An Evolutionary Cultural Algorithm based Risk-aware Virtual Machine Scheduling Optimisation in Infrastructure as a Service (IaaS) Cloud

Ming Jiang[1], Tom Kirkham[2] and Craig Sheridan[3]
[1]*Faculty of Applied Sciences, University of Sunderland, Sunderland, U.K.*
[2]*Scientific Computing Department, Science and Technology Facilities Council, Oxfordshire, U.K.*
[3]*Flexiant Limited, Livingston, U.K.*

Keywords: Cultural Algorithm, Service Reliability, Risk Management, Virtual Machine Scheduling, Optimisation.

Abstract: Cloud service reliability is one of the key common performance concerns of both Cloud Service Provider (CSP) and Cloud Service User (CSU). As the capability and scale of a Cloud infrastructure increase, the requirements of maintaining and improving the reliability of services is increasingly crucial for the CSP and CSU. Risk management is the process of analysing the potential risk factors associated with the reliability deterioration of a service provided by a CSP, assessing the uncertainties and consequences associated with this kind of deterioration, and finally identifying the system wide appropriate mitigation strategies for risk treatments. In this paper, an evolutionary Cultural Algorithm based risk management method is proposed to facilitate the identification (i.e., probability and consequences) and treatment (i.e., mitigations) of Cloud infrastructure reliability related risk for Virtual Machine scheduling optimisation.

1 INTRODUCTION

Cloud computing is an unprecedented and rapidly evolving paradigm/business model of provision and consumption of ICT services and resources. Reliability and elasticity are two of the key performance factors that directly affect the Quality of Service (QoS) and revenues of a successful modern Cloud Data Centre (CDC). As the capability and scale of a CDC increase, with the drastic demands of large scale and long-run Cloud services deployed inside it, how to understand and effectively manage the risk factors, such as hardware failures, malfunctioned system software, security breaches and human factors, which may downgrade the reliability and elasticity performance of a CDC, becomes an increasingly crucial and challenging question.

Numerous recent years surveys and studies consistently indicated that the reliability of Cloud service is one of the top concerns of the adoption Cloud computing business model, especially by Small and Medium-sized Enterprises (SMEs), to outsource the traditional in-house IT infrastructures and applications to a public Cloud (Internet Society Hong Kong and Cloud Security Alliance, 2014; NetPilot Internet Security (NIS) Ltd, 2013; Microsoft, 2013; Sahandi, et al., 2012). From the perspective of revenues and reputation of a Cloud Service Provider (CSP), this concern is at the heart of maintaining and improving QoS challenge facing the CSP. This paper proposes a risk management method which focuses on for the QoS improvement for CSPs by modelling, assessing and mitigating the potential reliability deterioration risk. In particular, the risk management method enables a CSP to identify and minimize the risk level of scheduling Virtual Machine allocations to the physical host resources in the Infrastructure as a Service (IaaS) Cloud computing model.

In the most general and simple terms, risk is characterized by the likelihood of a threat and associated impact of the threat (Institute of Risk Management, 2002). At the heat of a risk management process is to assess the risk in terms of likelihood and impact and identify an appreciate risk mitigation strategies for risk treatments. The likelihood of a threat is inferred from both live and historical data associated with the occurrence pattern of the threat and its value could be a probability value between 0.0 and 1.0. In the context of

Jiang, M., Kirkham, T. and Sheridan, C.
An Evolutionary Cultural Algorithm based Risk-aware Virtual Machine Scheduling Optimisation in Infrastructure as a Service (IaaS) Cloud.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 1*, pages 267-272
ISBN: 978-989-758-182-3

different applications, the probability can be converted into relative likelihood levels, such as 1 to 7 to donate extreme low, very low, low, medium, high, very high, and extreme high, with different thresholds. The impact of a risk depends on the context of the application. Since Cloud services are based on the Virtual Machines hosted in the Cloud hardware resources, in our work of managing the reliability risk of Cloud services, physical host failure is considered as the threat to the QoS of a Cloud service and the impact is modelled as the number Virtual Machines to be allocated to the physical hosts and potentially to be affected in case of physical host failures. In order to fit impacts into risk calculations they are given a scale, such as 1 to 7 to indicate the level to which the impact could be. The final risk value is calculated as likelihood multiplied by the impact level and multiplication result is then converted into a score scale of 1-7 to indicate the overall risk level.

