

**ONTOLOGY FORMATION FOR PUBLICATIONS ON SOCIAL  
ENGINEERING**

**ISSAM SHAABAN MALQOUT MOSHADED AL-SHANFARI**

**(Matric No: 3130136)**

**Thesis submitted in partial fulfillment for the degree of  
MASTER OF COMPUTER SCIENCE VIA MIXED MODE IN  
INFORMATION SECURITY AND ASSURANCE**

**Faculty of Science and Technology  
UNIVERSITI SAINS ISLAM MALAYSIA**

**Nilai**

**June 2015**

## AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: June 2015

Signature:

Name: Issam Shaaban Al-Shanfari

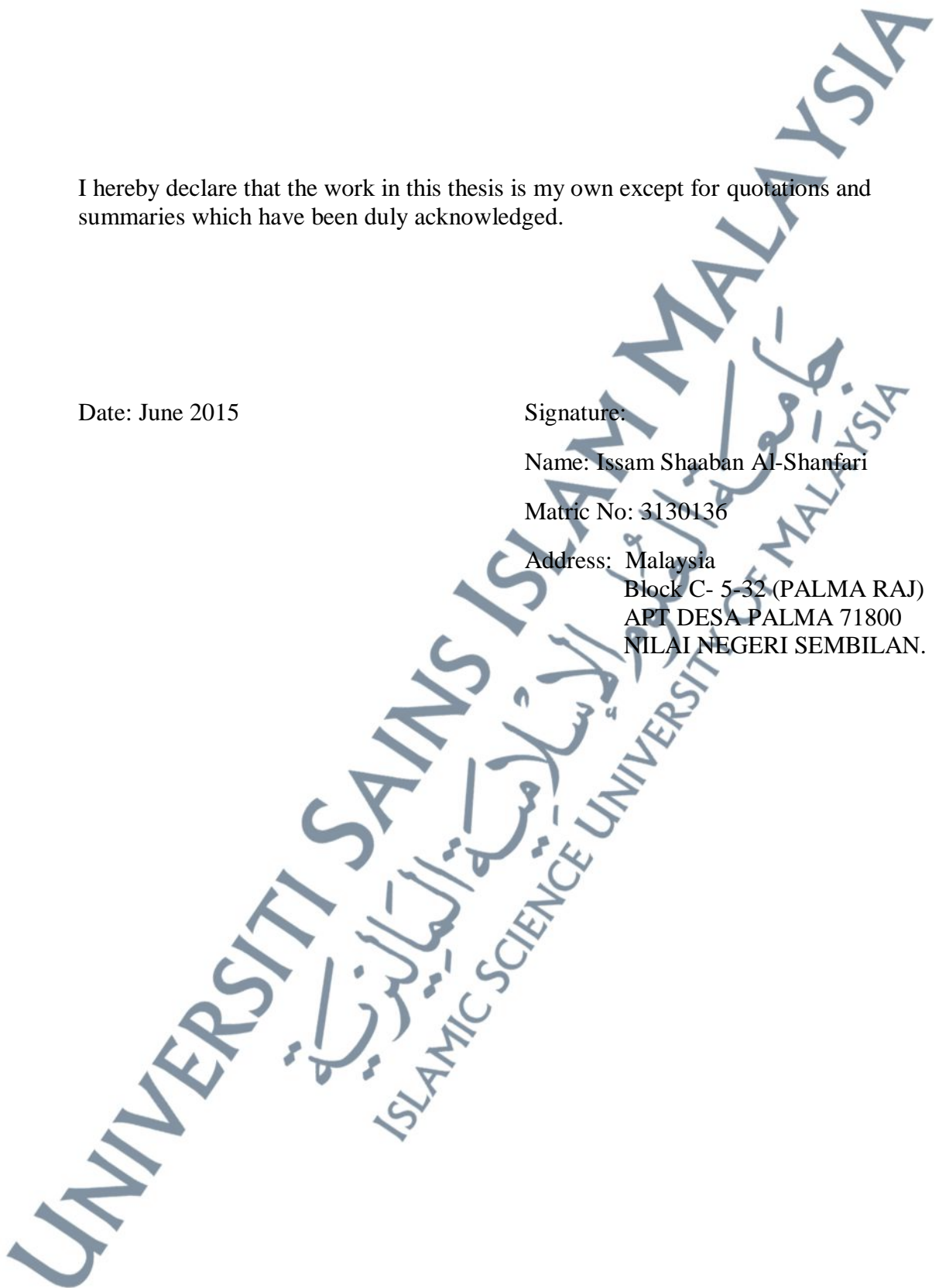
Matric No: 3130136

Address: Malaysia

Block C- 5-32 (PALMA RAJ)

