# CHAPTER 1
# INTRODUCTION

## 1.1 Background

As the time goes, information technology continues to develop. Nowadays, humans are getting more comfortable in life with technology that continues to evolve. Wireless technology is one of the technological developments that can facilitate human life, with wireless technology that allows long distance communication and information exchange without physical contact. The very rapid advancement of wireless technology has made cable technology less needed. Thus, wireless technology's advantages reach the most significant selling points in the transmission technology field worldwide [1].

One of the most widely used communication technology devices is Wireless Fidelity (Wi-Fi). Now its ability to access the Internet of Things (IoT) makes it easier for users who only need to connect them. Wi-Fi itself has penetrated the needs of work, education, and even commercial. Wi-Fi is also a lot of public areas for free, causing much misuse of Wi-Fi itself. Its use in this general area is the Wi-Fi owner's regarding password security and another misuse. In this case, it is common in restaurants that have free Wi-Fi service. Many take advantages of this free Wi-Fi by only ordering one or two orders and then staying for a long time. This case caused losses for the restaurant owner.

Wi-Fi has a password which is also a security solution for Wi-Fi itself. However, this password isn't perfect for being the ideal solution because customers can still ask for the Wi-Fi password by ordering food or drinks that they buy cheaply. Then they spread the password to their group friends. Therefore, in this final project, we are looking for a solution so that passwords are not misused, as in the previous case. The last weakness is in the data that was previously shared between the access point (AP) and gadget customers that can provide security. There are several references for designing this final project, one of which is according to an international journal from Alfredo Matos, Daniel Romao and Paulo Trezentos[2], but in that journal there is no bandwidth limitation on the connected wifi. Meanwhile, in the final project, it is designed to

limit the bandwidth of each user connected to wifi using a Captive Portal[3].

Therefore, in developing the research that has been done previously, this time the researcher will design a system and implement a system that can limit the bandwidth connected to wifi and apply NFC to connect wifi to the user's smartphone. Bandwidth limitation itself is carried out by Captive Portal and is made for longtime restaurant customers by doing bandwidth so that internet connections become slow and Near Field Communication technology can provide more secure security, with passwords that you don't need to tell. By connecting the smartphone to NFC then after that it can connect to Wi-Fi. With the owner of the free Wi-Fi service, it's lost, and there is no loss caused by irresponsible people using only unlimited free services.

## 1.2 Problem Formulation

Based on the previous background, the problem formulation in this undergraduate thesis has several formulas. Currently, many technologies are developing, including the emergence of NFC and Captive portal, which we discuss in this undergraduate thesis. This undergraduate thesis also analyzes the internet speed, which increases or decreases as the number of devices increases. Prevent anonymous people from connecting to Wi-Fi, limit Wi-Fi bandwidth using NFC and Captive Portal, and analyze whether NFC and Captive Portal usage can improve the security and management of Wi-Fi share bandwidth usage.

## 1.3 Objectives

The objectives of this research are to apply NFC and Captive Portal to secure and manage wifi, to prevent anonymous people from connecting to wifi, to apply wifi bandwidth limitations using NFC and Captive Portal, and to analyze the use of NFC and Captive Portal to secure wifi.

## 1.4 Scope of Works

So that the discussion is more oriented, this undergraduate thesis research focuses only on:

1. NFC work system, Captive Portal, and Wi-Fi.
2. Tools that will use in doing this thesis.

3. Application of NFC to secure public area Wi-Fi password.
4. Only focus on cellphone users that have NFC on their cellphones.
5. Implementation of Captive Portal to limit bandwidth and prevent direct internet connection access to public areas of Wi-Fi users without authorization. management of the bandwidth utilization parts of the Wi-Fi.
6. This application is only intended for Android users.

## 1.5 Methods of Research

The stages of the research evaluation methodology proposed in this thesis are as follows:

1. Study of literature study discusses understanding the concepts and theories of IoT, NFC, Captive Portal, and Wi-Fi. References from books, conference pages, journals, and articles are needed to complete ideas and approach this thesis.
2. Analyze the problem analysis in this final project is based on the problems listed in the problem's scope.
3. The simulation and experiment of this final project are carried out using smartphone components with NFC devices. Projects are installed in it using the Captive portal Feature.
4. Testing and analysis of the system, This stage is carried out to test the system that has been built. Testing the parameter is the time it takes a customer to scan their smartphone get Wi-Fi password via NFC, degree of freedom from trouble using NFC and Captive Portal, and the success rate for connecting customer's smartphone with Wi-Fi via NFC and Captive Portal (whether access is granted or not granted). Then, analyze the factors that affect system performance is then carried out to be done.
5. Preparation of the Final Project report. At this stage, the Preparation of a final report and submission is required documentation is complete. The reportformat follows the correct writing rules and complies with the provisions setby the institution.

## 1.6 Summary

The summary in chapters one to five explains that nowadays humans are more comfortable with life with technology that continues to develop. Wi-Fi is also free in many public places, which causes a lot of abuse of Wi-Fi itself. Therefore, in this final project we are looking for a solution so that passwords are not misused. Therefore, the recommended prevention in this final project is to limit bandwidth and implement Near Field Communication (NFC). The bandwidth limitation itself is carried out by Captive Portal and is made for old customers in restaurants by doing bandwidth so that the internet connection becomes slow. This design includes NFC tags and smartphones that already support the NFC reader feature and have installed the application made. The NFC Tag component must be placed on the back of the smartphone. This app can be used as an NFC Tag reader and to connect to a wifi network. From the results of testing the system in this study has a throughput speed of 23080 bps with a total delay of 15.12103 ms. This research is expected to help wifi owners to prevent losses for wifi owners.