CHAPTER 3

RESEARCH METHODOLOGY

3.1 IoT structure

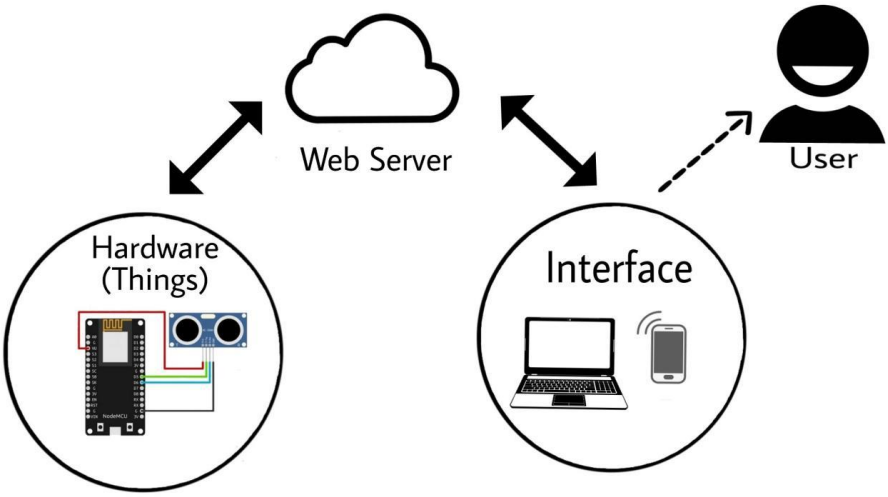

Figure 3.1 IoT Struture

Communication on the Internet of Things starts from the process of retrieving data obtained from sensors as input to be sent to the microcontroller, the microcontroller will process the data in such a way and after that the data will be transferred to a web server and users can access via devices, whether smartphones, PCs, and others. other. This data will be encrypted using the AES algorithm.

3.2 Security Methods

Before continuing research on Internet of Things (IoT) Data Security Using AES Algorithm, there are several security method processes that must be carried out:

3.2.1 AES Operations

The AES algorithm encryption process consists of 4 types of byte transformation, namely SubBytes, ShiftRows, Mixcoloumns, and AddRoundKey. At the beginning of the encryption process, the input that has been copied into the state will undergo an AddRoundKey byte transformation. After that, the state will undergo transformation ofSubBytes, ShiftRows, Mixcoloumns, and AddRoundKey repeatedly as many as Nr. This process in the AES algorithm is called a round function. The last round is

somewhatdifferent from the previous rounds where in the last round, the state does not undergo a MixColumns, transformation.

3.2.2 AES Encryption Structure

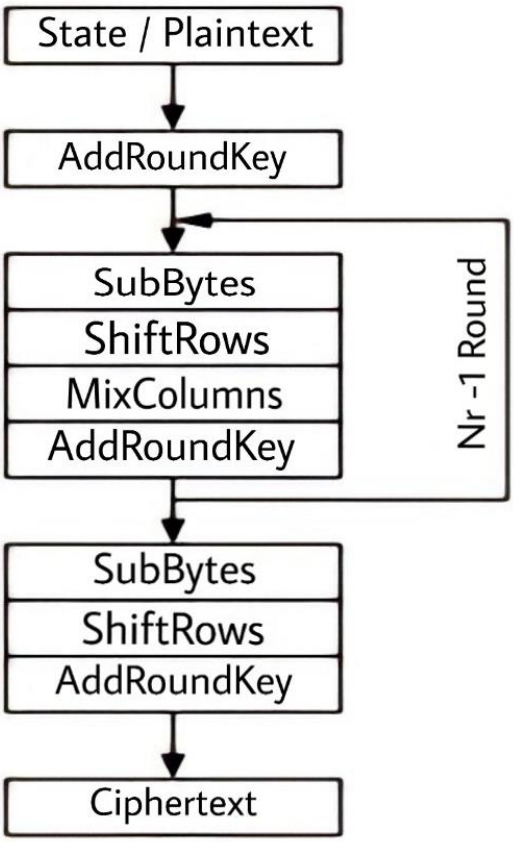

Figure 3.2 Encryption Process

The AES algorithm encryption process consists of 3 steps, namely:

