Simulation of Cloud Data Security Processes and Performance

Krishan Chand, Muthu Ramachandran, Ah-Lian Kor

School of Computing, Creative Technologies, and Engineering,
Leeds Beckett University,
Leeds, UK
K.Chand7596@student.leedsbeckett.ac.uk, {M.Ramachandran, A.Kor}@leedsbeckett.ac.uk

Abstract. In the world of cloud computing, millions of people are using cloud computing for the purpose of business, education and socialization. Examples of cloud applications are: Google Drive for storage, Facebook for social networks, etc. Cloud users use the cloud computing infrastructure thinking that these services are easy and safe to use. However, there are security and performance issues to be addressed. This paper discusses how cloud users and cloud providers address performance and security issues. In this research, we have used business process modelling and simulation to explore the performance characteristics and security concerns in the service development life cycle. The results show that Business Process Modelling Notations (BPMN) simulation is effective for the study of cloud security process in detail before actual implementation. The total simulation duration time was 51 days and 9 hours 40 minutes but the results are displayed in 7 seconds only.

Keywords: Cloud Computing, Performance, Security, Bonnita Soft.

1 Introduction

Cloud computing has increased impact on business and and other sectors. Cloud computing encompasses services which are provided by a company or third party provider on the internet and these services are accessible from anywhere over the internet. Increased demand for cloud computing services provides so many benefits over the web connected devices. Such web services use the cloud server to store massive amount of data.

As per the definition given by CSA [1] cloud computing also provides a platform where applications, infrastructure, and information sources are separated. According to techtarget.com, cloud computing has given the opportunity to businesses to use the computer resources as a utility rather than investing too much money on building a computing infrastructure. Companies can use the cloud servers to store data or use the infrastructure in the cloud instead of building one locally. That will also help to reduce the cost of maintenance [2].

Due to the growing popularity of cloud computing and the massive data available in the cloud, security are the biggest issue and challenge faced by cloud users. Khanghahi

adfa, p. 1, 2011.

and Ravanmehr [3] have stated that for better performance, cloud computing resources should be efficiently managed. A structured security framework is necessary for securing data in the cloud. Cloud data security is very important, it should be secure, authenticated and encrypted. According to an article on computerweekly.com, many small organizations are willing to take advantages of cloud computing yet they are also wary of the performance, privacy of the data and the reliability of the services. In addition, FSB (Federation of Small Business) also states that the use of cloud computing for small business would be a challenge because they are not sure who will be responsible if something went wrong [4].

Security and performance concerns provide the ground for this research. A framework has been designed to provide better services with security to the cloud users. The paper is divided into five sections. Section 2 describes the literature, security and performance concerns. Section 3 explains how a simulation and questionnaire have been used as an approach. Section 4 shows the results of simulation and questionnaire. Finally, Section 5 presents the conclusion of the report.

2 Background

Cloud computing is the fastest growing sector of the information technology field. According to Munir et al [5], data security and reliability is also a major concern for the cloud users. These security issues can be divided into two different classes: first is the security concern for cloud providers and the second is the security for the cloud user. Moreover, Khanghahi and Ravanmehr [3] also state that higher performance of services and whatever is connected to the cloud has a direct impact on cloud users and providers. Therefore, performance evaluation is also an important consideration for cloud users and providers.

Harauz et al [6] highlight security related regulatory and legal anxieties. Cloud providers should propose the encryption of data scheme at the time of data storage on the cloud so that consumers can avoid unapproved access and can also be assured of data integrity, confidentiality and availability. Strict access control tools and scheduled data backups mechanism should be proposed. According to NIST [7], it is also stated that three-level security should be applied in cyber security so as to ensure data confidentiality, integrity and availability.

Security and privacy issues are the main barriers in the acceptance of cloud computing. On the grounds of the discussed issues relating to security, data should be secured at the time when data is processed in the cloud. Additionally, data privacy should also be respected in order to win customers' confidence. A customer's privacy manager tool should be proposed so as to mitigate security issues and also to provide additional privacy features [8].

2.1 Security Issues in Cloud

Sarwar, et. al [9] suggest security threat is biggest when data in cloud are stored by a third party vendor at some remote location. Consequently, consumers will either have limited or less control on the data which is hosted in the cloud. Additionally, trust between the service provider and the client is extremely important in the context of cloud security. In this paper, some security related aspects of a Cloud Computing system will be discussed.

Mahmood [10] has listed data-related issues in a cloud environment:

- **Data Location and Data Transmission:** The variation in policies, regulation, environment, and legislation between client's country and service provider's country might lead to a potential risk.
- **Data Availability:** The unavailability of data when required might lead to service outage.
- **Data Security:** When data travels between two different territories with high speed internet technology, the likelihood of security breach increases.

