DECLARATION

I declare that the thesis entitled Two Tier Security Solution For Implantable Medical Devices submitted by me for the degree of Doctor of Philosophy is the record of research work carried out by me during the period from March 2011 to June 2016 under the supervision of Dr. Bhushan Trivedi and this has not formed the basis for the award of any degree, diploma, associate ship, fellowship, titles in this or any other University or other institution of higher learning.

I further declare that the material obtained from other sources has been duly acknowledged in the thesis. I shall be solely responsible for any plagiarism or other irregularities, if noticed in the thesis.

Signature of the Research Scholar: Date: / /2016

Name of Research Scholar: Monika Archit Darji

Place: Ahmedabad

CERTIFICATE

I certify that the work incorporated in the thesis Two Tier Security Solution for Implantable Medical Devices submitted by Smt. Monika Archit Darji was carried out by the candidate under my supervision/guidance. To the best of my knowledge: (i) the candidate has not submitted the same research work to any other institution for any degree/diploma, Associateship, Fellowship or other similar titles (ii) the thesis submitted is a record of original research work done by the Research Scholar during the period of study under my supervision, and (iii) the thesis represents independent research work on the part of the Research Scholar.

Signature of Supervisor: …… Date: / /2016

Name of Supervisor: Dr. Bhushan Trivedi

Place: Ahmedabad

Originality Report Certificate

It is certified that PhD Thesis titled Two Tier Security Solution for Implantable Medical Devices by Monika Archit Darji has been examined by us. We undertake the following:

a. Thesis has significant new work / knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.

b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.

c. There is no fabrication of data or results which have been compiled / analysed.

d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.

e. The thesis has been checked using https://**turnitin.com** (copy of originality report attached) and found within limits as per GTU Plagiarism Policy and instructions issued from time to time (i.e. permitted similarity index <=25%).

Signature of the Research Scholar: Date: / /2016

Name of Research Scholar: Monika Archit Darji

Place: Ahmedabad

Signature of Supervisor: Date: / /2016

Name of Supervisor: Dr. Bhushan Trivedi

Place: Ahmedabad

Thesis_Monika_Darji

ORIGINALITY REPORT

8%	1%	8%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Communications in Computer and Information Science, 2014. Publication	7%
2	Strydis, Christos, Robert M. Seepers, Pedro Peris-Lopez, Dimitrios Siskos, and Ioannis Sourdis. "A system architecture, processor, and communication protocol for secure implants", ACM Transactions on Architecture and Code Optimization, 2013. Publication	1%
3	dataspace.princeton.edu Internet Source	1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	< 1%
EXCLUDE BIBLIOGRAPHY	ON		

PhD THESIS Non-Exclusive License to GUJARAT TECHNOLOGICAL UNIVERSITY

In consideration of being a PhD Research Scholar at GTU and in the interests of the facilitation of research at GTU and elsewhere, I, Monika Archit Darji having enrollment number 119997493008 hereby grant a non-exclusive, royalty free and perpetual license to GTU on the following terms:

a) GTU is permitted to archive, reproduce and distribute my thesis, in whole or in part, and/or my abstract, in whole or in part (referred to collectively as the "Work") anywhere in the world, for non-commercial purposes, in all forms of media;

b) GTU is permitted to authorize, sub-lease, sub-contract or procure any of the acts mentioned in paragraph (a);

c) GTU is authorized to submit the Work at any National / International Library, under the authority of their "Thesis Non-Exclusive License";

d) The Universal Copyright Notice (©) shall appear on all copies made under the authority of this license;

e) I undertake to submit my thesis, through my University, to any Library and Archives. Any abstract submitted with the thesis will be considered to form part of the thesis.

f) I represent that my thesis is my original work, does not infringe any rights of others, including privacy rights, and that I have the right to make the grant conferred by this non-exclusive license.

g) If third party copyrighted material was included in my thesis for which, under the terms of the Copyright Act, written permission from the copyright owners is required, I have obtained such permission from the copyright owners to do the acts mentioned in paragraph (a) above for the full term of copyright protection.

h) I retain copyright ownership and moral rights in my thesis, and may deal with the copyright in my thesis, in any way consistent with rights granted by me to my University in this non-exclusive license.

i) I further promise to inform any person to whom I may hereafter assign or license my copyright in my thesis of the rights granted by me to my University in this non-exclusive license.

j) I am aware of and agree to accept the conditions and regulations of PhD including all policy matters related to authorship and plagiarism.

