

ESaaS 2014

EMERGING SOFTWARE AS A SERVICE
AND ANALYTICS

Victor Chang

Gary Wills

Robert Walters

Proceedings of ESaaS 2014

Emerging Software as a Service and Analytics

In conjunction with the International Conference on Cloud Computing
and Services Science - CLOSER 2014

Barcelona, Spain | April, 2014

Victor Chang
Gary Wills and
Robert Walters (Eds.)

Emerging Software as a Service and Analytics

**Proceedings of the
International Workshop on
Emerging Software as a Service and Analytics
ESaaSA 2014**

In conjunction with CLOSER 2014
Barcelona, Spain, April 2014

SCITEPRESS
Portugal

Volume Editors

Victor Chang

Leeds Metropolitan University and University of Southampton
U.K.

Gary Wills

University of Southampton
U.K.

and

Robert Walters

University of Southampton
U.K.

International Workshop on

Emerging Software as a Service and Analytics

Barcelona, Spain, April 2014

Copyright © 2014

SCITEPRESS

All rights reserved

Printed in Portugal

ISBN: 978-989-758-026-0

Depósito Legal: 372335/14

Foreword

The Emerging Software as a Service and Analytics– ESaaS 2014 was organized in conjunction with CLOSER 2014 in Barcelona, Spain. This workshop is primarily focused on high quality and innovative research papers from different fields related to the most recent developments in Emerging Software as a Service and Analytics.

Authors will have the opportunity to have their work selected for publication in a special issue of RonPub’s Open Journal of Cloud Computing (OJCC) and also a Cloud Computing book edited by the workshop chairs.

The workshop chairs will have set up their journal and extension of papers published in the workshop and main conference can also contribute to their journal, details of which will be available soon.

ESaaS has invited a number of scholars who have experience of publishing high-quality of papers. All the high-quality submissions were reviewed by at least two program committee members who were external to each group of authors. . Finally, 9 papers have been accepted and 1 short paper will also have the chance to be presented during the sessions due to the excellent quality of the research.

We would like to thank all the authors who took the time to submit papers to ESaaS, even though they were not finally accepted. We would also like to express our gratitude for the excellent work done by the Program Committee and the members of the Organisation Committee.

April 2014,

Victor Chang

Leeds Metropolitan University and University of Southampton, U.K.

Gary Wills

University of Southampton, U.K.

Robert Walters

University of Southampton, U.K.

Workshop Chairs

Victor Chang
Leeds Metropolitan University and University of Southampton
U.K.

Gary Wills
University of Southampton
U.K.

and

Robert Walters
University of Southampton
U.K.

Program Committee

Omar Abdul-Rahman, National Institute of Informatics, Japan
Reinhold Behringer, Leeds Metropolitan University, U.K.

Tony Bryant, Leeds Metropolitan University, U.K.

Victor Chang, Leeds Metropolitan University and University of
Southampton, U.K.

Darren Chong, Singapore, Singapore

Lee Gillam, University of Surrey, U.K.

Yi-ke Guo, Imperial College, U.K.

Takahiro Hirofuchi, National Institute of Advanced Industrial Science
and Technology, Japan

Neil Chue Hong, Software Sustainability Institute, University of
Edinburgh, U.K.

Guy-Bertrand Kamga, Alcatel-Lucent, France

Muthu Ramachandran, Leeds Metropolitan University, U.K.

Z. Cliffe Schreuders, Leeds Metropolitan University, U.K.

Jose Simao, Instituto Superior de Engenharia de Lisboa, Portugal

Robert Walters, University of Southampton, U.K.

Gary Wills, University of Southampton, U.K.

Tomasz Wiktor Wlodarczyk, University of Stavanger, Norway

Ken Wu, Gov, China

Renyu Yang, Beihang University, China

Fan Zhang, MIT, U.S.A.

Yicheng Zhang, Univ, Australia

Table of Contents

Foreword	iii
Workshop Chairs	v
Program Committee	v

Full Papers

Verifying Cloud Systems using a Bigraphical Maude-based Model Checker	3
<i>Zakaria Benzadri, Chafia Bouanaka and Faiza Belala</i>	
Modelling Financial SaaS as Service Components	13
<i>Muthu Ramachandran and Victor Chang</i>	
The Big Data Analysis for Measuring Popularity in the Mobile Cloud	21
<i>Victor Chang</i>	
Introduction to the Risk Visualization as a Service	30
<i>Victor Chang</i>	
Citizen Intention to Adopt e-Government Services in Saudi Arabia	38
<i>Sulaiman A. Alateyah, Victor Chang, Richard M. Crowder and Gary B. Wills</i>	
Performance Evaluation of Multi-Core Multi-Cluster Architecture (MCMCA)	46
<i>Norhazlina Hamid, Robert J. Walters and Gary B. Wills</i>	
A View at Desktop Clouds	55
<i>Abdulelah Alwabel, Robert Walters and Gary Wills</i>	
Cloud Security Proposed and Demonstrated by Cloud Computing Adoption Framework	62
<i>Muthu Ramachandran and Victor Chang</i>	

A Proposed Case for the Cloud Software Engineering in Security	71
<i>Victor Chang and Muthu Ramachandran</i>	

Short Paper

Review and Analysis of Cloud Computing Quality of Experience	83
<i>Fash Safdari and Victor Chang</i>	
Author Index	89

FULL PAPERS

Verifying Cloud Systems using a Bigraphical Maude-based Model Checker

Zakaria Benzadri, Chafia Bouanaka and Faiza Belala

LIRE Laboratory, Department of Software and Information Systems Technology,
University of Constantine II, Constantine, Algeria
benzadri@gmail.com, c.bouanaka@umc.edu.dz,
belalafaiza@hotmail.com

Abstract. Formal methods are system design techniques based on rigorous mathematical models to build software systems. Our aim in this paper is to define formal specifications of cloud systems and offer analysis support to formally model check their inherent properties. Hence, we define a formal semantic framework, based on Bigraphical Reactive Systems (BRS), for specifying cloud architectures and their shape shifting to ensure service availability and quick scalability. Then, we propose a Bigraphical Maude-based Model Checker to formally verify some properties.

1 Introduction

Complexity is in the core of today's Cloud systems, since large organizations have to manage increasingly heterogeneous cloud systems at different level: hundreds of services, thousands of servers, hundreds of thousands of transactions, more and more numerous and spread over the world users, whether customers or suppliers. The inexorable increase in the scope of cloud computing is accompanied by a concentration of risks and brought issues.

The evolutionary pressure imposed upon organizations, and the ever-increasing integration of dematerialization only accelerate this phenomenon and give a critical role to cloud systems. Adverse effects of such complexity are numerous, giving rise to many obstacles [1], such as service availability, performance unpredictability, quick scalability, bugs in large-scale distributed systems, etc., that handicap cloud computing adoption and growth. In this context, formal methods are an effective approach to ensure cloud systems reliability. Since, formal methods allow developing complex software under a firm mathematical foundation resulting in high quality, more correct software compared to conventional design methods. Nevertheless, some attempts have been proposed but do not deal with all fundamental concepts of cloud computing. Particularly, they focus on cloud computing technological concepts;

- Hanfei, et al. [2] and Grandison, et al. [3], gave some discussion and exploration on establishing relationships between virtualization and cloud computing. Throughout their work, they attempt to give out a formal definition of cloud computing from a virtualization viewpoint using its theoretical basic concepts.

- Shi-Xin, et al. [4], propose an access control model to achieve a fine-grained, data confidentiality and scalability via a formal definition of the HABAC model (Hierarchy Attribute-Based Access Control).
- Adamov and Hahanov [5], define a security model for individual cyberspace (ICS) protection as a means to ensure a secured user’s virtual environment, they establish an analysis of security issues related to ICS and propose a conceptual model for modern security environments.
- Freitas and Paul [6], present an abstract formalisation of federated cloud workflows using the Z notation. They define various properties using rules restricting valid options in two categories: security and cost.
- Binz, et al. [7], propose Enterprise Topology Graphs (ETG) as formal model to describe an enterprise topology. Based on the established graph theory, ETG bring formalization and provability to the cloud. Also, authors show how ETG can improve the environmental impact of the enterprise IT.

Consequently, cloud computing paradigm lacks a formal and verifiable model of its basic concepts: service delivery and deployment models, only some technological attempts are realized; for virtualization as it has been done in [2] and [3], for security as in [4], [5] and [6], or for enterprise IT as in [7].

In this work, we adopt, Bigraphical Reactive Systems (BRS), proposed by Milner [8], as a formalism to specify fundamental aspects of cloud computing. In particular, we propose a theoretical framework based on BRS aiming to formalize relationships between service providers and customers in different delivery and deployment models of cloud computing. Based on a judicious coupling between bigraphs theory as a semantic framework and Maude language[9] as a specification language, we propose the Bigraphical Maude-Based Model Checker (BMMC) that combines logical reflection and hierarchical structuring of the underlying adopted theoretical framework to simply execute and verify complex cloud systems. The proposed approach is validated through a concrete verification of two cloud computing inherent properties: service availability and quick scalability.

This paper is arranged as follows. In the next section we define the bigraphical model for cloud computing. Section 3 presents a mapping of the defined model to Maude-based specification and exploits it to formally verify cloud systems. Finally, conclusion and future work are addressed in section 4.

2 BRS for Cloud Computing Specification

A BRS (Bigraphical Reactive Systems) [8] consists of a category of bigraphs and a set of reaction rules that may be applied to transform these bigraphs. The bigraph as an ordinary graph is composed of nodes and edges, unlike nodes in a bigraph can be nested giving rise to hierarchical and larger bigraphs. Additionally, it is the resulting graph of composing a link graph; representing interconnection between nodes, and a place graph; expressing the physical locations of these nodes; hence the prefix "bi" in bigraph.

In this work, we adopt BRS for two reasons. On the one hand, our model emphasizes on both locality and connectivity that can be used to specify cloud elements location and interconnection (structural aspects)[10]. And on the other hand, bigraphical reaction rules are very useful to formalize cloud services elasticity providing them the ability to reconfigure themselves (dynamic aspects).

2.1 Structural Aspects

Main elements of a cloud architecture can be divided into two essential parts: front-end and back-end elements; that are usually connected via internet. The Front-end encloses customer's computer and necessary interfaces to access the cloud and the back-end contains cloud services. So, BRS modelling of cloud elements is realized as follows:

Cloud Services. A Cloud Service represents an abstraction of three different service delivery models that collaborate to ensure front end requests [11] Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Albeit, all available cloud services will be modelled by nodes, controls (kinds of node[8]) attached to them allow us to distinguish between the three service delivery models. We suggest that nodes of control IaaS and PaaS are active (node permitting reactions inside), and nodes of control SaaS are atomic (empty node). To offer several access modes to cloud services, we propose that each node or cloud service contains three different ports: Public, Private, and Community.

Cloud Customers. A Cloud Customer represents any entity that requests a cloud service. Two types of cloud customers are identified: End users accessing only SaaS, and ISV (Independent Software Vendor) accessing IaaS and PaaS. Thus, we model Cloud Customers as nodes equipped with specific controls to be able to distinguish between both types of Cloud Customers; End user and ISV. Both are atomic nodes and have one port to send their requests.

Cloud Architecture. Interconnecting cloud computing elements is modelled via two distinct relations: hierarchy for cloud services imbrication (IaaS, PaaS and SaaS) and interaction for service request. Formally, a BRS offers two types of independent graphs: Place graph and Link graph, that will be exploited as follows:

Place Graph. formally expresses cloud services and customers location. Figure 1 represents the hierarchy of cloud services within a place graph, where a node of control IaaS (infrastructure) can only contain nodes of control PaaS (platform), also, a node of control PaaS can only contain nodes of control SaaS (software), finally, a node of control SaaS do not contain any nodes.

Link Graph. is independent of locality and expresses service interactions, in terms of service demand/response relationship between cloud services and customers. Link graph of Figure 1 contains five customers: C1, C2, C3, C4, C5 and four cloud services: S1, S2, S3, S4 interconnected as follows: cloud customer C2 is relied to

cloud service S1 via its community port (green color), and cloud customers C4 and C5 are relied to cloud service S4, the first one with a public port (blue color) and the second one with a private port (red color).

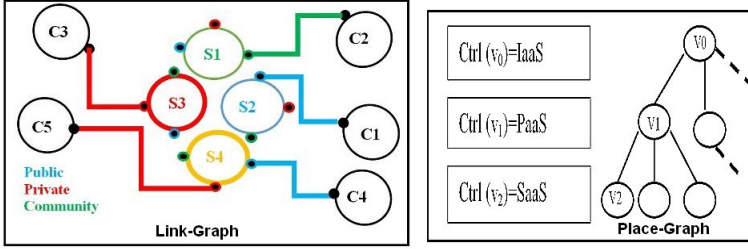


Fig. 1. Place and Link Graphs of a Cloud Architecture.

Composing link and place graphs gives rise to the suited bigraph as defined in what follows:

Definition 1. Cloud Architecture Bigraph takes the form:

$$(V_c, V_s, E, Ctrl_c, Ctrl_s, GP, GL)$$

where: V_c represents the set of cloud customer nodes, and V_s represents all cloud service nodes. E is a finite set of edges. Each node has a control(kinds of node), which is an identifier belonging to a set that is called a signature. $Ctrl_c: V_c \rightarrow S_c$ is a control map that assigns a control to each cloud customer where the signature S_c is defined by $S_c = [EU : (1, atomic), ISV : (1, atomic)]$, and $Ctrl_s: V_s \rightarrow S_s$ is the control map that assigns a control to each cloud service where the signature S_s is defined by $S_s = [IaaS : (3, active), PaaS : (3, active), SaaS : (3, atomic)]$. GP represents the place graph and GL represents the link graph.

2.2 Dynamic Aspects

Additionally to cloud architecture structural aspects formalization, BRS is expressive enough to be adopted for representing cloud dynamics. In this section, we define two categories of reaction rules: Service Allocation Reaction Rules (SARR) and SCalability Reaction Rules (SCRR).

Service Allocation Reaction Rules. We propose two reaction rules, defining the dynamics of bigraphs in terms of service allocation. This category affects bigraph linkage only, where the redex a left hand pattern (R) of a reaction rule, can match any cloud service (IaaS, PaaS or SaaS) and customer (EU or ISV) controls. Figure 2 shows a cloud customer (C1) allocating a cloud service (S1) representing the first reaction rule. Also, it shows a cloud customer (C2) liberating a cloud service (S2) representing the second reaction rule.

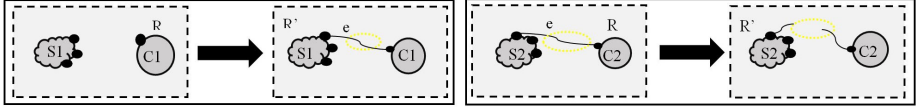


Fig. 2. Service Allocation/deallocation Reaction Rules.

SCalability Reaction Rules. The need of cloud services scalability is justified by system surcharge with customer requests rendering system services unavailable. One solution of cloud services unavailability is a scaling-up of the cloud system, by creating new instances of the concerned cloud service (loaded in memory). This instance will be responsible of taking in charge new customer demands (by doubling cloud service initial bandwidth). Also, a garbage collector can be automatically triggered when cloud customers liberate a cloud service. It models a scaling-down of a cloud system. Thus, we define two reaction rules; representing cloud system scaling up and down respectively (see Figures 3).

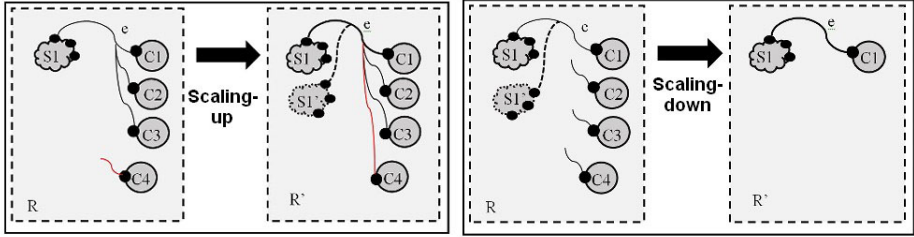


Fig. 3. Scaling-up/down Reaction Rules.

Table 1 bellow summarizes the correspondence between Cloud Computing elements and BRS concepts:

Table 1. Mapping cloud computing concepts to BRS.

Cloud Computing	Bigraphical Reactive Systems (BRS)
Service	Node.
Customer	Node.
Service models	Controls.
Customer types	Controls.
Cloud architecture	Bigraph.
Cloud dynamics	Reaction rules.

3 Verifying Cloud Systems

A set of tools is proposed for BRS edition as BigMC[12], BPLTool [13], DBtk [14], etc. However, during their exploration, we have been confronted with several limitations to verify a specific bigraph with new types of nodes (controls) adapted to the context of Cloud Computing. Therefore, we propose the Bigraphical Maude-Based Model Checker (BMMC) in which a cloud architecture can be easily executed and verified. It confronts system model to system invariants to produce two possible results. A positive

result is returned if the bigraphical model execution satisfies the desired properties or a negative result otherwise.

The use of rewriting logic via its Maude language[9], offers an executable and analysable specification that takes advantage of tools around Maude environment, as the model-checker for linear temporal properties verification[9].

3.1 BMMC Modules Description

A set of modules has been defined to map cloud bigraphical concepts to Maude. The following descriptions of modules show how the previous specification is translated to Maude.

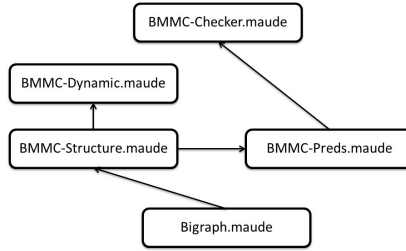


Fig. 4. Overview of BMMC modules.

Figure 4 gives a basic overview of the BMMC modules and their sub-module dependencies.

- The Bigraph module includes sort and operator declarations for Bigraph theory:

```

mod Bigraph is
...
sorts Node Bigraph Edge Port Control .
...
op _|_ :-> Bigraph Bigraph [ctor comm assoc id: null] .
op edge_: Nat-> Edge [ctor] .
...

```

Prime product operator (|) is a juxtaposition operator of nodes or bigraphs, since it takes as arguments two bigraphs with nodes being a sub-sort of bigraph.

- The syntax and semantics of cloud elements are defined in the BMMC Structure module:

```

mod BMMC-Structure is
...
op IaaS :-> Ss [ctor] .
op PaaS :-> Ss [ctor] .
op SaaS :-> Ss [ctor] .

```

```

op EU :-> Sc [ctor] .
op ISV :-> Sc [ctor] .
...
op service<_;;_>[_].{ _ } : Qid Ss S_State Port
                                Bigraph -> Vs [ctor] .
op customer<_;;_>[_] : Qid Sc Qid Port
                                Edge -> Vc [ctor] .

endm

```

Service operator serves to specify a cloud service, it takes as arguments:

- a Quoted Identifier to specify its name;
- a Control specifying its service delivery model;
- an Attribute specifying a service state (available, unavailable, and cloned).
- a set of Edges to be connected to its predefined ports;
- a set of child nodes being contained within the considered service.

Customer operator allows specifying a cloud customer, it takes as arguments:

- a Quoted Identifier to specify its name;
- a Control specifying its customer type;
- a Quoted Identifier to specify the requested service;
- a Port on which the requested service will be delivered;
- an Edge connected to its port.

- Cloud systems dynamics has been formalized with BMMC Dynamic module, containing a set of rewrite rules corresponding to BRS reaction rules. We assume that the term [Req] in customer operator characterizes a service requester, while the term [Lib] represents a customer who liberates a requested service.

```

mod BMMC-Dynamic is
...
rl [Service-Allocation] :
    service< i ; cs:Ss ; available >[ e1 , e2 , e3 ].{ b2 } |
    customer< i1 ; cc1:Sc ; i ; p:Port >[ Req ] | b1
=>
    service< i ; cs:Ss ; available >[ e1 , e2 , e3 ].{ b2 } |
    customer< i1 ; cc1:Sc ; i ; p:Port >[ e1 ] | b1 .
rl [Service-Liberation] :
customer< i1 ; cc:Sc ; i ; p:Port >[ edge na ] | b1
=>
customer< i1 ; cc:Sc ; i ; p:Port >[ Lib ] | b1 .
...

```

Reaction rules (defined in Section 2.2) will be transformed into rewrite rules. Thus, several rewrite rules are defined in terms of service allocation and system scalability.

- The BMMC Preds module represents a system specification property expressed in linear temporal logic. The relevant state predicates are typically part of the property specification. So, we propose two state predicates to identify whether a service is cloned or a customer is a service requester. These predicates can be parametrized with service and customer operators; their semantics is defined as follows:

```
mod BMMC-PREDS is
...
  subsort Bigraph < State .
  op requester : -> Prop .
  op cloned : -> Prop .
...
eq customer< i1:Qid ; c:Sc ; i2:Qid ; p:Port >[ Req ] | b
|=
requester = true .
eq service< i1:Qid ; c:Ss ; cloned >[e1, e2, e3].{ b1 } | b
|=
cloned = true .
...
```

- Model checking LTL formula is realized using a given initial state. For this reason, BMMC-Checker module, defines an initial state containing a service (s2) of control IaaS that is unavailable and a customer (c4) of control ISV requesting service (s2) via its public port. In this case and during execution, the system will automatically (by running the scaling-up rule) add an instance ("cloned") of service (s2) to treat customer (c4) request.

```
mod BMMC-CHECKER is
...
  op initial1 : -> Bigraph .
  eq initial1 =
service< s2; IaaS; unavailable>[edge 1, edge 2, edge 3].{null}
| customer< 'c4 ; ISV ; 's2 ; PbP >[ Req ] .
endm
```

3.2 Services Availability and Quick Scalability Properties

The BMMC, implemented in Maude as a system module, provides an executable specification of a cloud system. It can be exploited to simulate the cloud system so specified. But we can do more. Under appropriate conditions we can check that our bigraphical model satisfies some important properties. We deal here with simpler, yet very useful, properties such as service availability and quick scalability, while considering initial state specified in "BMMC-Checker" module in this example case. Figure 5 below shows model checking results of service availability and quick scalability properties that are both verified.

The specification of the considered properties:

- *"Services Availability is fulfilled if system model (in its canonical final states) do not contain an unsatisfied customer request".*

- “Quick scalability is verified if all states, in which no more rewrites are possible, contain at least one instance of a cloned cloud service”.

These specifications are expressed by the following LTL formulas:

- $O [] \text{not} (\text{requester})$.
- $O [] (\text{cloned})$.

```
Maude>
Maude> reduce in BMW_CHECK : modelCheck(initial1, O [] ~requester) .
rewrites: 11 in 14099565028ms cpu (1ms real) (0 rewrites/second)
result Bool: true
Maude> reduce in BMW_CHECK : modelCheck(initial1, O [] cloned) .
rewrites: 10 in 14099565028ms cpu (1ms real) (0 rewrites/second)
result Bool: true
```

Fig. 5. Verification of Services Availability and Quick Scalability properties.

4 Conclusion

Bigraphical Reactive Systems (BRS) have been adopted as a semantic framework for cloud computing specification. BRS seem adequate for two reasons. Firstly, the model emphasizes on both locality and connectivity that can be used to specify location and interconnection of cloud systems. Secondly, a set of reaction rules, providing to bigraphs the ability to reconfigure themselves, are very useful to formalize cloud system dynamics, especially cloud services elasticity. The defined bigraphical model allows developers to correctly reason about most cloud computing features as modelling, composition and reconfiguration. Particularly, we have shown how this model provides a flexible theoretical framework where cloud service delivery and deployment models can be naturally defined. A nice consequence of this axiomatization is that relationships between cloud services and cloud customers have been exploited to formally verify some properties. This would not have been possible without the proposal of the BMMC, which is the mapping of bigraphical model to a Maude-based formal executable specification. Compared to existing works, the proposed approach achieves a balance between understandability of representation and formal reasoning techniques.

As future work, we plan to exploit meta-modelling and model transformation tools to realize a graphical interface and a BMMC specifications generator in order to facilitate the exploitation of our proposed approach, thereby permitting graphical edition and automatic generation of the corresponding specifications.

