

AN INVESTIGATION OF FACTORS AFFECTING  
SECURE SOFTWARE DEVELOPMENT PRACTICES  
ADOPTION

BY

ZULFIKAR AHMED MAHER

A thesis submitted in fulfillment of the requirement for the  
degree of Doctor of Philosophy in Information Technology

Kulliyyah of Information and Communication Technology  
International Islamic University Malaysia

MAY 2021

## ABSTRACT

Consideration of security during software development from the initial design phase has not been consistently addressed by the software developers. As a result there is an abundance of software systems with weak security. The solution proposed by the academia and the industry is to integrate security within various stages of software development life cycle. Acceptance from all the software developers and stakeholders is necessary for successful adoption of this paradigm shift within the organization. A number of secure development methodologies have been proposed by the industry and the academia for secure development but most of them were ignored by the developers. The objective of this research is to identify the factors influencing developers to adopt secure software development practices. The extent to which developers adopt secure software development practices is crucial to the successful development of secure software. In this research an integrated model is proposed and validated based on the Unified Theory of Acceptance and Use of Technology model 2 (UTAUT2). This research uses sequential explanatory mix method research design to achieve the desired research aims. A survey questionnaire is used for quantitative data collection and interviews were conducted at second qualitative stage with 04 experts from software industry. According to the proposed conceptual model the adoption of secure software development practices were determined by eight factors i.e. performance expectancy (PE), effort expectancy (EE), Social Influence (SI), facilitating conditions (FC), Habit (HT), secure software development awareness (SSDAW), Top management involvement (TPM) and Readiness for change (RFC). The model was tested on a sample of 382 software engineers and developers around Klang Valley Malaysia. Using structural equation modeling with Smart-pls software, data analysis showed that 11 out of 14 hypothetical paths were significant. The results revealed that the performance expectancy (PE), effort expectancy (EE), Social Influence (SI), facilitating conditions (FC), Habit (HT), Top management involvement (TPM), Secure Software Development awareness (SSDAW) and Readiness for change (RFC) were found to have significant effect on developer's Behavioral intention (BI) to adopt secure software development practices and on use behavior (UB) among software developers. The findings revealed that behavioral intention is explained by PE, EE, FC, SI, HT, SSDAW, TPM and RFC. Similarly, use behavior is explained by behavioral intention, BI, SSDAW and FC. Findings of the study showed that the proposed model achieved an acceptable fit with the data. Based on identified key factors, an integrated model was developed and validated to predict the adoption of secure software development practices by software developers in the industry. In second phase of the study, qualitative results were obtained from the interviews from 04 experts of the industry to confirm the quantitative results. It was found that both quantitative and qualitative approaches contributed complementary results. This research seeks to supplement the existing literature regarding security integration in software development lifecycle for secure software development and provide software development firms with strategies and guidelines to successfully introduce and integrate secure software development practices within their organization. This research provide more reliable results as compared to previous studies as both quantity and qualitative technique are used in this study to find out the factors ,opinions and suggestions from the people working in software industry.

