ISSN :2721-6683
ESSN :2721-6675

Development Authentication and Authorization Systems of Multi Information Systems Based REst API and Auth Token

Indra Gita Anugrah, Muhamad Aldi Rifai Imam Fakhruddin
Dept of Informatics Engineering, Faculty of Engineering, Universitas Muhammadiyah Gresik
indragitaanugrah@umg.ac.id

ABSTRAK

Keamanan sebuah aplikasi merupakan permasalahan terpenting dalam sebuah proses integrasi sistem informasi. Proses authentication dan authorization biasanya dilakukan menggunakan Single Sign On (SSO). Metode authentication dan authorization digunakan untuk mengamankan data dalam sebuah sistem. Proses authentication dan authorization dilakukan pada sisi client (web browser) berupa session dan sisi server (web server) berupa cookie. Session dan cookie merupakan harta yang berharga dalam proses authentication dan authorization karena berisi data yang diperlukan dalam proses login sehingga session dan cookie perlu diamankan. Session merupakan data kombinasi dari username dan password yang telah dilakukan proses enkripsi sedangkan cookie menyimpan data informasi login agar tetap dalam keadaan memperoleh akses sesuai dengan privilege yang telah diberikan kepada user. Begitu pentingnya peranan session dan cookie dalam proses authentication dan authorization sehingga diperlukan sebuah cara untuk mengamankan data pada session dan cookie. Salah satu cara mengamankan data adalah menggunakan REst API dan Auth Token.

Kata Kunci: *REst, API, Token, Enkripsi, Single Sign On*

ABSTRACT

The security of an application is the most important problem in an information system integration process. The authentication and authorization process is usually carried out using Single Sign On (SSO). Authentication and authorization methods are used to secure data in a system. The authentication and authorization processes are carried out on the client side (web browser) in the form of a session and on the server side (web server) in the form of cookies. Sessions and cookies are valuable assets in the authentication and authorization process because they contain the data required for the login process so that the session and cookies need to be secured. Session is a combination of username and password data that has been encrypted while cookies store login information data so that they are still in a state of gaining access according to the privileges given to the user. So important is the role of sessions and cookies in the authentication and authorization process, so we need a way to secure data on sessions and cookies. One way to secure data is to use the REst API and Auth Token.

Keywords: *REst, API, Token, Encrytion, Single Sign On*

INTRODUCTION

The development of website technology today also affects application development by agencies or organizations. As an organization develops, the need for application development to support performance is usually done in stages and separately. The more applications that are developed independently, the greater the challenges in the integration process. One of the biggest challenges in the system integration process is during the login process. When

logging in, a system requires a process that requires authentication and authorization. The authentication process itself is a process to check the correctness of a data, in this case the data is in the form of a user and will then proceed to the authorization process which is the process of determining whether the user has permission to enter the system or not. In the information system integration process, the user authentication process uses Single Sign On (SSO) where the retrieval of user data or user properties is carried out for the benefit of several systems, this is also called "central authority".

The authentication and authorization processes are carried out on the client side (web browser) in the form of a session and on the server side (web server) in the form of cookies. Sessions and cookies are valuable assets in the authentication and authorization process because they contain the data required for the login process so that the session and cookies need to be secured. Session is a combination of username and password data that has been encrypted while cookies store login information data so that they are still in a state of gaining access according to the privileges given to the user. So important is the role of sessions and cookies in the authentication and authorization process, so we need a way to secure data on sessions and cookies. One way to secure data is to use the REst API and Auth Token.

LITERATURE REVIEW

REst dan API

Today's data exchange plays an important role in the integration of a system, API (Application Programming Interface) is a collection of

```
[
  {
        "id"          : "0123456",
        "user"        : "jokosantosa"
  },
  {
        "id"          : "9876543",
        "user"        : "yanuaradi"
   }
]
```

Figure. 2, XML or JSON Representation

statements in the form of interfaces that contain commands for applications to interact with other applications this collection of statements is stored in the form of a library. Easier API is a link that allows applications to communicate with each other and exchange data. REst (Representational State Transfer) is a type of API. The protocol that underlies data communication on REST (REpresentational State Transfer) generally uses Hypertext Transfer Protocol (HTTP) using XML or JSON format as its representation. In REST, the interaction between the client and the server is carried out using unique Universal Resource Identifiers (URIs) with several operational types (Lee, H.M. et al. 2013) and (Rahman, M.A. et al. 2013).

The way the REst API works is done where the server side provides data or resources while on the client side makes an HTTP request (Sinha, R. et al. 2014) and (Zhou, W. et al. 2014), to the server with a URL or Global ID, then the server will respond and send back the HTTP requested by the client as shown in Figure 1. The data on the REst API is represented in the form of objects and arrays. The Representation of objects and arrays in

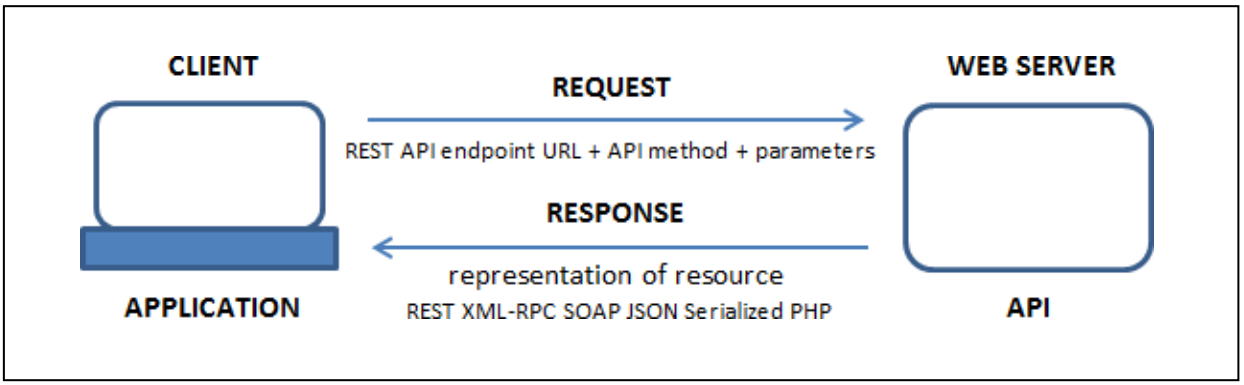

Figure. 1, API REst Overview Method

the REst API is usually in XML or JSON format as shown in Figure. 2 so that the information received is easier to use by the client. Usually REst is used in resource-oriented applications, for example in the use of web service (Prüter, S. et al. 2008). The purpose of resource-oriented is the provision of resources as a service, not a collection that manages resources in an application.

Client – Server

Information systems are built in a technology architecture, some of which are centralized, decentralized and client/server technology architectures. Client-server architecture is a form of architecture, client is a device that receives, displays and runs applications (computer software) while the server is a device that provides and acts as a manager of applications (Chen, M. et al. 2005), data, and security. A server is a computer that serves requests from clients, so it requires specially designed specifications that have specifications with large capacity and high performance. In its working system, it will receive requests, then process them and send back responses according to requests. For that, the device needed is a computer with a large capacity and high performance. This is because the server may receive multiple requests at the same time.

Authentication and Authorization

One of the challenges in information system development is the security mechanism when the user logs in. System developers are faced with several options for authentication scenarios during the login process. Authentication is a way to identify the user when logging in. Login requests usually consist of a username and password. Registered users will be allowed to access the requested page or function. After that the security process is continued with authorization. This process is intended to check the access rights of a user.

The authentication and authorization process on a web-based system involves Hyper Text Transfer Protocol (HTTP) headers and error messages where this process starts when the web

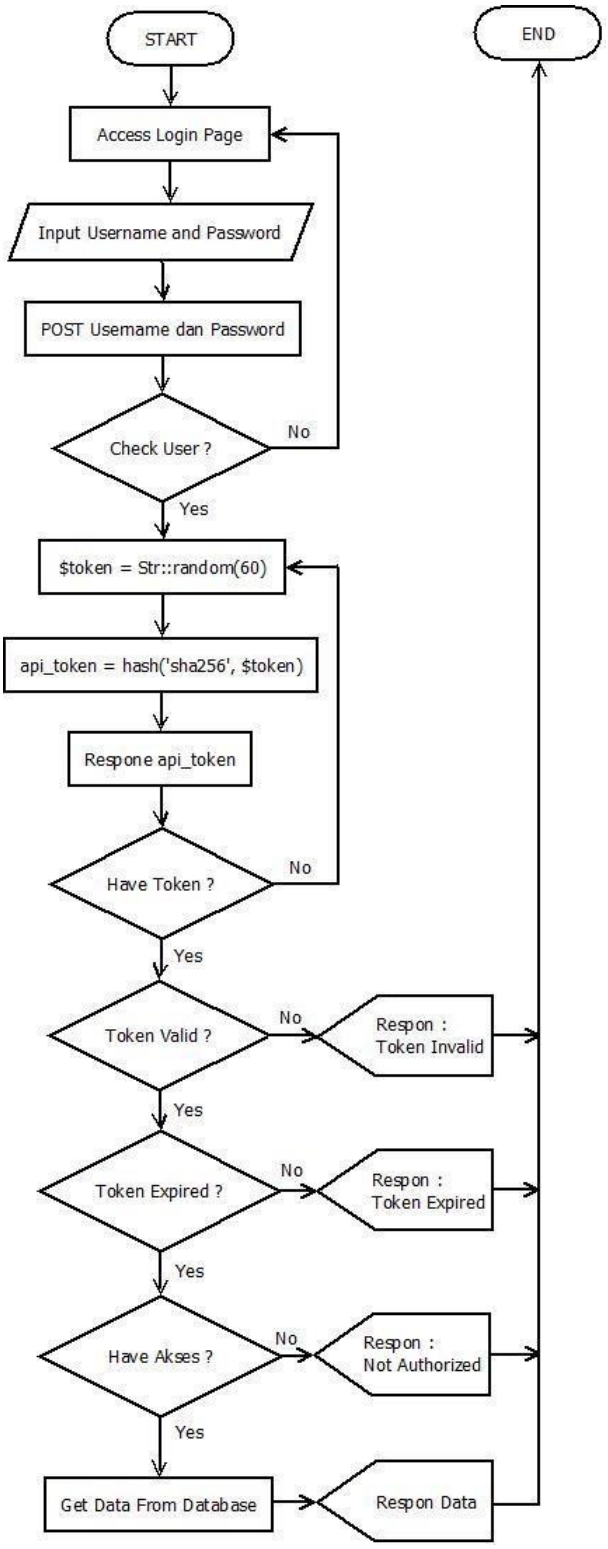

Figure. 3, Flow authorization with Token

browser makes a request such as HTTP-GET which will then be responded to by the Web server, until the web server provides user authentification and authorization. valid to access

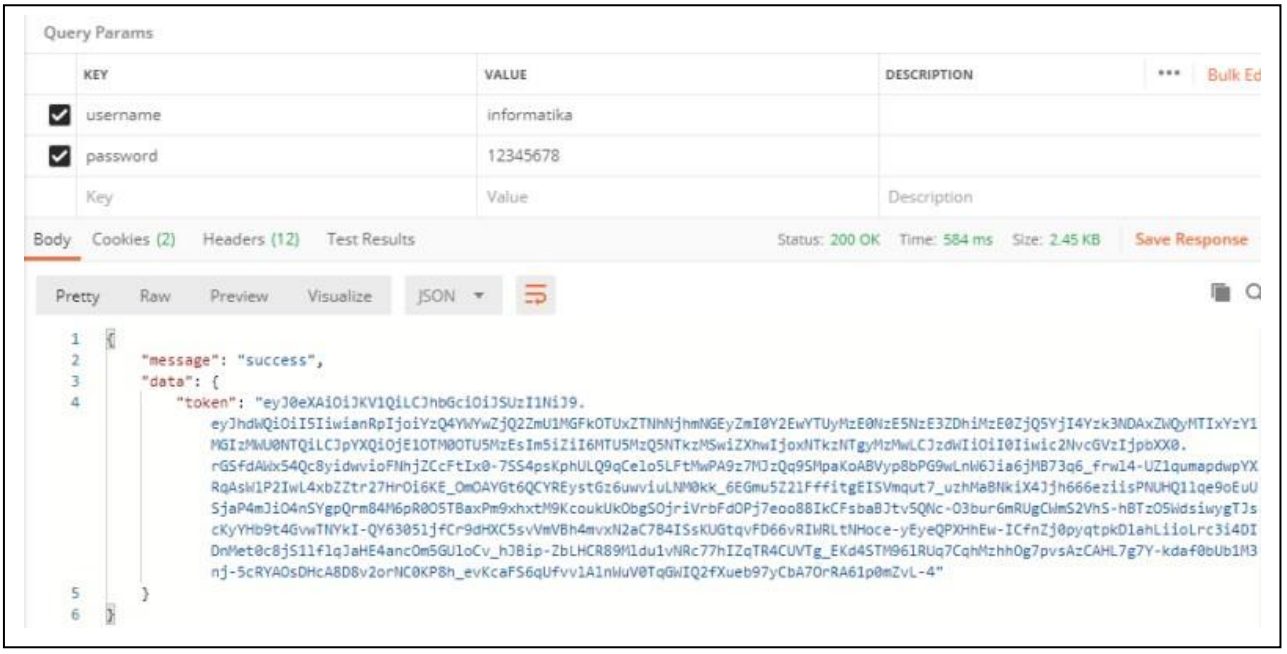

Figure. 4, Token Representation on Postman REst Client Application

the page according to the privileges that have been given.

Single Sign On

Single Sign On is a type or method of authentication performed by the user by doing it only once. Single Sign On can also be referred to as "central authority". Single Sign On is effectively carried out in an integrated system which is a combination of several Information Systems. Proper authentication and authorization methods are required by organizations to secure data, prevent identity theft and unauthorized access.

METHODE

The research method is carried out based on problem analysis of the problems found. First, the analysis of the formation of the access token is formed, the second is the analysis of the validation flow that explains the validation of the request for each request before the data is given, the third is the analysis of the request and response of the web service request. In this authentication and authorization system, the user will be given two checks, the first checking is about the authentication data username and password for checking and the second is the authorization token to access the application.

The generated token uses a 60-character scramble for the alphabet, then the encryption process is carried out using the sha256 method for cryptographic security. To pass token data To pass token data between applications, an API (Application Programming Interface) is used. This API can know the user's access rights to an application, if the user has valid access rights, the user can access the application according to their access rights. The process flow in the Development Authentication and Authorization Systems of Multi Information Systems Based REst API and Auth Token can be seen in Figure 3. In this implementation phase to test the API (Application Programming Interface) the Postman REst Client software is used, Postman has a function as a REst Client or an application used to test the Rest API that has been created.

To implement Authentication and Authorization Systems of Multi Information Systems Based REst API and Auth Token, some software and hardware are used as follows:

- Processor Intel (R) Core (TM) i5 @ 2.7 Ghz.
- Memory (RAM) 4 GB.
- System type 64 bit Operating System.
- Laravel 7 Framework.
- PHP 7.
- Tools Postman REst Client.

RESULT AND DISCUSSION

In this implementation phase, to test the API (Application Programming Interface) the Postman REst Client software is used, Postman has a function as a REst Client or an application used to test the Rest API that has been created.

There are two processes carried out at Postman, namely POST and GET. POST to send parameters in the form of a valid username and password to generate a token (Ahmadi, R. et al. 2016). This token serves as a key to gain access to make further requests. The GET process is carried out by entering the key or token that has been obtained during the POST process to obtain the desired data.

In Figure. 4 is a trial to log in using the POST method on the API using the Postman REst client application, when the user successfully logs in, a token will be generated as described in Figure 3. After the token is successfully regenerated, the token code will be used as a session used to store the login session on initial application and cookies used for validation on other applications. The use of login sessions on the user will then be applied to the single sign on method in several integrated applications.

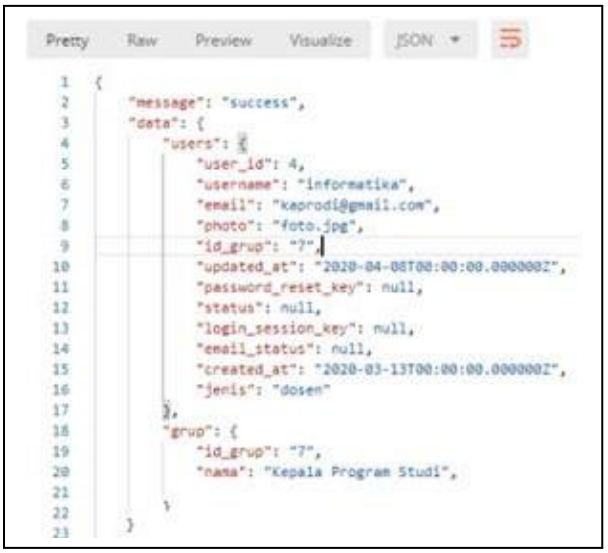

Figure. 5, User's access variable

To access the API login page using the POST method, a username and password is required. By using this method, the authentication and user authorization processes will be carried out in accordance with the access rights that have been previously set. After the user gets authorization, some data or variables will be taken. What is required by the system to impose restrictions on users as shown in Figure 5.When login fails or incorrectly enters the username and password, the response from api will display an error information as shown in Figure 6.

