

# **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 V1 .....	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.

# Chapter 1

## Introduction

Based on virtualisation and shared computer resources, cloud computing is seen as the technological evolution of outsourcing. It plays a critical role in the world IT development and it will develop dramatically in the next decades [1]. According to Gartner reports, the worldwide public cloud services market will increase 17.3 percent in 2019 to total \$206.2 billion, up from \$175.8 billion in 2018 [2]. However, clouds, as cyber infrastructures, with three service models (IaaS, PaaS, and SaaS), four deployment types (Private, Public, Hybrid, and Community), are facing challenging security issues. Cloud security spending is forecasted to reach \$12.6 billion by 2023, up from \$5.6 billion in 2018 [3]. According to IDC survey, 74% of CIOs in cloud computing organisations are concerned about security [4]. The Cloud Security Alliance (CSA) published a report “Top Threats to Cloud Computing”, describing seven threat areas considered most important to organisations using cloud services [5].

Many models have been developed to tackle cloud security issues such as “Cloud standards and security” by the European Union Agency for Network and Information Security (ENISA) [6], “Security guidance for critical areas of focus in cloud computing” by CSA [7]. However, one of the most difficult and crucial issues is the lack of a meaningful assessment of the security status of a cloud infrastructure. This assessment can help senior management to make the right security decisions for its stakeholders and assist security managers in taking appropriate actions to protect as well as preserve the confidentiality, integrity and availability of the infrastructure. Furthermore, few models consider the security of a system with a holistic assessment approach. It is known that a single minor vulnerability can bring down the whole system and there are myriads of these vulnerabilities. Additionally, the models lack an assessment process because they lack meaningful and relevant quantitative security metrics. Therefore, two main challenges have been found from the current cloud security models. First, a model can determine the overall security status of the cloud system. Second, existing quantitative

measures are not adequate in assessing the security level of security domains within a cloud space.

For the first issue, we have identified *capability maturity model* as a possible model for IT system management for assessing the quality performance level of domains/facets of a system. In 1989, Humphrey recommended a capability maturity model for assessing the software quality [8]. This basic model has been adapted for cyber security for several reasons. First, security models based on a capability maturity model have been applied with successes in several IT systems and business processes. Second, maturity models are found to be suitable for the management process of cyber security. Third, they have been applied for securing important traditional cyber space such as e-government, e-commerce, education, critical infrastructure [9]. However, it is difficult to find on the application of the model in cloud computing security. Until 10/2015, There is a research about cloud forensics released by Cloud Security Alliance [10]. Moreover, a conceptual capability maturity model for cloud incident handling was proposed with the integration of digital forensics [11]. Several cloud forensics models were analysed comprehensively in [12]. Clearly, the potential of maturity models in cloud security needs to be investigated. Despite having the benefits, maturity models have also revealed several drawbacks. One of which is that when organisations use maturity models, their goal is to reach the next level of maturity, but maturity levels are determined arbitrarily and subjectively. Another disadvantage is that maturity assessing metrics depend mainly on qualitative measurements. Assessment criteria are based on ticking the compliant boxes and intuitive judgment on various processes with a complicated guidance.

For the second issue, over the last decades, defining and measuring security states has become increasingly essential for assessing the security capability/status of a cyber space. Lord Kelvin [13] stated that “*when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind*”. However, it is difficult to measure the security state of a cyber space for several reasons. First, vulnerabilities are hard to be measured by anyone, even the owner of the system. Second, the set of weakness (vulnerabilities) known to an observer is not often known by the owner of the system and thus is not measured by the owner. Third, no system owner knows the totality of his/her adversaries [14]. Despite having difficulties in

security measuring, cyber security metrics can support an organisation in (1) verifying that their security controls are in compliance with the organisation's policies, processes, or procedures, (2) identifying their security strengths and weaknesses; (3) and identifying security trends, both within and outside the organisation's control [14]. Therefore, security metrics are needed to assess the security of the cyber space. Security metrics have been the focus of many organisations. The Centre for Internet Security (CIS) has designed the set of security metrics in management, operation, and technique [15]. The National Institute of Standards and Technology (NIST) has developed security metrics in implementation, effectiveness, and impact [16]. Many metrics thus have been established and used, but they are mainly based on qualitative methods and consequently, security assessments are only about compliance and guidance. They are mainly reactive and hence it is difficult to derive a meaningful action to identify the root cause and rectify wider damages of a security breach or predict future security issues [17]. Consequently, for more accurate, security assessment quantitative metrics are necessary for various aspects of cloud security.

In summary, an effective security model needs both qualitative and quantitative metrics to deal with the complexity of the human aspects of security and to tackle the technology aspects of security. On the qualitative assessment, qualitative metrics provide senior managers with a sound picture of security compliance of their system in terms of organisational policies, governance, culture, and human issues and relate the impact of the security assessment to their business plans and directions. On the quantitative assessment, effective quantitative security metrics support the identification of a specific security facet/issue of the system or an individual practice of the model and present appropriate security actions for achieving a higher level of system security. More importantly, effective quantitative metrics have to produce a clear mapping between the outcomes of a security assessment and the costs/benefits to the organisation. In this thesis, we focus on mainly developing quantitative security metrics involving cost or performance. Although qualitative metrics are critical in the assessing model, they are not in the scope of the thesis.

Therefore, to overcome the challenges in generating innovative quantitative security metrics and to take advantage of maturity models, we aim to propose a novel capability maturity model with quantitative metrics for cloud security that allows not only managers

to assess the security state of a cloud system for the decision making process but also allows practitioners to identify the gaps in security and to implement security responses systematically and quantitatively.

To achieve this above goal, we first identify the implementation and management problems in cloud security and maturity models. Then, we introduce a new maturity model for cloud security that addresses the overall security management through building up the framework of security domains and maturity levels for cloud computing. Subsequently, we investigate security quantitative metrics applicable to the assessment of the security maturity level of facets of a cloud system. Finally, we implement a system based on our proposed model and its quantitative metrics and conduct experiments to validate and evaluate the performance of the new model on cloud security.

This thesis is significant in that it provides a novel approach for applying a capability maturity model with specific-designed quantitative measures to protect a cloud system proactively. The expected outcome of this thesis is an approach to assessing cloud security levels through relevant security quantitative metrics.

The remainder of this chapter is organised as follows: Section 1.1 introduces Capability Maturity Models and Cloud Security Models. Section 1.2 explicitly describes the research problems tackled by this thesis and the research motivation. Section 1.3 presents the research aims and objectives. Section 1.4 indicates the major significant contributions of the thesis. Section 1.5 provides the research model and methodology that the thesis will use. Section 1.6 describes the structure of the thesis.

## **1.1 Capability Maturity Models and Cloud Security models**

The fundamentals of Capability Maturity Models and an overview of cloud security models and standards will be described in this section.

A question that has to be asked concerning a cyber space or a system is whether the cyber space or the system is secure or at least to what level it is secure. For example, is a cyber space secure when a huge number of bugs, viruses, spams and malwares have been found and fixed? Or is a cyber space secure when substantial investment in a firewall system and an IDPS (intrusion detection and prevention system) has been made? It is difficult to claim that a cyber space is safe and secure based on the number of vulnerabilities found and fixed as there may be a number of bugs still undetected. This

implies that vulnerability is only one of the many aspects of security. Yet, many of the current security models deal with security problems in an ad hoc manner; a specific security measure is put into action simply to treat the issue at hand without regard to or understanding of its impact on the whole cyber space. These models handle security from a bottom-up perspective and are case specific. They provide no assurance of the overall level of security of the protected entity.

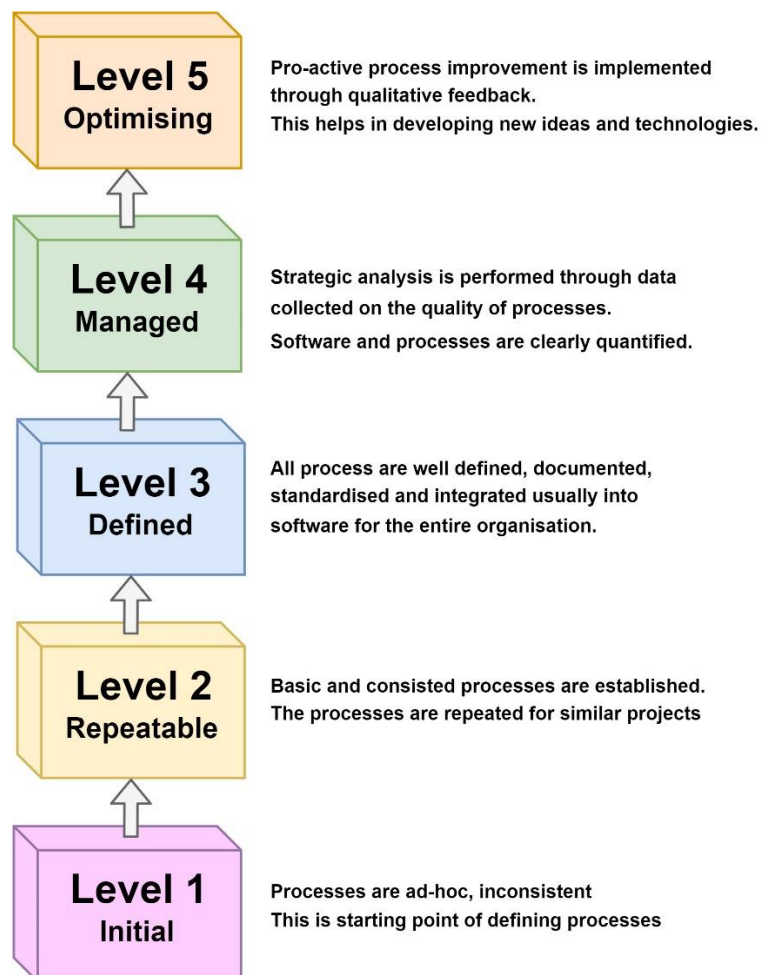
What is needed is to view and study cyber security holistically from a top-down perspective to produce a security model that allows us to make an assessment of the overall security level of the entity requiring protection. Furthermore, the model should allow us to identify the entity's weaknesses and the appropriate measures to deal with them. Measures may include an investment in resources, and the enforcement of practices. Among those proposed models, the cyber-security maturity model provides organisations to some extent with a roadmap for measuring, assessing, and enhancing cyber security. Relative to other models, it provides managers with a sound footing for making an informed security assessment of their organisation.

- **The fundamentals of Capability Maturity Models**

Maturity Models are based on the Capability Maturity Model (CMM). Humphrey [8] recommended the CMM to assess quality of software and to help software organisations improve the maturity of their software processes, evolving from ad hoc, chaotic processes to mature, disciplined software processes. The fundamental ideas of CMM are as follows: (1) the model is divided into 5 levels from initial to optimizing level, from simple to complex, from low requirement to higher requirement; (2) each level has its specific maturity requirements. It means that to achieve the definite maturity level, the standard requirements of quality and technology need to be implemented by several sets of practices; (3) to reach the higher level, the software must pass all lower levels (as seen in **Figure 1.1**). Eventually, maturity models show the level of perfection or completeness of certain capabilities. They define maturity levels which measure the completeness of the analysed objects via different sets of (multi-dimensional) criteria.

The structure of the cyber security maturity model can be described in terms of its functions, key components, and types of maturity model [18]. There are three main functions of a maturity model: a means of assessing and benchmarking performance; a roadmap for model-based improvement; and a means to identify gaps and develop

improvement plans. The key components include maturity levels which are the security measurement scale or transitional states; security domains are logical groups of practices, processes; attributes which are core contents of the model arranged by domains and levels; diagnostic methods for assessment, measurement, gap identification, and benchmarking; improvement roadmaps to guide improvement efforts such as Plan-Do-Check-Act or Observe-Orient-Decide-Act. The three types of maturity models are progression, capability, and hybrid. While a progression model describes levels as higher states of achievement, as with maturity progression for human mobility being from crawl, walk, jog to run, a capability model shows levels as the extent to which a particular set of practices has been institutionalised. The hybrid model is the combination of the best features of progression and capability maturity models, so that maturity levels express both achievement and capability. Most recent cyber security maturity models are hybrid models which take security levels and domains into the integrated framework.



**Figure 0.1** Capabilities maturity model process levels



- **Cloud security models and standards**

To combat cloud security problems, researchers, businesses, and organisations have been making efforts to mitigate cloud security risk and tackle security threats by development of cloud security standards and models. In 2014, the European Union Agency for Network and Information Security (ENISA) [19] released the report “Cloud standards and security” to provide an overview of standards relevant for cloud computing security. Cloud Security Alliance (CSA) introduced and developed “security guidance for critical areas of focus in cloud computing” through 3 versions including Version 1.0 [20], Version 2.1 [21] (2009), and Version 3.0 [7] (2011). The latest version (Version 3.0) is tailored for meeting the security demand change. The aim of this guidance is to introduce better standards for organisations to manage cyber security for cloud by implementation of security domains. The guidance approached cloud architecture with cloud service model (SaaS, PaaS, and IaaS) and four deployment models (Public, Private, Community, and Hybrid Cloud) with derivative variations that address specific requirements. The guidance principle is based on thirteen different domains which are divided into two general categories: governance and operations. The governance domains focus on broad and strategic issues as well as policies within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

This guidance is relevant to cloud computing, its service models and its deployment models. Regarding cloud security management, the guidance focuses on cloud-specific issues: interoperability and portability, data security, and virtualisation. Dividing the implementation domains into two groups with strategic and tactical categories is another salient point of the guidance. This approach allows cloud consumers and providers to bring financial and human resources into security consideration. Furthermore, the guidance can be mapped to existing security models such as “Cloud Control Matrix” [22], international cyber security standards ISO/IEC 27002 and other NIST Special Publications. Despite the benefits, however, the guidance has several drawbacks. The guidance lacks an assessment guide for each domain. It does not consider security metrics for security practices. Therefore, organisations find it difficult to determine the security level of a domain.

In addition, there are several standards concerning cloud security. The ISO/IEC 27017 Standard illustrates the information security elements of cloud computing. It assists with the implementation of cloud-specific information security controls, supplementing the guidance in ISO 27000 series standards, including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on the relationship management. The NIST released the following standards on cloud computing: NIST SP 500-291, 'Cloud Computing Standards Roadmap', NIST SP 800-146, 'Cloud Computing Synopsis and Recommendations', NIST SP 800-144, 'Guidelines on Security & Privacy in Public Cloud Computing', NIST SP 500-292, 'Cloud Computing Reference Architecture' and NIST SP 500-293, 'US Cloud Computing Technology Roadmap'.

## **1.2 Research Problem**

From the previous section, we can conclude that there are two major research challenges in recent security models for cloud computing. First, it is necessary to investigate a model that can depict the overall security status of the cloud system. Second, quantitative measures are needed to be developed for assessing security levels of security domains within a cloud space. For the first challenge, we found that the capability maturity model can adapt for cyber security for the following reasons. Capability maturity models have been applied in many fields such as IT, business. They can support a completed management process for cyber security. They can be extended to cover many security aspects or domains. Recently, a maturity model has been applied for securing important traditional cyber space systems such as e-government, e-commerce, education, and critical infrastructures. For the second challenge, although it is hard to quantify security status, cyber security metrics can assist management systems in (1) assessing that the security controls are in compliance with the organisation's policies, processes, or procedures, (2) indicating their security strengths and weaknesses; (3) and identifying security trends, both within and outside the organisation's control.

Thus, the research problem tackled in the thesis can be stated with the following question.

*“Can Capability Maturity Models be extended to a cloud security capacity maturity model to assess cloud systems and their cloud-specific security issues and which forms of metrics are necessary for quantitative cloud security assessment and management?”*

To solve this problem, we have addressed following research questions.

- **Can Capability Maturity Models support cloud computing security?**

**Hypothesis:** It can be done by taking advantage of previous security maturity models applied for traditional cyber systems. First, we need to investigate what are the fundamentals of Capability Maturity Models like the idea, the structure, the various kinds of models, the assessment procedures, and other properties. We need to identify these models can be applied in supporting quality management in different areas like economics, health, and IT fields. Then we study the literature review on how the capability maturity model is applied in the cyber security area. We identify strong and weak points from these applications.

- **Can a Capability Maturity model be extended to a cloud security capacity maturity model to assess cloud systems and their cloud-specific security issues?**

**Hypothesis:** The Capability Maturity model needs to be tailored to the cloud computing by investigation of the specification of cloud computing including service models, virtualisation, portability and interchangeability. From the study of the advantages and disadvantages of applying maturity models in cyber security, we select specifications that fit for cloud computing. For the purpose of good design of the model, we may have to create sets of policies, procedures, assessing level processes to support management in undertaking security activities. One of critical model components is a security metric framework that can be used to assess the suitable security metrics to determine the maturity security level of a particular security domain within the Capability Maturity Model.

- **Which forms of metrics are necessary for quantitative cloud security assessment and management?**

**Hypothesis:** It can be done by 2 ways. The first way is investigating qualitative metrics applied in previous security maturity models. These qualitative metrics can be transferred to quantitative metrics and can be used to compare the efficiency and the effect of this alternative to make a better decision. The second way is to create better quantitative

metrics and then compare these with previous metrics. In this thesis, we focus on measuring the impact of security breaches on security components and stakeholders involving a cloud computing system. This impact can be measured in terms of cost, time, or energy. However, one of the critical security issues is how we can quantify the probability of security threat materialised in the relation with security factors such as attackers, security vulnerabilities, favourable conditions, and defence systems. Therefore, to implement the quantitative security metrics, several security threat models can be designed to investigate the probability of security threats that have materialised into security attacks.

- **Can security threat models be developed to quantify the probability of a security threat materialised into security attacks?**

*Hypothesis:* By researching the security factors relating to a real security attack such as attackers, vulnerabilities, controllers, and favourable conditions, we will explore the concept, the function, and the role of each of these security factors that form a security threat. By investigating the process of a realistic security attack from the beginning until successful attacks or failure state for the real system, we will identify how the above security factors interact in the attack-defend process between attackers and defenders or controllers. As a result, we can develop security threat models that quantify the probability of security threats materialised into security attacks by applying a basic model like Markov, and Bayes or several mathematical models like search theory or combinatorics.

- **Can the proposed Cloud Security Capability Maturity Model be validated and evaluated by using the novel security metrics that take different security measurements on the probability of security threats?**

*Hypothesis:* To assess several security domains from Cloud Security Capability Maturity Model (CSCMM), we investigate the relationship between security threats and security domains within the CSCMM. Several above measurements of computing the security threat probability will be applied to generate the novel security metric (Mean Security Remediation Cost). Through the security metric framework, CSCMM will be validated by assessing the security levels of several security domains within CSCMM.

### 1.3 Research Aims and Objectives and Scope

In this section, we will investigate the stakeholders of the thesis that are people or organisations involved or are able to take advantages from the thesis. Subsequently, research aims, and objectives of the thesis will be presented.

The stakeholders of the thesis are: (1) cloud security managers who want to have an effective and efficient cloud security model with a set of security domains that not only shows the security level of the system but also shows the weakness; (2) cloud security experts who run and take responsibility for securing cloud system. They want a system of quantitative security metrics to provide for measuring the security levels and implementing security actions; (3) cloud security researchers in the field of cloud security who want to have a security model based on a maturity model to develop the theory of maturity and its application in cloud security.

The major interest of this thesis is to provide the solutions to develop a security model for cloud so that it can support security management to assess security levels of a cloud security system by taking into account numerous security metrics. Therefore, we *aim to investigate relevant quantitative security metrics and propose a novel Capability Maturity Model with quantitative security metrics for assessing and managing cloud computing security.*

To achieve the aim above, the objectives of the thesis can be expressed as follows.

*First*, we review and refine the definitions of cyber space and cyber security that are fundamental to the investigation of security issues and challenges in cloud computing, especially in cloud security models and standards.

*Second*, we investigate Capability Maturity Model and how these models can apply to support security management in cyber space. Then, we propose a cyber security maturity model for cloud computing that investigates specific security domains for cloud security and refines security maturity levels which are consistent with cloud security requirements.

*Third*, we develop three security threat models to quantify the probability of security threat that materialise into security attacks. These three models will be investigated in different aspects. The first model will consider a security threat materialised into attacks as a Markov chain. The second model will focus on the relationship between security factors such as attackers, vulnerabilities, and controllers. The third model will concentrate

on the capability of attackers and controllers, and the relations with the exploitation and mitigation of security vulnerabilities.

*Fourth*, we generate a new quantitative security metric in terms of security cost using the above computation of realised threat probability applied to assess cyber security maturity models for cloud computing.

*Fifth*, we demonstrate, validate, and evaluate the proposed Capability Maturity model and quantitative security metrics by applying the model to the database from security companies. Then all the research outcomes will be published in peer-reviewed international conferences and journals in cyber security and cloud computing.

The significances of objectives to the aims are: (1) By proposing a new cloud security capability maturity model, this will allow managers to make better decisions in security management, and practitioners to implement better security actions. In addition, by doing so, it contributes to the development of the maturity model theory. (2) By developing new quantitative security metrics, which are based on mathematical models, applied for the above model, this will assist security practitioners to identify the weaknesses of a system and implement security actions to protect the cloud system. (3) By validating, evaluating, and simulating the security metrics for CSCMM model, we will develop a tool assessing the security levels for the whole cloud system and reporting and giving advice for a more secure system.

- **The research scope of the thesis**

Although the proposed security model and security metrics can be applied for different IT areas, the thesis focuses on security in cloud computing. Moreover, it is impossible that a security metric can apply to measure security levels for all security domains. Therefore, to assess the security status of security domains within the model, we just concentrate on security metrics in terms of cost. Furthermore, in this thesis, we will investigate security domains that relate to cloud security threats. This means that several security factors like security attackers, vulnerabilities, and controllers will be investigated to identify the cloud security threat. Additionally, although an effective security model needs both qualitative and quantitative metrics to assess security activities related to human, management, and technical aspects, the thesis just focusses on security quantitative metrics.

In terms of database for validating and evaluating the model and the security metrics that the thesis proposes, we will use published security data from several prestige security companies such as IBM, BitDefender, Norton, and Gartner. For the database of security vulnerabilities, we will use the Common Vulnerability Scoring System (CVSS) database from 10/1999 until 10/2019.

In summary, the thesis will focus on the cloud security model based on applying the Capability Maturity Model. Specifically, we will be interested in several security domains/facets which relate to security breaches or attacks. The thesis will be limited to generating quantitative security metrics in terms of cost to assess the impact of security breaches on cloud security stakeholders. Therefore, many security domains within the cloud security model which do not relate to security attacks or breaches such as Governance, Security Policies, Education and Training will not be in the scope of the thesis. Furthermore, qualitative security metrics that relate to human or management factors are also not in the scope of the thesis.

## **1.4 Research Contributions**

The thesis concentrates on generating new quantitative security metrics to assess security levels of several security facets in our novel Cloud Security Capability Maturity Model (CSCMM). Despite many security models which have applied Capability Maturity Models to support security management and implementation, few studies have applied this theory in cloud security. This research will open the knowledge of Maturity Model theory. In addition, an extensive search of the literature shows that recent security maturity models or cloud security models mainly focus on qualitative metrics to assess the security level of the system. This thesis is interested in developing quantitative security metrics that are suitable for technical trends when almost all security events can be measured quantitatively, especially in the area of artificial intelligence and deep machine learning. Therefore, this research will make several significant contributions:

- A novel Cloud Security Capability Maturity Model (CSCMM) is proposed. This is a new approach to cloud security that allows managers or practitioners: (1) to identify the security gaps of the system via an assessment process; (2) to establish the security target on every security domain; (3) to plan to address security problems to fill the gaps

between security current and target state. The proposal of CSCMM model will contribute to the development of knowledge of Maturity model theory.

- Three security models are developed to quantify the probability of a security threat which has been materialised into attacks. These various models, which compute the probability of realised security threats, will be applied to our proposed security metric named Mean Security Remediation Cost. These models will investigate three perspectives of a security threat materialised into attacks including a security attack process as a Markov chain, an attack process as an exist-escape process of attackers and defenders, and a skill-based attack-control security threat that focuses on the capability or skill of attackers and controllers. Computing the probability of a security event is very critical in security research. It can be applied in many measurements in cyber security like security risk or insurance. Therefore, the novelty of these three proposed security threat models is not only applied for our security metric but also used in quantifying security risk or insurance.

- A novel security quantitative metric named Mean Security Remediation Cost (MSRC) is developed. Within this metric, a security stakeholder model is proposed to identify which stakeholder is involved in security breaches and assess how security breaches affect security stakeholders in terms of cost. The metric also investigates the relationship between security factors including security stakeholders, security components, classes of cloud threat, and relevant security threats. The novelty of this security metric is that it provides the method to measure the impact of materialised security threats (the above contribution) on security components. Specifically, it determines the cost that security stakeholders have to spend to remediate the system when a security threat materialises into attacks.

- The simulation results are demonstrated, validated, and evaluated by proposed Cloud Security Capability Maturity Model, Mean Security Remediation Cost metric, and three methods to compute the probability of security threat materialised into attacks. These research results will provide a tool to assess the maturity security level of specific security domains/facets of the CSCMM model via the above quantitative metric. These research results will support security managers in making security decisions and assist security practitioners in identifying any weaknesses of the cloud system to take security actions.

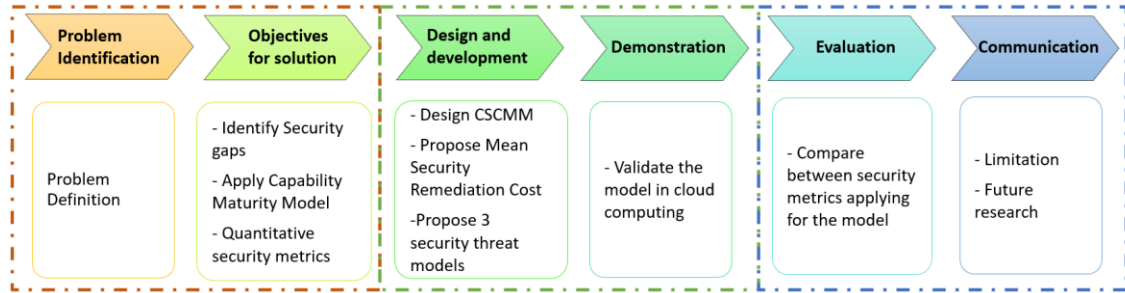


## 1.5 Research Model and Methodology

**Figure 1.2** illustrates the research model and methods based on Design Science Research Methodology (DSRM) [23]. The process includes three phases with six steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication. This first starts with problem Identification. This is the problem definition or research issues in this thesis. From the research questions and the literature review on cloud security, maturity models, and security metrics, we synthesise the research problems in existing cloud security models. We also point out the weaknesses of the maturity models. Then, moving to the objectives for solution step, we identify the security challenges; Apply Capability Maturity Model for securing Cloud Computing, the innovation of quantitative security metrics in assessing security levels for the cloud system.

Phase two embraces steps three and four when developing a new design security capability maturity model for cloud, create new security quantitative metrics named Mean Security Remediation Cost, and propose security threat models for quantifying the probability of a security threat materialised into attacks. Then we carry out the demonstration step. This is the implementation on the real cloud security data from prestige security companies. This research is designed as quantitative research. Therefore, data analysis, simulation and experiments need to be implemented. We will simulate the new model for each proposed quantitative security metric.

Phase three comprises steps five and six. Going to the evaluation step, we carry out the testing process to assess operating capabilities of the model and the advantages of the new quantitative metrics. This step can support the step 4 to refine simulation approaches. Additionally, different quantitative security metrics based on various security threat models will be compared and evaluated to determine which kind of metrics is suitable in which security scenario. Communication is the last step. This is the publications of research results in international conferences or journals. This step also identifies the limitations of the thesis and research works in the future.



**Figure 0.2** Design Science Research Methodology (DSRM)

## 1.6 Structure of the Thesis

This research has produced two published international conference papers, two journal papers, two under-review journal papers, and one conference paper ready to submit. The thesis is organised into nine chapters as follows.

Chapter 1 is the introduction of the thesis that expresses a general view of the whole research of the PhD study. Chapter 1 includes the statement and key issues of the thesis; the research aims, objectives, contributions, significance, and research methodology of the thesis.

Chapter 2 describes the background of the thesis. This consists of several parts related to Cloud Security, Cloud security model and metrics. We identify and clarify recent cloud security challenges and threats. Then we discuss previous research of security models on cloud computing and make a comparison with previous studies. The relevant mathematical background is also discussed to the proposed quantitative metrics in this thesis.

Chapter 3 proposes the Cloud Security Capability Maturity Model (CSCMM). We explore and investigate other models to consider the advantages and drawbacks to create the new model with 2 dimensions including security domains, and security maturity levels. We also propose a security metric framework that assesses security levels for several security domains within CSCMM.

Chapter 4 proposes a threat model using a Markov chain and Common Vulnerability Scoring System (CVSS) to quantify the probability of a security threat materialised into attacks. This proposes a novel approach to compute the probability distribution of cloud security threats based on a Markov chain and Common Vulnerability Scoring System

(CVSS). The chapter gives an application on cloud systems to demonstrate the use of the proposed approach.

Chapter 5 presents an exist-escape threat model for computing the probability of materialised threats and its application to Cloud. This chapter proposes a new security threat model and methods that allow the quantifying of the existence of a security threat and the probability that the security threat will materialise into attacks. A case study on cloud security is introduced to demonstrate the use of the proposed model and its computation.

Chapter 6 proposes a new security threat model named skilled-based attack-control. This model will focus on how to evaluate the skill of attackers and the capability of controllers. A mathematical theorem will be proposed to provide the solution to compute the probability of security threat existed, escaped, and materialised into attacks.

Chapter 7 proposes a quantitative metric named Mean Security Remediation Cost (MSRC) to indicate the cost for each involved cloud security stakeholder to remediate the system when a security threat has materialised into attacks. We provide a cloud security stakeholder model that indicates relevant stakeholders in the cloud security system. This deals with how they can be affected when a security threat can be materialised. MSRC will be validated in Cloud Computing to compute the cost for each cloud security stakeholder or for each security threat. MSRC metric is demonstrated as a security decision supporting tool for the organisation's senior management and for security managers to identify specific security concerns and take appropriate security actions.

Chapter 8 demonstrates the method to apply MSRC to evaluate the CSCMM model. We will assess several security domains within the CSCMM model that can be used by MSRC. Through the security metric framework and benchmarking method, MSRC will be used to assess the security maturity levels of several security domains within CSCMM. Several case studies will be demonstrated to show that MSRC can support security managers in making security decision and assisting security experts in taking security actions. Furthermore, two security models exist-escape and attack-control will be compared to investigate the advantages and disadvantages of each model.

Chapter 9 summarises the contributions of the thesis and draws the future research direction.

# Chapter 2

## Background

We are living in a world, in which, cyber space is indispensable and developing with an unprecedented rapid expansion. Almost all interactive information is transmitted, analysed, and processed via this space. Clearly a well-built cyber security is vital to ensure the security of the cyber space. However, the definitions and scopes of both cyber space and cyber security are still not well-defined and this makes it difficult to establish sound security models and mechanisms for protecting this space. Therefore, in this chapter, we first provide a review of various definitions of cyber space and cyber security in order to ascertain a common understanding of the space and its security. Recently, cloud security has become a new branch of cyber security. Identifying basic elements of cyber security will provide support for awareness of cloud security. Then, cloud security models and standards are investigated to identify the research gap for our proposed solutions. The thesis focuses on applying Capability Maturity Model for assessing cloud security by quantitative security metrics. Thus, this chapter investigates existing security maturity models, focusing on their defining characteristics and identifying their strengths and weaknesses. Then, we provide the background and related works on security metrics and measurements that are related to cyber security and security threats. Finally, the chapter presents the related mathematical foundation including Markov model, search theory, inclusive-exclusive principle that support computing methods for our proposed solutions.

The organisation of this chapter is as follows. Section 2.1 talks about the background of cyber space and cyber security. Section 2.2 presents an overview of cloud security models and standards. Section 2.3 expresses the review of existing Capability Maturity Models applying for cyber security. Section 2.4 discusses metrics and measurements relating to cyber security and security threats. Section 2.5 gives the mathematical background for the proposed solutions. Section 2.6 makes a conclusion of the chapter.

## **2.1 An overview of cyber space and cyber security**

Historically, the definition of cyber security has evolved greatly over the past decades. From the fundamental concept of security, it is defined as the quality or state of being secure - being free from danger [24]. For example, national security can be known as a system of multilayered processes that protect the sovereignty of a state - its assets, resources, and people against all kind of "national" crises. Therefore, cyber security can be thought of as a system of processes that protect the resources of cyber space. However, definitions of cyber security vary with different organisations. Some use the term “cyber security” but others prefer “information security” or “IT security” [25]. One of the reasons for this usage is that people consider both the cyber space and cyber security from different perspectives. The definition of cyber space has changed considerably since Wiener defined cybernetics in 1948 as “*control and communication in the animal and the machine*” [26]. Over the last few decades, academic organisations focused on the tangible elements in the cyber space when they paid more attention to the infrastructure components of IT systems, and on intangible elements such as the data or the applications within these systems. Recently, the cyber space has grown to include social networks, clouds, Internet of Things (IOTs), smart cities, smart grids, and other software-defined systems.

### **2.1.1 Cyber space**

According to the Oxford dictionary, it is a single word “cyberspace”. However, some authors use two words as in “cyber space”, and others prefer “cyber-space”. Some organisations use the term “information” as “cyber or cyber space”. In terms of the concept of cyber space, it has been defined and redefined over the years in order to take into account not only emerging technological developments but also the complexity of modern social networks. From the ITU [27], “the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, the latter with public and private incarnations”. With this definition, a cyber space covers computing element, resources, and the interconnecting infrastructure as well as users. However, it does not entail interaction among these elements.

Different countries, in their cyber security strategies, define cyber space in a narrow sense. According to Australia's Cyber Security Strategy [28], cyber security refers to the safety of computer systems. This implies that cyber space is just about computer systems and many elements are not included. According to Canada's Cyber Security Strategy [29], cyber space is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where people are linked together to exchange ideas, services and friendship. According to The Netherland's National Cyber Security Strategy [30], Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of Information and Communication Technology (ICT). Cyber space is all things within the realm of the ICT. According to Germany's Cyber Security Strategy [31], cyber space is the virtual space of all IT systems linked at data level on a global scale. According to New Zealand's Cyber Security Strategy, cyber space is considered as the global network such as the Internet [32]. The definition of cyber space is thus diverse and that leads to different emphases in the definitions of cyber security.

- **Elements of the cyber space**

In order to clearly identify elements of the cyber space, many authors classify them into categories. Rain Ottis and Peeter Lorents [33] took into account the time and human elements in defining cyber space. They defined cyber space as a time-dependent set of interconnected information systems and the human users that interact with these systems. With this definition, human and interaction are at the center of operation of cyber space. Shackelford [34] noted two aspects of cyber space including a physical interconnected critical infrastructure and a conceptual space for interaction.

From the discussion above on the definition of cyber space by various governments and organisations, we suggest that a cyber space consists of 3 key elements: real and virtual entities, interconnecting infrastructure, and interaction among entities through the infrastructure. Real and virtual entities include real things of physical devices such as computers, sensors, mobile phones, electronic devices and virtual abstraction of entities such as data/information, software, and services (i.e., things in Internet of Things). Infrastructure includes networks (e.g., the Internet), databases, information systems and storage that interconnect and support entities in the space. Interaction encompasses activities and interdependencies among cyber space entities (that are capable of

interacting including human beings) via the interconnecting infrastructure and the information within concerning communication, policy, business and management.

The **Table 2.1** shows the existence of these three key elements in various definitions from different countries and organisations. We identify that real-virtual entity is referenced in all definitions; most definitions explicitly include infrastructure; and some definitions consider interaction.

**Table 0.1** Cyber space entities referenced in the definition of cyber space by various cyber space government strategies and organisations

Organisation/ Nation	Real -Virtual	Infrastructure	Interaction
ITU	*	*	
EC	*		
Australia	*		
Canada	*	*	
Denmark	*	*	
Germany	*	*	
Japan	*	*	
Netherlands	*		
New Zealand	*		*
Norway	*	*	
UK	*	*	*
USA	*	*	*

\* Element referenced by the definition

In order to provide a common understanding of the space and its security, we suggest a unified definition of the cyber space as *the space that embraces all three key elements: real and virtual entities, interconnecting infrastructure, and interaction among entities*. In particular, the emphasis is on interaction as it is fundamental to security; without interaction among entities, including human beings, the question on security may not make sense.

### 2.1.2 Cyber security

As mentioned earlier, before the term “cyber security” came into existence, the terms computer security, IT security, or information security were used in security documents and literature. We highlight several definitions of cyber security for discussion and

clarification. According to Gasser and Morrie [35], computer security, also known as cyber security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. ITU [36] defines Cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. From these definitions, it is apparent that information security emphasises the confidentiality, integrity and availability of information whereas computer security focuses on the availability, integrity, and correct operation of systems. Cyber security, however, is more comprehensive in that it emphasises the protection of all of the organisation's assets using tools, processes, concepts and necessary interaction among elements within. Therefore, we suggest the following definition:

Cyber security can be considered as a collection of systems, tools, processes, practices, concepts and strategies that are used to prevent and protect the cyber space from unauthorised interaction by agents with elements of the space and to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources.

We believe that this definition unifies previous definitions and importantly it clarifies the scope of cyber security in three aspects. Firstly, the term cyber security is used instead of the terms information security or IT security to focus attention on the security of cyber space rather than security in a narrower sense. Secondly, prevention, not just protection is an integral part of the definition. It makes sense to look at security in a wider context where prevention and protection are interrelated. Preventing some vulnerability from being exploited can be considered protecting the space and on the other hand, knowing how to protect the cyber space implies to some extent the knowledge of how security breaches occur and how they can be prevented. Thirdly, with rapid emergence of many modern technologies, such as cloud, the Internet of Things, and social networks, additional considerations, including adaptability, non-repudiation or safety may be added to the triad rules of CIA (Confidentiality, Integrity, and Availability) of cyber security. Today, in order to achieve a model that is invariant to new and emerging technologies,



additional properties such as authenticity, accountability and safety may need to be included in the definition.

## **2.2 Cloud computing and Cloud security models and standards**

Cloud is a particular cyber space. Based on virtualisation and shared IT resources, cloud computing is seen as a technological evolution of cyber space. It plays an important role in the world IT development and it will continue to evolve extensively over the next decades [1]. However, clouds, as cyber infrastructures, with three service models (IaaS, PaaS, and SaaS), four deployment cloud types (Private, Public, Hybrid, and Community) are facing challenging security issues. Cloud security challenges are identified in various aspects including governance and compliance, virtualisation, identity management [37-39], and various security threats aspects [40, 41]. Cloud Security Alliance (CSA) published the security report namely “The Treacherous Twelve Cloud Computing Top Threats in 2016” providing organisations with the awareness of cloud security issues in making educated risk-management decisions [42]. To tackle these cloud security problems, researchers, businesses, and organisations have been making efforts to mitigate cloud security risk and handle security threats by development cloud security standards and models. In this section, the overview of cloud computing, cloud security models and standards will be expressed as follows.

- The concept of cloud computing

The definitions of cloud computing have changed by various viewpoints of different organisations. In 2011, National Institute of Standard and Technology (NIST) proposed a principal definition of Cloud Computing as a revolutionary method to share computing resources (e.g., servers, storage, networks, applications, and services), and accessed by on-demand network with minimal management effort for the end users and with minimum interaction from service providers [43]. Another definition considered a Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualised computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers [44].

According to NIST, the cloud model includes five essential characteristics, three service models, and four deployment models.

Five essential characteristics are: (1) *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. (2) *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). (3) *Resource pooling*. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth. (4) *Rapid elasticity*. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. (5) *Measured service*. Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

Three Service Models are: (1) *Software as a Service (SaaS)*. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, apart from limited user-specific application configuration settings. (2) *Platform as a Service (PaaS)*. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming

languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (3) *Infrastructure as a Service (IaaS)*. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Four Deployment Models are: (1) *Private cloud*. The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises. (2) *Community cloud*. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises. (3) *Public cloud*. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider. (4) *Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

In Cloud Computing, virtualisation is significantly integrated as an innovation technology. Virtualisation is considered as the logical abstraction of physical assets, such as the hardware platform, operating system (OS), storage devices, data stores, or network interfaces. Virtualisation can be implemented at various portions of the system architecture: (1) Processor virtualisation enables a processor to be shared across multiple application instances; (2) Memory virtualisation aggregates memory resources into a pool

of single memory and manages the memory on behalf of the multiple applications using it; (3) Network virtualisation entails virtual IP management and segmentation; (4) Storage virtualisation provides a layer of abstraction for the physical storage of data. In other words, Virtualisation is a conversion process that translates unique IT hardware into Emulated and Standardised software-based copies.

The hypervisor is responsible for managing the applications' OSs (guest OSs) and their use of the system resources (e.g., CPU, memory, and storage). It supports the isolation and manages multiple VM's running on the same host computer. A hypervisor is a small and specialised Operating system that runs on top of the base hardware. It creates and manages virtual machines (VMs). A hypervisor runs on a physical server (Host Machine) to allow physical resources to be partitioned into virtual resources (CPU, Memory, Storage, and Networks).

- Cloud security models and standards

Cloud is a particular cyber space. Based on virtualisation and shared IT resources, cloud computing is seen as a technological evolution of cyber space. It plays an important role in the world IT development and it will continue to evolve extensively over the next decades [1]. However, clouds, as cyber infrastructures, with three service models (IaaS, PaaS, and SaaS), four deployment cloud types (Private, Public, Hybrid, and Community) are facing challenging security issues. According to IDC survey, the top challenge for 74% of CIOs in cloud computing companies are concerned about security [4].

Identified cloud security aspects include governance and compliance, virtualisation, identity management [37-39], and various threats aspects [40, 41]. Cloud Security Alliance (CSA) published the security report namely “The Treacherous Twelve Cloud Computing Top Threats in 2016” providing organisations with the awareness of cloud security issues in making educated risk-management decisions [42].

To combat cloud security problems, researchers, businesses, and organisations have been making efforts to mitigate cloud security risk and tackle security threats by development of cloud security standards and models. In 2014, the European Union Agency for Network and Information Security (ENISA) [19] released the report “Cloud standards and security” to provide an overview of standards relevant for cloud computing security. Cloud Security Alliance (CSA) introduced and developed “security guidance for critical areas of focus in cloud computing” through 3 versions including Version 1.0 [20],

Version 2.1 [21] (2009), and Version 3.0 [7] (2011). The latest version (Version 3.0) is tailored for meeting the security demand change. The aim of this guidance is to introduce better standards for organisations to manage cyber security for cloud by implementation security domains. The guidance approached cloud architecture with cloud service model (SaaS, PaaS, and IaaS) and four deployment models (Public, Private, Community, and Hybrid Cloud) with derivative variations that address specific requirements. The guidance principal is based on thirteen different domains which are divided into two general categories: governance and operations. The governance domains focus on broad and strategic issues as well as policies within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

This guidance is relevant to cloud computing, its service models and its deployment models. Regarding cloud security management, the guidance focuses on cloud-specific issues: interoperability and portability, data security, and virtualisation. Dividing the implementation domains into two groups with strategic and tactical categories is another salient point of the guidance. This approach allows cloud consumers and providers to bring financial and human resources into security consideration. Furthermore, the guidance can be mapped to existing security models such as “Cloud Control Matrix” [22], international cyber security standards ISO/IEC 27002 and other NIST Special Publications. Despite the benefits, however, the guidance has a number of drawbacks. The guidance lacks an assessment guide for each domain. It does not consider security metrics for security practices. Therefore, organisations find it difficult to determine the security level of a domain.

In addition, there are a number of standards concerning cloud security. The ISO/IEC 27017 Standard illustrates the information security elements of cloud computing. It assists with the implementation of cloud-specific information security controls, supplementing the guidance in ISO 27000 series standards, including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management. The NIST released the following standards on cloud computing: NIST SP 500-291, ‘Cloud Computing Standards Roadmap’, NIST SP 800-146, ‘Cloud Computing Synopsis and Recommendations’, NIST SP 800-144, ‘Guidelines on Security & Privacy in Public Cloud Computing’, NIST SP 500-292, ‘Cloud

Computing Reference Architecture’ and NIST SP 500-293, ‘US Cloud Computing Technology Roadmap’.

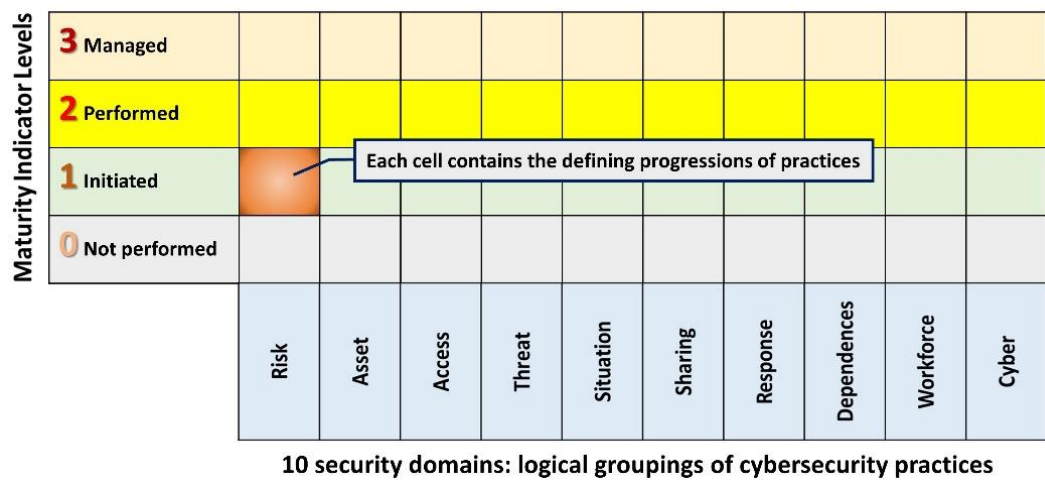
## **2.3 Cyber Security Maturity Model**

As mentioned from Chapter 1, once Humphrey recommended a capability maturity model for software quality assessing [8], this model was applied for security cyber space for mainly three reasons. First, maturity models propose a realistic management process including a completed domain system and a maturity level assess system for cyber security. Second, this model has been applied successfully for many fields including economic, business, IT, education, and critical infrastructure system management. Third, they can be extended to cover many security aspects or domains. Recently, maturity model has been applied for securing many important cyber spaces such as e-government, e-commerce, education, health, and particularly in critical national infrastructure such as electricity, water supply, petrol, and transportation [9]. This section provides a comprehensive review of twelve various prominent cyber security maturity models from 2000. These models will be discussed and analysed to identify how they apply to cyber security. Moreover, we will compare those existing security maturity models, underline their common aspects, highlight their differences, and more importantly identify features that have to be addressed in a cyber security maturity model.

Since 2000, City Group initiated cyber security maturity models with the name Information Security Evaluation Maturity Model (ISEM). Until now, twelve cyber security maturity models have been developed and applied to different fields and organisations of different scales.

In 2007, Information Security Management Maturity Model (ISM3) was developed by ISM3 consortium [45] with five levels: undefined, defined, managed, controlled and optimised. This model focuses on evaluating, specifying, implementing and enhancing process-oriented information security management systems. The advantage of the model is that it considers organisational culture as a security issue. Moreover, it is based on previous cyber security standards and practices like ISO 9000, and ISO 17799/27001. The ISM3 model is applicable to organisations of different sizes. Cyber security measurement is based on measuring activities, effectiveness and quality.

From 2007, in the program review for information security management assistance (PRISMA) [46], the National Institute of Standard and Technology (NIST) created Information Security Maturity Model (ISM2) to evaluate the cyber security level of an organisation. This model includes five levels: policies, procedures, implementation, testing, and integration. The key contributions of this model are evaluation capabilities and support system of documents to implement best practices for attaining standards of cyber security. The main metrics to assess cyber security levels are based on standards (mainly qualitative measurement).

