CHAPTER 1: INTRODUCTION

1.1 Background

Cloud computing is a platform wherein you can locate your applications and access them via the Internet. It enables users to minimise the costs of purchasing and maintaining hardware and software while storing a large amount of data (Qaisar & Khawaja, 2012). Cloud applications are available online and can be used by multiple users regardless of the time and location of data retrieval and access (Hatem et al., 2014; Ren& Lou, 2009). Cloud computing is described as an environment that incorporates different factors, such as resources, servers, applications and hardware with a group of networks (Mell & Grance, 2011). This setup helps firms maximise the effectiveness in communicating and structuring their organisations while using the minimum amount of resources and ultimately reduce cost levels.

Worm attacks against cloud computing software and platform services have become increasingly alarming and caused many problems for users and providers (Watson *et al.*, 2015; Hatem *et al.*, 2014; Fan *et al.*, 2013). The cloud worm is a malicious code responsible for damaging the functionality of the cloud, including minimised cloud system activity, by attacking the virtual and hypervisor machine (Singh *et al.*, 2014). The cloud infrastructure is known to be connected through the network, and a cloud worm can spread and propagate within the network and harm the whole cloud infrastructure (Waston, 2012; Zhang *et al.*, 2010).

The implications caused by worm attacks in the cloud manifest in different ways, such as the corruption of data and user information, which cause difficulty of access and use (Zunnurhain & Vrbsky, 2010). The hypervisor is known to provide multiple guest virtual machines (VMs) within the cloud system (Bharadwaja *et al.*, 2011). Another implication of worm attacks on the cloud is hypervisor attack which also affects VMs (Bouayad *et al.*, 2012). Thus, the cloud worm controls all the cloud structure and gains access to and steals sensitive user information (Arya *et al.*, 2013).

Recent studies have been conducted on cloud worm attacks because the worms keep on changing, and this affects the detection rate of cloud worms (Shahin, 2014). Moreover, many models have been proposed to detect and respond to cloud worm attacks. Some of these models, such as the genetic algorithms (GAs) (Durairaj & Manimaran, 2015; Mizukoshi & Munetomo, 2015; Modi *et al.*, 2013; Patel *et al.*, 2013), were inspired by artificial immune organs and biological models. However, these models need to be further improved to increase the detection rate of cloud worms (Marnerides *et al.*, 2015; Patrascu & Patriciu, 2013). The present research is motivated by the need for the continuous monitoring and development of new models to fight cloud worm attacks. This research also aims to improve the worm detection rate in the cloud. Consequently, this study summarises the academic studies conducted about cloud worm detection and corresponding responses.

Knowledge discovery in databases (KDD) is known as a process for identifying potentially useful, valid and understandable patterns in large data (Giudici, 2010). KDD is implemented and used in this study as a process for identifying the cloud worm patterns within the dataset. The KDD process includes dataset preparation, data cleansing, features selection, classification, clustering and interpretation. KDD has been integrated in this study to optimise the worm detection accuracy rate in the cloud.

Genetic Algorithm (GA) is a search algorithm based on the principles of natural selection. It is being used to solve numers problems. In cloud environment, GA aids in optimising the classification of cloud worms. Unlike other algorithms, GA is used in this research to predict cloud worm attacks and increase the accuracy rate of detection, as well as determine the unknown future cloud worm characteristic for detecting future attacks.

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people and ensure that the right people can obtain such information. Access must be restricted to those authorised to view the data in question. Data are usually categorised according to the amount and type of damage that could be done should they fall into

unintended hands, and certain measures can be implemented according to these categories.

Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorised people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorised users. Some means must be in place to detect any changes in data that may occur as a result of non-human-caused events, such as an electromagnetic pulse (EMP) or a server crash. Some data may include checksums, even cryptographic checksums, for integrity verification. Backups or redundancies must be available to restore the affected data to its correct state.

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. Keeping current with all necessary system upgrades is also important. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important.

According to Swanson, (2001) consider the information processed by the system and the need for protective measures. The processed information is related to each of these three basic protection requirements: confidentiality, integrity and availability. Moreover, categorising the system or a group of systems by sensitivity level is helpful.

1.2 Problem Statement

Cloud worms are known to have a devastating effect or impact on homogeneous and flexible cloud installations which could cause huge data losses. They are malicious codes designed to compromise the confidentiality, integrity and availability of the cloud computing system (Yadav & Gupta, 2013). They destroy application,

functionality and systems in a cloud environment by attacking hypervisors and VMs (Singh *et al.*, 2014; Chou, 2013; Qaisar & Khawaja, 2012).

Moreover, the worm attempts to forge and own an administration authority and generate a malicious service in the cloud environment. The worm can dynamically regenerate its representation based on the changes in the environment (Zunnurhain & Vrbsky, 2010). According to cloud based worm classification, a worm attack is a major representative of exploiting cloud system services (Zheng *et al.*, 2011).