Behl and Mahmood (2011) [11] states that security-related issues in the Cloud has emphasized on various aspects of data usage, treatment, and disbursal. Those issues are:

- **Availability and Performance:** Service Level Agreement forms an essential part in cloud data security because it helps with real time data monitoring.
- **Service Disruptions:** If the connections come from known IP tools and Domain Name Server then problems concerning non-availability of resources at the service provider's end would not exist.

In order to overcome the above challenges, it is significantly important to draft and design a security model which provides data security in cloud environment (ibid).

2.2 Performance issues in cloud

Due to increasing demand of cloud computing, many factors can affect its performance. According to Khanghahi and Ravanmehr [3], some of the factors are as follows:

- **Recovery:** At the time of errors and failures, data can be lost without reasons, and thus the volume of recoverable data can impact performance.
- **Network bandwidth:** This could be a major factor for the performance, if the bandwidth of a network of service provider is low then by default the performance will be low.
- **Number of users:** Overload of users can also reduce performance, as service providers have a limit on the number of concurrent users.
- **Unavailability:** Unavailability of the services and restricted access can reduce performance.

3 Approaches

Modelling and quantitative method have been used in this research. The modelling method is related to the simulation which will provide some graphical results and through these graphical analysis, the performance of the services provided will be evaluated. The quantitative aspect of the research involves a survey using a questionnaire. According to De Leeuw [12] use of a range of approaches can provide particular advantages to the researcher because they are complementary.

3.1 Simulation

According to Naim [13] simulation involves a series of processes for building a computerised model so that particular results can be achieved through the observation of the model. Simulation process includes assumption making and parameterization. An experimenter is the user or modeller who conducts experiments using the model.

In this research, the Business Process Modeling Notation (BPMN) with Bonita soft is used. Running the BPMN model will help to provide inghts into the performance and cloud business security process.

The BPMN process includes the different cyclic phases shown in figure 1. The process always starts with a green round notation that is called the client or user. The user sends a message which contains a task to a particular process. According to the particular processes defined by the experimenter, the process ends with the finishing red end circle.(Creation of BPMN process with green and red round notations are shown in figure 2). After the creation of the whole process, the next task for the experimenter is to provide appropriate notation and assign variable to each process. Subsequently, the next task is to manage resources and load profiles. And then finally, run the simulation. The experimenter can run the simulation multiple times according to the requirement of the process. The experimenter can change the variables and resources accordingly in order to enhance the performance.

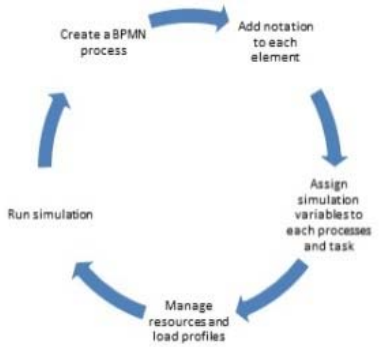

Fig. 1. BPMN Simulation Process Cycle

Simulation Framework

Many simulation tools are available in the field of computers but this research has used the BPMN with Bonita Soft for particular reasons. The main reason for using Bonnita Soft is that no waiting time is required to obtain the simulation results because it could generate the report within a minute. Simulation process has been used to optimize a cloud business security process to check the performance of the cloud. The researcher has used the BPMN simulation tool to check performance of the cloud servers before deploying the services for the benefit of cloud providers. Cloud users are not aware of these processes because these are part of the cloud internal framework which is used by every cloud provider. Through this BPMN model, cloud providers can check the performance of the cloud by experimenting with different parameters. This model can be used to check the performance of the cloud before deploying it. Before deploying the cloud, simulation process will provide the opportunity to diagnose faults, blockage in a system, resource management and how to manipulate the different variables in order to make optimize the process. The manipulation of resources and variables will enable cloud providers to uncover how performance can be improved to provide quality services with security. The following simulation design (figure 2) has been made to check the performance of the cloud services with security. This is the internal framework for cloud providers, which includes the different processes and task to provide better and optimized services with security. The different results of running the simulation will be discussed in the next section.

