CHAPTER 6

CONCLUSION AND FUTURE WORKS

This chapter concludes the overall research. The next following section outlines the research findings, research contribution and future works.

6.1 Research Objectives Analysis

This research has conducted to address three security issues of research problems that has been highlighted in 1.2 of chapter 1 which are the secure file storage in cloud, vulnerable of encryption key and unauthorized remote access on file at cloud storage due to lack of location-based access restriction. This research outcome has shown the ability of enhanced AES geo-key method that has been derived from existing AES method with modification at its key generation process via adopting the techniques of converting location coordinates into encryption key has secure the encrypted file stored in cloud storage from being accessed by unauthorized user outside the intended location.

In spite of the fact that enhanced AES geo-key method took 5.62% longer time to execute compared to existing AES method, the enhanced AES geo-key method has the ability to manage the vulnerable of encryption key issue when generated encryption key is formed by the combination of three hardly predictable parameters which are location information, device MAC address and user password. The following table summarizes the objective mapping with the outcome. Each objective is analysed to know how well the proposed topic accomplished the target. The objectives analysis is as follows in Table 6.1:

Table 6.1: Research objectives and deliverables analysis

	Research Questions & Objectives	Research Activity	Deliverables
Phase 1- Preliminary Study	**Research Question 1:** How data can be secured on different locations and what techniques can be applied? **Research Objective 1:** To identify existing encryption and decryption techniques for securing data based on geographical information.	Define and understand problem statement and scope of study. ↓ Literature review study on existing techniques of encryption and decryption based on location. ↓ Review features of common cloud storage services and its security issues.	• Three security issues in cloud storage were defined which are i) Secure file storage. ii) Vulnerable encryption key iii) Lack of access restriction based on location • AES method was found as the better performance in term of execution time speed in symmetric cryptography. • Two conference proceedings presentation and publication. • Two articles published in Journal of Physics and Malaysian Journal of Science, Health & Technology.
Phase 2 – Development	**Research Question 2:** How to design appropriate technique on protecting data privacy and security issues at different locations? **Research Objective 2:** To develop an encryption method based on geographical identification for protecting data file in storage.	Adoption of technique used by existing work in converting location coordinate into useful value to generate encryption and decryption key. ↓ Create a distance radius threshold calculation based on converted value of location coordinates. ↓ Modification on existing AES method by implementing the adopted technique into its key generation process.	• An enhanced AES geo-key method developed using Equirectangular projection method to convert longitude and latitude coordinates to generate geo-key. • A geo-key generated using retrieved location coordinate with the combination of device MAC address and user input password.
Phase 3 – Evaluation	**Research Question 3:** How to validate the new developed technique works for protecting data privacy and security issues at different locations? **Research Objective 3:** To evaluate the developed method by analysing the execution time performances, validating decryption successfulness at different location and verifying the data integrity of decrypted files.	Evaluate enhanced AES geo-key performance by analysing its execution time difference with existing AES. ↓ Validate enhanced AES geo-key decryption successfulness at difference location. ↓ Verifying decrypted file integrity are not corrupted and same as the original file before been encrypted using hash function.	• Small gap of time performance between both methods were counted where enhanced AES geo-key method were only taking 2.73% longer than existing AES method took for execute. • All files could not be decrypted when the decryption request is made outside the distance radius threshold. • All decrypted files having the same hash values as their original file's hash values before been encrypted.

6.2 Research Contribution

This research has published two conference proceedings and two articles as following.

a. Nur Syafiqah Mohd Shamsuddin, Sakinah Ali Pitchay and Farida Hazwani Mohd Ridzuan, Data Protection in Cloud Storage Using Location-Based Cryptography, E-Proceeding of USIM, 1st International Postgraduate Conference 2018.
b. Nur Syafiqah Mohd Shamsuddin and Sakinah Ali Pitchay, Malaysian Journal of Science, Health & Technology (MJoSHT), Location-based Cryptographic Techniques for Data Protection, Vol 4, Special Issue, eISSN: 2601-0003, 2019
c. Nur Syafiqah Mohd Shamsuddin and Sakinah Ali Pitchay (2019), Location-based Cryptographic Techniques: Its Protocols and Parameters, RITA 2018, Lecture Notes in Mechanical Engineering, pp 79-86.
d. Nur Syafiqah Mohd Shamsuddin and Sakinah Ali Pitchay (2020), Implementing Location-Based Cryptography on Mobile Application Design to Secure Data in Cloud Storage, J. Phys.: Conf. Ser. 1551 012008.

6.3 Future Works

Each research has their own limitation. The future works of this research can be improved on the device accuracy of retrieving location. Due to cost-effective for the purpose of this research, this research used the Raspberry Pi embedded with GPS module as a device to retrieved 2-D real-time location information which consist of longitude and latitude coordinates. However, this device have some limitation to retrieve accurate coordinates when it is placed at indoor environment. Therefore, more accurate location retriever device with higher specification should be used in order to get higher location accuracy regardless it is indoor or outdoor environment.

There are some strategies and technologies that should be considered in future works to enhance location detection in indoor environments which are:

a. Machine learning with sensors. Machine learning algorithms can be trained to make sense of sensor data for indoor positioning (Khokhar et. al). Besides sensors, other available advanced technology in 5G Ultra-Dense Networks (UDN) could be used with machine learning to estimate user equipment location (Ala'a Al-Habashna et. al).
b. Ultrasound-based systems use ultrasonic sensors to measure distances and locate objects indoors via different indor localization techniques such as angle of arrival, time of flight, return time of flight and received signal strength. (F. Zafari et. al)
c. Bluetooth Low Energy (BLE) Beacon is commonly used for indoor location tracking. It works by broadcasting signals that can be received and triangulated by nearby devices. (R. Faragher and R. Harle)
d. Wi-Fi-based positioning. Utilize Wi-Fi access points to triangulate a device's location based on signal strength and proximity to known access points. (Roy et. Al)