Given the rise and growth in technology, the recent cloud worms are becoming increasingly advanced and complicated and this phenomenon makes detection and containment extremely challenging (Biedermann & Katzenbeisser, 2012).

Watson *et al.*, (2015) conducted numerous studies on worm detection related to the cloud computing environment. The researchers used a technique based on a support vector machine to detect worms within the cloud computing infrastructure. Hatem *et al.*, (2014) suggested a new cloud worm detection technique using dynamic and static detections. The technique identifies malicious software in clouds. Each of the previous studies offer its own strength and weakness in which accuracy detection rate can be further improved to increase the worm detection level (Nancy *et al.*, 2016).

Marnerides *et al.*, (2015) presented a new detection technique to detect worm for the virtualised cloud environment. This technique used system and network analysis engines to analyse and monitor worm activities in VMs. However, this technique showed a low accuracy detection rate. A good accuracy rate is required to increase worm detection within the cloud environment (Banu *et al.*, 2017).

Accuracy detection tends to suffer from having incomplete optimisation; in turn, this phenomenon makes detection inaccurate. Another weakness for the accuracy and classification for worm detection is not having a continuous learning ability in their testing phase which leads to the high worm invasion of the system (Fouladvand *et al.*, 2016).

Therefore, based on the implications of the cloud worm attacks, developing a new cloud worm technique that detects and responds worm attacks in the cloud computing

environment is needed. Enabling cloud worm detection approach is crucial to protect the functionality of the cloud environment against any worm attack. Thus, finding a way to detect and respond to the cloud worms within the cloud computing system is important.

1.3 Research Questions

To challenge the previously mentioned problems, this research attempts to answer the following research questions:

1) How is a new cloud worm classification going to be proposed based on worm cloud features?
2) How is the enhanced cloud worm detection technique inspired by genetic algorithm going to be developed?
3) How is the response mechanism for worm cloud going to be proposed?
4) How is the performance of the proposed technique being measured?

1.4 Research Objectives

The main objectives for this research are as follows:

1) To propose new classification for the worm cloud based on cloud worm features.
2) To develop a cloud worm detection technique by integrating the enhanced genetic algorithm.
3) To propose a cloud worm response technique based on threat level.
4) To evaluate the proposed cloud worm detection technique.

