

CONTENTS

APPROVAL PAGE.....	i
SELF DECLARATION AGAINST PLAGIARISM.....	ii
ABSTRACT	iii
DEDICATION	iv
ACKNOWLEDGMENTS	v
CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES.....	x
LIST OF ABBREVIATION	xi
CHAPTER 1.....	1
THE PROBLEM	1
1.1 Rationale.....	1
1.2 Theoretical Framework	5
1.3 Conceptual Framework/Paradigm	7
1.4 Statement of the Problem	9
1.5 Hypothesis	9
1.6 Assumption.....	10
1.7 Scope and Delimitation.....	11
1.8 Importance of the Study	12
CHAPTER 2.....	12
REVIEW OF LITERATURE AND STUDIES	12
2.1 Machine Learning in Network Intrusion Detection.....	14
2.2 Feature Resampling using Random Oversampling	14
2.3 Selection Feature Embedded using Random forest with PCA.....	15
2.4 Stucking Feature Embedded using Clustering.....	15
2.5 Feature Extraction using PCA	16

2.6	Decision Tree (DT).....	16
2.7	Logistic Regression	17
2.8	K-Nearest Neighbor (KNN)	18
2.9	Naïve Bayes (NB).....	18
2.10	Random Forest	19
CHAPTER 3.....		17
RESEARCH METHODOLOGY		17
3.1	Research Methods	20
3.2	System Model.....	22
3.3	Dataset	24
3.4	System Flowchart	26
3.5	Testing Scenarios and Parameters	27
3.6	Implementation.....	30
CHAPTER 4.....		35
DATA PRESENTATION AND ANALYSIS		35
4.1	Results of UNSW-NB15 Dataset	35
4.2	Results of CIC-IDS-2017 Dataset	48
4.3	Results of CIC-IDS-2019 Dataset	64
CHAPTER 5.....		60
CONCLUSIONS AND RECOMMENDATIONS.....		60
5.1	Conclusions	78
5.2	Recommendations	78
REFERENCES		78