CHAPTER 1
INTRODUCTION

1.1 BACKGROUND

The concept of security that is familiar with most security professional is known as the CIA triad. It stands for Confidentiality, Integrity and Availability. The CIA triad model is designed to guide for creating the policy of security or for managing security in an organization. Confidentiality means information that can only be accessed by authorized parties. Integrity is the ability to protect information from being modified by unauthorized parties while availability is to ensure the authorized parties are able to access the information. This principle is applicable not only for database security but also includes the whole area of security analysis. Figure 1.1 shows the model of CIA triad.

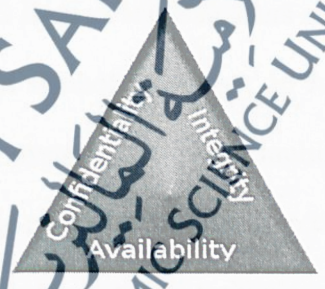

Figure 1.1: CIA triad

(Whatis.com, 17 August 2015)

Artificial Immune System (AIS) algorithm is part of the Computational Intelligence (CI) that applies CIA triad for security management. AIS algorithm is inspired from the theory of human immune system. The immune system protects the body from being attacked by

foreign microorganisms such as bacteria and virus, and also maintains our body health condition. It is anticipated that our immune system applied three keys of the CIA triad. As for the confidentiality, our body can only be accessed by authorized particles such as vitamins and nutrients. For the integrity, the immune system will protect organs and systems in our body from being modified by bacteria that can cause diseases and as for availability; it is to ensure only good things are able to access our body. Based on the complex system in the human body, researchers developed AIS algorithm for the computational area. This research intends to study classification of Short Message Service (SMS) spam messages using AIS algorithms.

SMS is one of the important communications between millions of people around the world. Majority of people use this service to communicate because of it is simple, easy access (i.e. easy to read), fast, reliable and lower in cost. Friedhelm Hillebrand stated that the maximum length of an SMS is up to 160 characters and these characters can comprise words, numbers, or punctuation symbols (Tatango, 16 June 2014). The advancement of mobile technology, operating system and many multifunction applications available attracts people to choose mobile phone and use SMS to communicate with each other. In addition, smart phones are becoming common technology during the past few years, as it integrates multiple wireless networking technologies to support additional functionality and services. Based on the statistics and researches, the usage of mobile phone is increasing every year and teenagers are the highest users of mobile phone for SMS. Research reported by e-Marketer clarified that more than 4.3 billion people in the world used mobile phone in 2013 and they predict this number will increase to 5 billion by

2017 (The Statistic Portal, 5 June 2015). Figure 1.2 shows that the Asian-Pacific region has the largest number of consumers using mobile phones in 2013.

