CHAPTER III

RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on presenting a systematic research methodology through the introduction of relevant research definitions, concepts, best practices and techniques, leading to a proposed integrated technique in eliciting security requirements and quantifying security requirements.

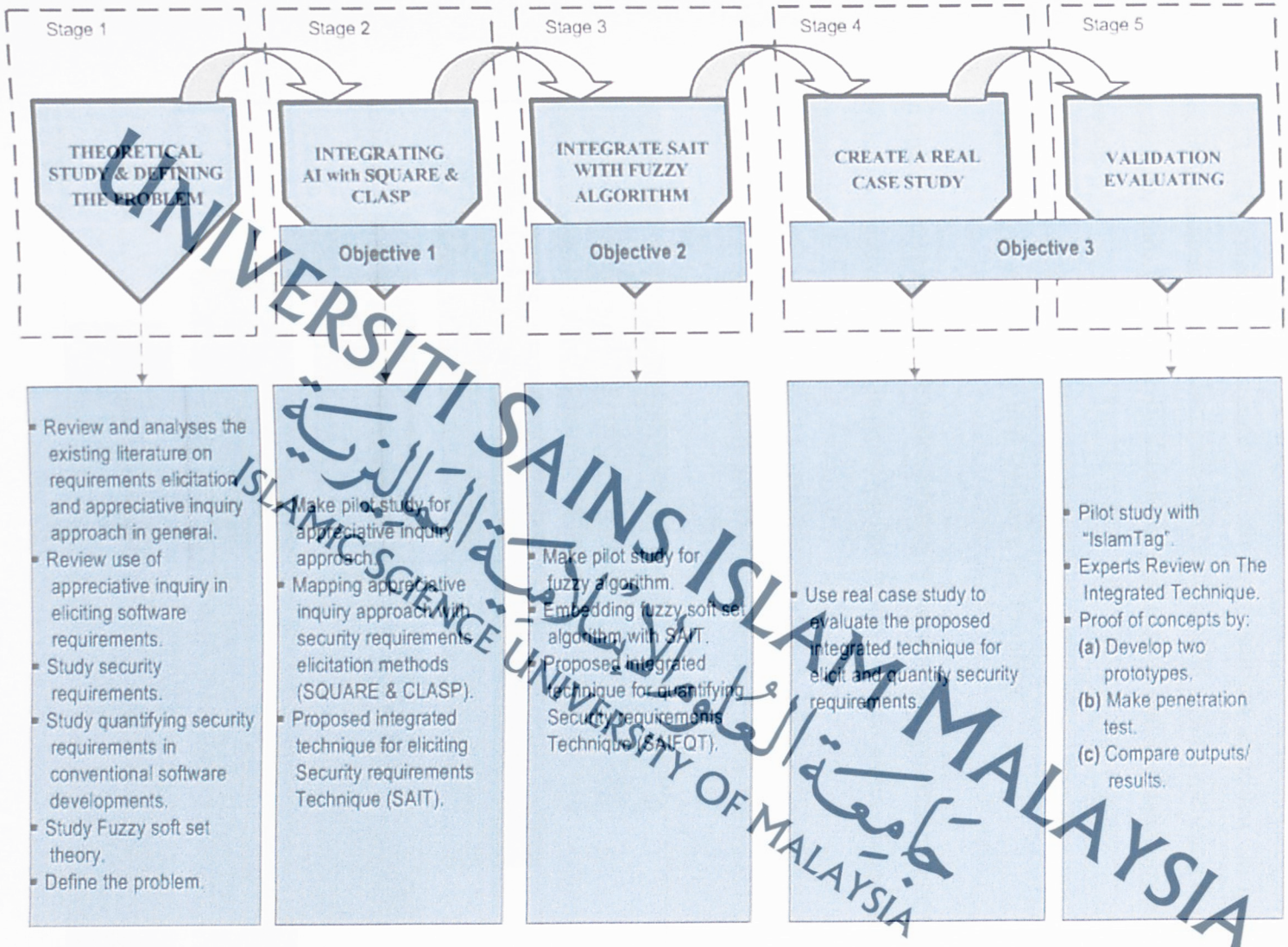
In order to decide an appropriate methodology for this study, a conceptual framework in this study has been proposed. As discussed in Chapter II, in theorizing the concepts of 'security requirements' 'requirement elicitation techniques' 'elicit and quantifying security requirements', are abstract, invisible, and technically complex. It should be recognized that those concepts are deeply embedded in practitioner's mind, thought or routines within an organization or between organizations.