## خلاصة البحث

لم يتم تناول مسألة الأمن أثناء تطوير البرامج من مرحلة التصميم الأولى بصورة متسقة من قِبَل مطوّري البرامج. ونتيجة لذلك كانت هناك وفرة من أنظمة البرمجيات الا انها تعاني من ضعف في مقاييس الأمان. الحل المقترح من قِبَل الأوساط الأكاديمية والصناعية هو دمج الأمن في مراحل مختلفة من دورة حياة تطوير البرمجيات. موافقةً جميع مطوري البرامج والجهات المعنية أمر ضروري لنجاح اعتماد هذا التحول في النموذج داخل المنظمة. وقد اقترحت الأوساط الأكاديمية والصناعية عددا من منهجيات التطوير المؤمّنة من أجل التنمية الآمنة، ولكن المطورين تجاهلوا معظمها. يهدف هذا البحث الى تحديد العوامل التي تؤثر على المطورين لاعتماد ممارسات تطوير البرمجيات الآمنة. إن مدى اعتماد المطورين لممارسات تطوير البرمجيات الآمنة أمر بالغ الأهمية لنجاح تطوير البرمجيات الآمنة. سيتم اقتراح نموذج متكامل في هذا البحث والتحقق من صحته على أساس النظرية الموحدة لقبول واستخدام التكنولوجيا، نموذج 2 (UTAUT2). تم استخدام الطريقة التفسيرية المتسلسلة في هذا البحث للوصول إلى الأهداف. وتم استخدام طريقة الاستبيان للدراسة الاستقصائية لجمع البيانات الكمية، وأجريت مقابلات في المرحلة النوعية الثانية مع أربعة (04) من خبراء صناعة البرمجيات. وفقا للنموذج المفاهيمي المقترح تم تحديد اعتماد ممارسات تطوير البرمجيات الآمنة من خلال ثمانية عوامل، أي متوسط العمر المتوقع للأداء (PE)، الجهد المتوقع (EE)، التأثير الاجتماعي (SI)، تسهيل الظروف (FC)، العادة (HT)، التوعية الآمنة لتطوير البرمجيات (SSDAW)، مشاركة الإدارة العليا (TPM)، الاستعداد للتغيير (RFC). حيث تم اختبار النموذج على عينة مكونة من 382 من مهندسي ومطوري البرامج حول وادي كلانج ماليزيا. باستخدام نمذجة المعادلة الهيكلية مع البرمجيات الذكية الثابتة والمتنقلة، أظهر تحليل البيانات أن 11 من أصل 14 مسارا افتراضيا كان كبيرا. كما كشفت النتائج أيضا أن متوسط العمر المتوقع لكل من الأداء (PE)، والجهد المتوقع (EE)، التأثير الاجتماعي (SI)، وتسهيل الظروف (FC)، والعادة (HT)، ومشاركة الإدارة العليا (TPM)، والوعي بتطوير البرمجيات الآمنة (SSDAW)، والاستعداد للتغيير (RFC) لها تأثير كبير على نية المطور السلوكية (BI) لاعتماد ممارسات تطوير البرامج الآمنة وعلى سلوك الاستخدام (UB) بين مطوري البرامج. وكشفت النتائج أن النية السلوكية تم تفسيرها من قبل PE، EE، FC، SI، HT، SSDAW، TPM و RFC. وبالمثل، يتم تفسير سلوك الاستخدام من خلال النية السلوكية، BI، SSDAW، FC. كما أظهرت نتائج الدراسة أن النموذج المقترح حقق توافقا مقبولا مع البيانات. واستنادا إلى العوامل الرئيسية المحددة، تم تطوير نموذج متكامل والتحقق من صحته في التنبؤ باعتماد ممارسات تطوير البرمجيات الآمنة من قبل مطوري البرامج في الصناعة. وفي المرحلة الثانية من الدراسة، تم الحصول على نتائج نوعية من المقابلات التي تم إجراؤها مع أربعة (04) خبراء في هذا المجال لتأكيد النتائج الكمية. وتبيّن أن كُلاً من النهجين الكمي والنوعي يساهمان في تحقيق نتائج تكاملية. يسعى هذا البحث إلى استكمال الدراسات السابقة المتعلقة بالتكامل الأمني في دورة حياة تطوير البرمجيات من أجل تطوير البرمجيات الآمنة وتزويد شركات تطوير البرمجيات باستراتيجيات ومبادئ توجيهية لإدخال ودمج ممارسات تطوير البرامج الآمنة بنجاح داخل مؤسساتهم. يوفر هذا البحث نتائج أكثر موثوقية مقارنة بالدراسات السابقة حيث يتم استخدام كل من التقنية الكمية والنوعية في هذه الدراسة لمعرفة العوامل والآراء والاقتراحات من الأشخاص العاملين في صناعة البرمجيات.

## **APPROVAL PAGE**

The thesis of Zulfikar Ahmed Maher has been approved by the following

---

Asadullah Shah  
Supervisor

---

Hazwani Bt Mohd Mohadis  
Co-Supervisor

---

Noor Hayani Binti Abd Rahim  
Co-Supervisor

---

Noor Azura Zakaria  
Internal Examiner

---

Ali Bin Selamat  
External Examiner

---

Zulfiqar Ali Memon  
External Examiner


---

Radwan Jamal Elatrash  
Chairman

## DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Zulfikar Ahmed Maher

Signature  .....

Date: 27-04-2021

**INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA**

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF  
FAIR USE OF UNPUBLISHED RESEARCH**

**AN INVESTIGATION OF FACTORS AFFECTING SECURE  
SOFTWARE DEVELOPMENT PRACTICES ADOPTION**

I declare that the copyright holders of this thesis are jointly owned by the Zulfikar  
Ahmed Maher and IIUM.

Copyright © 2021 Zulfikar Ahmed Maher and International Islamic University Malaysia. All rights  
reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system,  
or transmitted, in any form or by any means, electronic, mechanical, photocopying,  
recording or otherwise without prior written permission of the copyright holder  
except as provided below

1. Any material contained in or derived from this unpublished research may  
be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print  
or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieved system  
and supply copies of this unpublished research if requested by other  
universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM  
Intellectual Property Right and Commercialization policy.

Affirmed by Zulfikar Ahmed Maher

  
.....  
Signature

27-04-2021  
Date

## **DEDICATION**

*I would like to dedicate this thesis to my beloved parents for their love and unconditional support to me. I would also dedicate this thesis to my two sisters, my brother, my two kids Muhammad Amin and Yashfeen Amna and my loving wife.*

## ACKNOWLEDGEMENTS

First and foremost praises and thanks to the Almighty Allah, for his showers of blessings and help throughout my life and especially in accomplishing this research successfully.

This work would have been impossible without the continuous support and supervision of my respected supervisor, Professor Dr. Asadullah Shah for his kindness, continuous support and encouragement, and for that, I will be forever remain grateful, thank you for your support and patience.

