Journal of Applied Data Sciences
Vol. 3, No. 1, January 2022, pp. 33-43

ISSN 2723-6471

SHA-512 Algorithm on Json Web Token for Restful Web Service-Based Authentication

Naufal Rasyada [1,*]

[1] Universitas Amikom Purwokerto, Indonesia
[1] rasyada321@gmail.com*
* corresponding author

(Received: November 12, 2021; Revised: December 22, 2021; Accepted: January 7, 2022; Available online: January 25, 2022)

Abstract

The development of technology is getting faster and continues to grow so as to create various types of technology, architecture, to new programming languages. Surely this will be a new problem because of differences in technology, programming language, and architecture that must still be able to provide interconnected sources of information. So in order for the system to remain integrated, a Web Service (WS) is needed as a bridge in integrating between systems without differentiating the platform, programming language, or architecture used. One of the Web Service architectures that is widely used is REST (REpresentational State Transfer), but there will be problems in implementing REST Web Service because it does not have security standards in the authentication process. Then an authentication method is needed, namely JSON Web Token (JWT). In implementing JWT, a hash algorithm is needed, such as SHA-512. The results of this study indicate that the use of SHA-512 on the JWT has a good speed with an average data request speed of 512.8 milliseconds (ms) when compared to the SHA-256 algorithm which has an average data request speed of 515.55 MS. Meanwhile, in terms of data size, SHA-512 produces an average data request size of 0.75 kilobytes (kb) compared to SHA-256 which has an average data request size of 0.72 kb.

Keywords: Authentication; SHA-512 Algorithm; Web Service; REST API; JSON Web Token

1. Introduction

With the increasingly widespread development of technology, the need for information exchange is very rapid [1]. To provide information exchange facilities between two or more applications, it is necessary to have an API (Application Programming Interface) web service [2]. Web service is a standard and programming method for sharing data between different applications, distributing services using the internet to support information exchange [3]. The current trending web service architecture is such as Representational State Transfer (REST).

The results show that RESTful Web Service has a good performance [4]. However, REST does not have a standard for authentication in data access policies on the server side, so that anyone can access, modify, view, and delete data on the server [2]. With these problems, token-based authentication is used, namely using JSON Web Token (JWT) [5]. JSON Web Token is a concise URL (Uniform Resource Locators) representation tool to represent claims that will be forwarded between client and server [6].

One of the algorithms used in JWT is SHA (Secure Hash Algorithm). SHA is a hash function created by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard (FIPS). There are studies that have been carried out by applying the SHA-256 algorithm for JSON WEB TOKEN but it is very commonly used [7].

By referring to previous research, this study aims to apply the SHA-512 algorithm to JSON Web Token based on RESTful Web Service in application login authentication. This research is reinforced by the results of a study which

states that the SHA-512 algorithm has better performance than SHA-256 [8]. So in this study, we will discuss the SHA-512 algorithm on JSON Web Token for system authentication in RESTful Web Service architecture.

2. Literature Review

2.1. Secure Hash Algorithm (SHA)

The Security Hash Algorithm (SHA) is a one-way hash function designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard (FIPS) in 1993 and referred to as SHA-0. two years later published the next generation SHA 1 which is an improvement of the SHA-0 algorithm. In 2002, four other variations were published, namely SHA-224, SHA-256, SHA-384, and SHA-512, all four of which were referred to as SHA-2 [10]. The SHA-512 algorithm is an algorithm that uses a one-way hash function created by Ron Rivest. This algorithm is a development of the previous algorithms, namely the SHA-0, SHA-1, SHA-256 and SHA-384 algorithms. The way the SHA-512 algorithm cryptography works is to accept input in the form of messages of arbitrary size and produce a message digest that has a length of 512 bits [9].

2.2. JSON Web Token (JWT)

JSON Web Token (JWT) is a standard format for securing personal information into a claim that will be encoded into JSON form and become the payload of the JSON Web Signature. Claims can be protected with a digital signature such as a Message authentication code (MAC) or encrypted. JWT is a token in the form of a string consisting of three parts, namely: header, payload and signature which are used for authentication and information exchange [6].

```
xxxxxx.yyyyyyy.zzzzzzzzz
header.payload.signature
```

Figure. 1. JSON Web Token Concept

2.3. REST API Web Service

Web Service (WS) is software designed to support interoperability of device-to-device interaction in a network [11]. There are several types of web service architectures that are often used, such as Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) [4].

