

TABLE OF CONTENTS

CERTIFICATE.....	i
APPROVAL SHEET.....	ii
CANDIDATE’S DECLARATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT.....	vi
TABLE OF CONTENTS	vii
LIST OF FIGURES.....	xi
LIST OF TABLES.....	xv
ACRONYMS.....	xvi
Chapter – 1 Introduction	1
1.1 Introduction to Electronic Mail.....	1
1.2 Simple Mail Transfer Protocol (SMTP).....	2
1.3 Email Authentication.....	5
1.4 Problem Statement	5
1.5 Motivation for the Research	5
1.6 Objectives of Research.....	6
1.7 Research Contribution	6
1.7.1 Research Contribution to Society.....	6
1.7.2 Research Contribution to Computer Science.....	7
1.8 Scope of Problem Statement	7
1.9 Organization of the Thesis	8
1.10 Conclusion and Summary	9

Chapter – 2 Literature Survey	10
2.1 Introduction	10
2.2 Email Security	17
2.3 Email Spoofing.....	21
2.4 How Attackers Spoof Email	23
2.5 How Email Spoofing Works?	26
2.6 Why Does Email Spoofing Happens?	30
2.7 How To Identify Spoofed Email?	31
2.8 Anti-Spoofing Protocols	34
2.8.1 Sender Policy Framework (SPF).....	34
2.8.2 DomainKeys Identified Mail (DKIM).....	36
2.8.3 Domain-based Message Authentication, Reporting and Conformance (DMARC)	38
2.8.4 Authenticated Received Chain (ARC)	41
2.9 Gaps in Existing System.....	43
2.10 Conclusion and Summary	47
Chapter – 3 Architecture Setup and Experiment.....	48
3.1 Introduction	48
3.2 Setup of Email Server	48
3.2.1 Installation of Email Server	49
3.2.2 Reverse DNS setup	55
3.2.3 Setup of DKIM key for signing emails.....	57
3.2.4 Modification in Configuration Files	58
3.3 Implementation of Anti-Spoofing Protocols	60
3.4 Testing of Delivery of Email.....	61

3.4.1	Regular email from domain not having any anti-spoofing protocols	61
3.4.2	Regular email from domain having all three anti-spoofing protocols	62
3.4.3	Spoofed email from domain not having any anti-spoofing protocols	64
3.4.4	Spoofed email from domain having all three anti-spoofing protocols	65
3.5	Attacks on Anti-Spoofing Protocols	66
3.5.1	How to Bypass SPF?	66
3.5.2	How to Bypass DKIM?	68
3.5.3	How to Bypass DMARC?	69
3.6	Comparison of Genuine and Spoofed emails	71
3.6.1	Authentic Genuine Email	71
3.6.2	Spoofed Fake Email	73
3.7	Conclusion and Summary	76
Chapter – 4	Proposed System Architecture and Methodology	77
4.1	Introduction	77
4.2	Proposed Framework	78
4.2.1	Email Authentication Identity Code (EAIC)	79
4.2.2	Email Authentication Identity Score (EAIS)	81
4.2.3	Adaptive Authentication Framework for Email (AAFE)	83
4.3	Illustration of AAFE at Sending Mail Server Side	87
4.4	Illustration of AAFE at Receiving Mail Server Side	89
4.5	Adaptive Authentication Framework for Email (AAFE) Security	91
4.6	Conclusion and Summary	92
Chapter – 5	Performance Analysis	93
5.1	Introduction	93
5.2	Testing of Proposed Framework	93

5.3	Results	94
5.4	Scenario – 1: Email with SPF, DKIM & DMARC (mail-server.in).....	96
5.5	Scenario – 2.1: Spoofing with SPF, DKIM & DMARC (gmail.com)	97
5.6	Scenario – 2.2: Spoofing with SPF, DKIM & DMARC (outlook.com)	98
5.7	Scenario – 3: Spoofing with only DKIM (msubaroda.ac.in).....	99
5.8	Scenario – 4: Spoofing with only SPF (orthocarehospital.in).....	101
5.9	Scenario – 5: Spoofing with SPF and DKIM (orthocarehospital.in).....	102
5.10	Scenario – 6: Spoofing with no authentication (gujarattourism.in).....	104
5.11	Performance Analysis with Existing System	105
5.12	Conclusion and Summary	106
Chapter – 6 Conclusion and Future Enhancement		107
6.1	Summary	107
6.2	Limitation of the Proposed System.....	109
6.3	Outcome of Research Work	110
6.4	Future Scope of Work	111
6.5	Conclusion	111
REFERENCES.....		112
RESEARCH PUBLICATIONS		122