CHAPTER 4
ANALYSIS AND DESIGN

4.1 Analysis

This chapter provides an explanation of the problem being solved. The difference with the previous chapter is that here will be given a detailed explanation of why using or running the methods and tools that will be used.

The database used in this project is using Elasticsearch. The initial focus on the service made is searching; therefore Elasticsearch is an option because it is a highly scalable open-source full-text search and analytics engine. So that it will be faster in the searching process and also based on restful.

For authentication using JSON Web Token. JWT is used to authenticate the REST API, so that not all users can access the rest freely. By using this JWT, the user does not need to go to the authorization server because the user is already registered and has a private key.

The message sending method is also added with AES method. So if the service is sent, the recipient must also have the same key on the server to decrypt the message. This project using AES method because of its flexibility in encrypting a plain text and also the messages sent in the form of JSON. The key used in this AES method is a long-term key. So between the server and application has a key agreement.

4.2 Design

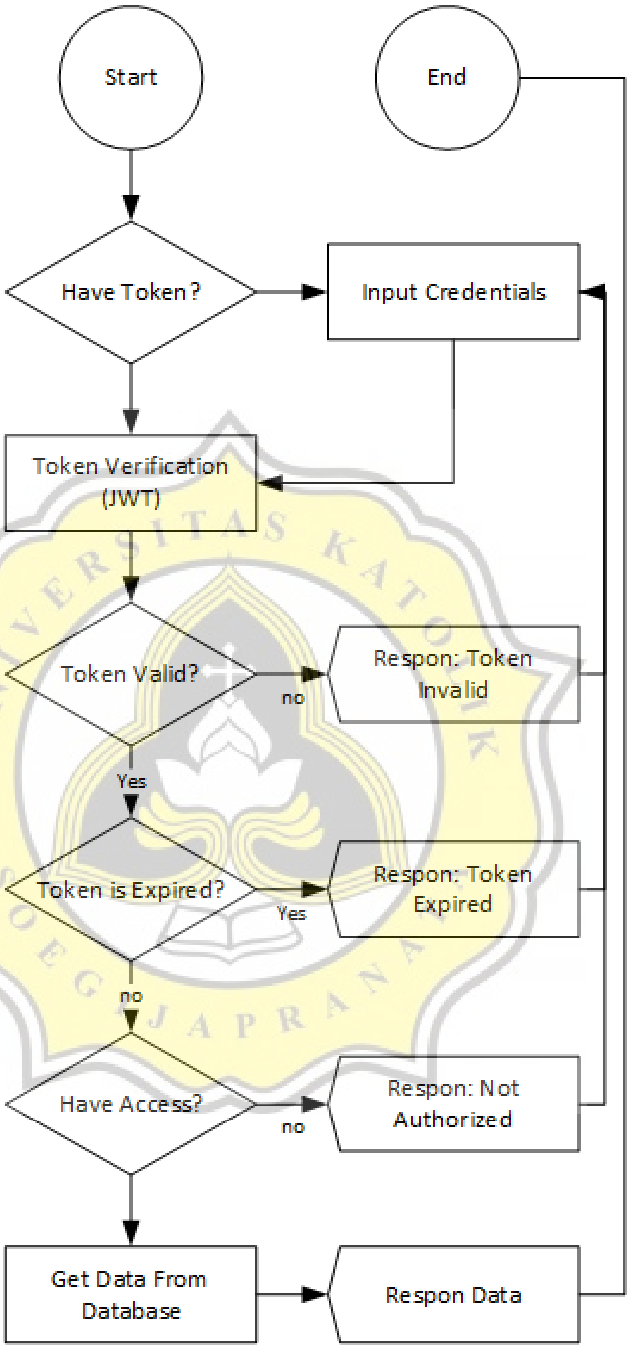

Illustration 4.1 JWT Flowchart

The illustration above explains how JWT performs the authentication of a user account while accessing the service. Checked tokens cannot be arbitrary tokens. Even though the token is not expired and the user is registered, the accessibility of that user is also checked, so that the level of each user is also detected.