3. Methodology

3.1. Method of collecting data

a. Observation

Observation is an expression term which is written or spoken related to a systematic review, observation, and recording in an object based on what is seen, felt and heard [12]. In this study, researchers made observations by observing the process of a running web service.

b. Literature review

Literature study is data collection by looking at data sources such as reference books, articles, and scientific journals [13]. At this stage, the research is carried out by understanding and studying books, reading journals from various sources related to research plus guide books as a reference in making this research.

3.2. Implementation

a. Application Design

ISSN 2723-6471

In the early stages of this research, application design was carried out such as an overview of the running system and an overview of the main appearance of the application.

b. Application Implementation

The design that has been made is then implemented using the javascript programming language.

c. Writing JSON Web Token Function with SHA-512 Algorithm

At this stage, the JSON Web Token (JWT) function is written in the application by applying the SHA-512 algorithm.

d. Test

The test was conducted to see the performance of the SHA-512 algorithm on the JSON Web Token (JWT).

e. Result Analysis

At this stage, the test results are analyzed to get the results.

4. Results and Discussion

4.1. Application Design

In the early stages of this research, application design was carried out such as an overview of the running system and an overview of the main appearance of the application. There are several menus that can be used to send, view, modify, and delete data. The following is the design of the login page as shown in Figure 2.

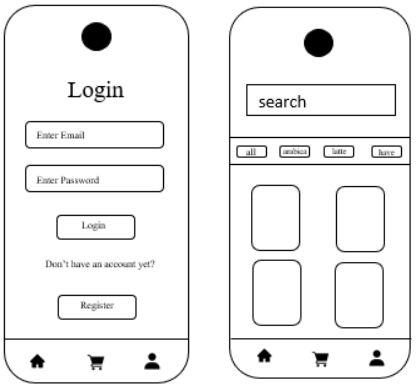

Figure. 2. Application Login and Main Page Design

While the design display on the user dashboard in accessing this application is as shown in Figure 2.

4.2. Application Implementation

The design that has been made is then implemented using the javascript programming language. The steps taken are to create a login page for user authentication by implementing a JSON Web Token with the SHA-512 algorithm as shown in Figure 3.

ISSN 2723-6471

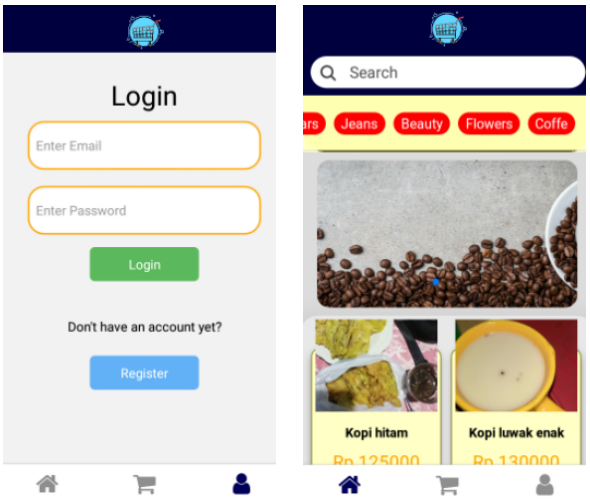

Figure. 3. Application Login Display and main application page

Next is the main page of the application, if the user successfully enters valid credentials then the user will be redirected to the main page of the application as shown in figure 3.

4.3. Writing JSON Web Token Function with SHA-512 Algorithm

At this stage, the JSON Web Token (JWT) function is written in the application by applying the SHA-512 algorithm. The flowchart of the application is described as follows.

