Faculty of Information and Communication Technology

ELICITING SECURITY REQUIREMENTS FOR INTERNET OF THINGS SOFTWARE APPLICATION DEVELOPMENT USING SEMI-FORMALIZED MODEL APPROACH

Asma Asdayana binti Ibrahim

Doctor of Philosophy

2022

ELICITING SECURITY REQUIREMENTS FOR INTERNET OF THINGS SOFTWARE APPLICATION DEVELOPMENT USING SEMI-FORMALIZED MODEL APPROACH

ASMA ASDAYANA BINTI IBRAHIM

A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy

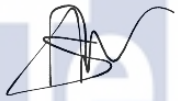
Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2022

DECLARATION

I declare that this thesis entitled “Eliciting Security Requirements for Internet of Things Software Application Development using Semi-formalized Model Approach” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : 

Name : Asma Asdayana binti Ibrahim

Date : 8 February 2022

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Doctor of Philosophy.

Signature : .....

Supervisor Name : Professor Ts. Dr. Massila binti Kamalrudin

Date : 8 February 2022

DEDICATION

I dedicate this thesis to

my beloved husband, Ir. Mohd Khalis Baharom,

my adorable children, Aish Daniyal, Alisha Sofea and Adelia Inara

my supportive parent, Hj. Ibrahim Ahmad and Hjh. Esah Mohamad,

my mother in law, Hjh. Hasnah and all my siblings.

For everything you all have done and continue to do, thank you very much!

I feel so blessed with you all by my side.

ABSTRACT

In today's era, there is a rapid increase in the demand for Internet of Thing (IoT) applications. Thus, securing the information content delivered among various entities involved in the IoT applications development has become an important issue. It is also identified that high cost is needed in implementing a secured IoT application as it requires efforts, skills, and knowledge to understand the security concern, especially when developers and requirement engineers do not have any formal training in software engineering and eliciting security requirements. Furthermore, security requirement is an important intangible requirement that could be taken as a burden on the smooth functioning of the system or application. Requirement engineers without adequate experience in security are at risk of overlooking security requirement, which frequently leads to the act of misuse. In addition, requirements engineers who are unfamiliar with the IoT applications face problems to elicit accurate security requirements. Motivated by this problem, the main objectives of this study are three-fold. The first objective is to determine the security requirements for the IoT applications. Secondly, the study aims to propose a model-based approach for security requirements elicitation of IoT application and finally, to evaluate the approach in terms of usability and correctness in eliciting the security requirements for the IoT applications. A model-based approach was developed in adopting Model-Design Driven (MDD) approach with semi-formalized models: Essential Use Cases (EUCs) and Essential User Interface (EUI). Security requirement pattern library and IoT technologies pattern library were developed to assist the correct elicitation from the EUC model. A new model was proposed to be a reference for IoT developers in developing secure IoT applications software. Here, automated tool support was also developed to realise the approach. Finally, a comprehensive evaluation of the approach, comprising the comparison study between the existing tool and our tool, experiments of correctness test, and usability test were conducted. This study also evaluated the feedback from the industry experts, especially on the usability of the approach and tool support. In summary, the findings of the evaluation show that our approach contributed to the body of knowledge of requirements engineering, especially in enhancing the performance and correctness level of security requirement elicitation and its usability for end-to-end elicitation. It is found that the approach was able to enhance the correctness level of the elicited security attribute compared to the manual task, and produce the correct generation of security requirement. The results of the usability test by the novice and experts show that the approach is useful and helpful in eliciting security requirements application software development and is able to ease the elicitation process of security requirements and technologies involved in IoT applications software development.

PENCUNGKILAN KEPERLUAN KESELAMATAN UNTUK PEMBANGUNAN PERISIAN APLIKASI INTERNET PELBAGAI BENDA MENGGUNAKAN KAEDAH MODEL SEPARA-FORMAL

