

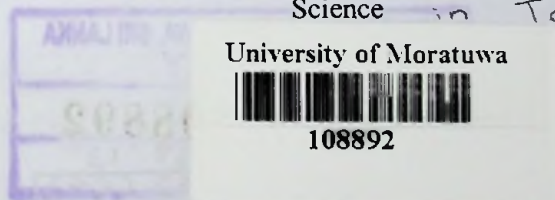
# SECURE CLOUD: A SECURITY FRAMEWORK FOR ORGANIZATIONS IN IMPLEMENTING SYSTEMS ON THE CLOUD

K.N.T. De Abrew

088356

LIBRARY  
UNIVERSITY OF MORATUWA, SRI LANKA  
MORATUWA

Thesis submitted in partial fulfillment of the requirements for the degree Master of Science in Telecommunications



Department of Electronic and Telecommunication Engineering

University of Moratuwa  
Sri Lanka

621.38 "13"  
-----  
621.39 (043)

108892

January 2013

108892

## DECLARATION

"I declare that this is my own work and this thesis/dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

### *UOM Verified Signature*

Signature:

30/05/2014  
Date:

The above candidate has carried out research for the Masters thesis under my supervision.

I.

### *UOM Verified Signature*

Signature of the supervisor:

08/07/2014  
Date

## ABSTRACT

### **Secure Cloud: A Security Framework for organizations in implementing systems on the cloud**

Nalin de Abrew, Dept. of Electronic and Telecommunication Engineering

**Supervisor:** Dr. Ajith Pasqual

**Keywords:** Cloud computing, Security, Virtualiazation, Multi-tenanat, Software, Framework,

Over the last decade the cloud has created a major impact on the global IT ecosystem. Due to positive characteristics such as fast deployment, scalability, cost effectiveness and many more, cloud implementations are growing by the day. However security remains the number one barrier in cloud adoption for CIOs as per several surveys conducted on cloud adoption.

When considering the research done on cloud security, most have focused on the security dependency according to the cloud service model (IaaS, PaaS, SaaS), and the cloud deployment models(Public, Private, Hybrid, Community). Research has also been done on security issues inherent to cloud deployments and how to overcome them. The Cloud Security Alliance (CSA), one of the leading organizations on cloud security together with the IEEE as presented 12 domains of cloud security that should be focused on, six of the domains would be considered as the base guidelines.

The motivation behind this research was to provide a set of security guidelines and processes for local IT firms to adhere to when migrating to the cloud, in order to improve cloud adoption. The research was based on six domains of security provided by the CSA and security guidelines were developed along with the input of additional resources and security incidents.

A step by step process for security assessment and implementation are presented along with security risk assessment matrix that will aid an organization to decide which resources are to be migrated to the cloud. The main contribution from

this work is the development of the security matrix which will clear the doubts of many prospective cloud migrants.

## DEDICATION

To all who encouraged me to pursue my higher studies.

## ACKNOWLEDGEMENTS

I express my gratitude to my supervisor Dr. Ajith Pasqual who guided me through the research and put me on the right track.

I sincerely thank the lecturers of Moratuwa, especially Mr. Kithsiri Samarasinghe, Prof. Dileeka Dias and Dr. Chandika Wavegedera.

I am thankful to my fellow colleagues in the MSc batch who extended their support in many ways.

A special thank goes out to Anjula De Silva, who always open doors when I needed it the most.

And finally I wish to thank my family who has always been behind me throughout my higher studies.

# TABLE OF CONTENTS

DECLARATION .....	i
ABSTRACT.....	ii
DEDICATION .....	iv
ACKNOWLEDGEMENTS .....	v
TABLE OF CONTENTS.....	vi
LIST OF FIGURES .....	viii
LIST OF TABLES .....	ix
1 INTRODUCTION .....	1
1.1 Motivation for the Research .....	3
1.2 Objectives and Scope of Work.....	3
2 CLOUD COMPUTING.....	6
2.1 What is Cloud Computing.....	6
2.2 History and Milestones of Cloud Computing.....	8
2.2.1 Idea phase.....	8
2.2.2 Build up phase.....	9
2.2.3 Cloud phase.....	10
2.3 The Future of Cloud .....	11
2.4 Service Models .....	12
2.5 Deployment models.....	14
2.6 Techniques that have contributed the cloud computing technology .....	16
2.7 Benefits of cloud computing .....	16
2.8 Barriers to cloud computing.....	18
3 SECURITY IN THE CLOUD .....	19
3.1 The importance of security in cloud computing.....	19
3.1.1 Lack of control .....	19
3.1.2 Multi- tenancy .....	19
3.1.3 Physical location .....	20
3.2 Security Issue inherent to Cloud systems.....	20
3.3 Cloud Computing Top Threats.....	21
3.4 Evolution of Cloud Security.....	24
3.5 The Cloud Security Alliance .....	24
3.6 Domains of Cloud security by Cloud Security Alliance .....	25

