CHAPTER 1

INTRODUCTION

1.1 Overview

This chapter will discuss on research problem statement that motivates on this research topic, describes the research questions, research objectives, research scopes, research plan and the organization of the thesis.

1.2 Problem Statement

Anything connected to the internet is exposed to cyber risks including the risk of a personal data breach in cloud storage. The use of the internet has risen significantly nationwide during the Covid-19 pandemic resulting in a huge number of cyber incidents being reported. According to the Internet Users Survey (IUS), 2020 report by the Malaysian Communications and Multimedia Commission (MCMC), the percentage of internet users in 2020 grew by 1.3% from 87.4% in 2018 to 88.7% in 2020 while a total of 8,669 cybersecurity incidents were reported to the Cyber Security Malaysia in 2021. Cloud adoption therefore becomes a significant means to stay ahead in a post COVID-19 world focused on flexibility for remote access. However, some businesses are still not moving with 66% of IT professionals citing security as their greatest concern in adopting an enterprise cloud computing strategy (Katie Costello & Meghan Rimol, 2020). They believe when everything is accessible online, data can be vulnerable and insecure. Data security, encryption in cloud and remote access restriction have been significantly a consistent security issues in cloud computing including cloud storage

which have been discussed by (Ali et al., 2021; Alsaadi et al., 2020; Tabrizchi & Kuchaki Rafsanjani, 2020; Wu et al., 2019; Yang et al., 2020; Zhang et al., 2018). It is a common concern for any technology, but it becomes a major challenge when Software-as-a-service (SaaS) users have to rely on their providers for proper security (Ali Pitchay et al., 2015; Tabrizchi & Kuchaki Rafsanjani, 2020).

To secure data in cloud storage, it involves preventing unauthorized people from accessing the data as well as to avoid data theft and to ensure uninterrupted operation. Whereas to build customer trust, commercial cloud services systems encode each user's data with a specific encryption key. When the user requests to view the data, the decryption key is applied to decrypt the data and then viewed by the users. Decrypted key can be stored either by the service itself, or by individual users. Most services keep the key themselves, letting their systems see and process user data (Tabrizchi & Kuchaki Rafsanjani, 2020). These services also access the key when a user logs in with a password and unlocking the data in order to use it. This is much more convenient than having users keep the keys themselves. However, there are still a possibility that their own application might be compromised or hacked, allowing an intruder to read user's files either before they are encrypted for uploading or after being downloaded and decrypted (Haibin Zhang, 2018).

While protecting data content in cloud environments, data encryption is not a new issue when it has raised numbers on set of data encryption protocols and key management considerations (Drew Wright, 2020; John Moore, 2014). National Institute of Standards and Technology (NIST) researchers and the experts are continuously investigating the key management challenges in a cloud environment where the cloud might complicate matters, but regardless of computing style, key management has been the perennial weak link in encryption (James Christiansen, 2019). Christiansen likened

the situation to a person who installs an expensive car alarm but leaves the keys in the door as the same thing in organizations of cloud storage, where attacker would not attack the AES-256 algorithm when the vulnerable encryption key is available to be attacked instead. Christiansen also suggest users to encrypt data before it goes to the cloud. When users move the data, users do not have to care about the data that is left behind with the cloud provider as the data is encrypted with user's keys, then the cloud provider or any attacker that gains access to the cloud provider's systems or backups cannot access user data.

During the Covid-19 situation, many company are encouraging staff to work from home remotely either using staff own device or company laptop. Remote access allows staff to access office systems at cloud via the internet from remote locations. Despite the many benefits, remote systems can expose company data to many risks. Staff will have to manage these risks to keep their remote access secure at all times, otherwise company business data might be exposed as remote working relies on the exchange of business data or services outside of the corporate infrastructure, typically over the internet which are outside the organisation's control. The remote environment in which staff devices are used may also pose risks. For example, security concerns may exist around the lack of physical security controls which creating a risk of device loss or theft. The worst-case scenario might happen if device being robbed, the theft which is someone that is non-authorized personnel gains access to the stolen device which give them opportunity to access company system or data, then monitor and manipulate confidential company data from any place of the theft location. In order to reduce this risk, encrypting confidential data is one of the security measures to prevent theft. Company might define specific location for each staff to do their work during work remotely from home as the key requirement to decrypt the confidential company data.

Staff who are working outside the define location unable to gain access on company data.