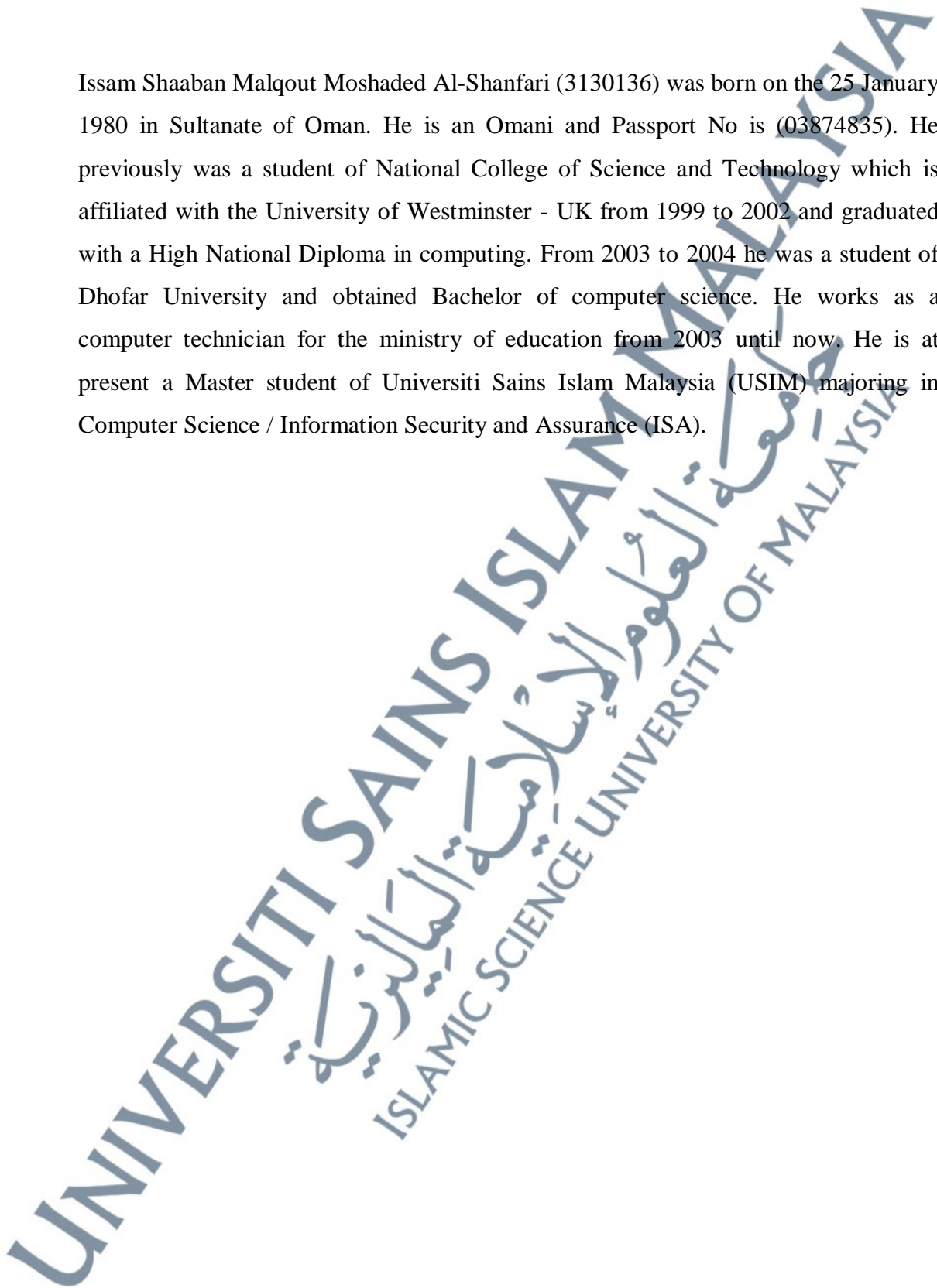
APT DESA PALMA 71800

NILAI NEGERI SEMBILAN.



## BIODATA OF AUTHOR

Issam Shaaban Malqout Moshaded Al-Shanfari (3130136) was born on the 25 January 1980 in Sultanate of Oman. He is an Omani and Passport No is (03874835). He previously was a student of National College of Science and Technology which is affiliated with the University of Westminster - UK from 1999 to 2002 and graduated with a High National Diploma in computing. From 2003 to 2004 he was a student of Dhofar University and obtained Bachelor of computer science. He works as a computer technician for the ministry of education from 2003 until now. He is at present a Master student of Universiti Sains Islam Malaysia (USIM) majoring in Computer Science / Information Security and Assurance (ISA).