Signature of the Research Scholar:

Name of Research Scholar: Monika Archit Darji

Date: / /2016 Place: Ahmedabad

Signature of Supervisor:

Name of Supervisor: Dr. Bhushan Trivedi

Date: / /2016 Place: Ahmedabad

Seal:

Thesis Approval Form

The viva-voce of the PhD Thesis submitted by Smt. Monika Archit Darji (Enrollment No. 119997493008) entitled Two Tier Security Solution For Implantable Medical Devices was conducted on …….…… (day and date) at Gujarat Technological University.

(Please tick any one of the following option)

☐ We recommend that he/she be awarded the Ph.D. Degree.

☐ We recommend that the viva-voce be re-conducted after incorporating the following suggestions:

☐ The performance of the candidate was unsatisfactory. We recommend that he/she should not be awarded the Ph.D. Degree.

---------- ----------

Name and Signature of Supervisor with Seal 1) (External Examiner 1) Name and Signature

---------- ----------

2) (External Examiner 2) Name and Signature 3) (External Examiner 3) Name and Signature

ABSTRACT

The development of MEMS (micro electro mechanical systems), SoC (System on Chip) and ultra low power wireless communication technology enabled the evolution of Implantable Medical Devices (IMDs). Implantable medical devices (IMDs) diagnose, monitor, and treat a wide range of medical conditions. This has lead to paradigm shift of the healthcare industry from doctor centric to patient centric by providing home-based treatment and remote monitoring and hence cost reduction. While these features improve healthcare diagnostics and decision making, security and privacy remain critical design aspects in wireless communication performed by these devices. As compared to previous ones, IMDs of current genre are complex embedded systems with networking capabilities that aid in wireless communication amongst IMDs and with other external devices. Due to their unique placement in human body and resource constraints like low power availability, computation and storage capacity, achieving security and privacy for wireless communication is difficult. Security for medical devices has gained attention in the recent years following some well-publicized attacks on Implantable Medical Devices, like pacemakers and insulin pumps. This has resulted in solutions being proposed for securing these devices, which are usually device specific and useful only for secure communication with external devices. Multiple IMDs may be implanted in a single patient therefore we argue that securing individual devices will not serve the purpose as these devices will be integrated sooner or later for advance therapeutic implications. Security solution rather than being device specific should be patient specific to cater to the security needs of IMDs of a patient. We provide a simple solution to detect active attacks on IMDs and then we provide an emergency aware access control framework for IMDs and also provide a Buddy System for secure communication with external devices. Finally, we provide an application layer security solution which not only allows secure communication between IMDs and external devices but also between interoperable IMDs for a single patient. We consider extreme resource constraints of IMD and explore the tradeoffs among different cryptographic primitives for use in IMDs to carefully design a lightweight protocol optimized for IMDs for mutual authentication and secure communication between the IMD and the proxy device. We also design a secure publish-subscribe communication protocol between the “proxy device” and external devices. Finally, we provide a proof-of-concept for the proposed two-tier security solution.

Acknowledgement

The perseverance required to come till here is the result of unmatched inspiration from my Guide, **Dr. Bhushan Trivedi,** Dean, Faculty of Computer Technology, GLS University; Director, GLS Institute of Computer Technology; Dean, Zone-I, MCA Programme, GTU. He never compromised in bringing out the best in me but at the same time gave me complete freedom to finish the work at my own pace. He allowed me to unfold my research work and never forced me to follow others footsteps. His go ahead would make me discover new ways of doing things and his remainder alarms helped me to stay focused and never wander too far. His expertise in the field helped me in developing a state-of-art solution.

The Doctorate Progress Committee (DPC) members: **Dr. Haresh Bhatt,** ISO, CIO and Mission Director, Information Security, Space Application Center (SAC), Indian Space Research Organization (ISRO) and **Dr. Devesh C Jinwala,** Professor and Dean, Research & Consultancy, Department of Computer Engineering, S V National Institute of Technology have helped me immensely in the entire work by giving their expert advises and by conducting earnest reviews.

I am also truly indebted to my co-guide **Dr. Pramode K. Verma,** Professor of Computer Engineering and Director of Telecom Engineering, University of Oklahoma, USA for supervising my work, providing invaluable inputs and motivating me.

