

**ENHANCED CLOUD SECURITY AND COMPLIANCE REFERENCE
MODEL FOR EMERGING SAAS CLOUD SYSTEMS CONSUMING
PUBLIC CLOUD SERVICES**

Palamandadige Ravindu Nirmal Fernando

(199320K)

CS6997 – MSc Research Project

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

June 2022

DECLARATION

I declare that this is my own work and this thesis 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

Candidate Signature:

(P.R.N Fernando)

Date: 14-06-2022

I certify that the declaration above by the candidate is accurate to the best of my knowledge and that this report is acceptable for evaluation for the CS6997 – MSc Research Project.

UOM Verified Signature

Supervisor Signature: .

(Dr. Shantha Fernando)

Date

16-06-20 22

ABSTRACT

Most businesses in operation at present have an online presence. This ranges from an E-Commerce application to a business that offers NoSQL database capabilities as a service to its customers. With the inception of cloud computing, consumers started aligning with a service model to obtain cloud computing services. Cloud computing service models fall under three main categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Many businesses, especially technologically driven startups, emerge by leveraging cloud service models. Most of those emerging businesses started to offer their services as a Software as a Service model. The growth of this trend has brought up new challenges for emerging startup businesses in managing the security, compliance and privacy of their services. Compliance and privacy have been popular among cloud consumers, cloud service providers, and governments worldwide. Governments have already started taking continuous initiatives to ensure the cloud-based software services comply with the standards, and the users' privacy is guaranteed in the cloud services offered. These regulations are compulsory for a cloud business to exist in most places. If this is addressed from the perspective of an emerging SaaS business, keeping up with rapidly changing complex compliance standards and privacy regulations while making the cloud services secure has been a difficult task.

This research mainly focuses on identifying methods for creating a threat model for SaaS cloud systems and determining how cloud security and compliance make a SaaS cloud system consuming public cloud services secure and compliant. Based on that, the research proposes an enhanced reference model that consists of patterns and best practices for designing and implementing a safe, compliant SaaS cloud system. Mapping of major categories within that reference model with existing cloud security and compliance standards was also carried out to make the proposed model more relatable to the real world. An implementation phase was conducted to showcase how this proposed model can be successfully applied to the real world. This included two major components: a machine learning model and an API service. The implemented API service allows users to retrieve insights and recommendations about their SaaS system security and compliance status by responding to audit questions. The insights and recommendations were generated based on clusters identified via the implemented machine learning models. The data required to develop the machine learning model were gathered by conducting an open survey among IT professionals working or with experience working at cloud-based software solutions offering companies in Sri Lanka, the majority being startups.

This overall process paved the way for answering the research objectives while creating a solid implementation that enabled continuous and active evolution of the proposed reference model.

Keywords: cloud computing, cloud security, cloud compliance, emerging cloud businesses, SaaS cloud systems

ACKNOWLEDGMENT

The success of this thesis depended a lot on the continuous support and guidance I received from many people. I'm incredibly privileged to have gotten this all-amazing support along with the completion of this MSc research project thesis.

I wish to thank Dr. Shahani Markus for providing me with the first insight into the main idea of this thesis and providing her guidance to make the completion of the thesis successful. I would also like to extend my sincere gratitude to Dr. Rashmika Nawarathne for his immense support for the implementation phase of this research. I would like to express my appreciation to Mr. Andun Sameera Liyagunwardana and Mr. Sachintha Rajith, my managers at Emojot (Pvt) Limited, for always supporting me and guidance in the completion of this thesis.

I owe my deep gratitude to Dr. Shantha Fernando for accepting my research title and the continuous guidance and necessary information to complete this thesis and research.

Finally, I would like to extend my deep gratitude specially to my family and friends who were always there for me and provided their full support in this endeavor.

TABLE OF CONTENTS

DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGMENT	iii
TABLE OF CONTENTS	iv
LIST OF FIGURES	vii
LIST OF TABLES	ix
LIST OF ABBREVIATIONS	xi
1 – INTRODUCTION	1
1.1 – Background	1
1.2 – Cloud Security and Regulatory Compliance Standards	1
1.3 – Problems related to cloud security and compliance standards for emerging SaaS businesses consuming public cloud services	2
1.4 - Research Problem	2
1.5 - Research Question	3
1.6 – Research Objectives	4
1.7 – Thesis Outline	5
2 - LITERATURE REVIEW	6
2.1 – Cloud Threat Modelling	6
2.2 – Security Threats for SaaS Cloud Systems	8
2.3 – Cloud Security Controls for SaaS Cloud Systems	11
2.4 – Cloud Regulatory Compliance Standards and frameworks for SaaS Cloud Systems	12
2.5 – Mapping between Cloud Threats and Cloud Regulatory Compliance Standards for SaaS Cloud Systems	16
2.6 – Reference Models on Cloud Security and Cloud Compliance	19
2.7 – Literature review related to the implementation phase	21
2.8 – Conclusive Remarks	23
3 – METHODOLOGY	24
3.1 – STRIDE-LM+ - An Optimized Threat Modelling Approach for Emerging SaaS Businesses consuming public cloud services	25
3.2 – Threat Analysis on CSA’s top threats using the STRIDE-LM+ threat model ...	29
3.3 – Enhanced Cloud Security and Compliance Reference Model for Emerging SaaS Cloud Systems consuming public cloud services	34