I would like to express my full gratitude to my beloved wife who helped me all the time and have to live away without me during this period. Similarly, many thanks to my parents, sisters, brother and my kids Muhammad Amin and Yashfeen Amna, who supported me with their prayers and encouragements and they endured the pain of being away for from me. I am also thankful to all my friends for their constant encouragement and support.

I would like to express my profound gratitude to my dearest friend Dr. Saifullah Bullo for his encouragement and financial support during the entire period of my PhD studies. I am also thankful to my friend Dr. Yaqoob koondhar for his moral support and unwavering belief in my abilities to accomplish this goal.

I am also greatly indebted to the financial support of Sindh Agriculture University, Tandojam, Pakistan for my providing me funds for my studies at International Islamic University Malaysia.



# TABLE OF CONTENTS

|                                                                                    |           |
|------------------------------------------------------------------------------------|-----------|
| Abstract .....                                                                     | ii        |
| Abstractin Arabic .....                                                            | iii       |
| Approval Page.....                                                                 | iv        |
| Declaration.....                                                                   | v         |
| Dedication .....                                                                   | vii       |
| Acknowledgements.....                                                              | viii      |
| Table Of Contents .....                                                            | ix        |
| List Of Tables .....                                                               | xiv       |
| List Of Figures .....                                                              | xvi       |
| List Of Abbreviations .....                                                        | xvii      |
| <b>CHAPTER ONE: INTRODUCTION .....</b>                                             | <b>01</b> |
| 1.1 Background Of The Research .....                                               | 01        |
| 1.2 Problem Statement .....                                                        | 02        |
| 1.3 Research Questions .....                                                       | 04        |
| 1.4 Research Objectives .....                                                      | 05        |
| 1.5 Research Scope.....                                                            | 05        |
| 1.6 Significance Of Research .....                                                 | 06        |
| 1.7 Research Motivation.....                                                       | 07        |
| 1.8 Research Methodology .....                                                     | 08        |
| 1.9 Thesis Structure .....                                                         | 09        |
| 1.10 Chapter Summary .....                                                         | 11        |
| <b>CHAPTER TWO: LITERATURE REVIEW.....</b>                                         | <b>12</b> |
| 2.1 Background Of The Research .....                                               | 13        |
| 2.1.1 Security Engineering .....                                                   | 13        |
| 2.1.2 Secure Architecture .....                                                    | 14        |
| 2.1.3 Search Strategy for the Literature Review .....                              | 15        |
| 2.2 Secure Software Development Practices And Methodologies.....                   | 15        |
| 2.3 Human Factors In Software Security .....                                       | 23        |
| 2.4 Secure Development Adoption Factor Identification.....                         | 28        |
| 2.5 Security Tools Adoption .....                                                  | 32        |
| 2.6 Information System Acceptance Models And Theories.....                         | 33        |
| 2.6.1 Theory of Reasoned Action (TRA) .....                                        | 34        |
| 2.6.2 Technology Acceptance Model (TAM) .....                                      | 36        |
| 2.6.3 Actual TAM.....                                                              | 36        |
| 2.6.4 Extended TAM 2 .....                                                         | 38        |
| 2.6.5 Extended TAM 3 .....                                                         | 39        |
| 2.6.6 Theory of Planned Behavior.....                                              | 40        |
| 2.6.7 Innovation Diffusion Theory (IDT).....                                       | 42        |
| 2.6.8 Unified Theory of Acceptance and Use of Technology<br>(UTAUT) .....          | 43        |
| 2.6.9 Extended Unified Theory of Acceptance and Use of<br>Technology (UTAUT2)..... | 45        |
| 2.7 Major Approaches For Change Management .....                                   | 47        |

