CHAPTER 3

RESEARCH METHODOLOGY

3.1 Overview

Every researcher requires a goal to conduct research. This can be helped by organizing a good research methodology. For the research process to be dependable, valid, and repeatable by other researchers, a clearly defined research technique is essential. It offers a guide for how the study will be conducted and aids in maintaining uniformity and rigor. Researchers can relate the objectives of the research, the processes necessary to achieve the objectives, and the output that can be anticipated from the processes with the help of appropriate planning and root cause analysis of the research scope. The outline of the research approach is highlighted in this chapter. The objectives and anticipated results of this research are presented in depth along with the research methods. Additionally, the research's materials and tools are mentioned. Furthermore, the chapter includes an in-depth discussion of the data collection techniques. This research encompasses three phases which are Analysis, Development, and Evaluation.

3.2 Research Methodology Overview

The research methodology encompasses several interconnected activities and phases that are used to fulfill the study objectives rather than merely collecting data (Silva *et al.,* 2020). The order of data-gathering techniques, procedures, and contents must thus be justified in the context of the growth of the research (Chu & Ke, 2017). Similar to this, the methods used to gather the data should be supported by the specific study goals associated with each approach (Mellenbergh *et al.,* 2003).

The research methodology, according to Mellenbergh *et al.* (2003), is the entire strategy of research development in accordance with a set of research objectives. Therefore, this plan's phases and methods should be obvious so that researchers may ensure the validity of their findings by quickly identifying any flaws in the development process. In contrast, a defined strategy for research development makes it easier for readers to comprehend the order of the research.

The main scope of this research is smartphone mobile user, thus the case study for this proposed model should be focused on academicians and industry experts in authentication for mobile user. These experts can give their insights on authentication and its significance in smartphones. The proposed User-Device Authentication Model that implements Digital Certificate can only be validated by experts who have in-depth knowledge regarding authentication.

Consequently, the research data will be collected from academicians that experts in authentication as well as relevant industry individuals who are authentication experts. This authentication model will not be validated by academicians and industry experts who are not experts in authentication for smartphone applications. This is to ensure that the data collected is more reliable to validate the proposed model and its significance for future implementations in smartphone.

3.3 Research Process

To make sure the objectives are reached and the results are what were anticipated, adequate methodology must be used when designing the research. The actions involved in carrying out this research are broken down into three phases: Phase 1 which is the analysis phase, Phase 2 which is the development phase, and Phase 3

which is the evaluation phase. The flow diagram of the process used in this research is shown in Figure 3.1.