3.4 – Major Components of the Proposed Model.....	36
3.4.1 – Step 1 - Identify SaaS Business Domain	36
3.4.2 – Step 2 – Assessment on Public Cloud Service Provider	36
3.4.3 – Step 3 – Assessment on SaaS Cloud System Resources.....	37
3.5 – Mapping between the proposed reference model and CSA CCM (Cloud Control Matrix) domains	39
3.5.1 – Selection of the most critical cloud controls from the CSA CCM domains depending on the identifications of the latest top cloud threats publication	40
3.5.2 – Mapping of CSA CCM domains with the proposed reference model	41
3.6 – Conclusive Remarks	43
4 – IMPLEMENTATION	44
4.1 – Implementation of the machine learning model	45
4.1.1 – Data collection and organization	45
4.1.2 – Feature selection for the machine learning model	49
4.1.3 – Selection of machine learning type and the algorithm.....	51
4.1.4 – Data Preprocessing.....	52
4.1.5 – Selection of technologies/ tools	52
4.1.6 – Final Implementation	53
4.2 - Implementation of the API service.....	72
4.2.1 – High-level architecture of the API service implementation	73
4.2.2 – Selection of technologies/ tools	74
4.2.3 – API service source code and database schema analysis	75
4.2.4 – API service contract	84
4.3 – Mapping of the core components of the proposed reference model with the NIST 800-53 R5	111
4.4 – Conclusive Remarks	111
5 – ANALYSIS AND FINDINGS	113
5.1 – Analysis	113
5.2 – Survey result findings	152
5.2.1 – Intro Questionnaire	152
5.2.2 – Assessing SaaS Business Domain	154
5.2.1 – Assessing the Cloud Service Provider	156
5.3 – Benchmark between existing cloud security models and proposed models	158
5.4 – Limitations identified in the research	161
5.5 – Conclusive remarks	161
6 – CONCLUSION	163
6.1 – Future Work	164
REFERENCES.....	166
APPENDICES	172
Appendix A - Mapping between the latest CSA top most cloud threats and the CSA Cloud control domains	172
Appendix B – Generic Survey Question Set	185

Appendix C - Mapping between the survey questions under Assessing SaaS Cloud system resources to each subcategory within Step 3 of the proposed reference model	186
Appendix D – Category A Governance Dataset Cluster Breakdown	191
Appendix E - Category A Operations Dataset Cluster Breakdown	194
Appendix F - Category B Governance Dataset Cluster Breakdown	197
Appendix G - Category B Operations Dataset Cluster Breakdown	201
Appendix H - Category C Governance Dataset Cluster Breakdown	205
Appendix I - Category C Operations Dataset Cluster Breakdown	209
Appendix J - Category D Governance Dataset Cluster Breakdown	212
Appendix K - Category D Operations Dataset Cluster Breakdown	216
Appendix L – Mapping between the proposed model and the NIST 800 53 R5 Standard.....	220
Appendix M – Source Code and Training Data set dump	229

LIST OF FIGURES

Figure 1 – Distribution of publications by threats and domains	9
Figure 2 – A simple cloud security process model	20
Figure 3 – Proposed reference model	35
Figure 4 – Assessment on Saas cloud system - Sub process	35
Figure 5 – Step-by-step process involved in the creation of correlation between the CSA CCM domains and the question set under each domain	47
Figure 6 – Component breakdown flow in the feature categorization process	50
Figure 7 – ML code analysis - Import the required libraries	54
Figure 8 – ML code analysis – Reading and conversion of the training data set	54
Figure 9 – ML code analysis – Training data set inspection	54
Figure 10 – ML code analysis – Data pre-processing	54
Figure 11 – ML code analysis – Calculation of cost for a range of k values	55
Figure 12 – ML code analysis – Plotting the cost function to a range of k values	55
Figure 13 – ML code analysis – KModes clustering	55
Figure 14 – ML code analysis – Appending of cluster values to the original data frame	55
Figure 15 – Elbow method for optimal k – Category A Governance	56
Figure 16 – Elbow method for optimal k – Category A Operations	57
Figure 17 – Elbow method for optimal k – Category B Governance	58
Figure 18 – Elbow method for optimal k – Category B Operations	59
Figure 19 – Elbow method for optimal k – Category C Governance	60
Figure 20 – Elbow method for optimal k – Category C Operations	61
Figure 21 – Elbow method for optimal k – Category D Governance	62
Figure 22 – Elbow method for optimal k – Category D Operations	63
Figure 23 – High-Level Architecture of API Service	73