References

1. Michael, A., Armando, F., et al.: Above the clouds: A berkeley view of cloud computing, EECS Department, University of California, Berkeley (2009)
2. Dong, H., Hao, Q., Zhang, T., Zhang, B.: Formal discussion on relationship between virtualization and cloud computing. In: PDCAT. (2010) 448–453
3. Grandison, T., Maximilien, E., Thorpe, S., Alba, A.: Towards a formal definition of a computing cloud. In: SERVICES, 6th World Congress on. (2010) 191–192

4. Luo, S. X., Liu, F. M., Ren, C. L.: A hierarchy attribute-based access control model for cloud storage. In: ICMLC. Volume 3. (2011) 1146–1150
5. Adamov, A., Hahanov, V.: A security model of individual cyberspace. In: EWDTs. (2011) 169–172
6. Freitas, L., Watson, P.: Formalising workflows partitioning over federated clouds. In: SERVICES, IEEE Eighth World Congress on. (2012) 219–226
7. Binz, T., Fehling, C., Leymann, F., Nowak, A., Schumm, D.: Formalizing the cloud through enterprise topology graphs. In: Cloud Computing (CLOUD). (2012) 742–749
8. Milner, R.: The Space and Motion of Communicating Agents. Cambridge University Press (2009)
9. Clavel, M., Durn, F., Eker, S., et al.: All about maude - a high-performance logical framework. Lecture Notes in Computer Science, Springer (2007)
10. Benzadri, Z., Belala, F., Bouanaka, C.: Towards a formal model for cloud computing. In: ICSOC 2013 Workshops. (2013)
11. Mell, P., Grance, T.: The nist definition of cloud computing, National Institute of Standards and Technology (NIST) (2011)
12. Perrone, G., Debois, S., Hildebrandt, T. T.: A model checker for bigraphs. In Ossowski, S., Lecca, P., eds.: SAC, ACM (2012) 1320–1325
13. Glenstrup, A. J., Damgaard, T. C., Birkedal, L., Hjsgaard, E.: An implementation of bigraph matching (2008)
14. Bacci, G., Grohmann, D., Miculan, M.: Dbtk: A toolkit for directed bigraphs. In: CALCO. Volume 5728., Springer (2009) 413–422

Modelling Financial SaaS as Service Components

Muthu Ramachandran and Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Leeds, LS6 3QS, U.K.
{M.Ramachandran, V.I.Chang}@leedsmet.ac.uk

Abstract. Financial applications demand better performance and accuracy in a cloud than the traditional computing platforms. Therefore, designing financial software as a service (FSaaS) requires engineering and systematic approach. This paper has designed a financial SaaS component model and a service architecture supporting required flexibility, scalability, and allowing change in environment. This paper has proposed an integrated service-oriented architecture and a SaaS component model for financial domain that provides required scalability, flexibility and customisation. We have also demonstrated the design and customisation of service component interfaces to the financial simulation so that it provides automatic prediction models for investors to know accurate results in buy and sale prices. Therefore, large-scaled simulations can be achieved within a matter of seconds (13.5 seconds).

1 Introduction

Financial applications require on-demand services that are offered by cloud computing with cost-benefits. Therefore, financial domain has begun to reap these benefits with emerging financial SaaS such as FinancialForce which is developed by Salesforce, NetSuite, Intacct, and Oracle's financial SaaS. NetSuite [11] claims helped companies to increase their revenues by 95% by moving to their financial SaaS. Accenture [1] report on financial technology trends and high performance computing predicts:

- Leveraging technology to address new & change in regulations
- Reliable and globally harmonised financial systems
- Add value through strategic applications
- Harvest benefits from technology

Accenture [1] report also claims SaaS to be a simple, efficient, engaging, accessible, clear structure, intuitive, and supportive. With keeping this set of requirements as design criteria, this paper has designed a SaaS component model and a service architecture supporting required flexibility, scalability, and allowing change in environment. This paper has proposed an integrated service-oriented architecture and SaaS component model for financial domains which provides required scalability, flexibility and customisation that are at the heart of a financial SaaS.

We demonstrate the system design and the implementations. Examples include the results of running software that can compute call and put prices. Results of simula-

tions also support the fact that all computations can be completed within seconds. To illustrate our key messages, the breakdown of this paper is as follows. Section 2 presents the overall view about SOA approach an FSaaS application. Section 3 discusses the service component model. Section 4 shows the results of running FSaaS and large-scaled simulations in seconds. Section 5 sums up issues covered and provides conclusion.

2 SOA Approach for FSaaS Applications

FSaaS applications require open, flexible, interoperable, collaborative and integrated architecture to provide services to integrate various stakeholders such as citizens and financial services (e-shares, e-stockbrokerage, e-fund-management, QoS, FSaaS cloud simulation services, e-health, e-tax, e-national security, e-pension, e-payment, e-education and training, e-work and employment, e-funding, etc), business organisations and vendors (e-procurement), and government agencies (both inter and intra governments). Therefore, designing architecture for FSaaS applications pose a design challenge. Software architectural design needs to be verified, assessed and evaluated for its quality before its development. There are well known generic design criteria such as flexibility, maintainability, testability, reusability, etc. The key to achieving good architectural quality for the system being developed is to extract key characteristics of this system from various sources such as non-functional requirements, customer requirements, existing systems, experts, research literatures [2-3 & 6-16] and so on. This paper identifies such characteristics from various perspectives supporting emerging technologies which are shown in Figure 1. These FSaaS application characteristics are the backbone for developing service-oriented architecture and components.



Fig. 1. Characteristics of FSaaS Applications.

To further expand on concepts in Figure 1, FSaaS applications need to work and interface with multi-platform and multi-vendor applications and therefore this needs

to be designed for interoperability. Multi-channel delivery of services has been recommended to deliver FSaaS services through various and emerging communication channels such as mobile phones, digital TV, cloud services, call centres, kiosks, emails, PCs, teleconferencing, e-gov apps, web, and webinars - some of these are not been used by any government at present. Each characteristic shown in Figure 1 represents not only the application attribute but it also provides a set of key design criteria and quality attributes for developing architecture that support emerging technologies for FSaaS. For example, the design criteria interoperability is paramount for FSaaS applications as they are multi-platform and multi-channel based. Interoperability is supported in the service-oriented architecture design for FSaaS applications by means of a service bus and loose coupling of the other components which is shown in Figure 2.

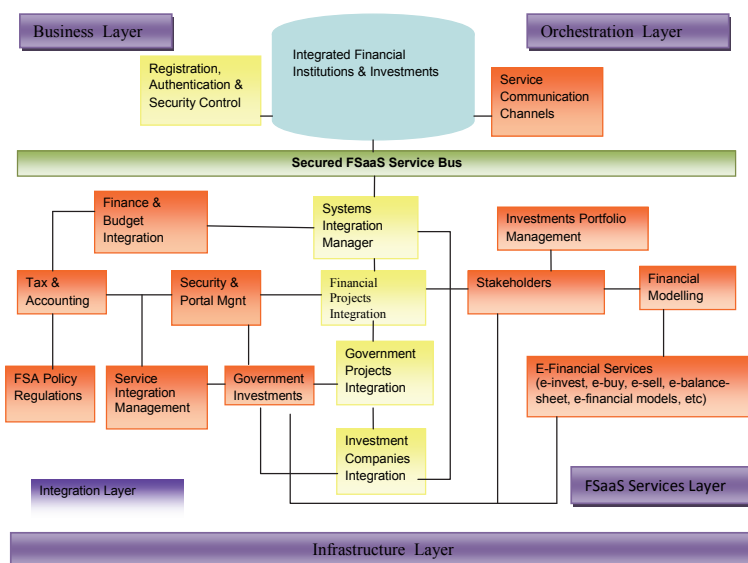


Fig. 2. Service-Oriented Architecture for FSaaS.

These services can be made available as stand alone, integrated, componentised, web based service component, composite service (a set of interconnected services), virtualised services (cloud based), and dynamically re-configurable services. The architecture presented in this paper is then based after a critical review and analysis of a number of existing architectures for FSaaS applications. As mentioned before, the SOA based architecture consists of four distinct levels of abstraction layers which are connected and communicated by messages through a core communication channel known as a service bus or a central bus. These layers are: 1) a business layer with a dedicated set of services, 2) an orchestration layer with a set of services where new services can be composed, 3) an FSaaS layer that supports integration of services, government departments and local governments, and 4) an e-business layer that supports new businesses and integration of data. The SOA based architecture for FSaaS services then ensures that it achieves the expected service-oriented design factors such as customisation, cost-effectiveness, availability, etc.

Referring to Figure 2, at the business and orchestration layers provide high level service composition based on new business perspective and policies (both political and economical factors). Mostly, the customisation and the new business needs arise from these two key variables. The sub-systems such as registration control, security control, integrated services for FSaaS applications control, and communications channels help to achieve customisation at a higher level of abstraction without affecting underlying business logic services. These are communicated and connected to layers below using a concept of service bus known as FSaaS secured service bus. The layer below the business layer provides services from various FSaaS departments, and external suppliers (e-Business layer).

3 Service Component Model for FSaaS Applications

This section proposes an approach to developing FSaaS applications which is based on developing a financial service component which has provides required customization extensibility. As stated before, e-government applications require open, flexible, interoperable, collaborative and integrated architecture to provide services. These services can be made available as stand alone, integrated, componentised, web based service component, composite service (a set of interconnected services), virtualised services (cloud based), and dynamically re-configurable services. This vision is similar to the Open Group's Service Integration Maturity Model (OSIMM) [13]. The OSIMM provides:

- A process roadmap for attaining key practices with metrics
- Seven levels of maturity to improve
- A quantitative model for assessing current practices and to improve with recommended practices

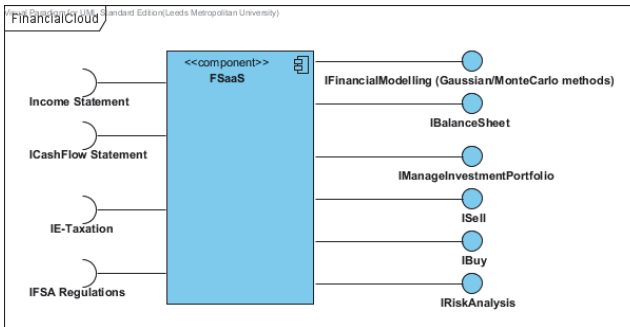


Fig. 3. FSaaS Service Component Model.

Figure 3 shows a design of software as a service component model for financial applications (FSaaS) where it shows two types of services such as provide (lollipop notation) and require services (arc notation and the naming convention starts with I). For example, FSaaS services include Income statement, ICashFlow statement, Ie-taxation, IFSA regulations). IFSA refers to providing interface service integration for Financial Authority regulations which any investment service providers should ad-

here to and is flexible for change in their regular change thus providing required scalability and flexibility of FSaaS characteristics discussed earlier.

Similarly, providers service interfaces are Ifinancial modelling, IBalancesheet as a service which is automatically produced from income and cashflow statements. The other provider interfaces include ImanageInvestment Portfolio, Isell, IBuy, and IRiskAnalysis services. In order to achieve the recommended process and key practices, we need to have interoperability, reconciliations and resiliency between systems, where interface linkages are appropriate to other services such as those of emerging technologies interfaces (e.g. Ie-taxation linked to E-Gov applications, and IFSA regulation service linked to FSA). Similarly, such reconciliations services must be automated for the sake of cost-efficiency. To develop an integrated FSaaS service-oriented architecture system, it is critical that service analysts and software engineers identify and address the key challenges when implementing e-government services. Some of relevant questions are listed below:

- How to adopt a new process and to identify the scope of the business services to be developed and supported?
- How data integrity will be achieved and secured?
- How data will be protected when needed to support management decisions?
- How systems will fit together to support service choreography and orchestration layers?
- How systems will fit together to support the enabling emerging technologies (system architecture needs to be service-oriented thereby any new emerging technologies in the future should easily be integrated more cost-effectively than with traditional system architectures)?
- How data and services will be safeguarded and secured to ensure the integrity and re-configurability of service operations and personal data (information assurance)?
- How new services can be composed and re-configured at run-time?

This paper has address some of these issues such as achieving business process using BPMN for identifying FSaaS component services, management decision are intergrted with service component interfaces as governance, SOA architecture model has been designed to illustrate other issues. Currently, we are working on developing a WSDL to link to relevant MATLAB code or any other simulation services as shown in Table 1 (discussed in the following section).

4 Demonstrations and Simulations for FSaaS

This section demonstrates how FSaaS can be used and explains the code and results during and after using FSaaS services. This mainly involves Monte Carlo Methods (MCM) and Black Scholes Model (BSM). Chang et al., [4] describe how to use MCM and BSM for financial computation. They demonstrate the use of risk analysis and financial modelling on Clouds based on MATLAB and Mathematica, which offer benefits such as performance, accuracy and integration with security. This includes the selection of Linear Square Method (LSM) that can compute 100,000 simulations

in one go, which takes between 4 to 25 seconds depending on the number of time steps. It can also work with IBM Fined-Grained Security Model, and it can provide a safer environment for FSaaS on Clouds.

Mathematical models such as MCM are used in Risk Management area, where they are used to simulate the risk of exposures to various types of operational risks. Monte Carlo Simulations (MCS) in Commonwealth Bank Australia are written in Fortran and C#. Running such simulations may take several hours or over a day [4, 5]. The results may be needed by the bank for the quarterly reporting period. MCM is suitable to calculate best prices for buy and sell, and provides data for investors' decision-making [4, 5]. MATLAB is used due to its ease of use with relatively good speed. While the volatility is known and provided, prices for buy and sale can be calculated. Part of the code (fareastmc.m) to is used to present formulas in MCM and demonstrate coding algorithm presented in Table 1. Variables are explained in [4].

Table 1. Coding algorithm in Monte Carlo in MATLAB for best buy/sell prices.

```
dt=T/(NSteps-1);
vsqrdt=sigma*dt^0.5;
drift=(r-(sigma^2)/2)*dt;
x=randn(NSimulations,NSteps);
Smat=zeros(NSimulations,NSteps);
Smat(:,1)=S;
for i=2:NSteps,
    Smat(:,i)=Smat(:,i-1).*exp(drift+vsqrdt*x(:,i));
end
```

The following demonstrates running the code and the calculated prices. Call prices are to buy and put prices are for sale. The program calculates the lower limit, the MCPrice value and the upper limit for each buy and sale category.

> fareastmc (this is the name of the MATLAB file)

[LowerLimit MCPrice UpperLimit]

Call Prices: [4.196694 4.248468 4.300242]

Put Prices: [7.610519 7.666090 7.721662]

Outliers are common while during computation and they do not fall into the expected results. To achieve a high level of accuracy, outliers need to be removed. Figure 4 is a good example. Two screenshots on the left half with “original gamma variables” show that financial indexes have outliers. In other words, they are not smooth and outliers need to be filtered out. The other two screenshots on the right half with “stratified gamma variables” means that all outliers are removed and the results are smooth and usable for predictive modelling or other financial computation. Removal of outliers can ensure a high quality of data analysis can be offered to investors. How removal of outliers relates to the architecture is as follows. It ensures numerical computations are as accurate as possible and do not provide results that may make investments or decisions that incur in the loss of money and reputation.

We then perform large-scale simulations to show that all computations can be achieved within seconds. The hardware infrastructure is as follows. The desktop has

2.67 GHz Intel Xeon Quad Core and 4 GB of memory (800 MHz) with installed. Two Amazon EC2 public clouds are used. The first virtual server is a 64-bit Ubuntu 8.04 with large resource instance of dual core CPU, with 2.33 GHz speed and 7.5GB of memory. The second virtual server is Ubuntu 7.04 with small resource of 1 CPU with 2.33 GHz speed and 1.5 GB of memory. There are two private clouds set up. The first private cloud is hosted on a Windows virtual server, which is created by a VMware Server on top of a rack server, and its network is in a network translated and secure domain. The virtual server has 2 cores of 2.67 GHz and 4GB of memory at 800 MHz. The second private cloud is a 64-bit Windows server installed on a rack, with 2.8GHz Quad Core Xeon, 16 GB of memory. Our FSaaS can work on both Octave or MATLAB. The experiment began for running the Octave 3.2.4 on desktop, private cloud and public cloud and started one at a time due to the licensing issue. Table 1 summarises the benchmark for the execution time, which involves running FSaaS simulations in five different platforms. It took longer time to run simulations in the public cloud with small instances, which is not recorded in Table 2. This is due to their low CPU and memory requirements resulting in longer completion time. The key advantage of designing FSaaS as a service component is any change in the financial models which can be changed without any ripple effect to the entire FSaaS architecture.

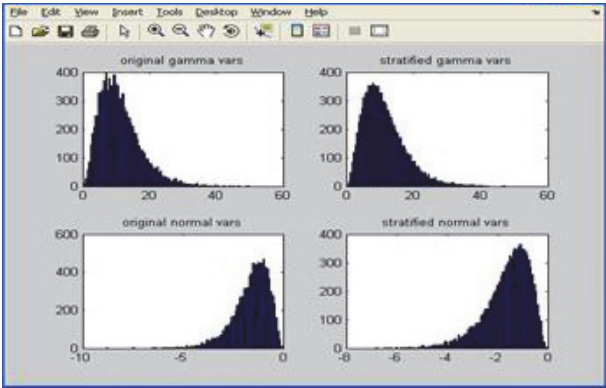


Fig. 4. Removal of outliers.

Table 2. Timing benchmark to run FSaaS code on Octave 3.2.4.

Number of simulations and time taken (sec)	5,000	10,000	15,000
Desktop	11.08	11.92	12.71
Public cloud (large instance)	11.95	12.30	13.15
Private cloud (default VMs)	11.31	12.13	12.90
Private cloud (large VMs)	9.63	10.51	11.48

5 Conclusion

Financial applications demand better performance and accuracy in a cloud than the traditional computing platforms. Therefore designing financial software as a service

(FSaaS) requires engineering and systematic approach. This paper has demonstrated a systematic approach to developing large scaled financial applications with current technology such as SOA which supports SaaS features to be integrated with cloud solutions. This paper has also demonstrated the design and customisation of service component interfaces to the financial simulation so that it provides automatic prediction models for investors to know accurate results in buy and sale prices. Therefore, large-scaled simulations can be achieved within a matter of seconds (13.15 seconds).

References

1. Accenture (2011) <http://www.slideshare.net/fullscreen/ramblingman/accenture-financial-saa-s-external-presentation-final/3>
2. Baresi, L., Di Nitto, E., and Ghezzi, C (2006) Towards open-world software: issues and challenges, *Computer, Special Issue on Software Engineering: the past and the future*, October 2006.
3. Cartwright I and Doernenburg E (2006) Time to jump on the SOA bandwagon, *IT Now*, British Computer Society, May 2006
4. Chang, V., Li, C.S, De Roure, D., Wills, G., Walters, R.J., Chee, C.: The Financial Clouds Review, *International Journal of Cloud Applications and Computing*, 1 (2), (2011) 46-63.
5. Chang, V., *Business Intelligence as Service in the Cloud*, Future Generation Computer Systems, (2014).
6. Erl, T (2005) Core principles for service-oriented architectures, August 2005, Retrieved Oct 2013, from www.Looselycoupled.com/opinion/2005/erl-core-infr0815.html
7. Groves, D (2005) Successfully planning for SOA, *BEA Systems Worldwide*, 11 Sept 2005
8. Helbig, J (2007) Creating business value through flexible IT architecture, *Special Issue on Service-oriented Computing*, *IEEE Computer*, V.40, No.11, November 2007.
9. Hohpe, G (2002) *Stairway to Heaven*, Software Development, May 2002
10. Nano, O. and Zisman, A. (2007) Realizing service-centric software systems, *Special issue on SoC*, *IEEE Software*, November/December 2007.
11. NetSuite (2014) <http://www.netsuite.co.uk/portal/uk/seo-landing-page/accounting-2/main.shtml?gclid=CLK9k5q-37sCFTHLtAodikoAzw>, accessed 2014
12. Open Group (2009) OSIMM, Retrieved Oct 2013, from <https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12450>
13. Ramachandran, M (2012) *Software Security Engineering: Design and Applications*, Nova Science Publishers, New York, USA, 2012. ISBN: 978-1-61470-128-6, https://www.novapublishers.com/catalog/product_info.php?products_id=26331
14. Ramachandran, M (2013) *Business Requirements Engineering for Developing Cloud Computing Services*, Springer, *Software Engineering Frameworks for Cloud Computing Paradigm*, Mahmood, Z and Saeed, S (eds.), <http://www.springer.com/computer/communication+networks/book/978-1-4471-5030-5>
15. Sellami, M. and Jmaiel, M (2013) A Secured Service-Oriented Architecture for FSaaS in Tunisia, www.redcad.org/PDFs/C33.pdf, accessed on 15th September.
16. Wauters, P., Declercq, K., van der Peijl, S., and Davies, P (2011) Study on cloud and service-oriented architectures for FSaaS, FP7 report ref. Ares(2012)149022 - 09/02/2012, Deloitte.

The Big Data Analysis for Measuring Popularity in the Mobile Cloud

Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Headingley, Leeds LS6 3QR, U.K.
V.I.Chang@leedsmet.ac.uk

Abstract. This paper presents the Big Data analysis for measuring popularity in the Mobile Cloud, which is an emerging area in the Cloud and Big Data Computing. Organizational Sustainability Modeling (OSM) is the proposed method used in this research. The twelve-month of German consumer data is used for the analysis to investigate the return and risk status associated with the popularity in the Mobile Cloud services. Results show that there is a decline in the usage due to the economic downturn and competitions in the market. Key outputs have been explained and they confirm that all analysis and interpretations fulfil the criteria for OSM. The use of statistical and visualization method proposed by OSM can expose unexploited data and allows the stakeholders to understand the status of return and risk of their Cloud strategies easier than the use of other data analysis.

1 Introduction

Cloud Computing provides added value for organizations; saving costs in operations, resources and staff – as well as new business opportunities for service-oriented models [3, 10, 13]. There are applications and services in emerging areas which have increased demands and are worthwhile exploring. One such area is Mobile Cloud. Current literature has emphasized in the system design, development and deployment examples [6, 8]. There is little literature about the surveys focusing on the customers and their rating of satisfaction towards using Mobile Cloud services. It is important and useful to understand consumer behaviors and preferences for mobile products and services to stay competitive in the market [6, 7, 12]. In order to define what to measure, propose how to measure and analyze data, a systematic method is required. A proposed method can systematically compute all these data and explain the interpretations of these data, in the form of statistical modeling or visualization. Reporting the status of risk and return of such Cloud adoption is important, since it can provide stakeholders an overview about their service rating, risk monitoring and analysis about whether their strategies of offering Cloud services have met their expected targets. In this way, the businesses can be more adaptable to the fast-paced requirement changes for Cloud Computing, particularly Mobile Cloud, which is a fast-growing area.

To address the requirements and challenges described in the last paragraph, Organizational Sustainability Modeling (OSM) is designed to measure and calculate risk and

return status for adopting Cloud Computing. This is designed to process and analyze Big Data and complete computation of results within seconds. It can provide explanations of the key statistics and interpret them in a way that makes the stakeholders to understand the status of their risk and return of Cloud adoption at regular periods. In summary, two advantages are available for using OSM: (i) it computes the status of risk and return of Cloud adoption; (ii) the use of visualization technique can simplify about the understanding of complex datasets and (ii) results provide empirical evidences to critically evaluate about the Cloud strategy and recommendations towards their return and risk status. The structure of this paper is as follows. Section 2 introduces OSM and explains how it can be used. Section 3 describes the data analysis process and presents the results and their interpretations. Section 4 sums up conclusion for this paper.

2 Organizational Sustainability Modeling (OSM)

Organizational Sustainability Modeling (OSM) is improved version based on the CAPM which is the analysis of return and risks for organisations or projects. Chang et al. [1, 2] demonstrate how OSM can be used to measure risk and return status for SAP, Vodafone/Apple and two projects in National Health Services, UK. The proposed approach is to divide return and risk in three areas: Technical, Costs (Financial) and Users (or clients) before and after deploying cloud solutions or products/services. In some context, it can be defined as expected return and actual return. The data to be collected are dependent on organizational focus. In this paper, the focus is on investigating the popularity in using iPhone 4S and their services for a twelve-month period of 2012 to compare the data collected in 2011. This keeps stakeholders informed of the consumers and market requirements, which can be fast-paced and competitive in the Mobile Cloud industry. In Chang et al [2, 3] statistical and visualization analysis, Apple iPhone and iPad have offered Vodafone between 22% and 26% of extra profits between 2009 and 2010. This means Vodafone has adopted the right strategies of using iPhone and iPad to increase their profits and market dominance.

