

Intelligent Trust Management Methodology for the Internet of Things (IoT) To Enhance Cyber Security

A Thesis Submitted for the Degree of
Doctor of Philosophy

By

Mohammad Dahman Alshehri



Faculty of Engineering and Information Technology
University of Technology Sydney

March, 2019

Copyright © 2019 by Mohammad Alshehri. All Rights Reserved

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I, Mohammad Dahman Alshehri declare that this thesis, is submitted in fulfilment of the requirements for the award of PhD, in the School of Software/Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:

Signature: Signature removed prior to publication.

Date: 26/03/2019



ACKNOWLEDGEMENTS

All praises are due to Allah, The Most Beneficent, The Most Merciful, Who has enabled me to accomplish my PhD study. All the goals that I have achieved are due to His mercy; while all the mistakes are mine.

I would like to express my sincere gratitude to my PhD principal supervisor, Associate Professor Farookh Hussain, for his continuous support, encouragement, precious and guidance throughout my study. Thank you for your accurate critical comments and suggestions, which have strengthened this study significantly. Your strict academic attitude, generous personality and conscientious working style have influenced me deeply, and will be of great benefit to me in my future research work and life.

I am most grateful to my father, Dahman Alshehri, who always believed in my ability to be successful. He had passed away when I just began my PhD journey. May Allah bless my father's soul and grant him the paradise.

Most of all, I would like to express my deepest appreciation to my mother. She was supporting me and always being there for me during my ups and downs. Pursuing a PhD was always a long term challenge for me and a dream of my mother. This dream would have not been achieved without the prayers, inspiration, great empathy and kind assistance of my mother. Hence, great appreciation and enormous thanks are due to my mother. Likewise, I would like to thank my entire family members.

Finally, I would also like to express my thanks to Taif University, Saudi Arabian Cultural Mission (SACM) in Australia and everyone supported me during my PhD journey.

LIST OF PUBLICATIONS

JOURNAL ARTICLES PUBLISHED

1. Alshehri, M.D., Hussain, F.K. & Hussain, O.K. 2018, 'Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM IoT)' *ACM/Springer Mobile Networks and Applications Journal*, vol. 23, no. 3 pp. 419-431. **(JCR (Q1), Impact Factor (3.259)-2017)**
2. Alshehri, M.D & Hussain, F.K 2018, 'A Fuzzy Security Protocol for Trust Management in the Internet of Things (Fuzzy-IoT)', *ACM/Springer Computing Journal*. **(Accepted)**. **(Excellence in Research Australia (ERA) CORE, A-Rank Journal)**

CHAPTER OF BOOK PUBLISHED

3. Alshehri, M.D., Hussain F., Elkhodr, M. & Alsinglawi, B. 2018, 'A Distributed Trust Management Model for the Internet of Things (DTM-IoT)', *Recent Trends and Advances in Wireless and IoT-enabled Networks*, Springer, pp. 1-9.

CONFERENCE PAPERS PUBLISHED

4. Alshehri, M, Elkhodr, M & Alsinglawi, B 2018 'Data Provenance in the Internet of Things' *32nd International Conference on Advanced Information*

Networking and Applications Workshops (WAINA-2018), Krakow, Poland, pp. 727-731.

5. Alshehri, M.D, & Hussain, F.K 2017 ‘A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT)’ *12th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA-2017)*, Barcelona, Spain, pp. 533-543.
6. Alshehri, M.D, & Hussain, F.K 2015 ‘A comparative analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things’, *22nd International Conference on Neural Information Processing (ICONIP2015)*, Istanbul, Turkey, pp. 596-605. (**Excellence in Research Australia (ERA) CORE, A - Rank**)

OTHER PUBLICATIONS

CHAPTERS OF BOOK PUBLISHED

7. Elkhodr, M., Alsinglawi, B. & Alshehri, M. 2019, 'A Privacy Risk Assessment for the Internet of Things in Healthcare', *Applications of Intelligent Technologies in Healthcare*, Springer, pp. 47-54
8. Alsinglawi, B., Elkhodr, M. & Alshehri, M. 2018, ‘RFID Localization in the Internet of Things’, *ACM/ Recent Trends and Advances in Wireless and IoT-enabled Networks*, Springer, pp. 73-81

CONFERENCE PAPER PUBLICSHED

9. Ikram, M.A., Alshehri M.D, & Hussain. F.K 2015 “Architecture of an IoT-based System for Football Supervision”, *IEEE 2nd World Forum on Internet of Things (WF-IoT 2015)*, Milan, Italy, pp. 14-16.