I heartily thank **Prof. Urja Mankad** and **Mr. Hetansh Mankad** who supported me throughout this endeavor. I also appreciate the work of all the researchers whose work helped me to understand my field of research and contribute to it in however small manner possible.

Dr. Akshai Aggarwal, Vice Chancellor, Gujarat Technological University initiated this programme and I am thankful to him for giving me this once in a lifetime opportunity.

I express my gratitude towards the reviewers who took out their precious time to read the thesis and review it.

At the end I wholeheartedly thank my husband, **Mr. Archit Darji** who made this journey an epitome of memorable moments by always being there for me. I can't thank God enough for bestowing oodles of luck on me in the form of a supportive family who stood

next to me in the thick and thins. My beloved son **Meghant** and adorable mother **Hasumatiben Darji** supported me immensely. My father **Mr. Sapan Mukherjee** was there for me whenever I needed his help. It is their unparallel love and good wishes that worked along with me in this journey. At the end I would like to dedicate this work to my papaji, **Prof. Arvindbhai Darji**, who was a wonderful teacher, an ace author, an orator and most importantly a marvelous human being!

Table of Content

CHAPTER – 1 Introduction		1
1.1.	Background	2
1.1.1.	Implantable Medical Devices	2
1.1.2.	Classification of Implantable Medical Devices	3
1.1.3.	Characteristics of Implantable Medical Devices	4
1.1.3.1.	Implantable Medical Device Communication	5
1.1.3.2.	Implantable Medical Device Design	6
1.1.3.3	Implantable Medical Device Networking	7
1.1.4.	Classification of Implantable Medical Device Data	7
1.1.5.	Our Findings	8
1.1.6.	Network and Communication Security	8
1.1.6.1.	Definition	9
1.1.6.2.	Security Objectives of Implantable Medical Device	9
1.1.6.3.	Challenges in Securing IMDs	11
1.2.	Motivation and Objectives	12
1.3.	Objective and Scope of work	13
1.4.	Contribution of the Study	14
1.5.	Research Methodology adopted for this Work	16
1.6.	Organization of Remainder of the Thesis	17
CHAPTER 2 Threat Modeling		18
2.1.	Introduction	18
2.2.	Threat Model	18
2.3.	Related Work	19
2.4.	Vulnerability and Threats in Existing IMDs	21
2.5.	A Hypothetical Attack Scenario	22

2.6.	Adversarial Model	23
2.7	Threat Modeling using SDL Tool	25
2.8.	Conclusion	27
CHAPTER – 3 Literature Survey		28
3.1.	Security Dimensions	28
3.2.	Design Dimensions	29
3.3.	Taxonomy of Security Models proposed in Literature	29
3.3.1.	Inhibiting Long Range Communication	29
3.3.1.1.	Use of small-range communication channel	30
3.3.1.2.	Enforcing Proximity	30
3.3.2.	Using Cryptography	31
3.3.2.1.	Using Symmetric Cryptography	32
3.3.2.2.	Using Asymmetric Cryptography	32
3.3.3.	Key Distribution and Management	33
3.3.3.1.	Putting Patient in the Loop	33
3.3.3.2.	Use of Patient Biometrics	33
3.3.3.3	Use of Physical Layer Approaches	34
3.3.4.	Using Trusted External Device	34
3.3.4.1.	Invasive Approaches	34
3.3.4.2.	Non-Invasive Approaches	37
3.3.5.	Emergency Access for IMDs	39
3.4.	Comparison of Security Models	39
3.5	Conclusion	41
CHAPTER – 4 A Buddy System for Securing Wireless IMDs		42
4.1.	Introduction	43
4.2.	Proposed solution: The Buddy System	43
4.3.	Features of Buddy Device	45

4.4.	Proposed Architecture using Buddy Device	46
4.4.1.	Buddy Device	46
4.4.2.	Implantable Medical Device	47
4.4.3.	Enhanced External Device (ED)	47
4.5.	Secure Communication Protocol	47
4.5.1.	MD-Buddy Device Pairing	48
4.5.2.	Reader Authentication	48
4.5.3.	Buddy Device-IMD Communication	48
4.5.4.	IMD-External Reader Communication	49
4.5.5.	Emergency Access	49
4.6.	Conclusion	50
CHAPTER – 5 Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs		51
5.1.	Introduction	51
5.2	Threat Model for Fail Open Security	53
5.2.1.	Assumptions	53
5.3.	Security Mechanisms proposed to be Installed on Proxy Device	53
5.3.1.	Authentication	53
5.3.2.	Access Control	54
5.3.2.1.	Traditional rule based model	54
5.3.2.2.	Role based access control model	54
5.3.2.3.	Context Aware Access Control Model	55
5.3.2.4.	Criticality Aware Access Control Model (CAAC)	56
5.4.	Proposed EAAC Architectural Framework	55
5.4.1.	Role Management	56
5.4.2.	Emergency State Management	56
5.4.3.	Emergency Management	57
5.5.	Conclusion	58