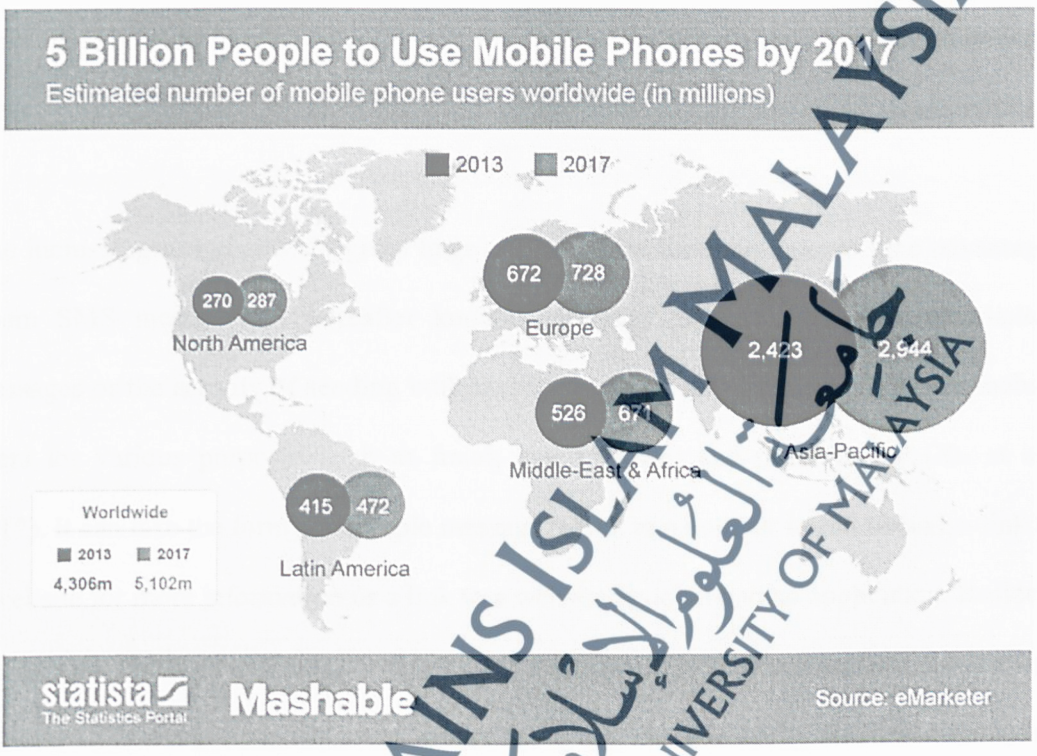

Figure 1.2: Statistic of consumers who use mobile phones around the world (The Statistics Portal, 5 June 2015)

Research by Experian in 2013 on the average number of texts (i.e. sending and receiving) per month by age among the U.S. people showed that teenagers aged 18-24 receive and send more text messages every month as compared to other age categories (Business Insider, 5 March 2014). Similarly in 2010, Yankee Groups conducted a survey among the U.S. consumers on the percentage of respondents who use SMS daily and found that teenagers were the highest group (Tatango, 4 March 2014). Without exception, in 2009,

Malaysia also had the highest usage of the mobile phone with 88.5% and teenagers aged 20-24 were the highest group compared to other age groups (SKMM, 22 April 2014). From these report, it can be suggested that spammers may aim to attack teenagers as their percentage of SMS usage are higher and they are easily attracted to the contents of spam messages as their feeling want to know something new.

The increasing usage of SMS gives huge opportunities for spammers to take advantage. Spam SMS messages or hereafter known as 'spam' text messages are unsolicited messages or the activity of sending bulk text messages to the known or unknown mobile users for various purposes such as fraud, entertainment and pornography (Xu et al., 2012). It can take the form of a simple message, a link to a number to call or text, a link to a website for more information or a link to a website to download an application. Besides, the type of messages that asks for sensitive information, the impersonation of companies, or asks for money in advance or seems too good to be truth (Canada's Anti-Spam Legislation, 2012) are also examples of the process of spam happens. Spamming is a serious problem for SMS today because it has caused loss of money among users and telecom companies because they may get summons from users (Xu et al., 2012).

Cook, a Chief Technology Officer of a security firm, Cloudmark warned that SMS spam is more dangerous than email spam because users look at every SMS they receive so that the SMS spam influences the users directly. In addition, the smaller screen on mobile devices makes it harder to detect malicious SMS (The M2 Computing, 8 March 2014). The increasing problems of 'spam' text messages give effect not only to the users

themselves but also indirectly give impact to the mobile companies and operators. There are many types of 'spam' text messages received by users such as prize, advertisement, financial and competition. The University of Minnesota reported that two-thirds of mobile phone users received short message service spam in 2012 and researchers uncovered 350000 variants of SMS spam in 2012 with 4.5 billion mobile spam messages performed (FierceMobileIT, 6 March 2014). Cloudmark also made a comparison about the types of text spam reported by the mobile users in 2012 and during the first six days of March 2013. Results showed that in 2012, '*receive a gift card*' is the most frequent type of text spam received by mobile users with 44% while in March 2013, only 7% of users received that type of messages (Tatango, 5 March 2014). Besides, Cloudmark made a review on the top five categories of SMS spam from the first quarter of 2013 by monitoring spam complaints from consumers and the known categories are '*receive a gift card scam*', '*payday loan spam*', '*job listing scam*', '*adult content spam*' and '*bank or account phishing*' (Cloudmark Security,26 June 2015).

