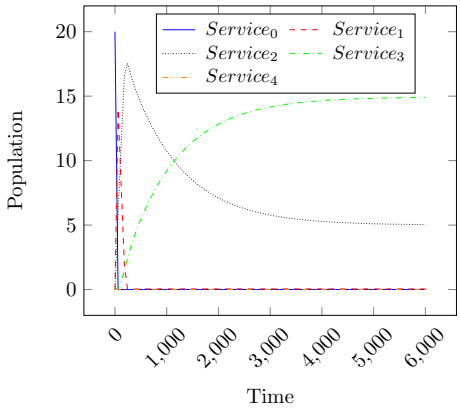

Fig. 13. ODEs of Communication Cost Option 1 model, using assump. 1 from Table 1, $M1 = 5$ and $N = 20$

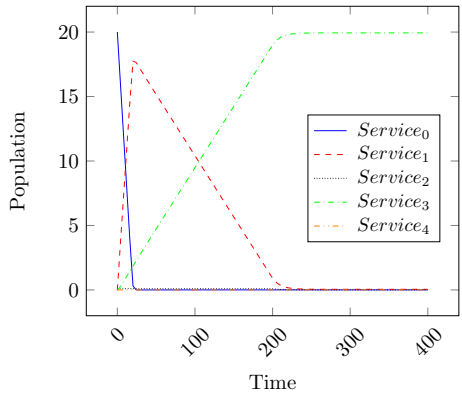

Fig. 14. ODEs of Communication Cost Option 1 model, using assump. 4 from Table 1, $M1 = 5$ and $N = 20$

5.3 Comparison of slow and fast rates of Option 1

In this section, the behaviour of *option 1* will be examined further by means of comparing the low rate and the high rate of the data transfer delay. Here we consider two extreme values of the range of communication costs. The aim is to find out how the communication cost will impact the performance of *option 1*. The comparison will include two sets of experiments using ODE analysis, where the system has 20 workflows and then 2000 workflows respectively.

Figure 13 and Figure 15 illustrate the transient behaviour of the Option 1 model using assumption 1 of Table 1, 5 and 10 public cloud instances and 20 workflows. The population of $Service_2$ in Figure 13 takes about 85% of the number of workflows then decreases steadily to reach 25% with the increase of the population of $Service_3$. However, by doubling the number of public clouds to be 10 as shown in Figure 15, $Service_3$ declined by 25% of the previous population, and also, $Service_2$ has raised and the steady state is reached quicker than the use of 5 public clouds. Increasing the rate of the *transferData* to be 1000 times faster as exhibited in Figure 14 and Figure 16, the system reaches steady state rapidly. Increasing the number of public clouds has no effect on the model behaviour, this is because of the relatively fast rate of the *transferData* action, meaning that the extra resources are not utilised.

Figures 17 – 20 illustrate the system evolution when the number of workflows is 2000. Although different parameters are used, the figures show near identical behaviour, with only a small difference in Figure 17 and Figure 19 where the data transfer rate is assigned a slower value. Nonetheless, this does not significantly affect the performance of the model. Increasing the number of public clouds instances has no effect on the performance because most of the population accumulates at the $Service_1$ and $Service_3$ (*anonymise* and *analyse*) actions respectively, since these services limit the performance of the model as they have comparatively slow rates.

To sum up, the comparisons of slow and fast rates of the *option 1* have shown that the use of the fast rate for the *transferData* action will result in similar performance provided by different deployment options (public and private). For example, Figure 10 of *option 4* in comparison against the Figure 18 of *option 1*. The popula-

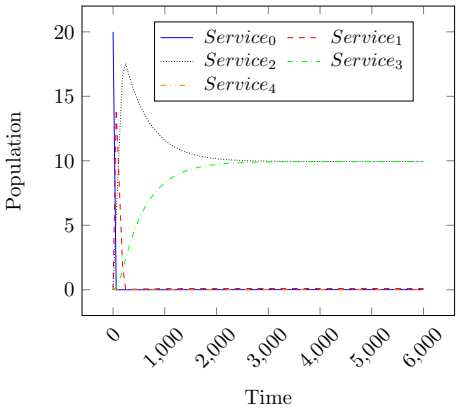

Fig. 15. ODEs of Communication Cost Option 1 model, using assump. 1 of Table 1, $M1 = 10$ and $N = 20$