CHAPTER – 6 Detection of Active Attacks on wireless IMDs using Proxy Device and Localization Information		59
6.1.	Introduction	59
6.2.	RF based localization techniques	60
6.2.1.	Time of Arrival (ToA)	60
6.2.2.	Time Difference of Arrival (TDoA)	61
6.2.3.	Received Signal Strength Indicator (RSSI)	61
6.2.4.	Angle of Arrival (AoA)	61
6.3.	Overview of components	61
6.3.1.	System Configuration	61
6.3.2.	Assumption	61
6.2.3.	Proxy Device Overview	62
6.4.	Signature Generation and Verification	62
6.5.	Proposed Proxy based Protocol	63
6.6.	Conclusion	65
CHAPTER – 7 Two Tier Model for Securing Wireless IMDs		66
7.1.	Introduction	66
7.2.	Design Goals of Security Model	67
7.3.	Requirements of Two-tier Security Model	68
7.4.	Assumptions	68
7.5.	Overview of Proxy Based Two-tier Security System	69
7.6.	Profiling of Security Mechanisms for Tier-1: IMD and Proxy Device communication	70
7.6.1.	Security Service: Message Confidentiality	71
7.6.2.	Security Service: Message Integrity and Authentication	72
7.6.2.1.	Authenticated Encryption Mode- GCM	73
7.6.2.2.	Initial Vector Format for Tier -1	75
7.6.3.	Security Service: Replay Protection	76

7.6.3.1.	Counters	76
7.6.3.2.	Nonce	77
7.6.4.	Security Service: Mutual Authentication	78
7.6.5.	Security Service: Access Control	78
7.7.	Profiling of Security Mechanisms for Tier-2: Proxy Device and External Device communication	79
7.7.1.	Components of the Communication Model	79
7.7.2.	Design Choices for Proxy and ED communication	80
7.7.3.	Public Key Cryptography	80
7.7.4.	Security Service: Massage Confidentiality, Integrity and Authentication	81
7.7.5.	Security Service: Replay protection	81
7.7.6.	Security Service: Access Control	81
7.7.7.	Security Service: Mutual Authentication	81
7.8.	The Proposed Architecture and its Components	81
7.9.	Proxy Device and its role in the two-tier Security Model	83
7.10.	Description of proposed protocol for Tier 1: IMD and Proxy Communication	87
7.10.1.	Protocol : Proxy initiating communication	87
7.10.2.	Protocol: IMD initiating communication	89
7.10.3.	Message Formats for Tier One: Proxy-IMD communication	91
7.11.	Description of proposed protocol for Tier 2: Proxy and External Device Communication	91
7.11.1.	Protocol: Communication between Proxy and ED as Publisher	93
7.11.2.	Protocol: Communication between Proxy and ED as Subscriber	95
7.12.	Essential Functions Provided by Proxy	97
7.12.1.	Topic Management	97
7.12.2.	Device Management	98
7.12.3.	Access Management	98
7.12.4.	Key Management	99

7.12.5.	Emergency aware Access Management	99
7.13.	Deployment Model	99
CHAPTER – 8 Implementation and Analysis		102
8.1.	Implementation	102
8.2.	Security Analysis	106
8.3.	Conclusion	107
CHAPTER – 9 Conclusions, Major Contributions and Further Work		108
9.1.	Objective Achieved	108
9.2.	Major Contributions	109
9.3.	Comparison of proposed Security Model with Existing Solutions	110
9.4.	Possible further Work	112

List of Abbreviations

BCC: Body Coupled Communication

DoS: Denial of Service

DDoS: Distributed Denial of Service

ECG: Electrocardiogram

HIPAA: Health Insurance Portability and Accountability Act

ICD: Implantable Cardiac Defibrillators

IMD: Implantable Medical Device

AIMD: Active Implantable Medical Device

MAC: Message Authentication Code

MICS: Medical Implant Communication Service

MITM: Man In The Middle

NFC: Near Field Communication

PV: Physiological Value

RF: Radio Frequency

RFID: Radio Frequency Identification

RSSI: Received Signal Strength Indicator

WISP: Wireless Identification and Sensing Platform

RSSI: Received signal strength indicator

TOA: Time of arrival

DTOA differential time of arrival

AOA: Angle of arrival

AES: Advanced Encryption Standard.

