A MODEL FRAMEWORK FOR MANAGING CYBER SECURITY CHALLENGES FACED BY CLOUD-BASED SMALL IT FIRMS

Munasinghe Arachchige Nadeesha Tharika Sewwandi

219406J

MSc in Computer Science Specialising in Security Engineering

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

May 2025

A MODEL FRAMEWORK FOR MANAGING CYBER SECURITY CHALLENGES FACED BY CLOUD-BASED SMALL IT FIRMS

Munasinghe Arachchige Nadeesha Tharika Sewwandi

219406J

Thesis/Dissertation submitted in partial fulfillment of the requirements for the degree MSc in Computer Science Specialising in Security Engineering

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

May 2025

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. I retain the right to use this content in whole or part in future works (such as articles or books).

27/05/2025

Signature: Date:

The above candidate has carried out research for the Masters thesis under my supervision. I confirm that the declaration made above by the student is true and correct.

Name of Supervisor: Prof. Shantha Fernando

Signature of the Supervisor: Date: 2025-05-27

ACKNOWLEDGEMENT

I would like to acknowledge and express my sincere gratitude to the following individuals who supported me to make this work possible. Their direction and advice carried me through all the stages of writing my project.

I am grateful to University of Moratuwa, Sri Lanka for providing me with the necessary resources and facilities to complete this project.

My supervisor, Dr. Shantha Fernando, for providing the valuable guidance and response throughout the course of my research.

I am grateful to all the small IT firms who send their valuable responses to complete this project.

Last but not least, I have to mention the care and encouragement of my family and friends. Their support was invaluable throughout my studies.

ABSTRACT

Security threats and other cyber security-related concerns are becoming more prevalent in the business world. Small-to-medium-sized organizations are frequently targeted by attackers, and some find it challenging to withstand such attacks. Due to a lack of experience and the high cost of security solutions, small IT firms frequently encounter difficulties when setting up and implementing security measures. Hence, small IT firms and its stake holders are required to acknowledge the risk of cyber threats and continue their businesses without having a proper solution for their security related issues. The researcher conducted a comprehensive survey that focuses on the requirement of technical implementation of several cyber security controls for cloud-based small IT firms in accordance with this particular research. The survey encompassed a range of questions including existing cloud security controls, policies and procedures, access control and authentication mechanisms, cryptographic controls, password security, employee security awareness, incident response, security assessments and digital forensic, which helps to identify and understand overall organizations' operational structure and its business environment with the requirement for cybersecurity. The survey was sent to the small IT firms who is handling healthcare business systems and the small IT firms who is handling retail business systems. The information collected was thoroughly reviewed and visualized to identify security related challenges for cloud based small IT firms. Based on the identified security requirements of different kind of businesses, a framework was implemented to build small IT firms' security infrastructure using feasible open-source solutions. The most suitable open-source solutions were selected based on the type of the organization, types of the data collected, existing IT infrastructure, etc. The attributes of the framework ought to be cost effectiveness and user friendliness.

Keywords: Small IT firms, Cyber Security Framework, Open-source tools for Cyber Security

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Description** **Page**

LIST OF TABLES

Table **Description** **Page**

LIST OF ABBREVIATIONS

Abbreviation	Description
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
C5	Cloud Computing Compliance Control Catalog
CI/CD	Continuous Integration and Continuous Deployment
COVID-19	Coronavirus disease 2019
CPU	Central Processing Unit
CSA Cloud Controls Matrix (CCM)	Cloud Security Alliance Cloud Controls Matrix
FedRAMP	Federal Risk Authorization Management Program
GB	Giga Byte
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HIPAA	Health Insurance Portability and Accountability Act
HMAC	Hash-based Message Authentication Code
HR	Human Resources
HTTPS	Hyper Text Transfer Protocol Secure
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO/IEC 27001	International Organization for Standardization/ International Electrotechnical Commission 27001
IT	Information Technology
JWT	Json Web Token
MFA	Multi Factor Authentication
ML	Machine Learning
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework

NIST SP 800-53	National Institute of Standards and Technology Special Publication 800-53
NISTIR 7621	National Institute of Standards and Technology Interagency Report 7621
OS	Operating System
OSINT	Open-Source Intelligence
PCI DSS	Payment Card Industry Data Security Standard
PCI DSS	Payment Card Industry Data Security Standard
RAM	Random Access Memory
RBAC	Role Based Access Control
SIEM	Security Information and Event Management
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
Wi-Fi	Wireless Fidelity

LIST OF APPENDICES