In order to support a large scale and flexible Virtual Machine scheduling optimisation, in this paper we propose an evolutionary Cultural Algorithm (CA) (Reynoids, 1994) based risk aware Virtual Machine allocation algorithm to minimize the risk of physical host failure. A CA framework consists of three major components: a population space, an external belief space, and a communication protocol that defines the interactions between the two spaces. Based on these components, a CA controls a dual interdependent inheritance process that harnesses the evolution of individuals both from the macro-evolutionary level as within the belief space and at the micro-evolutionary level as within the population space. Our case study indicates this dual interdependent inheritance process could effectively support the scheduling optimisation in large scale searching space and the traditional Genetic Algorithms.

In the Section 2, the historical data based modelling of physical host failure threat is introduced and this provides a basis for assessing the risk associated with the Virtual Machine allocations. In Section 3, a specific risk mitigation strategy is identified and designed as a risk impact minimisation problem, which is based on the searching and optimisation mechanisms of evolutionary Cultural Algorithm. Section 4 introduces and explains the main contributions of the work, which designs and implements an effective Cultural Algorithm to support a large scale and flexible Virtual Machine scheduling optimisation and demonstrate the performance of the optimisation algorithm with empirical comparisons with traditional Genetic Algorithm(GA). Section 5 briefly introduces the closely related works of general risk management frameworks for Cloud service provision and Virtual Machine scheduling specific approaches. Finally, the conclusion of current work in progress is presented in Section 6, in which future work is also introduced and discussed.

2 MODELLING PHYSICAL HOST FAILURE THREAT

In order to calculate the Probability of Failure (PoF) of a physical host, gathering data relating to past and current status of cloud resources is an essential activity. Monitoring resource failures is crucial in the design of reliable systems, e.g. the knowledge of failure characteristics can be used in resource management to improve resource availability. Furthermore, calculating the risk of failure of a resource depends on past failures as well.

There are various events that cause a resource to fail. Cloud resources may fail as a result of a failure of one or more of the resource components, such as CPU or memory; this is known as hardware failure. Another event which can result in a resource failure is the failure of the operating system or programs installed on the resource; this type is known as software failure. The third event is the failure of communication with the resource; this is referred to as network failure. Finally, another event is the disturbance to the building hosting the resource, such as a power cut or an air conditioning failure; this type is event is known as environment failure. Sometimes, it is difficult to pinpoint the exact cause of the failure, i.e. whether it is hardware, software, network, or environment failure; this is therefore referred to as unknown failure.

The Time To Fail (TTF) of a physical host is modelled as a life time random variable whose value is always more than zero. Given the physical host has been up until time t, the Probability of Failure (PoF) of it during future time interval x is a conditional probability $P\{X<=t+x|t\}$. In order to calculate the $P\{X<=t+x|t\}$, the general methodology is based on the following 5 steps:

Step 1: Collect observed historical data representing TTFs;

Step 2: Find a probability distribution model of TTF of the physical host by data distribution fitting;

Step 3: Estimate the particular parameters of the risk model by analysing the observations on the physical host;

Step 4: Evaluate the distribution model by comparing the risk model's predictions based on historical data and future observation data;

Step 5: Calculate P{X<=t+x|t} based on the model with these parameters.

As an example of a previous work (Jiang, 2013), the Weibull distribution mathematically characterizes the probability distribution of a lifetime variable with Probability Density Function (PDF):

$$f(t) = \frac{\alpha}{\lambda}(\frac{t}{\lambda})^{\alpha-1}e^{-(\frac{t}{\lambda})^{\alpha}} \quad (1)$$

And the Cumulative Density Function (CDF) of it is calculated, by an integration of PDF over time, as:

$$F(t) = 1 - e^{-(\frac{t}{\lambda})^{\alpha}} \quad (2)$$

The α and λ parameters of Weibull distribution can be statistically estimated by using the standard Maximum Likelihood Estimation (MLE) algorithm with historical observation data of TTFs. Hence, the *Probability of Failure (PoF)* of a physical host within future time *x*, given it has been on until time *t* can be calculated as:

$$\begin{aligned} PoF = P\{X \le t + x|t\} \\ = \frac{P\{t < X \le t + x\}}{P\{X > t\}} \\ = \frac{F(t + x) - F(t)}{1 - F(t)} \\ = 1 - e^{\frac{t^{\alpha}-(t+x)^{\alpha}}{\lambda^{\alpha}}} \end{aligned} \quad (3)$$

3 MITIGATION STRATEGY

Once the physical host failure is identified and assessed as the key threat to the QoS, appropriate risk mitigation solution and risk mitigation strategy of implementing the solution should be considered and decided respectively. In general, mitigation strategy can be risk avoidance, limitation, retention, transfer and acceptance (Institute of Risk Management, 2002). Within the context of our work, risk avoidance and limitation are the main strategies to be applied. The selection and execution of a mitigation solution will be based on the evaluation on its effect on minimising the potential risk of physical host failures on the running of Virtual Machines hosted on these physical hosts.