CBC: Cipher Block Chaining

MAC: Message Authentication Code

TDEA: Triple Data Encryption Algorithm.

TLS: Transport Layer Security

WISP: Wireless Identification and Sensing Platform

PSV: Publisher Specific Value

ED: External Device

ECC: Elliptic Curve Cryptography

ECDSA: Elliptic Curve Digital Signature Algorithm

FDA: Food and Drug Administration

IDS: Intrusion Detection System

List of Figures

Figure No	Title	Page No
1.1	Position of Implantable Body Area Network	2
1.2	A range of IMDs (Photos: Medagadget)	2
1.3	Classifications of IMDs	3
1.4	Phases Covered in Research Work	16
2.1	A Hypothetical Attack Scenario	22
2.2	Types of Attackers	23
2.3	Context Level DFD for IMDs	26
2.4	Level One DFD for IMDs	26
3.1	Allowing reconfiguration from smaller distance and remote monitoring from longer distance [29]	31
3.2	ECG readings taken simultaneously by IMD and external device is matched to allow access [81]	36
3.3	Shield Jamming Unauthorized Communication [84]	37
4.1	Architecture of Proposed Security Scheme using Buddy Device	46
4.2	Sequence Diagram for Buddy Device based communication protocol	49
5.1	Block Diagram for Emergency Aware Access Control	52
5.2	State Transition Diagram for Emergency Aware Access Control using Proxy Device [124]	58
5.3	The Proposed Proxy based Architecture [124]	58
6.1	Signature Verification [122]	63
6.2	Sequence Diagram for Signature Verification Protocol [122]	65
7.1	Overall view of two-tier architecture	69
7.2	Structure of GCM [141]	73
7.3	Block Diagram of AES-GCM	74

7.4	Structures of IV	
(a)	Structure of IV for IMD	75
(b)	Structure of IV for Proxy	75
7.5	Architecture of Proxy based Two Tier solutions	82
7.6	Work Flow Diagram of Proxy Device	86
7.7	Sequence Diagram for Protocol: Proxy Initiating Communication	88
7.8	Sequence Diagram for Protocol: IMD Initiating Communication	90
7.9	Format of Messages	
(a)	Format of authentication request made by Proxy	91
(b)	Format of request and response messages	91
(c)	Format of authentication requests made by IMD	91
7.10	Sequence Diagram for communication between Proxy and External Device as Publisher	94
7.11	Sequence Diagram for communication between Proxy and External Device as Subscriber	96
7.12	Deployment Model	100
8.1	Network Switch Screen and Device Startup Screen	103
8.2	Mutual Authentications between IMD and Proxy.	104
8.3	External device sending join request to Proxy	105
8.4	Communications between Proxy, IMD and EDs	106

List of Tables

Table No	Title	Page No
1.1	IMD Characteristics	5
2.1	Vulnerabilities and Threats in Existing IMDs	21
2.2	Classification of Adversary	24
2.3	Threat Analysis Report	27
3.1	Comparisons of Surveyed Security Models	40
6.1	Table of Notation	64
7.1	Benchmark suite of symmetric ciphers	71
7.2	Summary of components adopted in communication protocol for Tier One: Proxy-IMD communication	79
7.3	Summary of components adopted in communication protocol for Tier Two: Proxy-ED communication	81
7.4	Notations used in Tier One: Proxy- IMD communication	87
7.5	Description of messages for Protocol: Proxy initiating communication	89
7.6	Description of messages for IMD initiating communication	90
7.7	Examples of Mapping of Biometric data to Topic	92
7.8	States of External Device maintained by Proxy	92
7.9	Description of notations used in Tier – two communications	93
7.10	Description of messages for Proxy and Publisher External Device communication	95
7.11	Description of messages for Proxy and Subscriber External Device communication	96
7.12	Topic Management Database	97
7.13	Device Information Database	98
7.14	Device Access Control Database	98

9.1	Comparison of proposed solution with [153]	111
9.2	Comparison of proposed solution with solutions proposing use of external device	112