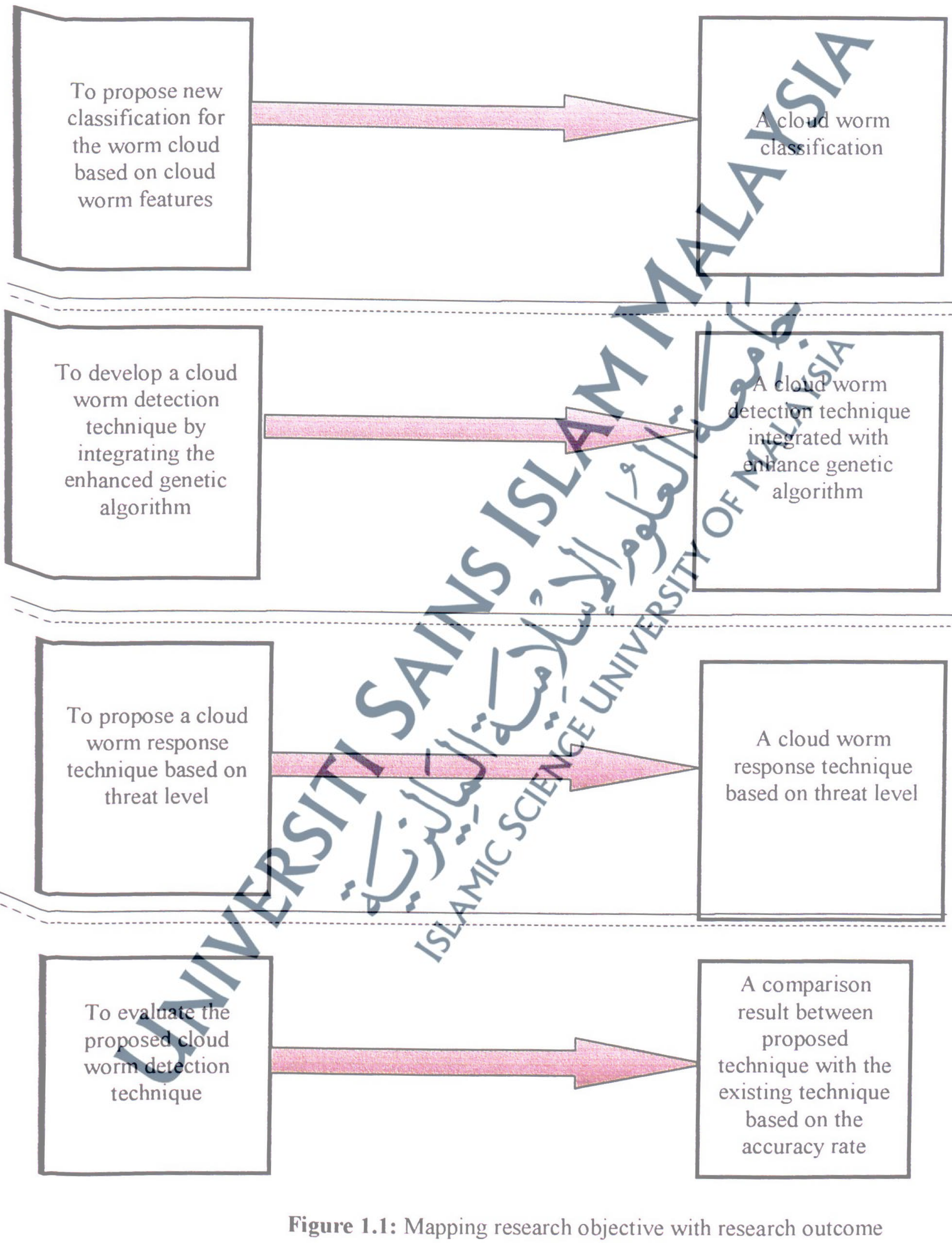

Figure 1.1: Mapping research objective with research outcome

1.5 Scope of the study

The scope of this research is to do a study on detection and response on the worm attacks for Windows operating system platforms based on a cloud computing environment (public, private and hybrid).The cloud is chosen because it has many users, which then makes the cloud highly prone to different attacks. For the past few years, an increasing number of worm attack vulnerabilities and exploitations have targeted this platform in the cloud environment. As compared with other related work for worm classification, these works have introduced different worm features that are limited to PC environment. As for this research, it is to implement a new classification for cloud worm which is to make it different from the prevouis exisiting works in which it is to be related to the infection part as a contribution for the new cloud worm classification. The research focuses on developing a new cloud worm classification. Cloud worm classification can be utilised as a basis for worm detection and response method which is to help increase the accuracy detection rate.

Additionally, a new technique to optimise the accuracy detection rate is also introduced by integrating the enhanced genetic algorithm. The enhanced genetic algorithm is used to enhance cloud worm detection and classification by using different method of selection, Crossover and mutation. Due to the fact of sustainable nature generation production, best parents are selected before the creation of new generation.

A response mechanism for cloud worm is also presented based on threat level. The threat level is being measured based on the impact on confidentiality, integrity and availability. Threat level is measured based on the assigned rules for weight and severity level. Additionally, threat score system is introduced based on threat weight and severity levels.

1.6 Research Contributions

The contributions for this research are as follows:

1) Development of cloud worm classification.

2) Development of a cloud worm detection technique by integrating the enhanced genetic algorithm.

3) Development of a cloud worm response technique based on threat levels representing the impacts on confidentiality, integrity and availability measured by the security metrics.

4) A better accuracy rate for the cloud worm detection technique compared with existing work.

This newly proposed technique helps ensure the high detection rate for cloud worms and the protection of valuable data and information in the cloud computing environment, and subsequently reduce the risk of worm attacks and improve the protection of cloud computing.

1.7 Structure of the thesis

The thesis is structured as follows:

Chapter 2: The literature review discusses related topics on the fundamental knowledge of the subject matter, such as the cloud computing architecture, worm attacks in cloud environment, worm detection and response techniques and GA.

Chapter 3: The methodology chapter discusses in detail the research methods used to achieve all the research objectives. This includes the lab architecture and the whole analysis and statistical data mining evaluation methods.

Chapter 4: This chapter presents a new cloud worm classification in detail. It consists of the worm cloud classification and experimental results which include the frequency analysis and statistical analysis.

Chapter 5: This chapter explains the cloud worm detection (EGA) technique using GA in detail. It consists of experimental results, different testing techniques and a comparison with existing data mining algorithms, conducted to prove the effectiveness of the EGA cloud worm model.

Chapter 6: This chapter discusses the cloud worm response (EGA) technique detail. It consists of the weight and severity based on confidentiality, integrity and availability (CIA).

Chapter 7: This chapter summarises the key findings and provide suggestions for future research.

1.8 Summary

This chapter provides a brief introduction to cloud computing and worms, the key area of study. The problem statement and objectives were discussed to highlight the main reason of this research. The significance and the scope of the study were also highlighted. Based on this thesis objectives and contributions, a new technique to detect and respond to the worm attacks in the cloud environment using genetic algorithm is to be developed.