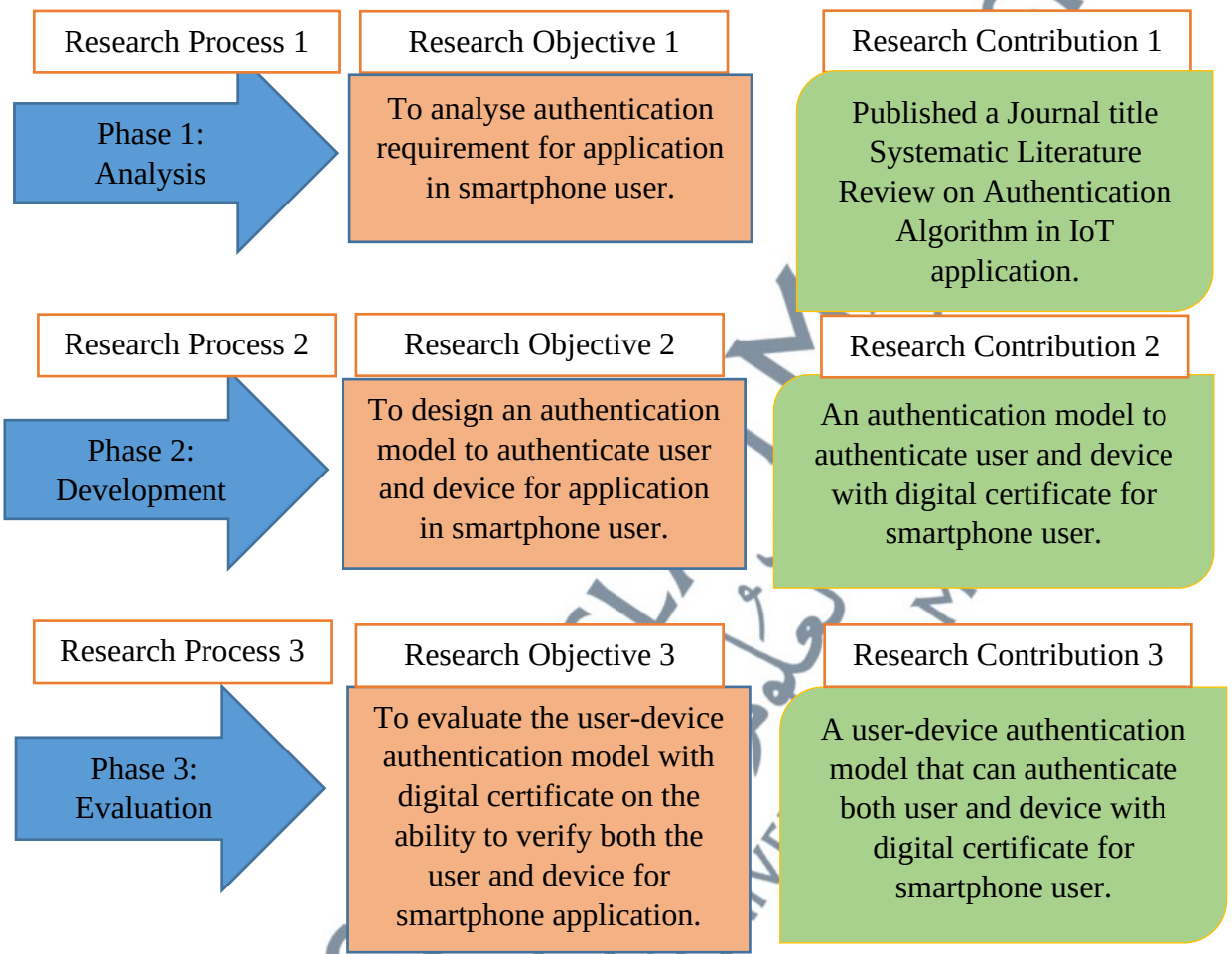

Figure 3. 1: Flow of Research Process

Table 3.1 maps the research question, research purpose, research procedure, and research contribution or a clearer understanding of the methodology used in this study. To make meaningful research contributions toward resolving the specified research problem, it is crucial to guarantee that every research question is addressed along with the specific research objective through a structured research procedure.

3.3.1 Phase 1: Analysis

Phase 1 is the first step in conducting research, as shown in Figure 3.2. It is a very important step leading to the direction of research. Research Objective 1 is to analyze authentication requirements for applications in smartphone user. To fulfill this objective requires two processes known as Research Methods. The first method is to define research areas, research problems, objectives and scope in proposing an authentication model for smartphone user. The second method is to conduct review literature on authentication requirements for smartphone user. These have been explained in Chapter 2 where the literature review has been done in order to explain all the components and research done related to authentication using digital certificate for smartphone user which producing Research Contribution 1 which is Systematic Literature Review on Authentication Algorithm in IoT application.

Table 3. 1: Research Methodology Mapping

Phase	Research Question	Research Objective	Research Method	Research Contribution
Phase 1: Analysis	1. What is the current research trend in authentication method algorithm for smartphone user?	1. To analyze authentication requirements for applications in smartphone user.	1. Define research areas, research problems, objectives and scope.	1. Systematic Literature Review on Authentication Algorithm in IoT application.
	2. What is the trend of attacks that jeopardize the authentication for smartphone applications?		2. Review Literature on authentication requirements for smartphone user.	
Phase 2: Development	3. What are the security requirements and mechanisms needed to solve the authentication attacks in smartphone applications for user?	2. To design an authentication model to authenticate user and device for application in smartphone user.	3. Identify the requirements and scope of the authentication model for smartphone user.	2. An authentication model to authenticate user and device with digital certificate for smartphone user.
	4. Which cryptography algorithm is suitable to use to achieve authentication requirements in smartphone applications?		4. Proposed an authentication model based on user and device authentication implementing digital certificate for smartphone user.	

Phase 3: Evaluation	5. How does the digital certificate used in the proposed model verify both the user and the device in smartphone user?	3. To evaluate the user-device authentication model with digital certificate on the ability to verify both the user and device for smartphone application.	5. Questionnaires answered by expert reviews to validate the user-device authentication model.	3. A user-device authentication model that can authenticate both user and device with digital certificate for smartphone user.
	6. Does the proposed authentication model applicable for authenticate user and device for smartphone user?		6. Calculate the outcome data using the mathematical formula used in the model.	