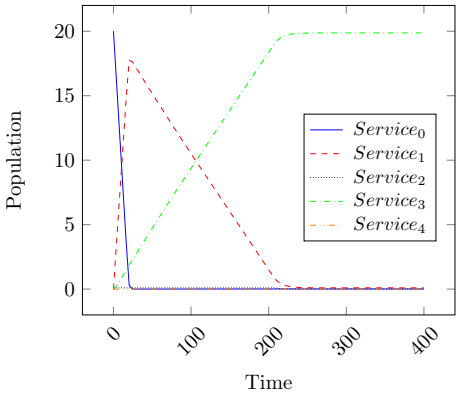

Fig. 16. ODEs of Communication Cost Option 1 model, using assump. 4 of Table 1, $M1 = 10$ and $N = 20$

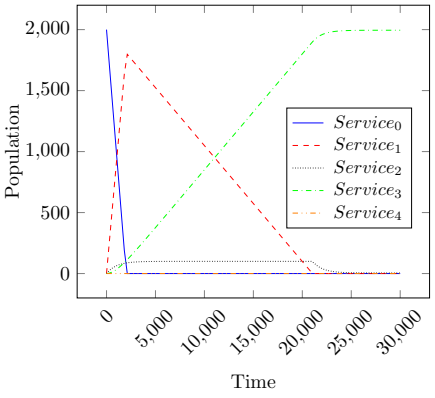

Fig. 17. ODEs of Communication Cost Option 1 model, using assump. 1 of Table 1, $M1 = 5$ and $N = 2000$

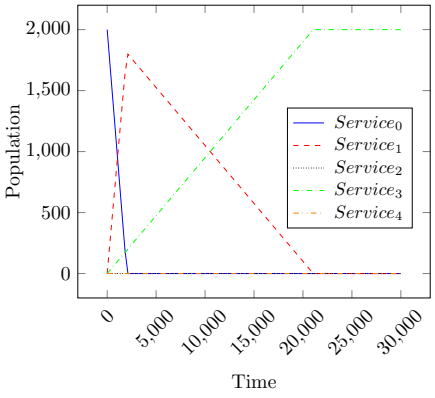

Fig. 18. ODEs of Communication Cost Option 1 model, using assump. 4 of Table 1, $M1 = 5$ and $N = 2000$

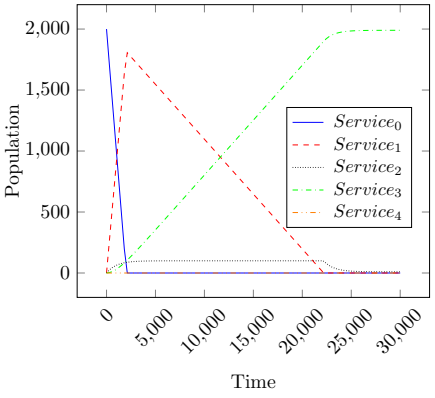

Fig. 19. ODEs of Communication Cost Option 1 model, using assump. 1 of Table 1, $M1 = 10$ and $N = 2000$

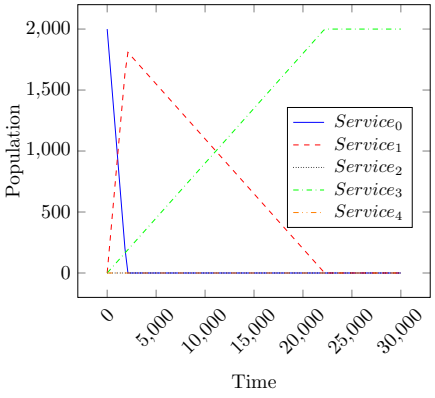

Fig. 20. ODEs of Communication Cost Option 1 model, using assump. 4 of Table 1, $M1 = 10$ and $N = 2000$

tion of both figures are extremely similar, although steady state is reached faster in the *option 4*. That is because in the case of *option 1* there are two services (*readData* and *anonymise*) that have been deployed on only one private server, which leads to more initial load.

