UNIVERSITI TEKNOLOGI MARA

MULTIPLE TRUSTED DEVICES SEAMLESS AUTHENTICATION SCHEME

QATRUNNADA ABDUL RAHMAN

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science

Faculty of Computer and Mathematical Sciences

May 2017

ABSTRACT

Ubiquitous computing paradigm is a significant progression of computing technology as it has changed the way computing hardware and devices are being set up and used in the surrounding infrastructures. Moreover it mostly populated with smart mobile devices which have networking capability and sensors. Its dynamic and volatile nature also brought many challenging issues in security implementations, particularly on how to provide an appropriate authentication scheme for devices and applications. Therefore authentication services are expected to focus on device to device interaction which is seamless and autonomous instead of user to device interaction which requires human participation. Furthermore, devices in such environment are said to be exposed to attacks such as identity impostor, unauthorized access and also man-in-the-middle attacks. For that reason, through this research an authentication scheme is developed, not only to ensure device's authenticity but also provides seamless authentication without either needing password login or human participation. This condition is achieved by employing a trusted device to authenticate another device seamlessly. Accordingly, the requirements for the proposed authentication scheme are trust and seamlessness. The authentication scheme was developed as a mobile application using Java and was implemented on Android platform. The authentication scheme has been successfully tested on a test-bed using smartphones. In conclusion, it is hoped that this study may establish a new research dimension in the security domain along with contributing towards safeguarding devices' authenticity and the information being shared in a Ubiquitous computing environment as well as enabling seamless device to device authentication.

ACKNOWLEDGEMENT

Praise be to Allah, I am able to complete the research and finish writing the thesis after confronting many trials and tribulations along the way.

There are many people who directly and indirectly involved with my journey in accomplishing my study, hence, I would like to extend my sincerest gratitude and respect for continuing to believe in me from the first day I started my research until the last days of completing the thesis.

First and foremost, I would like to thank my parents Abdul Rahman Itam and Siti Husna Habib as well as my brothers and sister, Mu'az Abdul Rahman, Muhammad Rasyady Abdul Rahman and Mahirah Abdul Rahman for their enduring unconditional support and belief that came in various forms. I really appreciate it, thank you very much.

I would like to express my greatest gratitude and respect to my supervisor Associate Professor Dr Kamarularifin Abd Jalil, for accepting me as a supervisee, providing valuable knowledge, guidance and advice throughout my research and writing journey as well as patiently assisting me dealing with various faculty and postgraduate institute matters. Thank you very much.

I am also grateful for all the tireless help and assistance that I have received from Dr Fuziyah Ishak, Mr. Muhd Azuzuddin Muhran and Mrs. Badariah Zainal Abidin, who professionalism shines while processing and handling all postgraduates related matters efficiently. Thank you very much.

Many thanks to the Faculty of Computer and Mathematical Sciences for providing research seminars, computer laboratory and other facilities. I am also thankful to the Institute of Graduate Studies (IPSis) for their contribution in facilitating my study and granted me many chances to continue my study despite the time limitation. Thank you very much.

To everyone that I have mentioned or may not mention, I am greatly grateful for everything that you have done and may Allah blessed all your good deeds and will.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

Proliferation of devices which either have basic functions or come with mobility and sensors have become the foundation of many computing paradigms most notably Ubiquitous Computing (Symonds, 2010), Cloud Computing (Rittinghouse & Ransome, 2010) and Internet of Things (McEwen & Cassimally, 2014). Likewise, the implementations of smart mobile devices bring endless technological potentials and convenience in human life (Dominguez-Peinado & Linaje, 2013). Nevertheless, with all the benefits procure from devices expansion, yet there are plenty of challenges particularly security issues (Goode, 2010). Although there is a plethora of security issues regarding smart devices (La Polla, Martinelli, & Sgandurra, 2012) this research concentrates on authentication, specifically on how to seamlessly authenticate a device using one or more devices in Ubiquitous Computing environment. Moreover, because of the diversity of the devices that are currently available and because it is not possible to include every one of them, this study focuses on smartphone only as it is the most commonly use now. The descriptions of the thesis organizations are in section 1.7, meanwhile the research's main topics of interest are as point out in Figure 1.1.

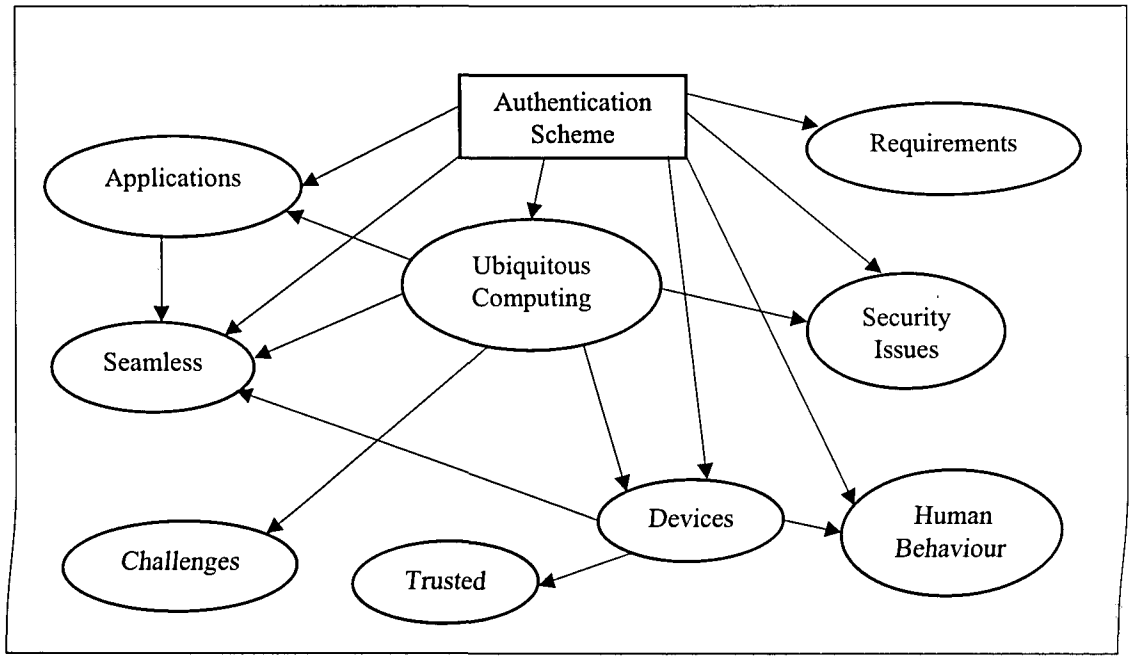

Figure 1.1: Topics of Interest