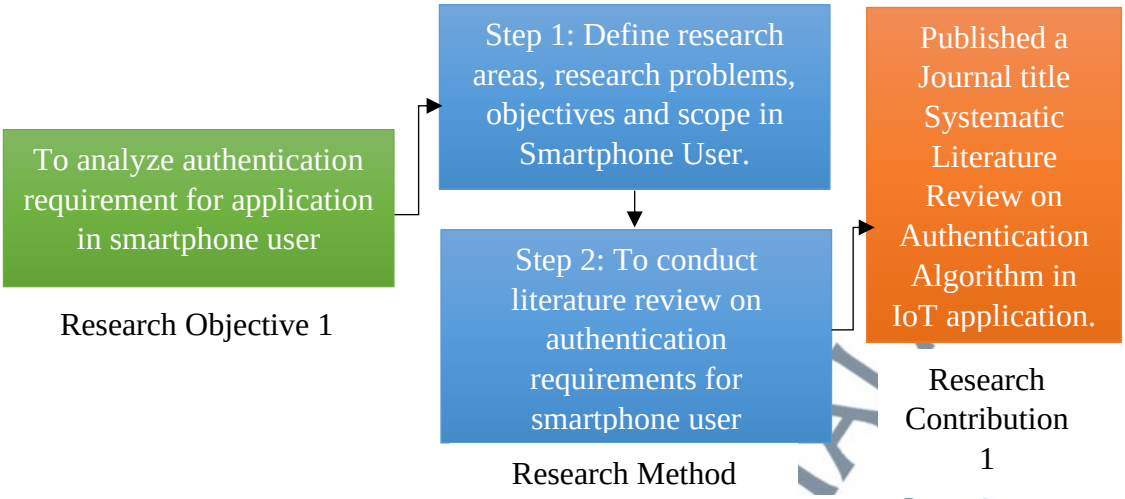

Figure 3. 2: Analysis Process

3.3.2 Phase 2: Development

Phase 2 is essential since the steps listed in phase 2 are required to fulfill Research Objective 2 which is to design an authentication model to authenticate user and device for application in smartphone user as shown in Figure 3.3. In this phase, a User-Device Authentication Model is designed and proposed by implementing Digital Certificate for smartphone user. The digital certificate is used as the component to authenticate both the user and the device. There are a few methods in fulfilling phase two which are the first identifying the requirements and scope of the authentication model for smartphone user. The second is to propose an authentication model based on user and device authentication implementing digital certificate for smartphone user. The authentication Model will be explained in detail in Chapter 4. These methods formed Research Contribution 2 which is the design of an authentication model to authenticate user and device with digital certificate for smartphone user.

The algorithm used in the proposed authentication model is the RSA algorithm as well as Digital Signature. The formula used to authenticate both the user and the

device implementing the RSA algorithm will be explained more in Chapter 4. The algorithm used in the proposed model is one of the famous algorithms and is suitable for use in Digital Signature. This will ensure that the algorithm used can authenticate both the user and the device.