With the above argument, this study adopts the mix method (i.e. qualitative and explorative approach), which recognizes that reality is not separated from social actors, but it is deeply internal to them, and it has subjective attributes.

The value and procedure of the knowledge management process cannot be easily accessed and observed with the quantitative or neutral methods. Instead, the mix method may allow the current research to focus more on the subjective aspects of the technique's perceptions on the knowledge extracting strategy for the logistics value. Furthermore, as the goal of this study is to understand and apply the aforementioned

technically complex strategy, it must try to deduce individual comprehension on the strategic issues, and to draw significant strategic implications from people's subjective understandings and opinions (Kamenou, 2002).

Such a method may also help to overcome the dangers of using mathematical evidence to arrive at a hasty conclusion on the technical complex world, which represents a common weakness of quantitative research (Kelle, 2006). This study follows the mix method as shown in Figure 6

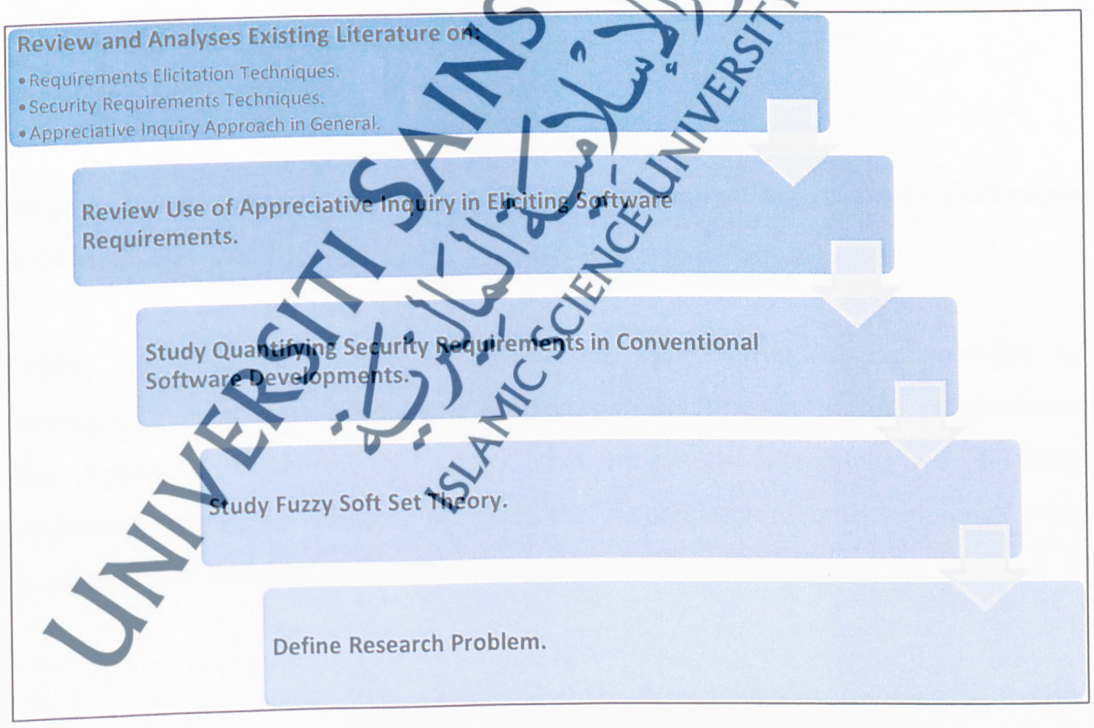


This study employs the mix method. This method consists of several stages (Sekaran, 2009) which begins with a defining the security requirement current problem, mapping between appreciative inquiry with security requirements methods (SQUARE & CLASP) stage later integrate with the fuzzy soft set algorithm to quantify the security requirements, conduct case study and to build a prototype using the proposed technique, and, finally, the validation through experts and evaluation by penetration testing.

Stage 1: Theoretical Study and Defining the Problem.

In order to have an in-depth understanding of the security requirements elicitation, the primary objectives of the literature review in this research as mentioned in figure 7 attempt to:

FIGURE 7: Theoretical Study and Defining the Security Requirement Elicitation Problem.