Figure 24 – Sequence diagram of API Service	73
Figure 25 – Survey – Type of SaaS business	153
Figure 26 – Survey – Number of employees	153
Figure 27 – Survey – Job area	154
Figure 28 – Survey – Job levels	154
Figure 29 – Survey – SaaS business domains	155
Figure 30 – Survey – Geographical locations of the customers	155
Figure 31 – Survey – Regulatory compliance standards awareness	156
Figure 32 – Survey – Cloud deployment method used by the SaaS platform	156
Figure 33 – Survey – CSP consumed by the SaaS platform	157
Figure 34 – Survey – Shared responsibility awareness	157

LIST OF TABLES

Table 1 – Cloud security compliance standards and remarks	13
Table 2 – Recommendations for security compliance model based on security threats that are presented in [9, Tab. 1]	17
Table 3 – Responsibilities of Cloud Consumers and Cloud Providers - Presented in [28, Tab. 1]	18
Table 4 - Summary of STRIDELM+ threat modelling	25
Table 5 - Threat Analysis Using STRIDELM+ threat model On CSA’s top threats to Cloud Computing - The Egregious 11	29
Table 6 - Mapping between categories within the Assessing SaaS Cloud System Resources step of the proposed reference model with CSA CCM domains	43
Table 7 – Mapping between subcategories under Assessing SaaS Cloud Resources with individual question ids	49
Table 8 – Python libraries used and their use cases	53
Table 9 – API details for Category A – Governance	84
Table 10 – API response details For Category A – Governance	84
Table 11 – API Details for Category A – Operations	87
Table 12 – API response details for Category A – Operations	88
Table 13 – API details for Category B – Governance	91
Table 14 – API response details for Category B – Governance	92
Table 15 – API details for Category B – Operations	94
Table 16 – API response details for Category B – Operations	95
Table 17 – API details for Category C – Governance	97
Table 18 – API response details for Category B – Operations	98
Table 19 – API details for Category C – Operations	101
Table 20 – API response details for Category C – Operations	101
Table 21 – API details for Category D – Governance	104

Table 22 – API response details for Category D – Governance	105
Table 23 – API details for Category D – Operations	108
Table 24 – API response details for Category D – Operations	108
Table 25 – Test scenario analysis of the implementation	114
Table 26 – Benchmarking between proposed model and the reviewed models	159

LIST OF ABBREVIATIONS

AAC	Audit Assurance And Compliance
AIS	Application And Interface Security
BCR	Business Continuity Management & Operational Resilience
BPASS	Business Process As A Service
CAIQ	Consensus Assessments Initiative Questionnaire
Cat A – Gov	Category A – Governance
Cat A – Ops	Category A – Operations
Cat B – Gov	Category B – Governance
Cat B – Ops	CATEGORY B – Operations
Cat C – Gov	CATEGORY C – Governance
Cat C – Ops	Category C – Operations
Cat D – Gov	Category D – Governance
Cat D – Ops	CATEGORY D – Operations
CCC	Change Control & Configuration Management
CCM	Cloud Control Matrix
CCPA	California Consumer Privacy Act
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DCS	Data Center Security
DMTF-CADF	Data Format And Interface Definitions Specification – Cloud Auditing
Data Federation	
DSI	Data Security & Information Lifecycle Management
EDRM	Electronic Discovery Reference Model
EKM	Encryption & Key Management
EU	European Union
FEDRAMP	Federal Risk And Authorization Management Program
GDPR	General Data Protection Regulation
GRM	Governance & Risk Management
GSOM	Growing Self Organizing Maps
HIPAA	Health Insurance Portability And Accountability Act
HRS	Human Resources Security
IAAS	Infrastructure As A Service
IAM	Identity & Access Management
IPY	Interoperability & Portability
ISO	International Standards Organization
IVS	Infrastructure & Virtualization Security
MOS	Mobile Security
MPAA	Motion Picture Association Of America
NIST	National Institute Of Standards And Technology
OSWAP	Open Web Application Security Project
PAAS	Platform As A Service
PCI SSC	Payment Card Industry Security Standards Council
SAAS	Software As A Service
SDLC	Software Development Life Cycle
SEF	Security Incident Management, E-Disc & Cloud Forensics
SOC	Service Organization Control
SOM	Self Organizing Maps

SOX
STIG
TVM

Sarbanes–Oxley Act
Security Technical Implementation Guide
Threat & Vulnerability Management