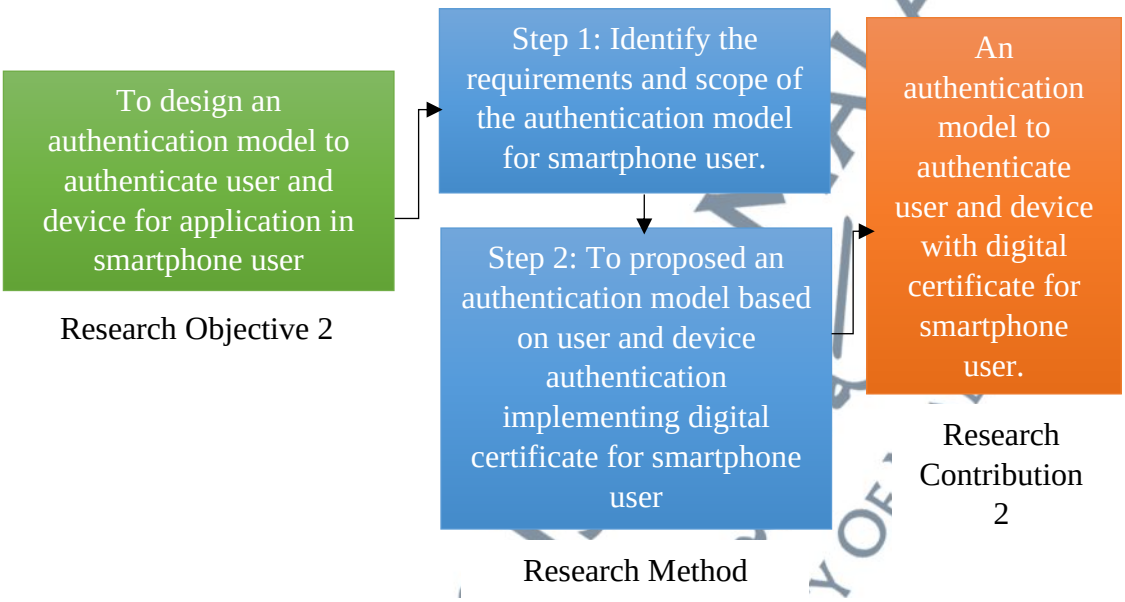

Figure 3. 3: Development Process

3.3.3 Phase 3: Evaluation

This phase explains the steps taken to evaluate the proposed authentication model implementing digital certificate for smartphone user as shown in Figure 3.4. Research objective 3 is to evaluate the user-device authentication model with digital certificate on the ability to verify both the user and device for smartphone application. There are two methods to evaluate the authentication model proposed and whether the proposed model is likely to be developed for future utilization in smartphones. The first method is to develop questionnaires to be answered by expert reviews to validate the user-device authentication model. The expert reviewers consist of academicians and industrial experts. The second method is to calculate the outcome data using the

mathematical formula used in the model. A simulated data is used to calculate the expected outcome of the authentication model using digital certificate formula used in this authentication model. These methods will be further discussed in Chapter 5. These methods produced the Research Contribution 3 which is a user-device authentication model that can authenticate both user and device with digital certificate for smartphone user.

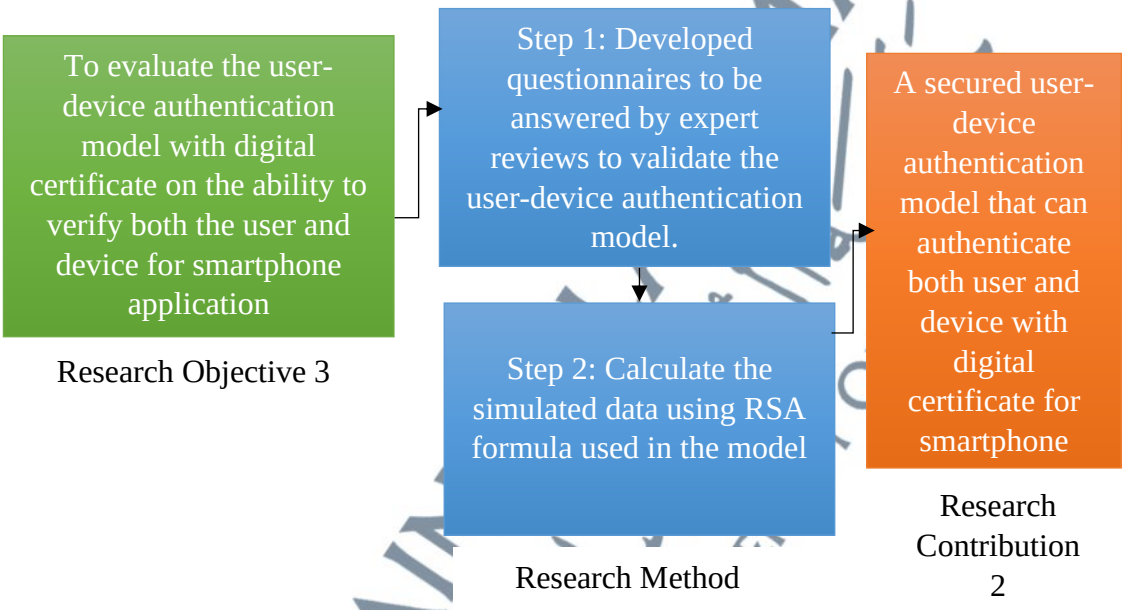

Figure 3. 4: Evaluation Process

3.4 Research Design and Tools

This section details each phase's activities in extensive detail. The research model suggests the recommended model for this research while the research design explains the selected sort of methodology used. The entire procedure for this study, including the proving method of the authentication model, will be decided by the following subsections 3.4.1 and 3.4.2.