## ACKNOWLEDGEMENT

At last, I am very glad to write this page with great thanks to Allah Almighty, who gave me the ability to complete my master's degree in Computer Science / Information Security and Assurance.

This master's thesis was written in 2014 at the Faculty of Science and Technology at Islamic Science University of Malaysia.

First of all, I wish to express my sincere gratitude to my supervisor, Dr. Roesnita Ismail, for her great support through the process of doing this thesis. I have received from her, including motivation and a lot of useful feedback. I wish her a great success in her academic career even in her different life's aspects.

It was also an honor to be able to study Information Security & Assurance at USIM University. I want to especially thank Prof. Dr. Kamaruzzaman Seman, Prof. Emeritus. Dr. Jalani Sukaimi, Prof. Dr. Norita Norwawi, Dr. Mohammed Zalisham, Dr. Mohammad Nasrin, Dr. Najwa Alwi, Dr. Nurlida Basir, Dr. Kamarudin Bin Saadan Dr. Azni Haslizan Binti Ab Halim, Dr. Sakinah Binti Ali Pitchay for teaching me and providing me a lot of support in the field of information security.

I wish to express my debt to all of the USIM staff and all of my sincere colleagues in FST for the useful discussions we had during our study.

With my sincere thanks for the Cultural Attaché Office - Embassy of the Sultanate of Oman in KL represented in person cultural attaché Dr. Khamis Saleh Al-Bulushi and the academic adviser Dr. Ghaith Khaled Ahmed.

Finally, I dedicate this work to my sincere parents, all my family members, my wife, and my friends, for their support to me. And finally, I will not forget my home country, Oman.

## ABSTRAK

Salah satu aktiviti yang signifikan ke atas bangsa pada zaman sekarang adalah bagaimana maklumat ditukar oleh pelbagai bentuk media, yang mencerminkan kepentingan perkongsian pengetahuan. Pada masa ini perkongsian pengetahuan antara objektif diperolehi secara sangat ad-hoc dan tidak mempunyai kefahaman yang sesuai makna data. Oleh itu, bagi memudahkan penggunaan semula dan perkongsian pengetahuan, ontologi mesti digunakan dalam situasi ini. Kejuruteraan sosial atau apa yang dikenali sebagai seni penembusan minda adalah koleksi teknik yang digunakan bagi memastikan orang berbuat sesuatu atau untuk mengisytiharkan tentang maklumat sulit. Kejuruteraan sosial ditakrifkan sebagai satu cara untuk mendapatkan maklumat yang bernilai mengenai sistem dari orang ramai secara umumnya, di mana-mana penyerang menggunakan sedikit maklumat yang dimiliki untuk memenangi kepercayaan mangsa, kepercayaan ini, membawa mangsa untuk memberikan maklumat sensitif kepada penyerang yang kemudiannya boleh menemui ciri-ciri sistem. Ontologi kejuruteraan sosial termasuk terjemahan dan penjelasan terma menerangkan jenis kejuruteraan sosial seperti serangan berasaskan manusia dan serangan berasaskan teknikal, ancaman, dan langkah-langkah tindakan. Peringkat-peringkat yang digunakan untuk pelaksanaan ini membentuk kaedah yang telah dicadangkan oleh Noy dan McGuiness (2000) bagi tujuan membangunkan ontologi. Kajian ini, berdasarkan penemuan dalam kesusasteraan, membangun taksonomi kejuruteraan sosial yang terdiri daripada dua kategori utama, menafsirkan penemuan dalam hierarki taksonomi dan membangunkan ontologi kejuruteraan sosial dengan menggunakan perisian 'Protégé'. Oleh itu, kajian ini bertujuan untuk menngumpul penerbitan berkaitan kejuruteraan sosial daripada pangkalan data terpilih. Kajian ini juga bertujuan untuk membangunkan koleks istilah yang berkaitan (taksonomi) berdasarkan pengestrakan penerbitan yang berkaitan dengan kejuruteraan sosial, untuk memudahkan perkongsian maklumat dan pengetahuan serta penggunaan semula pengetahuan mengenai kejuruteraan sosial.