Since the nature of mitigation is to take precautionary actions before the occurrence of risk, time constraint and cost of a mitigation solution are key factors for deciding which mitigation strategies to choose and how to deploy them. When multiple risk factors need to be mitigated at the same time, it will be more complex to make an optimized decision under time and cost constraints (Djemame et al., 2011). One example is that a set of risk mitigation tasks with known, arbitrary execution times, need to be implemented by some identical high level risk mitigation solution executers by a given deadline. The problem is to schedule all of the mitigation tasks onto the least number of executers so that the deadline is met. This is a classic One-Dimensional Bin Packing problem in particular and combinatory optimization problem in general. In practice, the efficiency of scheduling and execution of a particular risk mitigation strategy within the risk management process as a whole is also part of the Cloud infrastructure performance concerns from the perspective of IaaS operational decision making process. Hence, our work aims at investigating optimization algorithms to help make decisions for scenarios as illustrated in these examples.

In this paper we propose an evolutionary Cultural Algorithm(CA) (Reynoids, 1994) based risk aware Virtual Machine allocation algorithm to minimize the risk of physical host failure for a given elasticity commitment. The reliability risk aware virtual machine allocation problem is specified with a set of formal notations as follows:

Pi: Available Physical Host i

Vi: Number of possible newly added Virtual Machines of Pi

LBi: Low bound value of Vi

UBi: Up bound value of Vi

Li: Level of failure likelihood of Pi

Ri: Reliability risk of allocation Vi Virtual Machines to Pi and Ri= Li×Vi

TR: Total Risk of all associated physical hosts and TR=SUM(Ri)

TNV: Total Number of Virtual Machines allocated to all available physical hosts and TNV= SUM(Vi)

The reliability risk aware virtual machine allocation problem is to find an optimized combination of eligible Vi, for a targeted TNV, which is able to achieve the minimum TR: i.e., Minimise(TR), subject to a targeted TNV and LBi ≤ Vi ≤ UBi.

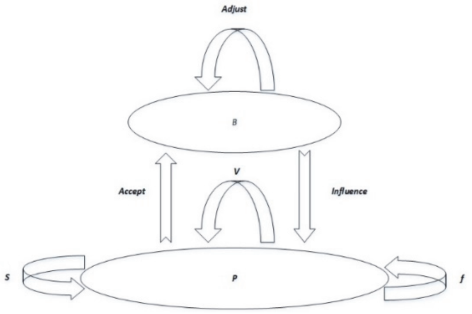
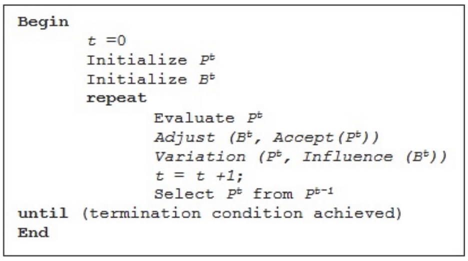


Figure 1: Cultural Algorithm Framework (Reynoids, 1994).

4 RISK-AWARE VIRTUAL MACHINE SCHEDULING

4.1 Cultural Algorithm Framework

Cultural Algorithm (CA) (Reynoids, 1994) framework consists of three major components: a population space, an external belief space, and a communication protocol that defines the interactions between the two spaces. Based on these components, a CA controls a dual interdependent inheritance process that harnesses the evolution of individuals both from the macro-evolutionary level as within the belief space and at the micro-evolutionary level as within the population space. With these major components and other associated operators, Cultural Algorithm framework can be defined by an 8-tuple: Cultural Algorithm = <P, S, Vc, f, B, Accept, Adjust, Influence>, where, P is a population; S is a selection operator; Vc is a variation operator; f is the performance function; B is the belief space; Accept is the acceptance function; Adjust is a belief space operator for changing the belief space knowledge, B; and Influence is a set of influence functions on the variation operator Vc, Accept and Influence together represents the communication protocol for a Cultural Algorithm. The belief space B stores five types' knowledge (Reynoids, 1994): Normative, Situational, Domain, Topographical and History.



```
Begin
        $t$ =0
        Initialize $P^t$
        Initialize $B^t$
        repeat
                Evaluate $P^t$
                Adjust ($B^t$, Accept($P^t$))
                Variation ($P^t$, Influence ($B^t$))
                $t$ = $t$ +1;
                Select $P^t$ from $P^{t-1}$
until (termination condition achieved)
End
```

