CHAPTER 3

METHODOLOGY

This chapter will present the methodology used in this research. The methodology will explain how the research workflow will be concurrent with the research objectives. It comprises three stages where every stage represents one objective that have to be achieved. Tools including software and hardware that will be used in this research also provided.

3.1 Research Process

This research is basically focuses on three main phases in its methodology process, which is preliminary study, followed by development and finally the evaluation phase. The methodology process is illustrated as in Figure 3.1.

As shown in Figure 3.1, the first phase of this research aims to study and examine the existing methods of encryption and decryption based on location. This phase also reviewing on cloud storage features to provide a literature review. The objective of the second phase is to develop enhanced key generation method. Finally, the objective of the third phase is to validate and evaluate the developed enhanced method.

A scientific research process makes use of multiple phases of process in its methodology where each phase has a relationship with the research questions, research objectives, research activities and research outcomes. Detail process that needs to perform in each of the phase are explained in the following research methodology.

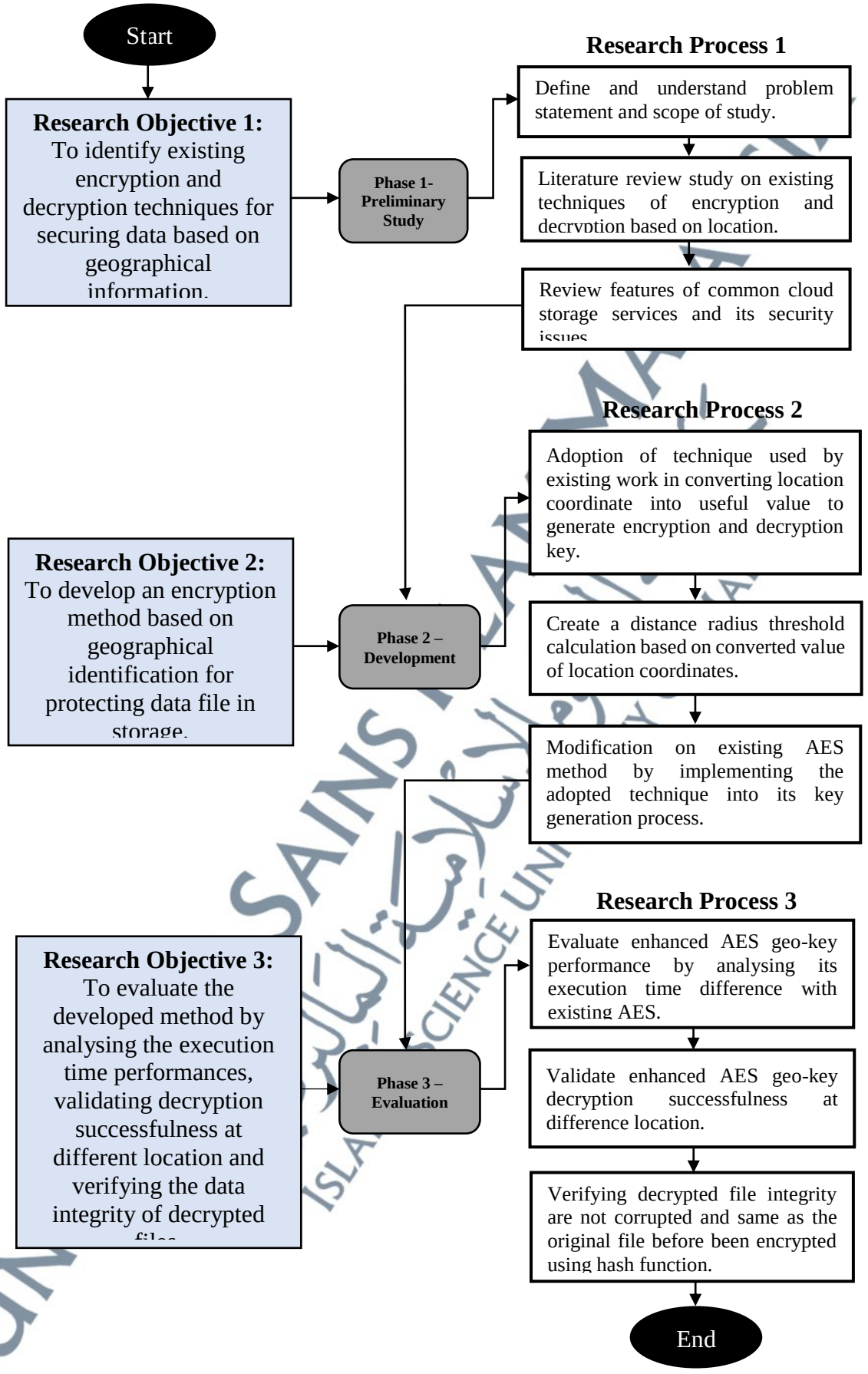

Figure 3.1: Research methodology process

3.1.1 Preliminary Study

In the first phase, existing works related to cryptography, encryption, decryption, geo-encryption and cloud storage is being reviewed thoroughly. This review on existing literature was performed in order to determine the best algorithm that can be used and enhance for method development in this research. Numbers of algorithm techniques were found in the literatures that related to this research study. Therefore, these techniques were compared with each other to determine their strength and weakness.