The use of OSM has a strong record of analyzing risk and return status for Cloud adoption, which include detailed analysis for profitability and risks for Vodafone with iPhone and iPad strategies [2, 3]. This includes advanced statistical computing and the innovative approach of presentation of complex data analysis in 3D Visualization, which offers two benefits:

- It exposes any hidden or unexploited data for analysis. There is no need to statistically analyze data several times.
- Anyone without prior backgrounds can find the analysis easier to understand due to the interpretation of statistical results and presentation of results in the form of visualization.

2.1 Organizational Sustainability Modeling

OSM is the improved model based on Capital Asset Pricing Model (CAPM) [1, 2, 4],

which has three major limitations. First, it does not support large data processing since it was originally designed in 1960s and large data processing is a requirement for Big Science. Second, it is a generic model for risk and return analysis and additional work is required to make it suitable for system adoption. Third, the risk-free rate does not exist in reality most of the times. Additional work is required to define how to control risk and monitor the changes in the risk-control rate. Based on these requirements, the OSM formula is presented as

$$e = r_c + (\beta(a - r_c)) \quad (1)$$

where a is the actual return (or performance) of a large computing systems project or investment.

r_c is the risk control rate. It can be interpreted as the rate that is free of risk, or the rate that risk can be managed. This is the rate for manageable risk.

e is the expected return (or performance) of a large computing systems project or investment, and β is the beta value to represent risk measure or uncontrolled risk. These are unpredictable events which cannot be managed and have a direct impact on the adoption of the system

The uncontrolled risk, beta, can be calculated once when the expected value, the actual value and risk-control rate in each dataset are available. A good approach is to calculate all beta values and average them out. Another approach for calculating beta is to perform linear regression, where the gradient of the slope is the value for beta [4, 11]. So the formula becomes

$$\beta = \frac{e - r_c}{a - r_c} \quad (2)$$

The steps above require the following input:

- Actual return values (a): the actual values obtained from the measurement.
- Expected return values (e): using the previous data (or previous measurement) as the benchmark, or using computation technique to model the expected values.
- Risk-control rate (r_c): the percentage that does not affect risk if targets are not met. It is often managed and controlled under 5% [4].

After collecting at least several hundred of metrics, these data can use OSM to calculate beta, and compute the overall risk and return values to present to stakeholders.

2.2 Motivation for iPhone 4S, a Representation of Mobile Cloud

Chang et al., [2] presented their Vodafone/Apple case study on Mobile Cloud and it had an overall coverage of iPhone and iPad models. The generalization provides useful recommendation for potential and current investors [3]. Based on our knowledge from investors' requirements, they feel analysis will be more useful if it can be focused on each specific model. This may include iPhone 4S model alone and its computational analysis about its business performance. We assert that the integrated approach has the following advantages:

- It is cost-effective and can provide data and results in the minimum amount of spending.
- The quality of analysis is at a high level of standard, since it goes through a series of quality assurance (QA) process.

The OSM approach can ensure a high quality of analysis and a low cost spending can be achieved. This can ensure a higher return status for investors. OSM reads each value in the dataset, sums up and averages key values. This means if there are 100 rows in the datasets, OSM can sum them up into 10 rows within one to two seconds, and then process datasets for the analysis. Eventually all computations can be completed in seconds. OSM also aims for 99.99% accuracy for all the analysis. Additionally, market contests between smart phones, mobile clouds, service providers and mobile applications for Clouds have become more competitive than before. It is useful to keep track of market demands and consumer requirements so that our Cloud strategies and recommendation can be kept up-to-date.

3 Data Analysis: The Rationale and the Process Involved

This section describes the computational analysis of the collected datasets and explains the interpretations of the data. The source of data is from Kantar Worldpanel ComTech [7], a market research company, as well as Anastaya, a consulting firm specializing in data analysis. The author worked in Anastaya for a period of time as a part-time consultant. A thorough data analysis approach has been adopted to ensure data analysis can be unbiased and reflect the actual risk and the return status of the mobile cloud adoption. The objective of this research is to analyze the rate of satisfaction and the rate of adoption in the EU zone such as Germany.

Although Kantar Worldpanel ComTech has published a report on the iPhone 4S performance in EU, it does not provide detailed statistical and computational analysis. It only offers an estimated percentage of performance downgrade and does not provide any detailed analysis. Therefore, we aim to provide a more comprehensive analysis with the following objectives:

- Compute the exact extent of performance downgrade (or improvement) in EU countries. In this paper, we focus on the German data because Germany is a country behind Euro backing and is a good reflection on how top-tier EU country performed in the economic crisis.
- To provide a rationale and analysis about their performance (downgrade) based on our results.

3.1 Data Processing Overview for the Mobile Cloud

Datasets follow the requirements of the OSM formula (2). Each row of data contains the numerical values for the actual value, expected value and risk-control rate of the German Mobile customer usage. The expected values included the 2010 to 2011 data taken a year before the study began. The actual values included the 2011 data, to in-

investigate the usage of mobile cloud adoption in 2012. The risk data between 2011 and 2012 was collected by Kantar Worldpanel ComTech. Each row of datasets contains the actual and expected values of measurement, and risk-control rate associated with each pair of actual and expected values. The data processing takes each row of datasets – reading all data values; putting data values into the formulas; and then perform statistical regression while using OSM. Another code algorithm is required for statistical analysis after the data processing from first round of OSM analysis. Statistical programs have two steps.

- The first step is to calculate the generic statistics including mean, standard deviation, p-value, t-value and R-squared value.
- The second step is to compute advanced features such as Durbin-Watson test, Sum of Squares Error (SSE), Degree of Freedom Error (DFE) and Mean Square Error (MSE).

The statistical program is written in SAS, a statistical software and language for analysis. Ordinary Least Square (OLS) is useful to compute regression modelling for linear model such as OSM, and is used for statistical program for data analysis. All numerical data for actual and expected values and risk-free rate can be computed based on the code algorithm [4]. The dataset has 1,000 rows of data. With the use of OSM, it sums up into 100 rows and computation can be completed within seconds.

3.2 OSM Data Analysis

This section presents results of the German data analysis and explains the interpretations of all these key statistical values. All the data is based on between January 2011 till December 2011, which provides twelve months of period of popularity measurement for iPhone 4S. OSM can be modelled by statistical languages, in which SAS is more suitable than other languages since it can compute more in-depth analysis [1, 2]. The data is carefully calculated, examined and randomized. Twelve months of data for this case study is sufficient to analyze its business performance, since this is a model specific approach and often Apple product performance can be determined within the first few months in the market release [7]. SAS program for OSM is coded for computation and Table 3 is the summary of key statistics.

Computational modeling of OSM will use a , e , r_c as the input to compute risk. The output should contain the following:

1. Beta (β) is a value to determine the risk measure (or the extent of the volatility), which is the uncontrolled risk that may affect the Mobile Cloud popularity.
2. Standard Error (SE) of the mean is the range of the mean that the experimental results fall into for OSM. The smaller the standard error, the smaller the difference between expected and actual return values [9].
3. Durbin-Watson (DW) is a test used to detect the presence of autocorrelation (a relationship between values separated from each other by a given time lag) in the residuals (prediction errors) from a regression analysis. The result of Durbin-Watson (DW) should be above 1 [9]. Durbin-Watson is used to test regression computed by OSM and accuracy of the output, and also the statistical behaviours.

The value for $Pr > DW$ corresponds to the negative autocorrelation test (residuals eventually wither off) and is a preferred method in the OSM approach, and the value of $Pr > DW$ should ideally get as close as to 1 to reflect the accuracy of the OSM regression. The p-value used by most of statistics is the positive autocorrelation value and can be worked out by subtracting the value of $Pr > DW$ by 1. See Table 1 for results.

- 4. Mean Square Error (MSE) is an estimator to quantify the difference between estimated and actual values. A low MSE value means there is a high correlation between actual and expected return values.
- 5. R-squared value is used to determine how the regression fits in a line. Both 95 and 99.99 Confidence intervals (CI) are computed. In this context, it is referred as “R-squared value for firm”, a term that is commonly used in econometrics to describe the percentage of risks in proportion to the external or internal organizations or factors [9]. If an organization has an R-squared value (99.99 C.I) of 0.3, this means 30% of risks are from external bodies or the market and 70% of risks come from the organization such as poor adoption decision, overspending, poor selection of equipment (resulting in accidents).

The results for OSM regression is as follows.

Table 1. OSM key statistics for German data in Mobile Cloud analysis.

Beta 54.56% of risks: external and 45.44% of risks: internal	0.5345	Durbin-Watson Pr>DW (negative autocorrelation: maximum of 1) Positive autocorrelation (p-value)	1.7068 0.9130 0.0870
Standard Error	0.1447	Regress R-Square (99.99 C.I)	0.7107
Mean Square Error (MSE)	0.15369	Regress R-Square (95 C.I)	0.5456

Further explanations are presented as follows.

- Beta is equal to 0.5345. The medium-low value suggests the project risk is maintained at a good control rate.
- Standard error is 0.1447. The low value suggests most metrics are close to each other and the data has fewer extremes. There is a high consistency between all metrics.
- The first order Durbin-Watson: $Pr > DW$ is the p-value for testing negative autocorrelation which favors OSM. Results show that there is a high negative autocorrelation (0.9130), which is close to 1 in favor of OSM and also has an acceptable quality of data and standard errors. The p-value is the positive autocorrelation and is equal to 0.0870.
- The low Mean Square Error (MSE) value suggests a good consistency between actual and expected return values.
- Main regression R-square is 0.5456. It means 54.56% of the risks are from the externals such as funders’ cost-saving plans and 45.44% of the risks are from the internals, which include the following reasons as confirmed by German user feedback analyzed by Anataya.

3.3 iPhone 4S in Germany: Actual and Expected Values in 3D

The next stage is to convert all datasets into 3D visualization. The rationale is that results in visualization can expose unexploited areas. Often data analysis needs to be read by the stakeholders and key-decision makers, who may not have the background to understand. The use of visualization can simplify the complexity of understanding these analysis. Chang et al. [1, 2, 5] demonstrate 3D Visualization is a simplified analysis for stakeholders and then to make the appropriate actions based on analysis. Mathematica allows data conversion and presents it in a visual format. Data is then computed in Mathematica and the 3D visualization models are presented in Figure 1.

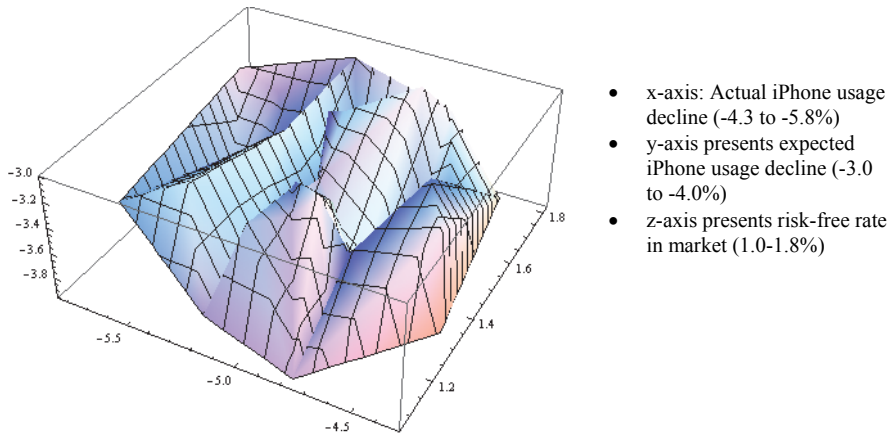


Fig. 1. iPhone 4S popularity in Germany comparing 2011 and 2012.

Figure 1 is the 3D Visualization for iPhone 4S popularity in Germany. The x-axis shows actual iPhone usage is between -4.3 to -5.8%, and the y-axis shows expected iPhone usage is between -3.0 to -4.0% and z-axis presents risk-control rate in the market is between 1.0 and 1.8%. The EU market has an economic downturn, which is expected to impact sales and popularity, but the actual performance is lower than the expected performance. This may mean iPhone 4S has tough competitions from other models with Android systems. These models tend to offer lower prices than iPhone models and have become more competitive in a downturn [12].

3.4 Discussions

This section describes discussions related to the use of OSM. First, it is about comparison between OSM and other methods such as Capital Asset Pricing Model (CAPM). Although CAPM can be used as a generic solution for analyzing return and risk for businesses, it cannot deal with big data. The assumption of risk-free rate is not true. CAPM is not designed for emerging technologies involved with Cloud Computing [4]. OSM is a more structured method that can handle Big Data processing, can explain how to manage risk-control rate and can be used for emerging technologies. Hence, OSM is a better model than CAPM. Second, the discussion about inclusion of data

with at least one more European country. The French data will also be jointly analyzed with the German data in the forthcoming research work, so that our work can have a better representation of European countries.

4 Conclusion

We present the use of OSM to analyze the popularity in the Mobile Cloud. We use the German data between 2011 and 2012 as the example and compare the actual values, expected values and risk-control rates in all the datasets. We explain the use of OSM to process datasets and the key statistics involved and their interpretations. We explain all the key results and show that there is a decline in the popularity due to the economic downturn and also competitions from other mobile systems.

Key results include the beta, standard error, Durbin-Watson, p-values, mean square errors and R-squared values. We confirm that all these key figures fulfil the criteria for the OSM analysis. The use of 3D Visualization can expose unexploited data analysis and also ensure the stakeholders can interpret analysis easily. OSM is an innovative approach which can be adapted in other research projects, in different disciplines and in other case studies. We will demonstrate how OSM can be used in other disciplines and also other European countries to study the popularity in the use of Mobile Cloud.

References

1. Chang, V., De Roure, D., Wills, G., Walters, R. and Barry, T.: Organisational Sustainability Modelling for Return on Investment: Case Studies presented by a National Health Service (NHS) Trust UK. *Journal of Computing and Information Technology*, 19 (2), (2011 a).
2. Chang, V., De Roure, D., Wills, G., & Walters, R. J.: Case studies and organisational sustainability modelling presented by Cloud Computing Business Framework. *International Journal of Web Services Research (IJWSR)*, 8(3), 26-53, (2011 b).
3. Chang, V., Walters, R. J., & Wills, G.: The development that leads to the Cloud Computing Business Framework, *International Journal of Information Management*, 33(3), (2013).
4. Chang, V.: A proposed model to analyse risk and return for a large computer system adoption, PhD thesis, University of Southampton, (2013).
5. Chang, V., *Business Intelligence as a Service in the Cloud*, Future Generation Computer Systems, (2014).
6. Ganti, R. K., Ye, F., & Lei, H.: Mobile crowdsensing: Current state and future challenges. *Communications Magazine*, IEEE, 49(11), 32-39, (2011).
7. Kantar Worldpanel ComTech: Kantar Worldpanel ComTech Global Consumer, White paper and VIP report, December, (2011).
8. Rimal, B. P., Jukan, A., Katsaros, D., & Goeleven, Y.: Architectural requirements for cloud computing systems: an enterprise cloud approach. *Journal of Grid Computing*, 9(1), 3-26, (2011).
9. Lee, C.F., Lee, A.C. and Lee, J. (Ed.), *Handbook of Quantitative Finance and Risk Management*, 1, Springer publisher, ISBN 978-0-387-77116-8, (2010).
10. Schubert, L., Jeffery, K. and Neidecker-Lutz, B.: *The Future for Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*, Expert Group report, public version

1.0, January, (2010).

11. Sharpe, W. F., Capital Asset Prices with and without Negative Holdings, Nobel-Prize Economics Lecture, pp 312-332, Dec 7, (1990).
12. USwitch survey, USwitch's Guide to Mobile Phones, September 2011.
13. Vouk, M. A.: Cloud Computing – Issues, Research and Implementations, Journal of Computing and Information Technology - CIT 16, page 235–246, Volume 4, (2008).

Introduction to the Risk Visualization as a Service

Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Headingley, Leeds LS6 3QR, U.K.
V.I.Chang@leedsmet.ac.uk

Abstract. This paper introduces the Risk Visualization as a Service (RVaaS) and presents the motivation, rationale, methodology, Cloud APIs used, operations and examples of using RVaaS. Risks can be calculated within seconds and presented in the form of Visualization to ensure that unexploited areas are exposed. RVaaS operates in two phases. The first phase includes the risk modeling in Black Scholes Model (BSM), creating 3D Visualization and Analysis. The second phase consists of calculating key derivatives such as Delta and Theta for financial modeling. Risk presented in visualization allow the potential investors and stakeholders to keep track of the status of risk with regard to time, prices and volatility. Results in experiments show that RVaaS can perform up to 500,000 simulations and complete all simulations within 22 seconds. RVaaS provides a structured way to deploy low cost, high quality risk assessment and support real-time calculations.

1 Introduction

Risk analysis is useful to help organizations to understand the extent of business and operational risks, which can vary from time to time. According to Lord Turner, Chair of the Financial Service Authority (FSA) UK, the problem was that the banks' mathematical models assumed a 'normal' or 'Gaussian' distribution of events. Although this reduces computational effort, it can seriously underestimate the real risk [4, 7]. More recently, debt problems in the US and Euro Zone have triggered a further downturn. A study by Hamnett [5] concluded that unsustainable mortgage lending leading to a housing bubble and subsequent collapse was the cause of the Global economic downturn; certainly the collapse of Lehman Brothers [3] which triggered the global financial crisis was the result of irresponsible mortgage lending. We present a case of Risk Visualization as a Service (RVaaS), which uses Cloud Computing to analyze risk and make risk visible. RVaaS is a Cloud based Software as a Service (SaaS) based on Mathematica and MATLAB designed to improve the accuracy and quality of both pricing and risk analysis in financial markets, compared with traditional desktop technologies. This allows investors to identify the status of risks in associations of changes in prices, market confidence and implied volatility. RVaaS has a two stage service in which the stages address the following challenges:

1. Performing a sufficiently high number of simulations in an acceptable time.
2. Quantifying risks and assisting with analysis by providing clear presentations of

results.

The structure of this paper is as follows. Section 2 introduces RVaaS, which includes Black Scholes, Delta and ta, the commonly used derivatives in financial computations. Section 3 describes a full use case scenario to explain how the command-line-like APIs, Black Scholes, Delta and Theta, can be used. Section 4 presents experiments of running RVaaS services. Section 5 presents discussions and Section 6 sums up Conclusion.

2 Risk Visualization as a Service

Better ways to identify risks, rectify errors and perform accurate and fast simulations are highly desirable. Requirements for the RVaaS include the followings:

1. Based on the reputable models – Our RVaaS adopts reputable models including Black-Scholes-Merton (known as Black Scholes Model, BSM) to run exhaustive cases and compute the best pricing and risks for different scenarios.
2. Identification and visualization of risks –BSM is used to identify risks and can make risks to be in visualized formats to expose risks and understand its extent of impacts of implied volatility.
3. High-performance simulations – Our RVaaS should not allow simplicity as the expense of the accuracy due to the use of Gaussian Copula on desktop (Chang, 2014). Our RVaaS should complete all simulations and derivative calculations with a quick time.

2.1 Black Scholes in Theory and Practice

The BSM is commonly used in financial markets and derivative calculations. It is also an extension from Brownian motion. The BSM formula calculates call and put prices of European options (a financial model) [6]. The value of a call option for the BSM is

$$C(S, t) = SN(d_1) - Ke^{-r(T-t)}N(d_2) \quad (1)$$

$$\text{where } d_1 = \frac{\ln(\frac{S}{K}) + (r + \frac{\sigma^2}{2})(T - t)}{\sigma\sqrt{T - t}} \quad \text{and } d_2 = d_1 - \sigma\sqrt{T - t}.$$

The price for the put option is

$$P(S, t) = Ke^{-r(T-t)} - S + (SN(d_1) - Ke^{-r(T-t)}N(d_2)) = Ke^{-r(T-t)} - S + C(S, t). \quad (2)$$

For both formulas [6],

- $N(\bullet)$ is the cumulative distribution function of the standard normal distribution
- $T - t$ is the time to maturity
- S is the spot price of the underlying asset
- K is the strike price
- r is the risk free rate
- σ is the volatility in the log-returns of the underlying asset.

BSM is used as a command-line API. It means users can type in the key figures in the command which compute the numerical values for prices and risk. Mathematica is used to support calculations of derivatives in the Cloud. Both BSM and auxiliary functions (delta and theta compute derivatives) take the same five variables as follows.

- p = current price of the stock.
- k = exercise price of the option.
- sd = volatility of the stock (standard deviation of annual rate of return)
- r = continuously compounded risk-free rate of return, e.g., the return on U.S. Treasury bills with very short maturities.
- t = time (in years) until the expiration date

The contribution from RVaaS is to develop BSM as an easy-to-use command-line API, which allow users to type in key values to get the final answer. The command is **BlackScholes [p,k,sd,r,t]**

2.2 Delta, Theta and Other Requirements

To facilitate the use of BSM command, additional command-line APIs are required. Two of them are known as Delta and Theta, which are part of financial derivatives of calculating advanced pricing and risk [1, 8]. Delta can indicate how much the price of an option will respond to a change of price of the stock. Delta is useful in risk management where a portfolio contains more than one option on the stock. The derivative function, D , is built in Mathematica, which explains why Mathematica is used. This much simplifies coding for Delta, which can be presented as

$$\text{Delta}[p,k,sd,r,t] = D[\text{BlackScholes}[p,k,sd,r,t],t]$$

$$\text{Theta}[p,k,sd,r,t] = -D[\text{BlackScholes}[p,k,sd,r,t],t]$$

To get an inverted Delta, a new function, Theta, is introduced. The operations of RVaaS include:

1. Risk calculation and analysis: This includes calculations of derivatives such as delta and theta which can calculate the accurate approximation for volatility, and the right prices and risk associated with it.
2. A visualization service using BSM: This translates all different types of risk into 3D Visualization so that there is no hidden or missing area of risk.

The benefits of using command-line APIs, BlackScholes, Delta and Theta, allow fast computation of results presented in Section 3.

3 Scenarios of Running 3D Risk

This section describes how RVaaS is used to calculate risk and pricing based on the market value. With regard to BSM, key values such as p , k , sd , r and t need to be known before the calculation. The value p , k and t are known because these values

represent the starting values and the target values. The value of sd can be obtained from Volatility S&P 500 (VIX) Chicago options [2], which releases the daily values of sd . The value of r can be obtained from the government body such as the US Treasury. There are two scenarios given in this case.

The first scenario involves profits/loss in relation to put price. The call price (buying price) for a particular investment is 60 per stock. The put price (selling price) to get zero profit/loss is also 60. The risk-free rate, the guarantee rate that will not incur loss, is between 0 and 1.5%. However, the profit/loss varies because of the impact of volatility in the market. In turn, this means selling prices between 50 and 60 will lead to different extents of loss due to the rapid fluctuations in the market. Similarly, selling prices between 60 and 70 will result in differing levels of profit. The intent is to find out the percentage of profit and loss for a massive sale and the risk associated with it. Using Black Scholes function (BlackScholes [p_,k_,sd_,r_,t_]) where

- p = current price of the stock, set between 40 and 60.
- k = exercise price of the option, 50 is the default.
- sd = volatility of the stock (standard deviation of annual rate of return), 0.45.
- r = continuously compounded risk-free rate of return, e.g., the return on Europe U.S. Treasury bills, 0.04.
- t = time (in years) until the expiration date, between 1 month and four years later.

Two types of results are presented. The first type can model all computed analysis into 3D visualization. This is beneficial to the analysts and stakeholders since they can understand the percentage of profits and loss associated with changes in put price, time and volatility. The second type is to calculate the numerical values of percentage of profits or loss by providing key inputs to the Black Scholes.

The First Type of Result for Black Scholes: The result can be computed in 3D swiftly by simply typing in:

BlackScholes [p,50, 0.45, 0.05 ,t], {p, 40, 60}, {t, 0.01, 4}

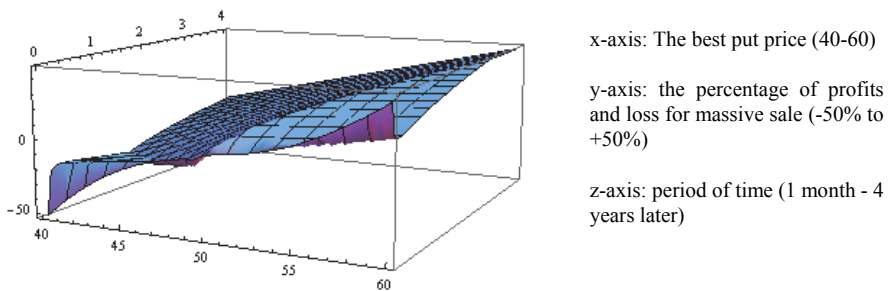


Fig. 1. The 3D risk analysis to investigate volatile percentage of profits and loss.

Fig. 1 presents results of risk modeling on the Cloud which transforms output into 3D. Fig. 1 confirms that the price of 50 is indeed a 'turning point', and profits will be made at the right time. If the selling period is getting caught with the fluctuations in the market, the loss will be made. Computation enabled by Cloud makes the modeling and analysis very easy. Risks associated with time, volatility and rapid change in the

market can be monitored, which can provide the investors and traders some insights for investment.

The Second Type of Result or Black Scholes: Inputs are the same as before, except the investor has a call price of 48.5 for a planned put price of 50. After 2 years, he/she wishes to know the percentage of profits. We can simply type in the Black Scholes command as:

BlackScholes[48.5, 50, 0.45, 0.04, 2]

and the output is equal to **8.11448** which corresponds to the value in the y-axis.

Computations and Visualization for Delta: Within Delta function, t is entered as 4, which means around 4 years will be lapsed since the crisis has started. Results will be different if it is typed in as 0, which means from now on. Again, auxiliary and Black Scholes functions are used to compute 3D Visualization swiftly. The command is **Delta[p,k,sd,r,t]** where all variables are the same as in Black Scholes. In order to get Delta RVaaS results by typing

Delta[p, 50, 0.45 0.04, t], {p, 40, 60}, {t, 0.01, 4}

The output is presented in Fig. 2. Similar to BSM command, we can also type in **Delta[48.5,50.,0.45,0.04,0.3]** to get the output and the result is **0.0483448**.

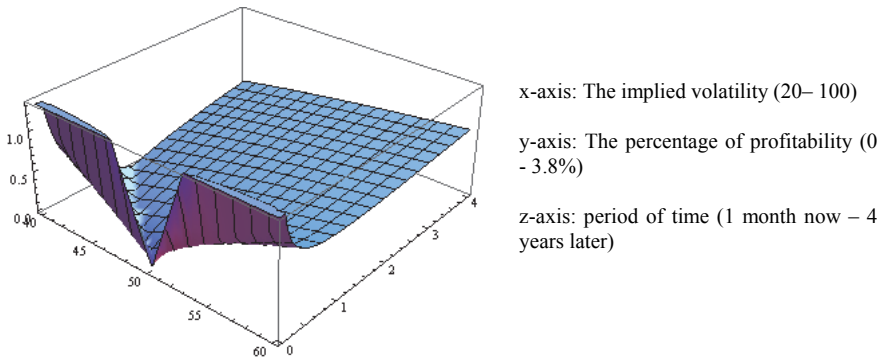


Fig. 2. The 3D risk analysis to investigate the best put price in relations to fluctuating volatility.

Computations and Visualization for Theta: Theta is another derivative calculated by financial modeling. The use of Cloud enable Theta calculations to be possible. Theta can be used to study the negative impact due to the economic crisis. The command is **Theta[p,k,sd,r,t]**. In order to get Theta RVaaS result, typing in

Theta[p, 50, 0.45 0.04, t], {p, 40, 60}, {t, 0.01, 4}

The output is presented in Fig. 2. Similar to BSM command, we can also type in **Theta[48.5,50.,0.45,0.04,0.3]** to get the output and the result is **-8.33054**.

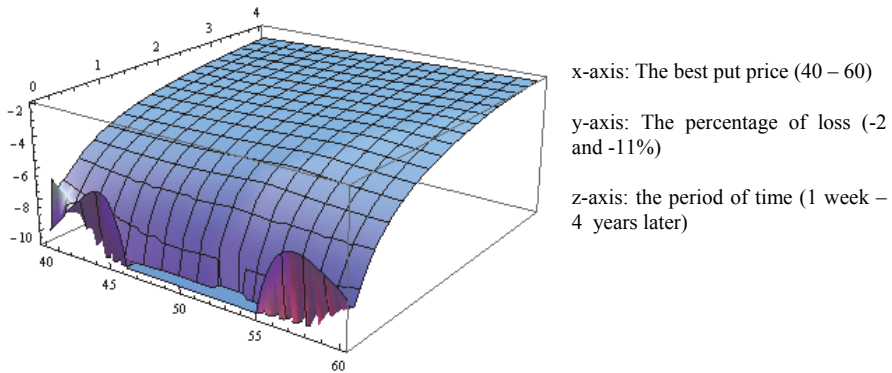


Fig. 2. The 3D risk analysis to explore the percentage of loss and the put price.

4 Experiments

This section describes the hardware set up and the results of experiments. Various simulations and experiments for RVaaS have been performed using a high specification desktop environment, private and public clouds. The desktop machine has 2.67 GHz Intel Xeon Quad Core and 4 GB of memory (800 MHz). The private cloud is used and it involves four sites in total; two in London and two in Southampton. The University of Southampton resources are used for all 3D Visualization, and are also used to connect the lead author's home cluster, Greenwich and London Data Centre. There are reliable computational connections between internal networks. The public cloud includes Amazon EC2 services which uses a large instance of Ubuntu 8.4 and 8 GB RAM.

The London Data Centre has advanced Cloud and parallel computing infrastructure and network attached storage (NAS) service. In total it has CPUs totaling 30 GHz, 60 GB of RAM and 12 TB of disk space in place. Experiments performed in this environment get the best benefit of advanced optical fiber networking. There are two servers at London Greenwich, with a total of 9 GHz CPU and 20 GB RAM. The two servers at University of Southampton both have 6.0 GHz and 16 GB RAM. For the home cluster, the total hardware capability is 24.2 GHz CPU and 32 GB RAM. Simulations and experiments on a desktop and two private clouds (one in Southampton and one in London) get the same results, and thus execution time to complete all simulation is the benchmark to differentiate their performance on different platforms.

Code written for BSM has been used for experimenting and benchmarking with some experimental Modelling of Assets (MoA) code. For example, our previous work [1] describes and explains code written for BSM which has been used for experimenting and benchmarking in the Clouds. Based on the core code algorithm, the objective is to calculate the best prices and risks, in regard to the use of American and European options. Execution time (based on the average of five results) is used as the performance benchmark. All results suggest standard deviations are kept within 0.1% to ensure a high level of accuracy. Five different sets of experiments were designed, and each set of experiments records, execution time from 50,000 to 500,000 simulations.

Using MATLAB the code can achieve up to 500,000 simulations in one go. Results for each set of experiments are recorded and shown in Fig. 3, which shows that 500,000 simulations can be completed within 22 seconds on all different platforms. BSM can achieve good execution time while maintaining a high level of accuracy. Results in RVaaS show that 500,000 simulations of undertaking BSM functions can be completed within 22 seconds.

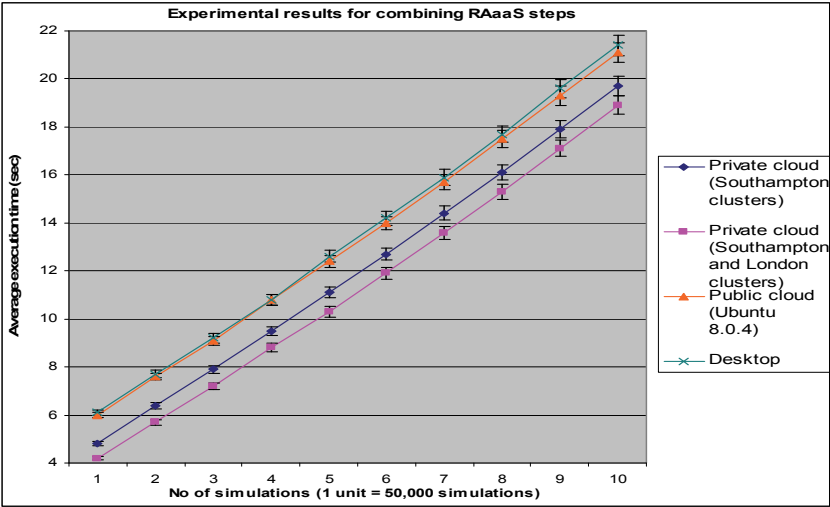


Fig. 3. Experiments of large-scale simulations (1 unit = 50,000 simulations).

5 Discussion

This section presents topics of discussions. First, the comparison with another similar Cloud such nas Python cloud. The combined Mathematica and MATLAB cloud has the advantage of using Python cloud, since 500,000 simulations of calculating risks and prices can be completed within 22 seconds. Additionally, RVaaS can present instant changes with regard to changes in the market. This allows investors to monitor changes. Second, computational results can compute risks. The contributions from RVaaS are to present numerical results in a form that allows investors (without computational background) to understand the analysis easily, so that they can make decisions quicker and better. Visualization can present a computational analysis that is appealing to investors. This area of the new study is related to Business Intelligence as a service in the Cloud (BlaaS) to simulate risk and prices in real-time and report to the investors the respective values in risks and prices of every instance in the market [2]. RVaaS offers a platform for scientists to simulate their risk, experiment with their proof-of-concepts and make it a more transparent platform than the current practice in the finance industry (which is reluctant to share about their practices).

6 Conclusion

In reply to the problems caused by the financial crisis, we propose Risk Visualization Service (RVaaS). The lack of visualization to track down the risks associated with the best put price, implied volatility, percentage of profits/loss and movement in the market mean their model is not real-time and ignoring some assumptions which are critical to reliable analysis. Using RVaaS in the Cloud permits organizations to break the constraints of the Gaussian copula and use the power of Cloud Computing to adopt more complex models and improve accuracy in risk analysis and prediction.

RVs operates in two phases:

- Calculating key derivatives such as Delta and Theta for financial modeling.
- Risk modeling in BSM, creating 3D Visualization and Analysis.

We use one real-case scenario to demonstrate our RVaaS. Results show that numerical results can be computed by typing the key variables obtained from different public sources and the targets set by the stakeholders. Risk presented in visualization form allow the potential investors and stakeholders to keep track of the status of risk with regard to time, prices and volatility. Results in experiments show that RVaaS can perform up to 500,000 simulations and complete all simulations within 22 seconds. RVaaS provides a structured way to deploy low cost, high quality risk assessment which avoids generating the unduly optimistic results which can arise from an implicit assumption in other techniques that favorable trading conditions will continue.

References

1. Chang, V., Li, C.S, De Roure, D., Wills, G., Walters, R.J., Chee, C.: The Financial Clouds Review, *International Journal of Cloud Applications and Computing*, 1 (2), (2011) 46-63.
2. Chang, V., *Business Intelligence as a Service*, *Future Generation Computer Systems*, DOI: <http://www.sciencedirect.com/science/article/pii/S0167739X13002926>, (2014).
3. *Financial Times: Lehman Brothers files for bankruptcy*, (2008).
4. *Financial Times: Interview with Lord Turner, Chair of Financial Services Authority*, in: *Financial Times*, London, (2009).
5. Hamnett, C.: *The Madness of Mortgage Lenders: Housing finance and the financial crisis*, in, King's College, London, London, UK, (2009).
6. Hull, J.C., *Options, Futures, and Other Derivatives*, Seventh Edition., Pearson, Prentice Hall, (2009).
7. Hutchinson, M.: *A Finer Formula for Assessing Risk*, in: *New York Times*, New York, (2010).
8. Miller, R. M.: *Option Valuation*, Miller Risk Advisors, Technical paper, (2010).

Citizen Intention to Adopt e-Government Services in Saudi Arabia

Sulaiman A. Alateyah¹, Victor Chang², Richard M. Crowder¹ and Gary B. Wills¹

¹Electronics and Computer Science, University of Southampton, Southampton, U.K.
{saaly10, rmc, gbw}@ecs.soton.ac.uk

²Leeds Metropolitan University, Leeds, U.K.
vic1e09@ecs.soton.ac.uk

Abstract. Although e-Government has been adopted in developed countries, it has not been widely adopted in developing countries particularly in the Arab world. This explains our motivation in identifying factors that can improve the adoption of e-Government in Saudi Arabia. While there are challenges ahead for e-Government adoption, we have identified ten factors that can influence successful delivery. These factors were defined and categorized and followed by an exploratory study to examine the importance of these factors. In order to validate our hypothesis, we used questionnaires to collect the views of three groups of Saudi citizens, and use the triangulation method to validate our results. Our statistical results show that we have very low t-test value in our one sample t-test which supports our hypothesis by identifying ten important factors for Saudi citizen adoption of e-Government services. We conclude that these ten factors can determine the successful adoption of e-Government in Saudi Arabia and meet the strategic plan set by the Saudi government in accessing what is required to increase adoption.

1 Introduction

The e-Government initiatives are recommended by the United Nations, which has a conceptual framework for E-government programmes United Nations [1]. Under their guidelines, the use of information and communication technologies (ICT) is at their centre of strategies to enable government services to be successfully delivered to the citizens of the participating UN states. The e-Government initiatives have been widely adopted, whereby the use of ICT can improve the digital connectivity and interactions between different citizens and organisations [2]. In these cases, the advancement in technology can enhance the efficiencies and collaboration between departments in the governments and ensure that services can be delivered to meet the requirements of all the stakeholders and citizens involved. This also ensures that the administrative processes and services of government can be offered by the electronic systems. Blending administrative processes and government services, the increment of the capacity and readiness of the public sector are essential in the areas of a country's technological and telecommunications infrastructure and the level of its human resources development [3].

2 Literature Review

2.1 Citizen Adoption

Yonazi et al., [4] state that developing countries can benefit from it enormously from the introduction of e-government. Based on the literature in [5], an existing challenge is how to enhance the e-government adoption and the use of their online government services. However, literature in [4] and [5] do not address e-Government adoption and the factors for successful adoption in developing countries, particularly in the Arab world [6, 7]. We undertook a comprehensive literature review as follows.

Firstly, Dong, et al. [8] explain why e-Government adoption is often not supported by the e-Government researchers, because citizens do not use online services [5]. Secondly, Carter and Belanger [9] assert that no study has identified the core factors that influence citizen adoption of e-Government initiatives, even though there are attempts to analyse user adoption of electronic commerce [10]. Thirdly, studies undertaken by Colesca [11] suggest that many studies regarding the citizen adoption of e-Government services focus on trust [12], security [13] and transparency [14] that influence e-Government adoption. Finally, research by Margetts [15], cited by Yonazi, et al. [4], indicate that improving the opportunity that e-Government might deliver benefits including social and economic to their public is based on high adoption of these initiatives.

2.2 Models Used to Measure Adoption of New Technologies

To make a fair justification for e-Government adoption, common models that used by researchers' and different contributions have been reviewed, including the Technology Adoption Model (TAM) by Davis [16], Diffusion of Innovations Model (DOI) by Rogers [17] and Unified Theory of Acceptance and Use of Technology (UTAUT) by [18]. Other researchers have developed their models based on the extended development of Davis [16] to propose factors that would encourage citizen to adopt e-Government. These models have a combination of factors which have been adopted from TAM, DOI and UTAUT include Trustworthiness by [19], model for citizen adoption by [20] and Rehman and Esichaikul [21] model of citizen adoption.

3 Discussion

Obtaining the views of prospective e-government users and experts in the field are important for the development of this research. Topics for considerations are as follows. Firstly, identify the challenges that would face the implementation and development of e-Government in Saudi Arabia. Secondly, the possible factors that would affect the citizens' intention to adopt E-government services. While addressing these two topics, key questions need to be asked and they are: (i) What are the challenges or barriers to implement and develop e-Government in Saudi Arabia?; (ii) What are the influential factors to be integrated in a model for implementing and

developing E-government in order to be adopted by the citizen? Supporting descriptions are described as follows.

3.1 Factors Influencing Citizens' Intention to Adopt e-Government Services in Saudi Arabia

There are related issues to be taken into consideration while addressing issues in this research question. The most important question is: "How can the Saudi government overcome challenges to help its citizens adopt e-Government?". In order to facilitate this, important factors are identified along with the development of answering questions in the survey. This key question to help people adopt e-Government services. All factors are presented in Table I which was based on literature reviews in 10 categories. Our next goal was to validate our hypothesis with these ten factors, so that we can demonstrate that our approach can meet the needs of Saudi citizens.

3.2 Methods to Validate This Research

Triangulation method is used to increase precision in empirical research [22] which is fully supportive to our proposal. Due to this reason, our validation technique is based on the Triangulation method. Another valid point to note regarding this approach is that according to Runeson and Höst [22], the triangulation method can offer a more comprehensive answer to address our research question. In this research, the proposed factors are validated using the triangulation method based on three key aspects which are, a detailed literature review has to be undertaken, as well as questionnaires based on these ten proposed factors need to be distributed among Saudis' citizens. Additionally, Saudi government's employees and experts will be asked to participate in the study.

4 The Exploratory Study and Its Results

4.1 Questionnaire for Saudi Citizens

Closed-ended questions were provided by us to facilitate the design of the Saudi citizens' questionnaire. The supporting reason is that closed-ended questions can find out how important the defined factors are and also how factors can influence Saudi citizens to use the e-Government services. Fourteen closed-ended questions were designed to focus on the identified factors under five categories including culture, security, privacy, trust and website design. The set of the questions are included in the appendix. The culture factor has been presented by two questions, one is about the direct effect on the citizen intention and the other is an indirect effecting on the citizens' trust. In addition, transaction security also has been presented by two questions.

4.2 About the Surveys and Results

This section describes the groups involved, the process by which the survey was undertaken and how the results associated with our study. Firstly, questionnaires with fourteen closed-ended questions were designed and distributed online to Saudi general public. Secondly, questionnaires with twenty three closed-ended questions were handed in person to the government employees. Thirdly, questionnaires with twenty nine closed-ended questions were designed for the experts' interview. Each expert was interviewed in person. The citizens' responses have been gathered using online surveys. Using the collated data, data analysis was undertaken by using SPSS and running a one-sample t-test against a set value of 3.5 and the citizens' questionnaires results are presented in Table II. Since the questionnaires have different questions and applies to different group, each set of data has been analysed separately. In this paper, only the results of the questionnaires apply to citizens are shown in table II. The data analysis and its results for the Saudi government's employees and experts are presented in previous work [23, 24].

Table 1. Factors influencing citizens to adopt e-Government services.

No	Factors	Applied to
1	Technical Infrastructure	Government employees and experts
2	Computer and Information Literacy • Age. • Gender. • Education.	
3	Lack of Awareness	
4	Security • Transaction Security. • Information Security. • Perceived Risk.	Citizen
5	Privacy	
6	Trust • Trust in Government. • Trust In Internet.	
7	Quality of Service • Service Quality. • Reliability. • Availability. • Speed of Delivery. • Information Quality.	Government employees and experts
8	Culture	Citizen
9	Diffusion Of Innovation • Compatibility. • Complexity. • Image. • Relative Advantage.	Government employees and experts
10	Website Design • Perceived Usefulness. • Perceived Ease of Use. • Multi-lingual Website • Usability. • Accessibility.	Citizen
		Government employees and experts

Table 2. The result of the one sample t-test of the questionnaires apply to Saudi citizens.

Factors	p-value	Result
Security	.005	statistically significant
Transaction Security	<.001	statistically significant
	.010	statistically significant
Information Security	<.001	statistically significant
Risk	<.001	statistically significant
Privacy	.034	statistically significant
Trust	<.001	statistically significant
Trust in Internet	<.001	statistically significant
Trust in Government	<.001	statistically significant
Culture	<.001	statistically significant
Indirect effect of Culture's on trust	0.222	statistically significant
Usefulness	<.001	statistically significant
Ease of Use	<.001	statistically significant

4.3 The Reliability of the Results

We use a reliable approach to minimize errors in measurement. In order to achieve that, we select a high confidence interval in our data analysis [25]. Reliability in this context, refers to the extent to which data analysis procedures will produce consistent results [26]. While investigating this further, the reliability value was argued by researchers. One research group [25] stated that the reliability value of 0.7 to 0.8 is an acceptable value for Cronbach's alpha (α). However, Liu and Arnett [27] explained that as a "rule of thumb" 0.6 could be accepted. Other approaches such as the use of a framework to improve the quality and reliability can also be used [28].

After the analysis of survey results, an assessment of the reliability was required and Cronbach's alpha was used to undertake the test. The result confirms that Cronbach's alpha had an acceptable outcome, with α being equal to 0.618. This means that the reliability coefficient for the questionnaire's result could be seen as adequate.

5 Conclusion

This paper presents an e-Government approach that addresses the needs of Saudi

Arabian citizens. We explain the importance of our Saudi e-Government initiative to meet the requirements of the Saudi government and the general public. We have undertaken studies to demonstrate that there are ten factors that can improve the e-Government adoption in Saudi Arabia. These factors have been defined and categorized followed by an exploratory study to examine the importance of these factors. In order to validate our hypothesis, we set questionnaires for three groups of Saudi citizens: general public; government employees and experts. We use the triangulation method to validate our results. Our statistical results show that we have very low t-test value in our one sample t-test which supports our hypothesis by identifying ten important factors for Saudi citizen adoption of e-Government services. We conclude that these ten factors can determine the e-Government adoption in Saudi Arabia and meet strategic plan set by the Saudi government in accessing what is required to increase the popularity in adoption. Results from our proposed approach can offer benefits to Saudi citizens. There are other challenges such as privacy, security, trust, culture, computer and information literacy, and IT infrastructure to be resolved.

Acknowledgement

The authors acknowledge the award of a King Abdullah scholarship to Sulaiman Alateyah to allow this research to be undertaken.

References

1. United Nations The united nations e-government development database. Available at: <http://www2.unpan.org/egovkb/about/index.htm>, Access date (05/07), 2010.
2. Al-Sobhi, F., Weerakkody, V., and Kamal, M. M., "An exploratory study on the role of intermediaries in delivering public services in madinah city: Case of saudi arabia," *Transforming Government: People, Process and Policy*, vol. 4, 2010, pp. 14-36.
3. United Nations "United nations e-government survey : Leveraging e-government at a time of financial and economic crisis," New York 2010 2010.
4. Yonazi, J., Sol, H., and Boonstra, A., "Exploring issues underlying citizen adoption of e-government initiatives in developing countries: The case of tanzania.," *Electronic Journal of e-Government*, vol. 8, Dec 2010, pp. 176-188.
5. Warkentin, M., Gefen, D., Pavlou, P. A., and Rose, G. M., "Encouraging citizen adoption of e-government by building trust," *Electronic Markets*, vol. 12, 2002, pp. 157-162.
6. AlShihi, H., "E-government development and adoption dilemma: Oman case study," in *The 6th International We-B (Working for eBusiness) Conference*, Victoria University, Melbourne, Australia 2005.
7. AlAwadhi, S. and Morris, A., "The use of the utaut model in the adoption of e-government services in kuwait," presented at the *Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, 2008.
8. Dong, X., Xiong, L., and Wang, W., "How adoption is g2c model e-government? — evidence from xi' an and nan jing," in *E -Business and E -Government (ICEE), 2011 International Conference on*, 2011, pp. 1-4.
9. Carter, L. and Belanger, F., "Citizen adoption of electronic government initiatives," in

System Sciences 2004. , Proceedings of the 37th Annual Hawaii International Conference, 2004, p. 10

10. Gefen, D., Karahanna, E., and Straub, D. W., "Trust and tam in online shopping: An integrated model," *MIS Quarterly*, vol. 27, 2003, pp. 51-90.
11. Colesca, S. E., "Increasing e-trust: A solution to minimize risk in e-government adoption," *JOURNAL OF APPLIED QUANTITATIVE METHODS*, vol. 4, 2009, pp. 31-44.
12. Srivastava, S. C. and Teo, T. S. H., "Citizen trust development for e-government adoption: Case of singapore," in "Proceedings of Pacific Asia Conference on Information Systems, 2005, pp. 721-724.
13. Colesca, S., "The main factors of on-line trust," *Economia. Seria Management*, vol. 10, 2007, pp. 27-37.
14. Marche, S. and McNiven, J. D., "E-government and e-governance: The future isn't what it used to be," *Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration*, vol. 20, 2003, pp. 74-86.
15. Margetts, H., "E-government in britain—a decade on," *Parliamentary Affairs*, vol. 59, 2006, pp. 250-265.
16. Davis, F. D., "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, 1989, pp. 319-340.
17. Rogers, E. M., *Diffusion of innovations*, 4th ed. New York: Free Press, 1995.
18. Venkatesh, V., Morris, M. G., Gordon, B. D., and Davis, F. D., "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, 2003, pp. 425-478.
19. Belanger, F., Hiller, J. S., and Smith, W. J., "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, vol. 11, 2002, pp. 245-270.
20. AlNuaimi, M., Shaalan, K., Alnuaimi, M., and Alnuaimi, K., "Barriers to electronic government citizens' adoption: A case of municipal sector in the emirate of abu dhabi," in *Developments in E-systems Engineering (DeSE)*, 2011, 2011, pp. 398-403.
21. Rehman, M. and Esichaikul, V., "Factors influencing the adoption of e-government in pakistan," in *E -Business and E -Government (ICEE)*, 2011 International Conference on, 2011, pp. 1-4.
22. Runeson, P. and Höst, M., "Guidelines for conducting and reporting case study research in software engineering," *Empirical Software Engineering*, vol. 14, 2009, pp. 131-164.
23. Alateyah, S., Crowder, R. M., and Wills, G. B., "An exploratory study of proposed factors to adopt e-government services," *International Journal of Advanced Computer Science and Applications*, vol. 4, 2013,
24. Alateyah, S. A., Crowder, R. M., and Wills, G. B., "Factors influencing citizen intention to adopt e-government in saudi arabia," in *Information Society (i-Society)*, 2013 International Conference on, 2013, pp. 250-255.
25. Field, A., *Discovering statistics using spss*: Sage Publications Limited, 2009.
26. Saunders, M. N. K., Lewis, P., and Thornhill, A., *Research methods for business students*, 5TH ed.: Pearson, 2009.
27. Liu, C. and Arnett, K. P., "Exploring the factors associated with web site success in the context of electronic commerce," *Information & Management*, vol. 38, 2000, pp. 23-33.
28. Chang, V., Walters, R. J., and Wills, G., "The development that leads to the cloud computing business framework," *International Journal of Information Management*, vol. 33, 2013, pp. 524-538.

Appendix

The List of the Questions That Applies to the Citizens' Questionnaires

1. Culture in general does influence citizens to use E-government services.
2. Culture can affect the trust of citizens who intend to use E-government services.
3. Sending information via network medium (e.g. Internet) is safe, which encourages me to use E-government services.
4. Providing critical information to E-government websites can be risky, which prevents me from using the E-services.
5. The transaction between E-government services and me is secure and influences my intention to use the online services.
6. The low level of the transaction security which might cause Losing information, encouraging me to use the paper-based system.
7. General security about my information, which I am concerned about, affects my intention to use E-government services.
8. Privacy is a critical issue that citizens are afraid of when they intend to use E-government services.
9. Trust in general is an important factor that influences citizens to adopt E-government services.
10. Trust in Internet does not affect the intention of citizens to use E-government services.
11. Trust in government has an impact on the intention of citizens to use E-government services.
12. The design of a government's website increases my intention to use the E-government Services.
13. Whenever the usefulness of a website is clear and easily perceived by me, I use the E-government services.
14. A website's perceived ease of use influences me to use the E-government services.

Performance Evaluation of Multi-Core Multi-Cluster Architecture (MCMCA)

Norhazlina Hamid, Robert J. Walters and Gary B. Wills

School of Electronics & Computer Science, University of Southampton,
SO17 1BJ, Southampton, U.K.
{nh3g11, rjw1, gbw}@ecs.soton.ac.uk

Abstract. A multi-core cluster is a cluster composed of numbers of nodes where each node has a number of processors, each with more than one core within each single chip. Cluster nodes are connected via an interconnection network. Multi-cored processors are able to achieve higher performance without driving up power consumption and heat, which is the main concern in a single-core processor. A general problem in the network arises from the fact that multiple messages can be in transit at the same time on the same network links. This paper considers the communication latencies of a multi-core multi-cluster architecture will be investigated using simulation experiments and measurements under various working conditions.

1 Introduction

In the past, it was a trend to increase a processor's speed to get better performance. Moore's Law, which states that the number of transistors on a processor will double approximately every two years has been proven to be consistent due to the transistors getting smaller in successive processor technologies [1]. However, reducing the transistor size and increasing clock speeds causes transistors to consume more power and generate more heat [2]. These concerns limit cost-effective increases in performance which can be achieved by raising processor speed alone. These issues gave computer engineers the idea of designing the multi-core processor, a single processor with two or more cores [3].

Multi-core processors are used extensively in parallel and cluster computing. As far back as 2009, more than 95% of the systems listed in the Top 500 supercomputer list used dual-core or quad-core processors [4]. The motivation in this realm is the advances in multi-core processor technology that makes them an excellent choice to use in cluster architecture [5]. From the combination of cluster computing and multi-core processor, the multi-core cluster architecture has emerged. The multi-core cluster architecture becomes more powerful due to the combination of faster processors and faster interconnection [6].

Overall performance of multi-core cluster always determined by the efficiency of its communication and interconnection networks [7]. Hence, performance analysis of the interconnection networks is vital. A general problem in the network may arise

from multiple messages being in transmission at once on the same network links and this will cause delays. Such delays increase the communication latency of the interconnection network and it is therefore important to minimise this. A high communication latency of interconnection network can dramatically reduce the efficiency of the cluster system [8].

Many studies [9-11] have been carried out to improve the performance of multi-core cluster but few clearly distinguish the key issue of the performance of interconnection networks. Although the cluster interconnection network is critical for delivering efficient performance, as it needs to handle the networking requirements of each processor core [8], existing models do not address the potential performance issues of the interconnection networks within multi-core clusters.

Scalability is a very important aspect to examine when evaluating clusters. Abdelgadir, Pathan, & Ahmed [12] find that having good network bandwidth and faster network will produce better scalability of clusters. Scaling up by adding more processors to each node to increase the processing power creates too much heat [3]. The conventional approach to improving cluster throughput is to add more processors but there is a limit to the scalability of this approach; the infrastructure cannot provide effective memory access to unlimited numbers of processors and the interconnection network(s) become saturated [13]. Technological advances have made it viable to overcome these problems by combining multiple clusters of heterogeneous networked resources into what is known as a multi-cluster architecture [14].

We describe a scalable approach to building heterogeneous multi-cluster architecture and are the first investigation into network latency within such architecture.

2 The Architecture

Multi-core processor is a single processor within a chip with two or more cores [3]. Multi-core processors are the answer for the deficiencies of single-core processors; as processor speed increase, the amount of heat produced and the amount of power consume by the processor increase with it. Multi-core processors can perform more work within a given amount of time by dividing the work between two or more cores while reduce the power consumption and dissipate the heat [15]. Due to their greater computing power and cost-to-performance effectiveness, cluster computing uses multi-core processors extensively [16].

A multi-core cluster is a cluster where all the nodes in the cluster have multi-core processors. In addition, each node may have multiple processors (each of which contains multiple cores). With such cluster nodes, the processors in the node share both memory and their connections to the outside. A new architecture known as the Multi-Core Multi-Cluster Architecture (MCMCA) is introduced in **Fig. 1**. The structure of MCMCA is derived from a Multi-Stage Clustering System (MSCS) [13] which is based on a basic cluster using single-core nodes. The MCMCA is built up of numbers of clusters where each cluster is composed of numbers of nodes. The numbers of nodes are determined at run time. Each node of a multi-core cluster has more than one processor. Cores on the same chip share local memory but have their own L2 cache. The interconnection network connects the cluster nodes.

Multi-Core Multi-cluster Architecture (MCMCA)

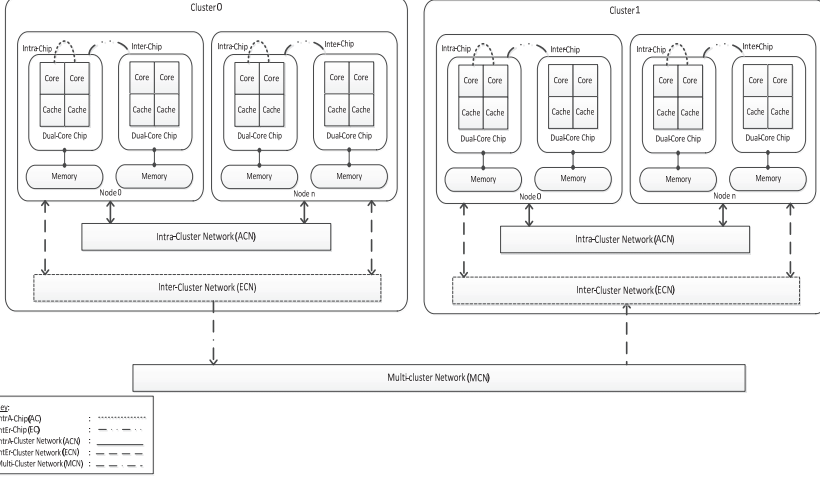


Fig. 1. Overview of the proposed Multi-Core Multi-Cluster Architecture (MCMCA).

3 Communication Network

The performance of a cluster system depends on its communication latency of the interconnection network. The research conjecture is that low communication latency is essential to achieving a faster network and increasing the efficiency of a cluster. In order to understand the communication network of the Multi-Core Multi-Cluster Architecture (MCMCA), this section explains in detail the different types of communication networks.

There are five communication networks in MCMCA. Three of them are commonly found in any multi-core cluster architecture, these are: the intra-chip communication network (AC); the inter-chip communication network (EC) and the intra-cluster network (ACN). The new communication networks introduced in this paper are the intercluster network (ECN) and the multi-cluster network (MCN).

The communication between two processor cores on the same chip is the intra-chip communication network (AC), as shown in **Fig. 2**. Messages from source A to destination B travel via the AC communication network, which acts as a connector between two processor cores on the same chip.

Fig. 3 shows an inter-chip communication network (EC) for communicating across processors in different chips but within a node. Messages travelling to different chips from source A in the same node first have to communicate within the chip via the intra-chip communication network (AC), and then travel between the chips via the EC network to reach their destination B. Each node has two communication connections which are intra-cluster network (ACN) for transmission within a cluster and inter-cluster network (ECN) for transmission between clusters.

An intra-cluster network (ACN) is used for messages within a cluster. In order for messages to cross the nodes, messages have to communicate with the intra-chip

communication network (AC) and the inter-chip communication network (EC) to pass between chips. Then messages travel via the ACN to enter different nodes to reach their destination, as shown in **Fig. 4**.

Messages travelling from source A to destination B between clusters communicate via two communication networks to reach other clusters, as shown in **Fig. 5**. An inter-cluster network (ECN) is used to transmit messages between clusters. The clusters are connected to each other via the multi cluster network (MCN). When the messages reach the other cluster, they have to communicate with the ECN of the target cluster before arriving at their destination.

All levels of communication are critical in order to optimise the overall performance of the Multi-Core Multi-Cluster Architecture (MCMCA). The overall communication latency gathered from all communication networks will be calculated. The derived simulation results will be analysed for comparison between the existing architecture and the MCMCA architecture.

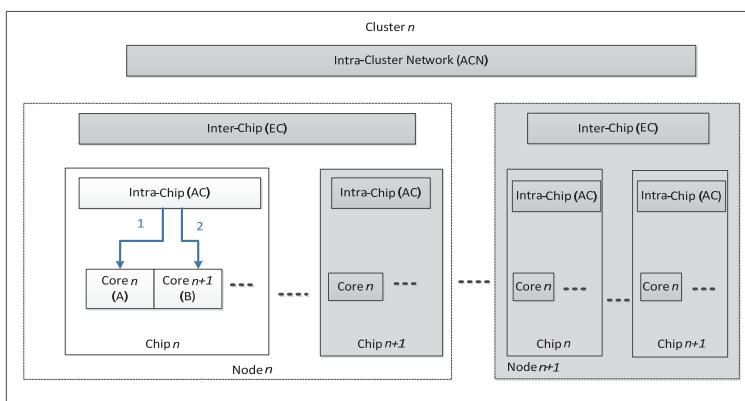


Fig. 2. Communication network flow A for message passing between two processor cores on the same chip.

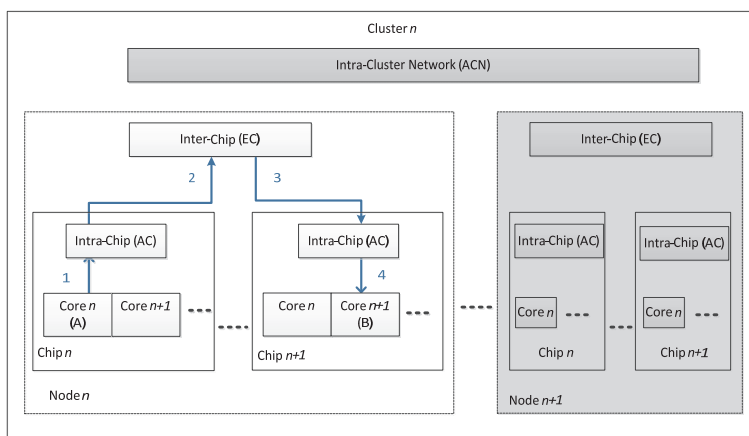


Fig. 3. Communication network flow B for message passing across processors in different chips but within a node.

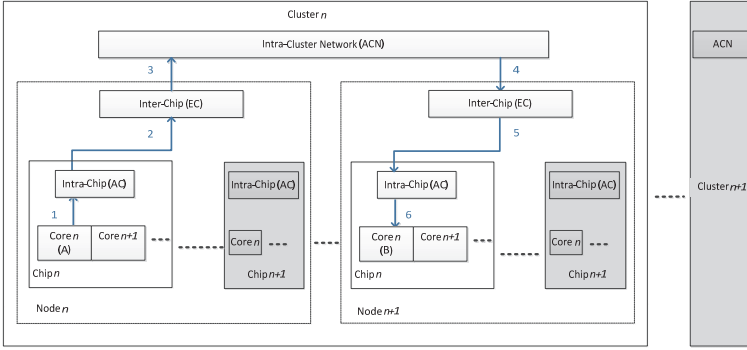


Fig. 4. Communication network flow C for message passing between processors on different nodes but within the same cluster.

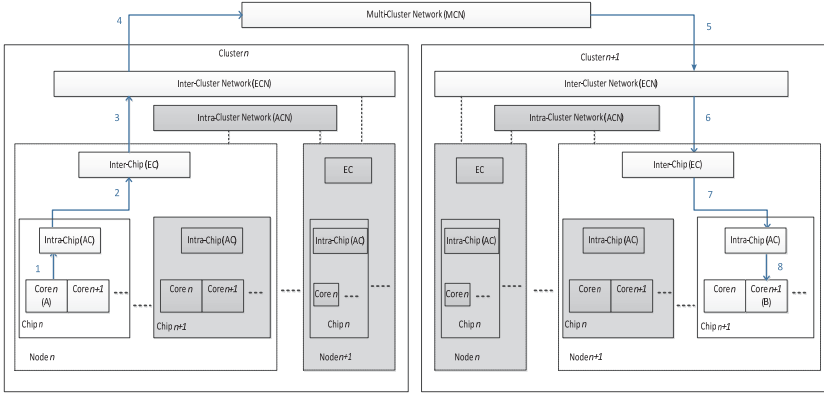


Fig. 5. Communication network flow D for transmitting messages between clusters.

4 Research Methodology

This work will use computer simulation to model the architecture. The model will be validated using computer simulation experiments.

4.1 Simulation Tool

OMNeT++ network simulation tool [17], a C++ based open-source discrete-event simulator has been chosen to model MCMCA. Comparison studies of network simulators have been conducted which involved OMNeT++, MATLAB, ns-2, ns-3, OPNet and QualNet [18-21]. NS-2 is still the most widely used network simulator in academia, but OMNeT++ provides more infrastructures. OMNeT++ is also popular in academia and industry because of its extensibility since it is also open source. There is also plentiful online documentation and mailing lists for general discussion. Although NS-3 demonstrated the best overall performance, NS-3 still needs to improve

its simulation credibility [19] and OMNeT++ can be considered as a viable alternative. OPNet has similar foundations to OMNeT++ although it is a commercial product, and contains an extensive model library and provides several additional programs and GUI tools. The other two commercial products are QualNet, which emphasises wireless simulations, and MATLAB, which needs several prerequisite components for its files to function normally.

4.2 Simulation Development

An early stage of simulation experiments under various configurations and design parameters has been completed. The performance evaluation focused on communication latency in the MCMCA architecture. As a preliminary study, the communication network performance experiments are based on a single-core multi-cluster architecture. A simulation model has been built to measure the performance of single-core multi-cluster architecture. This evaluation was then compared to the model of multi-cluster architecture presented by Javadi et al., [22] with the given configuration and parameters to match the work in their papers.

This work focuses on measuring steady-state performance of a network; the performance of a network with a stationary traffic source after it has reached steadiness. A network has reached steadiness when its average queue lengths have reached their steady-state values. To measure steady-state performance, the simulation experiments were conducted in three phases: warm-up, measurement and drain [7]. The network has necessarily reached a steady-state once the network is warmed up [22]. This means that the statistics of the network are stationary and no longer changing with time, which will determine an accurate estimation.

4.3 Simulation Setup

The model behaviour built into each Network Description (NED) file will be captured in C++ files as code and can be edited in the Integrated Development Environment [23]. Each NED file has its own C++ simple module source. Unlike many formats of deterministic discrete event simulation, the model is built at run-time to form a topology that represents the geometric structure and the communication links between the modules. At the start of each execution, the simulator reads the initialisation file (.INI file) that tells the tool which network file is to be simulated. In this initialisation file the parameters of the model, such as number of cores per node, number of clusters, number of messages to be generated, message length (M), flit length (F) and inter-arrival time, are specified. The simulation can also behave with different initialisation inputs and all the values can be stored in an .INI file, usually called omnetpp.ini, containing settings that control how the simulation is executed.

When the simulation is started, it will show how the messages hop from module to module following the routing algorithm. Each message will be partitioned into a sequence of packets first before being generated at each tree-node, following the assumptions that the message destinations are uniformly distributed by using a uniform random number generator. Packets travelling from source to its destination will ac-

cess the available processor through a chip first, where a chip can contain one or more processors. Then, each processor will divide the packets into the number of cores. If first processor is busy, it will pass the packets to another processor in the same chip within the same node first, before determining via the communication network if other processors in other chips can process the packets. Packets will access the processors, chips and nodes in the same cluster first before accessing other clusters via communication network.

The routing file will determine the path the packets will follow in the network from the source to the destination. Based on the path given, the packets will travel using communication switch to get through the communication network. If there is a situation where more than one packet needs to use the same route, the communication switch will determine which packet can go through first or if the packet needs to queue (buffer) until the route is available. Each packet is time-stamped after its generation and the message completion time is defined on each tree-node to compute message latency. Statistics will be gathered for every event in the simulation for analysis of the results.

5 Results and Discussion

A number of examples of the simulation of the single-core multi-cluster model have been examined to establish its performance under various workload conditions. The first case was performed for an 8-single-core cluster system with message length (M) = 32 flits, flit length (F) = 256 bytes and 512 bytes. The second case was performed with the same 8-single-core cluster system and the same flit length (F) = 256 bytes and 512 bytes but with longer message length (M) = 64 flits. The X axis denotes the traffic rate, while the Y axis indicates the communication latency.

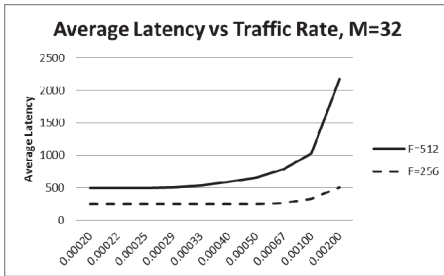


Fig. 6. Average latency of 8-cluster system with $M=32$ flits, $F=256$ bytes and 512 bytes.

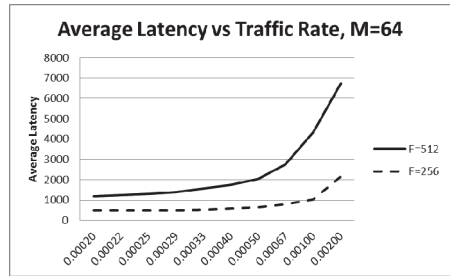


Fig. 7. Average latency of 8-cluster system with $M=64$ flits, $F=256$ bytes and 512 bytes.

Simulation experiments have revealed that the results obtained from the single-core multi-cluster architecture closely match the results from the model of multi-cluster architecture presented by Javadi et al. [22], when compared. The results have shown that as the traffic rate increases, the average communication latency increases following the assumptions that the messages are delayed by having to wait for resources before traversing into a network. At low traffic rates, latency will approach

zero-load latency. The results confirm that the simulation model is a good basis to measure the communication latency for a large-scale cluster, and can be extended to multi-core multi-cluster architecture.

6 Conclusion and Future Work

This paper has presented architecture for measuring the performance of communication networks in Multi-Core Multi-Cluster Architecture (MCMCA). Preliminary stage of the research involved the development of the single-core multi-cluster simulation model. Simulation experiments have been conducted to evaluate the single-core multi-cluster and baseline results were produced. Simulation results demonstrated that the simulation model is a good basis to measure the communication latency for a large-scale cluster, and can be extended to MCMCA.

Our future work will be developing a simulation model for MCMCA. Experiments will be run in simulation to investigate the model's performance under various configurations. This will provide communication network performance results for comparisons to be made between the model of the MCMCA and models of existing cluster architectures [15, 22]. The simulation will measure communication latency of a cluster when applying multi-core processor technology, under a multi-cluster architecture environment. The approach taken and accuracy of the simulation outcome will make it a good reference for predicting the performance behaviour of MCMCA.

References

1. Intel. (1997, Moore's Law and Intel Innovation. Available: <http://www.intel.com/about/companyinfo/museum/exhibits/moore.htm?wapkw=moore+laws>
2. D. Geer, "For Programmers, Multicore Chips Mean Multiple Challenges," *Computer*, vol. 40, pp. 17-19, 2007.
3. T. W. Burger, "Intel Multi-Core Processors: Quick Reference Guide," 2005.
4. Admin. (2009, TOP500 Highlights - November 2009. Available: <http://www.top500.org/lists/2009/11/highlights>
5. M. Soryani, M. Analoui, and G. Zarrinchian, "Improving inter-node communications in multi-core clusters using a contention-free process mapping algorithm," *The Journal of Supercomputing*, pp. 1-26, 2013/04/10 2013.
6. E. W. Bethel and M. Howison, "Multi-core and many-core shared-memory parallel raycasting volume rendering optimization and tuning," *International Journal of High Performance Computing Applications*, vol. 26, pp. 399-412, November 1, 2012 2012.
7. W. J. Dally and B. P. Towles, *Principles and Practices of Interconnection Network*: Morgan Kaufmann, 2004.
8. G. Shainer, P. Lui, M. Hilgeman, J. Layton, C. Stevens, W. Stemple, et al., "Maximizing Application Performance in a Multi-core, NUMA-Aware Compute Cluster by Multi-level Tuning," in *Supercomputing*. vol. 7905, J. Kunkel, T. Ludwig, and H. Meuer, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 226-238.
9. S. Ichikawa and S. Takagi, "Estimating the Optimal Configuration of a Multi-Core Cluster: A Preliminary Study," in *Complex, Intelligent and Software Intensive Systems*, 2009. CISIS '09. International Conference on, 2009, pp. 1245-1251.