Figure 2: Cultural Algorithms Pseudo-code (Reynoids, 1994).

Figure 1 illustrates the 8 components and their relationship in the Cultural Algorithm. Based on the 8 components, the pseudo-code of Cultural Algorithm is described in Figure2.

4.2 Virtual Machine Allocation Parameters Specification

In this section, we introduce a Virtual Machine scheduling example to demonstrate how to adopt Cultural Algorithm to optimise the risk level of allocating Virtual Machines onto physical host with potential failures.

Consider a pool of 128 physical hosts as Pi: P1, P2 ... P128.

The value of Vi, the number of possible newly added Virtual Machines of Pi, is bounded by a range of (LBi, UBi), which is (5, 9) and (0, 9) for two sets of experiments.

Li, the likelihood level of a failure, is defined by the corresponding element in a list which consists of 128 different values for different physical hosts: [34637275415112342115112373467752556141146 145561467752252214637274114271271264614234 377235335772712754712642343772353357725221 421].

The targeted number of Virtual Machine is 1000.

The reliability risk aware Virtual Machine allocation algorithm is to find the appropriate number of Virtual Machine for each physical host, so that the total number of Virtual Machine equals to the targeted number and the total risk is minimized.

4.3 Cultural Algorithm Functions Parameters Specification

The specified parameters for the Cultural Algorithm are the following:

Generate: A population of 200 random individuals is generated.

Evaluate: Total risk level of physical host failure is the fitness function for evaluation on an individual.

Select: A tournament method is used for selection and the size of tournament is 20. Elitism is applied to select the fittest individual into the next generation.

Accept: The fittest individual with the minimum risk level of physical host failure is accept to update the Belief Space.

Update: The belief space stores the fittest individual with the minimum risk level of physical host failure as the Situational Knowledge and the experimental range for individual gene mutation on genes as the Domain Knowledge.

Influence: Situational Knowledge is used to influence the selection of individuals for crossover and Domain Knowledge is used to influence the mutation on them with a rate of 0.002.

Mutation Operator: The Mutation Rate is set to 0.2 with a range of (-2, 2) for gene change value.

Crossover Operator: The Uniform Rate is set to 0.8.

Table 1: Comparisons of Two Sets of Experiments Results on GA and CA Algorithms (Targeted Virtual Machine is 1000, Average of 5 Runs).

Algo. Name	VM Bound	Num. of Evolution Gen.	Execution Time (Sec.)	Risk Level
GA	(5,9)	40000	301.426	3404
CA	(5,9)	39120	295.493	3404
GA	(0,9)	27995	210.498	3350
CA	(0,9)	18493	156.835	3350

4.4 Experiment Results and Analysis

In the following comparison study, Genetic Algorithm and Cultural Algorithm are compared with two sets of experiments.

In the first set of experiments, the range of a possible allocated Virtual Machine is set to between bounds (5, 9). In the second set of experiments, the range of possible allocated Virtual Machine is set to between bounds (0, 9). The searched optimal total risk for these two sets are different due to the different ranges of bounds and these bounds lead to different sizes of search spaces for testing the performance of the two algorithms.

As demonstrated in the Table 1, for both the sets of experiments, the convergence of Cultural Algorithm, in terms of number of generations and time, is faster than the Genetic Algorithm and it appears that with the increase of search space, the performance of Cultural Algorithm excels better than Genetic Algorithm does. This comparison empirically demonstrates the effectiveness of the dual interdependent inheritance process of a Cultural Algorithm.

5 RELATED WORK

In recent years, the methodologies and practices of risk assessment/management have been gradually applied into the robust provisioning of Cloud services at different levels for Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Djemame et al., 2011; Fitó et al., 2010).