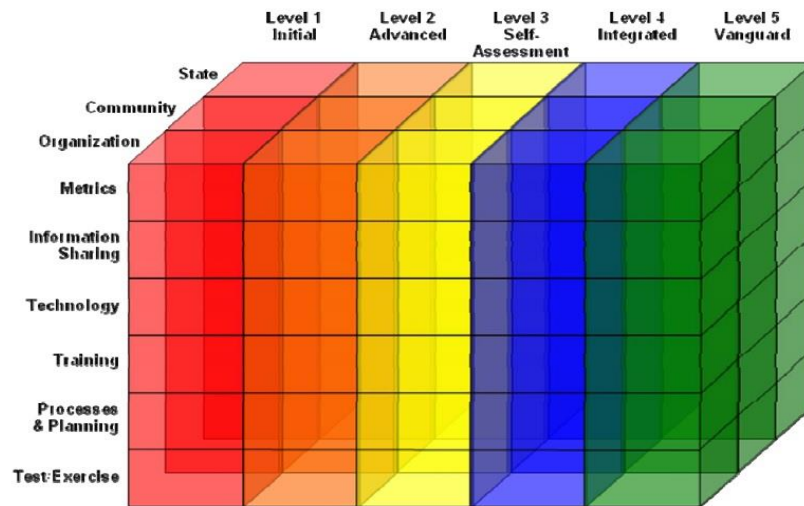


**Figure 0.1** Overall ES-C2M2 Structure

The Cyber security Capability Maturity Model (C2M2) was developed by the Department of Energy (DOE) to help critical infrastructure organisations evaluate and potentially improve their cyber security practices [9] (Figure 2.1). This model has been used to create Electricity Subsector Cyber Security Capability Model (ES-C2M2) and the Oil and Natural Gas Subsector Cyber Security Capability Model (ONG-C2M2). The specialty in the design of the architecture is that the model uses ten security domains and each domain contains a structured set of cyber security practices. Each set of practices represents the activities that can be performed to establish mature capability in the domain. To measure maturity level of a cyber system C2M2 uses a scale of maturity indicator levels (MILs) 0-3 (not performed, initiated, performed, and managed). For example, if a cyber-system attains level 2, all 10 domains must be at least level 2.

Another maturity model is Community Cyber Security Maturity Model (CCSMM) [47] (Figure 2.2). This model also has 5 levels from the initial to the vanguard level. The

significant point of this model is that the author added the third dimension namely geography with three different scales including organisation, community and state. This model is applicable to different cyber systems of different sizes from small size companies to big size organisations such as a ministry or a state. This model was implemented in five states within the United States of America with funding from the National Cyber Security Division of the Department of Homeland Security (USA).



**Figure 0.2** CCSMM Model

## 2.4 Metrics and measures in cyber security and security threat

In this section, we first review the fundamentals of metrics and security metrics including the concepts, the roles, the categories, the requirements, and the programs of security metrics. Then security metrics relating to security threats will be expressed. In this part we conclude several research identifications that are the basis for our proposed solutions to be represented in the coming chapters.

### 2.4.1 Fundamentals of metrics and security metrics

- Metrics and measures

To assess the level of a security state, metrics or measurements have been used. The usage of these two terms, however, has different meanings and implications. Metrics imply tools to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. A measure is a



concrete, objective attribute, such as the percentage of systems within an organisation that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide. Measures are quantifiable, observable, and objective data supporting metrics [48]. According to the Information Assurance Technology Analysis Center (IATAC), a measurement is the act or the process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined. A measure is a variable to which a value is assigned as a result of the measurement. A metric is a system of related measuring enabling quantification of some characteristic of a system, component or process. A metric is composed of two or more measures [49].

- Importance of security metrics

Lord Kelvin [13] stated that “when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind”. Therefore, metrics are needed to assess the security of the cyber space. In terms of software quality assessment, Humphrey [50] insisted that “quality management is impossible without quality measures and quality data. As long as software people try to improve quality without measuring and managing quality, they will make little or no progress”.

However, it is difficult to measure the cyber security state for 3 reasons: vulnerabilities is hard to measure by anyone, even the owner of the system; the set of weaknesses (vulnerabilities) known to the observer is not known by the owner of the system and thus is not measured by the owner; no system owner can know the totality of his adversaries. Despite having several difficulties in security measuring, cyber security metrics can support organisations in (1) verifying that their security controls are in compliance with a policy, process, or procedure, (2) identifying their security strengths and weaknesses; and (3) identifying security trends, both within and outside the organisation’s control [14].

- Security metrics categories

Security metrics can be categorised by what and how they are measured. What are measured may include process, performance, outcomes, quality, trends, conformance to

standard, and probabilities. How these things are measured may be categorised by the methods such as: maturity; multidimensional scorecards; value; benchmarking; modeling; and statistical analysis [51]. Based on fundamental characteristics of metrics, they can be grouped as follows: (1) Quantitative/Qualitative: Quantitative metrics (e.g., number of failed login attempts) are preferable to qualitative metrics (e.g., self-assessment levels); (2) Dynamic/Static: Dynamic metrics evolve with time while static metrics do not. Dynamic metrics are more useful than static because best practices change over time with technology; (3) Objective/Subjective: Objective metrics (e.g., mean annual downtime for a system) are more desirable than subjective metrics (e.g., amount of training a user needs to securely use the system); (4) Direct/Indirect: Direct metrics are generated from observing the property that they measure (e.g., the number of invalid packets rejected for a fire-wall). Indirect metrics are derived by evaluation and assessment.

In terms of management/organisational perspective, there are several security metric categorisations. In [52], the Center for Internet Security (CIS) divided security metrics into three groups which are Management, Operations, or both. Chew et al. [16] grouped security metrics by Implementation, Effectiveness and Efficiency, and Business Impact. Savola [53] differentiated metrics into Management, Operational, and Technical. These categorisations may overlap as well as interrelate. However, these taxonomies tend to simplify complex socio-technical or practice-theory relationships [54].

- Security metrics requirement

In a metrics system, several requirements of a good security metric are considered carefully and have been proposed by organisations and researchers. Jaquith [14] asserts that security metrics requirements should include consistently measured, cheap to gather, expressed as a cardinal number or percentage and using at least one unit of measure, and contextually specific. According to Wesner [55], security metrics should be “SMART” (Specific, Measurable, Actionable, Relevant, and Timely). Brotby [56] proposes “PRAGMATIC” requirement with P for Predictive, R for Relevant, A for Actionable), G for Genuine, M for Meaningful, A for Accurate, T for Timely) I for Independent, and C for Cheap. Herrmann [57] considers that a good security metric is one that possesses Accurate, Precise, Valid, and Correct characteristics.

- Security metrics program

Once the security metrics have been decided by an organisation for its system, a security metrics program has to be established to provide the organisation with a map to manage, control, or improve the system security domains [58]. Several methods to build up a security metrics program are deployed. First, Payne [59] proposed “Seven Steps model” to establish security metrics including: defining the metrics program goal(s) and objectives; deciding metrics to generate; developing strategies for generating the metrics; establishing benchmarks and targets; determining which metrics are reported; creating an action plan and act on it; and establishing a formal program review/refinement cycle. NIST also considered the metrics development and selection cycle via seven steps from identify stakeholders and interest to business mission impact [60].

Chew et al. [16] proposed five key components of making a metrics program plan: program initiation; development of information security metrics; analysis of information security metrics; reporting information security metrics; maintaining an information security metrics program. Campbell and Blades [61] listed five steps in a security metrics program: identifying the business drivers and objectives for the security metrics program; determining who your metrics are intended to inform and influence; identifying the types and locations of data essential for actionable security metrics; establishing relevant metrics; establishing internal controls to ensure integrity of data and data assessments and to protect confidentiality.

## **2.4.2 Metrics about security threats**

The demand for security of cyber systems is ever-increasing as critical infrastructures and their interconnection are constantly adapting to emerging sophisticated applications and IOT devices [62]. This leads to a large attack surface that a cyber-system has to cover to ensure its security. The development of security metrics is thus essential for supporting security management in terms of security decisions and security actions that can identify vulnerability aspects of the system, potential security threats, and security measures for protecting the system [63]. In particular, cyber security metrics can support an organisation in (1) verifying that their security controls are in compliance with the organisation’s policies, processes, or procedures, (2) identifying their security strengths and weaknesses; (3) and identifying security trends, both within and outside the organisation’s control [14]. Security metrics have been the focus of many organisations.

The Centre for Internet Security (CIS) has designed a set of security metrics in management, operation, and technique [15]. The National Institute of Standards and Technology (NIST) has developed security metrics in implementation, effectiveness, and impact [64].

Among this diverse set of security metrics that cover various aspects of a system, the most important security measure is the measure of the probability of a materialised threat. This measure is important for several reasons. First, there is no system that is 100% secured because of the complex nature of its underlying technologies, and the incompleteness of our understanding of the behaviour/interaction of the human beings internal and/or external to the system. System vulnerabilities and potential threats always exist and evolve along with the dynamics of the system and its users. The issue is how to quantify the measure of the probability of a threat materialised. Second, by definition, security risk is the product of probability of a security threat and its consequence when the security threat materialised [65]. Clearly, an essential component for the estimation of security risk is the measure of the probability that the threat materialised. Third, the measure of the probability that a threat materialised implicates the specific vulnerabilities associated with the threat and hence effective security measures that can be taken to prevent or mitigate the occurrence of attacks and their consequences.

- The fundamentals of security threats

The method of computing and the value of security threat/risk prediction are thus bound and restricted to the adopted security threat definition. We identify three problems concerning the selection of an effective security metric: adopting an appropriate definition of security threat, selecting a realistic set of security factors, and obtaining relevant security data. Regarding the definition, the problem is that there are no unique concepts/definitions of security threats among various organisations or individuals. According to the Oxford dictionary, threat is defined as “A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done” or “A person or thing likely to cause damage or danger” [66]. According to ISO 27005, security threat is a potential cause of an incident that may result in harm of systems and organisation. In terms of information assurance viewpoint, NIST gave the concept of security threat as any circumstance or event with the potential to adversely impact organisational operations [67]. Similarly, ENISA defined security

threat as any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service. Sandro et al. proposed the concept of security threat as every event that can result in information confidentiality, integrity and availability breaches, or with any other form of information system resources damage [68]. The premise for these definitions is somewhat loosely defined and hence the obtained value of the probability of a materialised security threat is not effective for security control.

Regarding the set of realistic security factors, an attack process is always unpredictable, and its tracing is complex because of many intertwined security factors. The security threat probability measure clearly depends on the security factor selected. Regarding relevant system security data, empirical metrics, which are generated from observation of real behaviour of the system, have been used to compute cloud security threat probability distributions [69]. The data for computing the security threat probability in cloud computing was collected in a year through the observation of attacks related to each specific cloud security threat. In [70], seven types of model-based metrics, which are created by integrating mathematical models and empirical measurements, are also used to calculate the probability of a security threat. In [71], the study used a semi-Markov model to investigate the attack process to compute the transition probability between security states.

Overall, most previous studies assumed that a security threat is any event that can harm the system. However, this assumption is rather vague and open for misinterpretation. An event that can harm the system could be remotely related to the actual and eventual security breach or attack. It is difficult to quantify a security threat and whether the value really reflects the link between the threat and its eventual attack.

Computation of security threat probability is vital for several reasons. First, to estimate a security risk, the most important factor is the quantification of the probability of successful attack or the probability of a security threat materialized into an attack. Second, quantitative security threat measures allow managers to make effective security decisions or assist security practitioners in taking appropriate security actions. Recently, there have been several studies on security threats and the computation of security threat or successful attack.

- Empirical metrics related to security threat

These types of metrics are also referred to as measurements-based metrics [72]. They are created from observation of real behaviour of the system. There are several security threats studies that use empirical metrics.

Ben et al. introduced a security metric called Mean Failure Cost (MFC). It is a value-based metric that quantifies the security of a computing system using random variables representing stakeholders, the amount of loss that results from security threats, and system vulnerabilities [69]. In this study, the probability of a security threat is an essential component of the MFC metric. However, the data was collected by an empirical method through observing the number of attacks related to the security threats in a year.

Ortalo et al. [73] proposed a metric called Mean Effort to Failure (METF). The authors conducted experiments on a large real system for almost two years to validate the proposed METF metric. The evaluation is based on a theoretical model called the privilege graph and in transformed into a Markov model which describes the system vulnerabilities that may offer opportunities to potential attackers to defeat some security objectives.

In [74], Jonsson et al. have conducted various experiments for better understanding the intrusion process in networks. Attacking process can be split into three phases: the learning phase, the standard attack phase, and the innovative attack phase. Also, the probability for successful attacks during the learning and innovative phases is expected to be small, although for different reasons. During the standard attack phase, it is expected to be considerably higher. One of significant results is to indicate that the times between security breaches are exponentially distributed.

These empirical metrics are consistent for directly measuring security properties. However, one of the drawbacks is that these metrics are not useful for security prediction.

- Model-based metrics related to security threat

Model-based metrics are also referred to as analytical metrics [72], which are needed when the relationship between the measurements and the security property being measured is not trivial. In this case, the target being evaluated is represented by a formal mathematical model and the metric values result from complex mathematical equations. Several models are used to evaluate security threats including attack graphs, Markov models, and Bayesian networks. In [75, 76], the authors considered model-based security

metrics as a part of “Cybersecurity Dynamics” approach that focuses on security factors including networks, vulnerabilities, defence, attacks, and cybersecurity state.

In one of our recent research [77], we used Markov chain and Common Vulnerability Scoring System (CVSS) to compute the probability distribution of cloud security threats. Markov chain is used to represent the attack process with different security states. CVSS is used to determine the transition probability between states. This model is applied in cloud computing with twelve security threats published by Cloud Security Alliance (CSA).

For Probability-Based Security Metrics related to a security threat, Probability-based security metrics usually express the likelihood of an adversary compromising the system or the probability that the system is secure [78]. Jha et al. [79] proposed a reliability metric, which represents the probability of an adversary not succeeding in an attack. This metric is obtained from a continuous time Markov chain generated from assigning transition probabilities to the edges of an attack graph. Formally, the reliability of the network is the probability that, in a sufficiently long execution time, the Markov chain will not be in a security failure state. In case not all transition probabilities are available, due to, for example, lack of data about attacks, the authors proposed a Decision Markov Process approach to compute the reliability metric. Li et al. [80] used a renewal stochastic process to estimate the likelihood that an adversary exploits a randomly selected system vulnerability.

From these background studies on security threats and attack processes, we observe the following: (1) different concepts of security give rise to different security models leading to different computation methods for security threat probability. Hence the value of the outcome (the quantitative measure of the probability of an attack) depends on how close the adopted security threat concept describes the reality; and (2) to our best knowledge, two essential and interrelated processes are missing in most models: the first process is the establishment and existence of a security threat; the other is the materialization of the existed security threat into an attack. Our proposed model integrates these processes by taking into account the attackers and their capabilities, the system vulnerabilities, and the security defender/controller capabilities.

Overall, the background of security metrics and measures in cyber security and security threats will be investigated comprehensively and used in the majority of our research. The theory of security metrics will be applied in Chapter 3, 4, 5, 6, 7, and 8. In

Chapter 3, to generate the security metric framework, which is used for assessing maturity security level for the cloud system, we will use much of knowledge about the concepts of security metrics and measures, the requirements of good metrics, the integration of choosing qualitative and quantitative metrics, the program to choose appropriate security metrics. In chapter 4, 5, and 6, we will propose three different security threat models. We will measure probability of security threat existed or materialised into attacks. Therefore, security metrics, which relate to security threats, are investigated critically to apply for our proposed method. In Chapter 7 and 8, we will propose a novel quantitative security metric named Mean Security Remediation Cost (MSRC), which uses the results from our proposed three security threat models, applied for assessing maturity security level of a cloud system. Additionally, a benchmark method will be used to determine the maturity level. As a result, the benefits of fundamentals of security metrics will be taken into our proposed metric.

## **2.5 Mathematical background**

In this section, we describe mathematical fundamentals required for our proposed security threat models. We first give the introduction of a Markov model which is considered as a security threat model including three states: security, threat, and failure. We then show Search theory which supports the method to compute the probability of the event that defenders detect attackers when both randomly enter a building. This theory will be applied in our security model to compute the probability of security threat materialised into attacks. Finally, the background of inclusive-exclusive principle will be described. This principle will be applied for our third security threat model to compute the probability of existing security threat in terms of modelling skill of attackers.

### **2.5.1 Markov chain and applied for security metrics**

A **Markov process** is a stochastic process whose dynamic behaviour is such that probability distributions for its future development depend only on the present state and not on how the process arrived in that state. If we assume that the state space,  $I$  is discrete (finite or countably infinite), then the Markov process is known as a **Markov chain**. If



we further assume that the parameter space,  $T$ , is also discrete, then we have a **discrete-time Markov chain** (DTMC) [81].

The property is that the probability of future actions is not dependent upon the steps that led up to the present state. This is called the Markov property. The conditional probability with the Markov Property can be expressed as

$$P(e_t | e_1, \dots, e_{t-1}) = P(e_t | e_{t-1}) \quad (2.1)$$

where  $e_t$  is the random variable of the Markov system at time  $t$ .

**Transition Matrices:** A transition matrix  $P_t$  for Markov chain  $X$  at time  $t$  is a matrix containing information on the probability of transitioning between states. In particular, given an ordering of a matrix's rows and columns by the state space  $S$ , the  $(i, j)^{th}$  element of the matrix is given by

$$(P_t)_{i,j} = P(X_{t+1} = j | X_t = i) \quad (2.2)$$

This means each row of the matrix is a probability vector, and the sum of its entries is 1.

- Security threat models using Markov chain

For a Markov process, the conditional probability distribution of future states of the process (conditional on both past and present states) depends only on the present state, not on the sequence of events that preceded it. Based on this property, several studies have deployed Markov for modelling security metrics.

In [82], Ariel et al. used Discrete Markov Chain Model to predict next honeypot attacks. In this study, to quantify the probability distribution of the next expected attacked honeypot in an attack session, malware or worm propagation is modelled as a directed graph representation of a Markov Chains model. The importance of this Markov model is how to compute the transition probability matrix. From this matrix, the probability distribution of the next expected attacked honeypot will be computed by the discrete time Markov chain equation. Estimation of transition from one honeypot to another honeypot was carried out by computing the ratio between the number of observed transition attacks from one ( $H_i$ ) to another ( $H_j$ ), divided by the number of all observed translations from ( $H_i$ ) to any honeypot.

In [83], Bharat et al. used Semi Markov Model (SMM) to quantify the security state for an intrusion tolerant system. In this work, Discrete Time Markov Chain (DTMC) steady-state probability was applied to compute the mean time to security failure (MTTSF).

In [84], Anderson et al. proposed a malware detection algorithm based on the analysis of graphs that represent Markov chains from dynamically collected instruction traces of the target executable.

For computing security threat probability using stochastic model, in [71], Jaafar et al. used the attack path concept and time is used to calculate transition probabilities. The authors used probability distribution functions to define the transitions of the model for characterizing the temporal aspects of the attacker and the system behaviour. The stochastic model was recognised to be a semi-Markov chain that was analytically solved to calculate the desirable quantitative security metrics, such as mean time to security failure and steady-state security. In [85], Almohri et al. proposed a probabilistic graph model, which is applied linear programming optimisation techniques, for analysing the security of complex networks to reduce the probability of successful attacks.

To our best knowledge, few studies consider applying Markov chain and for computing the probability distribution of security threats. Therefore, in chapter 4, we will use Markov chain theory to model a security threat to compute the probability of successful attacks.

## 2.5.2 Search theory

Search Theory is first introduced by Koopman in World War II [86]. The work was about the method to detect enemy submarines. Then, from this theory, much of the development was aimed at search and rescue (SAR) operations [87]. In 2002, Major proposed a terrorist detection model based on search theory [88]. This approach aimed to compute the probability that the defenders detect the terrorist in a building. It assumed that over a target with  $G$  possible locations,  $D$  defenders and  $A$  attackers are placed over the  $G$ -location grid and used the search theory [89] to determine the probability that the attackers are detected by the defenders.

The problem was stated as follows. We consider  $D$  defenders (guards) patrolling a target (a building) and  $A$  attackers (terrorist infiltrators) entering the area. Abstract this to

points placed on a grid. Say there are  $G$  grid locations. If the defenders and attackers are randomly placed on the grid, what is the probability that a type  $A$  point and a type  $D$  point end up at the same grid location?

Start with  $D = A = 1$ . The probability is clearly equal to  $1/G$ , because there is only one of the  $G$  locations where the defender is, and that is the one out of  $G$  chance that the attacker has of coinciding with the defender.

If  $D > 1$  and  $A = 1$ , the probability is really  $1 - (1 - 1/G)^D$ , reflecting the fact that each of the  $D$  defenders have an independent  $1/G$  chance of coinciding with the attacker. This is the complement of the probability that all  $D$  defenders independently miss the attacker,  $(1 - 1/G)^D$ .

Similarly, in the general case that  $D > 1$  and  $A > 1$ , the probability that the attack goes undetected is equal to  $(1 - 1/G)^{A \cdot D}$ . This represents the conjunction of the  $A$  independent events of all defenders missing a particular attacker.

Assuming that the “size of the search space”  $G$  is equal to the square root of the value of the target – while more valuable (read: bigger) targets need more defenders, it should not go up linearly. Further, we use the exponential approximation and set:

$$\Pr(\text{Escape Detection}) = \exp^{-\frac{A \cdot D}{\sqrt{V}}} \quad (2.3)$$

McQueen et al. [90] proposed a model based on Major’s work for estimating the time to compromise (TTC) of a system component that is visible to an attacker. The model provides an estimate of the expected value of the time-to-compromise as a function of known and visible vulnerabilities, and attacker skill levels. The time-to-compromise random process model is composed of three sub-processes associated with the attacker actions aimed at the exploitation of vulnerabilities.

Process 1 is for the case where at least one vulnerability is known, and the attacker has at least one exploit readily available that can be successfully used against one of the known vulnerabilities. Process 2 is for the case where at least one vulnerability is known, but the attacker does not have an exploit readily available that can be successfully used against one of the known vulnerabilities. Process 3 is the identification of new vulnerabilities and exploits. Process 3 is a parallel process constantly running in the background. The attacker of a particular system may use the results of process 3 or may be part of process 3. That is, the attacker may wait for new vulnerabilities/exploits to be identified or probe for new ones.

Each of these processes has a different probability distribution. Process 1 and 2 are mutually exclusive. Process 3 is ongoing and in parallel with the other two processes.

TTC is defined as the time needed for an attacker to gain some level of privilege on some system device. In other words, the TTC metric is obtained by breaking up the actions of the attacker into three statistical processes (the total time of all three processes) given by the formula:

$$T = t_1P_1 + t_2(1 - P_1)(1 - u) + t_3u(1 - P_1)$$

where,  $T$  is the expected value of time-to-compromise,  $t_1$  is the expected value of Process 1 (days),  $t_2$  is the expected value of Process 2 ( $5.8 * ET$ ),  $t_3 = ((V/AM) - 0.5) 30.42 + 5.8$ , the expected value of Process 3,  $u = (1 - (AM/V))^V$ , the probability that Process 2 is unsuccessful.

The probability that Process 1 happens is computed by

$$P_1 = 1 - e^{-Vm/k} \quad (2.4)$$

where,  $V$  is a number of vulnerabilities on the component of interest,  $m$  is number of exploits readily available to the attacker, and  $k$  is total number of vulnerabilities in the CVSS database.

$$ET = \frac{AM}{V} * \left( 1 + \sum_{tries=2}^{V-AM+1} \left[ tries * \prod_{i=2}^{tries} \left( \frac{NM - i + 2}{V - i + 1} \right) \right] \right) \quad (2.5)$$

where,  $ET$  is the expected number of tries,  $AM$  is the average number of the vulnerabilities for which an exploit can be found or created by the attacker given their skill level,  $NM$  is the number of vulnerabilities that this skill level of attacker will not be able to use ( $V - AM$ ).

Byres et al. followed Major's work and applied Markov model to estimate the system mean time to compromise (MTTC) [91].

This search theory will be applied in our research represented in chapter 5, which introduces a security threat model named the exist-escape security threat model. The model is composed of two phases including existing threat and escaping threat. We will use search theory to compute the probability of existing security threat when considering existed threat as the match of capability of attackers and the security vulnerabilities of the system. Then search theory also is used to calculate the probability of security threat materialised into attacks once considering attacker escaping the detection of defenders/controllers.

### 2.5.3 Concept of Inclusion-Exclusion Principle

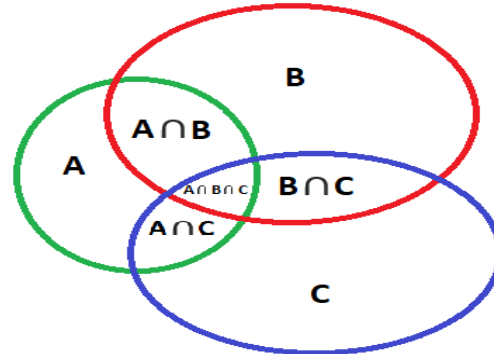
In combinatory (combinatorial mathematics), the inclusion–exclusion principle [92] is a counting technique which generalises the familiar method of obtaining the number of elements in the union of two finite sets; symbolically expressed as

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (2.4)$$

where, A and B are two finite sets and  $|S|$  indicates the cardinality of a set S (which may be considered as the number of elements of the set, if the set is finite). The formula expresses the fact that the sum of the sizes of the two sets may be too large since some elements may be counted twice. The double-counted elements are those in the intersection of the two sets and the count is corrected by subtracting the size of the intersection.

The principle is more clearly seen in the case of three sets, which for the sets A, B and C is given by

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \quad (2.5)$$



**Figure 0.3** Inclusion–exclusion illustrated by a Venn diagram for three sets

This formula can be verified by counting how many times each region in the Venn diagram figure is included in the right-hand side of the formula. In this case, when removing the contributions of over-counted elements, the number of elements in the mutual intersection of the three sets has been subtracted too often, so must be added back in to get the correct total.

The results of these examples give the principle of inclusion–exclusion.

To find the cardinality of the union of n sets:

1. Include the cardinalities of the sets.

2. Exclude the cardinalities of the pairwise intersections.
3. Include the cardinalities of the triple-wise intersections.
4. Exclude the cardinalities of the quadruple-wise intersections.
5. Include the cardinalities of the quintuple-wise intersections.
6. Continue, until the cardinality of the n-tuple-wise intersection is included (if n is odd) or excluded (n even).

In general, inclusion-exclusion principle is expressed in the following way.

Let  $U$  be a set of objects or can be called the universal set of objects, and let  $T(u_1), T(u_2), \dots, T(u_n)$  be subset of  $U$ . In other words, for  $1 \leq i \leq n$ , let  $T(u_i) \in U$  contain those objects that possess properties  $u_i$ . Let  $T(u_{i_1}, u_{i_2}, \dots, u_{i_k})$  be the set of objects that possess each of the properties  $u_{i_1}, u_{i_2}, \dots, u_{i_k}$ , defined as

$$T(u_{i_1}, u_{i_2}, \dots, u_{i_k}) = \bigcap_{i \in (i_1, i_2, \dots, i_k)} T(u_i) \quad (2.6)$$

Consider determining the number of objects  $U(0)$  that do not possess any of the properties  $u_i, 1 \leq i \leq n$ , which is given as

$$U(0) = |U| - \left| \bigcup_{1 \leq i \leq n} T(u_i) \right| \quad (2.7)$$

The inclusion-exclusion principle is effective when we have a set of properties for which set intersection is directly calculated. Finally, we have:

$$U(0) = |U| - \sum_{1 \leq i_1 \leq n} |T(u_{i_1})| + \dots + (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} |T(u_{i_1}, \dots, u_{i_k})| + \dots + (-1)^n |T(u_1, u_2, \dots, u_n)|$$

In [93], Andrea et al. investigated new challenges in network reliability. With the appearance of networks of giant dimensions such as Internet, the exhaustive searching techniques are no longer appropriate. This work used inclusion-exclusion principle as one of the useful techniques to compute the probability that two specific nodes (a source node and a destination node) are connected given the probability of the elements of the network (nodes, edges or both) of being up and down.

In [94], Luke et al. applied the Inclusion-Exclusion Principle to Cryptography application. The advantages of the inclusion-exclusion principle will be used by solving 8 problems of interest to cryptography. The problems concentrated on the enumeration of Boolean functions and permutations that have properties which are considered to be necessary for a cryptographic mapping to be secure.

One of the significant problems in this study is solved by inclusion-exclusion principle is that determination of distribution of blanks in a random text

The problem is expressed as follows. Given an alphabet  $A = \{a_1, a_2, \dots, a_n\}$ , let  $W$  be a random word of length  $N$  over the alphabet  $A$ . The character  $a_i \in A$  is said to be a blank in  $W$  if  $a_i$  does not appear in  $W$ . Consider determining the probability  $Pr(N, n, b)$  that  $W$  will have exactly  $b$  blanks, assuming that each  $N$  character word is equally likely to be selected. With these probabilities, for example, we can then determine if the ciphertext produced by an encryption function is behaving in a random manner with respect to the distribution of blanks.

The solution is expressed as follows. First, consider determining the probability that a word  $W$  contains no blanks. Let  $U$  be the set of all words over  $A$  of length  $N$ , and let  $T(a_i) \in U$  be the set of words that do not contains the character  $a_i, 1 \leq i \leq n$ . It follows that the inclusion-exclusion principle coefficients are symmetric and  $|T(k)| = |T(a_1, a_2, \dots, a_k)| = (n - k)^N, 1 \leq k \leq n$ . Then using inclusion-exclusion principle we have that

$$\begin{aligned}
 Pr(W \text{ has no blanks}) &= 1 - Pr(W \text{ has at least 1 blank}) \\
 &= 1 + \sum_{i=1}^n (-1)^i * \binom{n}{i} * \frac{|P(i)|}{n^N} \\
 &= \sum_{i=1}^n (-1)^i * \binom{n}{i} * \left(1 - \frac{i}{n}\right)^N \tag{2.8}
 \end{aligned}$$

Therefore, we now determine the distribution of blanks

$$Pr(N, n, b) = \binom{n}{b} \sum_{i=0}^{n-b} (-1)^i * \binom{n-b}{i} * \left(1 - \frac{b+i}{n}\right)^N \tag{2.9}$$

Proof: without loss of generality let the  $b$  characters  $a_1, a_2, \dots, a_b$  be blanks in  $W$ . equivalently,  $W$  has no blanks over the alphabet  $B = A - \{a_1, a_2, \dots, a_b\}$ . Therefore, we have:

$$\begin{aligned} \Pr(N, n, b) &= \binom{n}{b} \frac{(n-b)^N}{n^N} * \Pr(W \text{ has no blanks over alphabet } B) \\ &= \binom{n}{b} \sum_{i=0}^{n-b} (-1)^i * \binom{n-b}{i} * \left(1 - \frac{b+i}{n}\right)^N \end{aligned} \quad (2.10)$$

In chapter 4, we seek to find the probability of the union of security threats. In Chapter 6, we focus on quantifying the skill of attackers and controllers. The problem we face is to determine if a group of attackers at a given level of skill is able to exploit a known set of a system's vulnerabilities, and if the system controllers with a given level of capability is able to mitigate the known set of system's vulnerabilities. In Chapter 4 and Chapter 6, we model the relevant security scenarios, formulate the problems, and deploy and extend this inclusion-exclusion principle to find the required solutions.

## 2.6 Summary

In this chapter, we first refined and re-defined the concepts of cyber space and cyber security. We then gave an introduction to the background of Capability Maturity Models applying in cyber security. Subsequently, the fundamentals of cloud computing were provided along with the background of cloud security models and standards. Then we focused on reviewing the concepts of security metrics and measures. Security metrics related to security threats were investigated comprehensively to identify the research limitations that provide the motivation for our proposed solutions to research problems in this thesis. Finally, we introduced three mathematical backgrounds including Markov model, search theory, and inclusive-exclusive principle. These mathematical fundamentals provide support to computing the probability of a security threat materialised into attacks in our three proposed security threat models that will be introduced critically in chapter 4, 5, and 6.



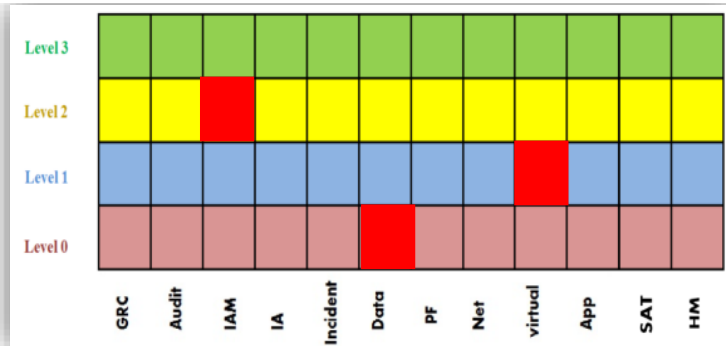
# Chapter 3

## A Novel Capability Maturity Model and a Metric Framework for Cloud Security

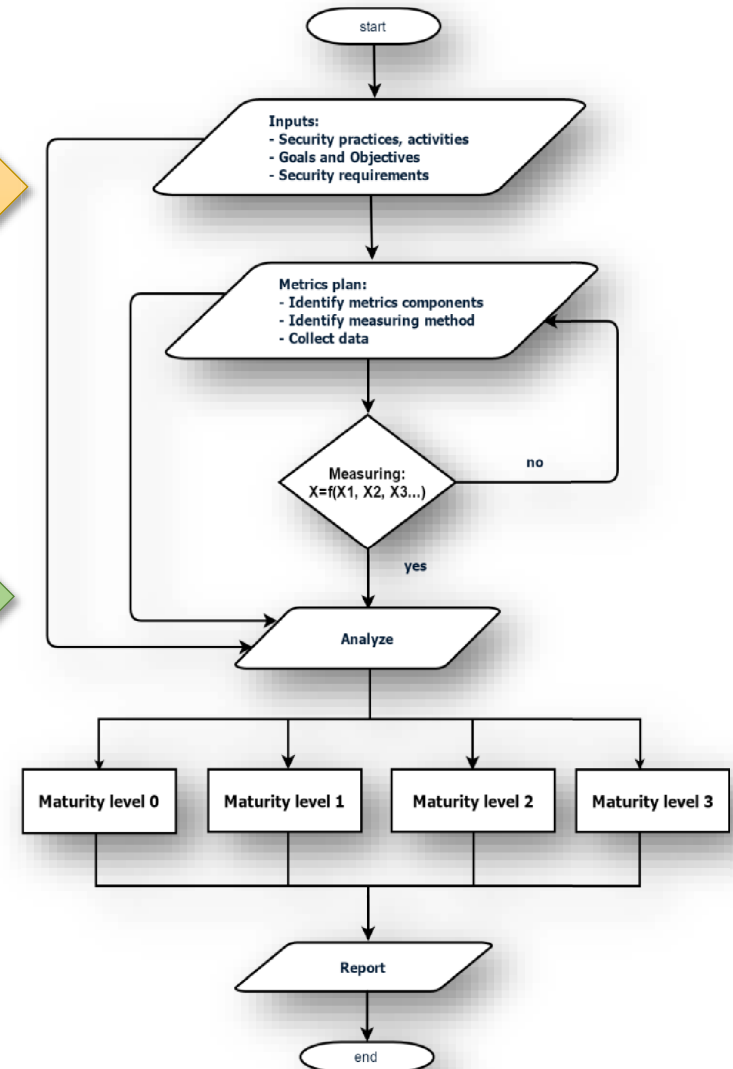
Before giving the introduction of this chapter, we would like to visualise an overview of our proposed research solutions through Chapters. From Chapter 2, we investigated the background of cyber space, cyber security, cloud security models, capability maturity models, and security metrics and measures. We indicated the research problems that our proposed research solutions address. **Figure 3.1** shows a general picture of three major phases of the thesis. First, we propose Cloud Security Capability Maturity Model (CSCMM) with twelve security domains and four maturity security levels (Paper 1 and Paper 3). Additionally, a security metric framework will also be created to choose appropriate security metrics to assess the security level of CSCMM. This content will be expressed in Chapter 3. Second, we propose three security threat models, which are Markov (Paper 2 and Paper 4), Exist-Escape (Paper 5), and Inclusion-Exclusion (Paper 6), supporting the computing of the probability of a security threat materialised into attacks. These three models will be described in Chapter 4, 5, and 6 respectively. Third, we propose a novel security metric named Mean Security Remediation Cost (MSRC) that uses the simulation results from the three threat models above to validate and evaluate CSCMM via the security metric framework (Paper 5 and Paper 6). The metric and simulation of this metric will be expressed in chapter 7 and chapter 8.

Figure 0.1 Overview of research solutions via Chapters

### Cloud Security Capability Maturity Model [1]



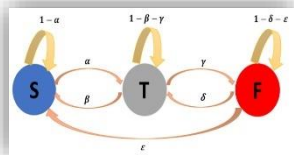
### Security Metrics Framework [1]



### Mean Security Remediation Cost metric [5]

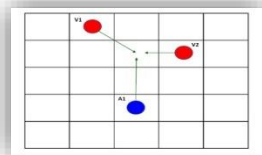
$$MSRC_{il} = \sum_{j \in T_l} ST_{ik} * CT_{kj} * PT_j$$

#### Markov and CVSS [2]



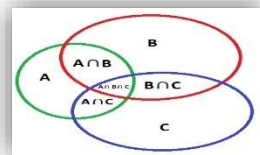
[1] Chapter 3 (Paper 1 and 3)  
[2] Chapter 4 (Paper 2 and 4)

#### Exist-Escape model [3]



[3] Chapter 5 (Paper 5)  
[4] Chapter 6 (Paper 6)

#### Inclusion-Exclusion [4]



[5] Chapter 7 and 8 (Paper 5 and 6)

### 3.1 Introduction

Nowadays, almost all IT systems are based on cloud computing from critical infrastructure, e-banking, e-government, to Internet of Things. However, we are also aware that a huge amount of data from cloud is spied upon each day, thousands of credit cards information is leaked every hour. There exist several cloud security models and standards dealing with emerging cloud security threats. However, these models are mostly reactive rather than proactive and they do not provide adequate measures to assess the overall security status of a cloud system. Capability Maturity Models (CMM), which have been used in quality management of areas like education, health, industrial systems, offer a realistic approach to address these problems using management by security domains and security assessment on maturity levels. From 2000, there are about twenty CMM models that have been developed to be applied for cyber security in different areas. However, to our best knowledge, CMM models have not been applied for securing cloud computing. This motivates us to investigate and propose a new CMM to apply for security cloud computing. This chapter proposes a Cloud Security Capability Maturity Model (CSCMM) that extends existing cyber security models. The model is structured with two dimensions. The horizontal dimension presents security domains. The vertical dimension describes security maturity levels. To choose appropriate security metrics to assess the maturity security levels, we create a security metric framework. It is designed as a diagram which is composed of three phases including choose, measure, and analyse. Finally, the selection of quantitative metrics applying for CSCMM will be proposed.

The remainder of this chapter is organised as follows. Section 3.1 gives the introduction of the chapter. Section 3.2 describes maturity models as they are applied in cyber security. Section 3.3 proposes a Cloud Security Capability Maturity Model (CSCMM). Section 3.4 presents the design of a security metric framework. Section 3.5 describes the quantitative metrics that can be applied for CSCMM. Finally, section 3.6 summarises the chapter.

### 3.2 Maturity Models Applied in Cyber Security

To consolidate our understanding of maturity models and how they are applied in cyber security, we compare a dozen cyber security maturity models. **Table 3.1** shows the features of these models.

In order to discuss the strengths and weaknesses of an existing model, we identify the similarities and differences among these models as follows.

*Similarities:*

- Type of maturity model: all models are hybrid maturity models with their multi dimensions including security domains and maturity levels.
- Security domains: basically, most security domains range from infrastructures, data, networks, to human, application, communications, compliance, legal and contractual.
- Maturity levels: most models use a 5-level framework to assess security state of each domain. These 5 levels can be seen as a 3-stage process. The first stage is the beginning with no security management, policy. The second stage focuses on implementing security standards to be able to control security issues. The last stage is an automatic security management with full security implementation. This stage is considered the resilient stage or highest security.
- International security standards: to implement best security practices, security standards such as NIST, ISO 27000 series, COBIT are applied to perform and measure security levels in all cyber security maturity models.
- Process: most models have an implementation process through 4 steps from evaluation, gap identification, priority and plan, and plan implementation.

*Differences:*

- Each model has different goals and advantages, with Information Security Framework, IBM wants to fill the gap between business and technical element, while DOE is interested in implementation and management in C2M2. CCSMM model tends to deal with community and sharing problems.
- Security domains: each model has several different specific domains with different security requirements because of the goals of the model. For example, DOE's C2M2 focuses on Event and Incident Response Continuity of Operations domain or Identity and Access management domain because the national critical infrastructure requires attention in incident response and authentication aspects of security.
- While almost models use 2 dimensions, model including domains and levels, CCSMM model has 3 dimensions by adding the community (organisation, community, state) dimension. This makes the model more suitable for organisations of different sizes; however, the model is complex as it incorporates many standards and implementing practices.

**Table 0.1** Synthesising and Analysing Cyber Security Maturity Models

	Cyber Security Maturity Models (CSM2)	Organisations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information Security Evaluation Maturity Model (ISEM), 2000	City Group	Security awareness and evaluation	Complacency	Acknowledgement	Integration	Common practice	Continuous improvement
2	Systems Security Engineering Capability Maturity Model (SSE-CMM), 2001	The US National Security Agency (NSA)	Evaluation of software security engineering processes	Performed informally	Plan and track	Well defined	Control	Continuous improvements
3	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimised
4	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimised
5	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
6	Gartner's Information Security Awareness Maturity Model (GISMM), 2009	Gartner	Security awareness, and risk management in large international organisations	Blissful ignorance	Awareness	Corrective	Operations excellence	
7	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
8	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
9	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
10	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimised		
11	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
12	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

Cyber security maturity models have shown that they help managers to better manage security of their organisations [95, 96]. They allow better security risk management, produce cost saving, promote self-improvement, and support good security procedures and processes. Critically, they encourage all stakeholders to take steps along a secure mature path as mapped out by the maturity model, rather than activating security controls blindly without regard to the security of the overall organisation. Despite all these benefits, maturity models only provide a bare minimum compliance model rather than an aspired cyber security model that can deal with emerging cyber environment, its demanding usage, as well as its sophisticated attacks. Therefore, three specific issues from security maturity models should be addressed: First, identifying the maturity levels of cyber security of each domain is arbitrary and subjective as a result of checking for compliances; a security model should be more than compliant. Second, most cyber security maturity models draw on International cyber security standards such as ISO27000 series or NIST. Security practices in these standards are mainly measured by qualitative metrics/processes; quantitative metrics should be essential for any security assessment. Third, the model should be flexible for addressing a specific dimension of a cyber space or extensible for dealing with emerging cyber spaces.

### **3.3 Cloud Security Capability Maturity Model (CSCMM)**

To solve all the above problems from cloud models and cyber security maturity models, we developed a Cloud Security Capability Maturity Model (CSCMM) with two dimensions including “domain” and “maturity level” (**Figure 3.2**). The first dimension presents twelve cloud security domains. Each domain is a set of cyber security practices. The practices within each domain are a number objectives achievement that are specified for cloud security. The second dimension shows four maturity levels which apply separately to each domain. The maturity levels indicate a parallel progression of maturity: general and specific.

The model is built from a combination of existing cyber security standards, frameworks, and innovations. It provides the guidance to support the organisations to implement and enhance their cyber security capabilities on cloud system. The model tends to be in general, therefore it can be tailored for its consistent goals with different cloud service model (IPSaaS) and deployments (Public, Private, and Hybrid Cloud).

### 3.3.1 CSCMM Domains


There is not a complete cloud security standard because cloud technology is evolving far faster than standards [97]. Therefore, creating a set of security domains just based on the current security standards is not adequate to take into account emerging issues and attack surfaces. For CSCMM, we choose a systematic review approach on existing cloud security models and standards, traditional security maturity models as well as trends in emerging technologies. Systematic review methodology is a means of evaluating and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest [98]. As a result, we investigated fourteen security models including five traditional and nine cloud security models. We found twelve in twenty one security domains that are suitable for cloud security (see **Table 3.2**).

The CSCMM model is composed of twelve security domains for several reasons as follows. First, they cover comprehensive aspects of cyber security based on different perspectives such as ISO (strategic, tactical, and operational), CSA (governance, operational), IBM (Process, Technical, and Operational). Second, they inherit eight security domains from traditional maturity models and standards including infrastructure and facilities security; identity and access management; governance, risk, and compliance; incident response and threat management; data and information protection; human resources management; security awareness and training; audit and accountability. The four remaining domains are cloud specifications such as cloud connections and communication; operability and portability; virtualisation; and application security. Third, several security domains from different models are integrated once the objectives of these domains are similar. Some others domains may be separated by important objectives within those domains. This is expressed comprehensively in specifying each cloud security domains below.

***These 12 domains are described below:***

1. Infrastructure and facilities security (IF): The security of an IT system also depends on the security of its physical infrastructure and facilities. In the case of cloud computing, this extends to the infrastructure and facilities of the cloud service provider. The customer must get assurance from the provider that appropriate security controls are in place. ISO 27007 can be used to ensure protection against external and environmental threats like-

	IF	IAM	GRC	IR	DIP	HM	APP	AT	AA	IP	VI	CCC
Level 3												
Level 2												
Level 1												
Level 0												

- 
- Security domain: Incident Response; Maturity level: 2
  - Description: establishing plans and programs to detect, analyze, and respond security incidents; Cloud security stakeholders are identified and involved; intrusion detection and prevention are applied

**Figure 0.2** CSCMM Model Architecture



-fire, floods, earthquakes, civil unrest or other potential threats that could disrupt cloud services; control of personnel working in secure areas; equipment security controls; and supporting utilities such as electricity supply, gas supply, telecommunications.

2. Identities and Access Management (IAM): This domain ensures authentication, authorisation, and administration of identities. The main concerns of this domain are related to identity verification, granting a correct level of access to cloud resources, policy managements, and role-based access controls. The purpose of IAM is to prevent unauthorised access to physical and virtual resources as this can threaten the confidentiality, availability, integrity, and other properties of users services and data. These domains can be applied by standards or technologies such as LDAP (Lightweight directory Access Protocol) to provide access to directory servers and SAML 2.0 (Security Authorisation Mark-up Language) for exchange of authentication and authorisation data between security domains.

3. Governance, Risk, and Compliance management (GRC): This domain focuses on establishing, operating, and maintaining cyber security risk management programs that identify, analyse, and mitigate cyber security risk to the organisation. This means governance and compliance policies and procedures are established to protect stakeholders property. This covers implementations of compliance following regulatory requirements between stakeholders. Compliance management is to maintain and provide compliance. It relates to execution of internal security policies, and different compliance requirements such as regulatory, legislative.

4. Incident response (IR): This domain concentrates on incident detection, response, notification, and remediation. The major concerns in incident response are related to establishing and maintaining plans, procedures, and technologies to detect, analyse, and respond to cyber security incidents and events. The incident response lifecycle as expressed in the National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST 800-61) should be used in this domain.

