

# **A Novel Capability Maturity Model with Quantitative Metrics for Securing Cloud Computing**

A thesis submitted in fulfilment of the requirements for  
the degree of Doctor of Philosophy  
in the Faculty of Engineering and Information Technology  
at the University of Technology Sydney

by  
Ngoc Thuy Le

Supervised by  
Professor Doan B. Hoang

2019

# Certificate of Original Authorship

I, Ngoc Thuy Le declare that this thesis, is submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:  
Signature removed  
prior to publication.

Ngoc Thuy Le

Date: 18/12/2019

# Dedication

To my parents and my parents in law

To my wife and daughter

To my brother

Thank you for your love and support

# Acknowledgments

During the writing of this thesis, I have received a myriad of lessons, supports, and encouragements. First, I would like to express my deep gratitude to Professor Doan B. Hoang, my supervisor, for his enthusiastic encouragement, patient guidance, and precious lessons in keeping my PhD progress on schedule. He is one of my very important people as a mentor not only in teaching me the beauty of scientific research but also in guiding me in the way to balance between my family and my works. Perhaps, at the moments in my life, I will remember his words “*Please treat people with your love*” as an inspiration for me to dedicate myself to upholding the values of the society.

I would also like to extend my thanks to people who manage the UTS-VIED joint scholarship. I received this scholarship for my PhD course. This has been a wonderful opportunity to study in one of the best Universities in Australia. I wish to thank the School of Electrical and Data Engineering for providing me the funds for attending international conferences.

My special thanks to all my colleagues and friends embracing Dr. Priyadarsi Nanda, Dr. Zenon Chaczko, Tham Nguyen, Dat Dang, Chau Nguyen, Sara Farahmandian, Tuan Ha, Minh Pham, Ashish Nanda, and John Hazelton for their advice and assistance.

Finally, I would like to thank my parents, my parents in law, my wife and daughter, my brother and my sister in law for their encouragement and love over the four years. My wife and baby daughter always support and encourage me in my PhD course. They are always here for me. I wish to thank my parents for their wise counsel and sympathetic ears. This thesis is dedicated to them.

*Sydney, December 2019.*

# The Author's Publications

## International Conference Publications and Proceedings:

- 1 **Ngoc T. Le** and Doan B. Hoang. "Can maturity models support cyber security?" in *Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International*, Las Vegas, USA, pp. 1-7. IEEE, 2016. (ERA Ranking: B)
- 2 **Ngoc T. Le** and Doan B. Hoang. "Threat probability computation using Markov and Common Vulnerability Scoring System" in *International Telecommunication Networks and Applications Conference (ITNAC), 2018 IEEE 28<sup>th</sup> International*, Sydney, Australia, 2018, pp. 1-7. (IEEE ITNAC); **Highly commended paper awards.** (ERA Ranking: B)

## Journal papers:

- 3 **Ngoc T. Le** and Doan B. Hoang, "Capability Maturity Model and Metrics Framework for Cyber Cloud Security," *Scalable Computing: Practice and Experience* 18, no. 4 (2017): 277-290.
- 4 **Ngoc T. Le** and Doan B. Hoang, "A Threat Computation Model using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security", *Journal of Telecommunications and the Digital Economy*, vol. 7, no. 1, pp. 37-56, Mar. 2019.
- 5 **Ngoc T. Le** and Doan B. Hoang, "A new security threat model and computation the probability of Cloud security threats," submitted to *IEEE Transactions on Dependable and Secure Computing*. (Under Review)
- 6 **Ngoc T. Le** and Doan B. Hoang, "A Quantitative Security Metric for cloud security," submitted to *IEEE Transactions on Information Forensics and Security*. (Under Review)

# Table of Contents

<b>Certificate of Original Authorship</b> .....	i
<b>Dedication</b> .....	ii
<b>Acknowledgments</b> .....	iii
<b>The Author’s Publications</b> .....	iv
<b>Table of Contents</b> .....	v
<b>List of Figures</b> .....	x
<b>List of Tables</b> .....	xii
<b>List of Abbreviations and Acronyms</b> .....	xiv
<b>Abstract</b> .....	xvi
<b>Chapter 1</b> .....	<b>1</b>
<b>Introduction</b> .....	<b>1</b>
1.1 Capability Maturity Models and Cloud Security models.....	4
1.2 Research Problem.....	8
1.3 Research Aims and Objectives and Scope .....	11
1.4 Research Contributions .....	13
1.5 Research Model and Methodology .....	15
1.6 Structure of the Thesis .....	16
<b>Chapter 2</b> .....	<b>18</b>
<b>Background</b> .....	<b>18</b>
2.1 An overview of cyber space and cyber security .....	19
2.1.1 Cyber space .....	19
2.1.2 Cyber security.....	21
2.2 Cloud computing and Cloud security models and standards.....	23
2.3 Cyber Security Maturity Model.....	28
2.4 Metrics and measures in cyber security and security threat .....	30
2.4.1 Fundamentals of metrics and security metrics .....	30
2.4.2 Metrics about security threats.....	33
2.5 Mathematical backgroud .....	38