TABLE OF CONTENTS

CERTIFICATE OF AUTHORSHIP/ORIGINALITY.....	i
ACKNOWLEDGEMENTS.....	iii
LIST OF PUBLICATIONS	iv
LIST OF FIGURES	xii
LIST OF TABLES.....	xiv
Abstract.....	xvi
Chapter 1 Introduction.....	1
1.1 Introduction	1
1.2 Research challenges related to the Internet of Things (IoT)	3
1.2.1 Challenges related to trust management in IoT.....	4
1.2.2 Challenges related to the scalability of trust management in IoT	6
1.2.3 Challenges related to security protocols for IoT	7
1.3 Objectives of this Thesis.....	8
1.4 Significance of the Thesis.....	9
1.4.1 Scientific Significance.....	9
1.4.2 Social Significance	10
1.5 Structure of the Thesis	11
1.6 Conclusion	15
Chapter 2 Literature Review	16
2.1 Introduction	16
2.2 Role of Trust Management in the Internet of Things (IoT).....	18

2.2.1 Trust Management in IoT	23
2.2.2 Solutions focusing on the scalability of trust management approaches	33
2.3 Context-aware Assessment for IoT	42
2.4 Security protocol for reliable trust management for IoT	45
2.5 Clustering-Based Trust for IoT.....	54
2.6 Fuzzy-logic based mechanisms for trust management in the IoT	60
2.7 Critical Evaluation and Summary of Shortcomings	65
2.8 Conclusion	69
Chapter 3 Problem Definition	71
3.1 Introduction	71
3.2 Explanation or definition of key terms and concepts	72
3.2.1 Internet of Things (IoT).....	72
3.2.2 IoT Security.....	72
3.2.3 Cyber Security.....	72
3.2.4 IoT Security Protocol	73
3.2.5 Trust	73
3.2.6 Trust Management.....	73
3.2.7 Trustworthy nodes.....	73
3.2.8 Fuzzy Logic.....	74
3.2.9 Cluster	74
3.2.10 Trust-based Clustering	74
3.2.11 Trust management platform	74
3.2.12 Scalability.....	74
3.2.13 Node	75
3.2.14 Super Node (SN)	75
3.2.15 Master Node (MN)	75

3.2.16 Cluster Node (CN)	75
3.2.17 Cyber-attacks.....	76
3.2.18 On-Off attacks	76
3.2.19 Contradictory behaviour attacks.....	76
3.2.20 Bad-mouthing attacks.....	76
3.2.21 Bad service attacks	77
3.2.22 Fuzzy bank	77
3.2.23 Routing score.....	77
3.3 Problem Overview and Problem Definition	77
3.4 Research Questions.....	79
3.5 Research Objectives	81
3.6 The Research Approach to Problem-Solving	82
3.6.1 Existing Research Methods	82
3.6.2 The choice of the Science and Engineering-based Research Method.....	84
3.7 Conclusion	88
Chapter 4 Solution Overview.....	89
4.1 Introduction	89
4.2 Overview of the Solution for the trust management platform for IoT-based clustering (TM-IoT).....	90
4.3 Overview of the solution to ensure TM-IoT scalability and reliability (CITM- IoT)	96
4.4 Overview of the solution to detect malicious nodes compromising TM-IoT (Fuzzy-IoT).....	104
4.5 Overview of the validation approach.....	108
4.6 Conclusion	109

Chapter 5 Trust Management Platform for the Internet of Things (TM-IoT) 110

5.1 Introduction	110
5.2 Trust management for the IoT platform mechanism (TM-IoT)	111
5.3 Super Node (SN) Mechanisms and Modules	114
5.3.1 API Module of the Super Node (SN)	116
5.3.2 Trust Management Module and Repository	117
5.3.3 The Trust Communication Module (TCM)	118
5.4 The Master Node (MN) Components	122
5.5 The Cluster Components	123
5.6 The Cluster Node (CN) Components	124
5.7 Conclusion	126