These 'spam' text messages are widely spreading all over the world. On March 2014, Chinese authorities arrested 1,530 spammers who had been driving around, spewing spam at people's phones from mobile and fake base stations (NakedSecurity, 4 April 2014). According to a report from the China's state press agency, Xinhua, over the course of the first half of 2013, the Chinese were bombarded with more than 200 billion spam messages, with the average Chinese people being hit more than 150 (NakedSecurity, 4 April 2014). The increasing numbers of 'spam' text messages are quite alarming because

mobile phone is one of the important tools for communication nowadays, but there are irresponsible people who take advantage of this for their self-interest.

Nowadays, many mobile messaging applications are developed for communication besides SMS such as WhatsApp[1], WeChat [2]and LINE[3]. These applications are the most popular among smartphone users because of their reliable performance (BBC NEWS, 17 August 2015). Spammers may change their main target to these applications as the increasing usage among users. According to the research firm Informa, instant messaging on chat applications such as WhatsApp has overtaken the traditional SMS text message for the first time and almost 19 billion messages were sent per day on chat application in 2012 compared with 17.6 billion SMS texts (BBC NEWS, 17 August 2015). Although the usage of chat applications seems popular, there are many consumers who use normal mobile phones and depend on SMS as their messaging tool. As we know, chat applications are used by consumers who own smart phones but for SMS, it can be used by all types of mobile phone. Besides, spammers can easily attack SMS users because by sending malicious messages, they will get money from the users' prepaid compared to chat apps that use data plan for the Internet.

[1]https://web.whatsapp.com/
[2]http://www.wechat.com/en/
[3]http://line.me/en/

1.2 PROBLEM STATEMENTS

There are several issues related to SMS spam on mobile phones. The first problem is related to the effect of technology among mobile users. The number of mobile phone users is increasing due to variations of application available, As a result, it attracts a large number of spamming activities. The dramatic increased in the volume of mobile 'spam' text messages in each country such as United State, China and also Malaysia gives a high risk of spam to users. These spam messages could exploit users for fraud (i.e. gift and loan), porn, incitement, and rumours which resulted in hatred, trauma, false information, loss and misinterpretation. Besides, mobile phone users could suffer from financial loss which also affects mobile network operators due to experiencing higher network operating costs and customer care.

The second problem is the level of awareness among mobile users related to the effect and impact of spam messages that could give a high risk of spam problems to them. Usually, users do not know how to response when they receive suspicious messages or spam messages. They are curious and interested with the contents of the received messages and tended to open or click it. Sometimes, users are confused whether messages that they received are considered as spam or not because of lack of exposure about this. Besides, users are not aware of the types of messages they received. For example, users receive a video and they think that the video is an advertisement, but when they open it, it contains inappropriate content.

The third problem is the inefficient algorithm to solve the spam problem due to lack study on the algorithm itself. Many researchers have investigated and applied algorithms on email, but less on SMS. Email spam is different from mobile spam as the algorithms used for email cannot be applied directly to the mobile phone. This is due to the limited size of text messages which is only 160 characters and structure information such as subject, mail header, salutation and the sender's address. For example, algorithms for clustering data document cannot be used for mobile messages because of the different structure of data and need to be enhanced by putting some functions and characters to support the mobile messages. As this research is focusing on clustering spam messages into several groups, there are less published articles found related to spam text clustering and algorithms for clustering process. Most of the previous researchers investigated on how to detect SMS spam, but they were not further studied on the spam itself such as the type of spam messages and their behaviour. The purpose of doing clustering is to identify the types of spam that are always sent by spammers and it helps to determine the level of danger for each type of spam. Besides, it helps us identify the characteristics and pattern of spam messages for every group of spam. Other than that, AIS algorithm is used for clustering SMS spam and this algorithm is inspired from the theory of BIS. There is a lack of study related to understanding how BIS can be mapped with AIS and how they are related to each other. Having understood the aforementioned problem and challenges, this study tries to solve the current problem related to 'spam' text messages.