10. C. Lei, A. Hartono, and D. K. Panda, "Designing High Performance and Scalable MPI Intra-node Communication Support for Clusters," in *Cluster Computing*, 2006 IEEE International Conference on, 2006, pp. 1-10.
11. A. Ranadive, M. Kesavan, A. Gavrilovska, and K. Schwan, "Performance implications of virtualizing multicore cluster machines," presented at the Proceedings of the 2nd workshop on System-level virtualization for high performance computing, Glasgow, Scotland, 2008.
12. A. T. Abdelgadir, A.-S. K. Pathan, and M. Ahmed, "On the Performance of MPI-OpenMP on a 12 nodes Multi-core Cluster," in *Algorithms and Architectures for Parallel Processing*, ed: Springer, 2011, pp. 225-234.
13. H. S. Shahhoseini, M. Naderi, and R. Buyya, "Shared memory multistage clustering structure, an efficient structure for massively parallel processing systems," in *High Performance Computing in the Asia-Pacific Region*, 2000. Proceedings. The Fourth International Conference/Exhibition on, 2000, pp. 22-27 vol.1.
14. J. H. Abawajy and S. P. Dandamudi, "Parallel job scheduling on multicluster computing system," in *Cluster Computing*, 2003. Proceedings. 2003 IEEE International Conference on, 2003, pp. 11-18.
15. C. Lei, G. Qi, and D. K. Panda, "Understanding the Impact of Multi-Core Architecture in Cluster Computing: A Case Study with Intel Dual-Core System," in *Cluster Computing and the Grid*, 2007. CCGRID 2007. Seventh IEEE International Symposium on, 2007, pp. 471-478.
16. L. Chai, "High Performance and Scalable MPI Intra-node Communication Middleware for Multi-core Clusters," PhD, Graduate School of The Ohio State University, The Ohio State University, 2009.
17. A. Varga. (2001). OMNeT++.
18. A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," presented at the Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems \& workshops, Marseille, France, 2008.
19. E. Weingartner, H. vom Lehn, and K. Wehrle, "A Performance Comparison of Recent Network Simulators," in *Communications*, 2009. ICC '09. IEEE International Conference on, 2009, pp. 1-5.
20. S. Mehta, N. Sulatan, and K. S. Kwak, "Network and System Simulation Tools for Next Generation Networks: a Case Study, Modelling, Simulation and Identification," in *Modelling, Simulation and Identification*, A. M. (Ed.), Ed., ed InTech, 2010.
21. J. Pan, "A Survey of Network Simulation Tools : Current Status and Future Developments," pp. 1-13, 2008.
22. B. Javadi, M. K. Akbari, and J. H. Abawajy, "A performance model for analysis of heterogeneous multi-cluster systems," *Parallel Computing*, vol. 32, pp. 831-851, 2006.
23. A. Varga. (2011, OMNeT ++ User Manual Version 4.2.2. Available: <http://www.omnetpp.org/doc/omnetpp/Manual.pdf>

A View at Desktop Clouds

Abdulelah Alwabel, Robert Walters and Gary Wills

Electronics and Computer Science School, University of Southampton, Southampton, U.K.
{aala10, gbw, rjwl}@ecs.soton.ac.uk

Abstract. Cloud has emerged as a new computing paradigm that promises to move into computing-as-utility era. Desktop Cloud is a new type of Cloud computing. It merges two computing models: Cloud computing and volunteer computing. The aim of Desktop Cloud is to provide Cloud services out of infrastructure that is not made for this purpose in order to reduce running and maintenance costs. This paper discusses this new type of Cloud by comparing it with current Cloud and Desktop Grid models. It, also, presents several research challenges in Desktop Cloud that require further attention.

1 Introduction

Desktop Clouds represent a new direction of providing Cloud services based on non-dedicated resources. The resources can be any form of computing devices such as PCs, laptops ...etc. The new type attempts to combine two computing models, namely Cloud computing and Volunteer computing in order to form a Cloud that provides services for less or no cost. Throughout this paper, Traditional Cloud (TC) refers to a Cloud that relies on dedicated resources to provide services, whereas Desktop Cloud (DC) refers to a Cloud that relies on non-dedicated resources. Amazon Cloud, for instance, is a Traditional Cloud.

The remaining of this paper is organised as follows. First, the paper starts by giving an overview about the meaning of Desktop Clouds. In addition, the advantages of Desktop Clouds are presented. A brief comparison study between Desktop Clouds, Traditional Clouds and Desktop Grids is presented in order to study similarities and differences. Finally, the paper finishes by discussing research issues in Desktop Cloud.

2 Desktop Clouds

The success of Desktop Grids motivates the idea of harnessing idle resources to build Desktop Clouds. Hence, the term Desktop comes from Desktop Grids because both of Desktop Clouds and Desktop Grids are based on Desktop PCs and laptops etc. Similarly, the term Cloud comes from Cloud as Desktop Cloud aims to provide services based on the Cloud business model. Several synonyms for Desktop Cloud have been

used, such as Ad-hoc Cloud, Volunteer Clouds and Non-Dedicated Clouds. The literature shows that very little work has been undertaken in this direction.

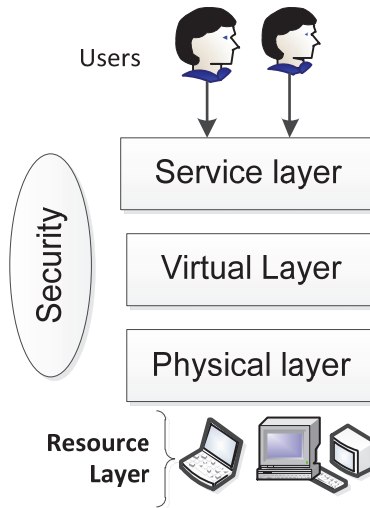


Fig. 1. Architecture of desktop clouds.

The overview architecture of Desktop Clouds is depicted in fig. 1. The architecture is consisted of several layers. The users contact the service layer in order to submit their demands. The physical layer is responsible of managing physical nodes that are aggregated the resource layer. The virtual layer plays a curtail role in terms of isolating Clients request from the physical nodes via virtualisation. Users are assigned virtual machines that are located in physical machines. Physical machines can be connected by LAN or WLAN.

Ad-hoc Cloud is the idea of harvesting distributed resources within an organisation to form a Cloud [1]. Nebula [2, 3] is a project aiming to exploit distributed resources in order to create a volunteer Cloud which offers services free of charge. Cloud@home [4, 5] is a project representing the @home philosophy in Cloud computing. The goal of Cloud@home is to form a new model of Cloud computing contributed to by individual users over the Internet. In addition to that, Cern¹ has announced an initiative to move their Desktop Grid project, which is called LHC@home, toward the Cloud [6]. It is suggested that non-dedicated resources can be exploited by Cloud providers in case their local infrastructure cannot meet requests by consumers at peak times [7].

2.1 Scenario

Suppose a group of universities wishes to benefit from its computing resources to form a Cloud. The resources range from PCs to servers etc, each of them is called a

¹ the European Organization for Nuclear Research

Cloud node. A node can join the Cloud when it becomes idle. This scenario is motivated by Condor [8]. Users in Desktop Cloud submit their request to acquire services with requirements as it is stated in the service level agreement between a client and the Cloud interface. The requests are processed in the virtualisation layer on top of Cloud physical nodes. The virtualisation isolates the guest operating system from the host physical machine. The isolation improves security and prevents unauthorised access between two parties.

Another scenario that can be considered is a universal Desktop Cloud which allows people to contribute their own computing resources to be used by Cloud clients [9]. This example can be considered as public Desktop Cloud. The people are asked to contribute their machines in order to form a Desktop Cloud. People can be stimulated to participate in DC to serve science within research communities.

Table 1. Desktop Cloud vs. Traditional Cloud.

Feature	Desktop Cloud	Traditional Cloud
Elasticity	√	√
Virtualisation	√	√
Idle Resources	√	X
Ease of Use	√	√

3 Desktop Clouds vs. Traditional Clouds

This section clarifies Desktop Clouds further by comparing them with related areas: Traditional Clouds, Grids and Desktop Grids. There are basic differences between Desktop Cloud and Traditional Clouds as it is shown in Table 1. Elasticity means that a consumer can acquire computing services. Then the user can scale up or down according to their needs. Both Traditional Cloud and Desktop Cloud rely heavily on virtualisation. The ease of use principle means that users can use a specific service without making a lot of changes to their work. Both Traditional Clouds and Desktop Clouds let their users harness services without making significant changes to their code. However, there are several differences between Desktop and Traditional Clouds. Firstly, the infrastructure of DC is made of resources that are non-dedicated, i.e. not dedicated to be part of Cloud infrastructure. In the contrary, the infrastructure of TC is made of a huge number of dedicated computing resources. Secondly, the resources in DC are highly distributed across the globe, whereas they are limited in TC to several locations in data centres. Furthermore, nodes in DC are highly volatile due to the fact that they can be down unexpectedly without prior notice. Resource high volatility has negative impact on availability and performance [10]. Although, resources in both TC and DC are heterogeneous, they are even more heterogeneous and dispersed in DC. Virtualisation plays a key role in Desktop Clouds which makes it different from other large scale systems.

Desktop Clouds have some advantages over Traditional Clouds. Firstly, Traditional Clouds have a negative impact on the environment since their data centres consume massive amounts of electricity [11]. The second advantage is cost effectiveness of Desktop Clouds for both Cloud services providers and their consumers. For

service provider, there is no need to build new data centres to meet the increasing demands of the future. Consumers will get their services at lower prices, if not free compared to Traditional Clouds. Also, Desktop Cloud helps in reducing energy consumption since it utilises already-running undedicated resources which would otherwise remain idle. Some studies show that the average percentage of local resources being idle within an organisation is about 80% [12]. Furthermore, Traditional Clouds are formed from a limited number of data centres located around the globe. Therefore, they are inefficient in terms of data mobility and pay little attention to the location of clients [3]. Finally, Traditional Clouds are centralised, which leads to the potential that there could be a single point of failure issue if a Cloud service provider goes out of the business. In contrast, Desktop Clouds manage and offer services in a decentralised manner.

Table 2. Desktop Cloud vs. Traditional Cloud.

Feature	Desktop Cloud	Desktop Grid
Elasticity	√	X
Virtualisation	√	X
Idle Resources	√	√
Ease of Use	√	X

4 Desktop Cloud vs. Desktop Grid

Desktop Clouds can be confused with other distributed systems, especially Desktop Grids. Table 2 shows a comparison between DC and Desktop Grid. Both Desktop Clouds and desktop Grids serve the same goal that is exploiting idle computing resources denoted by the public. However, Desktop Grid cannot offer services to clients in elasticity way as in Desktop Clouds. Elasticity means that users can require more computing resources in short term. Users, in Desktop Grids, are expected to know in-depth details about the middleware used in order to be able to harness the offered services [13]. Desktop Grids do not employ virtualisation to isolate users from the actual machines. People who wish to contribute their computing machines need to install a specific software in order to join a Desktop Grid.

5 Research Challenges

This section discusses several research issues that need further attention. Some of these challenges are inherited from Cloud computing while others are driven by the nature of used resources being highly volatile.

5.1 Security

Security is one of the major concerns that prevent organisations from moving to the cloud [14]. Ristenpart et al. show that an attacker can uncover the actual location of a

particular virtual machine (VM) [15]. Then, a cross-VM side channel attack can reveal critical information about the targeted VM by placing a malicious VM on the same physical machine.

More worries arise in DCs where both consumers and contributors are from the public. Therefore, security can be a major issue in this context. In addition to the previous threats presented in the cloud, both consumers and contributors take on risk themselves when they join a DC. A contributor can put his own data at risk by allowing access to a virtual image located in his machine. Likewise, consumers are vulnerable to malicious contributors. Nodes in DC are more likely to be vulnerable to outside attacks due to weaknesses in local antivirus software and firewalls.

Virtualisation can be vital in order to isolate the host completely from guest operating systems and, thus, prevent any unwanted access from either party. Trust mechanisms can be employed in this matter. For example, a DC can maintain a behaviour table which contains information about both consumers and contributors. The table can be used to decide which parties are trustworthy enough to join the cloud. Furthermore, VCCs should rely on autonomous mechanisms such as sandbox or certification in order to prevent various attacks from participants [16].

5.2 Resource Management

Resources in volunteer clouds are highly heterogeneous, therefore, managing them can be considered problematic. Virtualisation plays a key role in Desktop Clouds because it virtualises contributed resources and delivers them to users as VMs. DCs face a challenge of developing a resource allocation mechanism that is able to: a) manage non-dedicated, heterogeneous resources, b) deliver a virtualized machine to upper level in DCs and c) work closely with users' tasks in order to find most suitable nodes for each request.

It has been pointed out that lacking central management in DCs cause a major issue in terms of reliability and state maintenance in case of failures [17]. The infrastructure of DC is consisted of nodes that are highly volatile. Therefore, fault recovery mechanisms are crucial in order to improve reliability in this environment [10]. In addition, volunteer clouds require means to interact with other clouds for data migration or to gain extra computing resources [4].

5.3 Quality of Service

VCCs are expected to offer services at a low level of reliability and availability due to the fact that they depend on unreliable volunteered resources which can join or leave the cloud without prior knowledge for various reasons [7]. Availability of individual nodes is considered a primary issue in VCCs [10]. For example, it is estimated that resource unavailability can reach up to 50% in volunteer projects [18]. Availability of each individual node can affect the service quality of VCC. Andrzejak et al. [19] propose a technique to predict the availability of a group of high volatility resources.

6 Conclusion

This paper has introduced Desktop Clouds as being a new type of Cloud computing. Desktop Cloud aims at providing services based on Cloud business model on top on infrastructure that is not made for this purpose. The success of Desktop Grids projects has simulated the idea of applying the same concept within Cloud computing. However, the paper has presented several research issues that need further attention.

References

1. Kirby, G., Dearle, A., Macdonald, A., Fernandes, A.: An Approach to Ad hoc Cloud Computing. Arxiv Prepr. arXiv1002.4738. (2010).
2. Chandra, A., Weissman, J.: Nebulas: Using distributed voluntary resources to build clouds. Proceedings of the 2009 conference on Hot topics in cloud computing. pp. 2–2. USENIX Association (2009).
3. Weissman, J.B., Sundarajan, P., Gupta, A., Ryden, M., Nair, R., Chandra, A.: Early experience with the distributed nebula cloud. Proceedings of the fourth international workshop on Data-intensive distributed computing. pp. 17–26. ACM (2011).
4. Cunsolo, V.D., Distefano, S., Puliafito, A., Scarpa, M.: Volunteer computing and desktop cloud: The cloud@ home paradigm. Network Computing and Applications, 2009. NCA 2009. Eighth IEEE International Symposium on. pp. 134–139. IEEE (2009).
5. Cunsolo, V., Distefano, S.: From volunteer to cloud computing: cloud@ home. Conf. Comput. Front. 103–104 (2010).
6. Harutyunyan, a, Blomer, J., Buncic, P., Charalampidis, I., Grey, F., Karneyeu, a, Larsen, D., Lombrana González, D., Lisec, J., Segal, B., Skands, P.: CernVM Co-Pilot: an Extensible Framework for Building Scalable Computing Infrastructures on the Cloud. J. Phys. Conf. Ser. 396, 032054 (2012).
7. Andrzejak, A., Kondo, D., Anderson, D.P.: Exploiting non-dedicated resources for cloud computing. 2010 IEEE Netw. Oper. Manag. Symp. - NOMS 2010. 341–348 (2010).
8. Litzkow, M.J., Livny, M., Mutka, M.W.: Condor-a hunter of idle workstations. [1988] Proceedings. 8th Int. Conf. Distrib. 104–111 (1988).
9. Cunsolo, V., Distefano, S., Puliafito, A., Scarp, M.: Cloud@ home: Bridging the gap between volunteer and cloud computing. ICIC'09 Proc. 5th Int. Conf. Emerg. Intell. Comput. Technol. Appl. 2009. (2009).
10. Marosi, A., Kovács, J., Kacsuk, P.: Towards a volunteer cloud system. Futur. Gener. Comput. Syst. (2012).
11. Gupta, A., Awasthi, L.K.L.: Peer enterprises: A viable alternative to Cloud computing? Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on. pp. 1–6. IEEE (2009).
12. Arpaci, R.H., Dusseau, A.C., Vahdat, A.M., Liu, L.T., Anderson, T.E., Patterson, D.A.: The Interaction of Parallel and Sequential Workloads on a Network of Workstations. ACM (1995).
13. Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud computing and grid computing 360-degree compared. Grid Computing Environments Workshop, 2008. GCE'08. pp. 1–10. IEEE (2008).
14. Dillon, T., Wu, C., Chang, E.: Cloud computing: Issues and challenges. 2010 24th IEEE International Conference on Advanced Information Networking and Applications. pp. 27–33. IEEE (2010).

15. Ristenpart, T., Tromer, E., Savage, S., Shacham, H.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Computer and communications security*. pp. 199–212. ACM (2009).
16. Cao, B.Q., Li, B., Xia, Q.M.: A Service-Oriented Qos-Assured and Multi-Agent Cloud Computing Architecture. *Cloud Comput.* 644–649 (2009).
17. Endo, P., Palhares, A. de A., Pereira, N.N., Goncalves, G.E., Sadok, D., Kelner, J., Melander, B., Mangs, J.-E.: Resource allocation for distributed cloud: concepts and research challenges. *Network, IEEE.* 25, 42–46 (2011).
18. Kondo, D., Taufer, M., Brooks, C.: Characterizing and evaluating desktop grids: An empirical study. *Int. Parallel Distrib. Process. Symp.* 2004. 00, (2004).
19. Andrzejak, A., Kondo, D., Anderson, D.P.: Ensuring collective availability in volatile resource pools via forecasting. *Manag. Large-Scale Serv.* 149–161 (2008).

Cloud Security Proposed and Demonstrated by Cloud Computing Adoption Framework

Muthu Ramachandran and Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Headingley, Leeds LS6 3QR, U.K.
{M.Ramachandran, V.I.Chang}@leedsmet.ac.uk

Abstract. This paper presents the Cloud security by Cloud Computing Adoption Framework (CCAF) from its system design, development and implementation. We illustrate the required attributes and explain its significance, including the CCAF security design. To demonstrate how it works, software schema is developed. CCAF can perform quarantine and protective actions based on “Rescue”, an XML-based schema and feature for CCAF. The CCAF implementations have been illustrated to show how to enforce security and ensure all users are protected. It provides three layers of security in Access control and firewalls; Intrusion Detection Systems (IDS) and Prevention System; and Isolation Management to maintain a high level of Cloud security. CCAF security offers a framework to serve the Cloud community. The key characteristics have been explained. We will develop more service updates and demonstrations for our forthcoming projects to ensure that CCAF security can provide more use cases and added value to the Cloud community.

1 Introduction

Cloud Computing has been an agenda for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services [5, 7, 12]. With the rapid rise in Cloud Computing, software as a service (SaaS) is particularly in demand, since it offers services that suit users need. For example, Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. Health informatics help medical researchers diagnose challenging diseases and cancers [3]. Financial analytics can ensure accurate and fast simulations to be available for investors [4]. While more people and organizations use the Cloud services, security and privacy become important to ensure that all the data they use and share are well protected. Some researchers assert that security should be implemented before the use of any Cloud services in place [1, 9-10]. This makes a challenging adoption scenario for organizations since security should be enforced and implemented in parallel with any services. This motivates us to develop a framework, Cloud Computing Adoption Framework (CCAF), to help organizations successfully adopt and deliver any Cloud services and projects. In this paper, we demonstrate our security design, implementation and solution for CCAF. The breakdown of this paper is as follows. Section 2 presents security overview under CCAF. Section 3 describes security design by CCAF and Section 4 explains security development schema by

XML. Section 5 demonstrates CCAF security implementation. Section 6 explains how CCAF can serve the Cloud community and Section 7 sums up topics for Conclusion.

2 Security Overview under CCAF

We generalize the areas for security overview. The following are categories of CCAF security aims to cover:

- Application software security which deals with how we can build systems that can automatically protect itself.
- Network (LAN, MAN, GAN), Wireless network security, and Platform Security include Operating Systems, Virtualisation, and other systems software.
- VoIP security as the application is gaining popularity.
- Convergence network security where converging, multi-network media infrastructures, social networks and technologies, which is one of the emerging areas of research.
- Service-oriented security where issues related to system services such as denial of service attacks, distributed denial of services, and web services.
- Cloud security deals with services security, data security and privacy so that services delivered and assets are protected.
- Open-source software security deals with issues such as trust, certification and qualification models.
- Software components and architecture, security which deals with building components and architectures with security can be used as plug-ins.
- Web services security is essential to ensure secured services are delivered with integrity.
- Systems & Software security engineering deals with building security in (CCAF) right from requirements. This is also considered developing software applications with CCAF.

Caminao project [2] provides a comprehensive framework for systems engineering methods and concepts. However, it does not offer a complete solution for Cloud Computing. This motivates us to have a comprehensive design, implementation and service for Cloud security under the CCAF recommendation. CCAF is a framework for organizations that we previously demonstrate how CCAF can be offered in healthcare [3], finance [4] and education [6]. It is our goal to provide guidelines and recommendation for security and privacy. Computer security has been classified into a number of general concepts and processes such as identification, which identifies objects, functions, and actions, authentication, authorization, privacy, integrity and durability. The objective of the CCAF Cloud security is categorized and presented in Figure 1. We have so far well established basic security features with identification, authentication, authorization, and digital security encryption and decryption techniques. Key features with their explanations are as follows.

Identification is a basic and first process of establishing and distinguishing amongst

person/user & admin ids, a program/process/another computer ids, and data connections and communications. Often we use alphanumerical string as user identification key and some may use your email itself as the user identification key and this can be checked against when a user login into the system. Authentication and authorisation are two distinct form of allowing users to access what they are allowed not allowed to access any information in the system.

Privacy is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and team work on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/data/media content.

Integrity is defined as the basic feature of human being as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud user’s data with honesty, truthfulness and accuracy at all time. In cloud computing terms, we can achieve integrity by maintaining regular redundancy checks and digital certification in addition to other basic security features of maintaining identification, authentication, and authorisation.

Durability is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

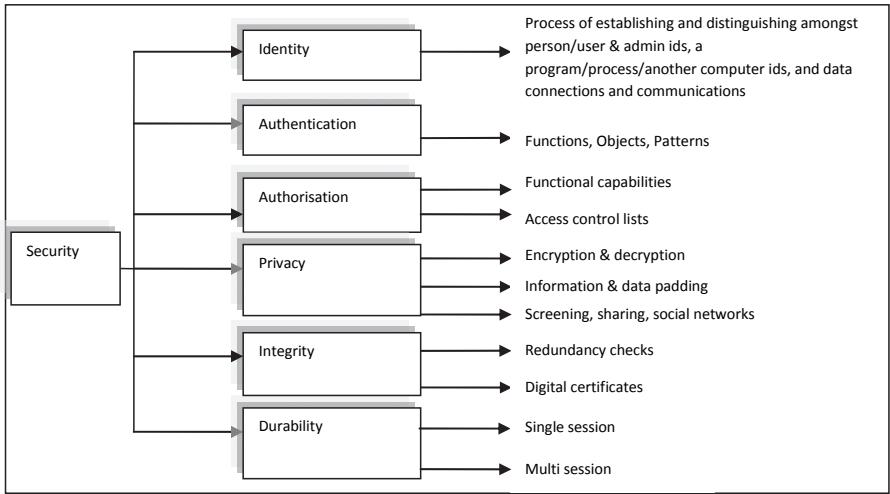


Fig. 1. CCAF digital research landscape.

3 CCAF Security Design

This section describes the system design required by CCAF. Capturing and identifying requirements for security explicitly is one of challenges in Cloud security for SaaS, which has an impact on the functionality of the system. Therefore, we need to be able specify security requirements explicitly throughout the security-specific life-

cycle phases as part of achieving CCAF (security requirements, design for security, security testing & securability testing). Tondel et al. [11] has provided an extensive survey on security requirements methods which help to identify security requirements systematically and structure them. For example, Mead [8] for the SEI's (software Engineering Institute) has identified a method known as SQUARE (Secure Quality Requirements Engineering) which has been extended SysSQUARE (Systems Engineering SQUARE) towards systems security engineering method. Our extended method consists of nine steps as follow:

- **Agree on definition** which means to define a set of acronyms, definitions, and domain-specific knowledge needs to be agreed by stakeholders. This will help identify and validate security-specific requirements clearly by stakeholders
- **Identify security goals** which means to clearly define what is expected of the system with respect to security of business drivers, policies, and procedures
- **Develop artefacts** which means to develop scenarios, examples, misuse cases, templates for specifications, and forms
- **Perform risk assessments** which means to conduct risk analysis for all security goals identified, conduct threat analysis
- **Select an elicitation technique** which includes systematic identification and analysis of security requirements from stakeholders in the forms of *interviews, business process modeling and simulations, prototypes, discussion and focus groups*. As part of this phase, one has also to identify level of security, cost-benefits analysis, and organizational culture, structure, and style
- **Elicit security requirements** which include activities such as producing security requirements document based security specific principle structure as part of our goal of developing CCAF earlier, risk assessment results, and techniques identifies for analysis such as *business process modeling and simulations, threat modeling, and misuse cases*, etc.
- **Categorize security requirements** which include activities such as classifying and categorizing security requirements based on company-specific requirements specification templates and to use our recommended security principles as this will help Systems Engineers to apply CCAF and track security-specific requirements for validation & verification at all stages of the systems engineering life-cycle.
- **Identify systems data security requirements** which include activities on extracting and carefully identifying data security and relevant sub-systems such as data centers, servers, cloud VM, and software security, SQL security, and other types of security that are relevant to data. This separation of concern allows systems engineers to integrate, track, design, and develop data security as part of enterprise wide systems development.
- **Prioritize security requirements** which include activities of selecting and prioritising security requirements based on business goals as well as cost-benefit analysis.
- **Inspect security requirements** which mean to conduct requirements validation process using requirements inspection and review meetings.