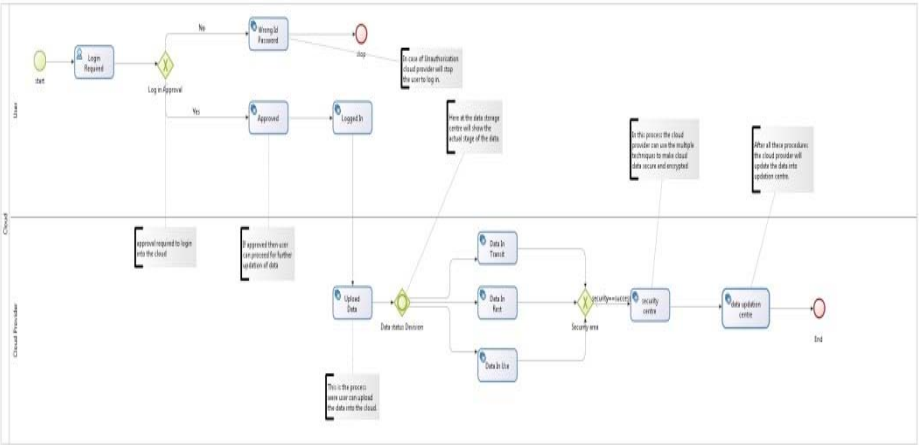

Fig. 2. Simulation Framework

The above figure 2 shows a design which includes all the different processes which cloud computing uses. Process starts with the log in authentication where Customers ID and passwords are required. If the id or password is wrong, it will not allow the user to proceed further. If id and password are valid then the user can go ahead with the data uploading process. In this state, a customer can upload the data through his account and the rest of the part is operated by the cloud providers. After the user has finished, the cloud provider checks the data status then the data will go through the security Centre,

where the data encryption techniques will be employed to encrypt the data in different codes. After encryption the data, the Centre stores the data in the cloud server.

3.2 Questionnaire

A questionnaire approach has been used to collect the quantitative data which will help to support the simulation data. Questionnaire is the most popular research method used in academic research [14]. Additionally, Bryan [15] has illustrated that questionnaire removes the distance factor between researcher and participant. Also the questionnaire is a tool used by the researcher to collect data in a limited time period [16].

The questionnaire includes questions relating to security concern of the cloud users and the performance availability. The questionnaire consists of four parts: (a) awareness about cloud computing in cloud users; (b) how the cloud user feels about data security; (c) data execution time while uploading the data on the cloud; (d) awareness of security settings of the cloud provider.

According to Cohen et al [14], there are so many ways to distribute the questionnaire to the respondents. For example: email, via online or can be delivered by hand. By distributing the questionnaire by hand will take less time but researcher needs to find the respondents in order to get the responses. Therefore, the method selected in the research is online, as the researcher has better access to a wider range of respondents.

4 Result and Analyses

4.1 Simulation Results

This section will describe the simulation results that the researcher obtained by running the simulation. To go to a starting point, the simulation has been set with the start date 11/04/2015 at 02:42:04 with the end date of 01/06/2015 till 12:22:04. Bonnita soft process gives results almost instantly without waiting till end date. The total simulation duration time was 51 days and 9 hours 40 minutes but, results came in 7 seconds only. The results are as follows:

Upload data instances execution time

Figure 3 shows the average, minimum and maximum execution time to upload data. The uploading time increases with the increase of user instances. In this scenario, a cloud user can put more resources to decrease the execution time, which results in the user getting better services.

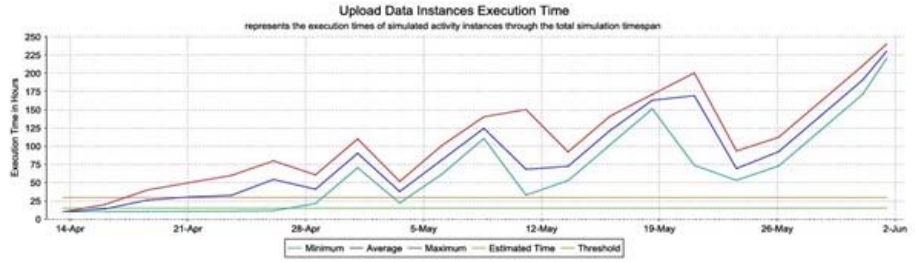

Fig. 3. Upload data execution time

Security Area

The simulation framework has been designed according to the current cloud providers situation.Therfore, this process has only one security pool , which is at the time of log in approval. But, from the data uploading to data encryption there is no security associated with the data. Any professional hacker can steal the data in the process of uploading the data, as the data is in use mode. There is no result for the security aspect and thus there is no variation in the security part, which can be seen in the figure 4. There should be alarm or trigger or any kind of alert, if somebody is trying to steal the data in between the process so that the cloud provider and user could be immediately alerted.