2.5.1 Markov chain and applied for security metrics .....	38
2.5.2 Search theory .....	40
2.5.3 Concept of Inclusion-Exclusion Principle.....	43
2.6 Summary.....	46
<b>Chapter 3.....</b>	<b>47</b>
<b>A Novel Capability Maturity Model and a Metric Framework for Cloud Security.....</b>	<b>47</b>
3.1 Introduction .....	49
3.2 Maturity Models Applied in Cyber Security .....	49
3.3 Cloud Security Capability Maturity Model (CSCMM).....	52
3.3.1 CSCMM Domains .....	53
3.3.2 Security Maturity Levels .....	59
3.4 Security Metric Framework.....	62
3.5 The Selection of Advanced Security Quantitative Metrics .....	65
3.6 Summary.....	67
<b>Chapter 4.....</b>	<b>68</b>
<b>A Threat Computation Model Using a Markov Chain and Common Vulnerability Scoring System and Its Application to Cloud Security.....</b>	<b>68</b>
4.1 Introduction .....	68
4.2 The Relationship Between Cloud Security Threats and Vulnerabilities .....	71
4.3 Markov Model for Successful Attacks .....	76
4.4 Distribution of Security Threat Probabilities .....	77
4.5 Estimation of Security Attack Probability.....	82
4.5.1 Relationship between Attack Types and Security Threats .....	82
4.5.2 Computing the Attack Type Probabilities .....	85
4.6 Summary.....	86
<b>Chapter 5.....</b>	<b>88</b>
<b>An Exist-Escape Security Threat Model for Computing the Probability of Materialised Threats and Its Application to Cloud .....</b>	<b>88</b>
5.1 Introduction .....	88
5.2 Modelling Security Threat.....	90
5.2.1 Security Threat Existence Phase .....	91

5.2.2 Security Threat Escape Phase.....	93
5.2.3 Security Threat Model Presented in a Venn Diagram.....	94
5.3 Quantifying the Probability of Threats Materialised .....	95
5.3.1 Computation of Probability of Threat Existence.....	95
5.3.2 Computation of Probability of Threat Escape .....	99
5.4 Application of the Security Threat Model to Cloud Computing.....	101
5.4.1 Computation of Probability of Threat Existence in Cloud Computing.....	101
5.4.2 Computation of Probability of Threat Escape in Cloud Computing .....	103
5.5 Data for the Proposed Threat Model .....	104
5.5.1 Attack Conditions.....	104
5.5.2 System Conditions.....	105
5.5.3 Control Conditions .....	106
5.6 Security Threat Model Simulation and Evaluation .....	108
5.7 Cloud Threat Probabilities.....	112
5.8 Summary.....	117
<b>Chapter 6.....</b>	<b>118</b>
<b>A Skill-based Attack-control Security Threat Model and Its Application to Cloud .....</b>	<b>118</b>
6.1 Introduction .....	118
6.2 Modelling a Skill-based Attack-control Security Threat.....	119
6.2.1 Skill-based Attack Process .....	120
6.2.2 Skill-based Control Process.....	121
6.3 Quantifying Probability Attackers are Capable of Exploiting Vulnerabilities .....	123
6.3.1 Simple Cases .....	124
6.3.2 Method 1: Using Combination Theory.....	129
6.3.3 Method 2: Using Inclusive-Exclusive Principle.....	130
6.4 Applying the Proposed Threat Model to Cloud Computing .....	133
6.4.1 Probability of a Cloud Existed Security Threat .....	134
6.4.2 Probability of a Cloud Security Threat Undetected and Materialised.....	135
6.5 Demonstration of the Proposed Threat Model to Cloud .....	136
6.5.1 Obtain Data for Cloud Simulation.....	136