As the scale of Cloud service increases at these different levels, there are challenging demands on the Quality of Service and associated risk management and mitigation considerations. The scalability of risk management process and the effectiveness of mitigation strategy together defines the overall of effect of risk-aware Cloud service provision. Regarding the Virtual Machine scheduling and Cloud infrastructure reliability related risks, work have been focused on (Guitart, 2013; Fu, 2009).

Although Cultural Algorithms have been widely applied into the many optimisation and searching problems in engineering and business management domains, some recent interesting work of introducing Cultural Algorithms into the computing resource management and task scheduling (Zhou, 2013) in the domain of Grid/Utility computing have appeared in literature. Our work aims to explore the feasibility of adopting Cultural Algorithms in a large scale searching and optimisation space problems as often raised in the resource and QoS management in Cloud Data Centre/IaaS Cloud.

6 CONCLUSION AND FUTURE WORK

In this paper, we identify and manage the risk caused by physical host failure threat to the QoS of Virtual Machines hosted in large scale Cloud infrastructure. An evolutionary Cultural Algorithm based risk management method is proposed and validated to facilitate the identification (i.e., probability and consequences) and treatment (i.e., mitigations) of Cloud infrastructure reliability related risk for Virtual Machine scheduling optimisation. The dual interdependent inheritance process of Cultural Algorithm is empirically validated to demonstrate its effective support of scheduling optimisation searching in large scale searching space.

In future, the physical host level risk management mechanism would be extended and integrated into relatively high level decision making or optimisation functional modules of an IaaS provision; the risk management will be also explored in the context of meta-management such as in case of Cloud resource brokerage at SaaS, PaaS and IaaS levels.

ACKNOWLEDGEMENTS

This work has been partially supported by the EU with 7th Framework Programme under contract EU-ICT-257115-Optimized Infrastructure Services (OPTIMIS) Project and EU-ICT-317715-Model-based Cloud Platform Upperware (PaaSage) Project.

REFERENCES

Djemame, K., Armstrong, D., Kiran, M., and Jiang, M. (2011). A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems. In *Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization*, Rome, Italy, September 2011.

Fitó, J. O., Macías, M., and Guitart, J. (2010) Toward business-driven risk management for cloud computing. In *Proceedings of International Conference on Network and Service Management (CNSM10)*, pages 238-241.

Fu, S. (2009) Failure-Aware Construction and Reconfiguration of Distributed Virtual Machines for High Availability Computing. in *Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid09)*, Shanghai, China, May 18-21, 2009, pages 372-379.

Guitart, J., Macías, M., Djemame, K., Kirkham, T., Jiang., M., and Armstrong, D. (2013). Risk-Driven Proactive Fault-Tolerant Operation of IaaS Providers. In *Proceedings of CloudCom2013*, pages 427-432.

Institute of Risk Management (2002). The Risk Management Standard. *The Association of Insurance and Risk Managers, National Forum for Risk Management in the Public Sector*, Volume 2008, 21st August, 2002.

Internet Society Hong Kong and Cloud Security Alliance (HK & Macau Chapter) (2014). *Report on Hong Kong SME Cloud Adoption and Security Readiness Survey*. 2 April 2014.

Jiang, M., Byrne, J., Molka, K., Armstrong, D., Djemame, K., and Kirkham, T. (2013). Cost and Risk Aware Support for Cloud SLAs. In *Proceedings of the Third International Conference on Cloud Computing and Services Science (CLOSER2013)*, Aachen, Germany, 8-10 May 2013.

Microsoft (2013). *Small and midsize businesses cloud trust study: U.S. study results*. June 2013.

NetPilot Internet Security (NIS) Ltd. (2013). A Study on UK SME adoption of Cloud. 3 October 2013.

Reynoids, R. (1994). An introduction to cultural algorithms. In *Proceedings of the 3rd Annual Conference on Evolutionary Programming*, Sebald, A.X., Fogel, L.J. (Editors), River Edge, NJ, World Scientific Publishing, 1994, pages 131-139.

Sahandi, R., Alkhalil, A., and Opara-Martins, J. (2012). SMEs' Perception of Cloud Computing: Potential and Security. In *IFIP International Federation for Information Processing 2012*, pages 186–195, 2012.

Zhou, W., Yan-ping, B. and Ye-qing, Z. (2013). The application of an improved cultural algorithm in grid computing, In *Proceedings of the Control and Decision Conference (CCDC)*, 25-27 May 2013, Guiyang, China, Pages 4565 – 4570.