1) Review and analyze the requirements elicitation and Appreciative Inquiry method; identify the advantages and weaknesses of these approaches and understand their functionalities, understand the use of Appreciative Inquiry

methods in eliciting software requirements, and identify the features that have to be included to the requirements after using this method to elicit software requirements.

2) Understand the security requirements; find out the significance of security, discover the association between normal requirements (Functional/Business Requirements), study the impact of security requirements over the quality of the whole system.

3) Understand the role of quantification of security requirements; discover the techniques in terms of quantifying security requirements.

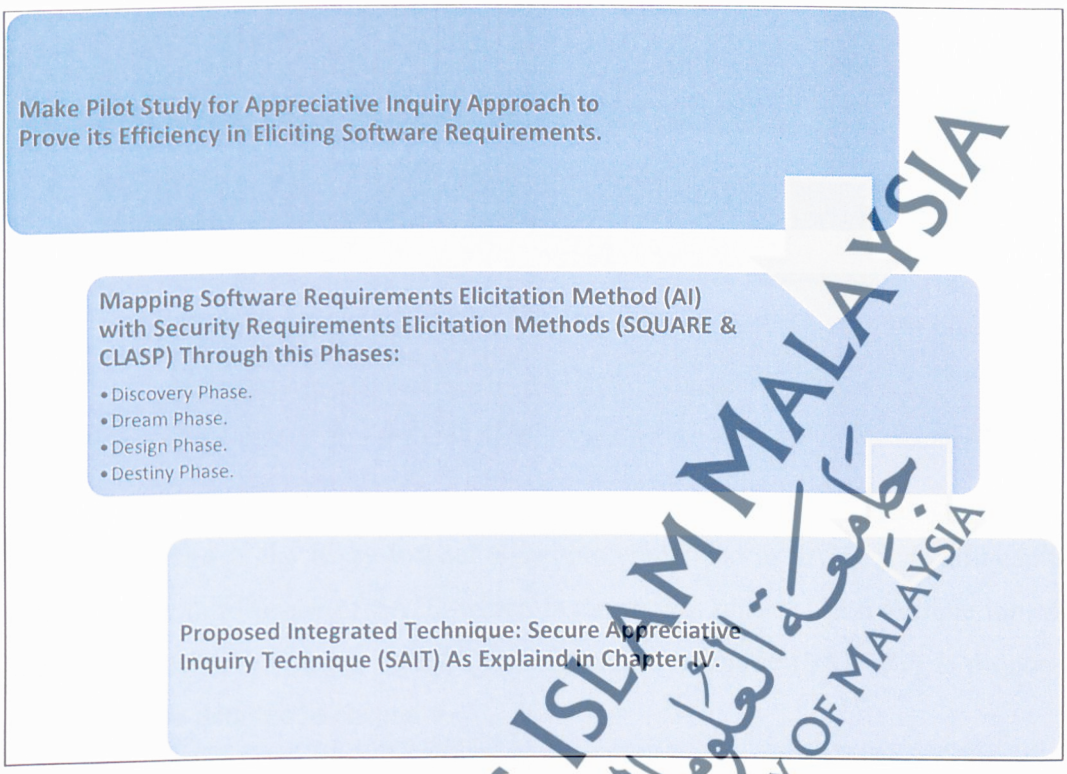
4) Introduce the characteristics of the fuzzy soft set theory; explore the application of the fuzzy theory in decision-making for quantifying security requirements

5) Define the current problem in specifying security requirement.

Stage 2: Integrate Appreciative Inquiry with Security Requirements Technique (SQUARE & CLASP).

Firstly, a pilot study was conducted on the appreciative inquiry approach to investigate and prove its ability and efficiency in eliciting the normal requirements (See Appendix A). Next, the Appreciative Inquiry is integrated with Security requirement technique through mapping the Appreciative Inquiry approach with Requirements Elicitation in four phases as shown in figure 8:

FIGURE 8: Integrating AI with SQUARE and CLASP.