6 Conclusion

In this paper, we have presented a methodology for investigating the cost of data transfer delay on the cloud computing using the Markovian Process Algebra PEPA. We have extended our previous work [8] with the intention to examine the communication costs of two different security deployment options on public and private clouds. We have considered the communications cost through adding some network delays between actions being undertaken in different public and private deployments. Although, the presented model is simple, it can still provide insight into the behaviour of the system.

The comparison between *option 1* (public) and *option 4* (private), has shown that at a small scale system the performance of *option 4* is identical to the *option 1*, specifically, by the use of relatively high rate for the *transferData* action in *option 1*; which means that the latter option is still cost effective. Nevertheless, for a larger scale system if we used a slow rate in the *option 1* the results have illustrated that *option 4* is offering better performance, due to the data transfer cost that overloaded the *option 1*. Increasing the rate of data transfer in *option 1* has noticeably risen the performance and presented behaviour which is similar to the *option 4*. The obtained outcomes have shown that the models are able to provide a prediction of the steady state for the given systems while considering different rates for the communication.

However, there are clearly some limitations, for example the presented work has not been validated against real implementation, which would clearly be beneficial. As stated, we have not considered data transfer delay cost to be subject to network contention, which may be the case when there are simultaneous large data transfers between domains. Modelling such behaviour would show a bigger impact on the data transfer when there is a mixed use of public and private clouds and may lead to alternative workflows being more attractive, for example using compression on large data sets.

References

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Commun. ACM*, 53(4):50–58, April 2010.

[2] D. E. Bell, L. J. La Padula, and Corporation Mitre. *Secure computer systems*. Mitre Corp. ; Distributed by National Technical Information Service, Bedford, Mass.; Springfield, Va., 1973.

[3] K. Chen, C. Hu, X. Zhang, K. Zheng, Y. Chen, and A. V. Vasilakos. Survey on routing in data centers: insights and future directions. *IEEE Network*, 25(4):6–10, July 2011.

[4] Yanpei Chen, Vern Paxson, and Randy H Katz. What's New About Cloud Computing Security. *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, 20, 2010.

[5] Tharam Dillon, Chen Wu, and Elizabeth Chang. Cloud Computing: Issues and Challenges. In *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pages 27–33, April 2010.

[6] Frank Gens. New IDC IT Cloud Services Survey: Top Benefits and Challenges, 2009.

[7] Elio Goettelmann, Walid Fdhila, and Claude Godart. Partitioning and Cloud Deployment of Composite Web Services under Security Constraints. In *2013 IEEE International Conference on Cloud Engineering (IC2E)*, pages 193–200, March 2013.

[8] Said Naser Said Kamil and Nigel Thomas. A Case Study in Inspecting the Cost of Security in Cloud Computing. *Electronic Notes in Theoretical Computer Science*, 318:179–196, November 2015.

[9] Konstantin Knorr. Dynamic Access Control through Petri Net Workflows. In *Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference*, pages 159–167, Dec 2000.

[10] Konstantin Knorr. Multilevel Security and Information Flow in Petri Net Workflows. In *Conference on Telecommunication Systems*, pages 613–615, 2001.

[11] Mehdi Sookhak, Abdullah Gani, Muhammad Khurram Khan, and Rajkumar Buyya. Dynamic remote data auditing for securing big data storage in cloud computing. *Information Sciences*, 380:101 – 116, 2017.

[12] L. Wang, F. Zhang, K. Zheng, A. V. Vasilakos, S. Ren, and Z. Liu. Energy-efficient flow scheduling and routing with hard deadlines in data center networks. In *2014 IEEE 34th International Conference on Distributed Computing Systems*, pages 248–257, June 2014.

[13] Paul Watson. A multi-level security model for partitioning workflows over federated clouds. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1):1–15, 2012.

[14] Paul Watson and Mark Little. Multi-level Security for Deploying Distributed Applications on Clouds, Devices and Things. In *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, pages 380–385, Dec 2014.

[15] Zhenyu Wen and Paul Watson. Dynamic Exception Handling for Partitioned Workflow on Federated Clouds. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, volume 1, pages 198–205, Dec 2013.

[16] Kan Yang and Xiaohua Jia. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems*, 24(9):1717–1726, Sept 2013.

[17] Wen Zeng, Maciej Koutny, Paul Watson, and Vasileios Germanos. Formal verification of secure information flow in cloud computing. *Journal of Information Security and Applications*, 2728:103 – 116, 2016.