In this research, a new spam management model is proposed, which is inspired from BIS for SMS spam. This model comprises three main components; namely spam

detection/filtering, spam classification/clustering and spam severity determination level. Each component uses AIS algorithms and their ability for detecting, classifying and determining the severity level of spam messages can be explored. This research focuses on the second component which is spam classification (also known as clustering). A new proposed algorithm is then introduced for this phase. This algorithm could help to classify the types of spam messages based on the patterns or keywords of the messages besides used to determine the level of danger for each category of spam messages.

1.3 RESEARCH QUESTIONS

The questions in this research are:-

1- How can BIS and AIS be further studied and mapped within the scope of managing spam?

2- Is it possible to cluster spam messages using the theory of Immune Network and Clonal Selection? And if yes, how can Immune Network and Clonal Selection be enhanced for clustering messages?

3- How to evaluate the proposed algorithm?

1.4 RESEARCH OBJECTIVES

This research works on the following objectives:-

1- To further study the relationship between AIS and BIS related to spam detection, classification and severity determination.

2- To propose an enhanced method for clustering spam messages using the combination of Clonal Selection and Immune Network Theory.

3- To conduct and evaluate the proposed algorithms.

1.5 SCOPE

A spam management model known as the Integrated Mobile Spam Model (IMSM) is proposed to manage the 'spam' text messages. There are three main phases involved namely; detection, classification and severity determination, as shown in Figure 1.3.

Figure 1.3: Model for managing 'spam' text messages inspired by AIS algorithms

Each stage in this model uses different types of AIS algorithms. **This study focuses on the second part of the model that is classification or also known as clustering.** The detection and severity determination phases are covered by other researchers.

Datasets used for this research was downloaded from various sources and all datasets contain ham and spam messages. Besides, the limited number of spam text messages available led us to collect and gather the spam messages from different sources manually into FadhilahSpam dataset. This dataset contains only spam messages and will be used in classification phase for validation. There are four different datasets used:-

- Dublin Institute of Technology (DIT SMS Spam Dataset, 2012)
- British English SMS Corpora (British English SMS Corpora, 2011)
- UCI Machine Learning (Almeida et al., 2011)
- SMSv.0.1. (SMS Spam Corpus v.0.1., 2011).

Datasets are landed in several ways:-

- Doing the cleaning process to remove unimportant symbol or data in text messages.
- Reviewing the content of SMS messages to identify the difference between ham and spam messages for detection phase.
- Reviewing the content of spam messages to identify the types of spam messages according to the meaning, keywords and behaviour of messages for classification phase.

- Analyse the messages in each dataset according to True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) after the detection and clustering process.

This spam management model uses AIS algorithms in each phase and for this research, only two types of algorithms used; Clonal Selection and Immune Network.

1.6 METHODOLOGICAL FRAMEWORK

Figure 1.4 shows the phases in this research and the explanation for each phase is described in Table 1.1, while Table 1.2 presents the process and deliverables for getting the research objectives.