1. Initial round, which is the process of copying the input into the state that will undergo the AddRoundKey transformation. AddRoundKey Transform: XOR between the initial state (plaintext) and the cipher key.
2. Process the round function as much as N r 1 times. The process for each round is as follows:
   - SubBytes: SubBytes is a byte transformation where each element in the state will be mapped using a substitution table (S-Box).
   - ShiftRows: Shiftrows transformation is basically a bit shift process where the leftmost bit will be moved to the rightmost bit (bit rotation).

- MixColumns: MixColumns operates on each element that is in a column in the state.AddRoundKey: XORs the current state with the round key.

3. Final round, which is the process for the last round. The last round is slightly different from the previous round, namely the state does not undergo a MixColumns transformation.

3.2.3 AES Decryption Structure

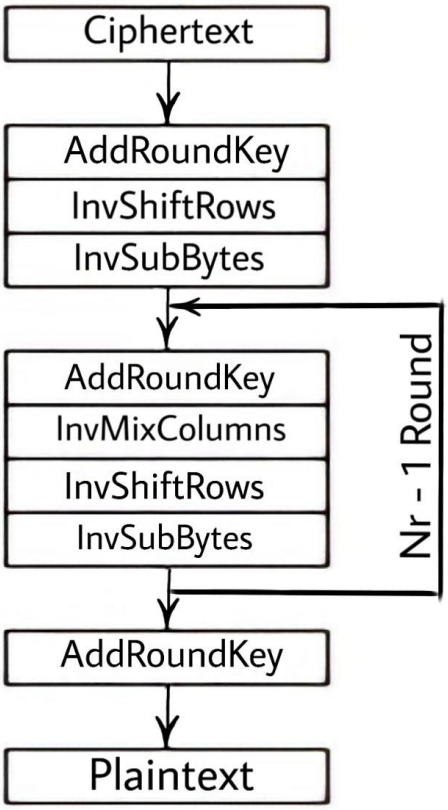

Figure 3.3 Decryption Process

In the encryption process that has been described previously, it is carried out to convert an original text (plaintext) into ciphertext using steps known as rounds. In the description process, there is a slight difference with the encryption process because basically this process will decrypt a ciphertext into the original text again (plaintext). The AES decryption algorithm uses an inverse transformation of all the basic transformations used in the AES encryption algorithm. So that in the basic transformation AES has an inverse, namely InvSubBytes, InvShiftRows and InvMixColumns.

- InvShiftRows : InvShiftRows is a byte transform as opposed to a ShiftRows transform. In the InvShiftRows transformation, the bit shift is performed to the right, while in the ShiftRows the bit shift is performed to the left.
- InvSubBytes : InvSubBytes is also a bytes transformation as opposed to a SubBytes transformation. In InvSubBytes, each element in the state is mapped using the Inverse S-Box table.
- InvMixColumns : InvMixColumns Each column in the state is multiplied by the multiplication matrix in AES.
- Inverse AddRounKey : The Inverse AddRounKey transformation is no different from the AddRoundkey transformation because in this transformation only a simple addition operation is performed with a bitwise XOR operation.

3.3 Hardware and Software Implementation of IoT

3.3.1 Tools

Before implementing the IoT device, there are several tools that must be prepared. The list of equipment used in this study will be written in table 3.1.

Tabel 3.1 Tools Needed

NO	Tools Name	Specification	Function	Total
1	Computer/ Laptop	Linux Mint 32/64bit	To create an application to be in hardware and software.	1 unit
2	Multitester	Analog/Digital	Used to measure voltage (ACV-DCV) and strong currents (mA-µA).	1 piece
3	Solderingiron	-	For attaching tin to components.	1 piece
4	Cable cutter	-	For cutting cables and component legs.	1 piece

3.3.2 Components

Before implementing the IoT device, there are several components that must be prepared. The list of components used in this study will be written in Table 3.2.