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| 2.7.1 ADKAR Model .....                                                    | 48        |
| 2.7.2 Bridge's Transition Model .....                                      | 48        |
| 2.7.3 Kotter's Change Management Theory .....                              | 49        |
| 2.7.4 Lewin's Change Management Model .....                                | 50        |
| 2.7.5 McKinsey 7 S Model.....                                              | 51        |
| 2.7.6 Nudge Theory .....                                                   | 52        |
| 2.8 Chapter Summary .....                                                  | 52        |
| <b>CHAPTER THREE: RESEARCH MODEL AND HYPOTHESIS.....</b>                   | <b>53</b> |
| 3.1.1 Introduction .....                                                   | 53        |
| 3.1.2 Rational for Research .....                                          | 55        |
| 3.2 Proposed Research Model .....                                          | 55        |
| 3.3 Hypothesis Development Behavioral .....                                | 59        |
| 3.3.1 Intention (BI) .....                                                 | 59        |
| 3.3.2 Effort Expectancy (EE) .....                                         | 60        |
| 3.3.3 Performance Expectancy (PE).....                                     | 60        |
| 3.3.4 Social Influence (SI).....                                           | 61        |
| 3.3.5 Facilitating Conditions (FC).....                                    | 61        |
| 3.3.6 Top Management Involvement (TPM).....                                | 62        |
| 3.3.7 Habit .....                                                          | 63        |
| 3.3.8 Readiness for Change .....                                           | 64        |
| 3.3.9 Secure Software Development Awareness.....                           | 65        |
| 3.4 Chapter Summary .....                                                  | 66        |
| <b>CHAPTER FOUR: RESEARCH METHODOLOGY .....</b>                            | <b>67</b> |
| 4.1 Introduction .....                                                     | 67        |
| 4.2 Research Approaches .....                                              | 67        |
| 4.3 Mixed Methods.....                                                     | 67        |
| 4.4 Sequential Explanatory Strategy .....                                  | 68        |
| 4.5 Why Mixed Method Research .....                                        | 68        |
| 4.6 Research Design .....                                                  | 69        |
| 4.6.1 Rationale For Each Step-In Design .....                              | 70        |
| 4.7 Data Collection .....                                                  | 72        |
| 4.7.1 Questionnaires.....                                                  | 73        |
| 4.7.2 Interviews.....                                                      | 73        |
| 4.8 The Population And Sample For Quantitative Data.....                   | 74        |
| 4.8.1 Type Of Sample .....                                                 | 74        |
| 4.8.2 Sampling Method Used in This Research.....                           | 75        |
| 4.8.3 Sample Size.....                                                     | 75        |
| 4.8.4 Data Collection .....                                                | 77        |
| 4.9 Questionnaire Content Development.....                                 | 79        |
| 4.10 Qualitative Data .....                                                | 83        |
| 4.10.1 The Population And Sample For Qualitative Data .....                | 83        |
| 4.10.2 Sampling technique.....                                             | 83        |
| 4.10.2.1 Expert Sampling.....                                              | 83        |
| 4.10.2.2 Sample Size.....                                                  | 83        |
| 4.10.2.3 Access Permission To Participants /Institutional<br>Approval..... | 83        |
| 4.10.3 Type of data to collect / Interview / One-on-One Interview.....     | 84        |

|                                                                 |                                                                               |            |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------|------------|
| 4.10.3.1                                                        | Process of Interview/Conducting Interview .....                               | 84         |
| 4.10.3.2                                                        | Data Recording Procedure.....                                                 | 84         |
| 4.10.4                                                          | Field and Ethical Issues .....                                                | 84         |
| 4.11                                                            | Pre-Testing And Pilot Study.....                                              | 85         |
| 4.12                                                            | Pre-Testing The Questionnaire.....                                            | 85         |
| 4.13                                                            | Pilot Study .....                                                             | 86         |
| 4.14                                                            | Demographic Details .....                                                     | 86         |
| 4.15                                                            | General Assessment Of Awareness About Software Security .....                 | 87         |
| 4.16                                                            | Reliability Of The Instrument.....                                            | 90         |
| 4.17                                                            | Pilot Study Conclusion .....                                                  | 92         |
| <b>CHAPTER FIVE: DATA ANALYSIS.....</b>                         |                                                                               | <b>93</b>  |
| 5.1                                                             | Introduction .....                                                            | 93         |
| 5.2                                                             | Response Rate.....                                                            | 94         |
| 5.3                                                             | Data Screening.....                                                           | 95         |
| 5.3.1                                                           | Missing Data Identification.....                                              | 95         |
| 5.3.2                                                           | Missing Data Treatment.....                                                   | 98         |
| 5.3.3                                                           | Outliers Examination .....                                                    | 98         |
| 5.3.4                                                           | Demographic Data Analysis .....                                               | 100        |
| 5.4                                                             | Descriptive Analysis.....                                                     | 104        |
| 5.4.1                                                           | Effort Expectancy (EE) Construct.....                                         | 104        |
| 5.4.2                                                           | Social Influence (SI) Construct .....                                         | 105        |
| 5.4.3                                                           | Top Management Involvement (TPM) Construct .....                              | 105        |
| 5.4.4                                                           | Habit Construct.....                                                          | 106        |
| 5.4.5                                                           | Secure Software Development Awareness Construct .....                         | 106        |
| 5.4.6                                                           | Performance Expectancy (PE) Construct .....                                   | 107        |
| 5.4.7                                                           | Readiness for Change Construct .....                                          | 108        |
| 5.4.8                                                           | Behavioral Intention Construct.....                                           | 108        |
| 5.4.9                                                           | Use Behavior Construct.....                                                   | 109        |
| 5.5                                                             | Reliability Test .....                                                        | 110        |
| 5.6                                                             | Structural Equation Modeling (SEM).....                                       | 111        |
| 5.6.1                                                           | Measurement Model .....                                                       | 112        |
| 5.6.2                                                           | Construct Validity .....                                                      | 114        |
| 5.6.3                                                           | Convergent Validity .....                                                     | 114        |
| 5.6.4                                                           | Discriminant Validity.....                                                    | 117        |
| 5.6.5                                                           | Structural Model .....                                                        | 121        |
| 5.6.6                                                           | Path estimation ( $\beta$ ): .....                                            | 124        |
| 5.6.7                                                           | Modifying the Structural Model by Eliminating Non-<br>Significant Paths ..... | 133        |
| 5.6.8                                                           | Coefficient of Determination ( $R^2$ ).....                                   | 134        |
| 5.6.9                                                           | Predictive Relevance $Q^2$ .....                                              | 135        |
| 5.6.10                                                          | Effect Size $f^2$ .....                                                       | 136        |
| 5.7                                                             | Chapter Summary .....                                                         | 137        |
| <b>CHAPTER SIX: QUALITATIVE DATA ANALYSES AND RESULTS .....</b> |                                                                               | <b>139</b> |
| 6.1                                                             | Introduction .....                                                            | 139        |
| 6.2                                                             | Research Approach For Qualitative Data .....                                  | 139        |
| 6.3                                                             | Data Analyses .....                                                           | 139        |
| 6.4                                                             | Results Of Qualitative Data Analyses .....                                    | 140        |

