CHAPTER 1
INTRODUCTION

1.1 Background

Computer security is a very important thing. Apart from the sophistication of the features contained in the computer, the security of the system is also very influential in the use of several features and applications that exist on the computer. This makes security a necessity for every application on the computer. There are many sides that must be considered in securing an application, one of which is on the communication path or also called the API. API (Application Programming Interface) is a set of advance tools that developers can use to integrate two parts of an application. The purpose of creating this API itself is to accelerate the creation and development of an application because it allows developers to access the features of the platform. The API form itself can be function, method, or URL endpoint. Web service / API is divided into two types, Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). REST represents that each unique URL is an object; the object of the content can be obtained using HTTP GET, and can be modify by using the POST, PUT, or DELETE method. For the security, because REST using HTTP or HTTPS the REST administrator (firewall) can see the intent of each message by analyzing the HTTP commands used in the request. The authentication and authorization from REST itself assumes that these affairs have been supported by the web server. SOAP is a structured message exchange protocol in the implementation of web services and using Extensible Markup Language (XML). SOAP requests use POST commands for certain services. The SOAP command itself is a resource-consuming command, where all request contents cannot be detected by most firewall. Security does not escape the term called cryptography. There are many applications where the service security system is still lacking. For example applications that send personal data but do not have authentication on the service, so other users can access the service.

Referring to the previous paragraph, this project discusses the solution of the authentication security problem. By utilizing JWT feature for authentication problems combined with the AES encryption method on the messages sent will be able to increase the level of security of the services made.

This method is expected to improve the security of a service security system. So the services made are not vulnerable to intruders.

1.2 Problem Formulation

The main focuses of the problem in this project are:

1. How JWT work in securing web services?
2. How encryption method works to protect the data from intruders?
3. How the performance of a service in dealing with many requests?

1.3 Scope

The limitations involved in this project is that the server is using local server, and this project only focuses on the web service part, so it doesn't take care of the UI/ front end parts and the network security.

1.4 Objective

The goal of this project is to analyze the performance of the service provided and compare the result of the response time that comes out when using encryption method. Also provide conclusions about the security system design of the web services.