Tabel 3.2. Components

NO	Name	Function	Total
1	NodeMCU	As a process of orders that will be carried out.	1 unit
2	HC-SR04 Sensor	Used as input to data.	1 piece
3	Lead	Used as a series adhesive.	1 roll
4	Cable	Used as connect / jumper all components.	10 piece

3.3.3 Software

Before implementing the IoT device, severalsoftware were used. The list of components used in this study will be written in Table 3.3.

Tabel 3.3. Software

NO	Name Software	Function
1	Arduino IDE	This software functions as a text editor to create, edit and also validate the program codeof the microcontroller used.
2	Visual Studio Code	Code Editor used to build Web Server

3.4 Flowchart

Flowcharts are made aiming to make it easier to make programs. Flowchart is an illustration of program logic to be made. In figure 3.2. The flowchart of the program that will be made in this study will be displayed.

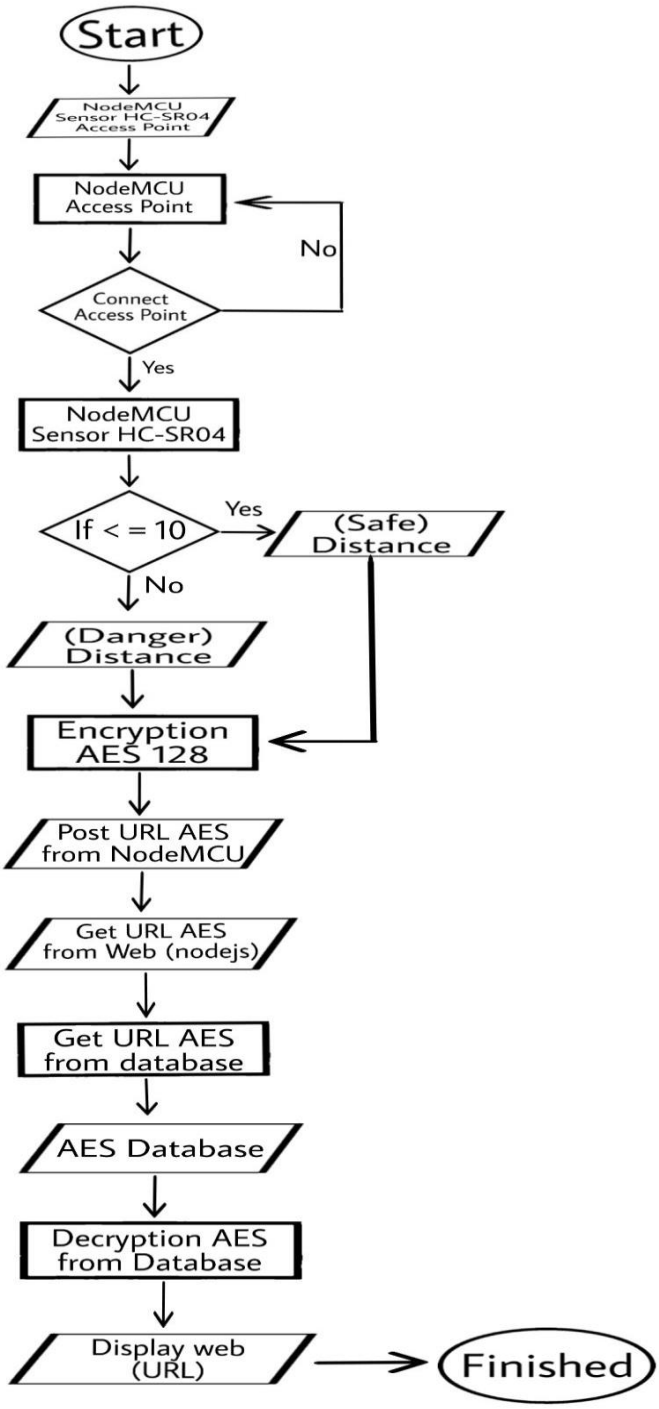

Figure 3.4 Flowchart

3.5 Research Flow

This research method will explain the research steps that will be carried out in building Internet of Things (IoT) Data Security Using AES Algorithm. As used in Figure 3.3.