6.5.2 Probability of Existed Threat with Various Attack Skills .....	137
6.5.3 Probability of Undetected Threat for Various Control Skills .....	139
6.5.4 Probability of Materialised Threats .....	141
6.6 Summary.....	143
<b>Chapter 7.....</b>	<b>144</b>
<b>Mean Security Remediation Cost as a Quantitative Metric and Application to Cloud Computing.....</b>	<b>144</b>
7.1 Introduction .....	144
7.2 Mean Security Remediation Cost as a Quantitative Security Metric .....	146
7.3 Stakeholder Matrix .....	151
7.3.1 Stakeholders in Cyber Systems .....	152
7.3.2 Cloud Security Stakeholder Model .....	153
7.3.3 Generating Stakeholder Matrix (ST).....	156
7.4 Threat Class Matrix (CT) .....	157
7.4.1 Generating Class of Threat Matrix (CT) .....	158
7.4.2 Probability Threat Vector (PT).....	158
7.5 Obtaining Data for MSRC's Components .....	159
7.6 Application .....	164
7.7 Summary.....	169
<b>Chapter 8.....</b>	<b>170</b>
<b>Assessing Security for Cloud Security Capability Maturity Model .....</b>	<b>170</b>
8.1 Introduction .....	170
8.2 MSRC applied for CSCMM.....	171
8.2.1 CSCMM Model.....	171
8.2.2 Select Security Domains for Using MSRC .....	173
8.3 Benchmark Method .....	174
8.4 Applications.....	175
8.5 MSRC by Using Different Security Threat Model.....	181
8.5.1 MSRC Demonstrated on Exist-escape Threat Model .....	181
8.5.2 MSRC Demonstrated on Attack-control Skill-based Threat Model .....	185
8.6 Comparison between the Two Security Threat Models .....	188
8.7 Summary.....	193

<b>Chapter 9</b> .....	<b>194</b>
<b>Conclusion and Future Work</b> .....	<b>194</b>
9.1 Research remarks and contributions of the thesis .....	194
9.2 Future Research Direction .....	197
<b>Bibliography</b> .....	<b>201</b>

# List of Figures

<b>Figure 1.1</b> Capabilities maturity model process levels .....	6
<b>Figure 1.2</b> Design Science Research Methodology (DSRM) .....	16
<b>Figure 2.1</b> Overall ES-C2M2 Structure .....	29
<b>Figure 2.2</b> CCSMM Model .....	30
<b>Figure 2.3</b> Inclusion–exclusion illustrated by a Venn diagram for three sets .....	43
<b>Figure 3.1</b> Overview of research solutions via Chapters .....	48
<b>Figure 3.2</b> CSCMM Model Architecture .....	54
<b>Figure 3.3</b> CSCMM metric framework diagram .....	64
<b>Figure 4.1</b> Diagram of attack model with defence and recovery .....	76
<b>Figure 4.2</b> Diagram of attack model with defence and without recovery .....	77
<b>Figure 4.3</b> Diagram of attack model without defence and recovery .....	77
<b>Figure 4.4</b> Security threat model with attack process .....	78
<b>Figure 5.1</b> Security threat model .....	90
<b>Figure 5.2</b> Security threats is the intersection of attack, system, and control .....	95
<b>Figure 5.3</b> Threat Existence phase .....	96
<b>Figure 5.4</b> Search theory between attacker capability and vulnerabilities of system in case $V=A=1$ .....	97
<b>Figure 5.5</b> Search theory between attacker capability and vulnerabilities of system in case $V>1, A=1$ .....	98
<b>Figure 5.6</b> Threat Escape phase .....	100
<b>Figure 5.7</b> Security threat model in cloud computing .....	101
<b>Figure 5.8</b> The probability of threat existence for various attacker skill levels .....	109
<b>Figure 5.9</b> the probability of threat escape given existing threat for various controller capability levels .....	110
<b>Figure 5.10</b> The probability of security materialised (successful attack) with max attack and min control levels .....	111
<b>Figure 5.11</b> The probability of threat materialised (successful attack) for various attacker skill levels and controller capability levels .....	112
<b>Figure 5.12</b> The distribution of probability of threat existence for different threats ...	113