Chapter 6 Clustering-Driven Intelligent, Scalable and Reliable Trust

Management for IoT (CITM-IoT)..... 127

6.1 Introduction	127
6.2 Architecture of the approach for scalable trust management in IoT (TM-IoT).....	129
6.3 Intelligent Algorithms for TM-IoT scalability and reliability	132
6.3.1 Algorithm for trust-based cluster boundary calculation.....	133
6.3.2 Algorithm for trust-driven node migration from one cluster to another to enable TM-IoT scalability	137
6.3.3 Algorithm to eliminate outliers for bad-mouthing attacks in the IoT	139
6.3.4 Algorithm for updating and checking the trust values of cluster and master nodes.....	142
6.4 Experimentation and Results for the proposed scalability and reliability algorithms of TM-IoT.....	146

6.4.1 Results of method proposed for countering bad-mouthing attacks in TM-IoT	151
6.4.2 Results of method proposed for countering extreme memory	156
6.6 Conclusion	159
Chapter 7 Reliable Fuzzy-Logic Based Protocol for Ensuring the Reliability of TM-IoT (FUZZY-IoT).....	160
7.1 Introduction	160
7.2 A Secure HEXA Decimal-Based Messaging System for Tamper Detection ..	162
7.3 Fuzzy Logic-Based Approach for Countering Attacks on IoT	164
7.4 Trust-Based Communication Protocol in TM-IoT	173
7.5 Simulation, Node Mechanisms, Results and Analysis	175
7.5.1 Simulation Settings: Basic Concept	176
7.5.2 Simulation Settings: (200 Nodes)	180
7.5.3 Simulation Settings: Large Scale IoT Network.....	184
7.5.4 Results and Analysis	189
7.6 Conclusion	196
Chapter 8 Conclusion and Future Work	198
8.1 Introduction	198
8.2 Problems Addressed in this Thesis	200
8.3 Contributions of this Thesis to the Existing Literature.....	201
8.3.1 Contribution 1: State-of-the-art Comprehensive Survey of the Existing Literature	201
8.3.2 Contribution 2: Methodology of Trust Management Platform for IoT (TM-IoT).....	202

8.3.3 Contribution 3: Clustering-Driven Intelligent, Scalable and Reliable Trust Management for IoT (CITM-IOT).....	203
8.3.4 Contribution 4: Fuzzy Logic-Based Algorithms for the Reliability of TM-IoT (FUZZY-IoT)	205
8.4 Conclusion and Future Work.....	207
References.....	208

LIST OF FIGURES

Figure 1-1 The structure of the thesis	14
Figure 2-1 Shows an overview of the literature review sections and sub-sections in this chapter.	17
Figure 3-1 Overview of the use the science and engineering-based research methodology is used in this thesis	85
Figure 4-1 Overview of the TM-IoT platform.....	91
Figure 4-2 The lifecycle solution for the trust management platform for IoT-based clustering (TM-IoT)	95
Figure 4-3 Overview of the solution for efficient trust management in TM-IoT	97
Figure 5-1 A Centralized platform for trust management of IoT mechanism (TM-IoT)	113
Figure 5-2 Centralized IoT super node (SN) modules.....	115
Figure 5-3 API module components	116
Figure 5-4 Receive message format.....	119
Figure 5-5 SendUpdate trust value message format MN to CN	120
Figure 5-6 SendUpdate trust value message format MN to SN.....	120
Figure 5-7 Response trust value message format CN to MN	121
Figure 5-8 Master node (MN) components	123
Figure 5-9 Cluster components	124
Figure 5-10 Cluster node (CN) component	126
Figure 6-1 Architecture of the TM-IoT	130
Figure 6-2 Base case SD of master memory usage.....	147
Figure 6-3 Base case average trust value of cluster nodes.....	149
Figure 6-4 Base case SD of average trust of cluster nodes for each cluster	150

Figure 6-5 Comparison of SD of master memory usage with and without outliers (proposed bad-mouthing algorithm – Algorithm 6.3).....	153
Figure 6-6 Comparison of average trust values of CNs with and without outliers...	154
Figure 6-7 Comparison of SD of average trust of CNs for each cluster with and without outliers	155
Figure 6-8 SD of master memory usage with memory thresholds (memory threshold 'on').....	157
Figure 6-9 SD of master memory usage without memory thresholds (memory threshold 'off')	158
Figure 7-1 General structure of a message	163
Figure 7-2 Membership function of fuzzy-logic.....	165
Figure 7-3 Flowchart showing pictorially the working of the algorithm 7.5.....	171
Figure 7-4 Trust-based message communication protocol in TM-IoT	173
Figure 7-5 Basic concept initial simulation settings	177
Figure 7-6 200 nodes IoT network initial simulation setting.....	182
Figure 7-7 Large-scale IoT network sample malicious cluster setting	185
Figure 7-8 Large-scale IoT network sample normal cluster setting	186
Figure 7-9 Large IoT network initial simulation setting.....	187
Figure 7-10 Rounds taken to detect malicious nodes	190
Figure 7-11 Time taken to detect a node carrying out on-off attacks	191
Figure 7-12 Number of contradictory behaviour attacks	191
Figure 7-13 Average trust score of all the IoT nodes during the simulation (n=20 nodes).....	193
Figure 7-14 Average trust score of all the IoT nodes during the simulation (n=200 nodes).....	194
Figure 7-15 Average trust score of all the IoT nodes during the simulation (n=2000 nodes).....	195

