

TABLE OF CONTENTS

Chapter No.	Title	Page No.
	List of Tables	x
	List of Figures	xi
	List of Abbreviations	xiv
	Abstract	xv
1	INTRODUCTION	1
1.1	Overview	1
1.2	Motivation	3
1.3	Problem Definition	3
1.4	Research Objectives	4
1.5	Scope	4
1.6	Contributions	5
1.7	Organization of the Research Work	5
1.8	Chapter Summary	6
2	LITERATURE SURVEY	7
2.1	Introduction	7
2.2	Internet Of Things	7
	2.2.1. Components of IoT	8
	2.2.2. Layered Architecture of IoT	11
	2.2.3. Applications of IoT	16
	2.2.4. Security Threats and solutions in IoT	17

Chapter No.	Title	Page No.
2.3.	Lightweight Cryptography	27
	2.3.1. Lightweight Encryption and Decryption Algorithms	31
	2.3.2. Cryptanalysis of Lightweight Cryptography Algorithms	35
2.4.	Supply Chain Management	36
	2.4.1. Challenges in Supply Chain Management	37
2.5.	Chapter Summary	41
3	PROPOSED SYSTEM ARCHITECTURE: SiC-Chain	42
3.1	Introduction	42
3.2	Research Gaps	42
3.3	Research Methodology	42
3.4	SiC-Chain Architecture	45
	3.4.1 Concepts and Features of SiC- Chain Architecture	45
	3.4.2 SiC- Chain Layered Architecture	49
	3.4.2.1 SiC-Chain Sensing layer	51
	3.4.2.2 SiC-Chain Security layer	52
	3.4.2.3 SiC-Chain Networking layer	52
	3.4.2.4 SiC-Chain Middleware layer	53
	3.4.2.5 SiC-Chain Application layer	54
	3.4.3 Mapping of SiC-Chain layers to SCM Environment	54
	3.4.3.1 Mapping of SiC-Chain Sensing layer to SCM	55
	3.4.3.2 Mapping of SiC- Chain Security Layer to SCM	56
	3.4.3.3 Mapping of SiC-Chain Networking layer to SCM	57
	3.4.3.4 Mapping of SiC-Chain Middleware layer to SCM	58
	3.4.3.5 Mapping of SiC-Chain Application layer to SCM	59
	3.4.4 Operations in SiC-chain	60

Chapter No.	Title	Page No.
3.5	Implementation	64
	3.5.1 Fishing industry: An application for SiC-Chain	64
	3.5.2 SiC-Chain Prototype Environment	67
3.6	Results & Evaluation	73
	3.6.1 Module Testing	73
	3.6.1.1 Testing & Evaluation of SiC-SBox	73
	3.6.1.2 Evaluation of SiC-Chain Backend on the Cloud	75
	3.6.1.3 Evaluation of SiC-Chain Application	79
3.8	Chapter Summary	84
4	DESIGN AND EVALUATION OF SiC-Chain SECURITY LAYER	85
4.1	Introduction	85
4.2	Need for Non-Linear S-Boxes	86
4.3	Development of Non-Linear S-Boxes	87
	4.3.1 S-Box Generation	87
	4.3.2 Algorithm for 16*16 S-Box Generation	88
4.4	Performance Evaluation	89
	4.4.1 Non-Linearity	89
	4.4.2 Differential Approximation Probability	91
	4.4.3 Linear Approximation Probability	93
4.5	Need for Dynamic key dependent algorithm	96
4.6	Proposed algorithm with dynamic key dependent S-Box	97
	4.6.1 Key Initialization	99
	4.6.2 Encryption Process	99
	4.6.2.1 Round Function	100
	4.6.2.2 Selection of Dynamic Key Dependent S-Box	101
	4.6.3 Decryption Process	103

Chapter No.	Title	Page No.
4.7	Overall Experimental Evaluation	103
	4.7.1 Strict Avalanche effect	104
	4.7.2 Average Encryption/Decryption Time	108
	4.7.3 Average Throughput and Memory Consumption	109
4.8	Chapter Summary	110
5	CONCLUSION AND FUTURE WORK	111
5.1	Conclusion	111
5.2	Future Work	112
	REFERENCES	113
	LIST OF PUBLICATIONS	127
	PLAGIARISM REPORT	