**Table 0.2** The appearance of security domains in security models

ID	Domains/Models	CSA	CSCC	ENISA	IBM	Cisco	ISIMC	FedRAMP	PCIDSS	SANS	SSE-CMM	ES-CMM	RMM	ISO	NIST-CSF	Number
1	Infrastructure and facilities security (IF)	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	13
2	Identity and access management (IAM)	✓	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓	11
3	Governance, Risk, and Compliance (GRC)	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	11
4	Incident response (IR)	✓		✓			✓	✓	✓	✓		✓	✓		✓	9
5	Data Information Protection (DIP)	✓	✓	✓	✓	✓			✓	✓					✓	8
6	Human resources management (HM)		✓	✓	✓	✓		✓				✓		✓		7
7	Application security (APP)	✓	✓	✓	✓	✓	✓				✓					7
8	Security awareness and training (AT)			✓			✓	✓			✓		✓		✓	6
9	Audit and accountability (AA)	✓					✓	✓			✓	✓				5
10	Interoperability Portability (IP)	✓		✓			✓									3
11	Virtualisation and Isolation (VI)	✓				✓	✓									3
12	Cloud Connections and Communications (CCC)		✓	✓	✓											3

5. Data and Information protection (DIP): Data protection is one of the critical security challenges in cloud computing. Control of data and compensating controls can be used to tackle the loss of physical control when moving data to the cloud. The concern of information management is who has onus for data confidentiality, integrity, and availability. Therefore, security controls as expressed in ISO 27002 including asset management, access control and cryptography can be applied. Other technologies such as HTTPS for regular connections from cloud services over the internet, VPN using IPSec or SSL for connections also can be used for implementing this domain. Moreover, encryption keys should be used by KMIP (the Key Management Interoperability Protocol) that supports a standardised way to manage encryption keys.

6. Human resource management (HM): People are often described as the weakest entity in any security system. This domain focuses on human resource process, from pre-employment, during employment, and through termination, to ensure that policies and procedures are in place to address security issues. The three areas of human resources security concerned are prior to employment; during employment; termination and change of employment. Human Resources Security in ISO 27002:2013 (Information Security Management) can be used for this domain.

7. Cloud application security (APP): This domain focuses on determining the application software on which type of cloud platform (SaaS, PaaS, or IaaS) for securing. The Open Web Application Security Project (OWASP) or Secure Software Development Life Cycle (SSDLC) can support cloud service entities to secure application running on cloud systems. In terms of technologies and techniques in cloud application security, firewall can be used to control access. VPNs can be considered to limit access to application to users for these domains.

8. Security awareness and training (AT): This domain aims to create a culture of security and ensure the ongoing suitability and competence of all personnel. Consistent training throughout the entire process ensures that employees and contractors are fully aware of their roles and responsibilities and understand the criticality of their actions in protecting and securing both information and facilities.

9. Audit and Accountability (AA): This domain aims to provide information about roles, responsibilities, and compliance regarding auditing. It addresses auditing of security controls including checking for proper server maintenance and controls to make

sure that it is properly done and security policies are being enforced. The policy may set the level and detail of auditing and specify types of events to be audited. The major procedures of this domain are auditable events; content of audit records, audit processing and monitoring; audit reduction and report generation; protection of audit information; and audit retention.

10. Interoperability and portability (IP): This domain is one of the special domains in cloud computing. It is the ability to move data/services from one provider to another, or bring it entirely back in-house. To ensure this domain, we can use open virtualisation formats to provide interoperability, while virtualisation can help to remove concerns about physical hardware, distinct differences exist between common hypervisors. It deals with different technologies virtual machine images are captured and ported to new cloud providers such as Distributed Management Task Force (DMTF) and Open Virtualisation format (OVF).

11. Virtualisation and isolation (VI): This domain focuses on the security issues related to system/hardware virtualisation, rather than a more general survey of all forms of virtualisation. This domain is associated with multi-tenancy, VM isolation, VM co-resident, hypervisor vulnerabilities, and other virtualised artefacts. Isolation is the technique used to protect each entity within the cloud infrastructure component of a system from unwanted interferences. Isolation is used to identify virtual and physical boundaries, partition containers, processes or logical functional entities, and isolate policy-based security violations.

12. Cloud connection and communication security (CCC): A cloud service provider must allow legitimate network traffic and block malicious network traffic. However, unlike many other organisations, a cloud service provider may not necessarily know what network traffic its customers plan to send and receive. Nevertheless, customers should expect certain external network perimeter safety measures from their cloud providers. For this domain, ISO/IEC 2703332 standards can be used to provide detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002.

In these twelve domains, we integrate isolation into virtualisation domain to generate a new domain namely virtualisation and isolation and offer domain interoperability portability as a new domain. It is clear that virtualisation and isolation have been important techniques in cloud security. Virtualisation is considered as the cloud enabling

technology and hence it is at the centre of cloud security. However, with emerging attacks recently on the virtualisation layer, this domain has to be taken seriously. Isolation technique has been emerging as a new approach for securing cloud computing. The development of isolation theory with assessing process is necessary. Clearly, a security model cannot exist in a long term. It can be changed by adding or removing the security domains. For example, with the emerging of 5G, industry 4.0, and data science, additional domains may have to be accommodated; the problem is then how to distill the new cloud specific concerns and identify traditional security issues from the new technologies.

### 3.3.2 Security Maturity Levels

To investigate the common features of each maturity level in previous security maturity models, we compared ten prominent professional security maturity models (**Table 3.3**).

Basically, there is no standard for dividing the number of security maturity levels. If a model has less levels like two or three levels, it is difficult to quantify the quality of each level. If a model has so many levels like six or seven, it is hard to manage and classify among levels. Normally, the number of security levels is four or five (as seen in **Table 3.3**). Or the definition of each level is different among models. This depends on the specifications of each model or the area the mode is built for. For example, compared between model ISO (model 1) and model ISM3 (model 2), both have five levels. But they have different purposes. Model 1 is used for risk management, whereas, model 2 is applied for preventing or mitigating incident. In model 2, the identification of security incident is important. Therefore, they name level 1 is undefined for meaning that the model has no plan to check or test security processes. In model 1, level 1 is named “performed”. This means the concepts of incidents are defined. At this level, it is assessed how well the process is performed.

As a result of this investigation, **we propose a compact CSCMM model that covers all important domains of a cloud system with four security maturity levels (SMLs) that provide a solid differentiation of cloud security levels.** Maturity levels are identified by the following attributes: (1) the SMLs apply independently to each domain. For instance, an organisation could be implementing at SML1 in one domain, and at SML2 in another domain; (2) the maturity level of a domain is determined by the minimum of all security practices within this domain. For example, to gain security maturity level at SML2 in one

**Table 0.3** Investigating Cyber Security Maturity Models

	Cyber Security Maturity Models	Organisations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimised
2	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimised
3	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
4	Gartner's Information Security Awareness Maturity Model (GISAMM), 2009	Gartner	Security awareness, and risk management in large international organisations	Blissful ignorance	Awareness	Corrective	Operations excellence	
5	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
6	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
7	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
8	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimised		
9	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
10	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

domain, the organisation has to implement all the security practices in both SML1 and SML2; (3) SML achievement should align with business objectives and an organisation's security strategy.

***These are common features that define each maturity level.***

- SML0 (Undefined): at this level, organisations are at the starting point with a commitment to establish a security maturity assessment model. They have no plan to check or test security processes.

- SML1 (Initiated): at this level, most organisations focus on basic security practices. Some basic security physical hardware devices or networks need to be implemented on IaaS, basic protections on virtual machine monitors, the access control and encryption on PaaS, the basic application security and the multi-tenancy on SaaS.

- SML2 (Managed): at this level, organisations focus on building and planning Information Security programs and applying cloud security standards. Cloud security stakeholders such as providers, consumers, and third-parties are identified and involved. Cloud security activities need to be guided by policies. Some cloud automatic security tools are applied such as intrusion detection and prevention systems. Especially, a security metric system needs to be applied at this level to support security decisions making. For IaaS, security mechanisms to protect network and data are applied to achieve selected security standards compliance. For PaaS, it is ensured that the virtual machine monitor needs to be protected by higher security policies. For SaaS, automatic security system for web-based, software, or database needs to be implemented.

- SML3 (Optimised): it is defined as the highest maturity level. This is a real-time protection level. All the security programs support 24/7 staffed operations and are fully automated. It is assured that all security policies and procedures are implemented. This is the ideal cloud security status with the optimal use of resources from facilities, time to costs and human resources. This level is called resilience when the organisation can detect and tackle security threats automatically proactively and the time to achieve resilience status is almost zero. Also, all people in the organisation have adequate skills and knowledge about security on cloud.

In an explicit summary, the CSCMM model has two dimensions. The vertical dimension is composed of twelve security domains. the horizontal dimension is consisted

of four security maturity levels. The CSCMM model is used to assess how good each security domain is. As seen in Figure 3.2, if the security maturity level of security domain IR (Incident Response) is two. This have to have requirements: (1) establish plans and programs to detect, analyse, and respond security incidents; (2) identify cloud security stakeholders; (3) apply intrusion, detection, and prevention systems.

### 3.4 Security Metric Framework

To assess the maturity level of CSCMM model in general and a security domain or a security activity in particular, we propose a security metric framework with the following steps (**Figure 3.3**).

**Inputs:** This first step describes the requirements for the security metric framework: security practices and activities, goals and objectives, security requirements. A set of security practices for a particular domain or multiple domains is defined and/or selected. This depends on the demand of upper management or the schedule of the assessment process of the CSCMM model. These securities then determine “what to measure”. What-to-measure may be one security activity or several security activities from the selected domains. Stakeholders are identified which include upper managers who decide on information requirements, managers who carry out the directives, practitioners who implement the security metrics, and security metrics consumers. Goals and Objectives define the goals and objectives of a security metric plan or program from the stakeholders’ viewpoint.

**Metric plan:** Classification of security activities or practices is also necessary to indicate the type of measurement (governance, management, operational, and technical) and to decide on the metric plan and the method to measure as security metrics should be SMART [55] or PRACMATIC [56]. Security metric components identification identifies the elements or dimensions related to the metrics. These may include real-virtual, infrastructures, and interaction of entities in the (cloud) cyber space, and others factors such as cost, time, threats, and vulnerabilities. Determination of measuring methods is based on the qualitative or quantitative nature of the security practices. Quantitative metrics are usually based on mathematical models and numerical data. The unit of measurement for each component of a security metric program is then derived. Data



collection has to be planned to meet the characteristic requirements such as obtainable, cheap to collect, quantitative express, automatically.

**Measuring:** Relevant and measurable metrics have already determined and selected from previous steps, this step carries out the actual measurement according to the measuring method and the data collection plan. In general, a security metric is a function of its measured components:

$$x = f(x_1, x_2, x_3 \dots) \quad x_1, x_2, x_3 \text{ are security metric components}$$

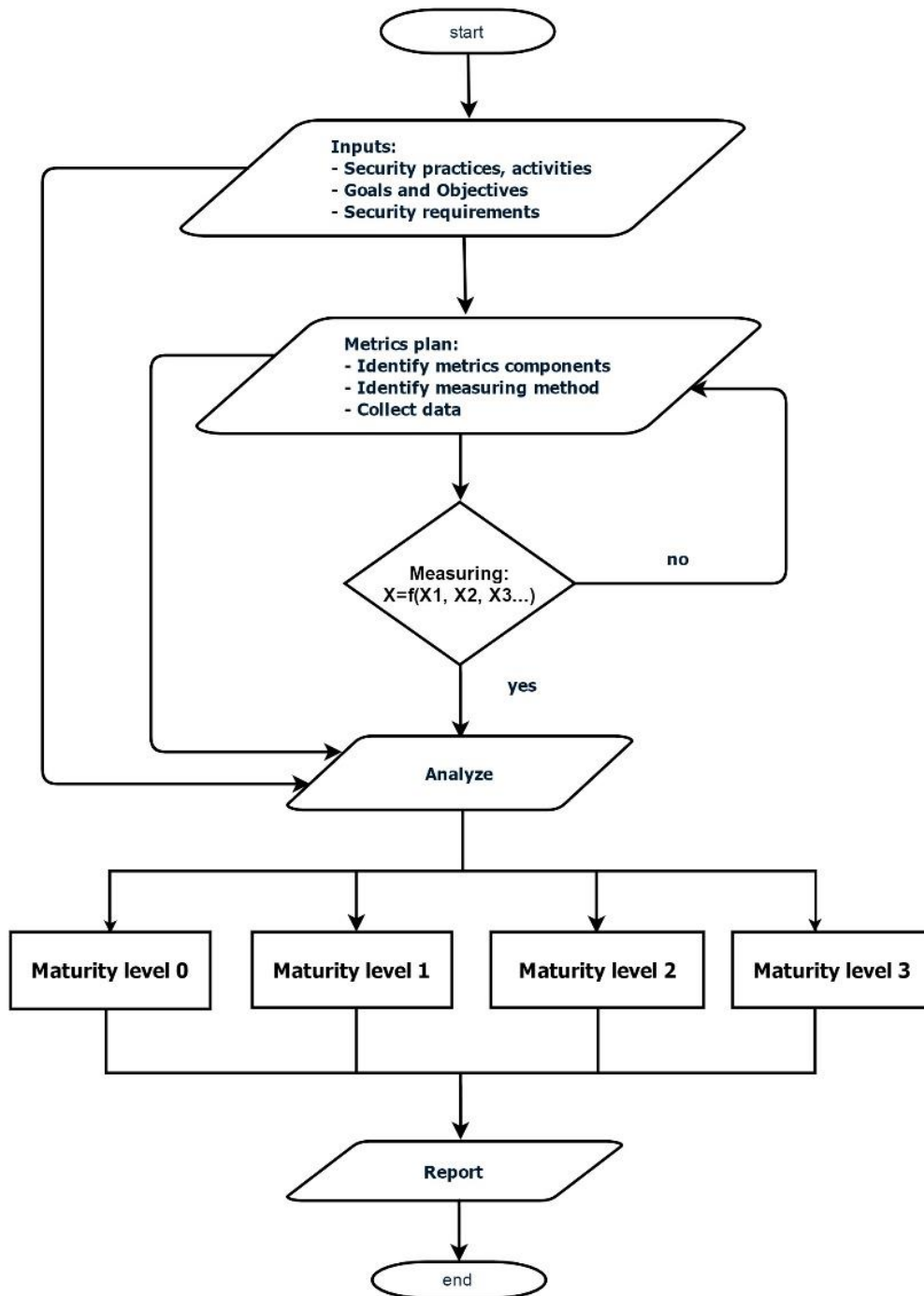
x could be a countable value based on a maturity benchmarking (next step). f is a function of the specification of security metrics identified in the metric plan. If x does not yield a value or it is impossible to implement the measurement one has to go back to the metric plan step to design the set security components and their impacts.

**Analyse:** This step consists of several operations such as the holistic analysis, interpretation, and consolidation. Holistic analysis means that the analysis takes into account not only the measured metrics but also the elements of the inputs and the metric plan steps of the metric framework. This is important as some quantitative metrics lose their original meanings when reduced to a pure numerical number. Interpretation of the obtained metric is to decipher the true security status of the cyber space under protection. Interpretation also provides the reasons and their impact on the measured result. The effectiveness and efficiency of the proposed metric should be evaluated.

**Maturity level determination:** Benchmarking is the process of comparing one's own performance and practices against peers within the industry or noted 'best practice' organisations outside the industry. Benchmarks can be used, for example, to determine a "minimum essential configuration" for workstations, servers, laptops, routers, firewalls, and other network devices or for the holistic system. The method for assigning maturity level depends on the specification of the security metrics. It could be assigned as a percentage range from Level 0 (say, 0-25%) to Level 4 (say, 75-100%); a weighted value; a value interval, or times to security incident response from months (level 0), days (level 1), hours (level 2), to real-time (level 3) [99].

**Report:** The last step informs the ultimate impacts and consequences to metric consumers. All steps of the metric need to be described. The frequency of reports depends on requirement of the organisation and the upper managers. On the one hand, the report provides the assessed security status of the cloud system and explains clearly the impact

of the security status to the management on the organisation business plan and direction. On the other hand, to the security experts and practitioners, the report identifies security weaknesses and suggests action plans for remedy and provides a roadmap for strengthening the security of the system.



**Figure 0.3** CSCMM metric framework diagram

### **3.5 The Selection of Advanced Security Quantitative Metrics**

With the proposed security metric framework, the overall security assessment can be balanced and complemented between existing qualitative assessment for senior managers of an organisation and quantitative assessment for its security experts. In terms of the qualitative assessment, capability maturity model theory provides senior managers with a sound picture of the security compliance of their system in terms of practices but it does not relate well the impact of the security assessment to their business plan and direction. In terms of quantitative assessment, advanced security metrics allow mappings between the outcome of security assessment and costs/benefits to the organisation. Furthermore, good quantitative security metrics allow the identification of a specific domain or an individual practice of the model and suggest appropriate security measures for achieving a higher level of maturity.

Among many quantitative security metrics, Mean Failure Cost (MFC) metric [55] is an excellent candidate metric for CSCMM. MFC is the predictive quantitative metric that quantifies the costs each (among many) stakeholder needs to invest to the mission for better security or the benefits the stakeholder stands to lose due to the lack of security. MFC is considered as an advanced security metric for a number of reasons. First, it includes the stakeholders, the impact of security properties on stakeholders, and the threats that can affect the system. Second, it can embrace traditional metrics such as Mean Time To Failure (MTTF), Mean Time To Explore (MTTE), and Mean Time Between Breaches (MTBB). Third, it meets many essential security metrics requirements such as SMART or PRAGMATIC.

In addition, the assessment process in the CSCMM model can deploy other state-of-the-art quantitative metrics including check-list based; state-based stochastic, Fuzzy Analytic Hierarchy, Attack graph based, Dynamic Bayesian Network (DBN) based, Tree weighting. For check-list based metrics, it proposes an advanced security measurement system that reflects the characteristics of each field (critical infrastructure facilities) to achieve effective information security management [100]. State-based stochastic metrics focus on the progression of an attack process over time. This applies for 4 types of significant attacks: Buffer Overflow, Man-in-the-middle, SQL injection, and Traffic Sniffing [71]. Microaggregation is the technique to protect cloud data through anonymity

in order to prevent exposure of person's identity [101]. Fuzzy Analytic Hierarchy presents a quantitative framework based on Fuzzy Analytic Hierarchy Process (FAHP) to quantify the security performance of an information system [102]. Attack graphs based AGB provides a method for quantitatively analyzing the security of a network using attack graphs that are populated with known vulnerabilities and likelihoods of exploitation and then exercised to obtain a metric of the overall security and risk of the network [103]. Dynamic Bayesian Network (DBN) based model is used to capture the dynamic nature of vulnerabilities that change over time. An attack graph is converted to a DBN by applying conditional probabilities to the nodes, calculated from the Common Vulnerabilities Scoring System [104]. Formal methods are being used for verification of cloud computing systems including verification of security in partitioned cloud, firewall, and big data [105]. Tree weighting proposes an initial framework for estimating the security strength of a system by decomposing the system into its security sensitive components and assigning security scores to each component [106].

We believe that a more meaningful security metric in terms of a realistic depiction of the scenario, is the probability that a threat really exists and its chance to materialise into an attack. Whether a threat exists or not depends on two main factors: the existence of system vulnerabilities and the existence of attackers who have the ability to exploit those vulnerabilities. On the other hand, the system's security management (security managers, experts) will exercise security measures to protect the system and thus preventing the possible attacks.

Clearly, a threat that exists (according to our definition earlier) will materialise depending on the capability of the system security manager and security measures. A successful attack is when an attacker exploits (or acts on) an existing vulnerability of a system to perpetrate a malfunction of the system in terms of confidentiality, integrity, and availability and causes damages. The question is when an attack is considered to exist and when it results in a successful attack.

Hence, identification of the existence of a potential attack and the chance this potential attack materialises is essential for security risks management. As a consequence, we pose two research questions: (1) how to compute the probability of the existence of a threat that has the potential to cause harm; and (2) how to calculate the probability that the threat materialises into an attack under certain control measures. These research questions will be

dealt with in chapter 4, 5, and 6 which propose three threat models to compute the probability of security threat materialised into attacks.

### **3.6 Summary**

This chapter proposed a Cloud Security Capability Maturity Model that includes cloud-specific security domains and provides the assessment of the overall security of the cloud under consideration. To provide for the measurement of security maturity levels, the security metric framework was introduced. This framework includes relevant quantitative metrics for a measurable assessment. It presented the balanced assessment of the overall security of an organisation/system qualitatively and quantitatively. For senior managers, CSCMM offers the meaningful security assessment of the security status of their infrastructure for making decisions concerning their business plan and direction. For security experts or practitioners, CSCMM with its quantitative metrics enables proactive measures and responsive actions. The chapter also suggested future research with advanced metrics that involve various stakeholders, components of cloud security systems.

# **Chapter 4**

## **A Threat Computation Model Using a Markov Chain and Common Vulnerability Scoring System and Its Application to Cloud Security**

### **4.1 Introduction**

This Chapter will describe the first security threat model that uses a Markov chain and Common Vulnerability Scoring System (CVSS) to quantify the probability of security threats (successful attacks) being materialised. This introduction section will describe our research motivation as to why quantifying the probability of realised security threat is critical, especially in supporting measures of the security levels of a cyber system. This section also gives the major research contributions of the chapter and the organisation of the chapter.

As cyber infrastructures and their interconnection are increasingly exposed to attackers while accommodating a massive number of IOT devices and provisioning numerous sophisticated emerging applications [107, 108], security incidences occur more often with severe financial damages and disruption to essential services. Securing cyber systems thus becomes more critical than ever. A simplistic approach to addressing this problem would be to prevent security breaches directly or fix them if they are unavoidable. The approach appears simple and straightforward; however, the achieved solutions are far from

satisfactory for several reasons. We have not developed effective predictive tools to anticipate what and where to launch preventive security actions. We may have developed a whole range of tools to deal with security breaches, but this constitutes only temporary and reactive solutions and we are still in the dark, not knowing what will come next!

We suggest a realistic and concrete approach: the goal is to determine the probability of a security threat materialised into an attack (a security breach) on a system, the cost consequences (what it hurts), and the distribution of the costs over the system's constituents or stakeholders (where it hurts) when the threat materialises. Knowing the probability that a threat materialised into an attack we are able to predict the chance that it will occur and take appropriate measures to reduce or prevent its occurrence. Knowing the consequences, we can make appropriate judgments whether the damages caused by the attack are significant enough to warrant a security response or if it can be written off as one of the components of the operational costs. Knowing "where it hurts" allows us to use our security knowledge and tools to respond appropriately to the security attack. Clearly, the central issues are the probability of a threat materialised and the distribution of its consequences. In this chapter, we only address the problem of determining the probability of a threat materialised into an attack.

The above discussion implies the need for a set of relevant security metrics that allows us to deal with security issues proactively and to set appropriate security goals for our systems and determine the performance of any solution for protecting the systems (both preventing potential incidences and tackling incidences head on). To ascertain the security of a system, it is necessary to develop meaningful metrics to measure appropriately the system's security level or status. Lord Kelvin stated that "when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind" [13]. To measure the security of a cyber space, standards organisations and researchers have proposed many security metrics. The Centre for Internet Security (CIS) published a number of security metrics in management, operation, and technique [15]. The National Institute of Standards and Technology (NIST) has developed security metrics in implementation, effectiveness, and impact [64] Other metrics have been proposed for risk assessment and network security evaluation [109, 110].

Recently, several security metrics related to the computation of the probability of security threats have been developed. In [70], seven types of model-based metrics, which are created by integrating mathematical models and empirical measurements, are also used to calculate the probability of a security threat. In [71], the study used a semi-Markov model to investigate the attack process to compute the transition probability between security states. Mean Failure Cost is one of the sound approaches to quantitative security metrics, taking into account various security components like stakeholders, security requirements, and security threats [69]. The probability distribution of security threats is central to this metric, but the computation is based largely on empirical or qualitative data. Several other security metrics relate to successful attacks, but they are specific to a particular type of attack and hence difficult to generalise.

With these considerations, we pose two questions: 1, how to model a security threat that involves three main security components: attackers, security vulnerabilities, and defenders? 2, how to predict the probability that the threat materialises into an attack? Considering cloud systems, we address these challenges by proposing a security threat model based on Markov theory to calculate the probability distribution of security cloud threats. For this purpose, the Common Vulnerability Scoring System (CVSS) will be applied to compute the probability of an attack. For evaluating the proposed method, cloud security threats reported by the Cloud Security Alliance (CSA) will be investigated to calculate the probability of cloud threats materialising and the probability of various types of attack. These computation results will generate the quantitative metrics to measure the security level of a cyber-system [111].

*Major contributions of this chapter are as follows:*

- It proposes a security threat model that takes known and major cloud security threats into account. For each security threat, security factors, like attackers, security vulnerabilities and defenders, are investigated to form attack paths for calculating the probability of a security threat being materialised.
- It proposes a method for computing the probability distribution of security threats based on a Markov chain application. The Common Vulnerability Scoring System (CVSS) is investigated to obtain the data for the computation.
- It provides a method for determining the probability of materialised cloud threats and types of attack using relevant data for supporting security management.



The remainder of the chapter is organised as follows. Section 4.2 analyses the relationship between security threats and vulnerabilities. Section 4.3 proposes the security threat model based on a Markov chain. Section 4.4 describes the computation method for computing the probability distribution of cloud security threats. Section 4.5 analyses the application of the proposed method in computing attack probabilities. Section 4.6 concludes the chapter.

## **4.2 The Relationship Between Cloud Security Threats and Vulnerabilities**

To describe the security model that we propose to compute the probability of realised security threats, first, we would like to express the relationship between security threats and vulnerabilities to identify potential attacks.

A security threat is considered as a potential attack leading to a misuse of information or resources, and vulnerability is defined as some flaws in a cyber space (system) that can be exploited by hackers. As a result, a security threat is a potential attack that may or may not eventuate, but with a potential to cause damage. First, we clarify the cloud security threats based on the Cloud Security Alliance (CSA) report [42, 112]. The report released twelve critical security threats specifically related to the shared, on-demand nature of cloud computing with the highest impact on enterprise business.

1. Data Breaches (DB). These are security incidents in which confidential or protected information is released, stolen or used without authority by an attacker.
2. Weak Identity, Credential and Access Management (IAM). Attacks may occur because of inadequate identity access management systems, failure to use multifactor authentication, weak password use, and a lack of continuous automated rotation of cryptographic keys, passwords, and certificates.
3. Insecure APIs (Application Programming Interfaces). The security of fundamental APIs is a vital key role in availability of cloud services. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

4. System Vulnerabilities (SV). These are exploitable bugs in programs that attackers can use to infiltrate a computer system for stealing data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.
5. Account Hijacking (AH). It is a traditional threat with attack methods such as phishing, fraud, and exploitation of software vulnerabilities.
6. Malicious Insiders (MI). It is defined as a malicious insider threat created by people in organisations who have privileged access to the system and intentionally misuse that access in a manner that negatively affects the confidentiality, integrity, or availability of the organisation's information system.
7. Advanced Persistent Threats (APTs). These are parasitical-form cyber-attacks that infiltrate systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property.
8. Data Loss (DL): for reasons like the deletion by the cloud service provider or a physical catastrophe (including earthquake or a fire) leading to the permanent loss of customer data. Providers or cloud consumers have to take adequate measures to back up data, following best practice in business continuity and disaster recovery – as well as daily data backup and possibly off-site storage.
9. Insufficient Due Diligence (IDD). An organisation that rushes to adopt cloud technologies and chooses cloud service providers (CSPs) without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks.
10. Abuse and Nefarious Use of Cloud Services (ANU). Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.
11. Denial of Service (DOS). DOS attacks are meant to prevent users of a service from being able to access their data or their applications by forcing the targeted cloud service to consume inordinate amounts of finite system resources so that the service cannot respond to legitimate users.
12. Shared Technology Vulnerabilities (STV). Cloud service providers deliver their services by sharing infrastructure, platforms or applications. The infrastructure

supporting cloud services deployment may not have been designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS) or multi-customer applications (SaaS). This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models.

A security threat usually exploits one or more vulnerabilities in components of a system to compromise it. The relationship between security vulnerabilities and these recognised threats is thus essential for threat modelling. Hashizume *et al.* [113] identified seven major security vulnerabilities in cloud computing:

1. Insecure interfaces and APIs (V1). Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The security of the cloud depends upon the security of these interfaces. Vulnerabilities are weak credentials, insufficient authorisation checks, and insufficient input-data validation. Furthermore, cloud APIs are still immature, which means that they are frequently changed and updated. A fixed bug can introduce another security hole in the application.
2. Unlimited allocation of resources (V2). Inaccurate modelling of resource usage can lead to overbooking or over-provisioning.
3. Data-related vulnerabilities (V3). This is one of the biggest cloud challenges involving data issues. Data can be co-located with the data of unknown owners (competitors, or intruders) with a weak separation. Data may be located in different jurisdictions which have different laws. Incomplete data deletion – data cannot be completely removed. Data backup is done by untrusted third-party providers. Information about the location of the data usually is unavailable or not disclosed to users. Data is often stored, processed, and transferred in clear plain text.
4. Vulnerabilities in Virtual Machines (V4). Beside data-related issues, vulnerability in Virtual Machines is a big challenge in cloud security. It includes several aspects: possible covert channels in the colocation of VMs; unrestricted allocation and de-allocation of resources with VMs; uncontrolled migration – VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance; uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage. Uncontrolled rollback could lead to reset vulnerabilities – VMs can be backed up to a previous state for

restoration, but patches applied after the previous state disappear. VMs have IP addresses that are visible to anyone within the cloud – attackers can map where the target VM is located within the cloud.

5. Vulnerabilities in Virtual Machine Images (V5). Uncontrolled placement of VM images in public repositories. VM images are not able to be patched since they are dormant artefacts.
6. Vulnerabilities in Hypervisors (V6). These vulnerabilities stem from the complexity of the hypervisor code.
7. Vulnerabilities in Virtual Networks (V7). The vulnerabilities are associated with the sharing of virtual bridges by several virtual machines.

We identify and tabulate the connection between security threats and vulnerabilities in **Table 4.1**. It is seen that a security threat may have several security vulnerabilities and one vulnerability may be exploited by several security threats. For example, in terms of threat Data Breaches (DB), five vulnerabilities are involved in this security threat: Insecure interfaces and APIs (V1), Data-related vulnerabilities (V3), Vulnerability in Virtual Machines (V4), Vulnerabilities in Virtual Machine Image (V5), and Vulnerabilities in Virtual Networks (V7). Ristenpart *et al.* [114] indicated that confidential information can be extracted from VMs co-located in the same server. An attacker may use several attacks to collect data by exploiting vulnerabilities in brute-forcing, measuring cache usage, and load-based co-residence detection data processing techniques in cloud systems. Therefore, data leakage depends not only on data-related vulnerabilities but also on virtualisation vulnerabilities.

**Table 4.1** indicates that the data-related vulnerability (V3) is involved in three security threats. First, it may cause the threat Data Breaches (DB), when an attacker uses several techniques like SQL injection or cross-site scripting to attack the cloud system. Second, it may lead to the threat Weak Identity, Credential and Access Management (IAM), where an attacker may leverage the data that is often stored, processed, and transferred in clear plain text to gain access to the cloud system. Third, it may cause the threat Data Loss (DL), when an attacker exploits several related vulnerabilities like different located data, incomplete data deletion, and data backup.

**Table 0.1** Relationship between security threats and vulnerabilities

	<b>Threat</b>	<b>Description</b>	<b>Vulnerabilities</b>	<b>Incidents</b>
1	DB	Data Breaches	V1, V3, V4, V5, V7	An attacker can use several attack techniques involved, like SQL, command injection, and cross-site scripting. Virtualisation vulnerabilities can be exploited to extract data.
2	IAM	Weak Identity, Credential and Access Management	V1, V3	An attacker can leverage the failure to use multifactor authentication, or weak password uses.
3	API	Insecure interfaces and APIs	V1	An attacker can take advantage of weaknesses in using APIs like SOAP, HTTP protocol. Bugs in APIs can be also exploited.
4	SV	System Vulnerabilities	V4, V5, V6, V7	An attacker can attack via vulnerabilities in Virtual Machine images, in Hypervisors, and in Virtual Networks.
5	AH	Account Hijacking	V1	To get system access, attackers can use the victim's account
6	MI	Malicious Insiders	V5, V7	An attacker can generate a VM image embracing malware, then propagate it.
7	APT	Advanced Persistent Threats	V1, V4, V5, V6, V7	An attacker can use several kinds of vulnerabilities from specific virtual cloud or APIs to infect bugs permanently in the target system for mainly scavenging data.
8	DL	Data Loss	V3, V4, V7	An attacker can use data-driven attack techniques to gain confidential information from other VMs co-located in the same server; or use the risk of data backup, storing process to scavenge data.
9	IDD	Insufficient Due Diligence	V4, V6	An attacker can leverage weaknesses in complying with rules in using cloud system like configuration of VMs, data and technology shares.
10	ANU	Abuse and Nefarious Use of Cloud Services	V4	An attacker can attack, through use and share of servers, data of customers by using an anonymous account.
11	DOS	Denial of Service	V1, V2	An attacker can request more IT resources, so authorised users cannot get access to the cloud services.
12	STV	Shared Technology Vulnerabilities	V4, V6	An attacker can sniff and spoof virtual networks or exploit the flexible configuration of Virtual Machines or hypervisors.

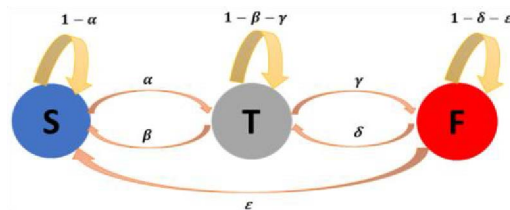
### 4.3 Markov Model for Successful Attacks

We introduce a Markov process to describe a cloud attack model and use the CVSS to determine the transition matrix of the proposed Markov model.

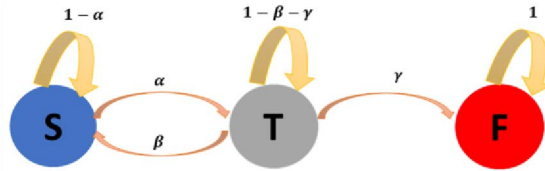
A security threat is a stochastic process. We model it as a Markov chain. The probability of transition from one state to others is based on the vulnerabilities present in the current state. An attacker exploits various vulnerabilities to arrive at a security threat state and eventually reaches the final failure state. At this stage, we mainly focus on a first level of abstraction with visible and quantifiable states and construct 3 states, namely the secure state (S), the threat state (T), and the failure state (F).

**Figure 4.1** depicts the proposed Markov model for modelling security threats and attacks with state transition probabilities, where  $\alpha$  denotes the transient probability from state S to state T,  $\beta$  denotes the transient probability from T back to S,  $\gamma$  denotes the probability to change the state from T to F,  $\delta$  denotes the transient probability from F state back to T state,  $\epsilon$  denotes the possibility from F state back to S state. The model takes all elements of an attack mode into account, including attack, defence and recovery factors of the system. We do not present the direct transition probability from state S to state F for several reasons. First, we are investigating the impact of security threats on system failure and how an attacker takes advantage of security threats. An attacker tries to exploit vulnerabilities to change from secure state to threat state. Second, the system collapses (goes directly from S to F) mainly in the case of natural disasters or similar catastrophes. This model is simple and practical for our consideration. Even with this 3-state model, it is difficult to derive a set of data for its complete description. We refine the model in several steps of our investigation.

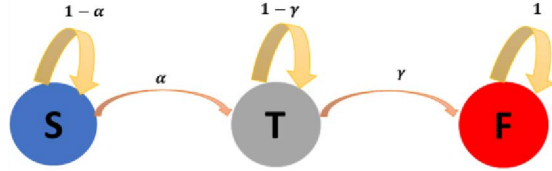
**Figure 4.2** shows the attack model with the defence elements absorbed into the failure state. It means there is no transient probability from F to T or from F to S. When the process reaches F, it stays there with probability 1. This means the recovery process is not taken into account.



**Figure 0.1** Diagram of attack model with defence and recovery



**Figure 0.2** Diagram of attack model with defence and without recovery



**Figure 0.3** Diagram of attack model without defence and recovery

**Figure 4.3** shows the attack model with the defence efforts absorbed both at the threat state and the failure state. We focus on this kind of abstraction of this model. The aim is to compute the successful chance of attacks by an attacker deploying vulnerabilities of a threat. We do not take into account the recovery element of the system at this stage of investigation, as it can be incorporated at a later stage. Furthermore, recovery efforts largely depend on the manager of the system and relevant data is not often disclosed. The probability from S to T also means the overall probability that includes the defence element that the system tries to change state from T back to S.

We are interested in finding the transition probability from state S to state F in the attack sequence. The Chapman–Kolmogorov equation [115] is available to find the transient probability between two states after a number of jump-steps. The transition probability can be calculated by matrix multiplication. Therefore, to derive the transition probability between two states in a number of steps, the Chapman–Kolmogorov equation can be used as follows:

$$P_{ij}^{m+n} = \sum P_{ik}^m P_{kj}^n \quad (4.1)$$

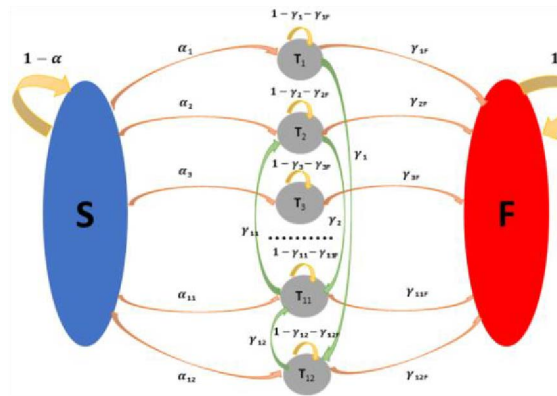
where P is the probability matrix of transitions in the state space.  $P_{ij}^{m+n}$  is the transition probability from state i to state j after (m + n) steps via any state k.

## 4.4 Distribution of Security Threat Probabilities

To compute the distribution of security threat probabilities based on a Markov chain, 3 phases can be presented as follows: modelling security threats as a Markov chain;

building a transition probability matrix; computing the transition probability from state S to state F via each threat T.

Phase 1: modelling security threats as a Markov chain. **Figure 4.4** shows an attack model that expands the general model in **Figure 4.3** with twelve attack paths. This is modelled as a Markov chain with fourteen states, including a security state, a failure state, and twelve threat states. The security state is defined as a state of the system that has no failure or security threats. The failure state is a state when the system fails to meet its minimum requirements. The threat state is considered as a middle state where an attacker could exploit a specific set of vulnerabilities. Attack path can be defined as a possible way that an attacker starts from security threat to reach failure state through threat states. In this model, we assume that the probability of an attack path is the overall probability that includes the defence element. This is a simplification, as it is possible that the system can move from one threat state to other determined threat states to reach the failure state.



**Figure 0.4** Security threat model with attack process

Phase 2: building transition probability matrix. The probability of each attack path is considered as the probability of changing state security to failure caused by each security threat. An attacker leverages security vulnerability of each security threat (the attack path) to attack to reach the failure state of the cloud system. From the attack model (see **Figure 4.4**) we arrive at a transition probability  $P_{ij}$  matrix with fourteen states including security, failure, and twelve threat states.

$$P = \begin{bmatrix} 1-\alpha & \alpha_1 & \cdots & \alpha_{12} & 0 \\ 0 & 1-\gamma_1-\gamma_{1F} & \cdots & \gamma_1 & \gamma_{1F} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1-\gamma_{12}-\gamma_{12F} & \gamma_{12F} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$



In the above matrix,  $\alpha$  is the sum of probability of all attack paths from S state to T states; and  $\gamma_F$  is the sum of the probability of all threat states to the failure state. Once the system is in the security state, it will remain in this state with probability  $(1-\alpha)$  and, once the system is in the failure state, the probability of remaining in this state is 1 (the absorbing state). The probabilities of attack paths representing from S to T states are  $\alpha_1, \alpha_2, \alpha_3$  etc. The probabilities of attack paths representing from threat states to the failure state are  $\gamma_{1F}, \gamma_{2F}, \gamma_{3F}$  etc. There are also transition probabilities from one state to other states. However, for demonstration purposes, it is assumed that there is one path from one threat state to another threat state. These probabilities are presented as  $\gamma_1, \gamma_2, \gamma_3$  etcetera.

Phase 3: computing the transition probability from state S to state F via threats  $T_i$ . According to attack paths theory, each attack-path represents the path that the attacker will take advantage of to reach the failure state (F) from a threat state (T) by exploiting the set of vulnerabilities ( $v_{ij}$ ) of each security threat. For example, we assume that attack path 1 represents the path where the attacker exploits vulnerability of threat 1 (Data Breaches-DB). Thus, there is a distribution of probability of attack paths when attackers may choose one path to attack in the space of attack paths. To quantify this distribution, we use the concept of weight of each path. CVSS [116] can be used to weigh each path from S to T, from T to F, or between threats to calculate transition probabilities. The weight associated with the transition from S to  $T_i$  is determined by computing the ratio between vulnerability scores from S to  $T_i$  and all vulnerability scores from S to all threats. By using (4.2) below, the transition probabilities ( $\alpha_i$ ) from S to  $T_i$  can be calculated. Similarly, the transition probabilities ( $\gamma_{iF}$ ) from  $T_i$  to F can be computed by using (4.3). To compute the transient probability S to F via  $T_i$ ,  $(P(SF)_i)$ , (4.1) can be used to compute the value in any number of jump-steps. However, at this stage, for the purpose of demonstrating the threat model based on the Markov chain, we compute  $P(SF)_i$  in two jump-steps using (4.4). In this case, the probability between threats may not be considered.

$$\alpha_i = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \alpha \quad (4.2)$$

$$\gamma_{iF} = \frac{\sum_j v_{ij}}{\sum_{k,l} v_{kl}} * \gamma_F \quad (4.3)$$

$$P^2(SF)_i = P^2 = \alpha_i * \gamma_{iF} \quad (4.4)$$

In these equations,  $i$  is the index of an attack path,  $v_{ij}$  is the vulnerability score of vulnerability  $j$  associated with path  $i$ ,  $k \in P$  is the set of attack paths.

To calculate the probability distribution of security threats, we need to determine elements of the Markov transition matrix based on the vulnerabilities associated with a threat. From the security state  $S$ , the total probability that the system moves to one of the threat states is assumed to be  $\alpha$  ( $\alpha = 0.0318$  [117]). We can determine the transition probability that the system moves from  $S$  to  $T_i$  as the ratio of the sum of vulnerability scores of threats associated with  $T_i$  over the total CVSS scores of all threats.

In this chapter, we use CVSS as the resource of security vulnerabilities to test our model [116]. The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of security vulnerabilities. CVSS embraces three metric groups: Base, Temporal, and Environmental. The Base group illustrates the qualities of a vulnerability that are constant over time and across user environments, the Temporal group describes the properties of a vulnerability that change over time, and the Environmental group shows the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

**Table 0.2** Vulnerability scores

Vulnerability	Acronym	Exploitability score
CVE-2017-14925	V1	8
CVE-2014-4064	V2	2
CVE-2015-5255	V3	3
CVE-2015-4165	V4	5
CVE-2016-0264	V5	7
CVE-2015-1914	V6	5
CVE-2017-6710	V7	7

**Table 4.2** shows the CVSS scores [116] associated with relevant vulnerabilities considered in this chapter. According to CVSS version 3, this number is a score out of ten. For example, V1 scores eight out of ten because the severity of this vulnerability is very high once it is related to cloud data breach vulnerabilities. In addition, to go to state

$T_1$  from S, an attacker needs to exploit the certain set of vulnerabilities associated with the security threat state  $T_1$ . In this case, vulnerabilities one, three, four, five, and seven will be exploited (see **Table 4.1**). Therefore, the number of vulnerability scores for the attack path one is  $W_1=V_1+V_3+V_4+V_5+V_7=30$  and the total number of all vulnerability score from S to any  $T_i$  is  $W=177$ . We can estimate the transition probability from S to  $T_1$  ( $\alpha_1 = 30/177 * \alpha = 0.00539$ ). Similarly, other transition probabilities from S to  $T_i$  will be computed by using (4.2). We assume that the transition probability from state  $T_i$  to F is highly likely with probability  $\gamma_{iF} = 0.95$  for any attack paths (see **Figure 4.4**). By computing  $\alpha_i$  and  $\gamma_{iF}$ , the transition probability matrix P is obtained. Then by using (4.1) and (4.4), we have the probabilistic distribution of twelve security threats expressed in **Table 4.3**.

**Table 0.3** Probability distribution of twelve security threats

	Threats	Formula	Probability ( $\times 10^{-3}$ )
1	DB	$\alpha_1 * \gamma_{1F}$	5.1203
2	IAM	$\alpha_2 * \gamma_{2F}$	1.8774
3	API	$\alpha_3 * \gamma_{3F}$	1.3654
4	SV	$\alpha_4 * \gamma_{4F}$	4.0962
5	AH	$\alpha_5 * \gamma_{5F}$	1.3654
6	MI	$\alpha_6 * \gamma_{6F}$	2.3894
7	APT	$\alpha_7 * \gamma_{7F}$	5.4616
8	DL	$\alpha_8 * \gamma_{8F}$	2.5601
9	IDD	$\alpha_9 * \gamma_{9F}$	1.7067
10	ANU	$\alpha_{10} * \gamma_{10F}$	0.8533
11	DOS	$\alpha_{11} * \gamma_{11F}$	1.7067
12	STV	$\alpha_{12} * \gamma_{12F}$	1.7067

As seen in **Table 4.3**, threat Advanced Persistent Threat (APT) has the highest probability (0.55%). The second highest probability is threat Data Breach with 0.51%. Threat Abuse and Nefarious Use of Cloud Services (ANU) has the lowest probability with 0.08%. From the distribution of security threat probability, the highest chance for attacking the cyber system relates to threat Data Breaches (DB). In terms of security management, security experts need to make a decision to protect data or to protect against advanced persistent attacks

## 4.5 Estimation of Security Attack Probability

In this section, to compute the security attack probability, the relationship between attack types and security threats will be investigated. Then, we introduce the probabilistic method to determine the security attack probability distribution.

### 4.5.1 Relationship between Attack Types and Security Threats

A security attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorised access or permission. In other words, a security attack is an attempt to gain unauthorised access to information resources or services, or to cause harm or damage to cyber systems. It is clear that an attack type relates to security threats. An attack type can use one or several security threats and one threat can involve several attack types. We investigate the relationship between attack types and security threats (**Table 4.4**). In [118], there are five major types of security attack in cloud computing. It is impossible that an attacker can exploit all vulnerabilities in the vulnerability space. Apparently, an attacker or a group of attackers just can exploit several determined security vulnerabilities. These vulnerabilities often are grouped into categories. These categories can be identified by different security threats. Each of these groups of attacks will have specific features that can be recognised and differentiated from other groups. Each group of attacks will fit several security threats.

As mentioned in Chapter 3, our CSCMM model embraces twelve security domains. Some of these domains are closely related to cloud security attacks. For example, regarding domain Identities and Access Management (IAM), this domain is mainly to prevent unauthorised access to physical and virtual resources. Therefore, several kinds of attacks like Authentication and Cloud malware injection attacks are needed to be considered in implementing domain IAM.

Five different groups of attack and their connection with security threats will be investigated as follows.

#### ***1. DOS attacks (A1)***

Attackers will take advantage of the availability feature of a cloud system; they aim to overload a target server with service requests in such a way that it is unable to respond to any new request and hence resources are made unavailable to its users. This can be illustrated in several scenarios: (1) Overloading a target with a large amount of junk data,

like UDP floods, ICMP floods etc.; (2) Using blank spaces in various protocols to overload target resources, like SYN floods, fragment packet attack, ping of death; (3) Initiating numerous HTTP requests so that they cannot be handled by the server in an HTTP DDOS attack or XML DDOS attack. It is clear that this attack type is related to the threat DOS (T11) and threat MI (T6), when attackers take advantage of a malicious insider to build the botnet for DDOS attacks.

### ***2. Cloud malware injection attack (A2)***

Attackers may try to inject a malicious service or even a virtual machine into a cloud system in order to hijack a user's service for their own purposes. These may include data modification, full functionality changes/reversals or blockings. Cloud malware injection attack groups tend to exploit security vulnerabilities that relate to security threats such as data breach, insecure interfaces and APIs, system vulnerabilities, malicious insider, and advanced persistent attack. This type of attack corresponds to 5 threats: DB (T1), API (T3), MI (T6), APT (T7) and DL (T8), when attackers use malicious insiders or advanced persistent threats to inject malware to take control of a cloud system, especially in database management.

