

LB/TH/43/2025

TH6013

**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

Declaration	i
Acknowledgement.....	ii
Abstract	iii
Table of Contents	iv
List of Figures	vi
List of Tables.....	vii
List of Abbreviations.....	viii
List of Appendices	x
Chapter 1	1
INTRODUCTION	1
1.1. Background	1
1.2. Motivation and Research Problem	3
1.3. Research Questions	5
1.4. Research Objectives	5
1.4.1. Main Objectives	6
1.4.2. Specific Objectives.....	7
1.5. Thesis Outline.....	8
Chapter 2	10
LITERATURE REVIEW.....	10
2.1 Gaps Among the Existing Security Standards	10
2.1.1 Disconnection between Conceptual Models and Real-World Applications	10
2.1.2 Inadequate Cybersecurity Frameworks Created for Small IT Firms .	11
2.2 Suggested Frameworks by Previous Researchers	12
2.2.1 Cloud Performance and Security Alignment based Cybersecurity Frameworks.....	12
2.2.2 Cybersecurity Frameworks Designed for Small IT Firms	15
2.2.3 Cybersecurity Framework for Cloud-based Systems.....	18
2.3 Open-Source Tools for Implementing Security	21

2.3.1	The benefits of open source for SMEs in terms of strategy and operations.....	21
2.3.2	Empirical Evidence for Real-World Application in SMEs.....	22
2.3.3	Validating End-to-End Open-Source Integration with Conceptual Frameworks.....	23
2.4	Conclusive remarks	24
Chapter 3		25
FRAMEWORK AND RESEARCH METHODOLOGY		25
3.1	Data Collection.....	26
3.2	Implementation of the Model Framework.....	42
3.2.1	Analyzing Tools for Features and Compatibility.....	46
3.2.2	Dataset Preparation: Open-Source Tools	53
3.2.3	Implementation of the Machine Learning Technique.....	55
3.2.4	Implementation of the Tool Catalogue	62
3.2.5	Final Product	67
3.3	Chapter Summary.....	70
Chapter 4.....		71
RESULTS AND DISCUSSION		71
4.1	Analysis of Responses Collected Through the Survey.....	72
4.2	Evaluation of the recommendation system	74
4.3	Discussion	80
4.3.1	Features and Benefits of the Model Framework.....	81
4.3.2	Success of the Model Framework.....	81
4.3.3	Efficiency Comparison.....	82
4.4	Chapter Summary.....	83
Chapter 5.....		84
CONCLUSIONS AND FURTHER RESEARCH AREAS		84
5.1	Introduction	84
5.2	Conclusions	84
5.3	Limitations and Further Research Areas	86
REFERENCES.....		88
APPENDICES		96

LIST OF FIGURES

Figure	Description	Page
Figure 1:	Impact of cyber-attacks on small businesses in 2022[21][22]	1
Figure 2:	Security domains in the existing security frameworks [24]	11
Figure 3:	Agent based cyber security framework for cloud environment [27].....	13
Figure 4:	A conceptual Framework for Managing the Cloud Security [11]	14
Figure 5:	Risk Management and Investment Cost Analysis Framework [20]	16
Figure 6:	CODCSSSB [29]	17
Figure 7:	Cyber security framework for cloud-based enterprise level organizations [33]	19
Figure 8:	Research Methodology	25
Figure 9:	Implementation Strategy of the Filtering Mechanism	55
Figure 10:	User Requirements Gathering Form	57
Figure 11:	Client Profile	59
Figure 12:	Download section on the Framework	66
Figure 13:	Product Architecture	68
Figure 14:	Suggested Tools List from the Recommendation System	69
Figure 15:	Tool Catalogue Preview	70
Figure 16:	Cybersecurity Challenges in Small IT Firms	73
Figure 17:	Feedback Form	74
Figure 18:	Feedback Form for Unsatisfied Responses	75

LIST OF TABLES

Table	Description	Page
Table 1:	Used Virtual Machine Information for Tool Analysis.....	47
Table 2:	Short Forms for Requirements.....	76
Table 3:	Responses of the User 1	77
Table 4:	Precision at K Value for Collected Responses	79
Table 5:	Efficiency Comparison of the Framework.....	82

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

Appendix	Description	Page
Appendix – A	Dataset.....	96
Appendix - B	Evaluation Results of the Recommendation System..	107
Appendix – C	Tool Catalogue.....	109