CHAPTER I
INTRODUCTION

1.1 Background

The challenges posed by the Internet world are increasingly widespread and almost cover the area for devices that require the internet. Internet of Things (IoT) now days has become the key to every device based on the Internet. IoT develops a big number of connections and services. The devices can be sensors, computers, smartphones, even home appliances related to daily needs. As for wireless communication, Low power wireless device is believed as the best solution for IoT use cases. Wireless communication system always requires a lot of power to work properly, and one of the solution to optimize the device that has low power energy is BLE. Bluetooth Low Energy (BLE) has become one of the revolutionize wireless communication between the device that allows the process of transferring data in the air with low level of power [8].

BLE can be applied in every device such as thermometer, smart watch, and in this thesis, specifically about Temperature Sensor. Temperature Sensor works to check how the condition from the body of the user can be detected within a second, but still under the given power from BLE. The information that has been detected from the Temperature Sensor will be sent right away and stored in the database. BLE is known for having a simple infrastructure of network security, which is causing the system to be attacked by unknown parties. There are so many possibilities type of attack that might occur on BLE, i.e., piggybacking, beacon hijacking, device spoofing [8], and Man-in-the-Middle (MITM) [9]. In the BLE protocol stack, there is a layer called 'Security Manager' which provides a security module for BLE. The encryption system used on BLE is 128-bit AES, which is short and symmetrical. The short length of the key which makes it easier for the attacker to crack the encryption key [10] and from that, there are few methods used to decrypt the key.

From the previous experiments and several papers, some new solutions are suggested. The first solution is Geo-location validation of BLE. Each BLE (BLE beacon) hardware, has been registered with geolocation information on online server or has been provided by the Global Positioning System (GPS) module for mobile users. This technique can be used to prevent spoofing attacks. However, it is un-

fortunate that in this technique many loopholes are found in the safety framework and make this technique monotonous. When the beacon user moves, there will always be a location update, which will automatically continue to use new information and consume geolocation information on the server. As for the second solution is cloud-based Token Authentication of BLE. In this solution, it is mentioned that BLE hardware (BLE beacon) provides an algorithm that will generate token values. This token value will be the identity of each beacon, which means that each beacon will have a different a token value and can only be encrypted by cloud server.

1.2 Formulation of Problem

The problem was taken as the undergraduate thesis to find a solution to prevent unwanted acts that might occur on the system by introducing new solution. From the previous method, it is stated that BLE is feared that has network security that is considered as weak, and can be easily attacked by third parties. Several papers have proved how to prevent the attack by using AES-CCM Encryption, but the disadvantage are the exchange keys are too fragile and exposed some of the secure information that can be used by an attacker.

1.3 Purpose of Research

The purpose of this thesis is focusing on how to introduce a new method for BLE security system, finding advantages, disadvantages and differences in theory given.

1.4 Scope of Problem

The problem scope of this thesis are given below.

1. This thesis will only discuss the performance and token authentication process of the device. The performance of the device that will be analysed are based on Quality of Service (QoS), which are Throughput, Delay and Jitter.

2. This thesis only focuses on the BLE security system with the Token Authentication method that occurs only at the beginning of the connection between Master and Slave.

3. This thesis will only discuss the process that occurs in authentication, based on the data read and obtained by sniffer device.

4. This thesis requires a Bluetooth connection version 4.1 or above.
5. The attack that will be applied in this analysis is Packet Sniffing.
6. Data that is sent to the database and showed on the screen consists of only integers and above and in scale of Celsius (°C).
7. This thesis only discusses the security mechanism on BLE devices. Apart from the BLE device, it is part of the android application developer.

1.5 Research Method

This Final Project is divided into 2 *work packages* (WP):

1. WP1: Literature Study

   Theory for this thesis is needed for analyze is taken from textbooks, journals, conference papers, theses, or dissertation books.

2. WP2: Simulation

   Simulation will be done to facilitate the process of understanding the analysis using the software and hardware provided.

1.6 Thesis Organization

The rest of this thesis is organized as follows:

- Chapter II BASIC CONCEPT
  This chapter contains of the conceptional of IoT, BLE and Temperature Sensor as the benchmark to understand the thesis.
- Chapter III TOKEN AUTHENTICATION MECHANISM FOR BLUETOOTH LOW ENERGY (BLE) NETWORKS
  This chapter contains of deeper explanation, design system, and workflow and mechanism of this thesis.
- Chapter IV EVALUATION
  This chapter contains the results of simulations and analysing results by comparing the data from the previous method.
- Chapter V CONCLUSION
  This chapter contains conclusions and suggestions that can be used for further learning or as a reference.