### ***3. Side-channel attacks (A3)***

An attacker could attempt to compromise a cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side-channel attack. Side-channel attacks have emerged as an active type of security attack targeting system implementation of cryptographic algorithms. This type of attack has a close relationship with several threats such as: (1) AUN (Abuse and Nefarious Use of Cloud Services – T10) when an attacker attacks through using and sharing the servers so that the attacker can implement its malicious virtual machine to perform a side-channel attack; and (2) STV (Shared Technology Vulnerabilities – T12).

### ***4. Authentication attacks (A4)***

Authentication is a weak point in cloud computing services and is frequently targeted by an attacker. Today, most of the services still use simple username and password type of knowledge-based authentication. Some authentication attacks are: (1) Brute Force Attacks, where exhaustive combinations of a password are applied to break the password security. This brute force attack is generally applied to crack encrypted passwords when they are saved in a form of encrypted text. (2) Dictionary Attack: unlike the brute force attack, rather than searching all possibilities, the dictionary attack tries to match a

password with most occurring words or words of daily life usage and hence it is more effective in terms of speed. (3) Shoulder Surfing: it is an alternative name for “spying” in which an attacker spies on a user’s movements to gain his/her password. Here, the attacker observes the way a user enters the password, i.e. what keys of the keyboard the user has pressed. (4) Other related attacks such as Replay Attacks, Phishing Attacks, and Key Loggers. The authentication attack group is related to password attacks; hence, it is pertinent to security threats including: (1) IAM (Identity and Access Management – T2), when an attacker can take advantage from the failure to use multifactor authentication or strong passwords; (2) AH (Account Hijacking) by using a victim’s account to get access to the target’s resources; (3) ANU (Abuse and Nefarious Use of Cloud Services – T10), when an attacker attacks through using and sharing the servers to gain access to customers’ data through an anonymous account. Therefore, A4 has a relationship with T2, T5, and T10.

#### ***5. Man-In-The-Middle Cryptographic attacks (A5)***

A man-in-the-middle attack is one in which an attacker intercepts messages in the public key exchange process and then retransmits them, substituting his/her own public key for the requested one, so that the two original parties still appear to be communicating with each other. Through this process, the two original parties appear to communicate normally without being aware of the intruder. The message sender does not recognise that the receiver is an unknown attacker trying to access or modify the message before retransmitting it to the receiver. Thus, the attacker controls the entire communication. MIM attacks include: (1) Address Resolution Protocol Communication (ARP) – in the normal ARP communication, the host PC will send a packet which has the source and destination IP addresses and will broadcast the packet to all the devices connected to the network; (2) ARP Cache Poisoning, in which the attacker sniffs the network by controlling the network switch to monitor the network traffic and spoofs the ARP packets between the host and the destination PCs and then performs a MIM attack; and (3) others including DNS Spoofing or Session Hijacking. This attack group (A5) is related to several threats: (1) IAM (Weak identity, Credential and Access Management – T2), when attackers leverage the weakness in using multifactor authentication or fake information leading to loss of credentials; (2) AH (Account Hijacking – T5) by sniffing the connection to catch the cookies of victims between their PC and the web server, then using the cookies to bypass the system. So A5 has connection with T2 and T5.

**Table 0.4** Relationship between security attack types and security threats

	Type	Description	Threats	Incident
1	A1	Denial of Service	T6, T11	Making overloaded requests to the system to stop availability of servers
2	A2	Malware Cloud Injection	T1, T3, T6, T7, T8	Injecting malicious virtual machine or service to get the victim's access to the cloud system
3	A3	Side-Channel attack	T10, T12	Using and sharing the servers
4	A4	Authentication attack	T2, T5, T10	Using weak passwords, sharing technology
5	A5	Man-in-the-middle	T2, T5	Using weakness of multifactor authentication and the cookies of users

### 4.5.2 Computing the Attack Type Probabilities

Probability computation of an attack type is based on the probability of the set of security threats. It can be presented mathematically as  $Pr(A_i) = Pr(T_1 \text{ and } T_2 \text{ or } T_3 \dots)$ . However, in this chapter, we assume that each attack path presents a security threat. There are no relations between these security threats: each threat is independent from other threats. Therefore, the probability of an attack type is the union of the probability of the attack-related security threats. It is formulated as follows:

$$P(A_i) = P\left(\bigcup_{j=1}^N T_j\right) = \sum_j P(T_j) - \sum_{1 \leq j < k \leq N} P(T_j \cap T_k) + \sum_{1 \leq j < k < l \leq N} P(T_j \cap T_k \cap T_l) - \sum_{1 \leq j < k < l < m \leq N} P(T_j \cap T_k \cap T_l \cap T_m) + \dots \quad (4.6)$$

This probability of the union of any number of sets can be expressed as the following steps: (1) Add the probabilities of the individual threats; (2) Subtract the probabilities of the intersections of every pair of events; (3) Add the probabilities of the intersection of every set of three events; (4) Subtract the probabilities of the intersection of every set of four events; (5) Continue this process until the last probability is the probability of the intersection of the total number of sets that we started with [119]. The probability of an attack type is computed by using (4.6). For example, to compute the probability of attack DOS (A1), we have  $Pr(A_1) = Pr(T_6 \text{ or } T_{11}) = Pr(T_6) + Pr(T_{11}) - Pr(T_6 \text{ and } T_{11}) = Pr(T_6) + Pr(T_{11}) - Pr(T_6) * Pr(T_{11}|T_6)$ . Because  $T_6$  and  $T_{11}$  are independent,  $Pr(T_{11}|T_6) = Pr(T_{11})$ , and therefore  $Pr(A_1) = Pr(T_6) + Pr(T_{11}) - Pr(T_6) * Pr(T_{11}) \approx 0.0041$ . Similarly, applying the above algorithm by using (4.6), we will have the probability distribution of five attack types seen in **Table 4.5**.

As seen in **Table 4.5**, attack type Malware Cloud Injection (A2) has the highest probability at 1.67%. The second highest probability is attack type Denial of Service (A1) at 0.41%. The lowest probability is attack type Side-Channel Attack (A3) with 0.2%. The distribution of attack probability provides several implications. For an attack countermeasure plan, security practitioners need to care about methods to prevent malware cloud injection attacks, because the chance of this type of attack is highest. For a security manager to make a decision on security investment, it may depend on not only the probability of an attack but also the consequences of this successful attack, because, in several scenarios, the probability of an attack is very small, but the impact is very high in terms of money. As a result, the average security cost, which is the product of the probability of an attack and the consequence of this attack, is quite high. In this case, the manager can prioritise security actions against the kind of attack that makes more damage – for example, if the consequence of denial of service attacks (A1) is ten times higher than that of malware cloud injection (A2), at \$1,000,000 and \$100,000, respectively. In this case, using the figures from Table 5, the security cost for A1 is  $\$1,000,000 \times 0.00409 = \$4,092$ , while the security cost for A2 is  $\$100,000 \times 0.016 = \$1,667$ . Therefore, the security cost for A1 is nearly two-and-a-half times higher than the security cost for A2.

**Table 0.5** Probability distribution of five attack type

	<b>Attack</b>	<b>Description</b>	<b>Probability (<math>\times 10^{-3}</math>)</b>
1	A1	Denial of Service	4.092
2	A2	Malware Cloud Injection	16.679
3	A3	Side-Channel attack	2.559
4	A4	Authentication attack	4.091
5	A5	Man-in-the-middle	3.240

## 4.6 Summary

This chapter has proposed a novel security threat model to compute security threat probability as a metric to measure the security of a cyber-system. For this purpose, we applied a Markov chain model with three states to identify the attack paths through various security threats. Twelve security threats reported by the Cloud Security Alliance and seven security vulnerabilities scored by the Common Vulnerability Scoring System were investigated to quantify the parameters of the proposed security threat model and to compute the probability distribution of security threats. The probability distribution for



cloud attack types also was calculated based on the security threat model. Several scenarios for using the probability distribution of security threats and attacks in cloud security management were explained. One of the limitations in the model is that the relationships between security threats have not been taken into account. This leads to our Markov computation of probability of realised security threat over two jump-steps. This threat model above just focused on the states of a cyber-system, which is based on the description of an attack path with the flow of security vulnerabilities. Thus, another gap from this model is that it has not taken the attackers and controllers into account such as the exploitation skills of an attacker, and the vulnerability mitigation capabilities of controllers. These research challenges motivate us to study the model that includes security factors including attackers, controllers, vulnerabilities, favourable conditions. Therefore, the next chapter (Chapter 5) will introduce an exist-escape threat model that deals with the above gaps.

# **Chapter 5**

## **An Exist-Escape Security Threat**

### **Model for Computing the Probability**

#### **of Materialised Threats and Its**

##### **Application to Cloud**

### **5.1 Introduction**

Identifying and quantifying security threats is one of the most important keys in cyber security management. Clearly, to estimate security risks, first and foremost is the task of computing the probability of materialised security threats. Security threat to a system is, however, a difficult concept to pinpoint as it interrelates multiple dynamic entities and time-varying factors including attackers, attack methods, system vulnerabilities, and security controls/controllers. Security management would be effective in terms of security decisions and actions if one can quantify and predict the probability of a threat materialised and its consequences. Measuring realised security threat probability is important for several reasons. First, there is no system that is 100% secured because of the complex nature of its underlying technologies, and the incompleteness of our understanding of the behaviour/interaction of the human beings internal and/or external to the system. System vulnerabilities and potential threats always exist and evolve along with the dynamics of the system and its users. The issue is how to quantify the measure of the probability of a threat materialised. Second, by definition, security risk is the product of probability of security threat and its consequence when the security threat materialised [65]. Clearly, an essential component for the estimation of security risk is the measure of the probability that the threat materialised. Third, the measure of the probability that a threat materialised implicates the specific vulnerabilities associated with the threat and hence effective security measures that can be taken to prevent or mitigate

the occurrence of attacks and their consequences. In a previous chapter (Chapter 4), a security threat model based on Markov and CVSS was created for quantifying the realised security threat probability. However, as analysed at the end of Chapter 4, this model has not taken several security factors such as attackers, controller into account. This chapter proposes the security threat model with two phases: (1) investigate the existing threat space to identify the relationship between attack conditions and vulnerable systems; (2) explore the materialised threats to discover the control factors that deal effectively with security threats. Based on this model, the computation of probability of security threat existed and security threat materialised will be presented. For validating and evaluating the model, a case study in cloud computing will be introduced and we will apply quantitative methods using search theory to compute the probability of security threats.

*Major contributions of this chapter are as follows:*

- It proposes the security threat model that relates three main factors for an eventual attack: the system vulnerabilities, the attackers and their capability of exploiting the vulnerabilities, and the system security manager and its capability to protect the system.
- It proposes a method for computing the probability of the existence of a security threat and the probability of the existed security threat materialising. Moreover, the Common Vulnerability Scoring System (CVSS) will be investigated to derive the data for the computation.
- It provides several case studies where the proposed model and the computation method are applied to the Cloud computing using relevant data on cloud systems in supporting the security decision making process and security actions.

The remainder of the chapter is organised as follows. Section 5.2 introduces an exist-escape security threat model with two phases. Section 5.3 describes the proposed measure to compute the probability of security threat through the analysis of the specification of the cyber system that relates to the security threat and the use of search theory to derive the mathematical equations to compute the probability of security threat. Section 5.4 expresses an example that applies the model and metric in cloud computing. Section 5.5 provides the methods for obtaining the data for the model. Section 5.6 evaluates the model on a generic security threat. Section 5.7 describes the application of the model to cloud security threats. Finally, Section 5.8 concludes the chapter with remarks.

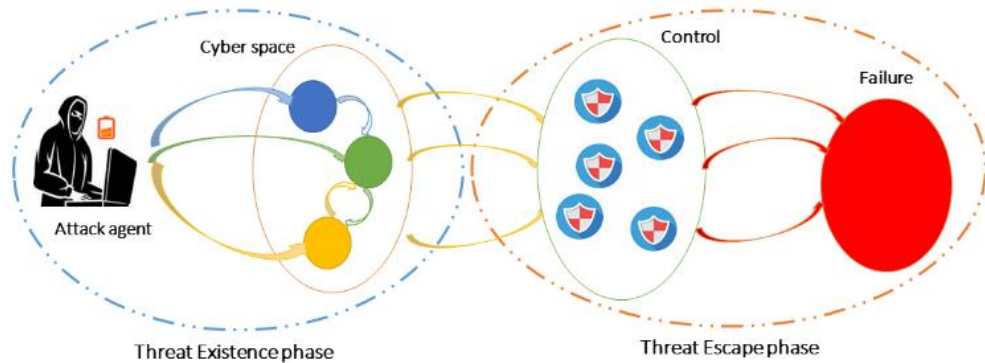
## 5.2 Modelling Security Threat

In this section we propose a model for security threats and explore the design of the model space in relation to the attacker space, the system vulnerability space and the security management space or control space. In particular we pay attention to the conditions for the existence of a threat relative to the vulnerabilities of a system and the conditions under which a threat can be realised into an attack.

In a previous study we considered cyber security as a collective whole that embraces systems, tools, processes, practices, concepts and strategies to prevent and protect the cyber space from unauthorised interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources” [17, 111]. Study of a security threat is thus the study of the relationship among security factors including attackers, attack conditions, vulnerabilities, controllers, and trigger conditions over a cyber space.

A real attack process should simply be divided into two sub-processes. First, potential attackers start with scanning the system to find the vulnerabilities of the system. If system security vulnerabilities exist, the attackers may discover them and use their skills to exploit the discovered weaknesses. Second, even the hackers have exploitations of those found vulnerabilities, to make the attack successfully the attackers need to avoid being detected and escape security countermeasures by the defenders or security controllers.

The aim of our investigation is to construct a model to define the existence of a threat over a system (or in general, a cyber space that is to be protected) and how the threat moves from the state where it exists to the state where it materialises into an attack. To address this aim we propose a two-phase model, the Exist-Escape security threat model: a threat existence phase and a threat escape phase as shown in **Figure 5.1**.



**Figure 0.1** Security threat model

## 5.2.1 Security Threat Existence Phase

The aim of this phase is to identify the conditions for the existence of a security threat and to quantify the probability of this existence.

We observe that there exists a relationship between the attacker(s) and the vulnerabilities of a system for an attack to occur. On the one hand, a system may expose many weaknesses, but if there are no attackers that can exploit these vulnerabilities, a threat never exists. On the other hand, attackers may be available and capable of exploiting the system's vulnerabilities, but if the system does not expose any vulnerability that the attackers can exploit, there will be no security threat. This implies that a threat is considered as existed only if there exists an attacker who can find and exploit the exposed vulnerabilities of the system. Clearly, there are different types of system vulnerabilities that may or may not be exposed (detected or discovered). For each vulnerability, there are methods for exploiting it. Similarly, there may exist many types of attackers who have different capabilities in terms of the know-how for exploiting vulnerabilities. Different forms of security attacks may result in depending on both the attackers and the system vulnerabilities. From this discussion, it can be said that the chance that a specific security threat exists depends on both the attacker space and the vulnerability space.

- Skill level of attackers

Basically, from the attacker viewpoint, to plan a security attack, it needs to gather enough information about the system or organisation and then analyse the data to identify any system vulnerabilities if they exist. If a vulnerability exists, the attacker will have to find it and assess the exploiting capability. If the attacker does not have the capability to exploit the vulnerability, further advance cannot take place. Clearly, the scanning, gathering, data analysis, and assessment of exploitation capability are pertained to the skill level of the attackers. The model needs to consider this skill level to account for the number of vulnerabilities an attacker can expose and the number of methods it can use to exploit a vulnerability.

Thus, a security threat exists over a system only if there is an overlap between the attacker space and the system vulnerability space where an attacker exists and has the ability to exploit the system vulnerability.

- Vulnerabilities of cyber space

Security vulnerability has been defined differently from various organisations. In ISO 27005, it is a weakness of an asset or group of assets that can be exploited by one or more threats. However, we consider vulnerability as an integral part of a security threat. The NIST definition is more relevant. According to NIST, a vulnerability is a flaw or a weakness in system security procedure, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) to cause a security breach or a violation of the system's security policy. Vulnerabilities can exist in any components of a system for various reasons. They can be in hardware components due to design faults or the stochastic nature of electronic subcomponents of the system. They can be introduced in software unintentionally by programmers and users or intentionally by malicious elements. They can be in network and connectivity components where physical or virtual devices interconnect. They also can be introduced by human activities over social engineering or social networking.

- Technology environment

Technology environment is an important part in the connection between attackers and vulnerable systems. It may initiate a new form of attacks or be responsible for a change in an attack method. For example, ten years ago ransomware was not well known. Recently, this form of attack has become widespread because of the acceptance of online payment systems and the lack of security knowledge of the users. Another influence of technology is the dramatic increase in denial of service attacks in Internet of Things (IOTs) systems because of the exponential increase in the number of IOT devices, with limited defence capability, connected to the Internet.

Apart from the above factors, others like attack methods, attack types, the intention and motivation of attackers, and time are also relevant to the security threat existence phase.

Mathematically, we can express the probability of the existence of a threat by (5.1), taking into account variables discussed above, including attacker's capability, system's vulnerabilities, time, attack methods, attack types, attack targets, attack motivations.

$$P\{\text{the existence of a security threat}\} = f(a, v, t, k, m, \dots) \quad (5.1)$$

where  $a$  is the capability (skill level) of attackers,  $v$  is the vulnerability of the system,  $t$  is the time that attackers take to carry out the exploitation from known vulnerabilities of the system,  $k$  is the kinds of attack,  $m$  is the attack method, and possibly other factors.

## 5.2.2 Security Threat Escape Phase

In the threat escape phase, the model aims to identify and quantify the factors that move an existing threat to the state that the threat materialises into an attack. After the first phase, attackers would have the exploitations of the vulnerable system. This means that realistic conditions for the existence of a security threat have been identified and the probability of the existence of the identified threat can be computed. However, for the threat to materialise, the attackers need to consider “favourable conditions” for an attack. Favourable conditions include all security factors that the attacker’s favour for the initiation of the attack. It is impossible to numerate all favourable factors. We limit ourselves to considering the main factors that can be controlled or exercised by a controller (or security manager) of the system as indicated in **Figure 5.1**.

- The security control system

A control system can be a countermeasure or a defence system that embraces actions, policies, and decisions for protecting a system by reducing system vulnerabilities, preventing security attacks, or policies to mitigate the consequences of an attack policy. Once an attacker can avoid, pass, escape, or penetrate the control system, the attacker initiates the attack and renders the system to a failure state. As a result, the system may be partly or whole damaged and the extent of the damage depends on the target of attackers and the resilience capability of the system. In this phase, there may exist a trigger condition that the attacker’s exploitation is undetected by the control system. This trigger condition can be an integration or accumulation of many factors like the time, the technology, the capability of the control system. However, in this chapter, we consider controllable factors in this phase. According to ISO 27002, the control system can be divided into three categories: logical, administrative, and physical. Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. Administrative controls consist of approved written policies, procedures, standards and guidelines. Physical controls monitor and control the environment of the workplace and computing facilities.

Probability that the existed threat from (5.1) avoids the system control measures is expressed by (5.2)

$$\begin{aligned} &P\{\text{the threat undetected by control systems} \mid \text{given the threat existed}\} \\ &= g(v_e, c_e, p_e, t_e, \dots) \end{aligned} \quad (5.2)$$

where,  $ve$  denotes the exploited vulnerabilities when attackers have exploits to attack the system,  $ce$  denotes the control factors in the materialising process,  $pe$  denotes security policies that affect the attack process,  $te$  denotes the time of the attack, and other factors.

Finally, the probability of a threat materialises into an attack is given by (5.3). It is the product to the probability of the existence of a security threat and the probability that the given existed threat escapes possible security system control measures:

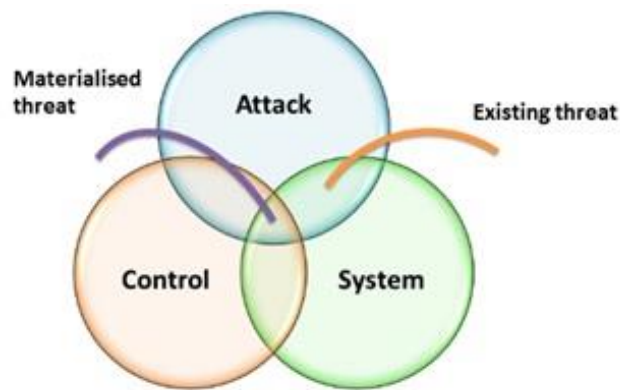
$$\begin{aligned}
 & P\{\text{the threat materialised}\} \\
 & = P\{\text{the existence of the security threat}\} \\
 & * P\{\text{the threat undetected by control systems} \mid \text{given the threat existed}\}
 \end{aligned} \tag{5.3}$$

### 5.2.3 Security Threat Model Presented in a Venn Diagram

The Venn diagram in **Figure 5.2** visualises the relationship among the three main entities of security threats. In this, there are three circle blocks representing three constituting security spaces including attack, system, and control blocks. The attack-block embraces attackers and attack conditions. The attack conditions embrace attack methods, time to analyse insecurity information of the system, the target that attacker wants to attack, the motivation of the attacker, the attacker skill level at the time to the attack. Regarding the system-block, it includes the system under consideration and its status. This means that the system block covers all key elements including real and virtual entities, interconnecting infrastructure, and interaction among entities. The emphasis is on the vulnerabilities of the system. As for the control block, it includes control measures, defence policies, and system management strategies and actions.

As seen in the **Figure 5.2**, in terms of security vulnerabilities, an existing threat is found within the overlap between attack and system blocks. This represents the system vulnerability exploitation- attacker(s) capability matched condition. Materialised threats can be found in the intersection region where all three attack, system, and control blocks are intersecting. This is also the intersection of existing threats with the control block.





**Figure 0.2** Security threats is the intersection of attack, system, and control

### 5.3 Quantifying the Probability of Threats Materialised

It is clear from the previous section that equations (5.1), (5.2), and (5.3) apply in an ideal situation where all variables can be accounted for in computing the probability of a threat materialised. Realistically, data for many of these environmental variables are not available or are unreliable. In our derivation of the probability of a threat materialised, we confine ourselves to the system vulnerabilities, the exploitations that can be exercised over the vulnerabilities by the attacker, and the control measures that can be actioned over the vulnerabilities.

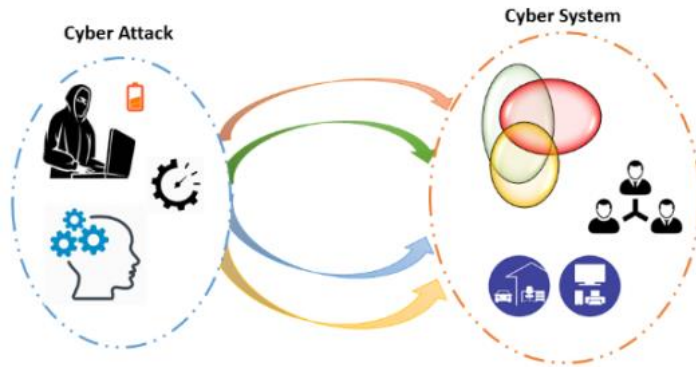
In this section, we propose a model to compute the probability that exploitations can be exercised by attackers over system vulnerabilities visible to the attackers. That is the probability that there exists a match between the exposed vulnerabilities and the exploitation capability of the attackers, or simply the probability of the existence of a threat.

#### 5.3.1 Computation of Probability of Threat Existence

The threat existence phase in **Figure 5.1** is expanded as shown in **Figure 5.3** to include the cyber-attack and the cyber system blocks. This phase depicts the conditions/situations for a threat to exist. Our model has several assumptions including: (1) for this phase, we assume two players in the cyber threat space where one player (an attacker in the cyber-attack block) seeks weaknesses of the other player (the cyber system block) to exploit; (2) the attacker's capabilities are represented by the system security vulnerabilities that it has exploitations; (3) the cyber system block with known vulnerabilities; (4) the threat existence

phase is valid for the period over which we wish to compute the probability of the existence of the threat; (5) technology factor is not taken into account.

Therefore, the probability of an existing threat is considered as the probability of a match between the attack capabilities from the cyber-attack block and the weaknesses of the cyber system block. We follow and open the Major's work [88] to compute the probability of threat existence. Explicitly, our model assumes that the probability that an existed threat is the probability that the attackers have exploitations (over a subset set of system vulnerabilities visible to them) over the set of vulnerabilities of the system.

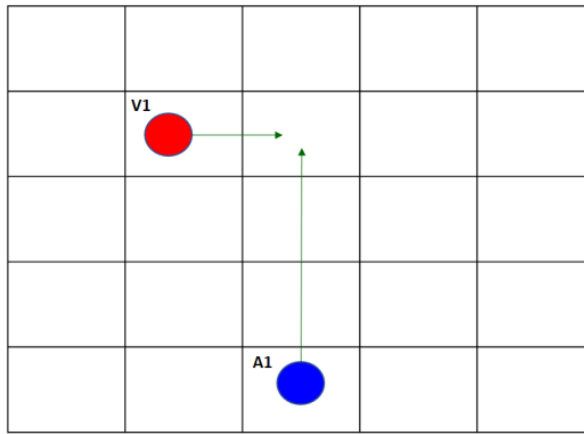


**Figure 0.3** Threat Existence phase

To model this link, we denote  $V$  as the number of vulnerabilities of the system and  $A$  as the number of exploitations on the vulnerabilities that the attackers are capable of finding and exploiting, randomly placed on a grid having  $T$  locations.  $T$  is expressed as the total number of known vulnerabilities in vulnerabilities space published by National Vulnerabilities Database (NVD). The probability of threat existence is the probability that a type  $A$  entity and a type  $V$  entity end up at the same grid location. This implies that there is at least one existed vulnerability in the system and an attacker has capability to exploit this vulnerability. To compute this probability, several cases are presented before the derivation of a general case.

**Case 1:**  $V = A = 1$ , the number of vulnerabilities in the system is one and the number of exploitations over the vulnerability that attackers can exploit is one.

In this case, the probability of a type  $A$  entity being at the same location with a type  $V$  entity is equal to  $T/T^2$  or  $\frac{1}{T}$ . Therefore, the probability of  $A$  missing  $V$  is  $(1 - \frac{1}{T})$  (**Figure 5.4**).



**Figure 0.4** Search theory between attacker capability and vulnerabilities of system in case  $V=A=1$

**Case 2:**  $V > 1$  and  $A = 1$ , the number of vulnerabilities in the system is more than one and the number of exploitations over the vulnerabilities that attackers can exploit is one (**Figure 5.5**).

The  $A$  entity is randomly placed on a location of the grid (out of  $T$  locations), each of the  $V$  entities has an independent  $1/T$  chance of being the same location of  $A$  (or exploited by  $A$ ). The probability of each  $V$  missing  $A$  is  $(1 - \frac{1}{T})$ . Hence, the probability of all  $V$  independently missing  $A$  is  $(1 - \frac{1}{T})^V$ . Therefore, the probability of at least one of  $V$  independently being on the same location with  $A$  (the chance of the attacker's capability matches the system's vulnerabilities) is  $1 - (1 - \frac{1}{T})^V$ .

**Case 3:**  $V > 1$  and  $A > 1$ , the general case where the number of vulnerabilities in the system is more than one and the number of exploitations over the vulnerabilities that attackers can exploit is more than one.

Similarly, the probability of all  $V$ s independently missing one of  $A$  is equal to  $(1 - \frac{1}{T})^V$ . Hence, the probability of all  $V$ s independently missing all of  $A$ s is equal to  $(1 - \frac{1}{T})^{V \cdot A}$ . Therefore, the probability of the event that at least one of  $V$ s and one of  $A$ s being at the same location is  $1 - (1 - \frac{1}{T})^{V \cdot A}$ . This is the probability that we need to determine the probability of security threat existed.

To find the approximated equation of this pronominal, Taylor series is applied as follows:

Put  $x = \frac{1}{T}$ ;  $V * A = k$ , so  $(1 - \frac{1}{T})^{V*A} = (1 - x)^k$  with  $|x| < 1$ , and  $x$  is a very small number.

Using Taylor and Maclaurin series for natural exponential function [120], we have

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!} + \dots$$

Replacing  $x$  by  $(-x)$  in above equation we have

$$e^{-x} = \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots - \frac{x^n}{n!} + \dots$$

When  $x$  is very small and  $|x| < 1$  then  $\frac{x^2}{2!} - \frac{x^3}{3!} + \dots - \frac{x^n}{n!} + \dots$  is close to zero, therefore

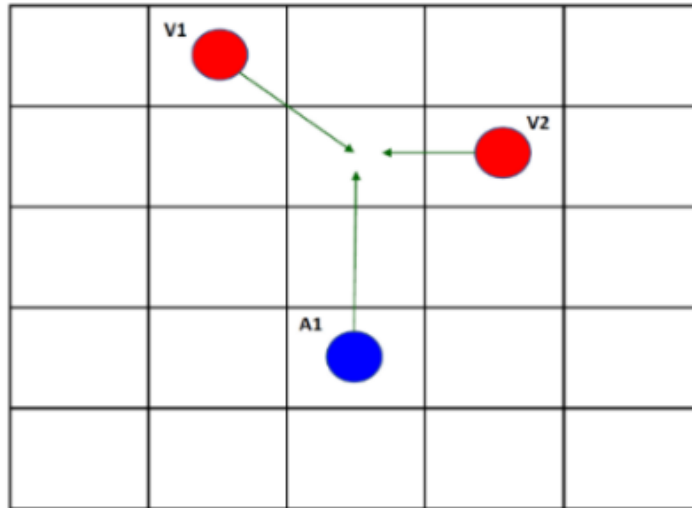
$$e^{-x} \approx 1 - x, \text{ so } e^{-kx} \approx (1 - x)^k$$

Substitute  $k = V*A$  and  $x = 1/T$ , we can approximate  $(1 - \frac{1}{T})^{V*A}$  by  $e^{-\frac{V*A}{T}}$

Hence, we can assume for large values of  $T$ ,

$$P_e = 1 - (1 - \frac{1}{T})^{V*A} = 1 - e^{-\frac{V*A}{T}} \quad (5.4)$$

where,  $P_e$  is the probability of threat existence,  $A$  is the number of exploitations that an attacker has over the vulnerabilities;  $V$  is the number of vulnerabilities existed in the system;  $T$  is the vulnerabilities space.

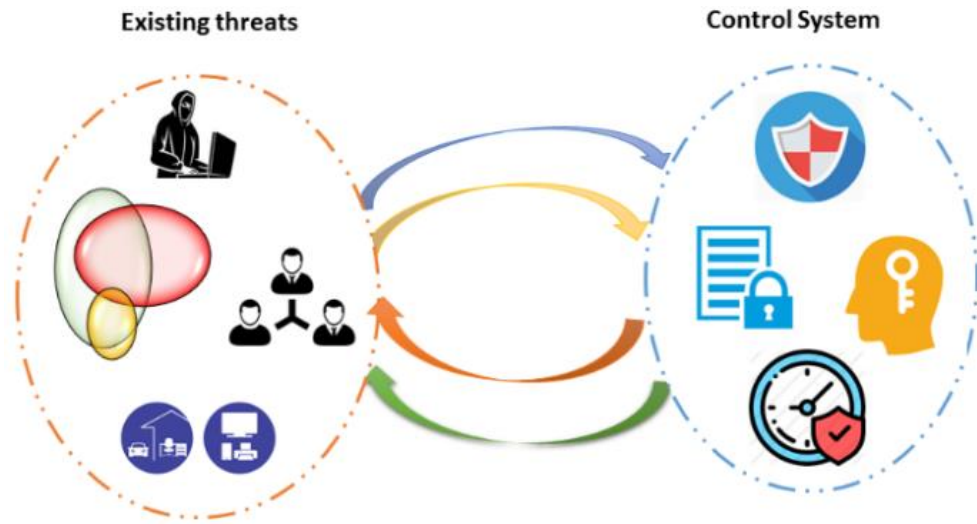


**Figure 0.5** Search theory between attacker capability and vulnerabilities of system in case  $V > 1, A = 1$

For this threat existence phase, we follow an approach similar to Major's work [88], but apply it to our new threat model. Instead of considering the attackers and the defenders we consider system vulnerabilities and the attackers, we focus on the capability of the attackers in seeing and exploiting exposed system vulnerabilities to derive the probability that there exists a match between the exposed vulnerabilities and the exploitation capability of the attackers.

### **5.3.2 Computation of Probability of Threat Escape**

The threat escape phase in **Figure 5.1** is expanded as shown in Figure 5.6 to include the existing threats block and the system control block. This phase depicts the conditions/situations for an existing threat to materialise (or an attack to occur). Once a threat is identified and quantified in terms of probability, the chance of its materialisation into an attack depends on other favourable conditions relating to the attack block, the system vulnerability block, the system control block as well as the interactions among these blocks. In this chapter we confine ourselves on the system control block and the security (or control) measures it can exercise over the system vulnerabilities. The system control block embraces security factors including control system, security policy, capability of defender, the time, and environmental technology. Basically, attackers will keep trying to use their exploitations to overcome control system to make the attack successfully. In other words, the attackers will take advantages of favourable conditions like the lack of security control, the limitation of security technology, the opportune time, and the un-updates in security policy. In this model, we confine ourselves to the capability of the system control block in terms of its security measures over the cyber system vulnerabilities. By doing so, similar approach deployed above for computing the probability of the existence of a threat can be used to compute the probability that an existing threat escapes the control measures and then the probability of the existing threat materialises into an attack.



**Figure 0.6** Threat Escape phase

Similarly, consideration of an existing threat and a control system as two players in an escape space, a successful attack event happens once the attackers are undetected by the defenders. We hypothesise that attackers would operate over vulnerabilities of the system ( $V$ ) in existing threat. This means that  $V$  represents the system vulnerabilities as in the first phase. The  $C$  entity represents the controllers' capability.  $C$  is the number of patches over vulnerabilities that controllers are capable of fixing.  $E$  is the control security measures (or patches) space. The two players (attackers and controllers) enter randomly the  $E$  locations grid that is the vulnerabilities having patches. In general, if  $V > 1$  and  $C > 1$ , the probability of all  $V$  independently missing  $C$  is  $(1 - \frac{1}{E})^{V*C}$ . Similar approximation as above, we have the equation:

$$P_m = (1 - \frac{1}{E})^{V*C} = e^{-\frac{V*C}{E}} \quad (5.5)$$

where,  $P_m$  is the probability of an existed threat escaping the control measures;  $V$  is the number of vulnerabilities of system;  $C$  is the number of patches over vulnerabilities that controllers can patch;  $E$  is vulnerabilities space having patches.

According to (5.3), (5.4), and (5.5) the probability of security threat materialised is measured by this formula below:

$$P = P_e * P_m = (1 - e^{-\frac{A*V}{T}}) * (e^{-\frac{V*C}{E}}) \quad (5.6)$$

This threat escape phase constitutes another innovation of the chapter. The approach considers the capability of the security controllers over the system vulnerability space and derives the probability that an existing threat materialises.

## 5.4 Application of the Security Threat Model to Cloud Computing

In this section, we consider the application of the proposed security threat model to cloud computing. To demonstrate this model in cloud, several assumptions are made. The attack block is assumed to include attackers and their capabilities, the system block is represented by security vulnerabilities of the cloud system, and the control block includes controllers and their capabilities.

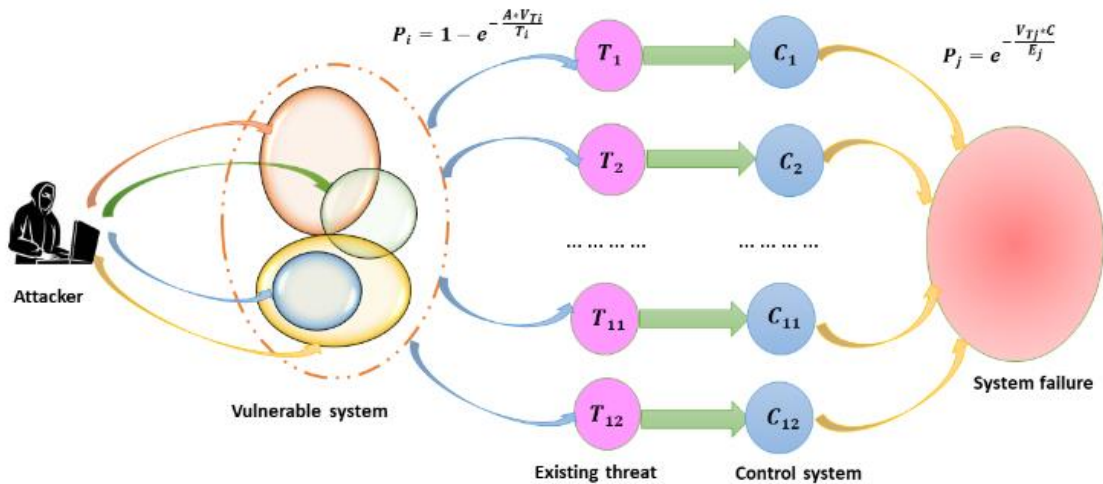


Figure 0.7 Security threat model in cloud computing

### 5.4.1 Computation of Probability of Threat Existence in Cloud Computing

As seen in Figure 5.7, attackers with their attack capabilities seek to exploit the security vulnerabilities of the system. In our first approximation of the proposed model, we confine ourselves with only the skills of the attackers and the security vulnerabilities in determining the existence of a threat. In the cloud computing, seven different categories of security vulnerability have been identified [113]. An attacker can exploit one or more different security vulnerabilities that constitute different categories of security threats, to build different forms of attacks. In our paper [77], seven kinds of cloud vulnerabilities and twelve security threats based on research of CSA (Cloud Security Alliance) [42], were investigated.

The seven cloud major vulnerabilities are Insecure interfaces and APIs (V1), Unlimited allocation of resources (V2), Data-related vulnerabilities (V3), Vulnerabilities in Virtual Machines (V4), Vulnerabilities in Virtual Machine Images (V5), Vulnerabilities in Hypervisors (V6), Vulnerabilities in Virtual Networks (V7). The CSA released twelve critical security threats specifically related to the shared, on-demand for cloud computing with the highest impact on enterprise business. These are: Data Breaches (DB-T1); Weak Identity, Credential and Access Management (IAM-T2); Insecure interfaces Application Programming Interface (API-T3); System Vulnerabilities (SV-T4); Account Hijacking (AH-T5); Malicious Insiders (MI-T6); Advanced Persistent Threats (APTs-T7); Data Loss (DL-T8); Insufficient Due Diligence (IDD-T9); Abuse and Nefarious Use of Cloud Services (ANU-T10); Denial of Service (DOS-T11); and Shared Technology Vulnerabilities (STV-T12).

- The relationship between security vulnerabilities and threats

In our recent research, we investigated and explained the relationship between cloud vulnerabilities and security threats. A security threat may arise from several security vulnerabilities and a vulnerability may play a role in several security threats. For example, in threats related to Data Breaches (DB), an attacker may use several attack techniques such as SQL injections, and cross-site scripting. Therefore, various vulnerabilities may be involved in this threat including Data-related vulnerabilities (V3), Vulnerability in Virtual Machines (V4), Vulnerabilities in Virtual Machine Image (V5), and Vulnerabilities in Virtual Networks (V7).

On the other hand, a vulnerability may play a role in several threats. For example, data-related vulnerability (V3) may be involved in three security threats: data breaches (DB) threat, Identity, Credential, and Access Management (IAM) threat, and data loss (DL) threat. DB threat is when an attacker uses several techniques involved SQL injection to attack a cloud system. IAM threat is when an attacker leverages the data that is often stored, processed, and transferred in clear plain text to gain access to a cloud system. DL threat is when an attacker exploits several vulnerabilities such as different located data, incomplete data deletion, and data backup.

According to (5.4), we derive the formula to compute the probability of threats existence in cloud computing as follows

$$P_{ei} = 1 - e^{-\frac{A*V_{T_i}}{T_i}} \quad (5.7)$$



where,  $P_{ei}$  is the probability of security threat  $i$ ,  $A$  is the number of exploitations over vulnerabilities visible to attackers. This is based on the attacker skill level (it is divided into three levels),  $V_{Ti}$  is the total number of vulnerabilities within the security threat  $Ti$  of the investigated system;  $Ti$  is the total number of vulnerabilities within security threat  $Ti$  in vulnerability space based on CVSS (Common Vulnerabilities Score System).

## 5.4.2 Computation of Probability of Threat Escape in Cloud Computing

After matching between the capability of attackers and the vulnerabilities of the system to quantify the existence of a security threat, we need to quantify its materialisation. To launch an eventual attack, the attacker needs to overcome or escape the control system (see **Figure 5.7**). Therefore, with each existing threat path, attackers have to face the subset of security measures of the security controller. In our first approximation of the proposed model, we confine ourselves with only the skills (or repertoires) of the controllers to implement measures over the system vulnerabilities in determining the chance of the threat materialised.

Imagine that, the battle between attackers and controllers is based on the process of exploiting and patching the security vulnerabilities. Attackers would keep exploiting the security vulnerabilities and the defenders will manage to patch these security vulnerabilities to mitigate or eliminate them. The capability of the controller will be determined by the number exploitations of security vulnerabilities and the ability of the controllers to patch them successfully. If the controllers are unable to patch any existing vulnerabilities, the probability of the existing threat materialised would be equal to the probability of the existence of the threat as computed in the first phase.

According to (5.5), the formula computing the probability of threat escaping the control security measures is given by

$$P_{mi} = e^{-\frac{V_{Ti} * C}{E_i}} \quad (5.8)$$

where,  $P_{mi}$  is the probability of threat escape given that existing threats,  $V_{Ti}$  is the number of ready vulnerabilities of the system that attacker has exploitations from first phase;  $C$  is the number of security patches (or security measures) over vulnerabilities the

controller has; and  $E_i$  is the total number of vulnerabilities in CVSS within security threat  $i$  that has the patches.

Therefore, according to (5.6), we have the formula to find the probability of threat materialised  $i$  is as follows:

$$P_i = P_{ei} * P_{mi} = (1 - e^{-\frac{A * V_{T_i}}{T_i}}) * (e^{-\frac{V_{T_i} * C}{E_i}}) \quad (5.9)$$

## 5.5 Data for the Proposed Threat Model

In this section, we will introduce the method to obtain the data for each of these blocks.

### 5.5.1 Attack Conditions

Representation of the attack condition block is the capability of attackers or skill level of attackers (variable A). The value of A is the number of exploits readily available to the attackers. This number is changeable and depends on the capability of attacker skill levels. The way we derive this number follows McQueen’s work [90]. Obtaining this number is based on empirical data. Identifying the methods and hence the number of exploits over a set of vulnerabilities is important but specific to a particular setting. Without losing generality, we assume that the number of possible exploits relates to the skill level of the attacker. Attacker(s) skills are assumed 3 different levels. Beginners are capable of using existing code and exploiting some simple known vulnerabilities level.

**Table 0.1** Attackers skill levels

Attack skill level	# of readily available exploits
Expert	2940
Intermediate	1082
Beginner	398

They can use simple existing code, tools, and attacks to exploit known vulnerabilities. An intermediate attacker can modify existing code, tools, and attacks to exploit known vulnerabilities. An expert attacker can create new code, tools, and attacks and can identify unknown vulnerabilities. According to Rapid7 Exploit Database [121],

on the day of this investigation (27th October 2018) the total number of exploits is 2,940. It is assumed that expert skill attackers are aware of all these exploits so the number of readily available exploits to expert will be 2,940. In [90], Mc Queen indicated that the number of readily available exploits is followed on exponential growth based on empirical data. Skill levels of attacker are defined in **Table 5.1**.

## 5.5.2 System Conditions

The data for system conditions is based on the number of security vulnerabilities of the system ( $V$ ) and the total number of security vulnerabilities in CVSS for each security threat ( $T_i$ ). To derive the data for these figures, we use the statistics from the National Vulnerabilities Database (NVD), which publishes CVSS every year [116]. According to this statistic, reported in the database of NVD from 10/1999 until 10/2019 is 108,898. It assumed that the number of cloud security vulnerabilities is about 80% of the total number of security vulnerabilities, therefore, we have the number of security vulnerabilities in cloud is  $80\% * 108,898 \approx 87,118$ . In the CVSS, the vulnerabilities are also grouped and rated. There are thirteen different kinds of security vulnerability such as DoS, Code Execution, Overflow, Memory Corruption, XSS, SQL injection, Gain information, Gain privilege, Directory traversal, Http response, Bypass, Cross-Site Request Forgery (CSRF), and File inclusion. For the sake of simulation, the rate of each type of cloud security vulnerability is based on the same rate of categorised vulnerabilities in CVSS as shown in **Table 5.2**.

**Table 0.2** The number of vulnerabilities for seven kinds of vulnerabilities

Cloud security vulnerability	Acronym	Number of cloud security vulnerabilities
Insecure interfaces and APIs	V1	13,590
Unlimited allocation of resources	V2	29,272
Data-related vulnerabilities	V3	16,291
Vulnerability in Virtual Machines	V4	5,750
Vulnerabilities in Virtual Machine Image	V5	4,704
Vulnerabilities in Hypervisors	V6	12,893
Vulnerabilities in Virtual Networks	V7	4,618

**Table 5.3** shows the average total number of vulnerabilities in the vulnerability space of each cloud threat. The reasons we use these mean numbers are (1) to observe the

change of probability of security threat in terms of the number of vulnerabilities existed in the system; (2) to compare the significant differences among cloud security threats.

**Table 0.3** The average number of vulnerabilities for each threat

Acronym	Threat	Average # of vulnerabilities
T1	DB	8991
T2	IAM	14941
T3	API	13590
T4	SV	6991
T5	AH	13590
T6	MI	4661
T7	APT	8311
T8	DL	8886
T9	IDD	9322
T10	ANU	5750
T11	DOS	21431
T12	STV	9322

### 5.5.3 Control Conditions

Representation of the control condition block is the capability of controllers. In other words, it is the number of vulnerabilities that a controller has patches for, to make sure an attacker cannot keep exploiting the existing vulnerabilities (C). Similar to the skill level of attackers, this number is variable representing the controller's capability in deploying various security measures or patches to eliminate or mitigate the system vulnerabilities or simply controller capability level. It is divided into 3 different levels: junior, senior, professional. Junior controllers can patch the known vulnerabilities published in the CVSS and several simple vulnerabilities not published in CVSS by using simple tools. Senior controllers can use several complicated tools for scanning the vulnerabilities and actively patch these vulnerabilities. Professional controllers can create the tools, code to actively scan vulnerabilities and automatically patch them. Moreover, professional controllers are able to discover unknown vulnerabilities and patch them.

**Table 0.4** Capability level of controllers

Skill level	C (number of patches)
Junior	2352
Senior	866
Professional	318

The capability levels of controllers are shown in **Table 5.4**. They represent the number of methods of existed vulnerability patches. Clearly, these numbers draw on the capability of controllers. Higher skilful controllers will have more ways to patch the security vulnerabilities and the diversity or severity of each vulnerability. There is no official document showing the number of patched vulnerabilities in terms of the capability level of the controller. However, it is assumed that these numbers will be less than the number of exploitations in terms of similar level of attacker capability. For the sake of simulation, the number of patched vulnerabilities is about 80% of the number of attack skill with level matching order. Therefore, the number of ready patches (c) can be 318 for junior, 866 for senior, and 2352 for professional (see **Table 5.4**).

**Table 0.5** The average number of vulnerable patches for each threat

Exploitation for threat	Average # of patches
$E_{T1}$	7193
$E_{T2}$	11953
$E_{T3}$	10872
$E_{T4}$	5593
$E_{T5}$	10872
$E_{T6}$	3729
$E_{T7}$	6649
$E_{T8}$	7109
$E_{T9}$	7458
$E_{T10}$	4600
$E_{T11}$	17145
$E_{T12}$	7458

To obtain the data for total number of patched vulnerability and the removed exploitations (E), it is based on the number of vulnerabilities. Normally, the number of patched vulnerabilities is less than the number of existed vulnerabilities in the CVSS space. After publishing the vulnerabilities, it is about eighty per cent of these vulnerabilities has been the patches. Therefore, **Table 5.5** shows the average number of vulnerable patches for each threat.