To achieve a fined-grained model for the iterated requirements, one can select key-words as objects and components.

4 CCAF Security Software Schema by XML

This section describes the software scheme required by CCAF. Extensible Markup Language (XML) is the language that can define the rule, permission, function and interactions in the use of SaaS and Cloud security. A proposed XML section type, Rescue, is described here as an example. “Rescue” is used to block virus, trojans and attacks such as denials of services and unauthorized access. In the event of hacking, all the files are backed up and retrieved from secure ports such as 21 for secure FTP and 443 for secure HTTPS. Instead of displaying IP addresses in the traditional method, the IP addresses in all virtual machines are assigned at runtime. There is an OVF ID that handles processing of the DR request. The syntax can be ovf:id =”rescue” presented in Table 1

Table 1. The CCAS Security Software Schema.

<pre><ns: Rescue ovf:required="true" xsi:type="ovf:Rescue_Type"> <Info> Rescued actions for SaaS security </Info> <Rule> <Info> Retrieve data and put them in safety </Info> <Protocol> tcp </Protocol> <DstAddr ovf:id="rescue" /> <DstPort> 21 </DstPort> <DstPort> 443 </DstPort> <SrcAddr> any </SrcAddr> <SrcPort> any </SrcPort> </Rule> <Rule> <Info> Destinations for quarantined files if infected </Info> <Protocol> tcp </Protocol> <DstAddr ovf:id="rescue" /> <DstPort> 3306 </DstPort> <SrcAddr ovf:id="rescue" /> <SrcPort> any </SrcPort> </Rule> <Origin> <Info> Firewall protection for all VMs </Info> <DateAdded> 2013-01-18 </DateAdded> <AddedBy name="Administrator" role="creator"></> </Origin> </Rescue></pre>
--

All the OVF IDs can be mapped to the required IP addresses when a VM is deployed. This allows “Rescue” to describe not just a single VM behavior, but expected communications and actions between VMs required for rescued actions. Another feature in Table 1 shows ovf:required=”true”. This means that Rescue action is on.

What triggers Rescue is when the security software detects activities from unknown IPs in the list of unknown hosts to ensure Rescue can protect all the users in real-time.

5 CCAF Security Software Implementation

CCAF security software implementation is demonstrated by the use of the Fined-Grained Security Model (FGSM), which has layers of security mechanism to allow multi-layered protection. This can ensure reduction in the infections by trojans, virus, worms, and unsolicited hacking and denial of services attack. Each layer has its own protection and is in charge of one or multiple duties in protection, preventive measurement and quarantine action presented in Figure 2.

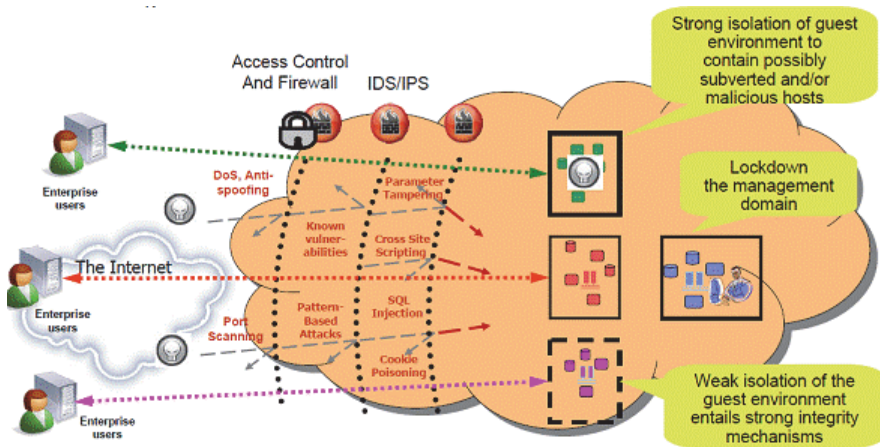


Fig. 2. The Fined-Grained Security Model offered by CCAF.

All the features in FGSM include access control, intrusion detection (IDS) and intrusion prevention (IPS), this fine-grained security framework introduced fine-grained perimeter defence. The layer description is as follows.

- The first layer of defence is **Access Control and firewalls** to allow restricted members to access.
- The second layer consists of **Intrusion Detection System (IDS) and Prevention System (IPS)**. The aim is to detect attack, intrusion and penetration, and also provide up-to-date technologies to prevent attack such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning.
- The third layer, being an innovative approach, **Isolation Management**, enforces top down policy based security management; integrity management. This feature monitors and provides early warning as soon as the behaviour of the fine-grained entity starts to behave abnormally; and end-to-end continuous assurance which includes the investigation and remediation after abnormality is detected.

Within isolation management, it has weak and strong isolation. Weak isolation focuses more on monitoring and captures end-to-end provenance to allow investigation and remediation to be greatly facilitated. Strong isolation and integrity management is also required when the first few vulnerabilities of the cloud are exposed. It backs up data safely; quarantine infected data; and isolate quarantined data till further notice. Part of this concept has been demonstrated in Section 4 to show how rescued actions can be implemented and delivered.

6 CCAF Security – A Framework Serving the Cloud Community

This section describes how CCAF security can serve the Cloud community. Cloud security is part of a quality requirements collection process and it consists of three different requirements sub-categories: *confidential & privacy* builds the trust (trust is one of the basic and backbone for establishing quality), *integrity*, and *availability*. Therefore, security needs to be identified early, designed and to be tested as part of the SaaS explicitly.

How CCAF can serve the community is described as follows. First, we need to identify all the attributes of SaaS security so that we can assess and evaluate each requirement against a set of security attributes that will enable us to extract security related requirements. Security is an essential part of the system for achieving, protecting systems and users. Security has several attributes that are related to a simple email system (where most of the attacks, such as virus, spam, intrusions, and identity fraud occur frequently); security baselines are standards that specify a minimum set of security controls that has to be met for most organizations under normal circumstances. Second, Cloud and SaaS security also include both technical and operational security concerns. Cloud computing has emerged to address the needs of the IT cost-benefit analysis and also revolution in technology in terms of reduced cost for internet data and speed. Therefore, the demand for securing our data in the cloud has also increased as a way of building trust for cloud migration and to benefit business confidence in the cloud technology by cloud providers such as Amazon, Microsoft, Google, etc. In this way, we can ensure that our CCAF security is applicable to cloud services as well as traditional systems. Figure 3 shows a model to structure cloud security attributes to develop and integrate CCAF across system development life-cycle. This model evolves based on further research and gain knowledge and experience of our own system and therefore the model will be expanded as and when we discover new attributes.

Most of the security attributes and principles identified earlier are clearly applicable to developing cloud services with systems engineering focus. However, there are some cloud-specific security related issues such as security in virtualisation and server environments. Cloud security attributes can be found in many-fold as shown in Figure 3. Although there are many attributes available, they can be further categorized as follows:

Confidentiality, Privacy and Trust – These are well known basic attributes of digital security such as authentication and authorization of information as well protecting privacy and trust.

Cloud Services Security – This includes security on all its services such as SaaS, PaaS, and IaaS. This is the key area of attention needed for achieving cloud security.

Data Security – This category is again paramount to sustaining cloud technology. This includes protecting and recovering planning for cloud data and service centers. It is also important to secure data in transactions.

Physical Protection of Cloud Assets – This category belongs to protecting cloud centers and its assets.

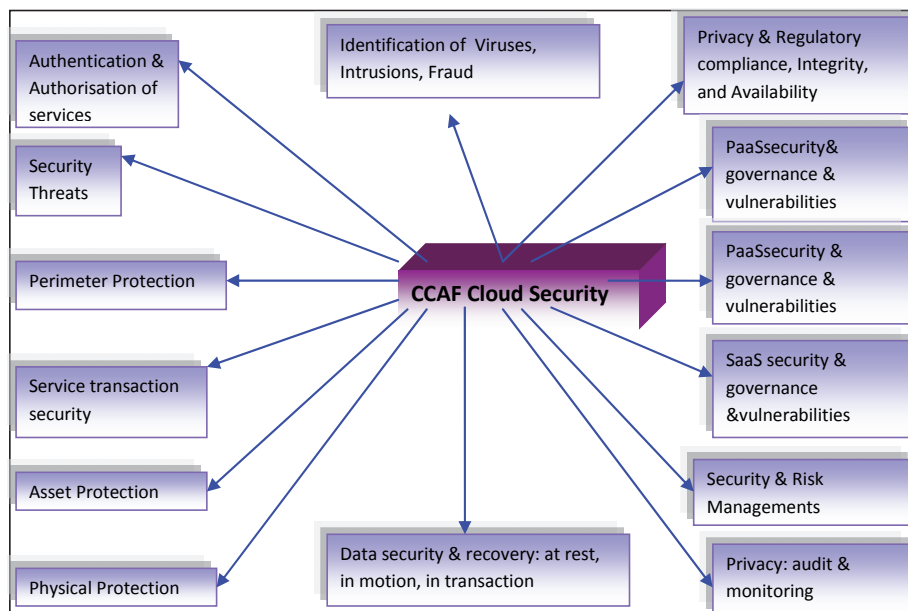


Fig. 3. CCAF Cloud Security Attributes serving for the community.

The above cloud security attributes/characteristics are essential and useful to understand non-functional aspects of services development and service provision. These attributes are also useful for building CCAF and maintaining security. The following section will use cloud security attributes and frameworks identified in this section as the main input for CCAF not developing security patches after cloud services has been delivered. Communities that have been positively influenced by CCAF in other projects include Guy's and St Thomas NHS Trusts (GSTT), King's College London (KCL), University of Southampton, University of Greenwich and Leeds Metropolitan University. Organizations that have been involved also include Commonwealth Bank of Australia (CBA), IBM in the US, SAP and University of Oxford in the development of Cloud services and projects [5]. Forthcoming Cloud projects include SAS and Mathematica for deliveries in modern education, and research and development.

7 Conclusion

We present the Cloud security presented by CCAF from its system design, development and implementation. We illustrate the required attributes and explain its significance for CCAF, including the security design. To demonstrate how CCAF works, software schema is developed. CCAF can perform quarantine and protective actions based on “Rescue”, a XML-based schema and feature. The CCAF implementations have been illustrated to show how to enforce security and ensure all users are protected. It provides three layers of security in Access control and firewalls; Intrusion Detection Systems (IDS) and Prevention System; and Isolation Management to optimize Cloud security. CCAF security offers a framework to serve the Cloud community. The key characteristics have been explained. Organizations that are involved in the development and adoption of CCAF have been presented. We will develop more service updates and demonstrations for our forthcoming projects to ensure that CCAF security can provide more use cases and added value for the Cloud community.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010), Above the Clouds: A Berkeley View of Cloud computing. *Communications of the ACM*, 53(4), 50-58.
2. Caminao Project, Caminao’s Way: Do systems know how symbolic they are? Modelling Systems Engineering Project, http://caminao.wordpress.com/overview/?goback=%2Egde_3731775_member_251475288, accessed on 21st June, (2013).
3. Chang, V., Walters, R. J., & Wills, G., Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research, Springer: CLOSER 2012, CCIS 367, pp. 245–264, (2013).
4. Chang, V., Business Intelligence as Service in the Cloud, *Future Generation Computer Systems*, (2014).
5. Chang, V., Walters, R. J., & Wills, G., The development that leads to the Cloud Computing Business Framework. *International Journal of Information Management*, 33(3), pp 524-538, June, (2013).
6. Chang, V., Brain Segmentation – A Case study of Biomedical Cloud Computing for Education and Research. In, *Learning Technologies Workshop*, Higher Education Academy (HEA), University of Greenwich, (2013).
7. Marston, S., Li, Z., Bandyopadhyay, S. and Zhang, J. and Ghalsasi, A., Cloud computing – The business perspective, *Decision Support Systems*, Elsevier, 51(1): pp 176-189, (2011).
8. Mead, N.R., et. al., Security Quality Requirements Engineering (SQUARE) Methodology, TECHNICAL REPORT, CMU/SEI-2005-TR-009, (2005).
9. Ramachandran, M., Software components for cloud computing architectures and applications, Springer, Mahmood, Z and Hill, R (eds.), (2011).
10. Ramachandran, M., *Software Security Engineering: Design and Applications*, Nova Science Publishers, New York, USA, 2011. ISBN: 978-1-61470-128-6, (2011).
11. Tondel, I. A et al., Security requirements for rest of us: a survey, *IEEE Software*, Special Issue on Security and Agile requirement engineering methods, Jan/Feb. (2008).
12. Vouk, M. A., Cloud Computing – Issues, Research and Implementations, *Journal of Computing and Information Technology - CIT* 16, page 235–246, Volume 4, (2008).

A Proposed Case for the Cloud Software Engineering in Security

Victor Chang and Muthu Ramachandran

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Headingley, Leeds, LS6 3QR, U.K.
{V.I.Chang, M.Ramachandran}@leedsmet.ac.uk

Abstract. This paper presents Cloud Software Engineering in Security (CSES) proposal that combines the benefits from each of good software engineering process and security. While other literature does not provide a proposal for Cloud security as yet, we use Business Process Modeling Notation (BPMN) to illustrate the concept of CSES from its design, implementation and test phases. BPMN can be used to raise alarm for protecting Cloud security in a real case scenario in real-time. Results from BPMN simulations show that a long execution time of 60 hours is required to protect real-time security of 2 petabytes (PB). When data is not in use, BPMN simulations show that the execution time for all data security rapidly falls off. We demonstrate a proposal to deal with Cloud security and aim to improve its current performance for Big Data.

1 Introduction

The advantages of adopting Cloud Computing have been discussed in numerous papers [1-2, 4-6, 14]. Although organizations that adopt Cloud Computing acknowledge benefits offered by Cloud services, challenges such as security and privacy remain a scrutiny for organizational adoption. While overseeing the importance of security, the software engineering and development process should always design, implement and test security features. The software engineering process should be robust enough to withstand attacks and unauthorized access. The secured services on offer can be guaranteed to provide benefits for users and service providers [13]. For example, users are safe and protected while using Cloud-based services. Service providers can ensure that their services have high extent of security, so that their customer satisfaction and company reputation can be improved. In order to achieve this, service providers have preventive measures and rescued actions to reduce risk imposed by security breach.

While acknowledging the importance of Cloud software engineering in security (CSES) in the previous paragraph, CSES should be undertaken early in the software development cycle. We explain the design and implementation of the CSES, and describe how we prototype a Business Process Modeling Notation (BPMN) as part of our CSES service to test the performance with a cloud platform that contains 2 PB of data. We review a number software engineering proposals, we notice that none of them provides the full solution from design, implementation and services for Cloud

security [1-3, 7-8, 13]. This motivates us to propose our Cloud software engineering in security (CSES) solution focusing on design and implementation. Before presenting our proposal, we review a few selected literature. We discuss what should be available in the design and then propose our own implementation by the use of BPMN. The breakdown of the paper is as follows. Section 2 presents a review of existing proposals suitable for our approach. Section 3 describes how BPMN can be used from design to implementation. Section 4 shows how BPMN can be used for implementation and results of simulations. Section 5 presents conclusion of this paper.

2 Review of Existing Proposals Relevant to Our Research

We review a few selected literature that is relevant for CSES described as follows. Gonzalez-Castillo [7] defines further classify software security engineering and its implementation into two major groups: *software acquisition security* (which includes the security specifications in all processes to buy, rent, or interchange software to use in an enterprise) and *systems & software development security* (which includes the security specifications in all processes to develop information systems). His approach is focused on system security for CSES as shown in Figure 1.

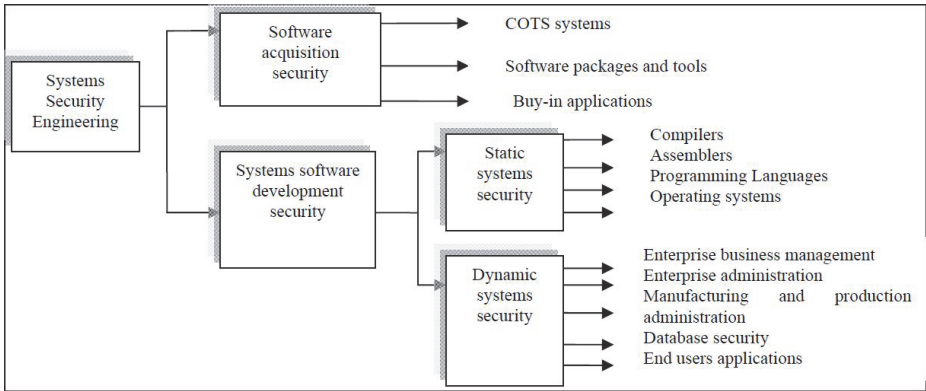


Fig. 1. Systems security taxonomy for CSES [7].

In Figure 1, software acquisition deals with COTs (component off-the-shelves), packages, and buy-in tools. Information systems development has been divided further into two main categories known as static and dynamic systems. Static systems security includes compilers (involves specification to develop compilers), assemblers, Programming Languages (PLs), and Operating Systems (OS). Dynamic systems security deals with enterprise business management (take control of business process information), enterprise administration (security specs to develop applications which objective is to provide control of administrative process information), Manufacturing systems, database systems, and end user systems which deal with developing applications for daily activity tools for end users. Design for security calls for specific design

rationale and features supporting security explicitly. We can also distinguish furthermore in defining security design where functional design artefacts are created as usual with security. McGraw [8] has identified a number of security techniques against each stage in the software development lifecycle (SDLC). Figure 2 illustrates a set of those techniques. For example, abuse cases, security inspection and security modeling should be conducted as part of the Requirement Engineering (RE) process, security risk analysis should be conducted during design phase, external review and risk based security test analysis should be done during test planning stage, static analysis for security at the code level (this may include code inspection or automated code analysis tools equipped with security), and penetration testing & security breaks should be conducted during operational and field testing.

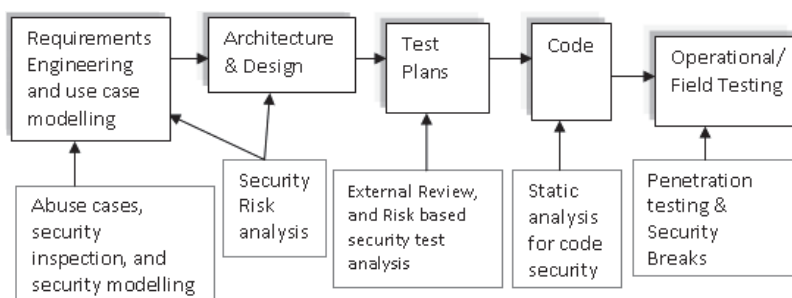


Fig. 2. Software Security Techniques (Build-In Security) [8].

There are different types of security designed for software as follows. Information security is the overall security for the whole enterprise and its network environment. Network security is to make sure the secured transactions and communications take place. Whereas application security is to make sure software systems as a whole is secured in its environment. All the software design work in CSES is suitable for information, network and application security. To demonstrate this concept, Ramachandran [9] proposes the Systems Security Engineering Life Cycle for CSES shown in Figure 3, with the emphasis in having a distinction between classical software engineering (SE) lifecycle vs. systems security engineering lifecycle (SSE) [10-11]. The SSE extracts and specifies security requirements using specific methods in addition to the usual functional modelling conducted during requirements engineering phase of SE lifecycle. This SE lifecycle can be used for CSES as follows. Ramachandran [11] has captured such good practices in the form of software guidelines across software development, reuse, and component based software engineering (CBSE). Software as a Service provides new abstraction for developing and delivering business application as part of the cloud. Service implementation is based on software component for implementing their core logics. Ramachandran [12] has produced a number of service component models for implementing services with build in security.

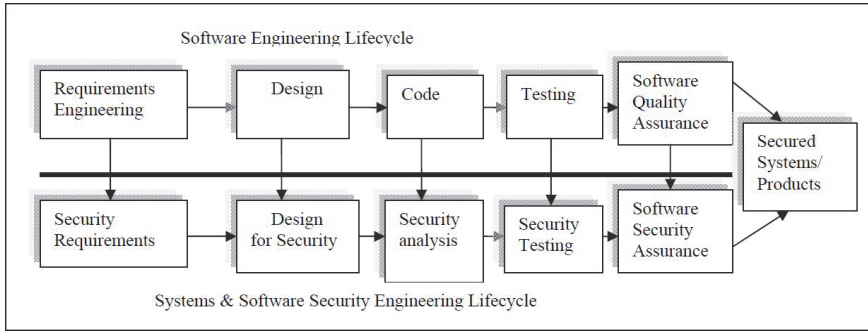


Fig. 3. Systems Security Engineering Life Cycle for CSES [9-12].

3 Business Process Modeling Notation: From Design to Implementation

This section describes the required steps to move from design to implementation phase in the development of CSES by the use of Business Process Modeling Notation (BPMN) in the Cloud.

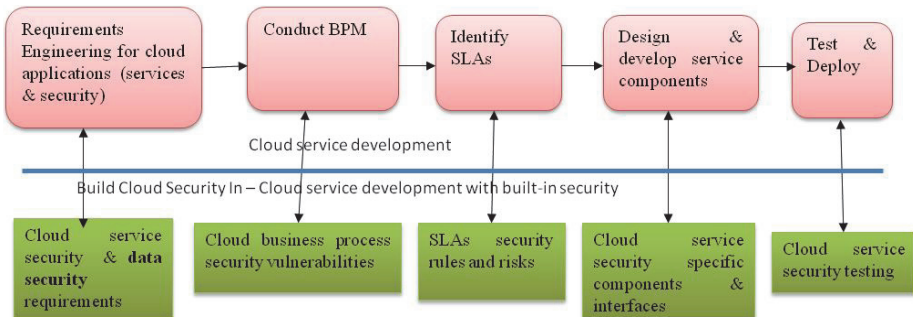


Fig. 4. Cloud security-based service development and integrating data security process with built-in security.

As shown in Figure 4, cloud service development are classified into a number of phases: 1) requirements engineering for cloud services during which time we can identify security related requirements from various stakeholders; 2) conduct business process modelling and simulations (BPM) for each cloud services during which time we can also simulate security aspects and study performance related measures and also introduce a possible number of intrusion and conduct simulations before actual service implementation take place; 3) identify Service Level Agreements (SLAs) identifies a number of service level agreements and regulatory and governance related compliances during this time we should be able to separate out security related SLAs and risks; 4) design and develop services during this phase we can actually implement security related threads that have been carried continuously from all phases, and finally; 5) test and deploy services that are developed with CSES. Additionally, we can:

1. The first step is to apply software security engineering techniques to all identified cloud services. This includes using security analysis tree and various other techniques specified by Ramachandran [10-11].
2. The second step is on identifying BPM which should include software security analysis for each business process identified. This will allow us to identify potential security threats that start with service requirements and business requirements as the input to conduct service security analysis using techniques such as Systems Secure Quality Requirements Engineering (SysSQUARE), and Microsoft Secure Development Lifecycle (SDL). The outcome of this process should yield a set of cloud services security requirements with clear indication of software security issues.

We can use BPM jointly with other framework such as Cloud Computing Adoption Framework presented in our other workshop paper or be used independently in the Cloud. Additionally, different states of user's data must be protected and managed logically and consistently. In order to use BPM to achieve this, additional work for BPM is required. This includes the Business Process Modelling Notation (BPMN) models shown in Figure 5. Several BPMNs (version BPMN2 2012) have been created for each of those scenarios to run a number of possible simulations with various business variability using an open source simulation tool, known as Bonita Soft BOS 5.8 [3]. Simulations of BPMN for Cloud Data Security and Application of the SysSQUARE method can be used to elicit security threats.

