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).

Candidate Signature: *UOM Verified 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.

Supervisor Signature: . *UOM Verified Signature*

(Dr. Shantha Fernando)

Date 16-06-2022

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 evolvement 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

LIST OF FIGURES

LIST OF TABLES

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