## ABSTRACT

One of the significant activities of the nations in the present days is how information is exchanged by different forms of media, which reflects the importance of knowledge sharing. Currently this sharing of knowledge between objectives is obtained in a very ad-hoc fashion and lacks appropriate comprehension of the data meaning. Therefore, in order to facilitate the reuse and knowledge sharing, ontologies must be used in this situation. Social engineering, or what is known as the art of mind's penetration, is a collection of techniques used to make people do something or to declare about confidential information. Social engineering is defined as a way to gain valuable information about the system from people in general, where any attacker using little owned information to win the confidence of his victim, this trust, leads the victim to provide sensitive information to attacker through which can be discovered the properties of the system. The social engineering ontology includes a formal and explicit representation of the terms describing social engineering types such as human-based attacks and technical-based attacks, threats, and countermeasures. The stages used for this implementation form the methodology that has been suggested by Noy and McGuiness (2000) for the purpose of developing ontologies. This study, based on the findings in the literature, develops social engineering taxonomy consisting of two major categories, interprets the findings in a taxonomic hierarchy and develops social engineering ontology by using Protégé software. Therefore, this research aims to compile related publications on social engineering from selected databases. This study also aims to develop a collection of related terms (taxonomy) based on the extraction of publications related on social engineering, in order to facilitate information and knowledge sharing as well as knowledge reuse on social engineering.