3.1.2 Development

During the development phase, a modification on existing encryption method will be designed which aiming to provide additional security mechanism via location information, device MAC address and user input password to address the security issue of access restriction based on location. The existing encryption method that will be used in this research is AES method from symmetric algorithm where it has better speed performance compared to asymmetric algorithms which has been explained in 2.3.1(i) in chapter 2. The modification of the encryption method will be focusing on how the encryption and decryption key will be generate based on the geo-location characteristics which are the latitude and longitude coordinate of where the decryption process should take place.

The generation process of encryption and decryption key in development phase are adopting an existing work that used location-based cryptographic technique which is Location Based Encryption Technique and Some of Its Applications (Scott & Denning, 2003). This location-based cryptographic technique has been defined from the preliminary study in phase 1. Figure 3.2 shows the encryption key generation process flow diagram of existing geo-encryption method and Figure 3.3 shows its overall

encryption and decryption process. Although this research was not a recent work, this research has defined a clear technique of its protocol and it is practical to be adopted in term of the technique of retrieving the location information.

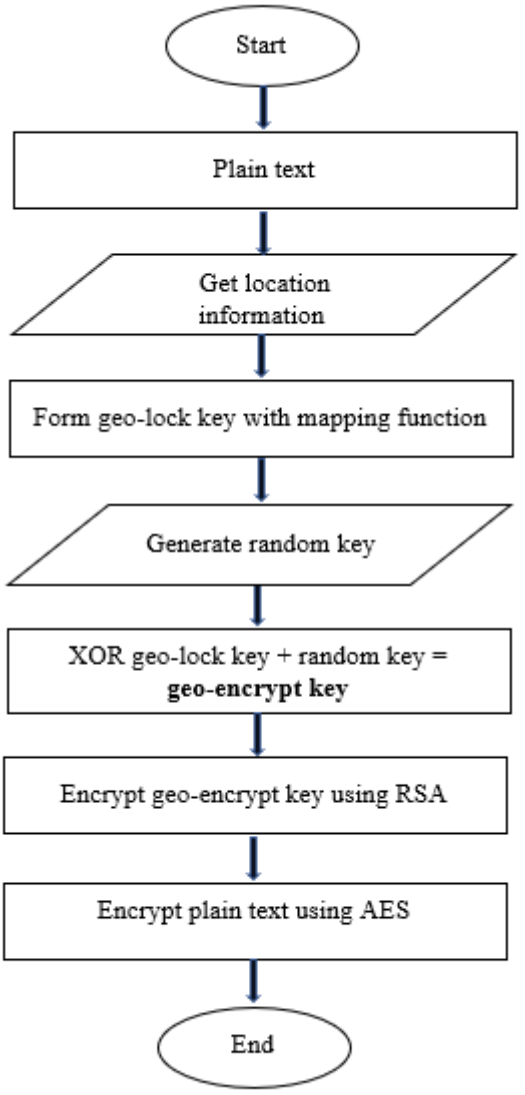

Figure 3.2: Existing key generation process in geo-encryption method.

The brief explanation on how the development of the key generation will be explained in Chapter 4.

