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

List of Figures

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.