## TABLE OF CONTENTS

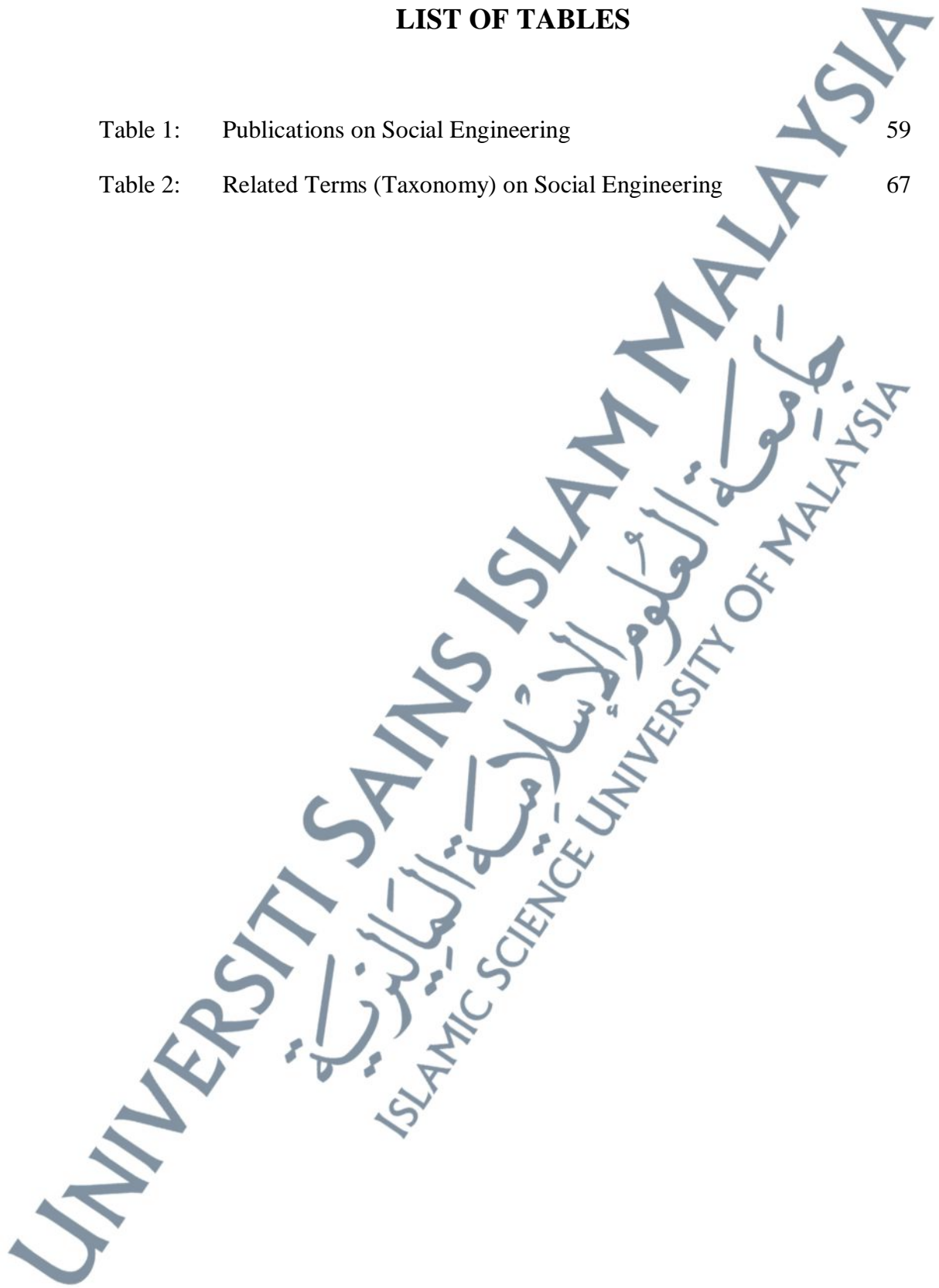
### CONTENTS

AUTHOR DECLARATION	ii
BIODATA OF AUTHOR	iii
ACKNOWLEDGMENT	iv
ABSTRAK	v
ABSTRACT	vi
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF APPENDICES	xi
<b>CHAPTER I INTRODUCTION</b>	<b>1</b>
1.1 Introduction	1
1.2 Research Problem	4
1.3 Research Objectives	5
1.4 Research Questions	6
1.5 Scope and Limitation of The Research	6
1.6 Research Significance	7
1.7 Description of the research process	7
1.8 Terminology	8
<b>CHAPTER II LITERATURE REVIEW</b>	<b>19</b>
2.0 Introduction	19
2.1 What is Semantic Web	19
2.2 What is Ontology	22
2.3 What is Social Engineering	25
2.3.1 Social Engineering Motivations	27
2.3.2 Social Engineering Attacks	28
2.3.2.1 Human-Based Attack	29
2.3.2.2 Technical-Based Attack	39
2.4 Related Studies on Ontology	42
2.5 Ontology Tools	47
2.6 Conclusion	50
<b>CHAPTER III MATERIALS AND METHODOLOGY</b>	<b>51</b>

3.0	Introduction	51
3.1	Materials	51
3.2	Research Methods	52
3.2.1	Developing Stages	53
3.2.2	Protégé Tool	55
3.4	Conclusion	56
<b>CHAPTER IV RESEARCH RESULTS</b>		57
4.0	Introduction	57
4.1	Compilation of Related Publications on S.E	57
4.2	Collection of Related Terms (Taxonomy) on S.E	65
4.3	Development Process of S.E Terms (Taxonomy)	77
4.3.1	Introduction	77
4.3.2	Development Process	77
4.4	Implementation in Protégé 4.2	85
4.4.1	Introduction	85
4.4.2	Implementation	85
4.4.3	Owl Visualization by WebProtégé	92
4.5	Conclusion	98
<b>CHAPTER V DISCUSSION AND CONCLUSION</b>		100
5.0	Introduction	100
5.1	Discussion	100
5.1.1	Extract Relevant Terms	101
5.1.2	Collect Extracted Terms	101
5.1.2.1	Human-Based Attacks	102
5.1.2.2	Technical-Based Attacks	102
5.1.3	Ontology Development	102
5.1.4	Threats and Vulnerabilities	105
5.1.5	Countermeasures and Prevention	106
5.2	Contributions	107
5.3	Limitations	108
5.4	Suggestion for Future Research	109
5.5	Conclusion	110
<b>REFERENCES</b>		111
<b>APPENDICES</b>		118

## LIST OF TABLES

Table 1:	Publications on Social Engineering	59
Table 2:	Related Terms (Taxonomy) on Social Engineering	67



## LIST OF FIGURES

Figure 1:	Semantic web layers	21
Figure 2:	Social Engineering Types	28
Figure 3:	Social Engineering main/sub- classes	77
Figure 4:	Social Engineering Human-based Taxonomy	79
Figure 5:	Social Engineering Technical-based Taxonomy	81
Figure 6:	Social Engineering Threats	82
Figure 7:	Social Engineering Countermeasures	84
Figure 8:	Top Level Social Engineering Taxonomy	85
Figure 9:	Middle Level Social Engineering Taxonomy	86
Figure 10:	Individuals "Facts" of Social Engineering Taxonomy	86
Figure 11:	Sample of class and its individuals	87
Figure 12:	Object property of Social Engineering Taxonomy	87
Figure 13:	Sample of Relationship view	88
Figure 14:	Sample of DL Query (1)	89
Figure 15:	Sample of DL Query (2)	90
Figure 16:	Example of Social Engineering class hierarchy	91
Figure 17:	Web Protégé home page	92
Figure 18:	Selection of an ontology format	93
Figure 19:	Web Protégé uploading ontology	94
Figure 20:	Ontology uploaded successfully	94
Figure 21:	Class description for social engineering ontology	95
Figure 22:	General view after uploading ontology	96
Figure 23:	Sharing settings as a public option	97
Figure 24:	Web Protégé social engineering individuals view	98

## LIST OF APPENDICES

Appendix A:	Research Timeline- Milestones	118
Appendix B:	Plagiarism Result	119
Appendix C:	Brief Biodata	120