3.4.1 Research Design

This subsection concentrates on deciding the design that will be used to propose the authentication model that can authenticate both the user and devices for smartphone user. As this research is to determine whether the proposed model can be adapted to smartphones, the type of data collection that is selected to be used in this research is a mixed mode between qualitative where the data is received from experts, and quantitative where simulated data is calculated using RSA Formula implemented in the proposed model. Many different pieces of software, hardware, and protocols support RSA, which has been in use for decades. RSA is still widely used in legacy systems and devices, which makes implementation simpler and eliminates the need for significant updates or compatibility problems. Furthermore, nearly all secure communications protocols, including Secure Socket Layer (SSL), support RSA. When designing the suggested authentication model, RSA can be more useful in settings where wide compatibility is crucial. RSA is faster at generating digital signatures because the signature operation in RSA involves simpler and more efficient modular arithmetic.

The qualitative method is multimethod in focus, involving an interpretive, natural approach to its subject matter. This means that qualitative experimenters study effects in their natural settings, trying to make sense of or interpret, marvels in terms of the meanings people bring to them. Qualitative exploration involves the studied use and collection of a variety of empirical accouterments for example, case studies, particular experiences, introspective, life stories, interviews, experimental, literal, interactional, and visual textbooks that describe routine and problematic moments and meanings in individualities' lives. It is crucial to have a plan for examining, illuminating, forecasting, and managing the qualitative factors in each interaction. Thus, the research

hypothesis is made to discover whether the proposed authentication model using digital certificate can authenticate the user and the device in smartphone user.

The qualitative method implemented in this research involved getting data from experts' reviews. Lists of questionnaires are constructed and given to the expert reviews. The criteria for choosing the expert review are based on two parties, the academicians and industry experts. These questionnaires will be explained more in Chapter 5 later. The questionnaires are constructed based on the problem statement, objectives, and hypothesis of this research. Based on the research objectives, the questionnaires are generated by analyzing authentication requirements for smartphone applications in terms of security of authentication and suggestion of algorithms used to authenticate the user and the device. The criteria such as the clarity of the authentication flow, the security adequacy implemented in the proposed model, and the practical implementation feasibility of the proposed model are referred to in generating the questionnaires.

The quantitative method used in this research involves calculating simulated data by using the RSA formula implemented in the proposed model. The calculation of the simulated data is shown in Chapter 5.

3.4.2 Research Proving Method

To evaluate and prove the proposed authentication model, there are two methods used in this research are qualitative method where experts review the proposed model, and the quantitative method where simulated data is created and used to calculate the expected outcome of the proposed model using the RSA Formula.

To select the experts, there are a few criteria to be fulfilled. Since the proposed model focuses on the authentication of smartphone user, thus, the background of the experts must be determined based on the criteria of the proposed model. There are two groups of experts that have been selected which are the academicians and industrial experts. The similarities of both groups are that they are experts in information security and authentication.

Academician experts can provide theoretical knowledge since they have a great deal of theoretical knowledge about cryptography, algorithms, and authentication techniques. Besides, experts in academia are usually engaged in research that advances theoretical underpinnings.

On the other hand, experts in the industry have hands-on expertise in setting up and managing authentication systems in real-world settings. Besides, in real implementations, industrial professionals are often well-versed in security dangers and compliance standards, and they are often susceptible to cost and resource limits.

To sum up, industrial experts offer practical insights and an emphasis on real-world execution, whilst academic experts contribute theoretical depth and understanding. The overall strength and suitability of the suggested authentication model are improved by a fair evaluation that includes both kinds of experts.

As for the quantitative method, generating simple simulated data are created using potential user Identification (ID) and device IMEI number. Since the proposed authentication model uses RSA for authentication and digital signature, thus the simulated data created is calculated using the RSA algorithm to encrypt and decrypt the simulated data.

3.5 Chapter Summary

In this chapter, the researcher explained the method and software used to analyze the development and Evaluation of the Authentication Model. These phases are the requirements to achieve the objectives. Phase 1 aims to analyze the authentication requirement to authenticate both the user and the device.

In phase 2, the researcher proposed and designed the authentication model to authenticate the user and the devices using digital certificate for smartphone user.

Phase 3, is the evaluation where 2 methods to evaluate the proposed method which is the expert's review and the mathematical calculation by implementing simulated data in the algorithm and formula used in the authentication model. In summary, the three stages of the research process may address all of the research questions and are in line with the study objectives. Each phase's research procedures are adequate for producing research contributions and resolving the issue statement discovered in the preliminary stages of the study.