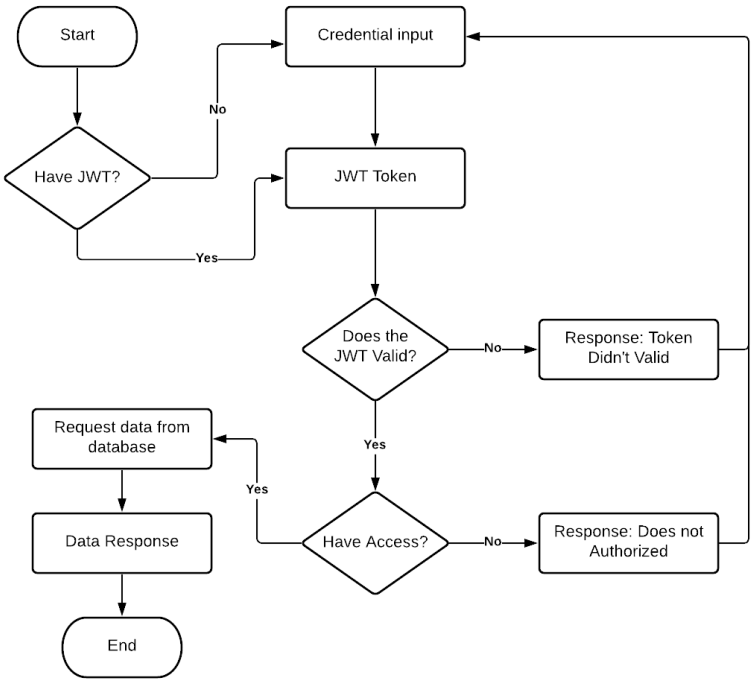

Figure. 4. JWT Authentication Flowchart

In Figure 4 is the flowchart of the application. The flow is the system will check whether the user has a token or not, if not then the user will be redirected to the login page, the user inputs the credentials to get the token, if the credentials are valid then the token will be obtained. Otherwise, the user will be redirected back to the login page.

Furthermore, the token will be used to request data, if the token is valid, then the requested request will be sent to the user.

4.4. Testing

At this stage, which is conducting a resource test, the result is that the application service will respond from the server if the resource is available and can be seen. This test is used to see the speed and size of the token used when testing.

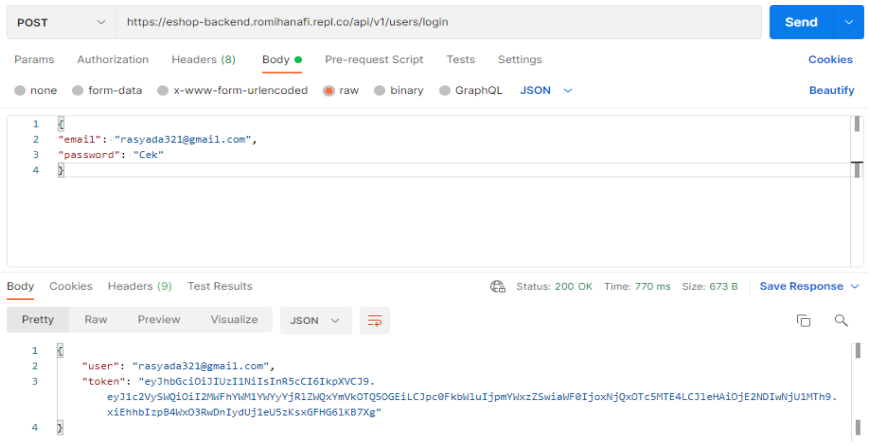

Figure. 5. POST Request with SHA-256

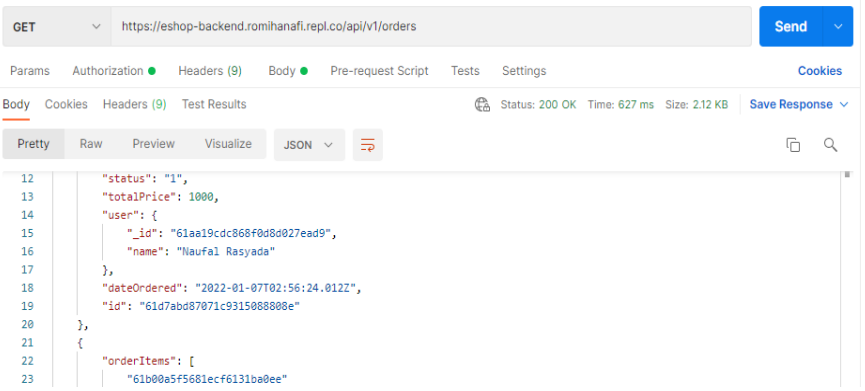

Figure. 6. GET Request with SHA-256

In Figure 5 a POST login request is made using a JSON Web Token with the SHA-256 algorithm, with a time of 770 ms and a size of 673 bytes, and in Figure 6 a GET request is made which results in a time of 627 ms with a size of 2.12 kb. The response of the resource request was successful with OK status.