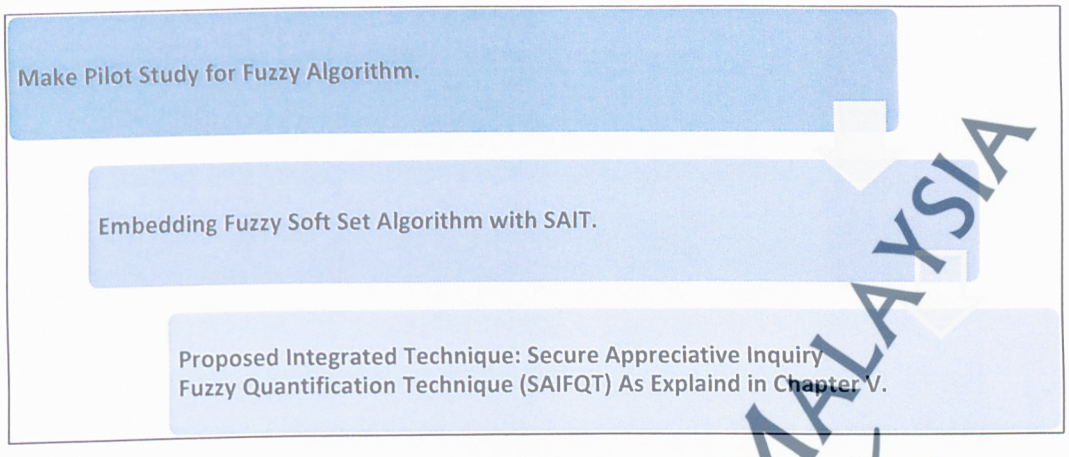


In order to develop such an integrated security requirement elicitation technique, there are some important steps which have to be accomplished at stages 2 and 3, which discussed in details in chapters IV and V. As the integration is complete, the Secure Appreciative Inquiry Technique (SAIT) is proposed, as discussed by the Chapter 4.

Stage 3: Integrate Secure Appreciative Inquiry Technique with Fuzzy Soft Set Algorithm to Quantify the Security Requirement.

Before embedding the fuzzy algorithm with SAIT the adapted fuzzy algorithm must be ensured to have a strong contribution in terms of quantifying security requirements in an accurate manner. A pilot study was carried out to quantify security requirements in an available system (See Appendix B). Figure 9 shows this stage in few steps.

FIGURE 9: Integrate SAIT with Fuzzy Algorithm.

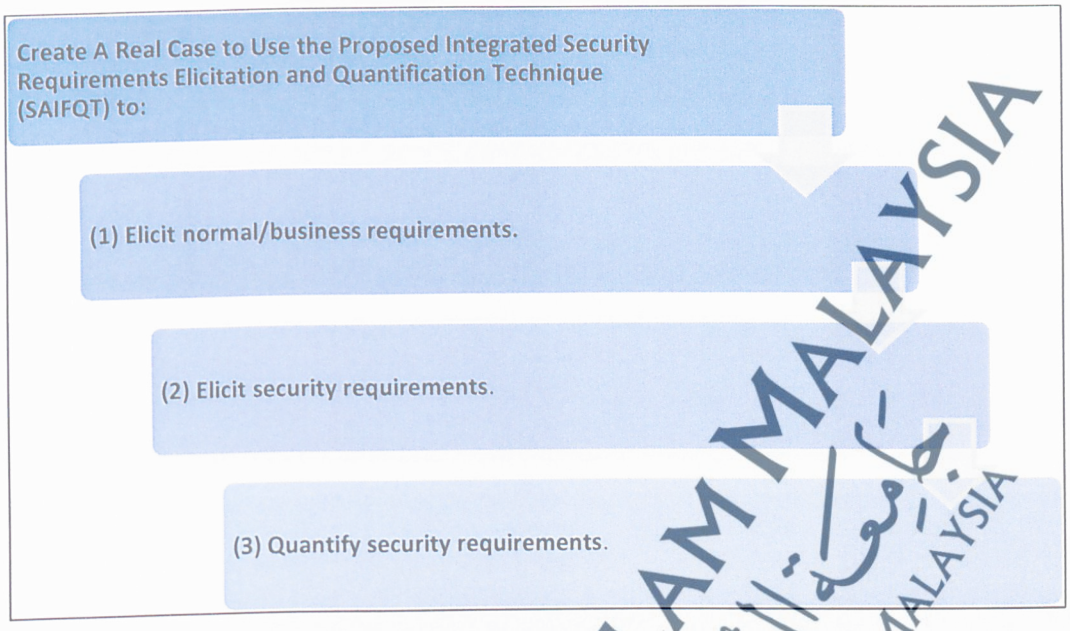


The diagram shows the fuzzy soft set algorithm embedded in SAIT. This embedding will be in the third phase of SAIT, which is the design phase. Upon completion, the Secure Appreciative Inquiry Fuzzy Quantification Technique (SAIFQT) is proposed as presented in detailed in chapter 5.