## 5.6 Security Threat Model Simulation and Evaluation

In order to validate our security threat model, we select and simulate a generic threat under a particular setting. We study the impact of the variables (attackers' skills, system vulnerabilities, and controllers' skills) on the probability of the existence of a threat and the probability of that threat materialised. For the sake of simulation, we use the values for *T*, *E*, and *V* as shown in table 5.6. *T* is the total number of vulnerabilities published by NVD ( $T=108,898$ ). *E* is the total number of vulnerabilities that have security patches. It is about eighty per cent of *T* ( $E=87,118$ ). *V* is the number of security vulnerabilities of the system and is a simulation variable ranging from 0 to 300. The simulation results for a generic threat with these settings are as follows.

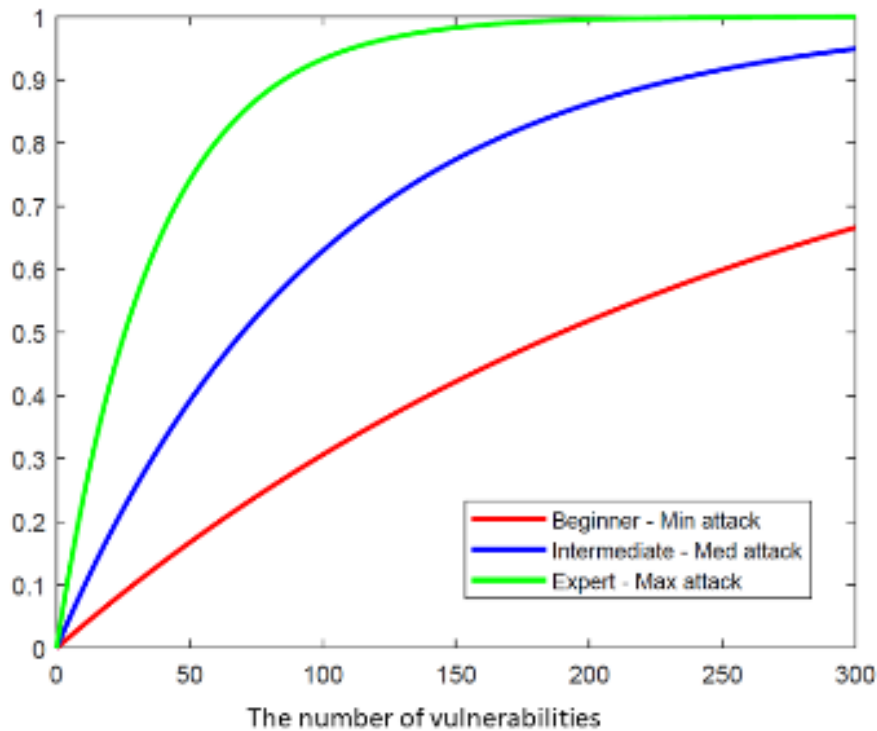
**Table 0.6** The variables for simulation

Variables	Value
T	108,898
E	87,118
V	[0:300]

- The probability of threat existence versus vulnerabilities at different attacker skill levels.

As seen in **Figure 5.8**, as expected, the probability of a threat existence increases with the number of the system vulnerabilities. Regarding the skill levels of the attackers, the higher the level of the attacker skill, the higher the chance of that the threat exists. Specifically, the probability of existence of the threat with respect to the expert-level attacker rises sharply from 0 to 0.94 when the vulnerabilities change from 0 to 100. With

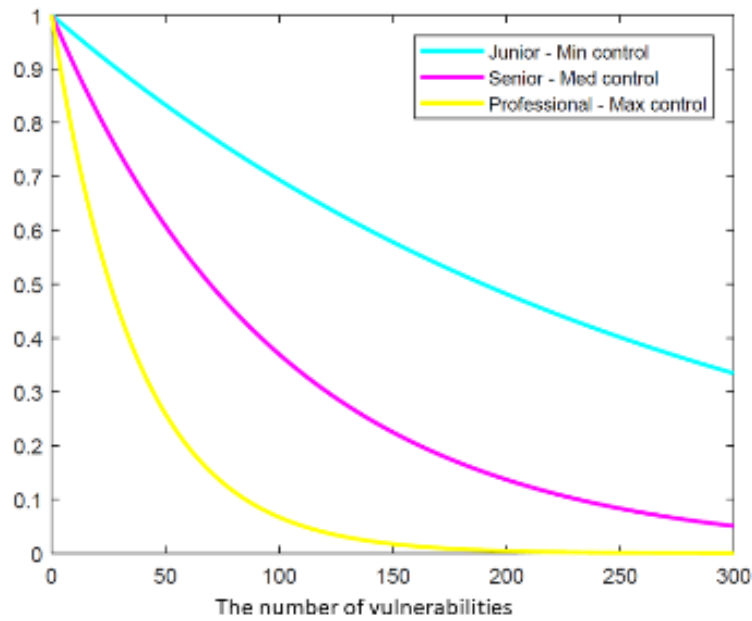
the same change of vulnerabilities from 0 to 100, the threat existence probability for intermediate-level attacker increases at a moderate rate from 0 to 0.6 and for beginner-level attacker it increases at a much lower rate from 0 to about 0.28. Overall, the increase of the probability of threat existence increases with the increase of number of system vulnerabilities and the level of the attacker skill.



**Figure 0.8** The probability of threat existence for various attacker skill levels

- The probability of threat escape given an existing threat versus system vulnerabilities at different controller capability levels.

As seen in **Figure 5.9**, as expected, the probability of a threat escape decreases with an increase in the number of vulnerabilities. When the number of vulnerabilities is 100, the probabilities of threat escape given existing threat for junior, senior, and professional are 0.72, 0.43, and 0.05 respectively. It is clear that the probability of the threat escape is lowest for the most capable controller (at the professional level). Eventually, given an existing threat, the probability of an escaping threat decreases with the increase of number of system vulnerabilities and the level of the controller capability.

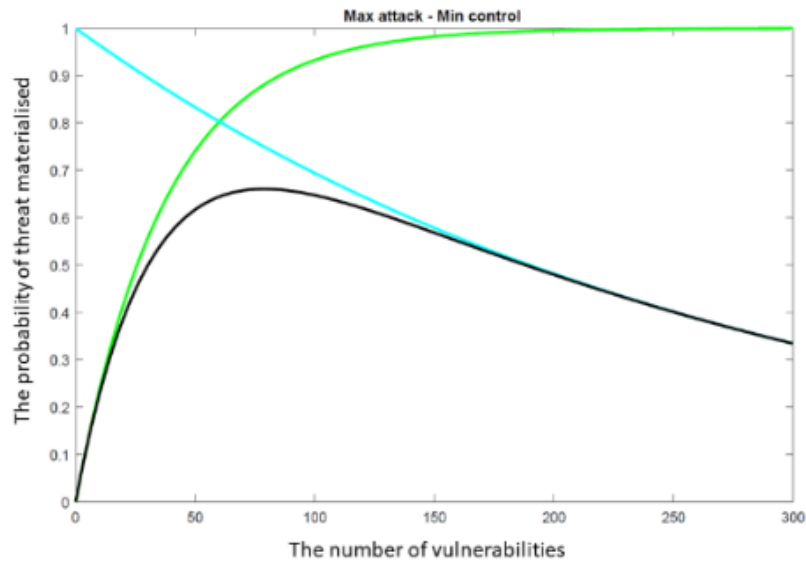


**Figure 0.9** the probability of threat escape given existing threat for various controller capability levels

- The probability of threat materialised (successful attack) given maximum attack skill level and minimum control capability level.

As seen in **Figure 5.10**, given this max-min assumption, the probability of the security threat materialised is shown by the black line for max attack levels and min control capability. Clearly, there exists a maximum value for which an existed threat is materialised when the attacker is most skilful (expert level) and the controller is least capable (junior level). Specifically, the probability of the threat materialised peaks at about 0.66 when the number of vulnerabilities is 80. After that, the probability falls gradually to 0.33 when the number of vulnerabilities reaches 300. Hence, the number of vulnerabilities 80 is the optimal number of vulnerabilities that an attacker can exploit to obtain the maximum of probability of successful attack. This means that if the attack skill level (A), the control capability (C), the total vulnerabilities space (T), and the total patch number (E) are known, the optimal number of vulnerabilities can be calculated using (9).





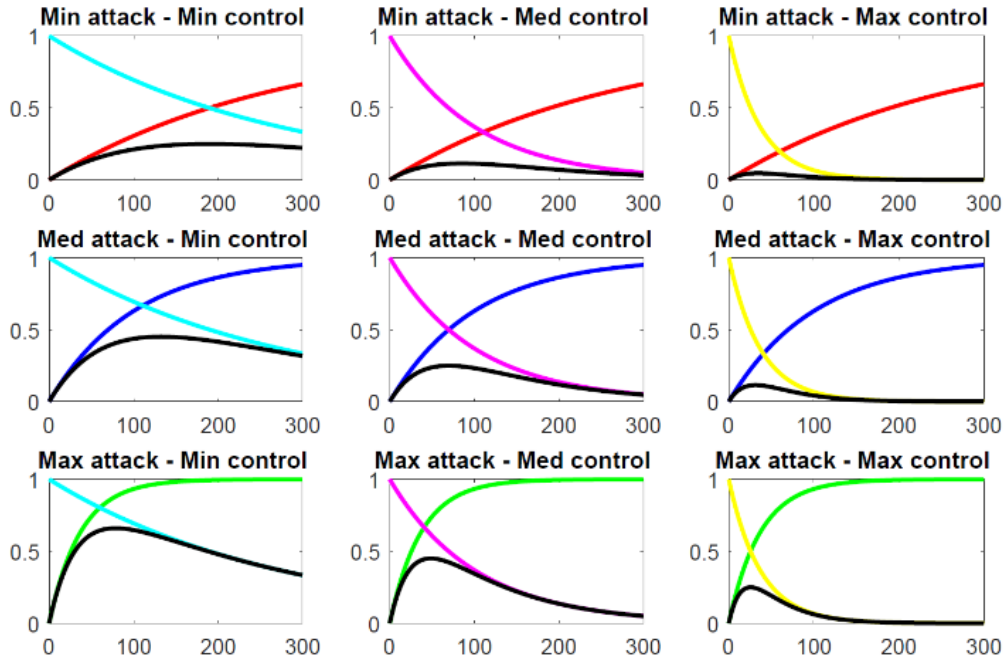
**Figure 0.10** The probability of security materialised (successful attack) with max attack and min control levels

The significance of this number is that in terms of attackers, they can limit the vulnerabilities to exploit to reach the highest successful chance of attack and in terms of controllers, they are aware of the vulnerabilities that attacker can reach the highest probability of successful attack. With this understanding, the controller may devise effective plans to mitigate the attack with measures and/or countermeasures. In conclusion, this investigation reveals that under a specific setting, there exists an optimal number of vulnerabilities that the probability of the threat materialised reaches its peak. Both attackers and controllers can take advantage on this optimal value for their own strategies.

- The probability of security threat materialised (successful attack) for various attacker skill levels and controller capability levels.

As seen in **Figure 5.11**, we consider 9 cases representing attacker skill levels and controller capability levels ranging from lowest to highest. The highest probability of a successful attack is for the case of maximum attack (expert attacker) and minimum control (junior controller) and the lowest is for the case of the minimum attack (beginner attacker) and maximum control (professional controller). The decreasing trend is from left to right as shown in figure 10. This means that at the same attacker skill level if controller capability is higher the probability is lower. On the other hand, the increasing

trend is from top to bottom. This means that at the same controller capability level if attacker skill level is higher the probability will be higher.



**Figure 0.11** The probability of threat materialised (successful attack) for various attacker skill levels and controller capability levels

## 5.7 Cloud Threat Probabilities

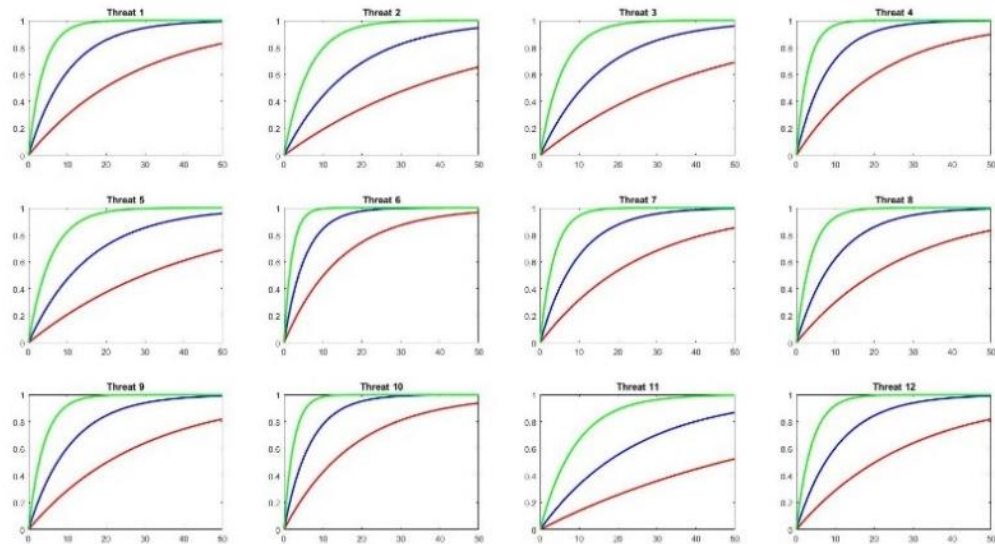
In this section, the security threat model will be applied to the cloud system discussed in section V using the data obtained in section VI. First, probability of threat existence and threat escaped given an existing threat will be compared among various threats. Second, the probability of threat materialised will be presented. Last, the impact of the change of number of total vulnerabilities of each threat on probability of threat materialised will be investigated. For the sake of simulation, we use the values for T,E for each threat in section 6. The number of vulnerabilities of the system ( $V$ ) will be variable from 0 to 50.

- **Probabilities of threat existence and threat escape for various threats**

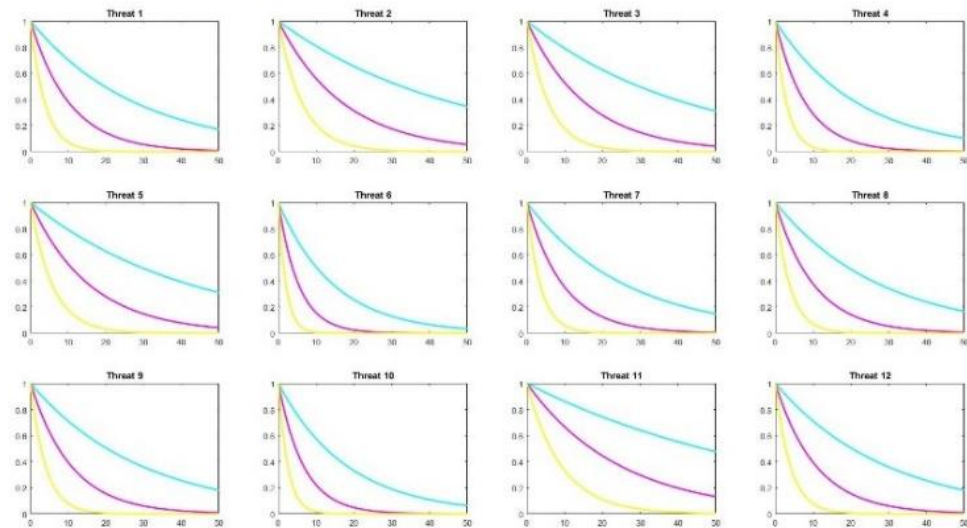
The distribution of the probability of existence for cloud threats 2, 3, 5, and 11 over cloud vulnerabilities is shown in **Figure 5.12**. At any given vulnerability value, the probability of existence of these threats is smaller than that of other threats. This can be explained by the fact that the total number of vulnerabilities ( $T_i$ ) for each of those threats

in the cloud space is higher than for others and hence  $P_{ei}$  for these threats are smaller according to equation (5.7).

It can be seen from **Figure 5.13** that the probability of each of these threats (threats 2, 3, 5, and 11) escaping the security control measures (the number of readily available patches) is higher. According to equation (8) the probability of threat escaping control measures increases with the total number of patches, given the number of patches for this threat remains the same.



**Figure 0.12** The distribution of probability of threat existence for different threats

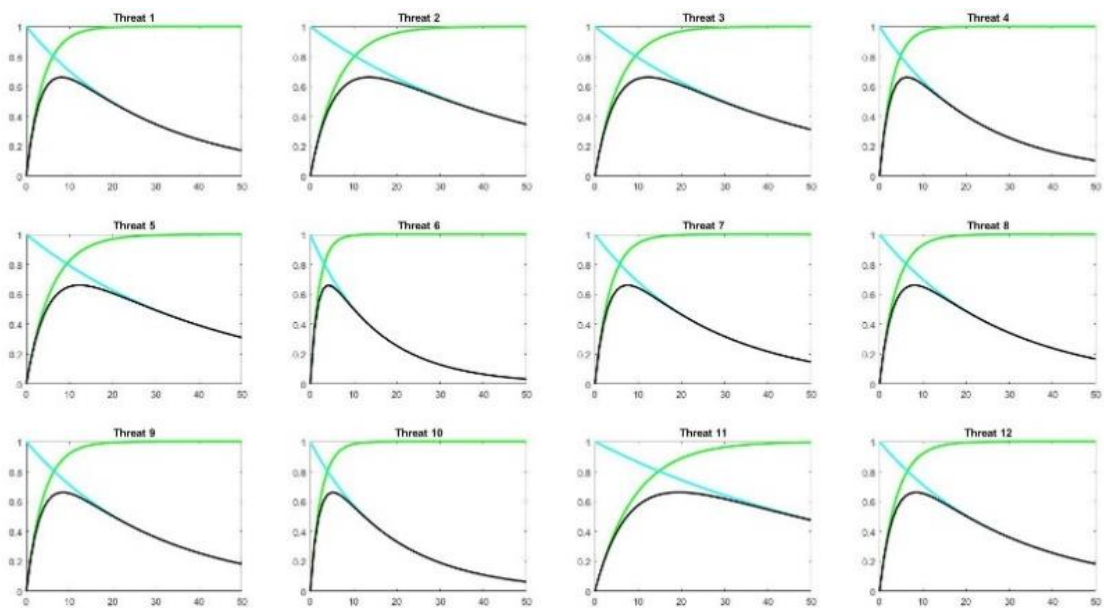


**Figure 0.13** The distribution of probability of escape threat given existing threats

- Probability of security threat materialised

**Figure 5.14** shows the probability distributions of all 12 cloud threats for the max attack and min control case studied earlier. Several points are noted for discussion. First,

the peak points of all these curves have roughly the same value, around 0.66 (from 0.6603 for threat 6 to 0.6610 for threat 8). This is probably from the fact that currently we treat all vulnerabilities in the same way without differentiating their impacts (or weights). This requires further investigation. However, the clear difference among these distributions is the spread of the curve around the peak (or the variance of each threat). It is seen that the variance is larger for higher probability of the materialised threat. It also can be seen from Figure 5.13 that with larger total of vulnerabilities ( $T_i$  for threat 2, 3, 4, and 11), the variance will be larger. This implies that for threats with larger total number of vulnerabilities space ( $T_i$ ) the variance of vulnerabilities is larger, and the probability of threat materialised is higher.



**Figure 0.14** The distribution of probability security threat  
(max attack-min control)

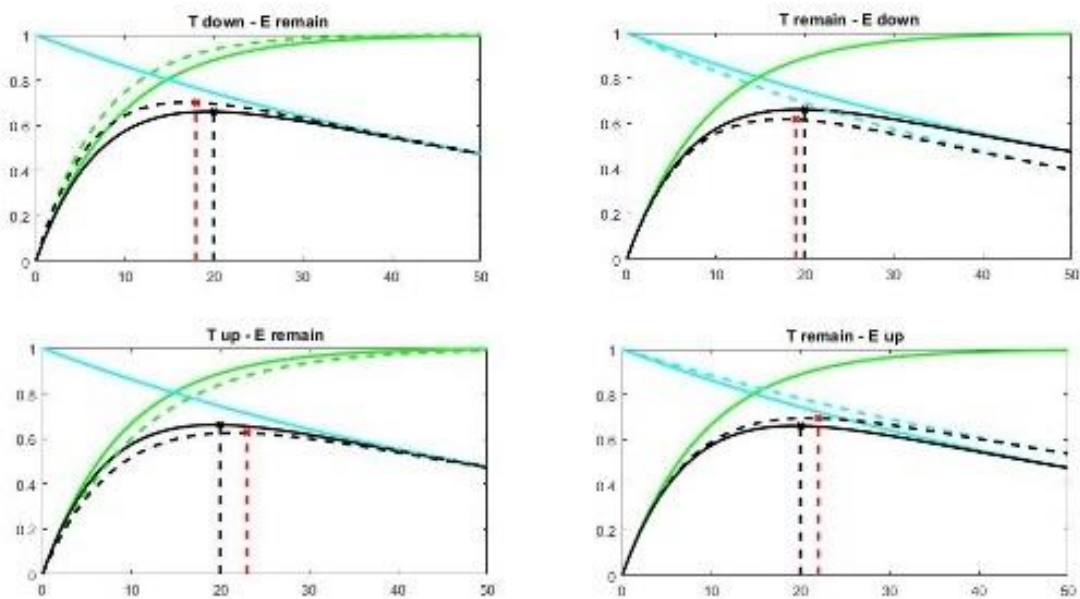
- The impact of  $T$  and  $E$  on the probability of threat materialised

Previous results show how attack skills and control capability levels affect the probability of security threat materialised. This section investigates the impact of the total number of vulnerabilities ( $T_i$ ) and the total number of vulnerabilities having patches ( $E_i$ ).

According to the NVD database, the total number of vulnerabilities changes annually. Overall, this number has increased gradually from 1999 to 2018; however, there were periods where this number decreased. For example, the number fell from 7,946 to 6,484 in 2014-2015 but it increased dramatically from 6,447 to 14,714 in 2016-2017. In this chapter, we will simulate the impact on threat 11 (Denial of Services) by considering 20%

change in the total number of vulnerabilities (T) and the total number of vulnerabilities having patches (E).

**Figure 5.15** shows the distribution of probability of security threat 11 (Denial of Services) for different total number of vulnerabilities ( $T_i$ ) and the total number of vulnerabilities having patches ( $E_i$ ). The black line (basic line) shows the probability distribution with no changes in T and E. The black dotted lines show the equations (9) when there are the changes in T or E. It can be seen that the highest probability of threat materialised is for the case T-down and E-remain. This line shows a peak at 0.722 representing an increase of 9.2% compared with the highest point of the basic line (0.661). Furthermore, the T-remain and E-down case is significant when the peak is at 0.592 representing a decrease of 10.4% compared with the basic line. As mentioned in the section 7, E decreases when the controllers mitigate or reduce the number of vulnerabilities in the system by patches.

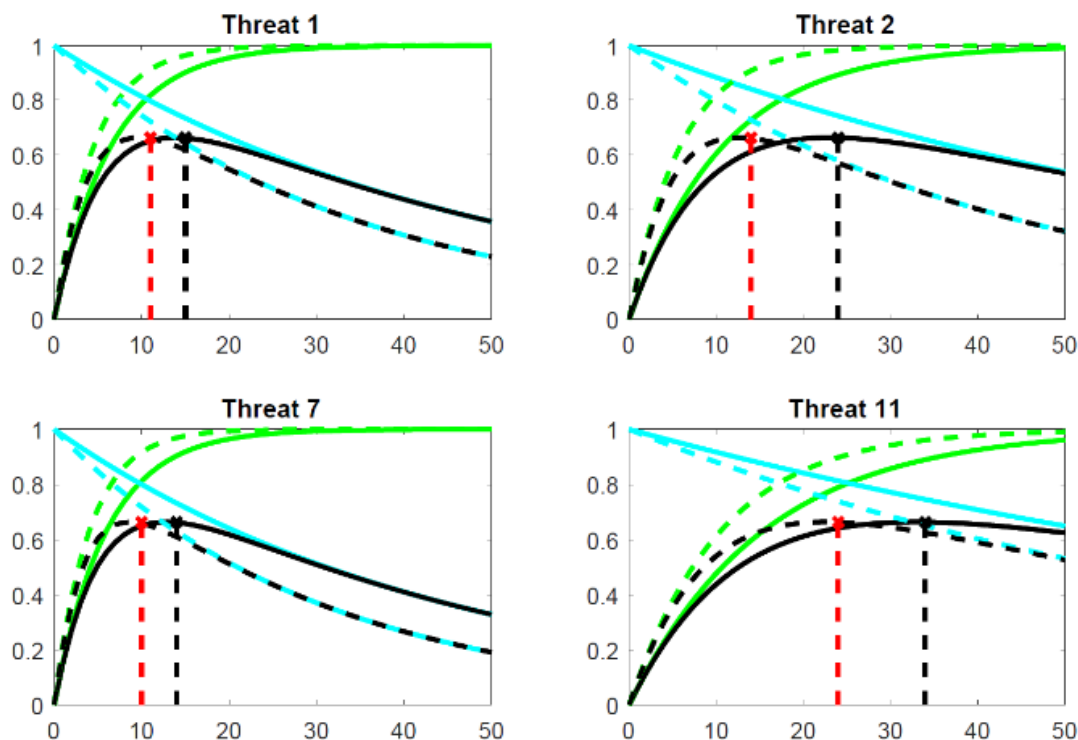


**Figure 0.15** Impact of ( $T_i$ ) and ( $E_i$ ) on the probability of security threat 11 (Denial of Services) materialised

- The impact of removing a type of vulnerabilities on the probability of threat materialised

In this part, we will change the structure of the vulnerabilities to observe how the probability of threat materialised will be affected. We hypothesise that the control system implements security actions to remove all the vulnerabilities related to Insecure interfaces

and APIs (V1). V1 relates to 6 threats including DB (T1), IAM (T2), API (T3), AH (T5), APT (T7), and DOS (T11), in which, threats API (T3) and AH (T5) just contain V1. Therefore, the probability of threat materialised for security threats three and five are zero. Other threats (T1, T2, T7, and T11) will be affected by this change.



**Figure 0.16** The distribution of probability security threat (max attack-min control case) when removing V1

**Figure 5.16** shows the distribution of security threat probability for T1, T2, T7, and T11 when removing V1. The solid black lines show the probability distribution with no changes. The black dotted lines show probability distribution for threats when removing V1 or the number of V1 equals to zero. Overall, when V1 is removed the probability of threat materialised that is affected by V1 will be lower. For example, for threat 2 the highest probability is 0.6638 when  $X=24$ , but the highest probability when removing V1 is 0.6636 when  $X=14$  (the red dotted line). Thus, the peak of probability of threat materialised does not change much. However, there is a big variation after the maximum point (when  $X=24$ ). We calculate at the point  $X=30$  (the number of vulnerabilities in the in the system is 30). The probability of threat 2 is 0.6514 (the solid black line) and the probability of threat 2 when removing V1 is 0.514 (the dotted black line). Hence, the probability of security threat 2 reduced by 21% compared with the state of not removing

V1. Another significant point to note is that the variance of the probability of threat materialised is also smaller when removing V1.

## **5.8 Summary**

Computation of probability of security threat is important in determining security risk and security management of a system. However, the result is far from satisfactory because of different organisations with loosely defined concepts of security threat and hence loose estimation of an attack chance. The chapter proposed a new security threat model with a comprehensive view that includes security factors like attackers, attack methods, period of time of attacks, security components, vulnerabilities, and controllers. The chapter also introduced a new method for quantifying security threat and applied it to the cloud computing scenario. This measure of security threat probability will be applied to the measure of security cost for individual stakeholders in the organisation and for security management in Chapter 8.

# Chapter 6

## A Skill-based Attack-control Security Threat Model and Its Application to Cloud

### 6.1 Introduction

In the previous Chapter, we proposed a security threat model with a threat space to identify the relationship between attack conditions and vulnerable systems. Furthermore, the model included the materialised threats to identify the control factors that deal effectively with security threats. However, the method to determine the skill levels of attackers and controllers is empirical and subjective. There, we used empirical data to assign the skill level of attackers based on the number of exploitations and the capability of controllers based on the number of security vulnerability patches. These considerations motivate us to search for a new security threat model that addresses these weaknesses. In this chapter, we will introduce an innovative security threat model (a skill-based attack-control security threat model) that quantifies the skill levels of attackers and controllers quantitatively.

Based on the proposed model, several concepts about probability of the attack process will be introduced including probability that the attackers are capable of exploiting security vulnerabilities, probability that a security vulnerability exists, probability that the controllers are capable of mitigating vulnerabilities. Then, the computation of probability of security threat existed and materialised will be described. We will validate and evaluate the proposed model by applying it to address cloud computing security.

The remainder of the chapter is organised as follows. Section 6.2 proposes a skill-based attack-control security threat model with two processes. Section 6.3 describes the



mathematical methods to quantify the probability that attackers exploit security vulnerabilities. Section 6.4 expresses the proposed threat model which will be applied to cloud computing. In particular, we will describe the method to compute the probability that controllers cover security vulnerabilities then showing the formula about the probability of existed and undetected security threats to form the general formula of the probability that a security threat materialised into attacks. Section 6.5 provides the methods to obtain the data to quantify the probability of materialised security threats. Then it describes the validation and evaluation of the proposed model to cloud security threats. Finally, section 6.6 concludes the chapter.

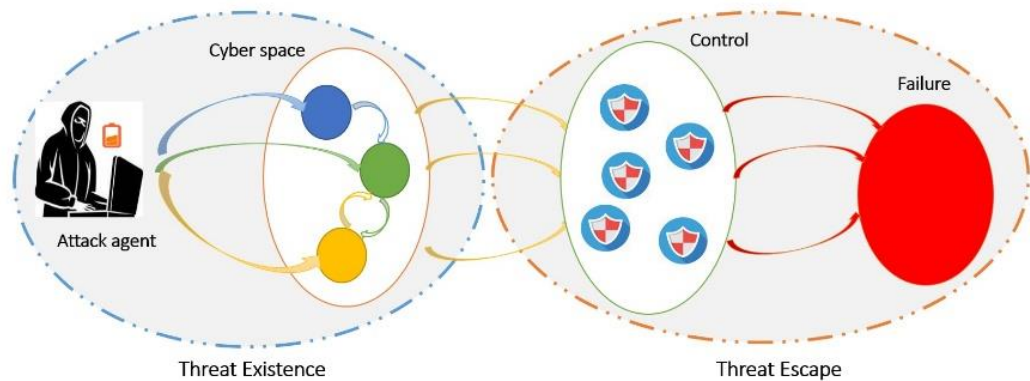
## 6.2 Modelling a Skill-based Attack-control Security Threat

We propose a security threat model that focuses on quantifying the skills of attackers and the capabilities of controllers in the relationships with security vulnerabilities within a security threat.

In previous chapter (Chapter 5), we investigated a security threat is the study of the relationship among security factors including attackers, attack conditions, vulnerabilities, controllers, trigger conditions over a cyber space. We also introduced a security threat model consisting of two phases that described the relationships between attackers, security vulnerabilities, and controllers. We use search theory to quantify the probability of a security threat existed and a security threat materialised. However, we considered the skill of attackers and the capability of controller somewhat qualitatively. That is, we used empirical data to quantify the number of exploitations for determining the attacker skill level and the number of security vulnerability patches for deciding the controller capability level. In this chapter we focus on a probabilistic approach to quantify the skill of attackers and the capability of controllers.

Our novel security threat model is illustrated in **Figure 6.1**. It simulates a real attack processing through two processes. We call the first named the skill-based attack and the second named the skill-based control. In the skill-based attack process, the attacker will find the exploitations to match with the security vulnerabilities existing in the system. We consider the probability that a security vulnerability exists in the system. Therefore, the existing threat will include the chance that the attacker's capability matches with the security vulnerabilities and the chance that security vulnerabilities exist. However, to

materialise the existing threat into attacks, attackers are undetected by security controllers. This is the process named skill-based control threat.



**Figure 0.1** Skill-based attack-control security threat model

### 6.2.1 Skill-based Attack Process

The aim of this process is to investigate the favourable needs for a security threat existed and to quantify the probability of this existence.

Considering a cyber system with several known security vulnerabilities, if no attacker is available and interested in attacking the system, security threats are considered non-existence as the probability of an attack is close to zero. On the other hand, if there exist attackers who are able to exploit any system security vulnerabilities, but the system is well protected with hardly any security vulnerabilities, security threats are also considered not existed. With this observation, the existence of a security threat entails two security factors: the attackers who have capabilities to exploit the security vulnerabilities of a system and the security vulnerabilities that have already existed in the system. It should be noted that other security factors may also be involved in the existence of a security threat such as opportune timing, available technologies and resources, and other favourable environmental conditions. However, in this study we focus mainly on the relationship between attack-skills and security vulnerabilities. Thus, the probability of existence of a security threat depends on the probability that security vulnerabilities exist in the system and the attacker skill levels (also in terms of probability) in exploiting the vulnerabilities.

In **Figure 6.2**, we model the security threat existed phase based on two main elements including attacker skills and security vulnerabilities. For the cyber system, each circle represents a security threat. Each security threat is composed of one or many security

vulnerabilities. Between security threats, there may be overlaps. This means that a security vulnerability may exist in several security threats. For the attacker, the skill of an attacker group is the number of attackers handling the security vulnerabilities of the system. This will be expressed comprehensively in section 6.3. Therefore, the chance of security threat existence is quantified by the simultaneous existence of two elements: the probability that attackers exploit security vulnerabilities and the chance that security vulnerabilities exist.

We can mathematically express the probability of the existence of a threat (Threat 1 for example) as follows.

$$P_{E_1} = P_{H_1} * P_{V_1} * P_{V_2} * P_{V_3} \quad (6.1)$$

where,  $P_{H_1}$  is the probability that attackers exploit the security vulnerabilities of the system. This will be computed by the formula in the figure that we will solve in section 6.3. The probability of existed security vulnerabilities is expressed by  $P_{V_1}, P_{V_2}, P_{V_3}$ .

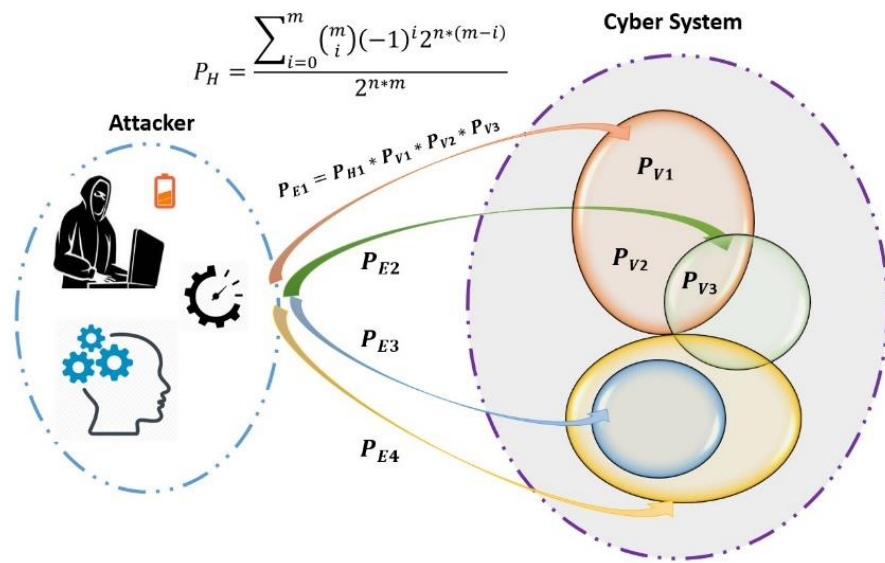


Figure 0.2 Attack process

## 6.2.2 Skill-based Control Process

In the skill-based control process, we investigate security factors including system conditions, controllers, and their relationship. This relationship provides a clear understanding of how existing threats are materialized into successful attacks. As illustrated in **Figure 6.3**, the cyber system embraces existed security threats from the first process (the

skill-based attack process). The control system contains the security control/defence measures including attack countermeasure, vulnerability mitigation, security policy, etc. The process of moving from the state where an existence of a threat has been established to the system failure state (the threat materialised) depends on the control measures and capability of the controller. In general, this process depends not only the control measures exercised by the controller but also on other favourable conditions to the attackers such as timing and environment. We restrict ourselves to the security controller and its capability in mitigating the vulnerabilities of the existed threat. We consider this a skill-based control process.

With this assumption, matching the capability of the controller to the vulnerabilities involved in the existed threat is similar to matching the collective capability of the attackers to the threat vulnerabilities the attackers can exploit. Let  $P_C$  be the probability that the controller can mitigate the threat vulnerabilities and  $P_U$  the probability that the existing threat avoids the control measure.  $P_U$  can also be considered as or equivalent to the probability that the existed threat is undetected by the controller; it can be expressed as follows.

$$P_U = 1 - P_C \quad (6.2)$$

Consequently, the probability of a materialised security threat is given by (6.3). It is the product to the probability that a given threat exist and the probability that controllers uncover or miss the existing threat:

$$P_T = P_E * P_U \quad (6.3)$$

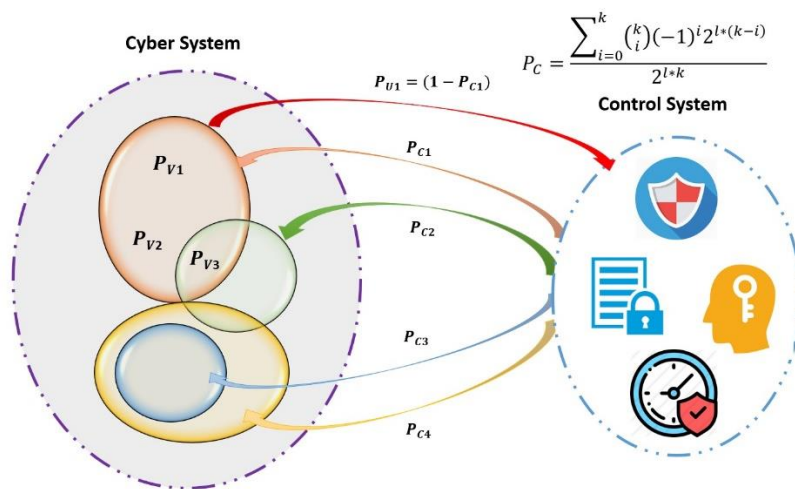


Figure 0.3 Control process

## 6.3 Quantifying Probability Attackers are Capable of Exploiting Vulnerabilities

As investigated above, to quantify the probability of a materialised threat, the probability of security threat existed and undetected have to be computed. To calculate these kinds of probability, we quantify the chance that attackers can exploit security vulnerabilities ( $P_H$ ) and the likelihood that controllers cover or mitigate security vulnerabilities ( $P_C$ ). In this section, we propose a method to compute  $P_H$ , and  $P_C$ .

In Chapter 5, to obtain the data for the skill of attackers, we used empirical data to determine the level of attacker's skill based on the number of exploitations of security vulnerabilities. This method to get the data was quite arbitrary and qualitative. Therefore, we propose the model to quantify the skill of attackers through solving the problem that  $n$  attackers can exploit  $m$  security vulnerabilities. Consider an attacker group with the intention to attack the system. We assume that the system operates under a threat constituted by  $m$  known vulnerabilities. We also assume that the capability of the attacker group is the ability of the group collectively to attack all  $m$  vulnerabilities of the threat. The attacker's capability is represented by: (1) the number of attackers  $n$ ; (2) each attacker member of the group can exploit 0, 1, 2, 3, ... or all  $m$  vulnerabilities of the system.

The problem is to determine the probability of the group on  $n$  attackers can collectively attack  $m$  vulnerabilities associated with a particular threat of a system. *This probability is a measure of the skill level of the attacker group.*

From the above explanation, we propose the mathematic problem and solve it to find the probability that attackers can exploit vulnerabilities as follows.

### **Theorem 6.1:**

Given  $n$  attackers and  $m$  vulnerabilities that each of the attackers may be able to exploit zero, one or more vulnerabilities (up to  $m$ ), the probability, which  $n$  attackers collectively may exploit  $m$  vulnerabilities, is expressed as follows.

$$P_{nm} = \frac{(2^n - 1)^m}{2^{n*m}} \quad (6.4)$$

**Proof:** We will introduce several simple cases to identify how to quantify the probability that one, two, or three attackers exploit from one, two, three security vulnerabilities. Subsequently, general case two attackers exploit  $m$  vulnerabilities will be

described. Finally, two mathematical approaches including combinations and inclusion-exclusion principle will be investigated to tackle the general case with  $n$  attackers exploit  $m$  vulnerabilities.

### 6.3.1 Simple Cases

We have  $n$  attackers and  $m$  vulnerabilities, the question is how many ways to let  $n$  attackers exploit all  $m$  vulnerabilities, given that each attacker can cover one or many vulnerabilities or cannot exploit any vulnerabilities, many attackers can take over the same vulnerability.

Let us consider a binary matrix  $P$  size  $n \times m$  that represents  $n$  attackers and  $m$  vulnerabilities, each entry of the matrix shows whether or not one security-vulnerability is exploited by a particular attacker.

$$P(i,j) = \begin{cases} 0, & \text{If attacker } A_i \text{ does not handle } V_j \\ 1, & \text{If attacker } A_i \text{ handle } V_j \end{cases}$$

$$P = \begin{bmatrix} 0 & 1 & \dots & P_{1j} & \dots & 1 & 0 \\ 0 & 0 & & \dots & & 0 & 0 \\ \vdots & \vdots & & \dots & P_{ij} & \dots & \vdots \\ 0 & 1 & & \dots & & 1 & 1 \\ 0 & 0 & & \dots & & 0 & 1 \end{bmatrix}$$

Therefore, we have the vector  $M_{1j}$  representing attacker 1 cover which vulnerability in  $m$  vulnerabilities. If  $M_{1j} = 1$ , this means that attacker 1 exploits the vulnerability  $j^{th}$ .

#### **Case 1: $n=1, m=1$ ; one attacker exploits 1 vulnerability**

We have a matrix  $M$  with only one entry.  $M_{11} = 1$  means the attacker exploits one vulnerability. This is the only case satisfying the conditions of the problem. Therefore, the probability that an attacker covers one vulnerability is  $\frac{1}{2}$ . This is because we have 2 possible chance of the 1 entry matrix is either 0 or 1. Table below shows the how matrix  $M$  satisfying the conditions of the above mathematical problem. The first column shows the number of vulnerabilities covered by the first attacker. The second column shows the vector  $M_{1j}$ . The last column shows the number of correct choices that attacker 1 cover 1 vulnerability.

# of vulnerabilities covered by the first attacker	Attacker 1	# of correct choices
1	1	1
Total number of correct choices		<b>1</b>
Possible outcome		2
Probability		$\frac{1}{2}$

**Case 2:  $n=1, m=2$ ; one attacker exploits 2 vulnerabilities**

We have 4 possible ways: 00, 01, 10, 11 for one attacker covers 2 vulnerabilities. We have only one way that satisfies the conditions is 11. So, we have the probability  $\frac{1}{4}$

# of vulnerabilities covered by the first attacker	Attacker 1	# of correct choices
1	11	1
Total number of correct choices		1
Possible outcome		4
Probability		$\frac{1}{4}$

**Case 3:  $n=2, m=1$ ; two attackers exploit 1 vulnerability**

For visualizing, we represent in the table below how two attackers exploit one vulnerability. The first column shows the number of vulnerabilities covered by the first attacker. If the first attacker does not cover any vulnerability, then the second attacker must cover the vulnerability (showing the second row of the table).

# of vulnerabilities covered by the first attacker	Attacker 1	Attacker 2	# of correct choices
0	0	1	1
1	1	0, 1	2
Total number of correct choices			3
Possible outcome			4
Probability			$\frac{3}{4}$

**Case 4:  $n=2, m=2$ ; two attackers exploit 2 vulnerabilities**

Similarly, the table below shows how two attackers cover 2 vulnerabilities. Therefore, we have 9 correct choices. The probability is  $\frac{9}{16}$ .

# of vulnerabilities covered by the first attacker	Attacker 1	Attacker 2	# of Correct choices
0	00	11	1
1	01	10, 11	2
	10	01, 11	2
2	11	00, 01, 10, 11	4
Total number of correct choices			9
Possible outcome			16
Probability			$\frac{9}{16}$

**Case 5:  $n=2, m=3$ ; two attackers exploit 3 vulnerabilities**

The table below shows how two attackers cover three vulnerabilities. Therefore, we have 27 correct choices. The probability is  $27/64$ .

# of vulnerabilities covered by the first attacker	Attacker 1	Attacker 2	# of Correct choices
0	000	111	1
1	001	110, 111	2
	010	101, 111	2
	100	011, 111	2
2	011	100, 101, 110, 111	4
	101	010, 011, 110, 111	4
	110	001, 011, 101, 111	4
3	111	000, 001, 010, 100, 011,	8
Total number of correct choices			27
Possible outcome			64
Probability			$27/64$

**Case 6:  $n=3, m=2$ ; three attackers exploit two vulnerabilities**

The table below shows how three attackers cover two vulnerabilities. Therefore, we have 49 correct choices. The probability is  $49/64$ .

# of vulnerabilities covered by the first attacker	Attacker 1	Attacker 2	Attacker 3	# of Correct choices
0	00	00	11	1
		01	10, 11	2
		10	01, 11	2
		11	00, 01, 10, 11	2
1	01	00	10, 11	2
		01	10, 11	2
		10	00, 01, 10, 11	4
		11	00, 01, 10, 11	4
	10	00	01, 11	2
		01	00, 01, 10, 11	4
		10	01, 11	2
		11	00, 01, 10, 11	4
2	11	00, 01, 10, 11	00, 01, 10, 11	16
Total number of correct choices				49
Possible outcome				64
Probability				$49/64$

**Case 6:  $n=3, m=3$ ; three attackers exploit three vulnerabilities**

The table below shows how three attackers exploit three vulnerabilities. Therefore, we have 343 correct choices. The probability is  $343/512$ .