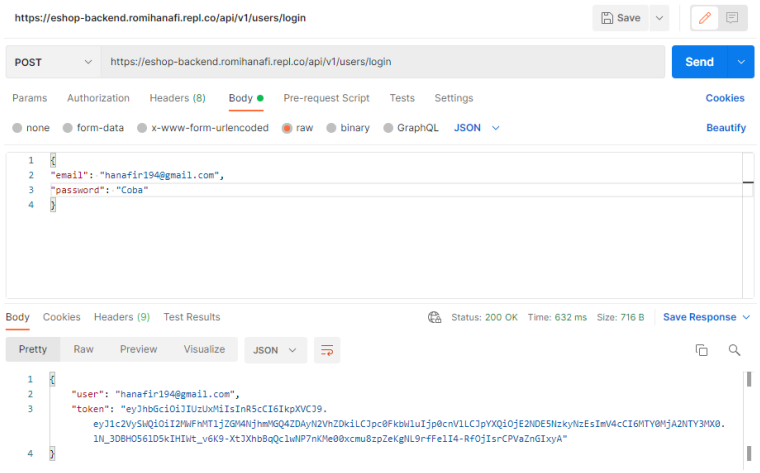

Figure. 7. POST Request with SHA-512

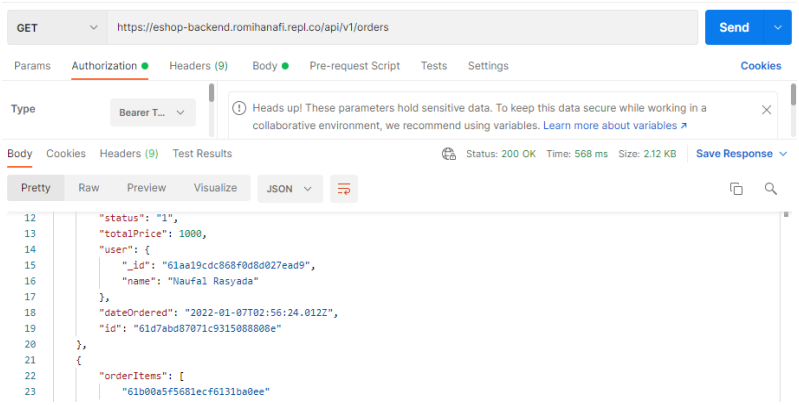

Figure. 8. GET Requests with SHA-512

In Figure 7, a POST login request is made using a JSON Web Token with the SHA-512 algorithm, with a time of 632 ms and a size of 716 bytes, and in Figure 8 a GET request is made which results in a time of 568 ms with a size of 2.12 kb. The response of the resource request was successful with OK status.

4.5. Result Analysis

At this stage, an analysis of the algorithm used in the JSON Web Token is carried out to determine its performance. After the test is carried out using postman by making comparisons between the algorithms used in the JSON Web Token. As a comparison, the SHA-256 algorithm has been widely used in the application of JSON Web Tokens. The following are the results of testing the JSON Web Token (JWT) with the SHA-256 and SHA-512 algorithms on the Representational State Transfer (REST) architecture. Below table 1 the results of Performance Comparison of SHA-256 & SHA-512.