Stage 4: Validating The Technique Using Real Test Case.

A real test case is to be conducted to use the proposed Secure Appreciative Inquiry Fuzzy Quantification Technique (SAIFQT), where the proposed technique steps are applied to: (1) elicit normal/business requirements, (2) elicit security requirements, and (3) quantify security requirements. New and unique security requirements are discovered in order to build a more secure system in the future (See Chapter VI). The re test case helps to identify the weak and strong points of the proposed technique, which will facilitate the proposal of having a minimum error technique. On the other hand, the outputs will be used to build the prototype in the next stage. The prototype will be built according to the elicited and quantified security requirements by SAIFQT for the purpose of evaluation. Figure 10 shows this stage in few steps.

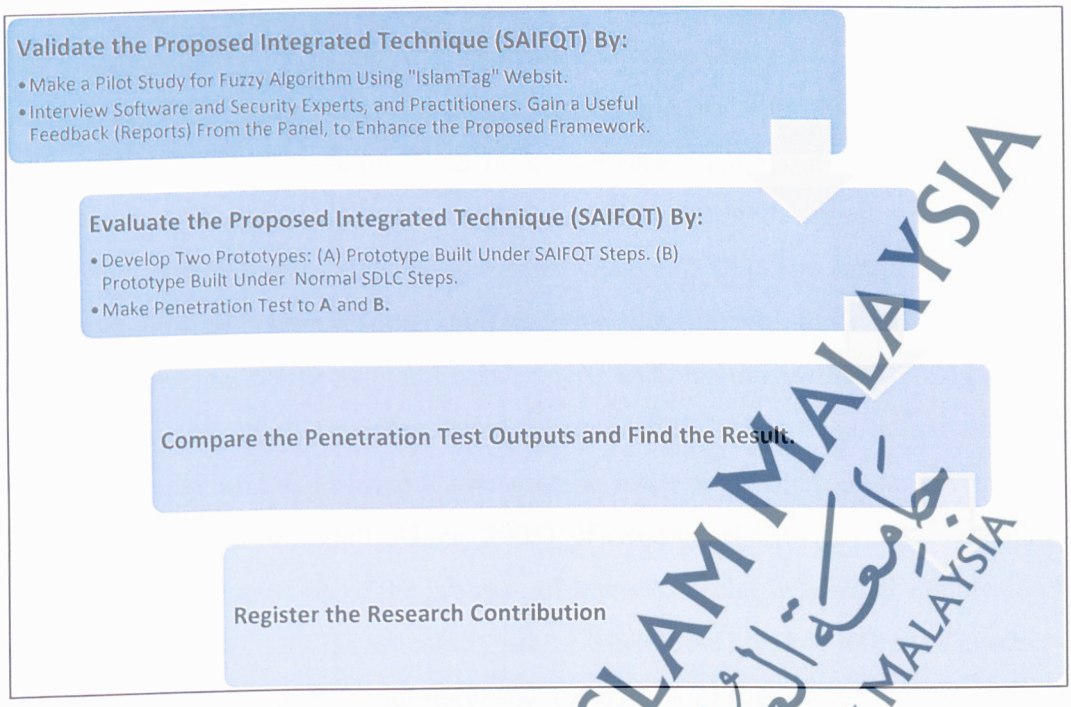
FIGURE 10: Conduct a Real Test Case and Build Prototypes.



Stage 5: Validation and Evaluation.

The final stage (stage 5) focuses on validating and evaluating the functional reliability and validity of the proposed integrated technique, SAIFQT (elicit and quantify security requirements), and figure 11 illustrates this stage in steps.

FIGURE 11: Validation and Evaluation.



3.2 Validation of Proposed Integrated Technique (SAIFQT)

Pilot Study "IslamTag at www.islamtag.com"

IslamTag social network, this network was created in 2010, it was invented from a PhD student of Faculty science and technology, USIM. His invention of islamtag was quite similar to facebook.