<b>Figure 5.13</b>	The distribution of probability of escape threat given existing threats.....	113
<b>Figure 5.14</b>	The distribution of probability security threat (max attack-min control)	114
<b>Figure 5.15</b>	Impact of ( $T_i$ ) and ( $E_i$ ) on the probability of security threat 11 (Denial of Services) materialised .....	115
<b>Figure 5.16</b>	The distribution of probability security threat (max attack-min control case) when removing $V_1$ .....	116
<b>Figure 6.1</b>	Skill-based attack-control security threat model .....	120
<b>Figure 6.2</b>	Attack process.....	121
<b>Figure 6.3</b>	Control process .....	122
<b>Figure 6.4</b>	Skill-based attack-control threat model applied to cloud computing .....	133
<b>Figure 6.5</b>	The probability of cloud existed security threat in terms of attack-skill ....	139
<b>Figure 6.6</b>	The probability of undetected security threat in terms of control-skill .....	140
<b>Figure 6.7</b>	The probability of materialised security threat for various attack skills with min control ( $* 10^{-3}$ ) .....	142
<b>Figure 6.8</b>	The probability of materialised security threat API (Threat 3) for various attack skills and different control skills ( $* 10^{-3}$ ).....	143
<b>Figure 7.1</b>	Cloud Security Stakeholder Model.....	154
<b>Figure 8.1</b>	CSCMM Model Architecture .....	172
<b>Figure 8.2</b>	Current maturity levels of three security domains (red box).....	179
<b>Figure 8.3</b>	Security Maturity Level of IAM is improved to level 2 (red box) .....	180
<b>Figure 8.4</b>	The distribution of probability materialised security threat for threat DOS (Denial of Service).....	182
<b>Figure 8.5</b>	The distribution of probability materialised security threat for 12 threats based on exist-escape threat model .....	184
<b>Figure 8.6</b>	The distribution of probability materialised security threat for 12 threats based on attack-control skill-based model .....	187
<b>Figure 8.7</b>	The distribution of probability materialised security threat for 12 threats between two security threat models: Exist-Escape and Attack-Control .....	191

# List of Tables

<b>Table 2.1</b> Cyber space entities referenced in the definition of cyber space by various cyber space government strategies and organisations.....	21
<b>Table 3.1</b> Synthesising and Analysing Cyber Security Maturity Models .....	51
<b>Table 4.1</b> Relationship between security threats and vulnerabilities .....	75
<b>Table 4.2</b> Vulnerability scores.....	80
<b>Table 4.3</b> Probability distribution of twelve security threats .....	81
<b>Table 4.4</b> Relationship between security attack types and security threats.....	85
<b>Table 4.5</b> Probability distribution of five attack type.....	86
<b>Table 5.1</b> Attackers skill levels .....	104
<b>Table 5.2</b> The number of vulnerabilities for seven kinds of vulnerabilities.....	105
<b>Table 5.3</b> The average number of vulnerabilities for each threat.....	106
<b>Table 5.4</b> Capability level of controllers .....	107
<b>Table 5.5</b> The average number of vulnerable patches for each threat.....	107
<b>Table 5.6</b> The variables for simulation.....	108
<b>Table 6.1</b> the probability of cloud existed security vulnerabilities .....	136
<b>Table 6.2</b> The probability of cloud existed security threat for different attack skill levels (* 10 <sup>-3</sup> ).....	138
<b>Table 6.3</b> The total probability of cloud existed security threats for various attack-skills .....	139
<b>Table 6.4</b> The probability of undetected security threat for various control skills.....	140
<b>Table 6.5</b> The probability of materialised security threat for various attack skills with min control (* 10 <sup>-3</sup> ).....	141
<b>Table 6.6</b> The probability of materialised security threat API (Threat 3) for various attack skills and different control skills (* 10 <sup>-3</sup> ) .....	142
<b>Table 7.1</b> Stakeholder matrix with probability distribution of classes of threats.....	150
<b>Table 7.2</b> Threat Class matrix .....	150
<b>Table 7.3</b> Probability distribution of twelve security threats materialised into attacks	159
<b>Table 7.4</b> One example of variables .....	161