Table. 1. Performance Comparison of SHA-256 & SHA-512

Test	Performance (ms)	
	SHA-256	SHA-512
1	328	322

2	350	348
3	354	351
4	361	359
5	382	379
6	385	382
7	389	387
8	391	389
9	412	410
10	420	417
11	432	429
12	516	514
13	518	516
14	523	520
15	540	539
16	554	550
17	612	610
18	616	614
19	712	709
20	1516	1511
Average	**515,55**	**512,8**

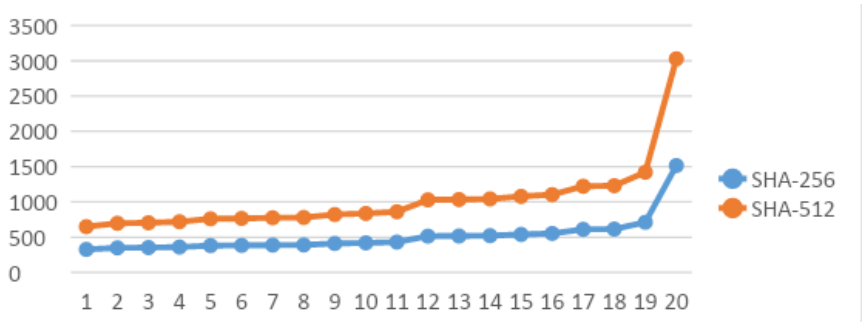

Figure. 9. Performance Graph of SHA-256 & SHA-512 Algoritma Algorithm

Based on the results in figure 9 above of the tests that have been carried out, the average performance of the JSON Web Token on the SHA-256 and SHA-512 algorithms is obtained. The average speed obtained in the SHA-256 algorithm is 515.55.2 milliseconds, and the SHA-512 algorithm is 512.8 milliseconds. The following is a comparison graph of the SHA-256 and SHA-512 algorithms. The performance of using SHA-256 on JSON Web Token has results from 20 trials showing the lowest request is at 328 m/s and the highest is 1516 m/s. While the performance of using SHA-512 indicated by the red line has the lowest request result at 322 m/s and the highest is 1511 m/s. Thus these results indicate that SHA-512 is faster than SHA-256 in the authentication process on the application. Next, an analysis is carried out to determine the size of each JSON Web Token (JWT) on the SHA-256 and SHA-512 algorithms, along with the results of the analysis of the JSON Web Token in terms of size in the RESTful Web

ISSN 2723-6471

service architect. Below table 2 results of Size Comparison of JWT SHA-256 & SHA-512. Figure 10 shows the result of a graph of data size on SHA-256 & SHA-512.

Table. 2. Size Comparison of JWT SHA-256 & SHA-512

Test	Size (Kb)	
	SHA-256	SHA-512
1	0,334	0,355
2	0,342	0,348
3	0,356	0,385
4	0,361	0,375
5	0,362	0,388
6	0,368	0,398
7	0,432	0,453
8	0,453	0,483
9	0,457	0,476
10	0,506	0,538
11	0,507	0,543
12	0,552	0,559
13	0,554	0,558
14	0,556	0,638
15	0,645	0,653
16	0,675	0,685
17	0,754	0,782
18	1,015	1,022
19	2,02	2,03
20	3,09	3,26
Average	**0,72**	**0,75**

ISSN 2723-6471

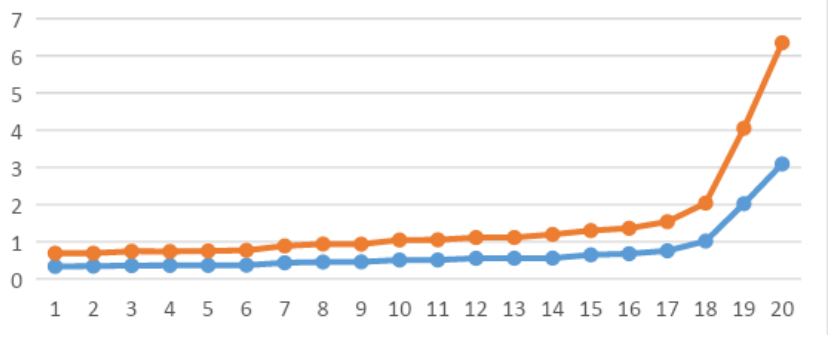

Figure. 10. Graph of Data Size on SHA-256 & SHA-512

4.6. Algorithm Tokens

Comparison of the JSON Web Token size on the SHA-256 and SHA-512 algorithms. The token obtained by SHA-256 has a size of 256 bits so that the size required by SHA-256 is quite small. In contrast to the size of the token generated by SHA-512 which has a size of 512 bits. The average token size using SHA-256 is 0.72 kb, while the average token size in the SHA-512 algorithm is 0.75 kb. The lowest size results obtained when using SHA-256 on JSON Web Token is 0.334 kb and the highest is 3.09 kb in 20 trials. Meanwhile, the lowest size obtained when using SHA-512 is 0.355 kb and the highest is 3.26 kb. This is because the size of the SHA-512 JWT is longer when compared to SHA-256 because of the different bits used by each algorithm.