The pilot study was done in stage 3 before the fuzzy algorithm is embedded in SAIT to ensure that the adapted fuzzy algorithm has a strong contribution in terms of quantifying security requirements accurately. The pilot study conducted serves to quantify the security requirements in an available system which is the "IslamTag" website. This pilot study will be used to validate the fuzzy algorithm in chapter VII. To investigate the pilot study in details, kindly refer to Appendix B.

3.2.1. Experts Review on Proposed Integrated Technique (SAIFQT)

The expert panel is one of the most fundamental components of a Delphi study. The strength of Delphi is the belief that 'n +1' participants are better than one (Crisp et.al., 1997; Verran, 1981). Traditionally there is little agreement about the sample size and no criteria exist against which the sample size can be judged; therefore, studies have been conducted with virtually any size panel (Akins, 2005). The sample size in most Delphi studies has been researcher- and situation-specific, with the use of convenience samples dependent on the availability of experts and resources (Akins, 2005). Using a convenience sample allows researchers to purposefully select experts that can apply their knowledge and experience to the specific issue or problem under investigation (Snyder-Halpern et al., 2000; Akins, 2005). If experts selected have similar training and general understanding of the problem of interest, a relatively small sample can be used (Akins, 2005). This is particularly useful when there are only a limited number of experts in a field of interest. Linestone and Turoff (2002) suggest the following mix of experts:

- Stakeholders or those who are or will be directly affected.
- Those with an applicable specialty or relevant experience.
- Those possessing skills in organizing, synthesizing and stimulating.
- Interdisciplinary members.

This research has selected 7 experts who have some in-depth and adequate knowledge and experiences in software engineering and security. Five of them has a degree in Doctorate of Philosophy in Computer Security in different universities in Malaysia, Jordan and UK whereas the other two experts are practitioner with a computer security background. A report was sent to the seven experts, which contains details about the proposed technique such as the purpose of the technique, objectives, and the problems that the study aims to solve.

Scheele argued that (2002), the reasons behind using the Delphi method for selecting the experts is to make the study benefit from subjective judgments which based on collective wisdom. The individuals needed to contribute to the examination of a complex problem representing diverse backgrounds, and where participants dispersed

over a wide geographical area. So that, face-to-face meetings had been done with the experts in Malaysia (Three Experts) and the remaining experts were interviewed via Skype and E-mail.

Besides, an interview appointment was determined to discuss the technique with the experts and to clarify ambiguous information in the report; these interviews were conducted face-to-face and by Skype meetings. Later, at different times, the seven experts had sent reports that contain the validation, and feedbacks about the technique regarding areas such as the features, weak points, and a number of notes to update the proposed technique of SAIFQT (See Appendix D).