# of vulnerabilities covered by the first attacker	Attacker 1	Attacker 2	Attacker 3	# of Correct choices
0	000	2 attackers cover 3 vulnerabilities (from previous case with $n=2$ , $m=3$ )		27
1	001	2 attackers cover 2 vulnerabilities (9 correct choices from previous case with $n=2$ , $m=2$ ). The last digits of 2 attackers can be 0 or 1 so we have 4 times of 9 ways.		4*9
	010	Similar above explanation		4*9
	100	Similar above explanation		4*9
2	011	2 attackers cover 1 vulnerability (3 correct choices from previous case with $n=2$ , $m=1$ ). The last 2 digits of 2 attackers can be 0 or 1 so we have 16 times of 3 ways		16*3
	101	Similar above explanation		16*3
	110	Similar above explanation		16*3
3	111	2 attackers should be any		64
Total number of correct choices				<b>343</b>
Possible outcome				512
Probability				343/512

- General formula for the case  $n=2$  and  $m=m$ : two attackers cover  $m$  vulnerabilities

# of vuls covered by 1 <sup>st</sup> attacker	Attacker 1	Number $\binom{m}{i}$	# of vuls covered by 2 <sup>nd</sup> attacker	Attacker 2	Number $2^i$	# of Correct choices
0	00..00	$\binom{m}{0}$	$m$	11..11	$2^0$	$\binom{m}{0} * 2^0$
1	00..01	$\binom{m}{1}$	$m - 1$	11...10, 11...11	$2^1$	$\binom{m}{1} * 2^1$
	00..10		$m - 1$	11..01, 11...11	$2^1$	
	...		$m - 1$	....	$2^1$	
	00...1..0		$m - 1$	11.. 0..1, 11...11	$2^1$	
	...		$m - 1$	...	$2^1$	
	10..00		$m - 1$	01..11, 11...11	$2^1$	
2	00..11	$\binom{m}{2}$	$m - 2$	11..00, 11...01, 11...10, 11...11	$2^2$	$\binom{m}{2} * 2^2$
	00..110		$m - 2$	11..001, 11...011, 11...101, 11...11	$2^2$	
	...		$m - 2$	....	$2^2$	
	00..11..00		$m - 2$	11.. 00..11, 11...01...11, 11...10...11, 11...11	$2^2$	
	...		$m - 2$	...	$2^2$	
	11..00		$m - 2$	00..11, 01...11, 10...11, 11...11	$2^2$	
...	...	...	...	...	...	...
i	...	$\binom{m}{i}$	$m - i$	...	$2^i$	$\binom{m}{i} * 2^i$
...	...	...	...	...	...	...
m	11..11	$\binom{m}{m}$	0	Any vector $M_{2j}, j \in (0, m)$	$2^m$	$\binom{m}{m} * 2^m$
<b>Total</b>						$\sum_{i=0}^m \binom{m}{i} 2^i$
<b>All space</b>						$2^{2*m}$
<b>Probability</b>						$\frac{\sum_{i=0}^m \binom{m}{i} 2^i}{2^{2*m}}$

### 6.3.2 Method 1: Using Combination Theory

**Theorem 6.2:**

The general formula for n attackers covering m vulnerabilities is

$$W = (2^n - 1)^m \quad (6.5)$$

**Proof:**

Let us consider the first column of the matrix P; it is column vector  $P_{i1}$ , in which  $i \in (1, n)$ . This vector  $P_{i1}$  represents whether or not  $V_1$  is exploited. It is clear that if at least  $\exists i$  makes  $P_{i1} = 1$ , that means at least the first vulnerability is exploited by attacker  $i^{th}$ . So, the question is how many ways ( $W_1$ ) to choose that makes  $V_1$  exploited. This number is  $W_1 = (2^n - 1)$ , because we have  $2^n$  different ways to form vector  $P_{i1}$ . Then we only remove the case vector  $P_{i1}$  is vector zero. This means that the value of all entries of the vector  $P_{i1}$  is zero.

$$P = \begin{matrix} & V_1 & V_2 & \dots & V_m & \\ \begin{bmatrix} 0 & 1 & \dots & P_{1j} & \dots & 1 & 0 \\ 0 & 0 & \dots & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \dots & P_{ij} & \dots & \vdots & \vdots \\ 0 & 1 & \dots & \dots & \dots & 1 & 1 \\ 0 & 0 & \dots & \dots & \dots & 0 & 1 \end{bmatrix} & A_1 \\ & & & & & & A_2 \\ & & & & & & \vdots \\ & & & & & & A_n \end{matrix}$$

Similarly, considering the second column of the matrix P, it is  $P_{i2}$ . We also have  $W_2 = (2^n - 1)$  different ways to make  $V_2$  exploited by at least one attacker.

To make two vulnerabilities  $V_1$  and  $V_2$  exploited by n attackers we have the number of different ways is  $W_{12} = W_1 * W_2 = (2^n - 1)^2$ .

Considering the  $j^{th}$  column of the matrix P, it is  $P_{ij}$ . We also have  $W_j = (2^n - 1)$  different ways to make  $V_j$  exploited by at least one attacker.

Considering the  $m^{th}$  column of the matrix P, it is  $P_{im}$ . We also have  $W_m = (2^n - 1)$  different ways to make  $V_m$  exploited by at least one attacker.

Therefore, to make  $m$  vulnerabilities  $V_1, V_2, V_3, \dots, V_{m-1}, V_m$  exploited by  $n$  attackers we have the number of different ways is as follows

$$W = W_1 * W_2 * \dots * W_j * \dots * W_m = (2^n - 1)^m \quad (6.6)$$

We have  $2^{n*m}$  ways to form the matrix  $P$ .

Therefore, the probability that  $n$  attackers exploit  $m$  vulnerabilities is calculated by the following formula

$$P_{nm} = \frac{(2^n - 1)^m}{2^{n*m}}$$

Let us test this formula for several above cases. We have exactly the same results.

$$\text{With } n = 2, m = 2, \text{ using (3) we have } P_{22} = \frac{(2^2 - 1)^2}{2^{2*2}} = \frac{9}{16}$$

$$\text{With } n = 2, m = 3, \text{ using (3) we have } P_{23} = \frac{(2^2 - 1)^3}{2^{2*3}} = \frac{27}{64}$$

$$\text{With } n = 3, m = 2, \text{ using (3) we have } P_{32} = \frac{(2^3 - 1)^2}{2^{3*2}} = \frac{49}{64}$$

### 6.3.3 Method 2: Using Inclusive-Exclusive Principle

Our problem is re-stated as all  $m$  vulnerabilities are exploited by  $n$  attackers (intersections of  $m$  vulnerabilities are exploited) is equal all space of matrix  $P$  minus  $m$  vulnerabilities are not exploited by any attackers (the union of  $m$  vulnerabilities are not exploited).

So, instead of finding the possible ways that  $m$  vulnerabilities are exploited by  $n$  attackers, we find the possible ways (the cardinalities) that  $m$  vulnerabilities are not exploited by any attackers.

Denote  $S$  is the space of matrix  $P$  with all possible. Therefore, the cardinality of space  $S$  is  $2^{n*m}$ .

Denote  $V_1$  is the cardinalities that the first vulnerability is exploited, so  $\bar{V}_1$  (the complement of  $V_1$ ) is the cardinalities that the first vulnerability is not exploited by any attackers.

Denote  $V_2$  is the cardinalities that the second vulnerability is exploited, so  $\bar{V}_2$  is the cardinalities that the second vulnerability is not exploited by any attackers.

Similarly, denote  $V_j$  is the cardinalities that the  $j^{th}$  vulnerability is exploited, so  $\bar{V}_j$  is the cardinalities that the  $j^{th}$  vulnerability is not exploited by any attackers.

Denote  $V_m$  is the cardinalities that the  $m^{th}$  vulnerability is exploited, so  $\bar{V}_m$  is the cardinalities that the  $m^{th}$  vulnerability is not exploited by any attackers.

So the problem is represented by De Morgan's laws [122]; we have

$$W = \left| \bigcap_{j=1}^m V_j \right| = \left| S - \bigcup_{j=1}^m \bar{V}_j \right|$$

This means that the cardinality of all  $m$  vulnerabilities are handled by  $n$  attackers (the intersections of  $m$  vulnerabilities are exploited by  $n$  attackers) is equal to all space  $S$  minus the cardinality of the union of  $m$  vulnerabilities unexploited.

$$\left| S - \bigcup_{j=1}^m \bar{V}_j \right| = |S| - \sum_{j=1}^m |\bar{V}_j| + \sum_{1 \leq j < l \leq m} |\bar{V}_j \cap \bar{V}_l| - \dots + (-1)^m |\bar{V}_1 \cap \dots \cap \bar{V}_m| \quad (6.7)$$

$\sum_{j=1}^m \bar{V}_j$  means the cardinality that any vulnerability is not exploited by  $n$  attackers. Let consider the first vulnerability is not exploited by any attackers in the matrix  $P$  below, we find that the column vector  $P_{i1}$  is zero vector, we have  $2^{n*(m-1)}$  possible ways for any  $(m-1)$  vulnerabilities remain with any attackers. Therefore, we have  $\binom{m}{1} * 2^{n*(m-1)}$  ways to choose any vulnerability is not exploited by any attackers.

$$P = \begin{array}{cccccc} & V_1 & V_2 & \dots & & V_m & \\ \left[ \begin{array}{cccccc} 0 & 1 & \dots P_{1j} \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \dots P_{ij} \dots & \vdots & \vdots \\ 0 & 1 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{array} \right] & \begin{array}{c} A_1 \\ A_2 \\ \vdots \\ A_n \end{array} \end{array}$$

Similarly, we have  $\binom{m}{2}$  pair of vulnerabilities are not exploited by any attackers. For each pair of vulnerabilities, we have  $2^{n*(m-2)}$  possible ways to choose (m-2) vulnerabilities remain with any attackers.

$$P = \begin{matrix} & V_1 & V_2 & \dots & V_m & & \\ \begin{bmatrix} 0 & 0 & \dots & P_{1j} & \dots & 1 & 0 \\ 0 & 0 & \dots & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \dots & P_{ij} & \dots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & 1 & 1 \\ 0 & 0 & \dots & \dots & \dots & 0 & 1 \end{bmatrix} & A_1 \\ & & & & & & A_2 \\ & & & & & & \vdots \\ & & & & & & A_n \end{matrix}$$

For choosing  $i$  vulnerabilities, we have  $\binom{m}{i}$  ways to choose  $i$  vulnerabilities are not exploited by any attackers. For each of these, we have  $2^{n*(m-i)}$  possible ways to choose (m-i) vulnerabilities remain with any attackers.

Thus, (4) will be expressed by

$$\left| S - \bigcup_{j=1}^m \bar{V}_j \right| = \binom{m}{0} 2^{n*m} - \binom{m}{1} 2^{n*(m-1)} + \binom{m}{2} 2^{n*(m-2)} - \dots + \binom{m}{i} (-1)^i * 2^{n*(m-i)} - \dots + \binom{m}{m} (-1)^m * 2^0 = \sum_{i=0}^m \binom{m}{i} (-1)^i * 2^{n*(m-i)}$$

Hence, the cardinality of all  $m$  vulnerabilities are handled by  $n$  attackers will be computed by

$$W = \sum_{i=0}^m \binom{m}{i} (-1)^i * 2^{n*(m-i)} \quad (6.8)$$

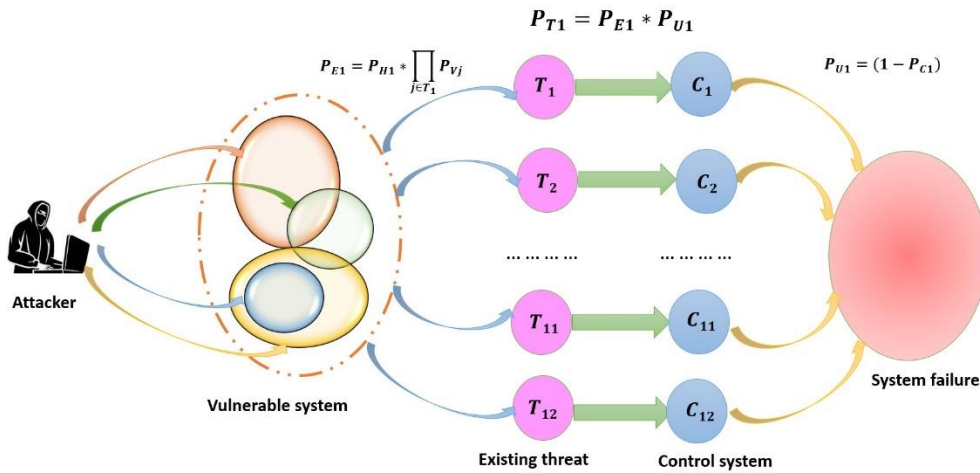
We find that this result is exactly equal to the consequence in (2) by expanding The Binomial Theorem Using Factorial Notation

$$W = \sum_{i=0}^m \binom{m}{i} (-1)^i * 2^{n*(m-i)} = (2^n - 1)^m \quad (6.9)$$

As a result, the probability that  $n$  attackers exploit  $m$  vulnerabilities is the same as (6.4).

## 6.4 Applying the Proposed Threat Model to Cloud Computing

As seen in **Figure 6.4**, we demonstrate the application of the proposed model above to cloud computing. It is assumed that attackers exploit security vulnerabilities of the cloud system. In the cloud system, there exists twelve security threats (see **Table 4.1** in Chapter 4). Each security threat embraces a number of security vulnerabilities. In this chapter, we just focus on how each security threat impacts on the system. Realistically, there may exist a relationship between cloud security threats. Therefore, we will have twelve different security attack paths. After the process that attacker's capability matches with the security vulnerabilities, the cloud system exists a security threat. Thus, there exists a probability of an existed security threat named  $P_E$ . To make the system failure, attackers have to overcome the monitor of controllers. There exists the chance that an event is undetected by controllers calling  $P_U$ . Therefore, the probability of a security threat materialised into attacks ( $P_T$ ) is the product of the probability of an existed threat ( $P_E$ ) and the probability of an undetected threat ( $P_U$ ). We will describe the method to compute these above probabilities ( $P_E, P_U, P_T$ ) in the following parts.



**Figure 0.4** Skill-based attack-control threat model applied to cloud computing

### 6.4.1 Probability of a Cloud Existed Security Threat

As seen in **Figure 6.5**, in existed threat process, attackers can exploit one or more various security vulnerabilities that categorise different security threats, to build distinct forms of attacks. In this process, it is important to identify the security vulnerabilities and security threats in cloud computing. In chapter 5, we analysed the relationships between seven kinds of cloud security vulnerabilities and twelve security threat categories. As a result, a vulnerability may play a role in several security threats, while a security threat may contain several vulnerabilities.

As investigated in section 6.3, the probability of a cloud existed security threat is the product of the probability that attackers exploit vulnerabilities and the probabilities of each vulnerabilities existed within the cloud security threat. Therefore, according to (6.1), we derive the formula to calculate the probability of each cloud existed security threat as follows

$$P_{E_i} = P_{H_i} * \prod_{j \in T_i} P_{V_j} \quad (6.10)$$

From section 6.3, we can quantify the probability that attackers exploit vulnerabilities for each security threat  $P_{H_i}$  as follows

$$P_{H_i} = \frac{\sum_{p=0}^m \binom{m}{p} (-1)^p 2^{n*(m-p)}}{2^{n*m}} \quad (6.11)$$

Therefore,  $P_{E_i}$  will be computed by the formula:

$$P_{E_i} = \frac{\sum_{p=0}^m \binom{m}{p} (-1)^p 2^{n*(m-p)}}{2^{n*m}} * \prod_{j \in T_i} P_{V_j} \quad (6.12)$$



## 6.4.2 Probability of a Cloud Security Threat Undetected and Materialised

It is assumed that an attack process is the action on security vulnerabilities between attackers and controllers. Attackers find the way to take advantages to exploit security vulnerabilities to attack the system. Whereas, controllers manage to mitigate the security vulnerabilities to remove favourable triggers to prevent attacks. Mirroring the method for computing the probability that attackers exploit a set of vulnerabilities presented in section 6.3, we use exactly the same method to calculate the probability that collectively controller(s) can mitigate a set of vulnerabilities. Given  $k$  vulnerabilities (already existed) and  $l$  the number of controllers or control measures, this probability is computed as follows.

$$P_{C_i} = \frac{\sum_{q=0}^k \binom{k}{q} (-1)^q 2^{l*(k-q)}}{2^{l*k}} \quad (6.13)$$

It should be stated that collectively, the controllers may be able to mitigate each vulnerability independently and may be able to cover a different set of vulnerabilities at different levels; however, we simply use the above formula to indicate the skill level of the controllers without considering other levels of complexity. In order for the attackers to attack the cloud system successfully they have to overcome the controllers' mitigation measures. According to (6.2), the probability of security threat undetected for each threat is computed as follows.

$$P_{U_i} = 1 - \frac{\sum_{q=0}^k \binom{k}{q} (-1)^q 2^{l*(k-q)}}{2^{l*k}} \quad (6.14)$$

Therefore, according to (6.3) the probability of a security threat materialised for each threat is the product of the probability of an existed security threat (6.12) and the probability of an undetected security threat (6.14). It is computed by the formula.

$$P_{T_i} = \frac{\sum_{p=0}^m \binom{m}{p} (-1)^p 2^{n*(m-p)}}{2^{n*m}} * \prod_{j \in T_i} P_{V_j} * \left(1 - \frac{\sum_{q=0}^k \binom{k}{q} (-1)^q 2^{l*(k-q)}}{2^{l*k}}\right) \quad (6.15)$$

## 6.5 Demonstration of the Proposed Threat Model to Cloud

In this section, we will introduce the method to obtain the data for security vulnerabilities and security threats based on investigating the Common Vulnerability Scoring System (CVSS). We then compute the probability of security threats existed, undetected, and materialised. Finally, we will discuss the simulation results.

### 6.5.1 Obtain Data for Cloud Simulation

Based on our investigation in Chapter 5 (**Table 5.2**) on the distribution of the cloud security vulnerabilities database from CVSS, with the total number of security vulnerabilities in cloud of 87,118, we obtain the probability distribution for seven security vulnerabilities as shown in **Table 6.1**. We consider these probabilities of cloud security vulnerabilities as the probability of existence of security vulnerabilities in the system.

**Table 0.1** the probability of cloud existed security vulnerabilities

Cloud security vulnerability	Acronym	# of vulnerabilities	Probability
Insecure interfaces and APIs	V1	13,590	15.60%
Unlimited allocation of resources	V2	29,272	33.60%
Data-related vulnerabilities	V3	16,291	18.70%
Vulnerability in Virtual Machines	V4	5,750	6.60%
Vulnerabilities in Virtual Machine Image	V5	4,704	5.40%
Vulnerabilities in Hypervisors	V6	12,893	14.80%
Vulnerabilities in Virtual Networks	V7	4,618	5.30%

In terms of data for the attacker skill, we simulate on the number of attackers with three levels. Particularly, one attacker is for the beginner level, two attackers are for the immediate level, and three attackers are for the expert level. Similarly, the capability level of controllers is based on the number of controllers. One controller is for the minimum control level, two controllers are for the medium level, and three controllers are for the maximum level.

## 6.5.2 Probability of Existed Threat with Various Attack Skills

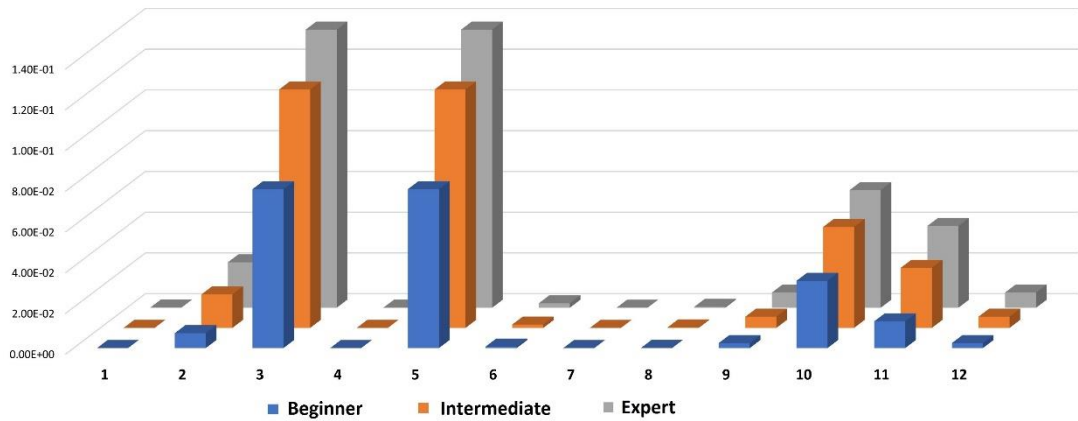
As mentioned in 6.4.1, the existed security threat depends on the skill level of attackers and security vulnerabilities of the cloud system. The number of attackers and the number of vulnerabilities form the exploit probability (Section 6.3). The probability of each vulnerabilities within each security threat is determined in Section 6.5.1. As analysed in Chapter 4 about the relationship between cloud security threats and vulnerabilities (**Table 4.1**), a security threat can obtain one or many vulnerabilities. A security vulnerability can exist in different security threats. By applying (6.12), we have the distribution of cloud security existed threat in terms of various attack skill levels (See **Table 6.2** and **Figure 6.5**).

As seen in **Figure 6.5**, threat Insecure interfaces and APIs (API) and Account Hijacking (AH) have highest probability of existed threat with 0.078 for attack level 1 (beginner level). The second highest probability is threat Abuse and Nefarious Use with 0.033 for beginner attack level. However, the lowest probability is for threat Advanced Persistent Threats (APT) with  $0.000136 * 10^{-3}$  for level 1. Regarding security management, security manager needs to consider security decisions to the cloud security platform or to prevent attacks relating to account hijack. Table 6.3 shows the sum of probability of cloud existed security threats in terms of skill-based attack levels. For the beginner level, it is 0.2151, whereas, the total probability for intermediate level is 0.3423 that increases by 59% compared with the beginner level. For the expert level, the overall

probability is 0.4109 increasing by about 20% compared with the intermediate level. As a result, the probability that an existed security threat increases with higher attack skill levels.

**Table 0.2** The probability of cloud existed security threat for different attack skill levels (\*  $10^{-3}$ )

Cloud security threat	Acronym	Beginner	Intermediate	Expert
Data Breaches	DB	0.00319	0.0242	0.0523
Weak Identity, Credential and Access	IAM	7.29	16.4	22.3
Insecure interfaces and APIs	API	78	117	137
System Vulnerabilities	SV	0.00175	0.00885	0.0164
Account Hijacking	AH	78	117	137
Malicious Insiders	MI	0.716	1.61	2.19
Advanced Persistent Threats	APT	0.000136	0.00103	0.00224
Data Loss	DL	0.0818	0.276	0.438
Insufficient Due Diligence	IDD	2.44	5.49	7.48
Abuse and Nefarious Use	ANU	33	49.5	57.8
Denial of Service	DOS	13.1	29.5	40.1
Shared Technology Vulnerabilities	STV	2.44	5.49	7.48



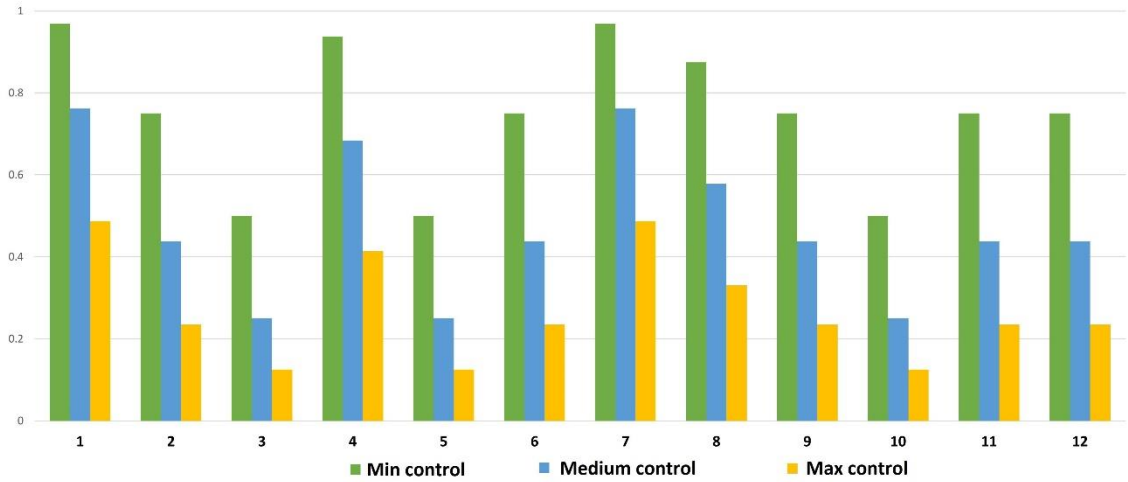
**Figure 0.5** The probability of cloud existed security threat in terms of attack-skill

**Table 0.3** The total probability of cloud existed security threats for various attack-skills

	Beginner	Intermediate	Expert
Probability	0.2151	0.3423	0.4109

### 6.5.3 Probability of Undetected Threat for Various Control Skills

By applying (6.14) we have the distribution of cloud undetected security threat probabilities in terms of various control skill levels. As seen in **Table 6.4** and **Figure 6.6**, overall, the probability of undetected security threat decreases with the increase of control skill levels. The threat Data Breaches, and threat Advanced Persistent Threats have the highest probability of undetected security threat with 0.968 for minimum control level, 0.762 for medium control level, and 0.487 for maximum control level. The second highest probability of undetected security threat is for threat System Vulnerabilities. In terms of security countermeasures for preventing attacks, security practitioners need to take consideration of three kinds of security threats including Data Breaches, System Vulnerabilities, and Advanced Persistent Threats.



**Figure 0.6** The probability of undetected security threat in terms of control-skill

**Table 0.4** The probability of undetected security threat for various control skills

Cloud security threat	Acronym	Min	Medium	Max
Data Breaches	DB	0.96875	0.76269	0.48709
Weak Identity, Credential and Access	IAM	0.75	0.4375	0.23437
Insecure interfaces and APIs	API	0.5	0.25	0.125
System Vulnerabilities	SV	0.9375	0.68359	0.41381
Account Hijacking	AH	0.5	0.25	0.125
Malicious Insiders	MI	0.75	0.4375	0.23437
Advanced Persistent Threats	APT	0.96875	0.76269	0.48709
Data Loss	DL	0.875	0.57812	0.33007
Insufficient Due Diligence	IDD	0.75	0.4375	0.23437
Abuse and Nefarious Use	ANU	0.5	0.25	0.125
Denial of Service	DOS	0.75	0.4375	0.23437
Shared Technology Vulnerabilities	STV	0.75	0.4375	0.23437

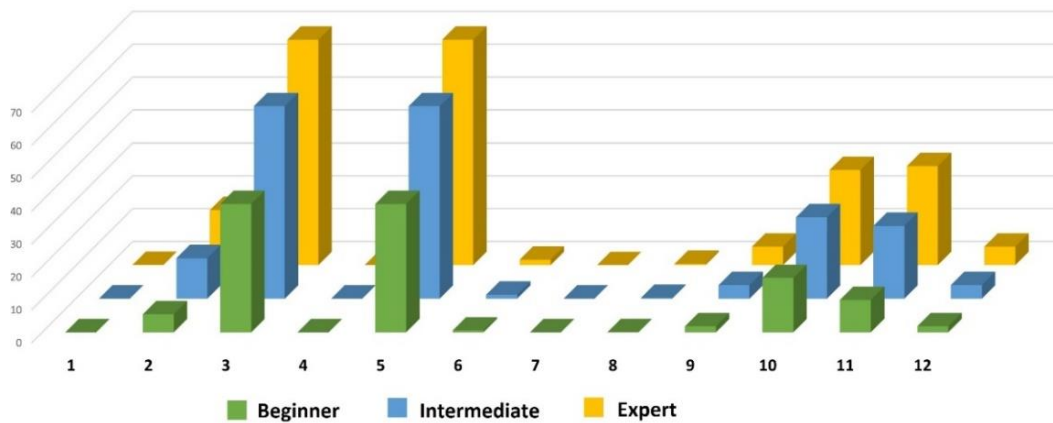
## 6.5.4 Probability of Materialised Threats

By using (6.14), we have the distribution of cloud materialised security threat probabilities in terms of various control skill levels and different skill controls. **Table 6.5** and **Figure 6.7** show the data for the case minimum control level. Overall, the probability of security threat materialised into attacks increases with the rise of attack skill levels. It can be seen in Figure 6.7 that the highest probability is for threat Insecure Interfaces and APIs and threat Account Hijacking with 0.039 for beginner attack level, 0.058 for intermediate level, and 0.068 for expert level.

**Table 0.5** The probability of materialised security threat for various attack skills with min control ( $* 10^{-3}$ )

Cloud security threat	Acronym	Beginner	Intermediate	Expert
Data Breaches	DB	0.00309	0.02344	0.05066
Weak Identity, Credential and Access	IAM	5.4675	12.3	16.725
Insecure interfaces and APIs	API	39	58.5	68.5
System Vulnerabilities	SV	0.00164	0.00829	0.01537
Account Hijacking	AH	39	58.5	68.5
Malicious Insiders	MI	0.537	1.2075	1.6425
Advanced Persistent Threats	APT	0.00013	0.00099	0.00217
Data Loss	DL	0.07157	0.2415	0.38325
Insufficient Due Diligence	IDD	1.83	4.1175	5.61
Abuse and Nefarious Use	ANU	16.5	24.75	28.9
Denial of Service	DOS	9.825	22.125	30.075
Shared Technology Vulnerabilities	STV	1.83	4.1175	5.61

**Table 6.6** and **Figure 6.8** shows the distribution of probability of security threat 3 (Insecure Interfaces and APIs) for different attack levels and different control levels. Overall, the probability of security threat materialised into attacks increases when the level of attack rises. It can be seen that the highest probability of threat materialised is for the case min control with 0.039 for beginner attack level, 0.058 for intermediate level, and 0.068 for expert level. However, the lowest probability of materialised threat is for the case max control with 0.0097 for beginner attack level, 0.0146 for intermediate level, and 0.0171 for expert level. This can be explained that when there is a lack of security actions (control capability), the probability of security threat materialise into attacks will increase.

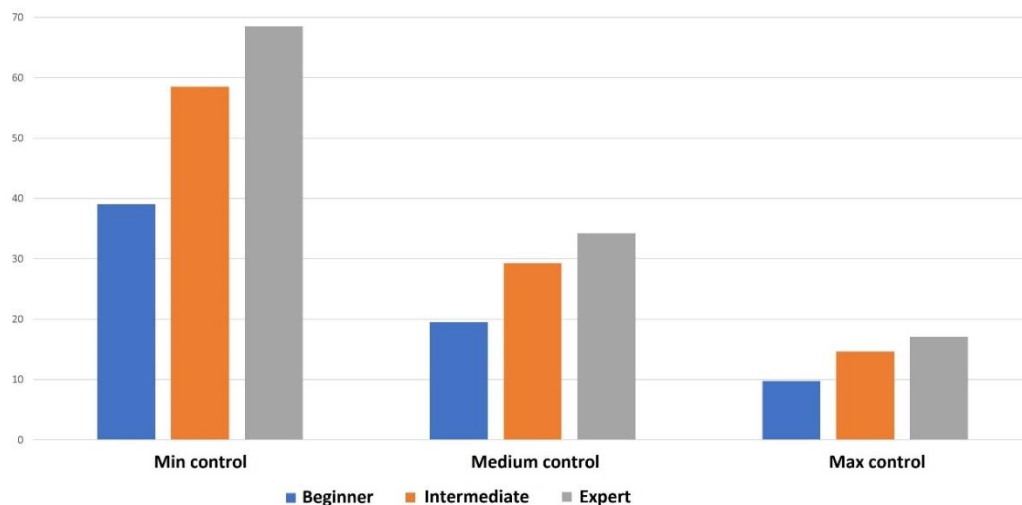


**Figure 0.7** The probability of materialised security threat for various attack skills with min control (\* 10<sup>-3</sup>)

**Table 0.6** The probability of materialised security threat API (Threat 3) for various attack skills and different control skills (\* 10<sup>-3</sup>)

	Beginner	Intermediate	Expert
Min control	39	58.5	68.5
Medium control	19.5	29.25	34.25
Max control	9.75	14.625	17.125





**Figure 0.8** The probability of materialised security threat API (Threat 3) for various attack skills and different control skills ( $\times 10^{-3}$ )

## 6.6 Summary

Quantifying security factors including attack and control skill, which are indispensable parts in studying cyber security threat, is critical in computing the probability of security threat materialised into attacks. The chapter proposed an innovative security threat model that takes attack and control skill into consideration. To the best of our knowledge, the chapter is the first introduction of the mathematical models (combination and inclusion-exclusion principle) to solve the problem that the probability of the number of attackers exploits the number of security vulnerabilities. This solution is not only applied for our proposed security threat model in this chapter but is also used for problems relating to attackers and vulnerabilities, especially in security risk problems in the future. Finally, the proposed security threat model was applied to cloud computing to compute the probability of security threat existed, undetected, and materialised for twelve specific cloud security threats.

# **Chapter 7**

## **Mean Security Remediation Cost as a Quantitative Metric and Application to Cloud Computing**

### **7.1 Introduction**

More than ever, measuring security quantitatively is vital for protecting cloud systems. Existing cloud security models do not equip themselves with sufficient measures to assess the overall security status of a cloud system. Existing security metrics are limited in that they are mainly qualitative and compliance checking. They do not reflect emerging security threats and their associated risks, inadequately consider the variance of measuring objects, and are often not meaningful to decision makers. This chapter proposes Mean Security Remediation Cost (MSRC) as a new quantitative security metric that measures the security impact in terms of the cost to each of the cloud stakeholders for remediating damages caused by a security incidence and the probability of the threats that materialise into the incidence. Specifically, the metric evaluates the impact/cost of the system vulnerabilities and their associated threats when they are materialised on all stakeholders. The term cost here is a general term that can be directly related to the defined impact. MSRC is evaluated as a function of the stakeholders, the threat classes associated with a cloud system, and the probability of materialised threats. For this purpose, we propose the cloud security stakeholder model that identifies security stakeholders and their interrelationships in a cloud environment. The research results in

computing the probability of a materialised cloud security threat in chapter 4 will be used in this metric. The proposed metric is applied to the Cloud Computing. The results demonstrate that MSRC can serve as an effective measure for security managers in judging the overall security status of their clouds and making proper security decisions, and for security experts in planning appropriate security actions.

*Major contributions of this chapter are as follows:*

It proposes the Mean Security Remediation Cost as a metric to address the challenge in quantifying security measures. It requires the multi-dimensional knowledge about cloud security stakeholders, classes of security threats, individual cloud security threats and the interrelationship among them.

It introduces a cloud security stakeholder model, with which one can identify all stakeholders and the impact on them when a system failure occurs due to security breaches.

It provides a case study where the proposed MSRC is applied to the Cloud Computing using relevant data on the cloud system in supporting the security decision-making process.

The remainder of the chapter is organised as follows. Section 7.2 introduces the concept of MSRC and its formulation of three major matrices: stakeholder, threat class, and cloud security threat. Section 7.3 provides the proposed cloud security stakeholder model and the generation of the stakeholder matrix. Section 7.4 describes the classification of security threats and the structure of threat class matrix, the relationship between threat class and individual security threat. Section 7.5 expresses how we obtain the data for simulation. Section 7.6 demonstrates MSRC in several case studies in cloud computing. Finally, Section 7.7 concludes the chapter with remarks along with directions for future research.

## **7.2 Mean Security Remediation Cost as a Quantitative Security Metric**

This section introduces Mean Security Remediation Cost (MSRC) as a new quantitative security metric that relates stakeholders to security class threats which in turn relate through system vulnerabilities to individual materialized (into an attack) threats. The metric provides a means for estimating the costs that stakeholders are expected to spend to remediate a system or component failure caused by a materialized security threat. In other words, MSRC is the average cost required to handle a system or component and restore it to the normal operating conditions. MSRC ultimately reflects how well an organisation responds to a problem and repairs it. MSRC is novel in two aspects: it embraces a new stakeholder model that can be tailored to a specific system and its security posture/composition, and a new method for computing the probability of a security threat materialized which is necessary for estimating each holder's share of the cost impact of a security breach (a materialised security threat).

One of meaningful quantitative metrics is Mean Failure Cost (MFC). This metric is the motivation for us to innovate MSRC. MFC is a value-based metric that quantifies the security of a computing system by the statistical mean of the random variable representing each stakeholder, the amount of loss that results from security threats and system vulnerabilities [69]. MFC uses technical and non-technical control elements to measure cyber security. It includes several desirable features: it identifies stakeholders and provides the cost for each as a result of a security failure; it quantifies the cost in terms of a financial loss per unit of operation time (\$/h). Despite these appropriate considerations, MFC has a number of drawbacks. Firstly, the security threats probability distribution is based on the simple empirical data, while security threats are changeable, dynamic, and specific to different IT systems. Due to the stochastic nature of threats, modelling their probability distributions has become a necessity for any security measuring and predicting system. The relevant and sound classification of threats, which relates to deployed vulnerabilities, attack motivation perspectives, and likelihood of

successful attacks, is essential to facilitate the identification of potential security threats and the development of security countermeasures. Secondly, stakeholder identification is based on the general business perspective. MFC does not take into account stakeholders related to security perspective. These gaps are the inspiration and motivation for us to propose the MSRC metric.

There are several rationales for the introduction of MSRC. Once a security breach occurs, its impact (costs or damages) may be felt by affected stakeholders of a cyber-system and the severity of the impact depends on the role and responsibility of the stakeholders. A stakeholder model is essential to address this important aspect of security. A security threat remains a security threat until it is materialised, and its damages follow. A security threat model is needed to predict the probability of a threat materialised (resulting in a security attack or breach). Furthermore, the model should allow one to trace back to the causes (or vulnerabilities) of the threat when it materialises into an attack. This is explained comprehensively in chapters 4, 5, and 6.

MSRC addresses both concerns. The stakeholder model is needed to investigate the relationship between the stakeholders and identified security threats as well as other dependent factors within the security system. The determination of the effect of security threats on each of the stakeholders will quantify the extent to which a stakeholder will bear the costs of (or be responsible for) for the security of the system. This supports system managers in making appropriate security decisions and attributing cost-effective plans for the security budget. The stochastic threat model is essential for identifying what and where a security breach has occurred and the possibility of its occurrence. What and where will entail vulnerabilities that lead to a threat and its materialisation into an attack. The metric supports security experts/managers in making proper decisions and actions for dealing with security threats and their mitigation.

MSRC is defined as a quantitative security metric estimating the costs that stakeholders are expected to spend to remediate a system or component failure caused by a materialised security threat. In other words, MSRC is the average cost required to

handle a system or component and restore it to the normal operating conditions. MSRC ultimately reflects how well an organisation responds to a problem and repairs it.

To responsible stakeholders, MSRC provides relevant and needed information for senior management to make sound decisions in terms of costs, such as repairing, replacing, hiring, or optimizing the system maintenance schedule. For example, a firewall system in a cloud data centre may fail in preventing intrusions under various circumstances due to its vulnerabilities. Security experts have to spend much of their time to remediate this component. A high cost of remediation is reflected by a large MSRC value. By analysing the MSRC, a replacement of the firewall may be a better alternative in terms of costs. All these cases will be investigated in application section 7.6 below.

MSRC expresses the relationship between stakeholders and security factors like security components, classes of threat, and individual security threats. In this chapter, MSRC will investigate the relationships among stakeholders, classes of threat, and security threats. The stakeholders are holders that share the responsibility for security of the system in terms of money. Specifically, for cloud computing services, stakeholders may include security providers, application providers, platform providers, infrastructure providers, and customers.

Security threats cover cloud threats that harm the system. The relationship between MSRC and security threats is the costs of remediation of damages caused by the materialised security threat.

Ultimately, a security threat accounts for some specific attacks; however, at a higher level, stakeholders relate better to security threats through common characteristics of their classes (e.g., insider/internal or outsider/external threats). Classes of threat are threat groups categorised by their sources (inside or outside), causes (human or technology), and intention (malicious or non-malicious).

Mean Security Remediation Cost is defined in terms of stakeholders, threat classes, and security threats. The security threat vector is modelled as a Markov stochastic process that allows us to determine the probability of a threat materialised (in chapter 4). Explicitly, MSRC is defined by (7.1).

$$MSRC = ST * CT * PT \quad (7.1)$$

where:

- MSRC is the mean security remediation cost vector whose component is the cost that a stakeholder spends to remediate the damages as a result of a security failure.

- ST is the stakeholder matrix where rows represent stakeholders, columns are security threats classes. The value of a cell in ST is the cost that a stakeholder spends to remediate when a threat class is materialised.

- CT is the threats class matrix where rows are threat classes, columns are security threats. The value of a cell in CT is the probability of a class threat when a security threat belonging to this class has materialised.

- PT is the security threat vector that is the distribution of threat probabilities.

Explanation for (7.1) will be discussed as follows. Assuming that there are  $m$  stakeholders,  $n$  classes of threat, the general expression of MSRC for a stakeholder  $S_i$  can be expressed in (2)

$$MSRC(S_i) = \sum_{1 \leq j \leq k} ST(S_i, CT_j) * P(CT_j) \quad (7.2)$$

where  $ST(S_i, CT_j)$  is the cost that a stakeholder  $S_i$  would spend to remediate the system when the system fails caused by a security attack because of a threat in one class of threats  $CT_j$  is materialised.  $P(CT_j)$  is the probability distribution of class of threat  $CT_j$ . (See **Table 7.1**).

To derive the probability distribution of threat classes  $P(CT_j)$ , we let  $T_1, T_2, T_3, \dots, T_n$  be the system security threats.  $P(CT_j)$  is calculated by the following formula:

$$P(CT_j) = \sum_{1 \leq h \leq n} P(CT_j|T_h) * P(T_h) \quad (7.3)$$

where  $P(CT_j|T_h)$  is the probability of class of threat  $CT_j$  given that  $T_h$  happens.  $P(T_h)$  is the probability of a security threat that leads to an attack making a system failure (see **Table 7.2**). Therefore, from (7.3), we substitute into (7.2) then we have (7.1).

**Table 0.1** Stakeholder matrix with probability distribution of classes of threats

		Threat Classes				
		$CT_1$	$CT_2$	$CT_3$	...	$CT_k$
Stakeholders	$S_1$					
	$S_2$					
	$S_3$					
	...				$ST_{i,j}$	
	$S_m$					
		Probability distribution of classes of threat				
					$P(CT_j)$	

**Table 0.2** Threat Class matrix

		Threats				
		T1	T2	T3	...	Tn
Threat classes	$CT_1$					
	$CT_2$					
	$CT_3$					
					$P(CT_j T_h)$	
	$CT_k$					

As a result, MSRC metric is the vector formed from the matrix multiplication of the three matrices ST, CT, and PT. ST represents the impact on stakeholders by threat classes. CT shows the relationships between threat classes and security threats. PT describes the probability distribution of security threats. In fact, the matrix components that form the MSRC metric can be more than three if we expand the investigation of the impact of other security factors on stakeholders in terms of money like security requirements, system components. However, for this study we focus on ST, CT, and PT.

In summary, MSRC is  $m \times 1$  vector where  $m$  is the number of stakeholders,  $ST$  is an  $m \times k$  matrix where  $k$  is the number of threat classes,  $CT$  is a  $k \times n$  matrix where  $n$  is the number of security threats.  $CT_l$  is a vector of threat classes where  $1 \leq l \leq k$ , and  $PT$  is a  $n \times 1$  vector. With these notations, MSRC can be expressed explicitly by the following equations.



Expanding equation (7.2), MSRC can be expressed in terms of threat classes as follows.

$$\begin{bmatrix} MSRC_1 \\ MSRC_2 \\ \vdots \\ MSRC_m \end{bmatrix} = \begin{bmatrix} ST_{11} & ST_{12} & \cdots & ST_{1k} \\ ST_{21} & ST_{22} & \cdots & ST_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ ST_{m1} & ST_{m1} & \cdots & ST_{mk} \end{bmatrix} * \begin{bmatrix} CT_1 \\ CT_2 \\ \vdots \\ CT_k \end{bmatrix} \quad (7.4)$$

Expanding equation (7.3), CT can be expressed in terms of security threats as follows.

$$\begin{bmatrix} CT_1 \\ CT_2 \\ \vdots \\ CT_k \end{bmatrix} = \begin{bmatrix} CT_{11} & CT_{12} & \cdots & CT_{1n} \\ CT_{21} & CT_{22} & \cdots & CT_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ CT_{k1} & CT_{k1} & \cdots & CT_{kn} \end{bmatrix} * \begin{bmatrix} PT_1 \\ PT_2 \\ \vdots \\ PT_n \end{bmatrix} \quad (7.5)$$

Finally, by expanding (7.1) and using (7.4) and (7.5), MSRC can be expressed by equation (7.6) and (7.7)

$$\begin{bmatrix} MSRC_1 \\ MSRC_2 \\ \vdots \\ MSRC_m \end{bmatrix} = \begin{bmatrix} ST_{11} & ST_{12} & \cdots & ST_{1k} \\ ST_{21} & ST_{22} & \cdots & ST_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ ST_{m1} & ST_{m1} & \cdots & ST_{mk} \end{bmatrix} * \begin{bmatrix} CT_{11} & CT_{12} & \cdots & CT_{1n} \\ CT_{21} & CT_{22} & \cdots & CT_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ CT_{k1} & CT_{k1} & \cdots & CT_{kn} \end{bmatrix} * \begin{bmatrix} PT_1 \\ PT_2 \\ \vdots \\ PT_n \end{bmatrix} \quad (7.6)$$

Or explicitly,

$$\begin{bmatrix} MSRC_1 \\ \vdots \\ MSRC_i \\ \vdots \\ MSRC_m \end{bmatrix} = \begin{bmatrix} (ST_{11}CT_{11} + ST_{12}CT_{21} + \cdots + ST_{1k}CT_{k1}) & \cdots & (ST_{11}CT_{1n} + ST_{12}CT_{2n} + \cdots + ST_{1k}CT_{kn}) \\ \vdots & \ddots & \vdots \\ (ST_{i1}CT_{11} + ST_{i2}CT_{21} + \cdots + ST_{ik}CT_{k1}) & \cdots & (ST_{i1}CT_{1n} + ST_{i2}CT_{2n} + \cdots + ST_{ik}CT_{kn}) \\ \vdots & \ddots & \vdots \\ (ST_{m1}CT_{11} + ST_{m2}CT_{21} + \cdots + ST_{mk}CT_{k1}) & \cdots & (ST_{m1}CT_{1n} + ST_{m2}CT_{2n} + \cdots + ST_{mk}CT_{kn}) \end{bmatrix} * \begin{bmatrix} PT_1 \\ PT_2 \\ \vdots \\ PT_n \end{bmatrix} \quad (7.7)$$

From these equations we can evaluate the  $MSRC_i$  for a particular stakeholder  $i$ , the  $MSRC_{il}$  for stakeholder  $i$  when the threat class  $l$  materialised, or the  $MSRC_{ij}$  for stakeholder  $i$  when the threat  $j$  materialised. Over the next few sections, we introduce in detail these three components and their formulations.

### 7.3 Stakeholder Matrix

To identify security stakeholders in a cloud system, it is vital to be aware the stakeholders in cyber systems in general. The interrelationships among cloud

stakeholders and their impact caused by security threats will be investigated. In this section, stakeholders in cyber systems will be described. We then propose a Cloud Security Stakeholder Model and the generation of the stakeholder matrix.

### **7.3.1 Stakeholders in Cyber Systems**

The concepts of stakeholders are different based on various perspectives. In the Oxford dictionary, a stakeholder is defined as a person or a company that is involved in a particular organisation, project, system, especially because they have invested money in it. Stakeholder may be considered as anyone who is a direct user, indirect user, manager of users, senior manager, operations staff member, the "gold owner" who funds the project, support (help desk) staff member, auditors, your program/portfolio manager, developers working on other systems that integrate or interact with the one under development, or maintenance professionals potentially affected by the development and/or deployment of a software project.

In [123], Wu et al. introduced a stakeholder/value dependency framework that indicated the relationship between stakeholders and dependability attributes covering security attributes. The stakeholders include Information Suppliers, Information Consumers, Information Brokers, System Dependents, System Controllers, Administrators, Developers, Maintainers, and Acquirers. The dependability attributes consist of Protection (safety, security, and privacy), Robustness (reliability, availability, and survivability), Quality of Service (performance, accuracy, and usability), Interoperability, Correctness, Cost, and Schedule. The main finding from this study is that various stakeholders have different values of level of services. However, all the hypotheses of the study were tested qualitatively. In [124], Haile et al. designed a value creation model for software service platforms. This includes three stakeholders including application service users, service developers, and service platform providers. In [125], Marston et al. considered cloud computing stakeholders as not only providers and customers but also enablers like vendors or aggregators and regulators belonging to a sovereign government body or international entity, in which, regulators, which are

considered as entities out of the cloud computing “value-chain”, play the vital role that permeates across the other stakeholders. Dealing with regulation problems is one of the cloud security solutions when data privacy, cloud infrastructure location issues or cloud forensics are taken into account. Markus et al. [126] proposed a generic value network of cloud computing that integrated the value chain and value network perspectives. Cloud stakeholders include application providers, platform providers, market platforms, infrastructure providers, consultants, aggregators, integrators, and consumers.

Our model reflects the stakeholders’ concerns in terms of business, human, technology aspects and relates them to the impact of security threats.