|                                                                           |            |
|---------------------------------------------------------------------------|------------|
| 6.5 Themes And Subthemes .....                                            | 142        |
| 6.5.1 Theme 1 Organizational Factors .....                                | 142        |
| 6.5.2 Subtheme-1a Policy Enforcement .....                                | 142        |
| 6.5.3 Subtheme-1b Change Management.....                                  | 143        |
| 6.5.4 Subtheme-1c Security Team.....                                      | 144        |
| 6.5.5 Sub theme 2-a Managers .....                                        | 145        |
| 6.5.6 Sub theme 2-b Security Expert.....                                  | 145        |
| 6.5.7 Theme 3 Motivating Factors .....                                    | 146        |
| 6.5.8 Sub theme 3-a Training .....                                        | 147        |
| 6.5.9 Subtheme 3-b Incentives .....                                       | 148        |
| 6.5.10 Sub theme 3-c Security Awareness.....                              | 148        |
| 6.5.11 Sub theme 3-d Performance Expectancy .....                         | 149        |
| 6.5.12 Sub theme 3-e Facilitating Conditions.....                         | 150        |
| 6.5.13 Theme 4- Attitude towards SSD .....                                | 150        |
| 6.5.14 Sub theme 4-a Demographic Characteristics .....                    | 150        |
| 6.5.15 Sub theme 4-b Need to use SSD .....                                | 151        |
| 6.5.16 Theme 5 Hardness/Issues Towards SSD Adoption .....                 | 151        |
| 6.5.17 Sub Theme 5-A No Clear Guidelines .....                            | 152        |
| 6.5.18 Sub theme 5-b Strict Project Timeline.....                         | 152        |
| 6.5.19 Sub Theme 5-C Lack Of SSD Knowledge .....                          | 152        |
| 6.5.20 Sub theme 5-D Ambiguous security requirements .....                | 153        |
| 6.6 Chapter Summary .....                                                 | 153        |
| <b>CHAPTER SEVEN: DISCUSSIONS.....</b>                                    | <b>155</b> |
| 7.1 Introduction .....                                                    | 155        |
| 7.2 Quantitative Results Discussion .....                                 | 155        |
| 7.2.1 Response Rate .....                                                 | 156        |
| 7.2.2 Participants Demographic Characteristics .....                      | 156        |
| 7.2.3 General Assessment Of Secure Software Development<br>Awareness..... | 157        |
| 7.2.4 Construct And Items Discussions .....                               | 159        |
| 7.3 Hypothesis Testing .....                                              | 165        |
| 7.3.1 Impact of BI on UB.....                                             | 165        |
| 7.3.2 Impact of EE on BI .....                                            | 166        |
| 7.3.3 Impact of PE on BI .....                                            | 166        |
| 7.3.4 Impact of SI on BI.....                                             | 167        |
| 7.3.5 Impact of FC on BI and UB .....                                     | 167        |
| 7.3.6 Impact of TPM on BI and UB.....                                     | 168        |
| 7.3.7 Impact of Habit on BI and UB .....                                  | 169        |
| 7.3.8 Impact of RFC on BI and UB .....                                    | 170        |
| 7.3.9 Impact of SSDAW on BI and UB.....                                   | 171        |
| 7.4 Summary Of Quantitative Discussion .....                              | 172        |
| 7.5 Qualitative Results Discussion .....                                  | 172        |
| 7.5.1 Introduction.....                                                   | 172        |
| 7.5.2 Response Rate .....                                                 | 173        |
| 7.5.3 Demographic Discussion .....                                        | 173        |
| 7.5.4 Discussion On Themes And Subthemes .....                            | 174        |
| 7.6 Mixed Methods Results .....                                           | 178        |
| 7.6.1 Answering the Research Question .....                               | 179        |

