Chapter 1

Introduction

1.1 Background

Nowadays when the technology become more advance people can obtain information easily and when people already get the information they can manipulate the data. In order to prevent the information or important data being manipulated by unauthorized person then people also try to develop new technology to secure the used of the information or data from unauthorized person. One way to protect the information or data is using password before people can use or get the information. Using password to acquire the information is very common nowadays; many people and many systems use this method to protect their information from unauthorized person. The password actually only known by the authorized user only, but nowadays the attacker can obtain the user password easily.

Since it use for security purpose then sometimes people wants to make it easy by using same password for login to a system, ATM, and etc. The password itself has characteristic that can only verify the user and cannot identify the user. This means whoever get the password can access the information or get it, although that person is not an authorized person to access the information. Besides using password to protect people try to use signature in particular system, such as for using the credit card where we must sign and the casher officer try to match the signature pattern with the one on the card, but the use of signature also has same problems with the password method. The problems are same since the signature's characteristic same like the password's

characteristic and it can caused same problem. If we lost our card and it is taken by unauthorized person, that person can learn to copy the owner signature and they can use that card, as long as the card owner is not call the bank to block the use of their credit card.

To overcome this password and signature method weaknesses then people try to develop new security system in order to protect the information from unauthorized person. The new technology that developed to overcome this weakness is called as Biometric technology. This technology is used human characteristic that taken to become a password for verify the user. The biometric technology provide two functions, there are verification and identification. The biometric technology can be divided into two classes, there are behavioral and physiological. The behavioral class related to people behavior which is contain signature and voice, so the signature and voice are used as a recognizer of that person. The physiological class more related to physical characteristic that owned by the person, such as fingerprints, iris, retinal, DNA, face, etc. [30]

Besides using the biometric technology to get any information and data that we need, the biometric technology can be used for attendance system where usually the company or university used manual system. The manual system means that the attendance system used clock printed on the paper or use personal signature. Using this system people can easily do cheating like the signed the attendance for their friends who do not come to work or attend the class. The biometric technology can prevent cheating because it uses the human uniqueness, such as fingerprints, as the ‘signature’ so the other people cannot sign in for their friends.

Nowadays the biometric technology is already used in office, school, etc; because the biometric technology is very safe and secure. Beside that the biometric technology very

easy to be used, so many company or school start to implement this technology in their system. The biometric technology might be needed now since the use of password or signature is not safe anymore. When we using password there is possibility that we forgot or lost it and also if we use signature there is possibility that someone copy it and use it, but if we use the biometric technology we cannot be forget it or copied by other person. Nowadays the biometric technology is safer than using the password in order to be recognized by the system if the user is authorized to use the information or not. The most common used biometric technology now is fingerprint where the scanner or the hardware to read the fingerprint pattern already sale in the market.

Although use people physical or behavior as the recognizer, but it already proved that people do not need worry if their physiological change. For example the use of fingerprints, people must know that their fingerprint might be change when they get older, but when they stop growing then the shape of their fingerprint will be the same. Beside that it already proven that the uses of hardware of fingerprint scan, iris scan, or retinal scan are safe; and even for the retinal and iris scan they already create a hardware that use some kind of infrared that the amount of light is still same like people walk around on the sunny day. [31]

1.2 Scope

There are several of human characteristic that implemented in biometric technology such as fingerprints, retina, iris, face recognition, and DNA; beside that there are common biometric that used in many university, which is signature. To prevent the thesis become so general then this thesis will be limited only to describe more deeply about one

technique that already used for long time, but now it try to be implemented in advance technology, which is the fingerprint.

This thesis will be focused on:

- How the fingerprints can act as a password to recognized and identify that the user is an authorized user
- How the fingerprints work in attendance system
- Comparison between the fingerprint technology with the retinal scan when both of these technology use as a password in attendance system

1.2.1 Constraint

To develop this thesis there are several constraint or limitation. The constraint or limitations are like :

- The implementation cost is high, since it needs additional hardware to scan the fingerprint of the user
- There is possibility that the fingerprints can be damaged because of the user had scratch in their finger
- The ability of the user to adapt with the new technology if this technology really implemented in that company or school
- The hardware for retinal scan still unavailable until now and the program for this technology still prototype

1.2.2 Assumption

To implement the biometric technology in one company or school then I have assumption that the company or school that want to implement this technology to their attendance system or login system already has all the requirement that needed to implement this biometric technology. Besides having all the requirements, the company or school must have talented worker who understand and can implemented the biometric technology to their system. I also assumption that the user fingerprint always can be read by the hardware and the shape of the fingerprint is never change. Other assumption is there will be no intrusion when the users use the hardware for scanning their fingerprints.

1.3 Aims and Benefits

The aim that I want to achieve from this thesis is to compare between fingerprint technology and retinal scan technology implemented in attendance system.

Beside the aim that I want to achieve in this thesis, this thesis can give some benefits to the reader. The benefits that reader can get are:

- Know the advantages of implementing fingerprint biometric technology as a recognized for their attendance system
- Know the reason why people try to develop the retinal scan even it already said that the fingerprint is already safe
- Know under what condition the fingerprint scanner cannot read the fingerprint pattern

1.4 Structural

This thesis content will be divided into seven chapters. The structure of this thesis will be as following:

- Chapter 1: Introduction
    - Background
    - Scope
        - Constraint
        - Assumption
    - Aims
    - Structure
- Chapter 2: Theory Foundation
    - Secure System and Biometrics Technology
        - Characteristic
        - Advantage
        - Disadvantage
    - How Biometric Works
    - Types of Biometric
        - Retina
        - Iris
        - Hand geometry
        - Face
        - Fingerprint

  - Real Implementation of Biometric Technology
  - Attendance System
- Chapter 3: Comparison Method
  - Case study
  - Method
  - Analysis data
- Chapter 4: Problem and Solution Analysis
  - Attendance System at BPPT
- Chapter 5: Comparison
- Chapter 6: Evaluation
  - Strength
  - Weakness
  - Thread
  - Opportunity
- Chapter 7: Conclusion and Discussion