3.7	Security Framework Scope.....	26
3.7.1	Topics of the security framework and Reasoning for the selection of domains	26
4	SECURITY FRAMEWORK FOR THE CLOUD .....	28
4.1	Information Management and Data Security .....	28
4.1.1	Information data security .....	29
4.1.2	Framework for Information management and data security .....	31
4.2	Incident Management .....	32
4.2.1	Preparation .....	33
4.2.2	Detection and Analysis .....	34
4.2.3	Containment and Recovery .....	34
4.2.4	Post Incident Management.....	35
4.2.5	Incident management security framework .....	35
4.3	Interoperability and Portability .....	36
4.3.1	Interoperability.....	36
4.3.2	Portability.....	36
4.3.3	How does interoperability and Portability affect Cloud Security? .....	37
4.3.4	Interoperability and Portability Security Framework .....	37
4.4	Availability and Disaster Recovery.....	38
4.4.1	Availability.....	38
4.4.2	Disaster recovery.....	39
4.4.3	Availability and Disaster Recovery Framework .....	41
4.5	Security as a Service.....	41
4.5.1	Security as a Service Security Framework.....	42
4.6	Application Security .....	42
4.6.1	Secure software development life cycle.....	43
4.6.2	Penetration testing .....	43
4.6.3	Monitoring Applications .....	44
4.6.4	Application security framework.....	44
4.7	Cloud Security Incident.....	45
4.7.1	Amazon EC2 Failure.....	45
4.8	Microsoft Azure outage.....	46
4.9	Cloud migration risk assessment model.....	48
4.9.1	Hypothetical Scenario 1 – XnovolIT IT Company .....	50



4.9.2	Hypothetical Scenario 2 – ABC Telecom Operator.....	53
4.10	Step by Step Security Framework Application to Cloud Adoption .....	58
5	RESULTS .....	62
5.1	Risk Assessment matrix .....	62
5.2	Step by Step Security Framework Application to a Cloud Adoption .....	63
6	CONCLUSION AND FUTURE WORK .....	64
6.1	CONCLUSION .....	64
6.2	FUTURE WORK .....	64
7	REFERENCES .....	65

## LIST OF FIGURES

Figure 1.1	: Barriers to Cloud Adoption .....	1
Figure 1.2	: Regional interest of cloud computing.....	2
Figure 2.1	: Cloud computing model .....	7
Figure 2.2	: Cloud evolution phases.....	8
Figure 2.3	: Cloud Computing search trend via google trends .....	11
Figure 2.4	: Cloud service models.....	12
Figure 2.5	: Cloud service model layers.....	13
Figure 2.6	: Cloud Taxonomy via OpenCrowd.....	14
Figure 2.7	: Cloud Deployment Models.....	15
Figure 2.8	: Properties of different types of cloud .....	16
Figure 4.1	: Data security classification.....	28
Figure 4.2	: End to End data security on the cloud .....	29
Figure 4.3	: Incident Management Cycle.....	33
Figure 4.4	: Separate Cloud service provider on hot standby .....	40
Figure 4.5	: Transfer local backup to new cloud service provider.....	41
Figure 5.1	: Security Framework application process.....	63

## LIST OF TABLES

Table 2-1: Cloud service providers and the provided resource.....	7
Table 4-1: Data Security Framework.....	32
Table 4-2 : Incident management security Framework .....	35
Table 4-3 : Interoperability and Portability Framework .....	38
Table 4-4 : Availability and Disaster Recovery.....	41
Table 4-5 : Security as a Service Security Framework.....	42
Table 4-6 : Application Security Framework .....	44
Table 4-7 : Availability Risk Matrix.....	49
Table 4-8 : Data Risk Matrix .....	49
Table 4-9 : Asset List XnovoIT .....	50
Table 4-10 : Asset Unavailability Impact - XnovoIT .....	51
Table 4-11 : Asset Data impact - XnovoIT.....	52
Table 4-12 : XnovoIT Risk Assesment.....	53
Table 4-13 : IT Assets - ABC Telco .....	54
Table 4-14 : Unavailability Impact - ABC Telecom.....	55
Table 4-15 : Data Impact - ABC Telecom.....	56
Table 4-16 : ABC Telecom Risk Assesment .....	57
Table 5-7 : Availability Risk Matrix.....	62
Table 5-8 : Data Risk Matrix .....	62