LIST OF TABLES

Table 2-1 An overview and comparative evaluation of the common approaches used for trust management in IoT	30
Table 2-2 Overview and comparative evaluation of trust management approaches in IoT focusing on scalability.....	40
Table 2-3 Overview and comparative evaluation of context-aware assessments in IoT	44
Table 2-4 Overview and comparative evaluation of the existing work on Security protocol for reliable trust management for IoT in the literature	50
Table 2-5 Overview and comparative evaluation of clustering-based trust for IoT...	57
Table 2-6 Overview and evaluation of the existing on fuzzy-logic based approaches used in IoT	63
Table 2-7 Critical evaluation of current IoT trust management approaches	68
Table 4-1 A Description of the general structure of a Message	105
Table 5-1 Trust value levels used in TM-IoT	119
Table 5-2 IoT CN trust management attributes (TMA).....	125
Table 6-1 Base case simulation parameters	146
Table 6-2 Bad-mouthing attack case simulation parameters	151
Table 6-3 Extreme memory simulation parameters.....	156
Table 7-1 A description of the general structure of a message.....	163
Table 7-2 Types of nodes in the security protocol.....	174
Table 7-3 Basic concept node initial clustering of the nodes in the simulation	177
Table 7-4 The basic concept properties of the nodes in the simulation.....	178
Table 7-5 Basic concept base case parameters	179
Table 7-6 Basic concept non-fuzzy case parameters	180

Table 7-7 (200 nodes) IoT network node initial clustering	180
Table 7-8 (200 nodes) IoT network node properties	181
Table 7-9 (200 Nodes) IoT network base case parameters	183
Table 7-10 (200 nodes) IoT network non-fuzzy case parameters.....	183
Table 7-11 (Large-scale) IoT network node initial clustering	184
Table 7-12 (Large-scale) IoT network base case parameter	188
Table 7-13 (Large-scale) IoT network non-fuzzy case parameters	189

ABSTRACT

Nowadays, the Internet of Things (IoT) connects billions of devices (things) using the Internet. The devices could be sensors, actuators etc. The number of IoT devices growing and interacting with each other raises the issues of security and trust. Most of the existing trust and security solutions do not present a comprehensive trust management solution for IoT addressing key trust management issues for the IoT. Many of the current solutions do not consider the scalability of the IoT trust management solution. With the rapid growth of IoT nodes a significant majority of the existing techniques do not address methods (or algorithms) to detect uncompliant behaviour or attacks on the trust management approach by the IoT nodes. The uncompliant behaviour may take the form of bad-mouthing attacks, on-off attacks, contradictory attacks and bad service attacks. In the existing literature there is no trust management approach that is scalable *and* resilient against attacks by uncompliant IoT nodes.

To address the above mentioned gaps in the existing literature body, in this thesis I propose an intelligent trust management platform for IoT (TM-IoT). The TM-IoT solution is centred on trust-based clustering of the IoT nodes. IoT nodes are grouped into clusters and each cluster is managed by a Master Node (MN). MN is responsible for all the trust management activities within each cluster. The Super Node (SN) oversees and manages the MNs. Intelligent fuzzy-logic based and non-fuzzy logic based algorithms are presented to counter untrustworthy IoT nodes from carrying out attacks such as bad-mouthing attacks, on-off attacks, contradictory attacks and bad service attacks.

To validate the proposed solutions in this thesis, simulations were conducted using Contiki network simulator for IoT environment (Cooja), which able to simulate large networks. Using the built prototype, I have evaluated and simulated our proposed solutions for the above-mentioned problems by using Cooja and C++ programming language. The obtained results demonstrate the effectiveness of the TM-IoT and also that of the algorithms in achieving their respective goals.