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

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.

Signature: Production Note: Signature removed prior to publication.

Date: 26/03/2019


بسم الله الرحمن الرحيم

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

LIST OF FIGURES

LIST OF TABLES

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 or 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 a 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.