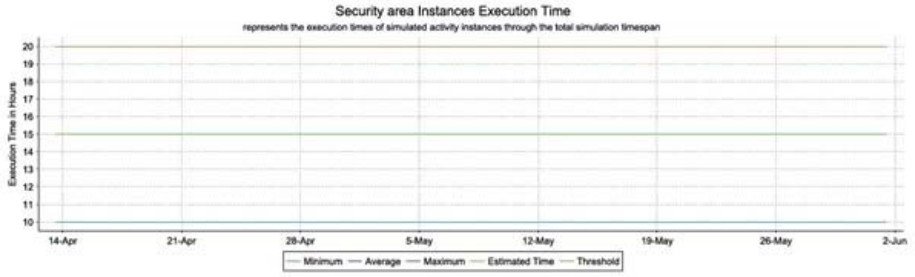

Fig. 4. Security area execution time

4.2 Questionnaire

This part of the paper explains the data collected through the questionnaire. This data is quantitative and provides insights into the respondents' views on cloud performance and security. The questionnaire was been sent to 50 participants and the researcher received responses from 39 respondents. Through these responses the researcher has concluded the following results:-

How safe is data on cloud?

The question was asked to obtain the views of cloud users with respect to cloud data security. The most popular cloud-based services is data storage in the cloud server. It can be seen in figure 5, that out of 39 responses , 48.7% of the participants felt that the data is not secure on the cloud. And 48.7% had no clue about data security. From the pie chart below, it can be concluded that almost 50% of the users were not aware of security concerns and the rest 50% had no idea about security.

Fig. 5. How safe is data on cloud server

Data uploading in the cloud

To check the performance of the services provided by the cloud users, a question asked was about data uploading. As figure 6 shows, a big proportion of users (i.e. 64%) had faced some kind of problem relating to data uploading. This could be ratified through proper resource management which could cope with users overload.

Fig. 6. Data uploading problem

5 Conclusion

The paper has proposed a design to check the performance and security before deploying the services to end users. Through the review of selected literature , it is found that the security and performance is affecting the cloud computing bussiness. The proposed design in Bonnita soft can help cloud users manage their business resources in order to give better services to the end users. It has also been found that, in the current

situation, no security aspect has been addressed at the time of data usage. Cloud providers can incorporate some alarm or trigger, when a data theft occurs. The Bonnita soft tool can be a useful guide for cloud providers.

References:-

1. CSA (2009 December) Security guidance for critical areas of focus in Cloud Computing v2.1, Cloud Security Alliance
2. Techtarget (2015) What is Platform as a Service (PaaS)? - Definition from WhatIs.com. [online] Available at: http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS [Accessed 29 May 2015].
3. Khanghahi, N. and Ravanmehr, R. (2013). Cloud Computing Performance Evaluation: Issues and Challenges. IJCCSA, 3(5), pp.29-41
4. ComputerWeekly.com (2015). Security fears stop small firms using cloud computing. [online] Available at: http://www.computerweekly.com/news/2240240940/Security-fears-stopping-small-firms-using-cloud-computing [Accessed 20 Apr. 2015].
5. Munir, k. and Palaniappan, S. (2013) Secure Cloud Architecture. Advanced Computing: An international Journal (ACfJ). 4 (I), pp. 9-22.
6. Harauz J., Kauifman L. and Potter B. (2009). Data Security in the World of Cloud Computing. IEEE Security & Privacy Magazine, 7(4), pp.61-64.
7. NIST, Guidelines on Security and Privacy in Public Cloud Computing, December 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
8. Siani and Miranda (2011). Security Threats in cloud computing. Abu Dhabi, United Arab Emirates: 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011.
9. Azeem Sarwar, Muhammad Naeem Ahmed Khan (2013) A Review of Trust Aspects in Cloud Computing Security.
10. Z. Mahmood, ―Data Location and Security Issues in Cloud Computing, IEEE International Conference on Emerging intelligent Data and Web Technologies, 2011
11. A. Behl (2011) Emerging Security Challenges in Cloud Computing, IEEE international Conference Information and Communication Technologies (WICT), 2011.
12. De Leeuw, E. (2005) To Mix or Not to Mix Data Collection Modes in Surveys. Journal of Official Statistics, 21(2), pp. 233-255.
13. Naim A. Kheir (1996) System modelling and computer simulation, second edition.
14. Cohen, L., Manion, L. and Morrison, K. (2007) Research Methods in Education. 6th ed. USA, Routledge.
15. Bryman, A. (1984) The Debate about Quantitative and Qualitative Research: A Question of Method or Epistemology?. The British Journal of Sociology, 35(1), pp.75-92
16. Best, J. and Kahn, J. (2006) Research in education. United States, Pearson Education Inc.