
CONTENTS

APPROVAL	ii
SELF DECLARATION AGAINST PLAGIARISM	iii
ABSTRACT	iv
ABSTRAK	v
DEDICATION	vi
ACKNOWLEDGMENTS	vii
CONTENTS	viii
LIST OF TABLES	x
LIST OF FIGURES	xi
LIST OF TERMS	xii
1 INTRODUCTION	1
1.1 Rationale	1
1.2 Statement of the Problem	3
1.3 Objective and Hypotheses	4
1.4 Scope and Delimitation	4
1.5 Significance of the Study	5
2 REVIEW OF LITERATURE AND STUDIES	6
2.1 Related Literatures	6
2.1.1 Dynamic Analysis	6
2.1.2 Random Forest	6
2.1.3 Support Vector Machine	6
2.1.4 Naive Bayes	7
2.1.5 n-Gram	7
2.1.6 Term Frequency-Inverse Document Frequency (TF-IDF)	7
2.1.7 Performance Evaluation	8
2.2 Related Studies	9
3 RESEARCH METHODOLOGY	13
3.1 Research Design	13
3.1.1 Problem Identification	13

3.1.2	Method Requirement Specification	14
3.1.3	Data Collection	14
3.1.4	Model Training and Evaluation Process	16
3.1.5	Proposed Response Time Detection Architecture	17
3.1.6	Analyze the result	17
3.2	Proposed Response Time Detection Architecture	17
3.2.1	Determination of Threshold Value	17
3.2.2	Determination Based on the Number of Windows	17
3.3	Tools for Data Analysis	18
4	PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA	22
4.1	Presentation of Data	22
4.2	Analysis of the Data	22
4.2.1	Performance Analysis Using n-gram on API Call Response Time Detection Dataset	23
4.2.2	Performance Analysis Using n-gram on System Call by Dib and Dabri (2022)	27
4.3	Analysis of Response Time Detection Windows	29
4.3.1	Dataset Response Time Detection	29
4.3.2	Dataset System Call by Dib and Dabri [11]	33
4.4	Execution Time of Response Time Windowing Framework	36
4.5	Identification of Distinct APIs in Ransomware and Benign Programs	36
4.6	Comparison with Related Work	41
4.7	Summary of Findings	42
5	CONCLUSION AND RECOMMENDATIONS	44
5.1	Conclusions	44
5.2	Recommendations	45
	BIBLIOGRAPHY	46
	Appendices	49