|                                                                                          |            |
|------------------------------------------------------------------------------------------|------------|
| 7.6.2 Expanding on the Quantitative Results .....                                        | 180        |
| 7.6.3 Additional Ideas Raised In Qualitative Part.....                                   | 180        |
| 7.6.4 Differences between the Quantitative Results and the<br>Qualitative Findings. .... | 182        |
| 7.6.5 Confirmation of Results .....                                                      | 182        |
| 7.6.6 Demographic Characteristics .....                                                  | 182        |
| 7.6.7 General Assessment Of Security Awareness .....                                     | 183        |
| 7.6.8 Construct Confirmation .....                                                       | 184        |
| 7.6.8.1 Dependent Variables (Use behavior, Behavioral<br>Intention) .....                | 184        |
| 7.6.8.2 Independent Variables.....                                                       | 185        |
| 7.6.9 Completeness of Results .....                                                      | 186        |
| <b>CHAPTER EIGHT: CONCLUSION .....</b>                                                   | <b>187</b> |
| 8.1 Introduction .....                                                                   | 187        |
| 8.2 Research Questions.....                                                              | 187        |
| 8.3 Research Implications.....                                                           | 190        |
| 8.3.1 Theoretical Implications .....                                                     | 190        |
| 8.3.2 Practical Implications.....                                                        | 191        |
| 8.4 Summary Of The Research Contribution .....                                           | 192        |
| 8.5 Limitations Of This Research.....                                                    | 193        |
| 8.6 Future Work.....                                                                     | 194        |
| <b>REFERENCES.....</b>                                                                   | <b>195</b> |
| APPENDIX A: Quantitative Questionnaire.....                                              | 214        |
| APPENDIX B: Qualitative Questionnaire.....                                               | 218        |
| APPENDIX C: Expert Profile .....                                                         | 220        |
| APPENDIX D: Publications .....                                                           | 221        |

## LIST OF TABLES

| <u>Table No.</u> |                                                                 | <u>Page No.</u> |
|------------------|-----------------------------------------------------------------|-----------------|
| 2.1              | Key Constructs of UTAUT                                         | 44              |
| 4.1              | Research Design Steps                                           | 69              |
| 4.2              | Questionnaires Response Rate                                    | 78              |
| 4.3              | Survey Questionnaire And The Source Of Items                    | 80              |
| 4.4              | Demographic Details                                             | 86              |
| 4.5              | General assessment of Security Practices                        | 88              |
| 4.6              | Reliability of Constructs                                       | 91              |
| 5.1              | Item-Level Missing Data                                         | 96              |
| 5.2              | Construct/Variable-Level Missing Data                           | 97              |
| 5.3              | Randomness of Missing Data                                      | 98              |
| 5.4              | Multivariate Outlier Detection                                  | 99              |
| 5.5              | Demographic Details of the Respondents                          | 100             |
| 5.6              | General assessment of Security Practices                        | 120             |
| 5.7              | Descriptive Statistics of EE Construct                          | 105             |
| 5.8              | Descriptive Statistics of SI Construct                          | 105             |
| 5.9              | Descriptive Statistics of HM Construct                          | 106             |
| 5.10             | Descriptive Statistics of Habit Construct                       | 106             |
| 5.11             | Descriptive Statistics of Secure Software Development Awareness | 107             |
| 5.12             | Descriptive Statistics of PE Construct                          | 107             |
| 5.13             | Descriptive Statistics of PIIT Construct                        | 108             |
| 5.14             | Descriptive Statistics of Behavioral Intention Construct        | 109             |
| 5.15             | Descriptive Statistics of Use Behavior Construct                | 109             |
| 5.16             | Cronbach's Alpha Values                                         | 111             |

|      |                                                |     |
|------|------------------------------------------------|-----|
| 5.17 | Multivariate Analysis Methods                  | 112 |
| 5.18 | Criterion for Assessment of Measurement Model  | 113 |
| 5.19 | Summary of Measurement Model Results           | 115 |
| 5.20 | Outer/Factor Loading with Cross-Loadings       | 117 |
| 5.21 | Fornell Correlations and Discriminant Validity | 119 |
| 5.22 | Criterion for Assessment of Structural Model   | 124 |
| 5.25 | Results of Effect Size ( $f^2$ ) Values        | 136 |
| 6.1  | Demographic Data                               | 140 |

## LIST OF FIGURES

| <u>Figure No.</u> |                                                    | <u>Page No.</u> |
|-------------------|----------------------------------------------------|-----------------|
| 2.1               | SDL's Awareness Among Developers                   | 28              |
| 2.2               | Reasons For Not Adopting SDL's By Developers       | 29              |
| 2.3               | Theory of Reasoned Action                          | 35              |
| 2.4               | Actual TAM                                         | 37              |
| 2.5               | TAM Excluding Mediator                             | 38              |
| 2.6               | TAM 2                                              | 39              |
| 2.7               | TAM3                                               | 40              |
| 2.8               | Theory of Planned Behavior                         | 41              |
| 2.9               | Innovation Diffusion Theory                        | 42              |
| 2.10              | Unified Theory of Acceptance and Use of Technology | 44              |
| 2.11              | UTAUT2                                             | 46              |
| 3.1               | Proposed Research Model                            | 58              |
| 4.1               | Research Design Process                            | 71              |
| 5.1               | Data Analysis Flow Chart                           | 94              |
| 5.2               | Measurement Model                                  | 120             |
| 5.3               | Result of Bootstrapping                            | 123             |
| 5.4               | Structural Model                                   | 127             |
| 5.5               | Final Model                                        | 134             |
| 6.1               | Themes and Subthemes                               | 141             |



