

CONTENTS

APPROVAL PAGE

SELF DECLARATION AGAINST PLAGIARISM

ABSTRACT i

ACKNOWLEDGMENTS ii

PREFACE iv

CONTENTS v

LIST OF FIGURES vii

LIST OF TABLES viii

LIST OF ABBREVIATION ix

I INTRODUCTION 1

1.1	Background	1
1.2	Problem Identification	2
1.3	Research Objective	2
1.4	Scope of Work	3
1.5	Hypothesis	3
1.6	Methodology	3
1.7	Research Methodology	4
1.8	Research Timeline	4

II BASIC CONCEPTS 6

2.1	State of the Art in Key Exchange for IoT-Based Early Warning Sys- tems	6
2.2	The EWS in IoT Concepts	8
2.3	Identity Based Encryption (IBE)	9
2.4	Hierarchical Identity Based Encryption (HIBE)	10
2.5	Boneh-Boyen Hierarchical Identity Based Encryption (BB-HIBE) Scheme	11

2.5.1	Illustrative Examples of BB-HIBE Equations	12
III	SYSTEM MODEL AND RESEARCH DESIGN	14
3.1	System Model	14
3.2	Attack Models	15
3.3	Simulation Environment and Workflow	16
3.4	Simulation Scenarios and Parameters	19
IV	PERFORMANCE EVALUATIONS	21
4.1	Comparison of Communication Overhead between TLS/ECDH and BB-HIBE	22
4.2	Comparison of Total Key Storage between TLS/ECDH and BB-HIBE	22
4.3	BB-HIBE Key Exchange Performance using Different Key Sizes (d_{id})	23
V	CONCLUSIONS AND FUTURE WORKS	25
5.1	Conclusion	25
5.2	Future Work	25
	REFERENCES	27