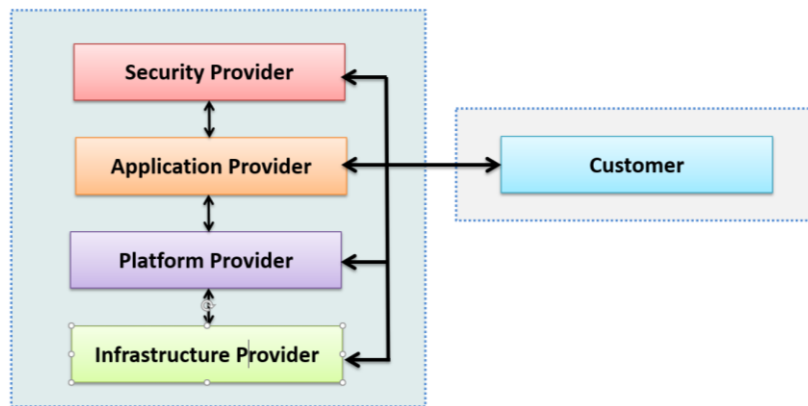
### **7.3.2 Cloud Security Stakeholder Model**

As mentioned earlier, two important quantitative measures are essential for effective security management of a cyber system. One measure is the probability that a security threat is materialised into an attack (security breach) and the other is the quantitative measure of the impact of the breach on the system or specifically on each of the constituents (or stakeholders) of the system. These allow system decision makers to predict the chance of attacks, identify the affected components, and exercise appropriate security measures where needed. In this section we identify a stakeholder model of a cyber system and the relationships among the stakeholders.

Security is the focus of our cloud stakeholder model as shown in **Figure 7.1**. This model will be used to demonstrate the use of our proposed mean security remediation cost. The stakeholders include application providers, platform providers, infrastructure providers, security providers, and customers. An application provider hosts/provides cloud application for its customers. Platform providers are responsible for providing platforms for developing and maintaining applications. Infrastructure providers are responsible for providing infrastructure supports including computing, storage, and networking resources. Customers request resources and services from the cloud system. Security providers are responsible for the security of the cloud system and its services.

- Application Provider

The application provider ensures a smooth operation of their applications. This includes monitoring, asset/resource management and failure/problem management [126]. When the cloud system fails as a result of a security attack on one of its components (for example a web server), the most affected stakeholder is the application provider. However, other entities may also play a part in this failure. Consequently, the application provider may be affected by a security failure from other stakeholders such as platform (vulnerabilities from operation systems), infrastructure (load balancing system failure) or from attacks such as Denial of Service (DoS) via their customers.



**Figure 0.1** Cloud Security Stakeholder Model

- Platform Provider

A platform provider provides an environment to develop, run and test applications. From a technical perspective, an operating environment, application programming interfaces (APIs), programming languages are provided to develop platform programs executed over datacentres [126]. Similar to the application provider, the platform provider is the middle player between other providers and customers. Hence, it is also affected by these stakeholders. For example, there exist several security vulnerabilities in an application programming interfaces that attackers can exploit to attack applications or infrastructures (databases, servers). For remediation, the platform provider needs to patch these vulnerabilities or apply measures to repair and recover the system.

- Infrastructure Provider

An infrastructure provider furnishes physical and virtual resources including computing elements, network connections, storages as well as security appliances to its customers. The infrastructure provider is thus responsible for its provisioned resources. Depending on the cloud service model and service level agreement (SLA), the customer may or may not assume the responsibility for the allocated resources. From the security perspective, a cloud infrastructure has to be secured because it contains most important and fundamental assets of a cloud computing.

- Security provider

A security provider offers an overall and integrated cloud security service, protecting the cloud, its stakeholders and cloud services. The security provider may be a third-party provider or may be component of the cloud provider. The service may be considered separately as “security as a service (SECaaS)” and often includes authentication, anti-virus/malware/spyware, intrusion detection, and security event management [127]. A security provider may be a central operator that monitors, cooperates, and makes a security decision to ensure operation of the cloud system.

- Customer

Based on the business perspective, customers seek cloud solutions from a cloud provider. The customers need cloud solutions that are best fit in terms of maximum resource utilisation and ease of management. They also seek services enabling them to migrate the infrastructure to a cloud computing model cloud readiness assessment (for infrastructure and applications), workload assessments, cloud migration, and so on [128]. The customers are stakeholders who may bear the impact of cloud security breaches or themselves be the sources of security risks.

### **Cloud security stakeholder model operation**

The cloud stakeholder model depicts stakeholders with their various roles, interrelationships and value exchanges. The value is created by producing fundamental

services and refining them throughout the value chain to customers. Products or cloud services are exchanged in return of either money or other benefits. From the security perspective, when a security incident occurs that causes a system failure, all cloud stakeholders are affected. However, different stakeholders experience different impacts depending on the type of failure or the nature of the security attack.

In the model there are two main blocks: a provider block and a customer block. The provider block includes infrastructure, platform, application, security providers that offer various cloud services for consumers. Within the provider block, service/value relationships are implemented between different providers. For example, an infrastructure provider offers infrastructure as a service for a platform provider to create their platform services. In turn, the providers exchange services among stakeholder's providers. The consumer block consists of all customers that request any kind of services (IaaS, PaaS, SaaS, SECaaS) directly from one or more service providers.

The stakeholder model thus identifies relevant cloud stakeholders including application, platform, infrastructure, security provider, and customer stakeholders. Among them, there exists the security service/value interrelationship. These relationships indicate impacts among the stakeholders when a security attack or security failure occurs. It should be noted that the composition of a stakeholder matrix may vary in both number of stakeholders and their roles in relation to system security concerns.

### **7.3.3 Generating Stakeholder Matrix (ST)**

The impact of an attack from a class threat may be quantified by an impact value. In our case, the impact value is represented by the remediation cost. A stakeholder may see different impacts from various attacks caused by different threat classes (or threats). For example, at one time there may be several cyber-attacks like DoS and flooding attacks on an application provider. A security threat may cause different impact values for different stakeholders. For example, a DoS attack may affect an application provider, a platform, an infrastructure, and customer stakeholders with different degrees of severity. Hence the impact values for the attack vary for each of the stakeholders. The relationship between

stakeholders and threat classes is best represented by a two-dimension matrix where the rows represent stakeholders and the columns show threat classes.

Stakeholder matrix defines the relationship between stakeholders and security threat classes.  $ST(i, j)$  presents the cost that each stakeholder spends to remediate when a system failure occurs by a security threat class materialised. As mentioned above, stakeholder matrix includes two dimensions. Rows have five stakeholders involved in a cloud system including Application Provider (AP), Platform Provider (PP), Infrastructure Provider (IP), Security Provider (SP), and Customer (CS) (see Figure 7.1). Columns include four threat classes embracing EH (External Human), ET (External Technology), IH (Internal Human), and IT (Internal Technology). These threat classes will be investigated comprehensively in the following section.

## 7.4 Threat Class Matrix (CT)

While there are many security threat classification methods [129], Jouini et al. [130] proposed a model to classify the classes of security threat based on the four following criteria: threat source is the origin of threat either internal or external; threat agents caused by human, accidental environmental or technological; security threat motivation; and the goal of attackers on a system which can be malicious or non-malicious; threats impact: damage result because of materialised threat. The purposes of this classification are: (1) Identify threat's properties into a group; (2) Countermeasure the group of threats; (3) Update threat's properties. In this chapter, for the purpose of data collection and evaluation the source and the nature of threats will be taken into account. Threat classes will be divided into four groups with the two criteria including the source and the cause of threats. The source of threats includes external and internal. The cause of threats is composed of human or technology. Therefore, four groups of security threat class are EH (External Human), ET (External Technology), IH (Internal Human), and IT (Internal Technology).

### **7.4.1 Generating Class of Threat Matrix (CT)**

In CT matrix, columns represent security threats that are described in 7.4.2. Rows represent threat classes. A cell  $CT_{ij}$  represents the probability of having Class  $CT_i$  once Threat  $T_j$  has materialised. To create the threat class matrix, the following conditions should be met: (1) One threat class includes at least two different threats; (2) a threat must belong to at least one threat class; (3) all threat classes add up to 100% (See Table 7.2).

### **7.4.2 Probability Threat Vector (PT)**

As mentioned in chapter 4, the computing result of the probability of a security threat materialised into attacks is used in this chapter as a critical part of the MSRC metric. From chapter 4, we explored the relationship between security threats and vulnerabilities to identify the likely potential attacks. We used a Markov process to describe a cloud attack model and used the common vulnerability scoring model to determine the transition matrix of the proposed Markov chain.

According to Cloud Security Alliance (CSA) report [42, 112], twelve critical security threats are Data Breaches (DB); Weak Identity, Credential and Access Management (IAM); Insecure interfaces Application Programming Interface (API); System Vulnerabilities (SV); Account Hijacking (AH); Malicious Insiders (MI); Advanced Persistent Threats (APTs); Data Loss (DL); Insufficient Due Diligence (IDD); Abuse and Nefarious Use of Cloud Services (ANU); Denial of Service (DOS); and Shared Technology Vulnerabilities (STV). The seven cloud major vulnerabilities include Insecure interfaces and APIs (V1), Unlimited allocation of resources (V2), Data-related vulnerabilities (V3), Vulnerabilities in Virtual Machines (V4), Vulnerabilities in Virtual Machine Images (V5), Vulnerabilities in Hypervisors (V6), Vulnerabilities in Virtual Networks (V7). By using Markov theory and common vulnerability scoring system (CVSS), we have the distribution of cloud materialised security threat probabilities seen



in Table 7.3. This distribution is the threat probability vector PT that we need for the MSRC metric.

**Table 0.3** Probability distribution of twelve security threats materialised into attacks

	Cloud security threats	Acronym	Probability ( $\times 10^{-3}$ )
1	Data Breaches	DB	5.1203
2	Weak Identity, Credential and Access	IAM	1.8774
3	Insecure interfaces and APIs	API	1.3654
4	System Vulnerabilities	SV	4.0962
5	Account Hijacking	AH	1.3654
6	Malicious Insiders	MI	2.3894
7	Advanced Persistent Threats	APT	5.4616
8	Data Loss	DL	2.5601
9	Insufficient Due Diligence	IDD	1.7067
10	Abuse and Nefarious Use	ANU	0.8533
11	Denial of Service	DOS	1.7067
12	Shared Technology Vulnerabilities	STV	1.7067

## 7.5 Obtaining Data for MSRC's Components

As mentioned above, MSRC is the product of three component matrices including the stakeholder matrix (ST), the class of threat matrix (CT), and the probability of threat vector (PT). The previous section indicated the value for the probability matrix (PT vector). In this section, we will discuss the method to obtain the data for the stakeholder matrix (ST) and the class of threat matrix (CT).

- Stakeholder matrix (ST)

The ST matrix includes rows representing stakeholders and columns showing threat classes. We have five stakeholders: Security Provider (SP), Application Provider (AP),

Platform Provider (PP), Infrastructure Provider (IP), and Customers (CS). In this thesis we are interested in threat source (external or internal) and threat cause (human or technology), resulting in four threat classes: External Human (EH), External Technology (ET), Internal Human (IH), and Internal Technology (IT).

To derive the ST matrix, we need to know the total cost of security management covering all security incidents of an organisation and the cost attribution to parties concerned (stakeholders). This information is, however, privileged and is generally not available to the public. Facing this difficulty, we need to find other solutions for obtaining elements of the ST matrix. Fortunately, we can obtain the security budget of many organisations and we use it as an approximation to the first degree of the total cost of managing security breaches. We then use this approximation to estimate and derive the proportion of the cost attributed to the remediation of the system when a threat class is materialised. Elements of the ST matrix can be determined by the formula:

$$ST_{ij} = B * X_j * Y_{ij} \quad (7.8)$$

where B is the budget that the organisation spends on the whole security management;  $X_j$  is overall percentage of a threat class  $CT_j$  in a year;  $Y_{ij}$  is percentage of the security fund stakeholder  $S_i$  used to remediate the class threat  $CT_j$ .

As mentioned earlier, it is difficult to get real data about security incidents or costs from the industry due to their unwillingness to share the information for various reasons including privacy and reputation. We have searched for data from several prestige security companies through many public reports.

First, we derive the cyber security budget of an organisation (B) using the data from SANS institute report [131] as follows. As an example, a medium company spends one million dollars on IT budget (bIT). The cyber security budget is bS. This is the security budget for remediating the real security threats occurred with the overall probability is p. To calculate the whole security budget (B), it is assumed to compute for one hundred percent that security threats happen. Hence, the value of B is estimated by  $B = bIT * bS * 100/p$ .

Second, to gain the data for the distribution of threat classes in a year ( $X_j$ ), we get data from “The IBM X-Force 2016 Cyber Security Intelligence Index” report [132]. The report showed that 60% of the attacks were carried out by insiders (percentage of internal threats =  $dI$ ). And in internal threats, it is about 80% of this figure by human (percentage of human threat given internal =  $dHI$ ). In 40% of outside attacks (percentage of external threats), 60% of this by human (percentage of human given external =  $dHE$ ). Therefore, we have the probability of each threat class ( $X_j$ ) illustrated in Table 7.4.

**Table 0.4** One example of variables

Variable		Value
Average IT budget of an organization (dollar)	$b_{IT}$	1,000,000
Average percentage on IT security budget	$b_S$	0.250
Percentage on overall security threat	$p$	0.030
Whole security management budget (B)	$b_{IT} * b_S * 100/p$	8.333.333
Percentage of Internal Threats	$dI$	0.60
Percentage of Human given Internal	$dHI$	0.80
Percentage of Technology given Internal	$1 - dHI$	0.20
Percentage of Internal Human	$dIH = dI * dHI$	<b>0.48</b>
Percentage of Internal Technology	$dIT = dI * dTI$	<b>0.12</b>
Percentage of External Threats	$1 - dI$	0.40
Percentage of Human given External	$dHE$	0.60
Percentage of Technology given External	$1 - dHE$	0.40
Percentage of External Human	$dEH = (1 - dI) * dTE$	<b>0.24</b>
Percentage of External Technology	$dET = (1 - dI) * (1 - dTE)$	<b>0.16</b>

**Table 0.5** One example of percentage of security fund for a stakeholder used to remediate each class threat ( $Y_{ij}$ )

	EH	ET	IH	IT
SP	0.08	0.10	0.10	0.04
AP	0.40	0.80	0.08	0.05
PP	0.40	0.05	0.10	0.40
IP	0.10	0.04	0.70	0.50
CS	0.02	0.01	0.02	0.01

Third, to acquire the data about the percentage of security fund for a stakeholder used to remediate one class threat, these percentages can be considered as variables and are determined according to the organisation and the security environment. For the sake of simulation in this paper, we derive an example to obtain data for these figures by analysing the severity of impact of each threat on a stakeholder and partly based on the CSA report [42]. The rationale for these percentages is as follows. When a threat occurred by human in the internal group (IH), the most affected stakeholder is IP (infrastructure) with about 70% of the budget for remediating this threat. Similarly, when a threat occurred by technology in the external group (ET), AP is most impacted with about 80% of the budget for remediating because there is a need to upgrade the technology for the cloud application. Therefore, we have the matrix by percentage showing the rates of fund for each stakeholder to remediate a class of threat occurred (see **Table 7.5**).

Using (7.8) with the example data from **Table 7.4** and **Table 7.5**, we obtain the ST matrix as shown in **Table 7.6**.

**Table 0.6** ST matrix (a) showing the variables, (b) one example by using (7.8) (in thousands dollar)

	EH	ET	IH	IT
SP	$B * X_1 * Y_{11}$	$B * X_2 * Y_{12}$	$B * X_3 * Y_{13}$	$B * X_4 * Y_{14}$
AP	$B * X_1 * Y_{21}$	$B * X_2 * Y_{22}$	$B * X_3 * Y_{23}$	$B * X_4 * Y_{24}$
PP	$B * X_1 * Y_{31}$	$B * X_2 * Y_{32}$	$B * X_3 * Y_{33}$	$B * X_4 * Y_{34}$
IP	$B * X_1 * Y_{41}$	$B * X_2 * Y_{42}$	$B * X_3 * Y_{43}$	$B * X_4 * Y_{44}$
CS	$B * X_1 * Y_{51}$	$B * X_2 * Y_{52}$	$B * X_3 * Y_{53}$	$B * X_4 * Y_{54}$

(a)

	EH	ET	IH	IT
SP	120	100	467	47
AP	600	800	373	58
PP	600	50	467	467
IP	150	40	3267	583
CS	30	10	93	12

(b)

- Class threat matrix (CT)

As discussed above, at the stakeholder's level, the stakeholders are not interested in an individual threat, but rather they are interested in the impact of threat classes such as human or technology, external or internal. CT is composed of rows showing classes of threat and columns representing security threats. To generate matrix CT we need to compute the possibility of one threat class given that a security threat occurred. We have four threat classes and twelve cloud security threats as explained above.

To discuss the relationship between classes of threats and security threats, Hashizume et al. classified threat classes based on the characteristics of individual security threats [113]. For example, in the class EH (external by human), there are four major security threats that occur most often including IAM (Weak Identity, Credential and Access) when attackers find the method to get the password to go through the system, AH (Account Hijacking) by using phishing attacks to access the targeted system, APT (Advanced Persistent Threats) by leveraging system vulnerabilities for attacking from outside, and DOS (Denial of Services). Additionally, DB (Data Breaches) is the security threat that attackers from outside intent to focus on. It should be noted that we can parameterise elements of the threat class matrix. However, their numerical values should be based on historical data and evidence. We obtain data for the CT matrix by analysing the severity and frequency of each threat and derive statistical data from [117] (see Table 7.7). In this,

for the EH class, the probability of threat APT is 0.3, the probabilities of three security threats IAM, AH, and DOS are equal with 0.2, and the probability of security threat DB is 0.1. For ET class, the major security threats often occur for threats API, APT, and STV. For IH class, the highest possibility for threat DB with 0.3, the probabilities of IAM, SV, and DL are 0.2, and the probability of DOS is 0.1. For IT class, the highest probability is for threat MI with 0.3. Threats DB, API, and APT share equal portions with 0.2 each, and the probability of DL is 0.1 (Table 7.7).

**Table 0.7** The probability of threat classes given that cloud security threat materialised

	DB	IAM	API	SV	AH	MI	APT	DL	IDD	ANU	DOS	STV
EH	0.1	0.2	0	0	0.2	0	0.3	0	0	0	0.2	0
ET	0	0	0.2	0.1	0.1	0	0.3	0	0	0.1	0	0.2
IH	0.3	0.2	0	0.2	0	0	0	0.2	0	0	0.1	0
IT	0.2	0	0.2	0	0	0.3	0.2	0.1	0	0	0	0

## 7.6 Application

Once the elements of ST, CT, and PT are determined, the proposed Mean Security Remediation Cost (MSRC) metric can be used to evaluate the impact of various materialized threats on cloud stakeholders. In this section we apply MSRC to three different use cases to investigate the consequences of materialized security threats on each security stakeholder. In each use case, we analyse the significances of the metric in terms of security management and implementation perspectives.

- Use case 1: MSRC cost for security stakeholders

To compute the mean security remediation cost for each cloud security stakeholder, we can expand from (7.7) to (7.9) as follows

$$MSRC_i = \left( \begin{array}{l} (ST_{i1}CT_{11} + ST_{i2}CT_{21} + \dots + ST_{ik}CT_{k1}) * PT_1 \\ + \dots + \\ (ST_{i1}CT_{1j} + ST_{i2}CT_{2j} + \dots + ST_{ik}CT_{kj}) * PT_j \\ + \dots + \\ (ST_{i1}CT_{1n} + ST_{i2}CT_{2n} + \dots + ST_{ik}CT_{kn}) * PT_n \end{array} \right) \quad (7.9)$$

**Table 7.8** shows mean security remediation cost for each cloud security stakeholder. It is clear that the highest security remediation cost is for Infrastructure Provider with \$13,699. The second highest amount is for Application Provider with \$5,660. Platform Provider spends less than Application Provider with \$5,193. The lowest cost is for Customers with \$481.

**Table 0.8** Mean Security Remediation Cost for each cloud security stakeholder

Stakeholders	Acronym	MSRC Value
Security Provider	SP	2417
Application Provider	AP	5660
Platform Provider	PP	5193
Infrastructure Provider	IP	13699
Customers	CS	481
Total		<b>27450</b>

In terms of security management in financial area, a security manager should plan to invest more budget for security in infrastructure when this figure takes about 50% of the remediation budget when security threats materialised into attacks. This figure also reveals that the most affected cloud security stakeholder is Infrastructure Provider when attacks occur. For the security remediation cost of the security provider, this figure is the fourth one after Infrastructure, Platform, and Application provider. This may indicate that security provider is not so important when security threats materialised into attacks. Security policies may be critical as soon as using cloud security services. For the security remediation cost of customers (\$481), there is a significance that insurance companies may consider this figure to apply the security insurance policy to impose on their

customers. For the total remediation security cost (\$27,450), insurance companies can use this figure to calculate the insurance cost for the cloud company with the budget scale for IT and security as demonstrated in this chapter.

- Use case 2: MSRC cost for various security classes

By using (7.9) for each security threat class, we have the security remediation cost for various security classes (see **Table 7.9**). It can be seen that the highest remediation cost is for threat class Internal Human with \$15,930. It accounts for 58% of the remediation total cost (\$27,450), in which, Infrastructure Provider takes most cost with \$11,152.

In comparison between internal and external security threat, we can see that the total remediation cost for external is \$7,594, while this figure for internal is \$19,853 that is equal to 2.61 times of external cost. This also indicates the difficulty of preventing from internal attacks to the system.

**Table 0.9** Mean Security Remediation Cost regarding the cloud security threat class

	EH	ET	IH	IT
SP	377	288	1594	158
AP	1884	2308	1273	195
PP	1884	144	1594	1570
IP	471	115	11152	1960
CS	94	29	317	40
Total	4710	2884	15930	3923

Regarding comparison between human and technology security threat, it can be seen that the total remediation cost for technology threat is \$6,807, whereas this figure for human is \$20,640, that is, three times more than that of technology. In terms of security implementation, human aspect, especially internal human, is very vital in securing the



cyber space. This can be understood that staff operating in an organisation have their privileges to access the cyber system. Importantly, these people can access the important database of the organisation. Intentionally or unintentionally, this is the resource of potential damaged by attackers because of their access right to the cloud system.

- Use case 3: MSRC cost by different security threats

To compute the mean security remediation cost for cloud security stakeholder  $i$  when threat  $j$  materialised, we can expand from (7.7) to (7.9) as follows

$$MSRC_i = (ST_{i1}CT_{1j} + ST_{i2}CT_{2j} + \dots + ST_{ik}CT_{kj}) * PT_j \quad (7.10)$$

By using (7.10) for each security threat, we have the security remediation cost for various security threats (see **Table 7.10**). As seen in Table 7.10, the highest remediation cost is for security threat Data Breaches (DB) with \$9,133. The second highest figure is for Advanced Persistent Threats (APT) with \$5,371. However, there is no remediation cost for security threat Insufficient Due Diligence (IDD). It can be explained that there is no security threat class probability when threat IDD materialised.

From the figure, there are several significant observations that security managers and practitioners can take advantage of. First, considering the two threats Data Breaches (DB) and Advanced Persistent Threat (APT), although the probability of threat APT (0.00546) is 6.6% higher than threat DB (0.00512), the security remediation cost for APT (\$5,371) is 70% less than that for DB (\$9,133). In terms of security financial, security manager should consider threat DB more than APT even though the chance of APT is more than that of DB. Second, the remediation cost for stakeholder Infrastructure Provider (IP) when threat DB materialised is \$5,692, which is the highest cost in Table 7.10. As seen in Table 7.9, the remediation cost for IP when threat class IH (Internal Human) materialised is \$11,152 that is the highest cost. From these two figures, it can be explained that the security cost to remediate the system for the internal attacks by human targeting to the database of the organisation is highest. This leads to the conclusion that

countermeasures for security should concentrate on protecting data from internal attacks by human.

**Table 0.10** Mean Security Remediation Cost regarding cloud security threats

	DB	IAM	API	SV	AH	MI	APT	DL	IDD	ANU	DOS	STV
SP	827	220	40	424	46	34	412	251	0	9	121	34
AP	940	365	234	633	273	42	2357	206	0	68	268	273
PP	1503	401	141	403	171	335	1575	359	0	4	285	17
IP	5692	1283	170	2693	46	418	948	1822	0	3	609	14
CS	171	46	6	80	10	9	79	51	0	1	26	3
Total	9133	2315	591	4233	546	838	5371	2689	0	85	1309	341

As a result, the security decisions from managers or security actions from practitioners depend on not only the probability of security threats when they materialise into attacks but also the security cost that is spent to remediate the attacker to make the system resilient. There are several security countermeasures that are applied to change the probability of security threat materialised or the remediation cost. In terms of applying hardware, several methods will be used such as using firewalls, loading balance. Regarding software, several methods can be applied such as anti-virus, software alteration, software upgrade, and a new and innovative method now is software define security. The investigation of these methods will be explained comprehensively in the next chapter when we apply MSRC metric in assessing security maturity levels for security domains of the CSCMM model (Chapter 3) and in counter measures to securing the cyber system.

In conclusion, the above application of the MSRC metric demonstrates its use with the data analysed from different security reports. MSRC can be tailored for a specific cloud system once the system is analysed and relevant input data are obtained. The number of stakeholders and the role of each stakeholder of the model needs to be

identified. The relationships among involved security elements, which are stakeholders, classes of security threat, security threats, and other security components are investigated. The realistic data, which is related to stakeholders, threat classes, security threats matrices, is obtained.

## **7.7 Summary**

Precise assessment of the security state of a cloud cyber space is critical to organisations because of the risks and impacts of security breaches on them. The challenge is to determine the relevant measures required to produce a meaningful security assessment. This chapter proposed Mean Security Remediation Cost (MSRC) as a new security metric that quantifies the remediation costs, borne by each stakeholder, caused by a security failure when a security threat materialised. To implement MSRC, a new cloud security stakeholder model is introduced to account for the security impact on each stakeholder. On application of MSRC to Cloud Computing, we demonstrate MSRC metric as a security decision supporting tool for the organisation's senior management and for security managers to identify specific security concerns and take appropriate security actions. The MSRC metric is deemed applicable to other systems or organisations in providing a quantitative assessment of systems/organisations overall security status. Our next chapter applies this new quantitative metric for measuring maturity levels of different security domains of our proposed CSCMM.

# Chapter 8

## Assessing Security for Cloud Security Capability Maturity Model

### 8.1 Introduction

In this chapter, all research results from five previous chapters from chapter 3 to chapter 7 will be integrated and investigated to assess the security level of our proposed security model Cloud Security Capability Maturity Model (CSCMM). In this chapter, the MSRC metric will be applied to assess maturity security levels of several security domains of CSCMM. For this purpose, the selection of security domains of CSCMM for MSRC entries will be investigated. Furthermore, a benchmark method to assess maturity security levels will be introduced. Subsequently, two different simulation results about the distribution of materialised security threat probabilities from chapter 5 and 6 will be validated and evaluated for MSRC. The simulated results between two different security threat probability computations will be investigated to indicate the advantages and disadvantages of each security threat model.

*Major contributions of this chapter are as follows:*

- It provides case studies where the proposed MSRC is applied to the Cloud Security Capability Maturity Model using relevant data on the cloud system in supporting the security decision making process.
- It proposed a benchmark method, which is based on computations of MSRC cost of each stakeholder for various security threats, to determine maturity security levels for investigated security domains of the CSCMM model.
- It provides different evaluations of MSRC to apply for CSCMM based on various methods to compute the distribution of materialised security threat probabilities.

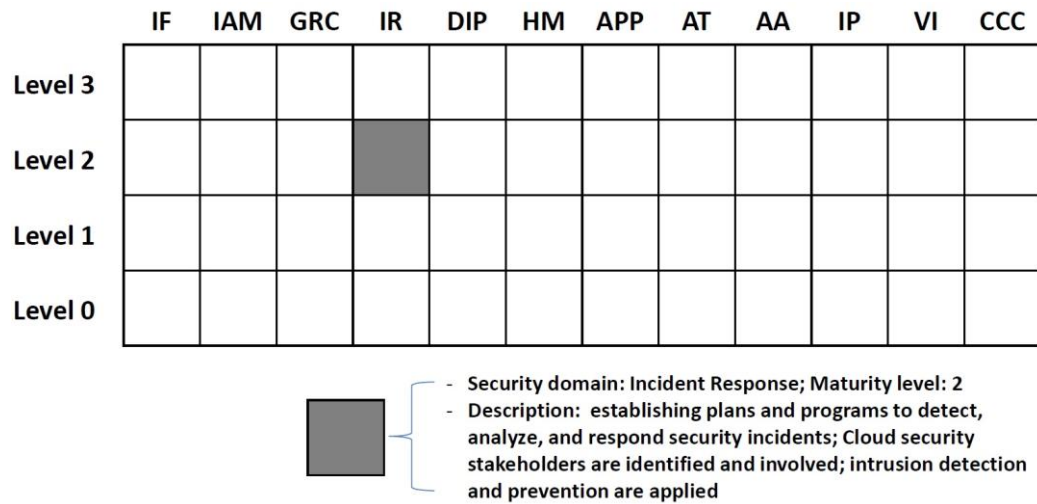
The remainder of the chapter is organised as follows. Section 8.2 introduces the application of MSRC to CSCMM and the choice of security domains for MSRC entries. Section 8.3 provides the benchmark method to determine maturity security levels of investigated security domains of CSCMM. Section 8.4 demonstrates several case studies applied for CSCMM. Section 8.5 investigates the comparison of various applications of MSRC on different computations of materialised security threat probabilities. Section 8.6 gives the comparison between the two security threat models. Finally, Section 8.7 concludes the chapter.

## **8.2 MSRC applied for CSCMM**

In this section, we demonstrate MSRC metric from chapter 7 that is applied for our proposed Cloud Security Capability Maturity Model (CSCMM) model to measure security levels of relevant security domains of the model. Several cases will be presented the effectiveness of MSRC metric in supporting not only security managers in making security decisions but also security practitioners in the security implementation. We will provide a brief summary of the CSCMM model, describe the applications of MSRC for CSCMM, and obtain the necessary parameters for MSRC.

### **8.2.1 CSCMM Model**

It is clear that a holistic security model needs to include a comprehensive number of security domains that can be assessed by either quantitative or qualitative metrics. This is essential to make a definitive statement concerning the overall status of security of a system. In terms of quantitative metrics, assessable factors such as security incidents, attack impacts, security vulnerabilities can be expressed in numbers and measured with mathematical tools. However, other factors, such as governance, human, or security awareness, are best assessed by qualitative metrics like the checking compliance, ticking boxes, survey results. This indicates that it is difficult to quantify many aspects of a security process such as users' behaviour, level of security education.



**Figure 0.1** CSCMM Model Architecture [111]

Cloud Security Capability Maturity Model (CSCMM) is such a holistic model that was introduced in [111]. The model has two dimensions: the security domain and the security maturity level. The domain dimension covers comprehensively all relevant security aspects/facets of a cloud system and the maturity dimension indicates the levels which each security domain achieves (Figure 8.1). It is created from the comprehensive consideration and the analysis of existing cyber security standards and frameworks. It presents the guidance to assist implementing and enhancing the cyber security capabilities on cloud systems. The model can be tailored for consistent goals of organisations with different cloud service model (IPSaaS) and deployments (Public, Private, and Hybrid Cloud) (see Chapter 3).

The horizontal dimension of the model covers twelve security domains including Infrastructure and Facilities (IF); Identities and Access Management (IAM); Governance, Risk, and Compliance management (GRC); Incident Response (IR); Data and Information Protection (DIP); Human Resource (HM); Cloud Application security (APP); Security Awareness and Training (AT); Audit and Accountability (AA); Interoperability and Portability (IP); Virtualisation and Isolation (VI); and Cloud Connection and Communication security (CCC).

The vertical dimension has four Security Maturity Levels (SMLs). Maturity levels are identified by the following attributes: (1) the SMLs measured separately in different domains; (2) the maturity level of a domain is determined by the minimum of all security practices implemented in that domain; (3) SML achievement should align with business objectives and organisation's security strategy. To ascertain a maturity level of a security domain, security metrics are needed to measure and analyse relevant security information to determine the level of security achieved. A metric framework was designed in Chapter 3, with six steps including inputs, metric plan, measuring, analyse, maturity level determination, and report. To cover all facets of a system, multiple metrics (both qualitative and quantitative) are needed. MSRC is a quantitative metric that can be used to evaluate security levels of relevant domains of a cloud system as described below.

### **8.2.2 Select Security Domains for Using MSRC**

With CSCMM, security facets of a cloud are represented by its domains and we need to analyse the characteristics and the contents of each CSCMM domain to identify the security domains that benefit from the use of the MSRC metric. We recognise three relevant domains that can be measured: The Identities and Access Management (IAM), the Data and Information Protection (DIP), and the Virtualisation and Isolation (VI) domains. As the purpose of IAM is to prevent unauthorised access to physical, virtual resources, and other properties of user's services and data, it can be seen that this domain is affected by account hijacking and identity and access management threats. Through exploiting these two security threats, attackers can leverage the failure in using multifactor authentication, weak password, or they can use the victim's account to get access to the target's resources. Similarly, security threats analysis applies to the DIP and the VI domains.

The overall analysis results in the identification of 3 cloud domains and 7 threats that can be quantified by our MSRC metric as summarised in **Table 8.1**. These threats include: Weak Identity, Credential and Access Management (IAM); Account Hijacking (AH);

Data Breaches (DB); Data Loss (DL); Advanced Persistent Threats (APT); System Vulnerabilities (SV); and Shared Technology Vulnerabilities (STV).

In terms of the relationship between security domains and classes of cloud security threat, all security cloud threat classes are involved in these three domains because of the following reasons. Security breaches within these three security domains are caused by threats that can be either external or internal. Security incidents occurred within these three security domains are caused by either human or technology threats.

**Table 0.1** Relationship between CSCMM security domains and threats

<b>Domains</b>	<b>Threats</b>	<b>Incidents</b>
<b>IAM</b>	<b>IAM, AH</b>	An attacker can leverage weak passwords uses or using multifactor authentication
<b>DIP</b>	<b>DB, DL, APT</b>	An attacker uses various attack techniques like SQL injections, cross-site scripting or exploits vulnerabilities from specific virtual cloud to extract data.
<b>VI</b>	<b>SV, STV</b>	An attacker can exploit vulnerabilities in virtual machine images, hypervisor, and network to attack isolated virtual machines

### 8.3 Benchmark Method

In the Oxford dictionary, benchmark is defined as “something that can be measured and used as a standard that other things can be compared with”. In the security management model, the benchmark method is used to standardise security action plans. In particular, in security standards such as The International Organisation for Standardisation (ISO) and The National Institute of Standards and Technology (NIST), the benchmark is expressed by maturity or hierarchical levels from one to five. In measuring security, Centre for Internet Security (CIS) used percentages to assign the level from 0 (0-25%) to Level 4 (75-100%) [15]. Other unit of time is also used by benchmark with maturity model in Lentz’s research when identifying the security levels from months (level 0), days (level 1), hours (level 2), to real-time (level 3) [99]. In this chapter, we



propose a benchmark method in terms of cost for calculating MSRC to assess the security levels of each security domain

## 8.4 Applications

In this section, we apply MSRC over four CSCMM use cases: assessing the maturity levels of three security domains of the CSCMM, improving maturity level of a security domain, supporting managers to recognise anomaly security breaches, and differentiating the impact of threat classes on security domains.

**Table 0.2** Probability distribution of seven security threats PT matrix ( $* 10^{-3}$ )

Domain	Threat	Probability ( $*10^{-3}$ )
IAM	IAM	1.877458
	AH	1.365424
DIP	DB	5.120339
	DL	2.560169
	APT	5.461695
VI	SV	4.096271
	STV	1.706780

To demonstrate MSRC on CSCMM model, we need to determine the element matrices of the MSRC metric that embrace ST, CT, and PT (see Chapter 7). We inherit the data for these three matrices from chapter 7 (Table 7.5 for ST, Table 7.6 for CT, and Table 7.3 for PT). As mentioned in 8.2.2, the relationship between three CSCMM security domains and seven security threats was investigated. From table 7.3, we have the probability distribution of seven security threats related to threat security domains represented in Table 8.2.

- Use Case 1 - Assessing maturity levels of security domains

The MSRC of each stakeholder for each investigated security domain can be calculated using (8.1) where a domain may cover multiple threats. The results will be used to determine the maturity level of a domain.

$$MSRC_{il} = \sum_{j \in T_l} ST_{ik} * CT_{kj} * PT_j \quad (8.1)$$

where i is the index of the stakeholder, l is the index of the security domain, and j is the index of the security threat.  $T_l$  is the threat space of domain l that may include several individual threats.

Or, specifically MSRC of each stakeholder for a domain is computed using (8.2)

$$MSRC_{il} = \sum_{j \in T_l} (ST_{i1}CT_{1j} + ST_{i2}CT_{2j} + \dots + ST_{ik}CT_{kj}) * PT_j \quad (8.2)$$

Using (8.2), we compute the MSRC of each stakeholder for each domain that represented in Table 8.3. For example, measuring MSRC of stakeholder AP for domain IAM ( $i = 2, l = 1, j = 2$  or  $5$ ) is shown in (8.3).

$$MSRC_{21} = (ST_{21}CT_{12} + ST_{22}CT_{22} + \dots + ST_{25}CT_{52}) * PT_2 + (T_{21}CT_{15} + ST_{22}CT_{25} + \dots + ST_{25}CT_{55}) * PT_5 = 1.1306 \quad (8.3)$$

**Table 0.3** MSRC of each stakeholder for each domain ( $* 10^{-3}$ )

Stakeholder	Acronym	$MSRC_{iam}$	$MSRC_{dip}$	$MSRC_{vi}$	$\sum MSRC$
Security Provider	SP	266	1490	458	2214
Application Provider	AP	638	3503	906	5047
Platform Provider	PP	572	3437	420	4429
Infrastructure Provider	IP	1329	8462	2707	12498
Customer	CS	56	301	83	440
Total		2861	17193	4574	24628

In the maturity level determination step of the metric framework [111], to compute the “benchmark value” of each security domain, a weighting method is applied. In the case when we have enough empirical data, we can set up these weights exactly. However, these data relate to security implementation of a company. Therefore, it is difficult to obtain the real data. For the sake of the simulation in this chapter we give an example for the table of domain weight value for each stakeholder (see Table 8.4). In this table, the weight value of each domain for each stakeholder (out of ten) is determined by the impact of a security domain on a stakeholder when a security failure occurs. Again, the weights can be considered as variables that depend on the organisation and the security environment. For example, the domain DIP (Data and Information Protection) has its weight value for stakeholder IP (Infrastructure Provider) of 9 because when a security failure happens the stakeholder IP is affected most. For stakeholder CS (Customers), the weight value for domain IAM is quite high at four in comparison with domains DIP and VI are one and one respectively. This is because when a security failure occurs in domain IAM, the most seriously impacted stakeholder is CS.

**Table 0.4** Domain weight value for each stakeholder (out of 10)

	$W_{IAM}$	$W_{DIP}$	$W_{VI}$
SP	3	5	3
AP	5	8	5
PP	4	6	4
IP	5	9	5
CS	4	1	1

Then the benchmark value (Bvalue) for each domain can be computed by:

$$Bvalue(DMi) = \sum_{j=1}^5 MSRC_{ij} * W_{ij} \quad (8.4)$$

where i is the index of the security domain; j is the index of the stakeholder.

Using (8.4), the benchmark values of the three security domains are shown in the **Table 8.5**.

**Table 0.5** Benchmark value for each domain

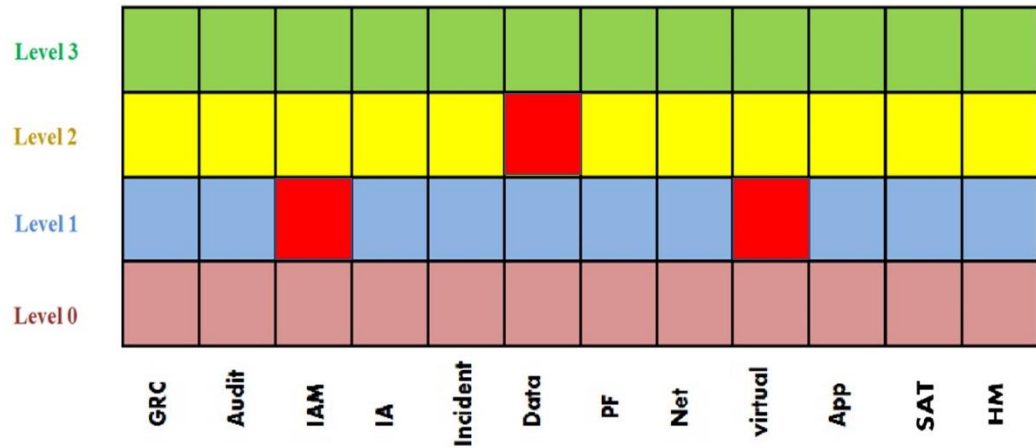
Domain	B-value
IAM	13.14
DIP	132.55
VI	21.20

The benchmark value of a domain can be compared with the corresponding standard maturity level (**Table 8.6**) to determine the maturity level of the domain.

**Table 0.6** Maturity level table

	Domain B-value		
Maturity level	$W_{IAM}$	$W_{DIP}$	$W_{VI}$
<b>0</b>	> 13.99	> 139.99	> 21.99
<b>1</b>	12 – 13.99	135 – 139.99	20 – 21.99
<b>2</b>	10 – 11.99	130 – 134.99	18 – 19.99
<b>3</b>	< 10	< 130	< 18

As the result of the comparison, the maturity level of each domain is determined as follows. The maturity level for domain IAM is at level 1, domain DIP at level 2, and domain VI at level 1 (see Figure 8.2). By determining the maturity level of each security domain quantitatively as done above, we arrive at a clear understanding of the implications associated with the security states of each security domain and hence we can devise sound strategies and appropriate actions to improve the security for each domain.



**Figure 0.2** Current maturity levels of three security domains (red box)

- Use Case 2 - Improving maturity level of a security domain

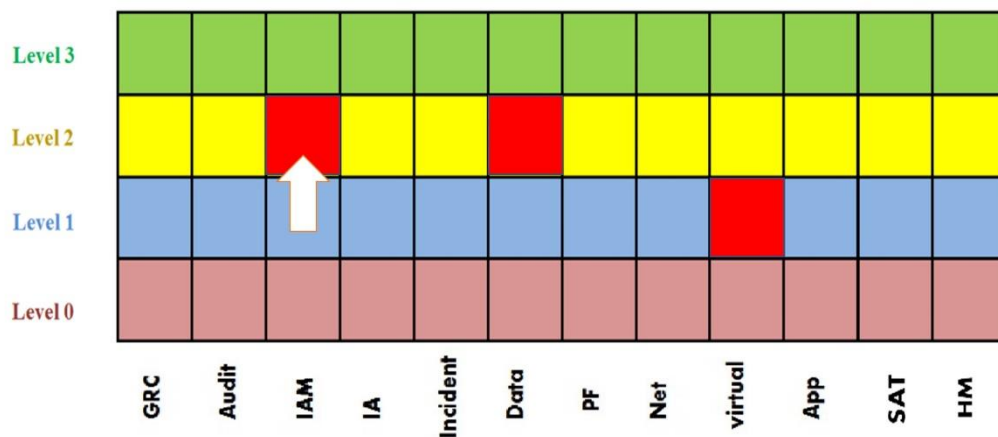
Maturity levels of security domains clearly depend on the security threat vector according to the MSRC-CSCMM framework. If the probability of security threats reduces, the maturity level will increase. Assuming that we can apply several security techniques to enhance security for domain Identities and Access Management (IAM), for example, suggest some standards or technologies such as LDAP (Lightweight Directory Access Protocol) to provide access to directory servers and SAML 2.0 (Security Authorisation Mark-up Language) for exchange of authentication and authorisation data between security domains [42].

**Table 0.7** Threat probability change

	Threats	Probability (*10 <sup>-3</sup> )	New Probability (*10 <sup>-3</sup> )
1	IAM	1.877458	1.715343
2	AH	1.365424	1.191252

This application will lead to a decrease in the probability of occurrences of the two security threats IAM and AH (Table 8.7). Using these new values of security probabilities in computing the new MSRC of each stakeholder for the security domain IAM, we obtain a new benchmark value of 11.91 for the IAM domain. Comparing this figure with the

benchmark table (Table 8.6), we find that the maturity level of security domain IAM has moved to a higher level (level 2) from a lower level (level 1) (See Figure 8.3). As a consequence, we can compute the estimated different MSRC cost between the old and new MSRC. This cost can be used for upgrading the maturity security level for domain IAM. From the business standpoint, this cost can be predicted and used to invest in potential security projects for enhancing security for domain IAM in the future.



**Figure 0.3** Security Maturity Level of IAM is improved to level 2 (red box)

- Use Case 3 - Supporting managers to identify anomaly security breaches:

Computing MSRC of each stakeholder for each security threat can support managers in identifying security breaches, calculating cloud security services costs, or finding the most cost-affected stakeholder. For example, security managers can make an effective decision by comparing MSRC costs of different security threats. For example, the probability of security threat Data Breaches – DB (0.00512) is lower than that of threat Advanced Persistent Threats (0.00546), however, the MSRC cost of the DB (\$9,133) is much higher than that of threat APT (\$5,371). This indicates that mitigating DB threat may be more critical than mitigating APT. Another significance of MSRC is that cloud security service costs can be quantitatively computed. For example, the MSRC of stakeholder CS (Customers) for domain DIP is 301. This cost is nearly five times higher than that for domain IAM with 56 (see Table 8.3). These figures can be used as the

reference points for calculating the costs of consumer cloud security services. In addition, we can use MSRC to recognise the most affected stakeholder. The total MSRC cost of the stakeholder IP (Infrastructure Provider) for all three domains is highest at 12,498 (see Table 8.3). This means that when security failures happen in three investigated domains (IAM, DIP, and VI), the most impacted stakeholder is IP and security decisions have to be made accordingly.

## **8.5 MSRC by Using Different Security Threat Model**

The significant key in the computation of MSRC is the probability of security threat materialised. Validation and evaluation above of MSRC is based on the distribution of security threat probability proposed in Chapter 4 in which the security threat model is based on a Markov chain and CVSS. This section will demonstrate MSRC for different security threat models from Chapter 5 and Chapter 6.

### **8.5.1 MSRC Demonstrated on Exist-escape Threat Model**

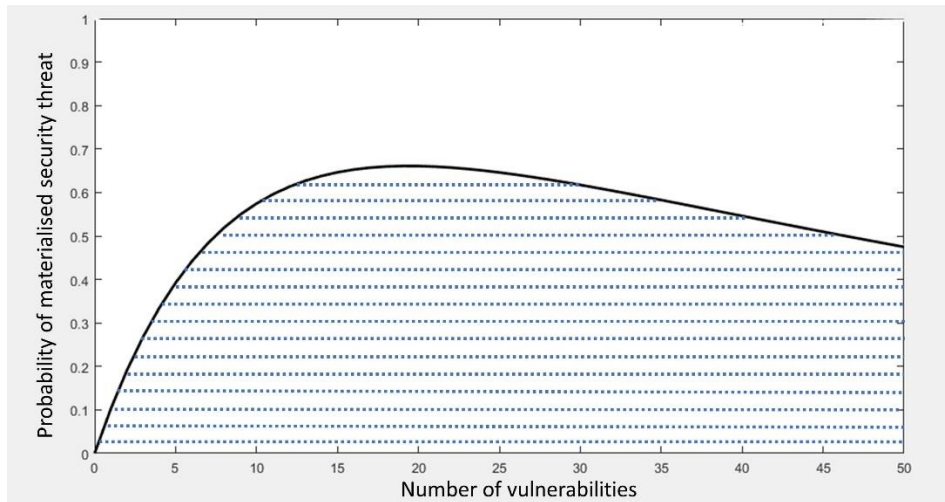
To compute MSRC for each stakeholder and compare MSRC among materialised security threats, the probability of security threat is determined. In this part, we will introduce the method to compute the distribution of the probability of materialised security threat based on exist-escape threat model investigated in Chapter 5. Then MSRC will be computed for each stakeholder, and for each security threat materialised.