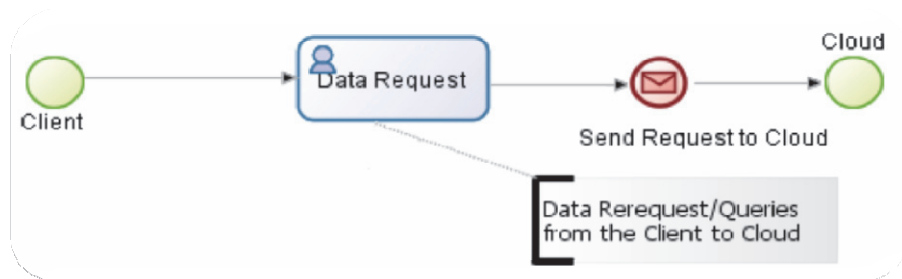


Fig. 5. Data Request Business Process Model for Cloud Security.

The Client of Cloud Computing contains a computer software or/and a computer hardware which depends on cloud computing architecture to support the application deliveries, or which designed specifically for cloud service deliveries. A Client of Cloud Computing Architecture is an interface of common cloud user through the web browsers or thin terminals. Cloud provider is the one who offers the Cloud Service Delivery Models to Client through the internet. According to our proposed system the client just sends a request to the cloud then the remaining process is being taken care of cloud service provider who consists of Cloud Management Teams, Data Centres/Security pools and the Intrusion Detection Mechanisms. The hardware infrastructure is based on Southampton private cloud platform described in [5]. Figure 5 represents the BPMN process of Data Request flow from Client to Cloud. Our proposed solution can opt to use a framework for classifying cloud securities and policies. Cloud security is the key to business sustainability and hence we need to struc-

ture security related aspects into a simple framework that helps us to evolve and improve over a time period.

4 Business Process Modeling Notation: Implementation and Results

This section describes how to use BPMN for implementations and the results of simulations in the private cloud environment. Simulating a process allows us to study its behavior for their external events/triggers. Process simulation has been successful in several applications from low-end to high-end systems. Hence, simulating a BPMN model will help us to study business behaviors/performance for various expected and unexpected scenarios. The BPMN simulation process consists of a number of cyclic phases as shown in Figure 6. BPMN starts with an actor called Client with a small circle notation which sends a message to a process (Data Request with rounded square) which task has been devoted to take action based the request and therefore send a message to the cloud (finishing circle). The second phase is to annotate each element in the process and thirdly to create tasks, assign simulation variables (different types of requests both valid and invalid) to process and tasks in that process. Finally, create messages between elements in the process and run a number of simulations.

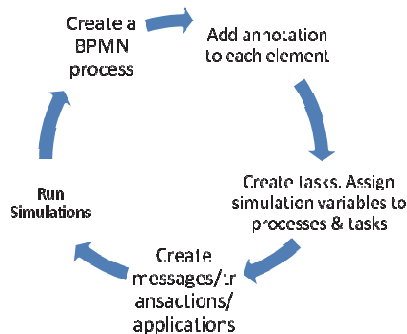


Fig. 6. BPMN Simulation Process for CSES.

The data centers are the essential asset of Cloud Computing corporations, these all connect to all applications, storage services and servers. The business relies on the cloud data centers supports the business values and operations and drive maximum efficiencies. The data centers play key roles that need to be managed and planned carefully to meet growing performance requirements/demands from users and applications. The use of BPMN can simulate the daily operations in the data centers, which contain up to 2 petabytes (PB) of data. Figure 7 shows the BPMN model for different states of models for data security. The data center can use this model to study the performances of selected cloud data architecture. This process starts with a data status decision (diamond symbol) passes that data based on that decision to any one of the paths of the cloud storage processes (data at rest, data in use, and data in

change/transition). This in turn passed on to a data security pool which is a separate lane with dedicated security processes (such as data security area and data center update) to study security controls in place before it ends.

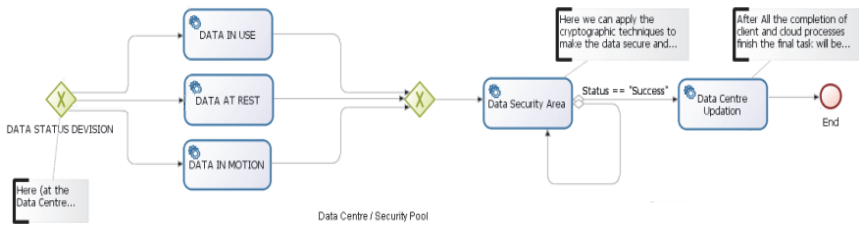


Fig. 7. BPMN model for three types of cloud data security.

Cloud security is the key to business sustainability and hence we need to structure security related aspects into a simple framework that helps us to evolve and improve over a time period. In the implementation to result phase, we use BPMN for raising alarm in data security while all 2 PB of data in the Cloud has been intensively in used.

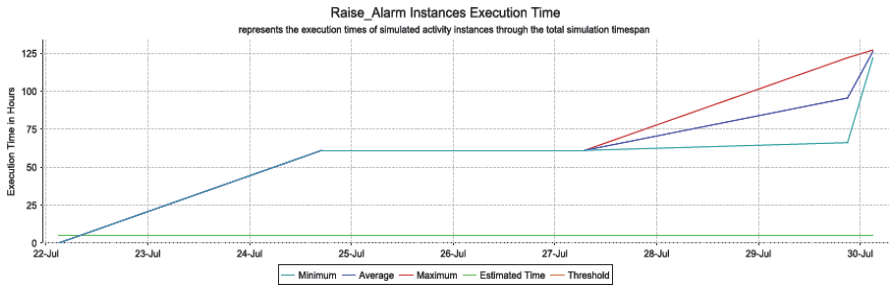


Fig. 8. Data Security Area Peak Access- High execution time when data in use.

Figure 8 shows a graph with peak execution time for entering the data security area of the business process. Results show that increased steadily from 0 to 60 hours between July 22 and the middle of July 24, 2013. The execution time stayed stable at 60 hours between the middle of July 24 and beginning of July 27. Some execution time increased due to the increasing demand in security. The implications of this result show that data security instances execution time can be high when data was constantly in use. On the other hand, the execution time was less than 2 hours if data was not in use.

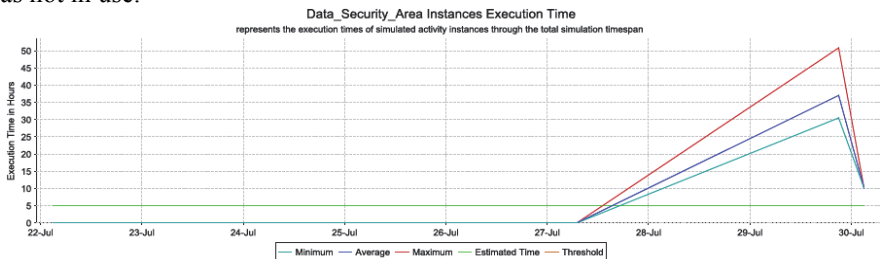


Fig. 9. Raising Alarm by BPMN for 2 PB data.

Figure 9 shows a graph with execution time when the BPMN process raised a security alarm. The execution time rose from 0 to three peaks (51, 36 and 30 hours) between July 27 and right before July 30, before falling to 10 hours of execution time right after July 30, 2013. The increment in execution time was necessary since BPMN alarm checked every single file and instance in 2 PB of data in the Cloud. This explained why such a long execution time was required. We plan to develop algorithms or methods that can optimize the security performance. The execution time to run each BPMN process only takes 2 seconds all the times, which has a very low execution time. This ensures that fast and efficient BPMB process can meet the requirement of business agility.

5 Conclusion

We present our Cloud software engineering in security (CSES) proposal from its system design to implementation phase. We review a few selected literatures and assert that none of them has the solution from design to implementation of Cloud security as yet. We then propose a unique approach to combine the recommended software engineering process with an emphasis on security. We use Business Process Modeling Notation (BPMN) to illustrate design to implementation of a good Cloud service. We use BPMN to demonstrate implementation for CSES with its supporting results. BPMN can be used to simulate the case of raising alarm for protecting Cloud security in real-time. BPMN simulation results demonstrate long execution time of 60 hours of protecting Cloud security of 2 PB. When data is not in use, BPMN can take less than 2 hours of their execution time. We are in the process of developing methods or algorithms to optimize the performance and hope to disseminate our research outcome in the next twelve months.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010), Above the Clouds: A Berkeley View of Cloud computing. *Communications of the ACM*, 53(4), 50-58.
2. Binz, T., Breiter, G., Leyman, F., & Spatzier, T. (2012). Portable Cloud Services Using TOSCA. *IEEE Internet Computing*, 16(3).
3. Bonita Soft (2012) BOS 5.8, Open source BPMN simulation software, <http://www.bonitasoft.com/resources/documentation/top-tutorials>
4. Chang, V., Walters, R. J., & Wills, G., Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research, Springer: CLOSER 2012, CCIS 367, pp. 245–264, (2013).
5. Chang, V., Business Intelligence as Service in the Cloud, *Future Generation Computer Systems*, DOI: <http://dx.doi.org/10.1016/j.future.2013.12.028>, (2014).
6. Chang, V., Walters, R. J., & Wills, G., The development that leads to the Cloud Computing Business Framework. *International Journal of Information Management*, 33(3), pp 524-538, June, (2013).
7. González-Castillo, O. Y., Selected Quality Metrics for Digital Passport Photographs, Logos

- Verlag Berlin, ISBN 9783-8325-1965-0 (2008).
- 8 McGraw, G, Software Security: Building Security In, IEEE Security & Privacy, March/April, (2004).
 9. Ramachandran, M (2008) Software components: guidelines and applications, Nova Publishers, NY.
 10. Ramachandran, M., Software components for cloud computing architectures and applications, Springer, Mahmood, Z and Hill, R (eds.), (2011).
 11. Ramachandran, M., Software Security Engineering: Design and Applications, Nova Science Publishers, New York, USA, 2011. ISBN: 978-1-61470-128-6, (2011).
 12. Ramachandran, M (2012) Service Component Architecture for Building Cloud Services, Published: August 20th, 2012, Service Technology Magazine Issue LXV, <http://www.servicetechmag.com/I65/0812-4>.
 13. Santos, N., Gummadi, K. P., and Rodrigues, R., Towards trusted cloud computing, In Proceedings of the 2009 conference on Hot topics in cloud computing, (2009).
 14. Vouk, M. A., Cloud Computing – Issues, Research and Implementations, Journal of Computing and Information Technology - CIT 16, page 235–246, Volume 4, (2008).

SHORT PAPER

Review and Analysis of Cloud Computing Quality of Experience

Fash Safdari and Victor Chang

School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University,
Headingley, Leeds LS6 3QR, U.K.
{F.Safdari, V.I.Chang}@leedsmet.ac.uk

Abstract. Cloud computing is gaining growing interest from industry, organizations and the research community. The technology promises many advantages in terms of cost saving by allowing organizations and users to remotely gain access to a huge pool of data storage and processing power. However, migrating services to cloud computing introduce new challenges in performance and service quality. Quality of service (QoS) is and has been used as a means of monitoring cloud service performance. However, QoS is based on network parameters which do not necessarily reflect users' quality of experience. This paper discusses cloud computing quality of experience as perceived by the person using the cloud-based applications and services. We also review a selected current contribution to the quality of experience (QoE). We have expert reviews undertaken to identify six key performance indicators (KPIs). Based on these six KPIs, we sent our surveys, collected feedback and analyze data to confirm that QoE measurement can meet organizational goals, user satisfaction and stakeholders' requirements.

1 Introduction

Cloud computing is a new phenomenon in information system and communication technology and has gained a lot of interests from industry, organizations and the research community. Moving services to cloud mean that applications that used to run on users' PCs will reside in data centers distributed across different continents. Cloud computing promises economic benefits. However, migrating services to cloud computing introduce new challenges in service performance, quality and reliability; traditionally service level agreements are used as a means of guaranteeing the delivery of acceptable service performance level. Existing QoS metrics and service level agreements (SLAs) offered by cloud service providers do not include anything about the performance of service from user point of view and are not adequate to meet users' quality of service expectations [16]. Organizations are unlikely to adopt cloud computing if users' experience is not as good as it was before moving to cloud or performance does not meet users' perceived quality of experience and performance expectations [8]. However, due to subjective nature of users' quality of experience, measuring, capturing and quantifying QoE remains an open research question. In this paper, we review selected current contributions to QoE. The remainder of this paper is struc-

tured as follows: Section 2 describes QoE. Section 3 provides an overview of the related work on QoE. Section 4 presents the results and discussions from the expert review and the survey. Section 5 concludes this paper.

2 Quality of Experience (QoE)

Many definitions for QoE have been proposed in literature. In [15] QoE is referred to as ‘the basic character or nature of direct personal participation or observation’.

Descriptions in [6] states QoE as ‘a concept comprising all elements of a subscriber's perception of the network and performance relative to expectations’. Synthesis in [17] gives the following description for QoE: ‘QoE is a multi-dimensional construct of perceptions and behaviors of a user, which represents his/her emotional, cognitive, and behavioural responses, both subjective and objective, while using a system.’. ITU-T [9] defines QoE as ‘overall acceptability of an application or service, as perceived subjectively by the end user’. There is no a universally acceptable definition of QoE [15], QoE is outlined in various literatures as a subjective measure.

To model and measure QoE appropriate QoE metrics need to be identified. While network performance parameters and QoS metrics are well-defined, in contrast QoE metrics are not well understood and remain an open research question. A large volume of publications has been dedicated to the study of QoE. In section 3, we review a selected list and summarize their findings and proposals.

3 Summary of Existing QoE Studies

Casa et al., [2] studied QoE in remote virtual desktop services. Authors outlined a three layer QoE evaluation framework, consisting of user layer, application layer, and network layer. Network layer deals with QoS parameters such as bandwidth, application layer includes response time, screen compression rate, and colour parameters. User layer is based on user feedback using Mean Opinion score (MOS). They performed subjective experiment using 52 participants. Their experiment was focused on users’ overall experience and round trip time. Their main finding is the correlation between QoE and application QoS requirement. Interactive applications are more delay sensitive, high RTT degrades user quality of experience. This indicates a direct correlation between network bandwidth and QoE, low bandwidth has negative impact on user experience.

Chen et al., [5] argue that obtaining user feedback after they used an application is not the most appropriate mechanism. They proposed a QoE capture framework called OneClick where users click a particular button indicating they are not satisfied with the quality of an application. They assert that dissatisfaction refers to all QoE dimensions and QoE is application specific as applications have different QoS requirements. Authors in [5] investigated QoE a group of 52 users using ‘The Box’, a Dropbox-like application in a controlled lab environment. They observed a correlation between poor user QoE and low network bandwidth. [8] state that QoE has the potential to become the new guiding standard for cloud computing quality management.

Authors argued that understanding and managing QoE of cloud services involves a multidisciplinary view including network, user, and business aspects. Technical factors that influence cloud computing QoE vary from application to application. QoE-based classification of application based on level of interactivity, usage domain, and service complexity is presented.

A QoE management framework was proposed [12], where five steps are outlined: Service classification provides service contents; Main quality parameters extraction selects key quality metrics; user feedback collection, QoE analysis predicts reasons affecting service quality and Performance upgrade. The framework uses simple real-time oneclick [5] feedback mechanism. They performed an experiments using a 100-second video streaming, only two network parameters, delay per packet, and packet loss were measured. Their findings indicate increase in packet delay and packet loss result in poor QoE. On the other hand, it is not easy to measure QoE in a unified form because many factors affecting QoE [14]. Authors affirmed that taking into account all factors could result in a complex QoE metrics; simple QoE metrics are more practical. An in-service feedback QoE framework is introduced, which runs over a multi-agent environment, and abstract functions of different agents were discussed.

Kist and Brodie [15] did a case study using two groups of seven and eleven students to identifying the effect of QoS on QoE. Their findings indicate that flow (level of interruption to concentrate on a task), achievability (sense of completing the task), and extra time needed to complete the task were directly affected by QoS. Their findings are rather generic as there is no mapping of QoE and different QoS metrics. Statements in [16] assert that QoE will play a major role in the success or failure of cloud service. The authors argue that understanding QoE requires a multi-disciplinary view of network, user and business aspects. A conceptual view of cloud services QoE landscape is proposed, which consists of three main branches: user profile, application, and network QoS.

In table 1 we summarized a list of factors identified by different authors that could have an impact on QoE.

Table 1. Summary of authors’ views on factors affecting QoE.

R e f e r e n c e	User demographics	User personality	User interface	Device usability	Application characteristics	Volume of data	Response time	Delay	Jitter	Bandwidth	Packet loss	CPU Consumptions	Service reliability
[2]	✓	✓		✓	✓		✓	✓		✓	✓		
[3]				✓						✓	✓		✓
[6]					✓					✓	✓		
[8]	✓	✓			✓					✓	✓		
[9]	✓				✓	✓			✓	✓	✓		
[13]					✓			✓	✓	✓	✓		✓
[15]				✓				✓		✓	✓		
[16]								✓		✓		✓	
[17]	✓		✓		✓	✓		✓	✓	✓	✓		

4 Results from the Expert Review and Survey

QoE is an area that requires the support of results from surveys and quantitative analysis demonstrated by Chang [3], who identifies six key performance indicators (KPI) for IT success and explains how these six KPIs can be used in measuring the success of IT project delivery. The demonstrated examples by [3] are relevant to QoE, in which expert reviews have been involved. Based on the extension of the work, we have presented the summary of the importance of six KPIs as follows.

- Relevance for usability for Cloud QoE adoption is important with the support of real use cases.
- Achieving good performance is an essential for Cloud QoE adoption.
- Security concern is a main reason for some organizations not to adopt Cloud Computing which researchers describe challenges and issues to be improved.
- Data accuracy is important to compute accurate results so that organizations have a higher trust and confidence in Cloud QoE adoption.
- Service and data portability are highly relevant to Cloud QoE adoption that researchers demonstrate their usefulness for QoE.
- Scalability is a core characteristic for Cloud and the ability to scale up and down resources promptly for different demands is essential for Cloud QoE adoption.

These six KPIs are essential for the development of QoE adoption and measurement. While feedback from experts are important, the feedback from users (in this case, students) are essential for the development of QoE adoption and measurement. Questions are based on these six PKIs. Each participant was asked their opinions and rated the importance of these six KPIs. In this case, we identified that students are likely to use or get involved in QoE at some stage, which explains why students take part in this study. As a result, we sent out surveys and collected feedback from students about their feedback about Cloud QoE adoption.

Analysis of variance (ANOVA) provides statistical test of whether means of several groups are equal and can generalize t-test or F-test for two or more groups [4]. ANOVA can be used when these two cohorts have close means and each group has two sets of data. Table 6 shows the ANOVA analysis with F-test for cohort group one, where “grp_with_Cloud” is the shorter version of “group_with_Cloud”. Cohort group one has F-value = 2.78 and Prob > F is 0.1148 (the smaller, the better). The R-squared value is 0.7875 (the higher, the better) and the root mean square error (MSE) is 2.74874 (the lower, the better). These key results confirm that the statistical analysis agrees that the use of Cloud QoE adoption help students in their motivation for learning. Statistical results confirm a good extent of accuracy in analysis by having high R-squared values; low root mean square values and high F-test values. These results confirm that we can achieve the stakeholders’ requirements in the first stage of QoE investigation. The p-value is below 0.1 and is considered a good result. To ensure smooth delivery, p-value should be as small as possible. In this case, variations in p-value have been explained by the variations before and after using Cloud QoE adoption. Based on direct feedback from some participants, Cloud QoE adoption can enhance learning and understanding of the subject involved.

Table 2. ANOVA Analysis for the Student Cohort Group.

Number of obs = 30 R-squared = 0.7875					
Root MSE = 2.74874 Adj R-squared = 0.5042					
Source Partial SS df MS F Prob > F					
-----+-----					
Model 168 8 21 2.78 0.0943					
grp_with_Cloud 168 8 21 2.78 0.0943					
Residual 45.3333333 6 7.55555556					
-----+-----					
Total 213.333333 14 15.2380952					

5 Conclusion and Future Work

This research has focused on the literature on the current state of QoE of cloud computing. The assessment of cloud computing QoE cannot be based only on datacenters performance efficiency, SLA, and network QoS parameters due to the fact many different intermediate networks and providers are involved in providing users access to cloud services. Many factors affect QoE, having a framework that capture all individual factors could result in a complex QoE management model. It is more practical and efficient to capture and model users’ overall acceptability of quality of service in real-time. Individual applications and services have different QoS requirements. It is important to monitor network parameters and QoE for individual application and identify parameters and factors that influence QoE for a given application. This provides a fundamental start towards developing a model understanding correlation between QoE and network performance metrics. Apart from the consolidation of literature, we present that the use of expert reviews and the survey analysis help shake up the research for QoE adoption. We confirm that the six KPIs essential and statistical results for the proposed QoE framework to ensure that stakeholders, users and students are well engaged in the development work. Their feedback will be useful for a successful delivery of QoE implementation to ensure that adoption and measurement can meet the organizational goals, user satisfaction and stakeholders’ requirements. We also identify more user groups that require QoE, collect their feedback and analyze our collected data.

References

1. Armbrust, M. Fox, A. Griffith, R. Joseph, A. D. Katz, R. H. Konwinski, A. Lee, G. Patterson, D. Rabkin, A. Stoica, I. Zaharia, M. ‘Above the Clouds: A Berkeley View of Cloud Computing’, Technical Report, No. UCB/EECS-2009-28, UC Berkeley, (2009).

2. Casas, P. Seufert, M. Egger, S and Schatz, R. ‘Quality of Exeperience in Remote Virtual Desktop Services’, IFIP/IEEE IM2013 Workshop: 1st International Workshop on Quality of Experience Centric Management (2013).

3. Chang, V., 'Business Intelligence in the Cloud, Future Generation Computer Systems, DOI: <http://www.sciencedirect.com/science/article/pii/S0167739X13002926>, (2014).
4. Chang, V. and Wills, G., 'A University of Greenwich Case Study of Cloud Computing – Education as a Service', E-Logistics and E-Supply Chain Management: Applications for Evolving Business, IGI Global, April, (2013).
5. Chen, K. Tu, C, and Xiao, W. 'OneClick: A Framework for Measuring Network Quality of Experience', IEEE, (2009).
6. Empirix. 'Assuring QoE on Next Generation Networks, Empirix white paper', (2001).
7. Fischer, H. Casas, P. Suetter, S and Schatz, R. 'First Look at Quality of Experience in Personal Cloud Storage Services', IEEE International Conference on 1st International Workshop on Mobile Cloud networking and Services, (2013).
8. Hobfeld, T. Schatz, R. Varela, M. and Timmerer, C. 'Challenges of QoE Management for Cloud Applications', IEEE Communications Magazine, (2012).
9. ITU-T. 'Vocabulary and effects of transmission parameter on customer opinion of transmission quality', (2006),
10. Laghari, K. Crespi, N. Molina, B. 'QoE aware Service Delivery in Distributed Environment', IEE Computer society (2011).
11. Jarschel, M. Schlosser, D. Scheuring, S and Hobfeld, T. 'An Evaluation of QoE in Cloud Gaming Based on Subjective Tests', IEEE computer society., (2011).
12. Jie, Z and Kim, H, 'User Feedback Oriented Quality of Experience Management Framework', China communications., (2013).
13. Khalil, R. Crespi, N. Molina, B. and Palau, C. 'QoE aware Service Delivery in Distributed Environment', 2011 workshop of International Conference on Advanced Information Networking and Applications', (2011).
14. Kim. H. Lee, K. and Zhang, J. 'In-Service Feedback QoE Framework', 2010 Third International Conference on Communication Theory, Reliability, and Quality of Service, (2010).
15. Kilkki, K. 'Quality of Experience in Communications Ecosystem', Journal of Universal Computer Science, vol. 14, no. 5 (2008).
16. Varela, M. and Sankala, J, ' Understandin Quality Issues in the Cloud', IEEE compting, (2010).
17. Wu, w. Arefin, A. Rivas, R. Nahrstedt, K. Sheppard, Z. Yang, Z.: 'Quality of Experience in Distributed Interactive Multimedia Environments: Toward a Theoretical Framework', Proceeding of ACM internamtionl conference on Multimedia, (2009).

Author Index

Benzadri, Z.	3
Bouanaka, C.	3
Chang, V. . 13, 21, 30, 38, 62,	
71, 83	
Crowder, R.	38
Hamid, N.	46
Ramachandran, M. 13, 62, 71	
Safdari, F. 13, 21, 30, 38, 62,	
71, 83	
Walters, R.	46, 55
Wills, G.	38, 46, 55



Proceedings of ESaaS 2014

Emerging Software as a Service and Analytics

ISBN: 978-989-758-026-0

www.closer.scitevents.org