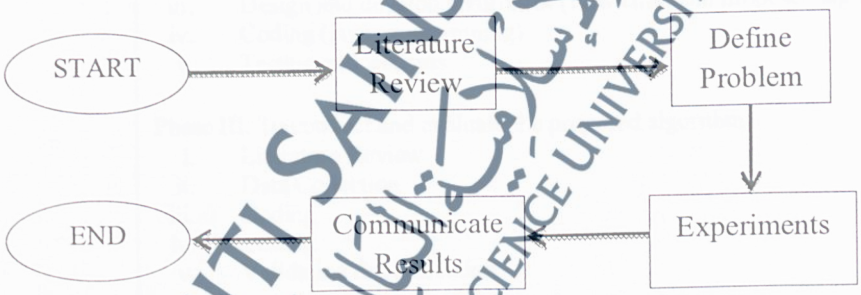

Figure 1.4: Research Phases

Table 1. 1: Research Activities in each phase

Phase	Activities
Literature Review	• Review Journals, books, websites and blogs. • Understand the concept of BIS and AIS. • Map information between AIS and BIS. • Understand Clonal Selection and Immune Network Theory in classification. • Collect dataset of spam messages. • Study and understand the use of WEKA for data mining. • Review several techniques for detection and classification (i.e. clustering). • Report in chapter two.
Define the problem	Identify the problems related to spam messages.
Experiment	CLASSIFICATION OF SPAM MESSAGES Phase I: To further study on the relationship between AIS and BIS related to spam detection, classification and severity determination. i. Literature Review ii. Data Collection iii. Testing Phase II: To propose an enhanced method for clustering spam messages using the combination of Clonal Selection and Immune Network Theory. i. Literature Review ii. Data Collection iii. Design and develop algorithms (flow chart and proposed algorithm) iv. Coding (java programming) v. Testing and analysis Phase III: To conduct and evaluate the proposed algorithms. i. Literature Review ii. Data Collection iii. Coding iv. Testing v. Validation & verification
Communicate results	• Writing thesis/Journal/Conference. • Publish paper. • Presentation (thesis/ conference).

Table 1. 2: Summary on the research activities

Research Questions	Research Objectives	Method	Activities and Deliverables
How can BIS and AIS be further studied and mapped?	To further study the relationship between AIS and BIS related to spam detection, classification and severity determination.	1. A literature review about the concept and theory of BIS and AIS by reading journal papers, articles, books and Internet.	1. Further understanding on the concept of BIS and AIS. 2. Able to identify the relationship between BIS and AIS, and to apply in three phases (detection, classification and severity determination). 3. Produce a paper for KMICE 2014 conference with the title **Integrated Mobile SPAM Model using Artificial Immune System Algorithms.**
Is it possible to cluster spam messages using the theory of Immune Network and Clonal Selection? And if yes, how can Immune Network and Clonal Selection be enhanced for clustering messages?	To propose an enhanced method for clustering spam messages using the combination of Clonal Selection and Immune Network Theory.	1. Do literatures review about detection and Classification (i.e. Clustering) techniques. 2. Explore the use and function of WEKA (an open source tool for machine learning) for detection and clustering. 3. Develop a program using Java to clean noisy character in messages. 4. Propose content and non-content features in detection SMS messages. 5. Develop a program to detect spam messages into ham and spam. 6. Propose an algorithm for clustering spam messages using AIS algorithm. 7. Develop a program to categorize spam messages according to right class or group.	1. Understand the existing techniques and algorithms used for detection and classification (or clustering). 2. Use WEKA to detect and cluster spam messages. 3. Clean all messages in each dataset to remove punctuation marks. 4. Produce five algorithms for detecting SMS messages using content and non-content features. 5. Detect SMS messages into ham and spam. 6. Produce a new algorithm for clustering spam messages named **Hybrid Immune Clonal Network Algorithm (HICNA).** 7. Cluster Spam messages into several groups of spam. 8. Produce a paper for the ICOCOE'2015 conference and the title is **A New SMS Spam Detection Method Using Both Content-Based and Non Content-Based Features**.
How to evaluate the proposed algorithm?	To conduct and evaluate the proposed algorithms.	1. Clustering spam messages using HICNA and WEKA and comparing their results.	1.Experiment 1: Results spam messages clustering using four different datasets (for testing). 2.Experiment 2: Results spam messages clustering using FadhilahSpam dataset (for validation). 3.Results of clustering using WEKA. 4.A paper entitled "**Spam Messages Clustering inspired by the Artificial immune System Theories**" (submitted to IF Journal).

1.7 THESIS STRUCTURE

The rest of this thesis is organised as follows. Chapter 2 highlights the literature review related to AIS algorithm and BIS, how they are mapped between each other and the existing research related to spam messages in detection and clustering process. Chapter 3 then introduces the spam management model named Integrated Mobile Spam Model (IMSM) while Chapter 4 presents several experiments conducted for both detection and classification phases. Chapter 5 provides the results for the experiments conducted together with the discussion. The thesis concludes with limitation, contribution and future work in Chapter 6.