
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	xii
LIST OF ABBREVIATIONS	xiv
LIST OF NOTATIONS	xv
1 INTRODUCTION	1
1.1 Rationale	1
1.2 Theoretical Framework	3
1.3 Conceptual Framework/Paradigm	4
1.4 Statement of the Problem	4
1.5 Objective and Hypotheses	4
1.6 Assumption	5
1.7 Scope and Delimitation	5
1.8 Significance of the Study	5
2 REVIEW OF LITERATURE AND STUDIES	7
2.1 Review of Two-Factor Fuzzy Commitment for IoT Devices Security	7
2.2 Foundational Theory to Support the Proposed Method	9
2.2.1 Physical Unclonable Function (PUF)	9
2.2.2 Authentication Decidability	13
2.2.3 Fuzzy Commitment	15
2.2.4 Error Correction Code	17
2.2.5 Physical or Environmental Parameters for Authentication	19

3	RESEARCH METHODOLOGY	20
3.1	Research Framework	20
3.2	Research Design	21
3.2.1	Genuine PUF Design	21
3.2.2	Attacker PUF Design	27
3.2.3	System Parameters	27
3.2.4	CRPs Dataset Generation & Optimization	29
3.2.5	Enrollment Phase	32
3.2.6	Reproduction Phase	34
3.2.7	IoT Device Communication Scheme	35
3.3	Population/Sampling	36
3.4	Instrumentation and Data Collection	37
3.5	Tools for Data Analysis	37
3.6	Experiment Scenario	38
4	PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA	39
4.1	Presentation of Data	39
4.1.1	PUF Performance	39
4.1.2	External Noisy Source	59
4.1.3	System Performance	65
4.2	Analysis of the Data	75
4.2.1	PUF Performance Evaluation	75
4.2.2	Combined Noisy Source Performance Evaluation	78
4.2.3	System Performance Evaluation	80
4.3	Summary of Findings	81
5	CONCLUSION AND RECOMMENDATIONS	84
5.1	Conclusions	84
5.2	Recommendations	85
	BIBLIOGRAPHY	86
	Appendices	91