UNIVERSITI TEKNOLOGI MARA

A DELIVERY MODEL FOR ENTERPRISE CONTEXT-AWARE SECURITY AS A SERVICE IN MOBILE CLOUD COMPUTING

MUAAMAR AMER
ABDULHAFEDH AL-KUBATI

Thesis submitted in fulfilment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Computer & Mathematical Sciences

April 2019

ABSTRACT

Enterprise Mobile Cloud Computing (MCC) environments have become typical nowadays especially with practices such as Bring Your Own Device (BYOD). These environments are not only highly complex and dynamic but also have an enormous number of users and devices, thus exposing these enterprises to higher security risks with possible confidential enterprise data and information residing in their workers' personal devices. As opposed to the conventional static environments where devices are less dynamic, protecting enterprise MCC environments requires security approaches that are dynamic and fine-grained, especially approaches that are based on contexts such as the state of devices, users or environment. However, constructing MCC applications in enterprise environments with context-aware security is very complex and costly due to the diverse tasks, scalability and effectiveness issues involved. These issues may impede the adoption of context-aware security among enterprises, which may lead to an inadequate response to security risks. To overcome these issues, this thesis aims to simplify the construction of enterprise context-aware security applications in MCC, especially in BYOD environments, by proposing a model to deliver context-aware security as a service called CASECaaS. Accordingly, the research objectives are to design a model to provide context-aware security as a service, and to evaluate the feasibility and effectiveness of the model. Employing design science methodology for both objectives, the model is first designed to abstract the complexity of constructing context-aware security applications and enable enterprises and developers to seamlessly and easily empower their applications with context-aware security by subscribing to a cloud service. The model is divided into four major components: (i) a context-aware cloud backend that is responsible for context management tasks and acts as the backbone of the model, (ii) an enterprise cloud frontend to enable administrators and developers to easily define security contexts, (iii) a developer API that can be easily integrated with enterprise applications and (iv) a mobile client that reads sensor data from mobile devices and sends it to the cloud backend for analysis. The model is then implemented using scrum agile methodology to demonstrate its feasibility and provide concrete artifacts to evaluate its effectiveness. The model is rigorously evaluated using three complimentary methods; namely performance analysis, simulation and case study. The performance analysis showed an acceptable response time of 1 second for 1000 concurrent users on a scalable group of 10 low-end 1GB servers while the simulation results showed that the model is scalable and effective to be used in a multi-tenant environment with a large number of tenants and devices with an average response time of 112.6 milliseconds per request for 1000 tenants, each with 1000 devices and 100 security contexts. Thus, the performance analysis and simulation results revealed that the CASECaaS model is both scalable and effective. The case study in a real-world environment with testers on an existing university enterprise mobile application revealed that the model is feasible and can be realistically effective. The two major contributions of this thesis is delivering context-aware security as a service through the CASECaaS model and the CASECaaS prototype.

ACKNOWLEDGEMENT

First and foremost, all praise goes to Allah for his blessing in allowing me to complete this work. My sincere gratitude goes to my supervisor, Dr. Syed Ahmad Aljunid, who put in his continuous effort to make this work see the light. Without his advice, guidance and comments, this work would be far from being as complete as it is now. Many thanks to my co-supervisor, Dr. Jemal Abawajy, for his invaluable feedback and advice given during the course of this research.

My sincere thanks to my parents, whom I owe more than what words can say, and to my dear brothers and sisters for their support and prayers at all times. My sincere gratitude also goes to my parents-in-law for their continuous motivation and support.

Special thanks and appreciation to my wife who shared all the moments of this journey with me, and stood by me throughout all difficulties. Without her support, patience and prayers, completing this work would be impossible.

Finally, I would like to thank all my friends and everyone who had helped me in completing this work whether directly or indirectly.

Thank you very much.

Sincerely,

Muaamar Amer

TABLE OF CONTENTS

		Page
CONFIRMATION BY PANEL OF EXAMINERS		**ii**
AUTHOR'S DECLARATION		**iii**
ABSTRACT		**iv**
ACKNOWLEDGEMENT		**v**
TABLE OF CONTENTS		**vi**
LIST OF TABLES		**xii**
LIST OF FIGURES		**xiii**
LIST OF ABBREVIATIONS		**xvii**
CHAPTER ONE: INTRODUCTION		**1**
1.1	Introduction	1
1.2	Problem Background	2
1.3	Problem Statement	5
1.4	Research Questions	7
1.5	Research Aims and Objectives	7
1.6	Research Scope	8
1.7	Research Significance	9
1.8	Thesis organisation	9
CHAPTER TWO: LITERATURE REVIEW		**11**
2.1	Introduction	11
2.2	Cloud Computing	12
	2.2.1 Characteristics of Cloud Computing	13
	2.2.2 Cloud Computing Delivery Models	14
	2.2.3 Cloud Computing Deployment Models	15
2.3	Mobile Computing	15
2.4	Context-aware Computing	16

CHAPTER ONE
INTRODUCTION

1.1 Introduction

There are many technologies that have changed the computing landscape over the last few years. Arguably, mobile and cloud computing are amongst the most prominent ones. The fast technology advances have caused mobile devices to become an essential and integral part of our daily life. The increasing adoption, together with the nature of mobile devices such as their mobility, ubiquity and resources scarcity have increased the issues that these devices are prone to (Leavitt, 2011). These issues have become more critical, especially with the integration of mobile devices and cloud computing which forms a new computing model known as the Mobile Cloud Computing (MCC) (Cremene & Borda, 2013).

The amalgamation of these two paradigms has resulted in several growing issues, such as the power consumption, availability, integration and application of development frameworks. It is noteworthy that among these issues, security in MCC is the focus of the recent researches due to its complexity and prominence (Abid Shahzad & Mureed Hussain, 2013; Lee, 2012; Miettinen, Heuser, Kronz, Sadeghi, & Asokan, 2012; Schüring, 2011).

Security is becoming more important and relevant in MCC environments, particularly in the enterprise environments, where cloud-powered mobile devices are being widely adopted. What makes enterprise environments in MCC more challenging, as opposed to conventional environments, is that they tend to be highly heterogeneous and fast changing, and consequently raising the security magnitude for enterprises to keep their systems and confidential data protected.

Furthermore, the security of users and devices are becoming a key issue for enterprises, especially with the emerging Bring Your Own Device (BYOD) trend, whereby users are allowed to bring their preferred mobile devices to work (Brunette & Mogull, 2009; Mahesh & Hooter, 2013; Meshach & Babu, 2013).