CONCLUSION

From the research experiments above, the authentication system using REst API and Auth Token is able to meet the security needs of an integrated Information System. REst API and Auth

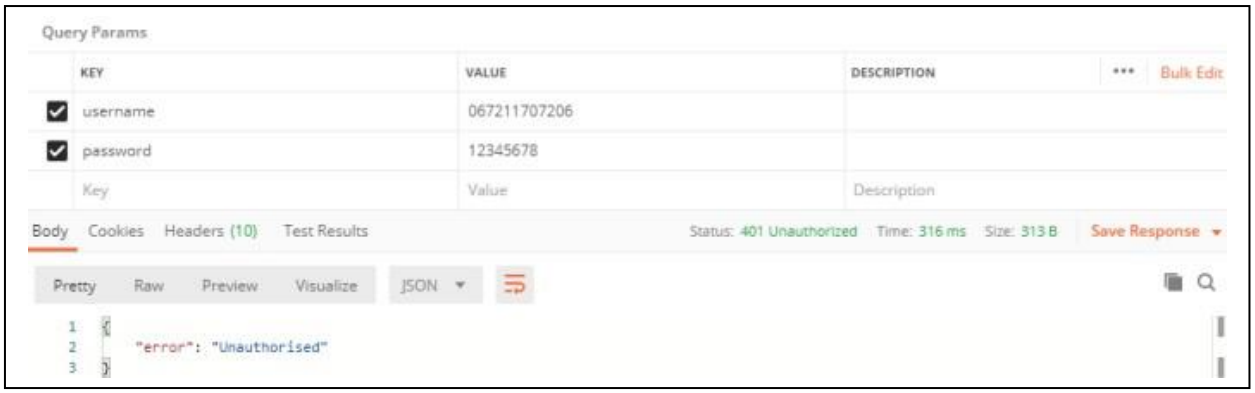

Figure. 6, User Unauthorized Notification

Token based security methods can cover security holes in authentication systems that use sessions and cookies. This is because the authentication method genreates using a method by randomizing the letters of the alphabet along 60 characters, then the encryption process is carried out using the sha256 method for cryptographic security.

REFERENCES

Ahmadi, R., Heidari, E. and Zand, M. (2016). Security Enhancement for Restful Web Services. Journal of Fundamental and Applied Sciences, 8(2S), pp. 2804-2817.

Chen, M., Zhang, D. and Zhou, L. (2005). Providing web services to mobile users. International Journal of Mobile Communications, 3(1), pp. 1-18.

Kurniawan, Y.K., Oslan, Y. and Kristanto, H. (2013). Implementasi REST-API Untuk Portal Akademik UKDW Berbasis Android. Jurnal Eksplorasi Karya Sistem Informasi dan Sains, 6(2), pp. 29-40.

Lee, H.M. and Mehta, M.R. (2013). Defense against REST - based web service attacks for enterprise systems. Communications of the IIMA, 13(1), pp. 57-68.

Prüter, S., Moritz, G., Zeeb, E., Salomon, R., Golatowski, F. and Timmermann, D. (2008). Applicability of web service technologies to reach real time capabilities. Object Oriented Real-Time Distributed Computing (ISORC), 11th IEEE International Symposium, pp. 229-233.

Rahman, M.A., Kuswardayan, I. and Hariadi, R.R. (2013). Perancangan dan Implementasi RESTful Web Service untuk Game Sosial Food Merchant Saga pada Perangkat Android. Teknik Informatika ITS, 1(2), pp. 1-4.

Sinha, R., Khatkar, M. and Gupta, S.C., Design & Development of a REST based Web Service Platform for Applications Integration on Cloud. International Journal of Innovative Science, Engineering and Technology, 1(7), pp.385-389.

Zhou, W., Li, L., Luo, M. and Chou, W. (2014). REST API design patterns for SDN northbound API. In Advanced Information Networking and Applications Workshops (WAINA), 28th IEEE International Conference. pp. 358-365.