3.3 Evaluation of Proposed Integrated Technique (SAIFQT)

3.3.1. Develop Two Prototypes

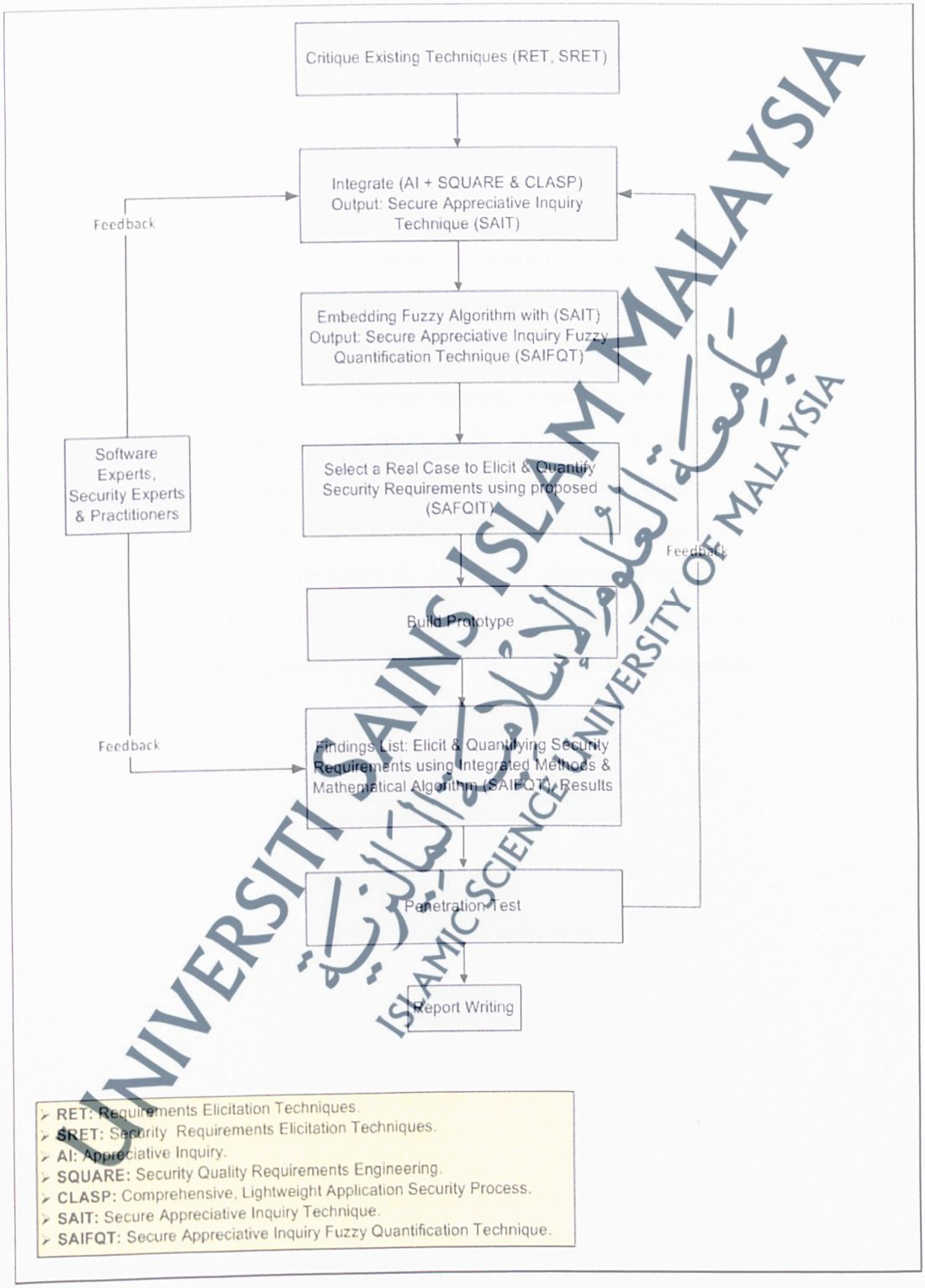
By using the output of stage 4, normal requirements, security requirements, and the quantification of security requirement results will build the first prototype. The prototype will be built according to elicited and quantified security requirements by SAIFQT for the purposes of evaluation, see chapter VI and VII. On the other hand the normal SDLC will be used to build the same prototype. This prototype will be used for the evaluation purpose.

3.3.2. Penetration Test

A penetration test was imposed on the two prototypes using the OWASP ZAP tool version 2.2.2. See chapter VII.

Evaluating the Results: the results of the proposed technique (penetration test report) will be compared with the outcomes of another techniques' results (building another prototype with the same business requirements and programming language, but use the normal SDLC, then using the same penetration testing tool), in order to evaluate the efficiency of the proposed technique and to register the contributions of this study; by comparing the penetration test results for both prototypes. (See Appendix E).

FIGURE 12: Research Process.



The research process gives a road map for this research, it presents the concerned research steps. It also conducts the necessary methods and it offers a number of choices to get the desired results. By referring closely to figure 12 an initial overview to the whole research can be taken to understand the nature of research's aims.

3.4 Summary

This chapter discusses the related literature and methods employed by this study. Research design and research methodology, methodological choices or discussion and the process of the research have been introduced. A mix method has been chosen to investigate and develop a conceptual framework, which aims to identify the used techniques in eliciting and quantifying security requirements, and then develop the technique to elicit and quantify security requirements in the requirements phase. To conduct the mix method analysis, an explorative case study method has been considered, and the quality of the method is diagnosed by means of assessing the validity and reliability of the method. An initial explorative case study targeting at eliciting and quantifying security requirements in the software industry will be conducted as the effort to understand all the issues involving the research topic.