- Calculate the weight and probability of cloud security threats

As introduced in chapter 5, we used the exist-escape threat model to investigate the probability of existed threat, realised threat, and threat materialised. We had the distribution of probability of materialised security threats for twelve cloud security threats seen in Figure 5.13. This showed the function of the probability of materialised security threats based on the number of vulnerabilities, the attack and control skills. The value of security threat probability varies by the number of vulnerabilities of the system. However, to compute MSRC, threat vector PT needs to be valued. Therefore, based on the

distribution of materialised security threat probability, we propose a weight method to determine the value of probability of materialised security threats in general.

The weight for each security threat is valued by the area shaped by the probability function. Figure 8.4 shows the distribution of the materialised security threat probability for threat DOS that is extracted from Figure 5.13 in section 5.7, Chapter 5.



**Figure 0.4** The distribution of probability materialised security threat for threat DOS (Denial of Service)

By using MATLAB simulator, we compute the area for twelve materialised security threat distributions showing in Table 8.8.

To make the model realistic, we take the probability of security vulnerabilities into consideration. For example, for threat Weak Identity, Credential and Access (IAM), it has two kinds of security vulnerabilities: insecure interfaces and APIs (V1) and Data-related vulnerabilities (V3). According to Table 6.1 in Chapter 6, the probability of cloud existed security vulnerabilities for V1 and V3 are 15.60% and 18.70% respectively. Therefore, after computing the security threat following the exist-escape model, we scale this distribution with consideration of the probability of cloud existed security vulnerabilities for each threat. As mentioned in chapter 4, the overall probability of all materialised security threats is about 0.03. Therefore, by scaling the weight with the

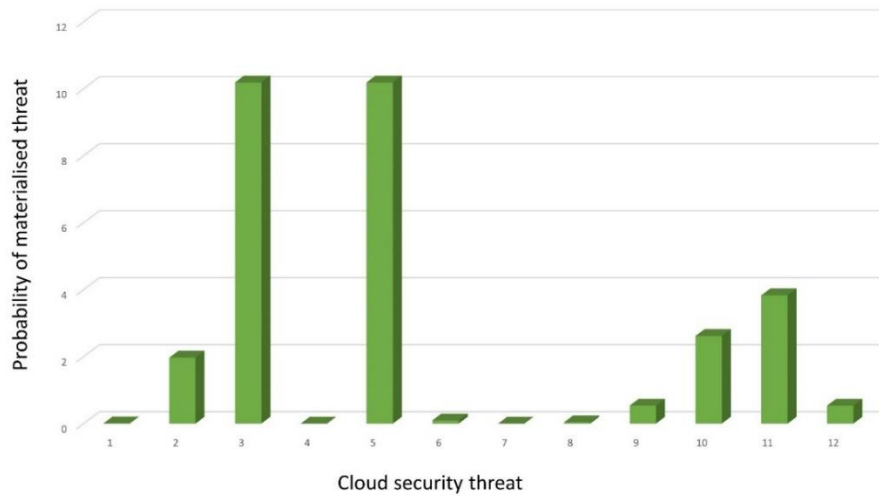


probability of cloud existed security vulnerabilities for each security threat, we have the distribution of materialised security threat probabilities for 12 security threats illustrated in Table 8.8 and Figure 8.5.

As seen in Table 8.8, the highest probability of materialised security threat is for threat APIs and AH with 0.0101 following by threat DOS, ANU and IAM with 0.0038, 0.0026, 0.0019 respectively. However, the lowest figure is for threat APT with  $0.0002 \times 10^{-3}$ .

**Table 0.8** Weight and probability of materialised security threat for 12 threats based on exist-escape threat model

Threat	Acronym	Weight	Probability (* $10^{-3}$ )
Data Breaches	DB	20.10595	0.005491
Weak Identity, Credential and Access	IAM	25.19959	1.967334
Insecure interfaces and APIs	API	24.40315	10.18799
System Vulnerabilities	SV	17.12751	0.001281
Account Hijacking	AH	24.40315	10.18799
Malicious Insiders	MI	12.44792	0.095342
Advanced Persistent Threats	APT	19.18775	0.000224
Data Loss	DL	19.97002	0.034959
Insufficient Due Diligence	IDD	20.52152	0.536455
Abuse and Nefarious Use	ANU	14.81104	2.616061
Denial of Service	DOS	27.30639	3.83042
Shared Technology Vulnerabilities	STV	20.52152	0.536455



**Figure 0.5** The distribution of probability materialised security threat for 12 threats based on exist-escape threat model

- MSRC cost for each security stakeholder in general and for each threat

By using (7.9) from Chapter 7, we calculate the MSRC for each stakeholder in general. Table 8.9 illustrates Mean Security Remediation Cost (MSRC) for each cloud security stakeholder. It can be seen that the highest security remediation cost is for Application Provider with \$5,072. The second highest amount is for Infrastructure Provider with \$4,390. Platform Provider may spend less with \$3,424. The lowest cost is for Customers with \$228.

**Table 0.9** MSRC for each stakeholder using exist-escape threat model

Stakeholders	Acronym	MSRC Value
Security Provider	SP	1190
Application Provider	AP	5072
Platform Provider	PP	3424
Infrastructure Provider	IP	4390
Customers	CS	228
Total		<b>14304</b>

By using (7.9) from Chapter 7 with the security threat probability above, we have the MSRC for each threat (see Table 8.10). As seen in Table 8.10, the highest mean security remediation cost is for security threat Insecure interfaces and APIs (API) with \$4,415. The second highest figure is for Account Hijacking (AH) with \$4,074. However, the lowest remediation costs are for security threat APT and IDD with \$0 in value

**Table 0.10** MSRC for each threat using exist-escape threat model

	DB	IAM	API	SV	AH	MI	APT	DL	IDD	ANU	DOS	STV
SP	1	231	300	0	346	1	0	3	0	26	271	11
AP	1	383	1748	0	2038	2	0	3	0	209	603	86
PP	2	420	1053	0	1273	13	0	5	0	13	639	5
IP	6	1344	1269	1	346	17	0	25	0	10	1366	4
CS	0	48	45	0	71	0	0	1	0	3	59	1
Total	10	2426	4415	1	4074	33	0	37	0	261	2938	107

## 8.5.2 MSRC Demonstrated on Attack-control Skill-based Threat Model

In this part, we introduce the method to calculate the probability of security threat materialised based on the attack-control skill-based threat model that is proposed in Chapter 5. Subsequently, based on the distribution of probabilities of twelve materialised security threats, MSRC will be demonstrated for each stakeholder, and for each security threat.

- Calculate the weight and probability of cloud security threats

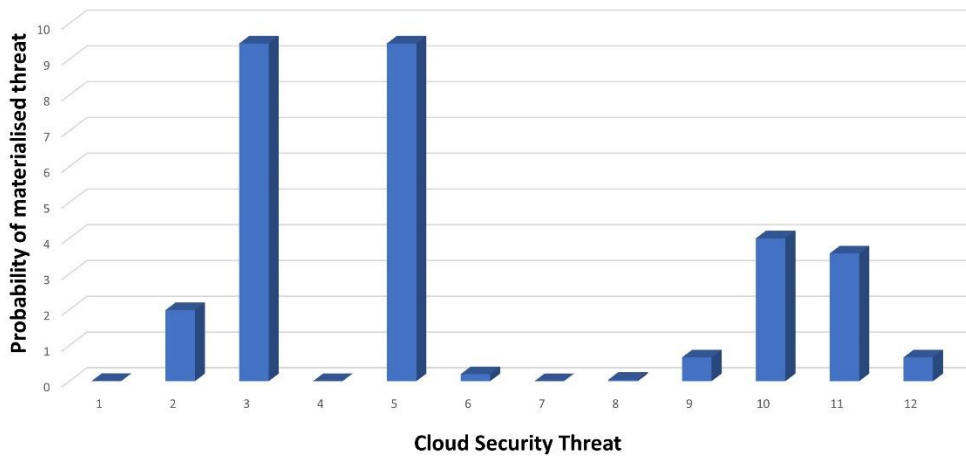
In Chapter 6, the attack-control skill-based model was proposed to compute the probability of a security threat materialised into attacks, in which, to investigate a threat model closed to reality, we focused on quantifying the attack and control skill. Especially,

in computing the process of security threat probability, we took consideration of the existence of security vulnerabilities of the system. As a result, we had the distribution of probability of materialised security threat for twelve cloud security threats seen in Table 6.4 and Figure 6.7 in Chapter 6. These show the data for different attack skill levels within the case min control level. As discussed in the previous part, to demonstrate MSRC, we need the vector PT in a determined case study. In this Chapter, we choose the case study of intermediate attack skill, as in table 8.11. Similarly, as mentioned in Chapter 4, the overall probability of all materialised security threats is about 0.03. Thus, we have the distribution of materialised security threat probabilities for 12 threats described in Table 8.11 and Figure 8.6.

Overall, the highest probability of the materialised security threat is for threats API (Insecure interfaces and APIs) and AH (Account Hijacking) with the same value of 0.0094. The lesser figures than API and AH are ANU and DOS with the value of 0.0039, and 0.0035 respectively. However, the probability of APT is lowest with  $0.00016 \times 10^{-3}$ .

**Table 0.11** Probability of materialised security threat for 12 threats based on attack-control skill-based model

Cloud security threat	Acronym	Weight	Probability (*10 <sup>-3</sup> )
Data Breaches	DB	0.02344	0.00378
Weak Identity, Credential and Access	IAM	12.3	1.98503
Insecure interfaces and APIs	API	58.5	9.44098
System Vulnerabilities	SV	0.00829	0.00133
Account Hijacking	AH	58.5	9.44098
Malicious Insiders	MI	1.2075	0.19487
Advanced Persistent Threats	APT	0.00099	0.00016
Data Loss	DL	0.2415	0.03897
Insufficient Due Diligence	IDD	4.1175	0.66449
Abuse and Nefarious Use	ANU	24.75	3.99426
Denial of Service	DOS	22.125	3.57062
Shared Technology Vulnerabilities	STV	4.1175	0.66449



**Figure 0.6** The distribution of probability materialised security threat for 12 threats based on attack-control skill-based model

- MSRC cost for each security stakeholder in general and for each threat

To quantify MSRC cost for each security stakeholder, we use (7.9) from chapter 7. Table 8.12 shows Mean Security Remediation Cost (MSRC) for each cloud security stakeholder. The greatest mean security remediation cost is for Application Provider with \$4,890. The second highest amount is for Platform Provider with \$3,236. The lowest cost is for Customers with \$218.

**Table 0.12** MSRC for each stakeholder using attack-control skill-based threat model

Stakeholders	Acronym	MSRC Value
Security Provider	SP	1145
Application Provider	AP	4890
Platform Provider	PP	3236
Infrastructure Provider	IP	4216
Customers	CS	218
Total		<b>13705</b>

Similarly, by using (7.9) from chapter 7 for each cloud security threat above, we have the MSRC for each threat (see Table 8.13). The highest mean security remediation cost is for security threat Insecure interfaces and APIs (API) with \$4,092. The second highest figure is for Account Hijacking (AH) with \$3,776. However, the lowest remediation costs are for security threat APT and IDD with \$0 in value.

**Table 0.13** MSRC for each threat using attack-control skill-based threat model

	DB	IAM	API	SV	AH	MI	APT	DL	IDD	ANU	DOS	STV
SP	1	233	278	0	321	3	0	4	0	40	252	13
AP	1	386	1620	0	1888	3	0	3	0	320	562	106
PP	1	424	976	0	1180	27	0	5	0	20	595	7
IP	4	1357	1176	1	321	34	0	28	0	16	1274	5
CS	0	49	42	0	66	1	0	1	0	4	55	1
Total	7	2449	4092	1	3776	68	0	41	0	400	2738	132

## 8.6 Comparison between the Two Security Threat Models

In this section, to reinforce our awareness of security threat models and how they are used in computing the probability of security threat materialised into attacks, we compare the two security threat models introduced in Chapter 5 and 6. These are exist-escape and attack-control skill-based models. First, we will analyse the similarities and differences between these two models to identify the strengths and weaknesses of each model in assessing the security state of the system. We then compare the probability distribution among these two models. Subsequently, MSRC for each stakeholder and each security threat between two different models will be analysed.

- Similarities and differences between two security threat models

The concepts and specifications of these two models were introduced and analysed in Chapter 5 and 6 comprehensively. In this part, we indicate the similarities and

differences of these two models in order to identify the advantages and disadvantages of each model in assessing security of the system to make security decisions to invest security budget in implementing security actions.

*Similarities:*

- The purpose of the models is to investigate security components related to a security threat and to identify the process by which a security threat is accomplished and materialised into attacks.

- The security components in the security model embrace attackers, security vulnerabilities of the system, controllers.

- The structure of the model is divided into two phases. The first phase indicates how a security threat exists. The second phase investigates how an existing security threat is undetected by the control system to make the system failure. Overall, the security model identifies how a security threat is accomplished, existed, escaped then materialised into attacks.

- In terms of the relationship between security vulnerabilities and security threats, both models used twelve different cloud security threats categorised by CSA. These twelve threats have closed relationship with seven kinds of cloud security vulnerabilities.

- Regarding the data demonstrated, Common Vulnerabilities Scoring System (CVSS) is used in both models.

*Differences:*

- The method to compute the probability of security existed, escaped, and materialised: for exist phase, while exist-escape model used search theory to determine the probability that attacker's capability to match with the security vulnerabilities of the system, attack-control model proposed the realistic model based on combinatorial mathematics to compute the probability of security existed, the chance that attacker is undetected by controllers. Because of different methods to compute the probability of materialised security threats, the formulas to compute this probability are also various.

- The probability of security vulnerabilities existed individually in the system: the exist-escape model does not take this probability into consideration, whereas the attack-

control model considered the probability of existed security vulnerabilities by using CVSS.

- In terms of data for attack and control skill level: while exist-escape model used empirical data to determine the skill levels of attackers and controllers, attack-control model used combinatory model to decide these levels.

- Probability of materialised security threats between two models

**Table 0.14** Probability of materialised security threat for 12 threats based on Exist-Escape and Attack-Control models

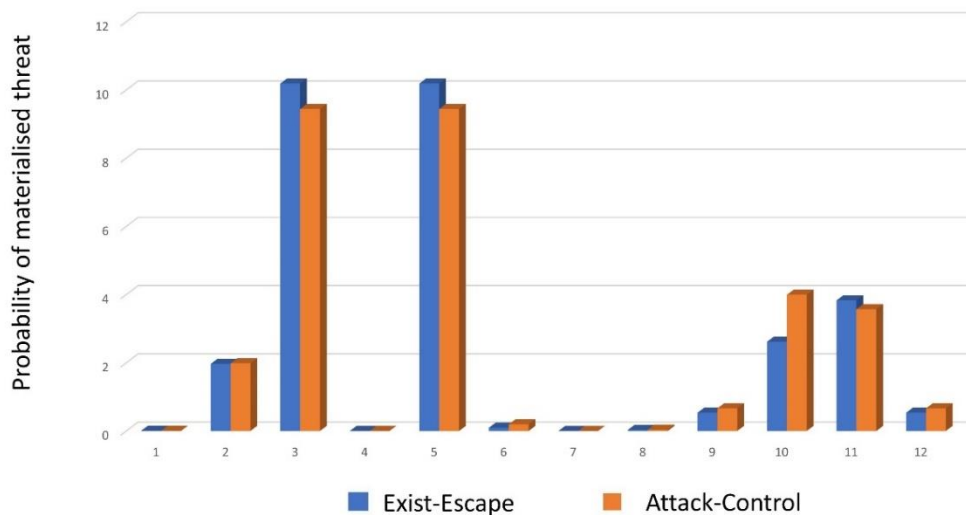
Threat	Acronym	Exist-Escape	Attack-Control
Data Breaches	DB	0.005491	0.00378
Weak Identity, Credential and Access	IAM	1.967334	1.98503
Insecure interfaces and APIs	API	10.18799	9.44098
System Vulnerabilities	SV	0.001281	0.00133
Account Hijacking	AH	10.18799	9.44098
Malicious Insiders	MI	0.095342	0.19487
Advanced Persistent Threats	APT	0.000224	0.00016
Data Loss	DL	0.034959	0.03897
Insufficient Due Diligence	IDD	0.536455	0.66449
Abuse and Nefarious Use	ANU	2.616061	3.99426
Denial of Service	DOS	3.83042	3.57062
Shared Technology Vulnerabilities	STV	0.536455	0.66449

From **Table 8.8** and **Table 8.11**, we have the comparison between the two materialised security threat probability distributions as seen in **Table 8.14** and **Figure 8.7**. Overall, the probability value of each threat is quite closed for both two models. Two security threat models (exist-escape and attack-control) have similar probability distributions. The probability of several security threats like Data Breaches (DB), Insecure interfaces and APIs (API), Account Hijacking (AH), Advanced Persistent



Threats (APT), and Denial of Service (DOS) in exist-escape model is higher than those in attack-control model. By contrast, the remainders in exist-escape are lower than those in attack-control model. In particular, the highest probability of materialised security threat is for threats API (Insecure interfaces and APIs) for exist-escape model at 0.0101, and for attack-control model it is 0.00944. The probability of APT is lowest with  $0.000224 \times 10^{-3}$  for exist-escape model, and  $0.00016 \times 10^{-3}$  for attack-control model

As a result, although there are several differences in problem solving approaches, and the method to compute the probability of materialised security threat between the two security threat models, simulation results prove that the figures are close and trustable between the two security threat models.



**Figure 0.7** The distribution of probability materialised security threat for 12 threats between two security threat models: Exist-Escape and Attack-Control

- MSRC for each stakeholder or each security threat between two security threat models

From Table 8.9 and Table 8.12, we have the comparison about MSRC for each security stakeholder between the two security threat models as seen in Table 8.15. It can be observed that the total MSRC between the two models is quite close with \$14,304 for exist-escape model and \$13,705 for attack-control model. The highest mean security remediation cost is for Application Provider with \$5,072 for exist-escape model, and

\$4,890 for attack-control model. The second highest amount is for Infrastructure Provider with \$4,390 for exist-escape model, and \$4216 for attack-control model. The lowest cost is for Customers with \$228 for exist-escape model, and \$218 for attack-control model.

**Table 0.15** MSRC for each stakeholder between Exist-Escape and Attack-Control threat models

Stakeholders	Acronym	Exist-Escape	Attack-Control
Security Provider	SP	1190	1145
Application Provider	AP	5072	4890
Platform Provider	PP	3424	3236
Infrastructure Provider	IP	4390	4216
Customers	CS	228	218
Total		<b>14304</b>	<b>13705</b>

From Table 8.10 and Table 8.13, we have the comparison about MSRC for each security threat between the two security threat models as seen in Table 8.16. The highest mean security remediation cost is for security threat Insecure interfaces and APIs (API) with \$4,415 for the exist-escape model, and \$4,092 for the attack-control model. The second highest figure is for Account Hijacking (AH) with \$4,074 for the exist-escape, and \$3,776 for the attack-control model, whereas, the lowest remediation cost is for security threat APT or IDD with \$0 in value for both security threat models.

**Table 0.16** MSRC for each threat between Exist-Escape and Attack-Control threat models

	DB	IAM	API	SV	AH	MI	APT	DL	IDD	ANU	DOS	STV
Exist-Escape	10	2426	4415	1	4074	33	0	37	0	261	2938	107
Attack-Control	7	2449	4092	1	3776	68	0	41	0	400	2738	132

## 8.7 Summary

Determination of security levels of the cloud system in general or each cloud security domain and identification of the cost which each stakeholder stands to lose when security failure occurs are very critical to an organisation. This supports security managers in making security decisions like the distribution of security budget for stakeholders or management security budget to the right place in implementing security actions. This chapter proposed the method to apply MSRC for CSCMM model. In particular, through analysing the collective of security domains within CSCMM that can be used for MSRC and through a benchmarking method, MSRC was applied successfully for CSCMM to assess the security maturity levels for three security domains like IAM, DIP, and VI. The chapter also investigated three case studies to analyse the application of MSRC. Furthermore, we compared two security models exist-escape and attack-control in terms of distribution of probability of materialised security threat and MSRC applications. The research results from the comparison of these two models are significantly close. This showed that the two proposed security threat models to compute the probability of materialised security threats are trustable to apply not only for MSRC computation but also for security risk calculation. Security risk cost estimation will be our potential research target that can incorporate the research results from these above proposed security threat models.

Regarding the above application of the MSRC metric for assessing the security of the CSCMM, this is a specific example to show that the MSRC can be used to assess partly the maturity security levels of several security domains within the CSCMM. The concepts of the MSRC and the CSCMM remain unchanged; however, they can be tailored for application to specific cloud systems provided the real data pertained to MSRC and CSCMM components is available.

# Chapter 9

## Conclusion and Future Work

In this chapter, we will conclude the research remarks and contributions of the thesis. Then future research directions will be described.

### 9.1 Research remarks and contributions of the thesis

Recently, we have observed that almost all IT systems are based on cloud computing, from critical infrastructure like E-Government, E-banking and now Internet of Things (IOTs), big data analytics, and software-defined systems/services. Cloud computing, which has benefits like flexibility, automatic software updates, increased collaboration, capital-expenditure free, work from anywhere, and environmentally friendly, has changed the way people work and communicate over the Internet. However, due to these benefits of cloud computing, clouds, as cyber infrastructures, are facing new security issues and challenges. There are several standards and models for cloud security. However, cloud security problems still occur.

We investigated previous cloud security models and identified that there are two major research gaps. First, security models lack a holistic model with an assessment to assess the security level for [17] a cloud system. Moreover, they have been reactive rather than proactive. They just focused on handling the security breaches when they occurred. They lack predictive models that could forecast potential attacks in the future. Second, these models mainly are based on qualitative measurements, which focus on the method of ticking the box or checking compliance. Quantitative metrics based on numerical measurements have been not taken into account. Out of existing models, Capability Maturity Models (CMM), which have been used by many organisations, offer a realistic

approach to address these problems using management by security domains and security assessment on maturity levels.

In this thesis, we aimed to investigate appropriate quantitative security metrics and proposed a novel Capability Maturity Model with these above quantitative security metrics for securing cloud computing. For this effort, first, we proposed Cloud Security Capability Maturity Model (CSCMM) with twelve security domains and four maturity security levels. Furthermore, we designed a security metric framework to select relevant security metrics to assess the security level of CSCMM. This content was described in Chapter 3 that addressed the first two research questions. Second, we identified the importance of determination of computation of materialised security threat probability; we developed three new security threat models, which are Markov, Exist-Escape, and Skill-Based Attack-Control, calculating the probability of security threat materialised into attacks. These three models were investigated and presented in Chapter 4, 5, and 6 that addressed the research question 4. Third, we proposed a novel quantitative security metric named Mean Security Remediation Cost (MSRC) that uses the simulation results from the three threat models above to validate and evaluate CSCMM via security metrics framework. MSRC metric was discussed in Chapter 7 that addressed the research question 3. A Cloud Security Capability Maturity Model (CSCMM) with one quantitative security metric Mean Security Remediation Cost (MSRC) and three various security threat models for computing security threats probability were validated, evaluated, and research results compared with previous studies. The application of MSRC in CSCMM was described in Chapter 8 that addressed the research question 5. As a result, the major research results of the thesis were delivered in academic papers submitted and published in international peer-reviewed journals and conferences in cyber security and cloud computing.

However, for validation and evaluation, we used published security database from security companies such as IBM, BitDefender, Norton, and Gartner. With achieved research results, we strongly believe that the CSCMM model will be applied effectively with a real cyber security database.

Although the thesis still has several limitations needed to be addressed, it has several significant research contributions:

- The definitions of cyber space and cyber security are reviewed and refined. Furthermore, we proposed new concepts of cyber space and cyber security. By doing this, we were thoroughly aware of the fundamentals to investigate security issues and challenges in cloud computing, especially in cloud security models and standards that the thesis focused on.

- We proposed a novel Cloud Security Capability Maturity Model (CSCMM). The model also supports security managers to set the security target for each security domain within the CSCMM. Additionally, the model significantly assists security practitioners to deal with a security issue once the CSCMM model indicates where the system is damaged. Furthermore, we proposed a security metric framework to assess the level of each security domain of the CSCMM model. The framework also indicated the importance of using quantitative security metrics. The proposed CSCMM model and security metric framework contribute to the development of knowledge of Maturity model theory.

- We developed three security threat models that quantify the probability that a security threat has been materialised into attacks. For the first model, we modelled a security threat as a Markov chain. To compute the probability of a materialised security threat, we did use CVSS database. As a result, the distribution of cloud security threat probabilities was computed. For the second model, we re-defined a security threat with two sub-processes calling exist and escape that took attackers, security threats, security vulnerabilities, controllers into consideration. We used search theory to compute the probability of each of the sub-processes and overall probability of materialised security threats. For the third model, we developed a security threat model by taking the method to determine the skill levels of attackers and controllers into account. This method allowed the computation of the probability of a security threat existed that is close to reality. We did compare our solutions with previous study to compute the probability of materialised security threats. These three models were significant inputs in generating our

proposed MSRC metric for assessing CSCMM. Furthermore, the research results in computing probability of a materialised security threat from these three models also are significant in determining security risk and insurance.

- We created a new security quantitative metric named Mean Security Remediation Cost (MSRC). This metric provided the method to estimate the cost that security stakeholders have to spend when a security threat materialised into attacks. For this purpose, a security stakeholder model was designed to indicate security stakeholders involved in security breaches and assess how security breaches impact a security stakeholder in terms of cost. We demonstrated MSRC metric as a supporting tool of security making-decision for the senior management to indicate specific security weaknesses and take appropriate security actions

- The simulation results are demonstrated, validated, and evaluated by proposed Cloud Security Capability Maturity Model, Mean Security Remediation Cost metric, and three security threat models to compute the probability of materialised security threats. Via MSRC, the specific costs for each of the cloud security stakeholders were indicated. Based on this result, security managers can make security decisions in distributing the security budget among cloud security stakeholders. Furthermore, MSRC also was used to compute the cost in terms of security threats. This indicated where the system is impacted most and suggested which security actions to tackle security attacks materialised by security threats that costs most. Importantly, MSRC was also used to assess the maturity security level of specific security domains/facets of the CSCMM model. The significance of security maturity level determination is that it indicated where the cloud security system is and how to improve the security levels through being aware of weaknesses of the cloud system.

## **9.2 Future Research Direction**

In summary, the thesis contributed to the theoretical body of knowledge in cloud security. The thesis proposed for the first time a Capability Maturity Model for cloud security. Additionally, the novel model will be used in practice by the managers, security

experts and practitioners for both assessing the overall security status of the organisation/system and taking new quantitative measures to strengthen weaknesses of any specific aspects of the system as identified by the assessment. Although the thesis has significant research results, it has several limitations.

First, in terms of the CSCMM model, the stakeholder model can be refined to narrow down specific parties impacted by an attack. By doing this, we can determine which stakeholder closely impacts on the system. In this thesis, three security domains within the CSCMM model were investigated, other security domains/facets have not been taken into account.

Second, regarding security threat models, we have not considered several security factors, which are complex and pertained to a specific environment, including the probability that an attacker exists given the environment, the additional capabilities of the security controller (organisational policies, available budget), and the time that events occur.

Third, the thesis focused on developing a quantitative metric named MSRC that paid attention to estimating the cost. More quantitative metrics to cover a more set of domains of the CSCMM model will be explored in the future.

Fourth, the database for validating and evaluating CSCMM model and MSRC metric was just used from the published security reports. The model needs the real security data about security vulnerabilities from cloud companies and organisations for testing, adjusting, and tailoring the MSRC metric and CSCMM to their specific environments. However, with achieved research results, we strongly believe that the CSCMM model will be applied effectively with a real cyber security database.

From identifying the research results and limitations of the thesis, future research directions will be described as follows.

First, we will keep researching security threat models to identify remaining security factors that the thesis has not been able to consider such as the existence of attackers, favourable conditions for launching a security attack. Moreover, we will develop advanced quantitative security metrics in terms of time and performance which need to



be developed to measure a wider variety of security domains within CSCMM. Furthermore, qualitative security metrics also need to be considered to measure which security domain relates to organisational, culture, and other human aspects.

Second, to fully evaluate the proposed CSCMM model and the MSRC metric, we will focus on working with specific companies to obtain database: (1) Collecting data from different type of cloud private, public, or hybrid; (2) Obtaining data about security stakeholders in terms of spending for cyber security in general for each security domain in particular; (3) Taking data about security vulnerabilities specific in cloud computing; (4) Gathering data about consequences when a cyber-attack occurs; (5) Furthermore, obtaining data about attackers, defenders, and other favourable security factors like technology environment and the time.

Third, we will develop a software that automatically measures security levels of security domains within the CSCMM. Several recent security models or standards have been mainly using ticking the box or checking compliance methods to assess security levels of each of the security activities or actions. This is done manually and is based partially on the subjective assessment of staff in an organisation. We are also aware that qualitative metrics are critical because of many organisational or cultural aspects. Our proposed software will support measuring security levels automatically for several security activities that relate to security vulnerabilities and other technical performances. The software will automatically collect the data, measure security levels of each security action, analyse to determine security maturity levels, and finally report to responsible managers and experts.

Fourth, we will use our proposed security threat models and the computation of the probability of security threat materialised into attacks in researching security risk especially in estimating security risk cost. In general, cyber risk is involved in any risk of financial loss, disruption or damage to the reputation of an organisation resulting from the failure of its information technology systems. Cyber security risk refers to the chance of a security threat materialised into attacks and the consequences estimated when

security breaches related to the security threat occur. For this purpose, we will investigate security risk models and tailor our threat model to estimate security risk cost.

In conclusion, the thesis has investigated the broad diversity of definitions, technologies, and models in cyber security, especially in cloud security. The aim of the thesis was to address the research challenge that has not been tackled before: a novel Capability Maturity Model with quantitative metrics for securing Cloud Computing. The thesis has proposed directions for future research. From the outcomes, a software package can be developed and used as a valuable tool for assessing the security of a cloud system. The proposed model and the quantitative metrics can be tailored to a particular cloud on implementation once relevant data can be provided.

# Bibliography

- [1] M. C. Lacity, *Advanced outsourcing practice: Rethinking ito, bpo and cloud services*. Palgrave Macmillan, 2012.
- [2] Gartner 16 January 2019, *Forecast: Public Cloud Services, Worldwide, 2016-2022, 4Q18 Update*, accessed 1 May 2019, <<https://www.gartner.com/document/code/343437>>
- [3] Forrester 2018, *Forrester Analytics: Cloud Security Solutions Forecast, 2018 To 2023 (Global)*. accessed 1 May 2019, <<https://www.forrester.com/report/Forrester+Analytics+Cloud+Security+Solution+s+Forecast+2018+To+2023+Global/-/E-RES148715>>
- [4] Clavister, "Security in the cloud," *White paper*, 2008.
- [5] Cloud Security Alliance 2010, "Top threats to cloud computing, version 1.0," accessed 1 May 2019, <<http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>>
- [6] European Union Agency for Network and Information Security 2014, "Security standards for cloud usage," accessed 1 May 2019, <https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf>.
- [7] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing v3. 0," *Cloud Security Alliance*, 2011.
- [8] Humphrey, "CMM," (in Eng), *IEEE*, vol. 1, no. 1999, 16/7/2001 1989.
- [9] P. D. Curtis and N. Mehravari, "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," in *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*, 2015, pp. 1-6.
- [10] Cloud Security Alliance 2015, "Cloud Forensics Capability Maturity Model", accessed 1 December 2019, <<https://cloudsecurityalliance.org/artifacts/cloud-forensics-capability-model/>>
- [11] N. H. Ab Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *computers & security*, vol. 49, pp. 45-69, 2015.

- [12] B. Manral, G. Somani, K.-K. R. Choo, M. Conti, and M. S. Gaur, "A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, p. 124, 2019.
- [13] W. Thomson, "Lord Kelvin: Electrical units of measurement. Popular lectures and addresses," ed: Macmillan, London, 1889.
- [14] A. Jaquith, *Security metrics*. Pearson Education, 2007.
- [15] Center for Internet Security, "The CIS (Center for Internet Security) security metrics," ed, 2010.
- [16] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, *Performance measurement guide for information security*. 2008.
- [17] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 2016, pp. 1-7.
- [18] J. Allen and N. Mehravari, "How to Be a Better Consumer of Security Maturity Models," Citeseer2014.
- [19] European Union Agency for Network and Information Security 2014, "Security standards for cloud usage," accessed 5 December 2019, <https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf>.
- [20] J. Archer and A. Boehm, "Security guidance for critical areas of focus in cloud computing," *Cloud Security Alliance*, vol. 2, pp. 1-76, 2009.
- [21] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2. 1," *Cloud Security Alliance*, pp. 1-76, 2009.
- [22] B. Swain, P. Agcaoili, M. Pohlman, and K. Boyle, "Cloud controls matrix," ed, 2010.
- [23] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45-77, 2007.
- [24] M. Whitman and H. Mattord, *Management of information security*. Cengage Learning, 2013.
- [25] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97-102, 2013.
- [26] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*. MIT press, 1961.

- [27] International Telecommunication Union, *Overview of cybersecurity (ITU-T X.1205)*. 04/2008, p. 8.
- [28] Australia's Government, *Strong and Secure. A Strategy for Australia's National Security*. accessed 10 November 2015, [http://apo.org.au/files/Resource/dpmc\\_nationalsecuritystrategy\\_jan2013.pdf](http://apo.org.au/files/Resource/dpmc_nationalsecuritystrategy_jan2013.pdf)
- [29] Canada's Government, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada (2010)*, accessed 10 November 2015 <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-scrt-strtg/cbr-scrt-strtg-eng.pdf>
- [30] The Netherland's Government, *National Cyber Security Strategy 2: From Awareness to Capability (2013)*, accessed 10 November 2015 [http://english.nctv.nl/images/national-cyber-security-strategy-2\\_tcm92-520278.pdf](http://english.nctv.nl/images/national-cyber-security-strategy-2_tcm92-520278.pdf)
- [31] Germany's Government, *Cyber Security Strategy for Germany (2011)*, accessed 10 November 2015, <https://ccdcoe.org/cyber-security-strategy-documents.html>
- [32] New Zealand's Government, *New Zealand's Cyber Security Strategy*, accessed 10 November 2015, <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-december-2015.pdf>
- [33] R. Ottis and P. Lorents, "Cyberspace: Definition and implications," in *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, pp. 267-270.
- [34] S. J. Shackelford, "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance," *Am. UL Rev.*, vol. 62, p. 1273, 2012.
- [35] M. Gasser, *Building a secure computer system*. Van Nostrand Reinhold Company New York, NY, 1988.
- [36] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining Cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.
- [37] A. Behl and K. Behl, "An analysis of cloud computing security issues," in *Information and Communication Technologies (WICT), 2012 World Congress on*, 2012, pp. 109-114.
- [38] D. Catteddu, "Cloud Computing: benefits, risks and recommendations for information security," in *Web Application Security*: Springer, 2010, pp. 17-17.
- [39] Cloud Standard Customer Council 2015, "Security for Cloud Computing Ten Steps to Ensure Success Version 2.0," accessed 10 November 2015, [203](http://www.cloud-</a></p>
</div>
<div data-bbox=)

council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf.

- [40] W. R. Claycomb and A. Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges," in *2012 IEEE 36th Annual Computer Software and Applications Conference*, 2012, pp. 387-394.
- [41] S. Farhan Bashir and S. Haider, "Security threats in cloud computing," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, 2011, pp. 214-219.
- [42] Cloud Security Alliance 2016, *The Treacherous Twelve - Cloud Computing Top Threats in 2016*. accessed 15 November 2017 <https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/>
- [43] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.
- [44] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation computer systems*, vol. 25, no. 6, pp. 599-616, 2009.
- [45] I. Consortium, "Information security management maturity model," ed: Versión, 2009.
- [46] G. Karokola, S. Kowalski, and L. Yngstrom, "Secure e-government services: Towards a framework for integrating it security services into e-government maturity models," in *Information Security South Africa (ISSA), 2011*, 2011, pp. 1-9: IEEE.
- [47] G. B. White, "The community cyber security maturity model," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, 2011, pp. 173-178: IEEE.
- [48] P. E. Black, K. Scarfone, and M. Souppaya, "Cyber security metrics and measures," *Wiley Handbook of Science and Technology for Homeland Security*, 2008.
- [49] B. Bates, K. M. Goertzel, and T. Winograd, *Measuring Cyber Security and Information Assurance: A State-of-the Art Report*. Information Assurance Technology Analysis Center, 2009.
- [50] W. S. Humphrey, *A discipline for software engineering*. Addison-Wesley Longman Publishing Co., Inc., 1995.

- [51] W. K. Brothby, "Information security management metrics," *A definitive guide to effective security monitoring and*, 2009.
- [52] Center for Internet Security, "The CIS security metrics," ed, 2010.
- [53] R. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," in *Software Engineering Advances, 2007. ICSEA 2007. International Conference on*, 2007, pp. 60-60: IEEE.
- [54] S. Kowalski, R. Barabanov, and L. Yngström, "Information Security Metrics: Research Directions," 2011.
- [55] J. P. Ravenel, "Effective operational security metrics," *Information Systems Security*, vol. 15, no. 3, pp. 10-17, 2006.
- [56] W. K. Brothby and G. Hinson, *Pragmatic security metrics: applying metametrics to information security*. CRC Press, 2013.
- [57] D. S. Herrmann, *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. CRC Press, 2007.
- [58] S. E. Schimkowitsch, "Key Components of an Information Security Metrics Program Plan," Citeseer, 2009.
- [59] S. C. Payne, "A guide to security metrics," *SANS Security Essentials GSEC Practical Assignment Version*, vol. 1, 2010.
- [60] W. Jansen, *Directions in security metrics research*. Diane Publishing, 2010.
- [61] G. Campbell and M. Blades, "Building a metrics program that matters," *Journal of healthcare protection management: publication of the International Association for Hospital Security*, vol. 30, no. 1, p. 116, 2014.
- [62] A. Nourian and S. Madnick, "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 2-13, 2018.
- [63] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, "k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 30-44, 2014.
- [64] E. Aroms, "NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems," 2012.
- [65] V. Bellandi, S. Cimato, E. Damiani, G. Gianini, and A. Zilli, "Toward economic-aware risk assessment on the cloud," *IEEE Security & Privacy*, vol. 13, no. 6, pp. 30-37, 2015.

- [66] Oxford Dictionary, *Defintion of Threat*, accessed 10 November 2015 <https://en.oxforddictionaries.com/definition/threat>
- [67] National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, accessed 20 May 2019 <https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf>
- [68] S. Gerić and Ž. Hutinski, "Information system security threats classifications," *Journal of Information and Organizational Sciences*, vol. 31, no. 1, pp. 51-61, 2007.
- [69] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and computing a value based cyber-security measure," *Information Systems and e-Business Management*, vol. 10, no. 4, pp. 433-453, 2012.
- [70] S. Patel and J. Zaveri, "A risk-assessment model for cyber attacks on information systems," *Journal of Computers*, vol. 5, no. 3, pp. 352-359, 2010.
- [71] J. Almasizadeh and M. A. Azgomi, "A stochastic model of attack process for the evaluation of security metrics," *Computer Networks*, vol. 57, no. 10, pp. 2159-2180, 2013.
- [72] R. Böhme and F. C. Freiling, "On metrics and measurements," in *Dependability metrics*: Springer, 2008, pp. 7-13.
- [73] R. Ortalo, Y. Deswarte, and M. Kaâniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, no. 5, pp. 633-650, 1999.
- [74] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *IEEE Transactions on Software Engineering*, vol. 23, no. 4, pp. 235-245, 1997.
- [75] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, p. 62, 2017.
- [76] S. Xu, "Cybersecurity dynamics: A foundation for the science of cybersecurity," in *Proactive and Dynamic Network Defense*: Springer, 2019, pp. 1-31.
- [77] N. T. Le and D. B. Hoang, "Security threat probability computation using Markov Chain and Vulnerability Scoring System," in *The 28th International Telecommunication Networks and Applications Conference*, 2018.



- [78] A. Ramos, M. Lazar, R. Holanda Filho, and J. J. Rodrigues, "Model-Based Quantitative Network Security Metrics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2704-2734, 2017.
- [79] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*, 2002, pp. 49-63: IEEE.
- [80] X. Li, P. Parker, and S. Xu, "A stochastic model for quantitative security analyses of networked systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 28-43, 2011.
- [81] K. S. Trivedi, *Probability and statistics with reliability, queuing, and computer science applications*. Wiley Online Library, 1982.
- [82] A. Bar, B. Shapira, L. Rokach, and M. Unger, "Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis," in *Software Science, Technology and Engineering (SWSTE), 2016 IEEE International Conference on*, 2016, pp. 28-36: IEEE.
- [83] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 1, pp. 167-186, 2004.
- [84] B. Anderson, D. Quist, J. Neil, C. Storlie, and T. Lane, "Graph-based malware detection using dynamic analysis," *Journal in computer Virology*, vol. 7, no. 4, pp. 247-258, 2011.
- [85] H. M. Almohri, L. T. Watson, D. Yao, and X. Ou, "Security optimization of dynamic networks with probabilistic graph modeling and linear programming," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 4, pp. 474-487, 2015.
- [86] B. O. Koopman, "Search and screening," *OEG Rep.*, 1946.
- [87] J. Frost, "Principles of search theory, part I: Detection," *Response*, 17 (2), pp. 1-7, 1999.
- [88] J. A. Major, "Advanced techniques for modeling terrorism risk," *The Journal of Risk Finance*, vol. 4, no. 1, pp. 15-24, 2002.
- [89] B. O. Koopman, "A THEORETICAL BASIS FOR METHOD OF SEARCH AND SCREENING," COLUMBIA UNIV NEW YORK 1946.

- [90] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," in *Quality of Protection*: Springer, 2006, pp. 49-64.
- [91] E. J. Byres and D. J. Leversage, "Estimating a System's Mean Time-to-Compromise," *IEEE Security & Privacy*, vol. 6, pp. 52-60, 2008.
- [92] R. B. Allenby and A. Slomson, *How to count: An introduction to combinatorics*. CRC Press, 2011.
- [93] A. Bobbio, C. Ferraris, and R. Terruggia, "New challenges in network reliability analysis," *CNIP*, vol. 6, pp. 554-564, 2006.
- [94] L. O'Connor, "The inclusion-exclusion principle and its applications to cryptography," *Cryptologia*, vol. 17, no. 1, pp. 63-79, 1993.
- [95] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, no. 5, pp. 267-270, 2009.
- [96] B. Stevanović, "Maturity models in information security," *International Journal of Information*, vol. 1, no. 2, 2011.
- [97] B. Duncan and M. Whittington, "Compliance with standards, assurance and audit: does this equal security?," in *Proceedings of the 7th International Conference on Security of Information and Networks*, 2014, p. 77: ACM.
- [98] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1-26, 2004.
- [99] R. Lentz. 2015, *Security Intelligence Maturity Model*. Logrhythm, accessed 12 November 2019, <https://logrhythm.com/security-intelligence-maturity-model-ciso-2015/>
- [100] Y. You, I. Cho, and K. Lee, "An advanced approach to security measurement system," *The Journal of Supercomputing*, vol. 72, no. 9, pp. 3443-3454, 2016.
- [101] S. M. Tonni, M. Z. Rahman, S. Parvin, and A. Gawanmeh, "Securing big data efficiently through microaggregation technique," in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2017, pp. 125-130: IEEE.
- [102] S. Thalia, A. Tuteja, and M. Dutta, "Towards quantification of information system security," in *Computational Intelligence and Information Technology*: Springer, 2011, pp. 225-231.

- [103] S. Noel, S. Jajodia, L. Wang, and A. Singhal, "Measuring security risk of networks using attack graphs," *International Journal of Next-Generation Computing*, vol. 1, no. 1, pp. 135-147, 2010.
- [104] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring network security using dynamic bayesian network," in *Proceedings of the 4th ACM workshop on Quality of protection*, 2008, pp. 23-30: ACM.
- [105] A. Gawanmeh and A. Alomari, "Challenges in formal methods for testing and verification of cloud computing systems," *Scalable Computing: Practice and Experience*, vol. 16, no. 3, pp. 321-332, 2015.
- [106] C. Wang and W. A. Wulf, "Towards a framework for security measurement," in *20th National Information Systems Security Conference, Baltimore, MD*, 1997, pp. 522-533.
- [107] H. Ghayvat, S. Mukhopadhyay, J. Liu, A. Babu, M. E. E. Alahi, and X. Gui, "Internet of things for smart homes and buildings," *Australian Journal of Telecommunications and the Digital Economy*, vol. 3, no. 4, 2015.
- [108] D. Hoang, "Software Defined Networking? Shaping up for the next disruptive step?," *Australian Journal of Telecommunications and the Digital Economy*, vol. 3, no. 4, 2015.
- [109] K. Huang, C. Zhou, Y.-C. Tian, W. Tu, and Y. Peng, "Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks," in *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*, 2017, pp. 1-6: IEEE.
- [110] Q. Hu, M. R. Asghar, and N. Brownlee, "Evaluating network intrusion detection systems for high-speed networks," in *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*, 2017, pp. 1-6: IEEE.
- [111] N. T. Le and D. B. Hoang, "Cloud Maturity Model and metrics framework for cyber cloud security," *Scalable Computing: Practice and Experience*, vol. 4, pp. 277-290, 2017.
- [112] D. B. Hoang and S. Farahmandian, "Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies," in *Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications*, S. Y. Zhu, S. Scott-Hayward, L. Jacquin, and R. Hill, Eds. Cham: Springer International Publishing, 2017, pp. 3-32.

- [113] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 5, 2013.
- [114] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 199-212: ACM.
- [115] S. M. Ross, *Introduction to probability models*. Academic press, 2014.
- [116] National Vulnerability Database, accessed 15 May 2019, <http://nvd.nist.gov/>
- [117] M. Jouini and L. B. A. Rabai, "Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study," *JCP*, vol. 10, no. 3, pp. 184-194, 2015.
- [118] A. Singh and D. M. Shrivastava, "Overview of attacks on cloud computing," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, 2012.
- [119] C. Taylor, *Probability of the Union of Three or More Sets*. accessed 5 March 2019, <https://www.thoughtco.com/probability-union-of-three-sets-more-3126263>
- [120] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1965.
- [121] Rapid7, *Exploit Database*, accessed 10 May 2019, <https://www.rapid7.com/db/modules/>
- [122] J. L. Kelley, *General topology*. Courier Dover Publications, 2017.
- [123] D. Wu, Q. Li, M. He, B. Boehm, Y. Yang, and S. Koolmanojwong, "Analysis of stakeholder/value dependency patterns and process implications: A controlled experiment," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1-10: IEEE.
- [124] N. Haile and J. Altmann, "Value creation in software service platforms," *Future Generation Computer Systems*, vol. 55, pp. 495-509, 2016/02/01/ 2016.
- [125] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing—The business perspective," *Decision support systems*, vol. 51, no. 1, pp. 176-189, 2011.

- [126] M. Böhm, G. Koleva, S. Leimeister, C. Riedl, and H. Krcmar, "Towards a generic value network for cloud computing," in *International Workshop on Grid Economics and Business Models*, 2010, pp. 129-140: Springer.
- [127] R. Ko and R. Choo, *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*. Syngress, 2015.
- [128] N. Sabharwal and P. Wali, "Cloud Stakeholders and Value Chain," in *Cloud Capacity Management*: Springer, 2013, pp. 9-14.
- [129] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833-851, 2012/06/01/ 2012.
- [130] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014.
- [131] SANS Institute 2016, "IT Security Spending Trends," accessed 10 May 2019, <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>.
- [132] IBM 2016, "The IBM X-Force 2016 Cyber Security Intelligence Index," accessed 12 August 2019, [https://www.foerderland.de/fileadmin/pdf/IBM\\_XForce\\_Report\\_2016.pdf](https://www.foerderland.de/fileadmin/pdf/IBM_XForce_Report_2016.pdf).