Based on the given problem, there are three major concerns that need to be enhanced which are (i) secure file storage, (ii) vulnerable encryption key and (iii) lack of remote access restriction on file at cloud storage. In general, existing works by (Abolghasemi et al., 2013; Lin et al., 2017a, 2017b; Tse et al., 2014) prefer to store the key together with the data in cloud storage data file. However, this thesis proposes to study the existing encryption and decryption methods for security data storage where the encryption key being stored by the user machine. Existing encryption methods use keys that produced from the combination of user password and random key-generation or pseudo random key-generation (Kolapwar, 2015; Kumari et al., 2018; Lin et al., 2017a; Mamun et al., 2021; Tysowski & Hasan, 2013). In attempt to protect against unauthorized remote access on stored data, no recent work has discussed to solve unauthorised remote access from different location during work from home. Thus, this thesis aims to include location information as an additional requirement parameter to protect data in cloud storage via encryption and decryption process. The location information which consist of latitude and longitude coordinates will be used to generate the encryption key using establish strong private key encryption which is AES algorithm (Mamun et al., 2021; Smid & Foti, 2021). Besides the location information, this thesis proposes to enhance the encryption key by merging the user password, user's location information and user's device unique identification, MAC address to generate the encryption key known as geo-key in order to overcome the three major concerns of security issues while securing data in cloud storage.

This thesis is implementing three parameter which are user password, user's location information and user MAC address to generate the geo-key as the encryption key to add

an extra layer of security to a system. This approach is often used in scenarios where security is of utmost importance. The user's password is a common and widely accepted way to authenticate a user. Password ensures that only authorized users can generate the encryption key. Passwords should be kept secret and are something only the user knows. Second parameter, which incorporating user location information adds an additional factor to the authentication process. User location can be used to ensure that the user is in a specific physical location when generating the encryption key. This is useful for applications in this thesis where physical presence is critical for file access or data decryption. Third parameter, which the MAC address of the user device provides a hardware-based identifier. Including MAC address in the key generation process can add a layer of device-specific security by ensuring that the encryption key is tied to a particular device, making harder for attackers to use the key on a different device even if the attacker know the password. Combining these three parameters in the key generation process makes the geo-key more difficult for unauthorized users to gain access to the encrypted file or generate decryption keys. Even if an attacker manages to obtain the user's password, the attacker would also need to know the user's location and have access to the user's device specific MAC address to generate a valid encryption key.

1.3 Research Questions

The research questions are defined as follow:

a. How data can be secured on different locations and which method can be applied?
b. How to design appropriate method on protecting data privacy and security issues at different locations?

c. How to validate the new designated method works for protecting data privacy and security issues at different locations?

1.4 Research Objectives

The research objectives are defined as follow:

a. To identify existing encryption and decryption methods for securing data based on geographical information.
b. To develop an encryption and decryption method based on geographical identification for protecting data file in storage.
c. To evaluate the developed geo-key method by analysing the execution time performances, validating decryption successfulness at different location and verifying the data integrity of decrypted files.

1.5 Research Scopes

The research scopes are defined as follow:

a. This research focuses on enhancing the existing encryption methods for securing data in storage based on location access restriction.
b. The encryption and decryption key will be generated using the combination of location information, user password and MAC address.
c. Existing related works focuses mainly on plain text only (Karimi & Kalantari, 2011; Liao & Chao, 2008), this research aims to encrypt and decrypt data that support variety types of format as following:
    i. Documents in pdf, doc, pptx, xlxs and txt file extension of format.
    ii. Audio in MP3, and WMA format.
    iii. Video in MP4, WMV, and WAV format.

iv. Photo in JPEG, and PNG format.

`

1.6 Thesis Organization

This research is organized into five related chapters. Chapter 1 describes the overview of the research. This chapter discusses briefly the research background and the problem statements. This chapter also consist of research questions, research objectives, research scopes, research expected outcomes and the research organization.

Chapter 2 discusses the literature review on cryptography algorithm, which are made up of symmetric and asymmetric key. This chapter also reviews on types of encryptions and decryption in cryptography. A summarized the existing work on location-based encryption also provided in this chapter.

Chapter 3 presents the methodology that being used to achieve the objective of this research. In this chapter, the research workflow also been delivered. It includes the operation of text encryption and decryption and the tools used to develop the application.

Chapter 4 will deliver the findings and analysis of this research. It describes the results of using the enhanced algorithm of geo-encryption and its evaluation.

Chapter 5 summarizes the conclusion and describes the future works.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA