



Data Security Related Study in Multi-Tenancy Cloud Computing

J.Jeyaweera

(Reg. No.: MS20906030)

M.Sc. in IT

Specialized in Information Technology

Supervisor: Assist. Professor Dr. Windhya Rankothge

December 2021

**Department of Information Technology
Faculty of Graduate Studies and Research
Sri Lanka Institute of Information Technology**

Table of Contents

Table of Contents	2
List of Figures	5
List of Abbreviations	6
Abstract	7
Chapter 1	8
Introduction	8
Contents	8
1.1. Chapter Overview	9
1.2 Problem Domain	9
1.3 Resource Requirements	10
1.3.1 Hardware requirements	10
1.3.2 Software Requirement	11
1.4 Project Document Structure	11
Chapter 2 - Research question	11
Chapter 3 - Research Objectives	11
Chapter 4 - Literature review	11
Chapter 5 - Methodology	11
Chapter 6 - Timeline	12
1.5 Chapter Summary	12
Chapter 2	13
Research Question	13
Contents	13
2.1 Chapter Overview	14
2.2 Project Aim	14
2.3 Research Questions	14
2.4 Chapter Summary	14
Chapter 3	15
Literature Review	15
Contents	15
3.1 Chapter Overview	16
3.2 Literature Review	16
3.2.1 Empirical literature	18

3.2.1.1 Multi-Tenancy Generic ideology	18
3.2.1.2 Cloud computing aspect of Multi-Tenancy	19
3.2.1.3 The Policy of ENISA	21
3.2.2 Theoretical literature	24
3.2.2.1 Cloud Deployment Models	24
3.2.2.2 Types of Service models.....	26
3.2.2.3 OpenStack Architecture	28
3.2.2.4 Multi tenancy Tree.....	28
Chapter 4.....	37
Research Objectives.....	37
Contents.....	37
4.1 Chapter Overview	38
4.2 Research Main Objectives.....	38
4.3 Sub Objectives.....	38
Chapter 5.....	39
Research Methodology	39
Contents.....	39
5.1 Chapter Overview	40
5.2 Overview of the methodology	40
5.2.1 Different problems and attacks on the Cloud.....	40
5.2.1.1 SQL injection attacks.....	41
5.2.1.2 The Path Traversal attack.....	41
5.2.2 Cloud Simulators	41
5.2.2.1 Zed Attack Proxy (ZAP).....	42
5.2.2.2 Process of Simulation.....	42
5.2.2.3 Research outcome	44
Chapter 6.....	46
Timeline	46
Contents.....	46
6.1 Chapter Overview	47
6.2 Working Plan	47
6.3 Time Schedule	47
Chapter 7.....	48
Discussion and Conclusion.....	48

Appendix 1.....49
References.....53

List of Figures

Figure 1 General overview of Multi-tenancy Cloud Architecture [37]	32
Figure 2 Overview of Architectural explanation for multi-tenancy [37].....	34
Figure 3 Traditional network attack and Multi-tenancy Attack [37]	35
Figure 4 - process of simulation I	42
Figure 5 Process of Simulation II.....	43
Figure 6 Process of Simulation III.....	43
Figure 7 Process of Simulation IV.....	44
Figure 8 Results of the simulation attack I.....	44
Figure 9-Results of the simulation attack II	45

List of Abbreviations

NIST - National Institute of Standards and Technology

AWS - Amazon Web Service

MS - Microsoft Azure

ENISA - European Union Agency for Network and Information Security

ICT - Information and Communications Technology

CA – Cloud Providers

Abstract

Cloud Computing is one of the major concepts of the computing model, in the Industry of Information technology. It has enabled many optimized services on-demand computing. There are many benefits for cloud services consumers. Multi-Tenancy cloud environment, which is a part of them and on the other hand, biggest challenges are security and privacy concerns. This proposal covers some of the security issues and the challenges of Multi-Tenancy. In Cloud computing, the risk that refers to where the resource sharing and it entails in terms of privacy and reliability could be despoiled and this could consider as a security issue. Specially, The SaaS model, which is a promising technology and it, grows each year in high demand. However, at the security level, there are many hindrances, and becomes a major problematic against its adoption. Therefore, there must be effective security solutions and strategies need to be proposed to have a good understanding of attack vectors and attack exteriors. This paper discussed several types of attacks, also how to prevent those, and finally, the recommendations for a multi-tenancy environment.

Keywords: Cloud Computing, Multi-tenancy, Attacks, Simulation, Data security, Data privacy, etc.