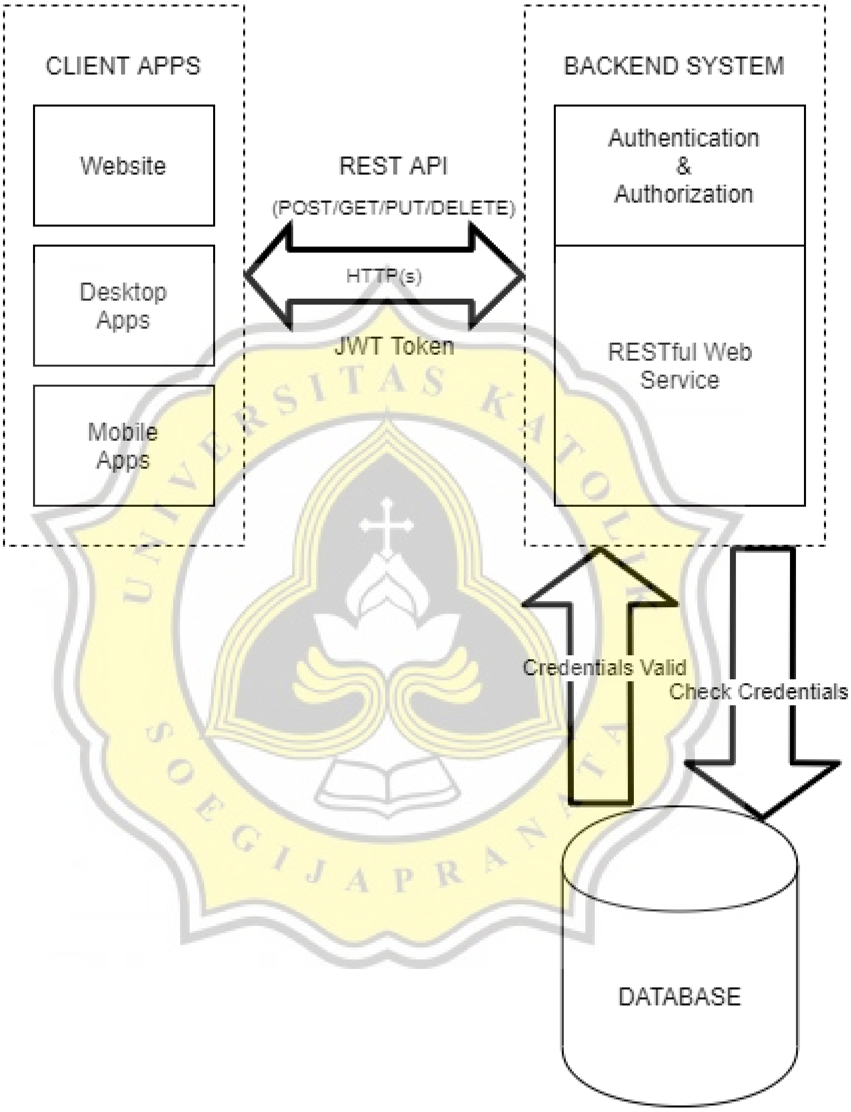

Illustration 4.2 Application of JWT on RESTFUL web service architecture

The illustration above shows the process of the journey in the rest architecture service. Requests that enter the service are checked for authentication and authorization from that user. After succeeding the next service will check the credentials or IDs of users who request to be registered in the database.

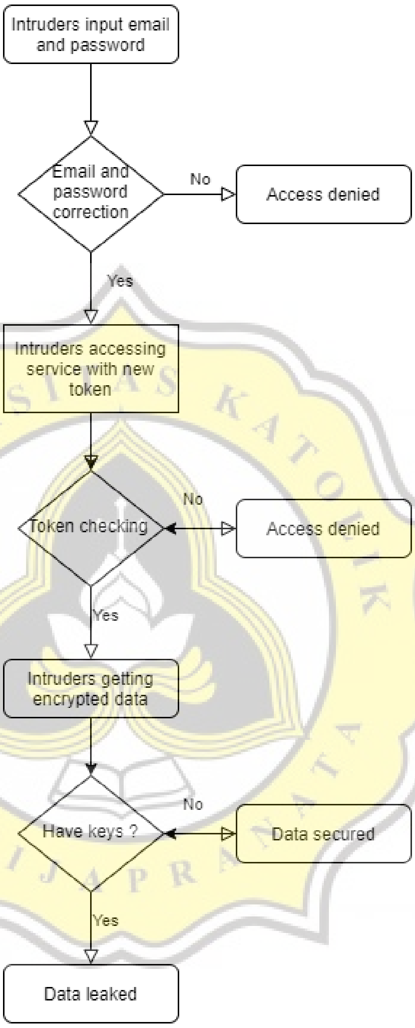
Intruders input email and password
Email and password correction
No
Access denied
Yes
Intruders accessing service with new token
Token checking
No
Access denied
Yes
Intruders getting encrypted data
Have keys ?
No
Data secured
Yes
Data leaked

Illustration 4.3 Intruders Testing Flowchart.

Here is the illustration for intruder testing. When the intruders get email and password accidentally, they will get tokens for accessing the services. The data from login will be obtained and use it for accessing another services. With tokens obtained together with the data sent from login services, then the things needed for accessing the services are fulfilled. After intruders accessing the services, they will get the data returned form the server. But the data has been encrypted with AES method and can only be decrypted with the same key that has been set.