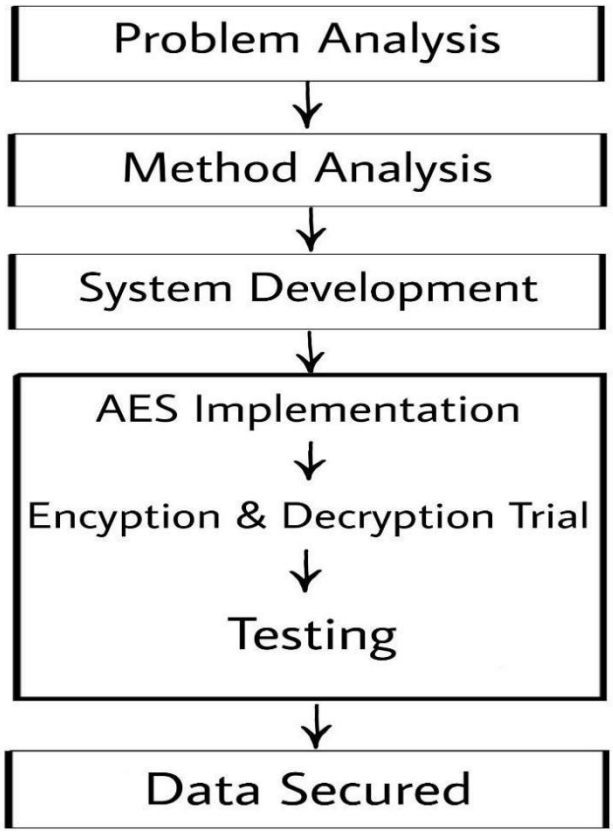

Figure 3.5. Research Flow

3.6 Literature Study

In this literature study section, it is a part to find thesis writing materials that are relevant to topics that can be obtained from books, journals and websites related to Internet of Things (IoT) Data Security Using AES Algorithm.

3.7 Problem Analysis

In Internet of Things (IoT) Data Security Using AES Algorithm we need to analyze what are the problems that occur to set goals for this research. This part of the problem analysis was carried out in the first week to the second week of May.

3.8 Analysis of Methods

Method analysis is one of the main things that must be done in Internet of Things (IoT) Data Security Using AES Algorithm. Method analysis is useful for determining the appa method that will be used in research. In this study the AES 128 algorithm was chosen as a method to secure data. The analysis of this method was carried out in the first week to the last week of May.

3.9 System Development

This stage is the stage of developing the IoT system. At this stage assembling the modules and coding so that the system can run so that it can obtain data that will later be used for the encryption and decryption process. The system development stage is carried out in the first week to the last week of June.

3.10 Implementation of the AES Algorithm

At the implementation stage of the AES algorithm, encryption and decryption of data are carried out, as previously mentioned, the encryption and decryption process uses the AES 128 bit algorithm with 10 rounds. This stage also includes testing the encryption and decryption whether it is running properly. After testing the next process is testing. The AES implementation process takes a long time starting from the fourth week of June to the third week of August.

3.11 System testing

After the design and implementation is done, the next step is testing the design that has been made. At this stage the results of the design that have been made will be tested such as response testing, encryption and decryption testing. This test aims to determine whether the data is encrypted.

3.12 Schedule of Activity Implementation

The schedule for carrying out activities is made to make it easier to work on tools and proposals, besides that it aims as a flow or guide so that the activity process is carried out in accordance with a predetermined schedule. The schedule of activities will be carried out as in table 3.4.

Table 3.4 Activity Planning Schedule

ACTIVITY	Mei				June				July				August			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Problem Analysis																
Method Analysis																
Chapter Writing 1,2,3																
System Development																
AES Implementation																
Encryption & Decryption Trial																
Testing																
Data Secure																
Chapter Writing 4,5																