ABSTRAK

Pada zaman sekarang, terdapat peningkatan permintaan aplikasi Internet Pelbagai Benda (IoT) yang pesat. Oleh itu, penyampaian maklumat di antara pelbagai entiti yang terlibat dalam pembangunan aplikasi IoT telah menjadi isu penting. Perkara ini dikenalpasti memerlukan kos yang tinggi untuk memastikan aplikasi IoT yang selamat kerana memerlukan usaha, kemahiran dan pengetahuan untuk memahami masalah keselamatan, terutama ketika pemaju dan jurutera keperluan tidak mempunyai latihan formal dalam bidang kejuruteraan perisian dan menimbulkan syarat keselamatan. Selain itu, keperluan keselamatan adalah salah satu keperluan yang paling penting untuk kelancaran fungsi sistem atau aplikasi. Jurutera keperluan tanpa pengalaman yang mencukupi berisiko mengabaikan keperluan keselamatan, yang sering menyebabkan tindakan penyalahgunaan. Di samping itu, jurutera keperluan yang tidak biasa dengan aplikasi IoT menghadapi masalah untuk mendapatkan keperluan keselamatan yang tepat. Didorong oleh masalah ini, objektif utama kajian ini adalah tiga tujuan. Pertama, adalah untuk menentukan keperluan keselamatan untuk aplikasi IoT. Kedua, untuk mencadangkan pendekatan berasaskan model untuk mendapatkan syarat keselamatan dan akhirnya, menilai pendekatan dari segi kebolehgunaan dan kebenaran dalam mendapatkan syarat keselamatan untuk aplikasi IoT. Pendekatan berasaskan model dengan mengadaptasi pendekatan Rekabentuk Berpandukan Model (MDD) telah dibangunkan dengan model separa- formal: Kes Berguna Penting (EUCs) dan Antara-muka Penting (EUI). Pangkalan data keperluan keselamatan dan pangkalan data teknologi IoT juga dibangunkan untuk membantu pembentukkan model EUC. Satu model juga direka untuk menjadi rujukan bagi pembangun IoT dalam mengembangkan aplikasi IoT yang selamat. Di sini, sokongan alat automatik juga dikembangkan untuk merealisasikan pendekatan tersebut. Akhirnya, penilaian komprehensif pendekatan, yang merangkumi kajian perbandingan antara alat yang ada, eksperimen ujian ketepatan dan ujian kebolehgunaan dilakukan. Di sini, maklum balas daripada pakar industri telah dinilai terutamanya mengenai kebolehgunaan pendekatan dan sokongan alat. Ringkasnya, penilaian menunjukkan bahawa pendekatan ini mampu menyumbang kepada pengetahuan mengenai kejuruteraan keperluan terutama dalam meningkatkan prestasi dan tahap kebenaran ketentuan keselamatan dan kebolehgunaannya. Didapati bahawa pendekatan dapat meningkatkan tahap ketepatan atribut keselamatan yang diperlukan berbanding secara manual, dan menghasilkan keperluan keselamatan yang betul. Kemudian, hasil ujian kebolehgunaan oleh perintis dan pakar menunjukkan bahawa pendekatan ini berguna dan bermanfaat dalam keperluan keselamatan pada tahap awal pembangunan perisian aplikasi dan dapat meringankan proses pemenuhan syarat keselamatan, juga teknologi yang terlibat dalam pembangunan perisian aplikasi IoT.

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful First and foremost, I would like to thank and praise Allah S.W.T, for everything I received since the beginning of my life. I would like to extend my appreciation to the Universiti Teknikal Malaysia Melaka (UTeM) for providing the research platform. Thank you also to the Malaysian Ministry of Higher Education (MoHE) for the financial assistance.

My utmost appreciation goes to my main supervisor, Professor Ts. Dr. Massila binti Kamalrudin Universiti Teknikal Malaysia Melaka (UTeM) for all her support, advice and inspiration. Her constant patience for guiding and providing priceless insights will forever be remembered. Also, to my co-supervisor, Assoc. Prof. Dr. Mohd Faizal bin Abdollah, Universiti Teknikal Malaysia Melaka (UTeM) who constantly supported my journey. My special thanks go to all my postgraduate friends and officemates of Sultan Azlan Shah Polytechnic for all the help and support I received from them.

Last but not least, from the bottom of my heart, I would like to express my sincerest gratitude to my beloved husband, Ir. Mohd Khalis bin Baharom, for his encouragement and has been the pillar of strength in all my endeavors. My eternal love also to all my children, Aish Daniyal, Alisha Sofea and Adelia Inara, for their patience and understanding. I would also like to thank my beloved parents and mother-in-law for their endless support, love and prayers. Finally, thank you to all the individual(s) who had provided me the assistance, support, and inspiration to embark on my study.

.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
SDL	-	Security Development Lifecycle
RE	-	Requirement Engineer
SE	-	Software Engineering
SRE	-	Security Requirement Engineering
SRS	-	Software Requirement Specification
SR	-	Security Requirement
BoK	-	Body of Knowledge
EUI	-	Essential User Interface
EUC	-	Essential Use Case
NFR	-	Nonfunctional Requirement
Wi-Fi	-	Wireless Fidelity
RFID	-	Radio Frequency Identification
GPS	-	Global Positioning System
WSN	-	Wireless Sensor Network
GPRS	-	General Packet Radio Services
WiMAX	-	Worldwide Interoperability for Microwave Access
WLAN	-	Wireless Local Area Network
CIA	-	Confidentiality, Integrity and Availability Model

AAA	-	Authentication, Authorization and Accountability Model
M2M	-	Machine-to-machine
SLR	-	Systematic Literature Review
IT	-	Information Technology
ISO	-	International Organization for Standardization
IEEE	-	Institute of Electrical and Electronics Engineers
NIST	-	National Institute of Standards and Technology
CC	-	Common Criteria
IV	-	Independent Variables
DV	-	Dependent Variables
USE	-	Usefulness, Satisfaction and Ease of Use
CD	-	Cognitive Notation
RAD	-	Rapid Application Development
UI	-	User Interaction
SR	-	System Responsibility

LIST OF PUBLICATIONS

1. Ibrahim, A. A. Kamalrudin, M., Sidek. S., 2019. Common Practices in Eliciting Security Requirements of Internet of Things (IoT) Applications. *Journal of Theoretical and Applied Information Technology (JATIT),* 96(14), pp. 3880-3891. (E-ISSN 1817-3195 / ISSN 1992-8645; SCOPUS indexed, Q3, SJR 0.23)

2. Ibrahim, A. A., and Kamalrudin, M., 2019. Eliciting Security Requirements of IoT Applications using Essential Use Case. *International Journal of Information System and Computer Sciences (IJSSC)*, 8(6). pp. 168- 175. (ISSN 2319 – 7595)

3. Ibrahim, A. A., and Kamalrudin, M., 2018. Security Requirements and Technologies For The Internet Of Things (IoT) Applications: A Systematic Literature Review. *Journal of Theoretical and Applied Information Technology (JATIT),* 96(17), pp. 5694 – 5716. (E-ISSN 1817-3195 / ISSN 1992-8645; SCOPUS indexed, Q3, SJR 0.23)

4. Ibrahim, A. A., and Kamalrudin, M., 2018. A Comparison Analysis Study of Tools Support to Analysis Security Requirements for Internet of Things (IoT) Application. *The Turkish Online Journal of Design Art and Communication (TOJDAC).* September 2018 Special Edition, pp. 2497-2502. In: International Symposium on Research in Innovation and Sustainability (ISoRIS 2018).

5. Kamalrudin, M., Ibrahim A.A., Sidek S., 2018. A Security Requirements Library for the Development of Internet of Things (IoT) Applications. In: *Kamalrudin M., Ahmad S., Ikram N. (eds) Requirements Engineering for Internet of Things. APRES 2017. Communications in Computer and Information Science (CCIS)*, Vol 809. Springer, Singapore, pp. 87 – 96.

6. Ibrahim, A.A., Kamalrudin M., Abdollah M.F., 2017. A New Approach to Elicit Security Requirements for Internet of Things (IoT) Application. *Proceedings of Postgraduate Research Seminar in Conjunction with International Symposium on Research in Innovation and Sustainability (ISORIS) 2017*, pp. 235-242.

7. Ibrahim, A.A., Kamalrudin M., Abdollah M.F., 2017. Poster: Eliciting Security Requirements for Internet of Things (IoT) Application. *Proceedings of Postgraduate Research Seminar in Conjunction with International Symposium on Research in Innovation and Sustainability (ISORIS) 2017*, pp. 343-346.

8. Ibrahim, A.A., Kamalrudin M., Roslee, M. 2021. Secure IoT Application Software Development (SecIoTA) Model for Security Requirement Elicitation. *IEEE Access* – In Review

9. Ibrahim, A.A., Kamalrudin M., Grindy, J. Roslee, M. 2021. SecIoT_MEReq: An Automated Tool to Elicit Security Requirement for IoT Application Software Development. *IEEE Access* – In Review

CHAPTER 1

INTRODUCTION

1.1 Introduction

Internet of Things (IoT) is currently growing at a rapid rate in all business applications. IoT is defined as a coordination of multiple machines, devices, and appliances connected to the Internet through multiple networks (Smith and Bailey, 2016). These devices include everyday objects such as tablets and consumer electronics. Other machines such as vehicles, monitors, and sensors equipped with communication capabilities that allow them to send and receive data are also considered as IoT devices. Recent reports highlighted that the number of connected 'things' is set to explode and expected to reach 100 billion by 2025 (Rose et al., 2015b). As IoT is significant in practically every industry, there will be numerous applications that influence the IoT itself and subsequently, software engineers and developers to have the expertise and the tools to execute IoT component that assume a part in their systems. An early initiative such as defining some adequate security requirements before the IoT application is in place is critical. However, there is no single set of standards in IoT development and this causes the developers to consistently depend on flexible technologies to develop or deploy everywhere to integrate with other related applications. Subsequently, to adapt to the fracture in standards and heterogeneous biological communities of devices interaction, new strategies for programming advancement that are adaptable and allow quick development and simple integration with an assortment of different stages are required. Additionally, requirements engineers always fail to analyse the IoT security requirements due to lack of knowledge in security and possess poor