CONTENTS

Contents i
List of figures v
List of Tables vii
List of Equations ix
CHAPTER I 12
INTRODUCTION 12
1.1 Background 12
1.1.1 The Growth of IoTs and Attack Challenges 12
1.1.2 Attacks Detection Systems 13
1.2 Related Works 14
1.2.1 Traditional Detection System 14
1.2.2 Detection System in IoT Environment 15
1.2.3 Detection System on Resource Constraint Devices 15
1.2.4 Public Detection System 16
1.3 Challenging Issues 16
1.4 Problem Statement 18
1.5 Overview of the Thesis 18
1.6 Research Purposes 21
1.7 Benefits of Research 22
1.8 Contributions 22
1.9 Organization of the Thesis 23
CHAPTER II 25
THEORETICAL BACKGROUND AND LITERATURE REVIEW 25
2.1 IoT, Challenges and Attacks 25
2.1.1 IoT Architecture 25

2.1.2 IoT Environment and Its Applications 26
2.1.3 The Challenges of IoT devices 27
2.1.4 Attacks in IoT 29
2.2 Theoretical Background 30
2.2.1 Intrusion Detection System 32
(i) *Misused-Based Detection* 35
(ii) *Anomaly-Based Detection* 38
(iiI) *Machine Learning-Based Detection* 40
2.2.2 Machine Learning Algorithms 40
(i) *Tree-Based Algorithms* 41
(ii) Naïve Bayes 46
(III) Artificial Neural Network (ANN) 46
2.2.3 Feature Selection 57
(I) GAIN-RATIO 62
(II) CORRELATION-BASED FEATURE SELECTION (CFS) 63
2.3 Review of Literature 65
2.3.1 IDS in Conventional Network 68
(I) Misused-Based IDS 68
(II) Anomaly-Based IDS 69
2.3.2 IDS in IoT Environments 71
2.3 Research Questions 79
CHAPTER III 80
RESEARCH METHODOLOGY 80
3.1 Equipment and Materials 80
3.2 The Course of Study 82
3.2.1 Data Collection and Analysis 83
3.2.2 Methods 87
(i) Feature Transformation and Normalization 88

(ii) Correlated-Set Thresholding on Gain-Ratio (CST-GR) 89
(iii) Detection 91
3.2.3 System Design and Implementation 93
(i) System Design 93
(ii) Implementation for Attack Detection 96
3.2.4 Evaluation Methods 98
(i) Confusion Matrix 98
(ii) Evaluation Metrics 99
(iii) CPU & Memory Performance 101
CHAPTER IV 102
EXPERIMENTAL RESULTS 102
4.1 The Selected Features from Datasets 103
4.1.1 UNSW-NB15 103
4.1.2 Bot-IoT 106
4.1.3 Observations 108
4.2 Detection Performance 110
4.2.1 Experiment - 1 110
4.2.2 Experiment - 2 115
4.2.3 The Performance of Device 118
4.2.4 Observations 121
4.3 Performance Comparisons 123
CHAPTER V 125
DISCUSSION 125
5.1 Attack Detection Architecture 125
5.2 Feature Selection Approach 126
5.3 Contributions 131
CHAPTER VI 136
Conclusion 136

6.1 Conclusion 136
6.2 Limitation and Future Works 138
REFERENCES.....140
INDEX.....153