<b>Table 7.5</b> One example of percentage of security fund for a stakeholder used to remediate each class threat ( $Y_{ij}$ ).....	162
<b>Table 7.6</b> ST matrix (a) showing the variables, (b) one example by using (7.8) (in thousands dollar) .....	163
<b>Table 7.7</b> The probability of threat classes given that cloud security threat materialised .....	164
<b>Table 7.8</b> Mean Security Remediation Cost for each cloud security stakeholder.....	165
<b>Table 7.9</b> Mean Security Remediation Cost regarding the cloud security threat class	166
<b>Table 7.10</b> Mean Security Remediation Cost regarding cloud security threats .....	168
<b>Table 8.1</b> Relationship between CSCMM security domains and threats .....	174
<b>Table 8.2</b> Probability distribution of seven security threats PT matrix ( $* 10^{-3}$ ).....	175
<b>Table 8.3</b> MSRC of each stakeholder for each domain ( $* 10^{-3}$ ).....	176
<b>Table 8.4</b> Domain weight value for each stakeholder (out of 10).....	177
<b>Table 8.5</b> Benchmark value for each domain.....	178
<b>Table 8.6</b> Maturity level table .....	178
<b>Table 8.7</b> Threat probability change.....	179
<b>Table 8.8</b> Weight and probability of materialised security threat for 12 threats based on exist-escape threat model .....	183
<b>Table 8.9</b> MSRC for each stakeholder using exist-escape threat model .....	184
<b>Table 8.10</b> MSRC for each threat using exist-escape threat model .....	185
<b>Table 8.11</b> Probability of materialised security threat for 12 threats based on attack-control skill-based model .....	186
<b>Table 8.12</b> MSRC for each stakeholder using attack-control skill-based threat model	187
<b>Table 8.13</b> MSRC for each threat using attack-control skill-based threat model .....	188
<b>Table 8.14</b> Probability of materialised security threat for 12 threats based on Exist-Escape and Attack-Control models .....	190
<b>Table 8.15</b> MSRC for each stakeholder between Exist-Escape and Attack-Control threat models .....	192
<b>Table 8.16</b> MSRC for each threat between Exist-Escape and Attack-Control threat models .....	192

# List of Abbreviations and Acronyms

APT	Advanced persistent threat
CIA	Confidentiality, Integrity, and Availability
CIS	Centre of Internet Security
CMM	Capability Maturity Model
CSA	Cloud Security Alliance
CSCMM	Cyber Security Capability Maturity Model
CVSS	The Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DOE	Department of Energy of the USA
DOS	Denial of Service
ENISA	European Union Agency for Network and Information Security
HTTPs	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a service
ICT	Information and Communication Technology
IDC	International Data Corporation
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OS	Operating System
OVF	Open Virtualisation Format
OWASP	The Open Web Application Security Project

PaaS	Platform as a service
QoS	Quality of Service
SaaS	Software as a service
SECaaS	Security as a service
SLA	Service Level Agreements
SQL	Structured Query Language
VPN	Virtual private network



# Abstract

Cloud computing is a cutting-edge technology for building resource-sharing, on-demand infrastructures that support Internet of Things (IOTs), big data analytics, and software-defined systems/services. However, cloud infrastructures and their interconnections are increasingly exposed to attackers while accommodating a massive number of IOT devices and provisioning numerous sophisticated emerging applications.

There exist several cloud security models and standards dealing with emerging cloud security threats. They provide simplistic and brute-force approaches to addressing the cloud security problems: preventing security breaches by cautiously avoiding possible causes or fix them through trial and error attempts. Two major issues have been identified with the current approach to cloud security. First, it lacks quantitative measures in assessing the security level of security domains within a cloud space. Second, it lacks a model that can depict the overall security status of the cloud system.

In the light of the above, the aim of this dissertation is to investigate relevant quantitative security metrics and propose a novel Capability Maturity Model with Quantitative Security Metrics for Securing Cloud Computing. First, we propose a new security metric named Mean Security Remediation Cost to assess the cost attributed to cloud stakeholders when a security attack has occurred. Moreover, we propose three different quantitative novel models for quantifying the probability of a cloud threat materialising into an attack. Second, a new Cloud Security Capability Maturity Model (CSCMM) for the cloud will be proposed. The model includes cloud-specific security domains and the quantitative assessment of the overall security of the cloud under consideration. To support the measuring of security maturity levels, a security metric framework is introduced. The CSCMM Model will be quantitatively validated by proposed security metrics. We evaluate the model in a cloud computing environment and compare the consequences by simulating different parameters of the proposed security quantitative metric.

The thesis contributes to the theoretical body of knowledge in cloud security. The thesis proposes for the first time a Capability Maturity Model for cloud security. Additionally, the novel model will be used in practice by managers, security experts and

practitioners for both assessing the overall security status of the organisation/system and taking new quantitative measures to mitigate weaknesses of any specific aspects of the system as identified by the assessment. The major research outcomes from the thesis have been delivered in academic papers published in international peer-reviewed journals and conferences in cyber security and cloud computing.