CHAPTER 1

PRELIMINARY

1.1 Background

Internet of Things (IoT) is not new in this modern era. The rapid development of the Internet of Things has had an impact on both individuals, groups, business people, and professional workers [1]. IoT uses the internet as its connectivity so that it can provide real-time information without distance restrictions and without human intervention, or what is often called machine-to-machine communication [2].

Along with the rapid growth of the Internet of Things today, it is necessary to have a data security method on the Internet of Things. Without a data security method, of course, there is a risk that sensitive and valuable information can be accessed by inappropriate or illegal users. Which if this happens, it is likely to harm and even endanger the data owner, service owner, or even users related to the system. In addition, data accessed by inappropriate or illegal users may cause data to be damaged or lost.

Devices that are constantly connected and communicating with one another use different types of communication protocols. This protocol has the opportunity to cause data to be accessed by users who do not have access rights [1]. The IoT security method can be a solution in keeping data in a wide network channel so that data can still be accessed by users connected to the IoT service. So, to protect data on the Internet of Things, a security method is needed that can protect the data. The foundation of the IoT security method lies in control, data management, and IoT services.

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.

Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to synchronize data. The AES algorithm is a symmetric ciphertext block that can encrypt (encipher) and decrypt (decipher) information [3]. Encryption changes data that can no longer be read called ciphertext, conversely, decryption is changing the ciphertext data into its original form which we know as plaintext. The AES algorithm uses cryptographic keys 128, 192, and 256 bits to encrypt and decrypt data. The Advanced Encryption Standard is one of the most common methods of encrypting critical data, which has been used by major world organizations such as Apple and Microsoft to the NSA [4].

This study will propose an Internet of Things (IoT) data security method where the data to be secured is the data contained in the database server. This study also uses AES 128, where AES 128 uses 10 rounds to perform the encryption process [5]. AES 128 is suitable for encrypting data because it has a shorter processing time compared to AES 192 and AES 256. AES 128 also has a good level of security [25].

This study aims to model data security on IoT services and test data security methods. This study proposes an IoT data security method using the AES algorithm. This research was conducted using data obtained from the sensor.

1.2 Research Scope

Based on the results of the research that has been done, the scope of this research is:

1. This research uses a 128-bit AES algorithm with 10 rounds of encryption.
2. This research uses the same key for encryption and decryption.
3. This research uses NodeMCU as sensor data manager and data encryption.

1.3 Problem Formulation

Based on the journal "Arduino Due Based HCSR04 Ultrasonic Sensor for Altitude Monitoring System" [16], this journal aims to create a prototype digital distance measuring instrument based on the Arduino Due microcontroller using the HCSR04 sensor. The research method used is direct comparison test method and telemetry measurement. The measurement results are displayed in a computer device for easy reading. This design is controlled via Arduino Due. The results of testing the prototype tool can run well and can be accessed in real time.

The above research was built without any data security method, even though data security is very important for IoT devices, therefore the Internet of Things (IoT) Data Security Using AES Algorithm research proposes securing data obtained from the HC-SR04 sensor and designed using NodeMCU ESP2866. Data security uses AES 128 bit because it has a faster processing time compared to AES 192 and AES 256. AES 128 has 10 repetitions and has good security.

1.4 Research Objectives

1. Modeling data security on IoT services.

2. Propose IoT data security using AES algorithm.

3. Analysis IoT data security methods.

1.5 Analysis Benefits

1. Secure data on IoT service.

2. Describe data security by referring to the simulation results of data security on IoT.

1.6 Writing Systematics

Systematics of writing that is used in the task end is divided into a few basic topics, namely :

CHAPTER 1 INTRODUCTION

The chapter contains the background behind the problems, the formulation of the problem, the limit of the problem, the purpose of the research, and the benefits of research.

CHAPTER 2 LITERATURE REVIEW

Chapter is contained on the theory - a theory that is associated with the "Internet of Things (IOT) Data Security Using AES Algorithm".

CHAPTER 3 RESEARCH METHODOLOGY

Methods of research, the chapter is to explain the methods that are used in the design as well as the measures that are used to secure the Internet of Things (IOT) Data Security Using AES Algorithm.

CHAPTER 4 RESULTS AND DISCUSSION

Chapter This contains about implementation work flow, analysis and discussion o f the grooves are designed.

CHAPTER 5 CONCLUSIONS AND SUGGESTIONS

Chapter This contains the conclusion of the testing system as well as advice whether the research it can be used as appropriate and developed.

REFERENCES