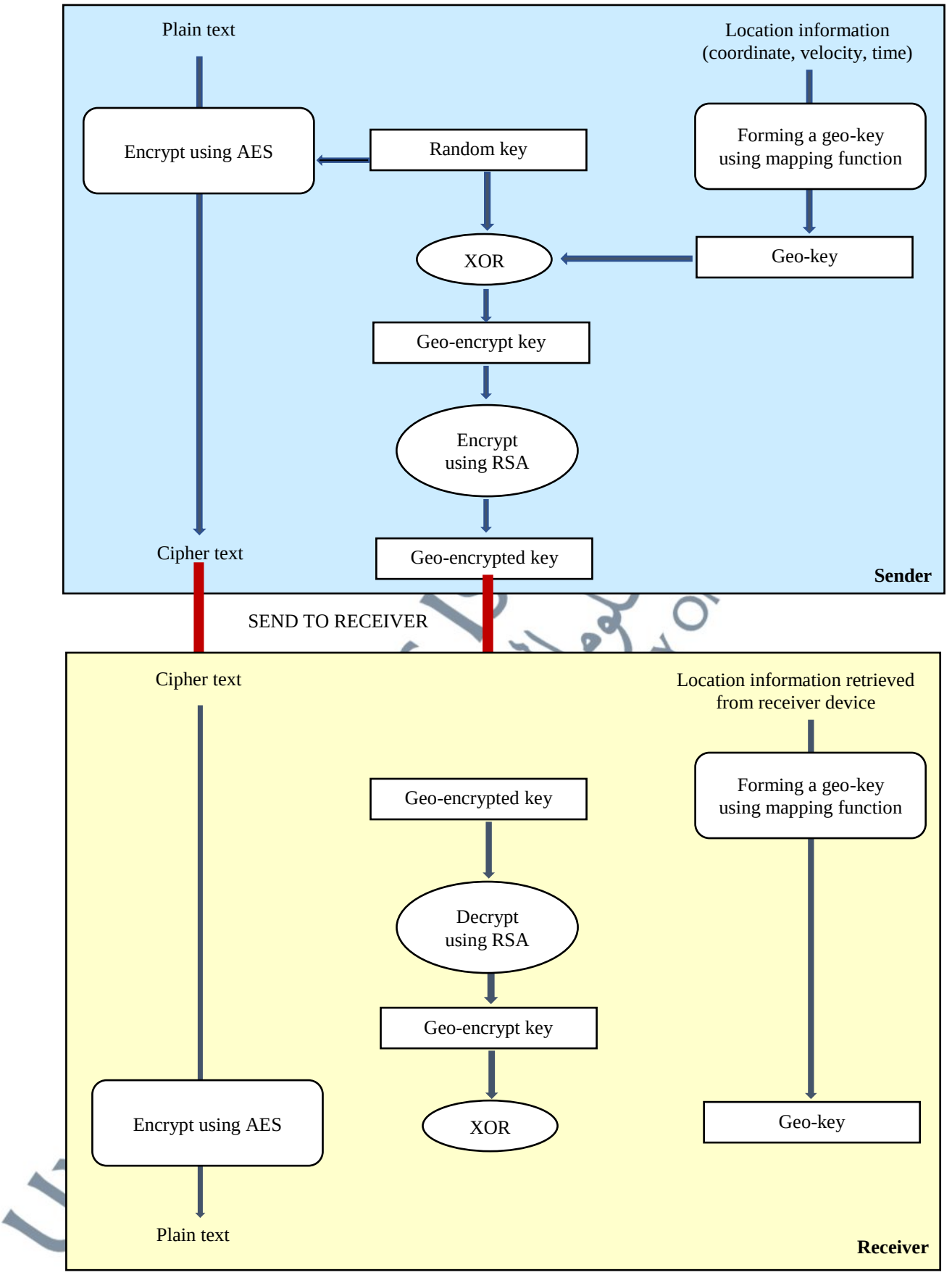

Figure 3.3: Overall process of key generation in existing geo-encryption method

3.1.3 Evaluation

For this final stage, after enhanced AES geo-key method has been developed, three experiment will be conducted to evaluate the method. For this first evaluation experiment, a time-performance comparison for encryption and decryption process between using the existing AES method with using the enhanced AES geo-key method will be conducted. This comparison is carried out to evaluate whether the enhanced AES geo-key method is having a huge gap in term of time performance with the existing AES method.

Second experiment is conducted to validate either the encrypted files could be decrypted outside the intended location. As one of the security issue which this research wanted to address is the lack of remote access restriction based on location, this experiment outcome should present that all the content of the encrypted file are only can be decrypted and can be accessed inside the range of intended location. This experiment is conducted outdoor to verify some range of distance which has been set up during the initial process of file encryption.

Third experiment is conducted to evaluate the integrity of file that has been encrypted and decrypted. Hash value comparison method has been used in this experiment to evaluate either the original files are corrupted or not after been encrypted and decrypted with the enhanced AES geo-key method. The original file and decrypted file are computed using two type of established hash function which then will be compared to validate whether it produces the same hash values after going through the encryption and decryption process.

The brief explanation on how the evaluation experiment conducted will be explained in Chapter 5.

3.2 Summary

This chapter explained the methodology used to conduct this research based on three research phases that has been highlighted in this chapter. The methodology focuses on the identifying the existing method related encryption and decryption and identifying existing techniques used for geo-encryption. Next configuring how the second objective of this research should be carried out in order to come out with the enhanced AES method. Last but not least, this chapter has also highlighted on how the evaluation on the proposed solution should take placed in order to verify either developed solution in objective two could address the research problem that has been identified in Chapter 1.