## LIST OF ABBREVIATIONS

|           |                                                         |
|-----------|---------------------------------------------------------|
| BI        | Behavioral Intention                                    |
| CC        | Common Criteria                                         |
| CFA       | Confirmatory Factor Analysis                            |
| CLASP     | Comprehensive, Lightweight Application Security Process |
| DOI       | Diffusion of Innovation                                 |
| DTPB      | Decomposed Theory of Planned behavior                   |
| EE        | Effort Expectancy                                       |
| EFA       | Exploratory Factor Analysis                             |
| FC        | Facilitating Condition                                  |
| GOF       | Goodness of Fit                                         |
| HT        | Habit                                                   |
| ICT       | Information and Communication Technology                |
| IDT       | Innovations Diffusion Theory                            |
| IoT       | Internet of Things                                      |
| IS        | Information System                                      |
| MM        | Measurement Model                                       |
| MM        | Motivational Model                                      |
| MPCU      | Model of PC Utilization                                 |
| MPS       | Malaysian Public Service Organization                   |
| Open SAMM | Open Software Assurance Maturity Model                  |
| OSS       | Open source software                                    |
| PBC       | Perceived behavioral control                            |
| PE        | Performance Expectancy                                  |
| PEOU      | Perceived Ease of Use                                   |
| PN        | Perceived Need                                          |
| PU        | Perceived Usefulness                                    |
| RFC       | Readiness for change                                    |
| SCT       | Social Cognitive Theory                                 |
| SD        | Software Development                                    |
| SDL       | Security Development Lifecycle                          |
| SDLC      | Software Development Lifecycle                          |
| SEM       | Structural Equation Modeling                            |
| SI        | Social Influence                                        |
| SMEs      | Small and Medium Enterprises                            |
| SOP       | standards Operational Procedures                        |
| SSD       | Secure Software Development                             |
| SSDAW     | Secure Software Development Awareness                   |
| SSDM      | Secure Software Development Model                       |
| SPSS      | Statistical Package for Social Sciences                 |

|        |                                                     |
|--------|-----------------------------------------------------|
| TAM    | Technology Acceptance Model                         |
| TPB    | Theory of Planned Behavior                          |
| TPM    | Top Management Involvement                          |
| TRA    | Theory of Reasoned Action                           |
| TSP    | Team Software Process                               |
| UB     | User Behavior                                       |
| UML    | Unified Modeling Language                           |
| UTAUT  | Unified Theory of Acceptance and Use of Technology  |
| UTUAT2 | Unified Theory of Acceptance and Use of Technology2 |

# CHAPTER ONE

## INTRODUCTION

### 1.1 BACKGROUND OF THE RESEARCH

Software applications are often produced in the fastest and cheapest way, with no or little focus on security. Software security is a relatively new field and has been pointed as an afterthought. Firstly, the software is released, and then the security problems that are found during its usage are fixed. Realizing security at later stages of software development (SD) results in increased risks of occurring security flaws. Fixing system risks and vulnerabilities after software development cost high for developers and users. This fact can be observed when reading the release notes of a software product, which usually indicate some patches to fix vulnerabilities. The problem with this reactive approach is that there could be potential consequences with the exploitation of the discovered breaches such as brand reputation damage and money losses.

Software security is essential for protecting assets, resources and the information of an organization and the individuals. Data is the most valuable asset and to protect the data of an organization is very important. There is a need of consideration for software security during software development process. Usually, security is often addressed after the software implementation phase and its being ignored at initial phases of the software development. Historically, security has been considered as an afterthought in software development, where the focus was mainly on functionality (McGraw, 2006). However, increasing threats led to acknowledging the importance of addressing security in the development lifecycle (Geer, D. 2010). From recent past, big software firms are taking initiatives for security integration within their development life cycle, Such as, Google has appointed an independent

Security Team which is responsible for reviewing security during the design and implementation phases of their software development, this team also provides consultation and related remedies on security risks . Microsoft has employed a security-oriented software development process called Microsoft Security Development Lifecycle (SDL) since 2004 (Chess & McGraw, 2004). This process considers security concerns from the early stages of software development life cycle (SDLC). Many proposals have been presented for incorporation of security in SDLC (Fonseca & Vieira, 2013) by integrating security from the early stages of the SDLC when vulnerabilities are less expensive to mitigate. Considering security at early stages has showed much better outcomes. as compared to when security was viewed as an additional task (Microsoft. 2019).

Despite these efforts, software vulnerabilities persist (NVD, 2019). With increasing connectivity and progress towards the Internet of Things (IoT), threats have changed (Howard & Lipner, 2006) and software security is often critical. Also, the security threats are not limited to the large enterprises; even Small and Medium Enterprises (SMEs) are frequently been targeted by the cyber-attacks (J. Sophy, 2019).

## **1.2 PROBLEM STATEMENT**

Developing secure software is not a straight forward task; expertise from a number of people is needed to accomplish this task. Initially requirement engineers and software designer are required to collect security requirements along with the functional requirements of the software to be developed to accommodate the software developers. From software functional and non-functional requirements, its architectural diagrams are defined in a way that it can facilitate software developers to develop secure software system. There are a number of considerations in this process

of developing secure software which includes; technical limitations of the software developers, a set of constraints, and functional goals of the system to be developed. Taking into consideration that most of developers are expert at coding functionality of the software system but they lack expertise in security implementation. Developing a secure system needs expertise in secure software development practices. Proper knowledge of security implementation and how to develop security mechanisms in a software system is a challenging job for a developer.

From the recent past, software industry has focused on the need of the support for software developers to adequately address security and privacy concerns (Acar et al. 2016; Green & Smith, 2016; Pieczul et al. 2017). Developers, although considered experts in their own domain, are typically not security experts (Green & Smith, 2016). They sometimes make mistakes that affect the privacy and security of their whole system (Acar et al. 2016; Green & Smith, 2016]. It is difficult for the non-security expert software developers to understand security constraints as there is a lack of common methods related to security modeling. Most of the software developers lack security expertise (Bouaziz & Kammoun, 2016) due to which they face difficulty in deploying security constraints (Vieira and Antunes, 2013). The complexity of security mechanisms makes it difficult for an ordinary software developer to understand the security mechanisms and fulfill the security requirements to achieve the secure implementations goal. Identifying potential security threats and security vulnerabilities during software development process is not easy for software developers as they are not usually security experts (Kobashi et al. 2015). For this challenge, there is no clear solution has been provided (Fernandez, 2009). Software developers find it difficult to select appropriate security mechanisms because a number of security mechanism are present in the literature as well as from the industry without providing concrete

guidelines for their use, secondly location of the security code within the system along with its abstraction is also deemed difficult by the developers (Bouazizet et al., 2011). Software developers need concrete guidelines for developing secure applications (Lodderstedt et al., 2002). Guiding developers about different security attacks and their mitigation within the developing system is also very important (Lincke et al., 2012). Lack of security tools to model and analyze the secure system is also discussed by (Vysoky., 2012). A number of methods have been presented in literature for addressing security requirements at early software development phases, but there is a lack of connection between these security requirements in relation to design of secure architectures (Howard & Lipner, 2009). Despite of the fact that there are a number of methodologies present for the development of secure software system, majority of the developers are reluctant to use them because most of the software developers lack the skills and experience needed to use these methodologies. However, software developers working in the industry might not be willing to use these methodologies because of the additional time, costs, and effort needed for secure development.

### **1.3 RESEARCH QUESTIONS**

In this research work, there are three research questions which help to achieve the research objectives. These questions will also help to understand the overall purpose and contribution of this research.

RQ 1: What is the current adoption level of security practices in the software industry?

RQ 2 Which are the influencing factors for adoption and failure of security practices among programmers and developers for secure software development?

RQ 3 What are essential behavioral factors that affect developer's intention to use secure software development practices?

#### **1.4 RESEARCH OBJECTIVES**

There are also three objectives of this research to answer the research questions.

1. To assess the adoption Level of security practices in the software industry.
2. To examine the influencing factors for adoption and failure of security practices among programmers and developers for secure software development in industry.
3. To develop a model of the determinants of secure software development practices adoption based on technology acceptance model 2 (UTUAT2) and other grounded theories.

#### **1.5 RESEARCH SCOPE**

Software security focuses on the resistance of software applications to vulnerability exploitation. This is different from security functions, which can be expressed as functional requirements, such as authentication and authorization (Xie, 2011). In this thesis, we focus on ensuring software security with special focus on the human in the development loop. Security functions are out of the scope of this thesis. Thus, terms such as "security" and "secure" used herein refer to software security. The scope of this study covers adoption of secure software development practices among software developers for the understanding and better adoption of secure software development practices in software industry. The main purpose of this investigation is to measure the behavioral intention of the software developers towards adoption of secure software

development practices. While going through literature review, it was analyzed and found that, limited research publications is available on this area mostly focused on limited number of respondents and more precisely in the context of Malaysia. As there are more number of private sector companies/organization are involved in huge number of software development projects in Malaysia and the researcher is a foreigner student and he does not have access to public sector organizations in Malaysia, therefore, this study is intended to investigate the UTUAT2 model along with some external constructs in the context of adoption of secure software development practices. Data collection was performed using survey method from private sector software development companies/organizations within Klang Valley Malaysia.

In addition, the main focus of this study are human actors (such as; software engineers and developers) who are responsible for developing secure software. This study is intended to understand the behavior of software developers that how they deal with the process of developing a secure software system. Technological support to secure software development process is out of the scope of this research.

## **1.6 SIGNIFICANCE OF RESEARCH**

The significance of this research can be defined as, this study will contribute by closing the research gap by performed a theoretical based empirical investigation of the determinants related to secure software development use by the developers in software industry. Second, it was noted from the prior research that technology acceptance models like UTAUT and UTAUT2 cannot be a complete and final version to be evaluated in any environment. Thus, UTAUT2 model has been extended in this study by developing, validating a theoretical model based on collected empirical data during this study. The model validated in this study will contribute to more systematic