5. Conclusion

The use of the SHA-512 algorithm on the JSON Web Token has a good and fast performance in the authentication process. The results of this study indicate that the use of SHA-512 on the JWT has a good speed with an average data request speed of 512.8 milliseconds (ms) when compared to the SHA-256 algorithm which has an average data request speed of 515.55 Ms. Meanwhile, in terms of data size, SHA-512 produces a larger average data request size of 0.75 kilobytes (kb) compared to SHA-256 which has an average data request size of 0.72 kb. From the analysis that has been done, the use of the SHA-512 algorithm on the JSON Web Token has good and fast performance in the authentication process. Tokens with the SHA-512 algorithm have a greater hash value than tokens with the SHA-256 algorithm, this is evidenced by the token size obtained where the size of the SHA-512 token is longer than SHA-256.

References

[1] Y. Winoto, N. Aufa and R. K. Anwar, "Model Literasi Informasi Pengajar dalam Mengembangkan Model Kecerdasan Ruang Visual (Spatial Intelligence) : Studi pada Para Peserta Bimbingan Belajar Villa Merah Bandung," PUSTABIBLIA: Journal of Library and Information Science, pp. 59-78, 2020.

[2] A. Ardiansyah and M. Kurniasih, "Implementasi Algoritma AES-256 Untuk Pengamanan Layanan API Pada Restful Dengan Autentikasi Json Web Tokens," Seminar Nasional Inovasi Teknologi – SNITek, pp. 315-327, 2019.

[3] H. Hamad, M. Saad and R. Abed, "Performance Evaluation of RESTful Web Services for Mobile Devices," International Arab Journal of e-Technology, Vol. 1, No. 3, pp. 71-78, 2010.

[4] S. Mumbaikar and P. Padiya, "Web Services Based On SOAP and REST Principles," International Journal of Scientific and Research Publications, Volume 3, Issue 5, pp. 1-4, 2013.

[5] P. Sahoo, N. K. Janghel and D. Samanta, "Securing WEB API Based on Token Authentication," International Journal on Advanced Electrical and Computer Engineering (IJAECE), pp. 1-4, 2017.

[6] M. B. Jones, J. Bradley and N. Sakimura, "JSON Web Token (JWT)," Internet Engineering Task Force (IETF), pp. 1-30, 16 May 2015.

[7] P. F. Tanaem, D. Manongga and A. Iriani, "RESTFul Web Service Untuk Sistem Pencatatan Transaksi Studi kasus PT. XYZ," Jurnal Teknik Informatika dan Sistem Informasi, pp. 1-10, 2016.

[8] A. Sebastian, "Implementasi dan Perbandingan Performa Algoritma Hash Sha-1, Sha-256, dan Sha-512," Program Studi Teknik Informatika, Institut Teknologi Bandung, Bandung, 2007.

[9] D. Juardi, "Kajian Vulnerability Keamanan Data dari Eksploitasi Hash Length Extension Attack," Incomtech VoL 6, No 1, pp. 48-58, 2017.

[10] FIPS, "Secure Hash Standard (SHS)," Information Technology Laboratory, Gaithersburg, 2008.

[11] G. Tendra and D. Wulandari, "Implementasi Representational State Transfer dan Geotagging pada Aplikasi Pelaporan Kecelakaan Lalu Lintas," Jurnal Intra Tech, pp. 7-16, 2020.

[12] A. R. S. A. Mugianto, "Pengembangan Perencanan Pembelajaran Menulis Teks Laporan Hasil Observasi Model Pembelajaran Berbasis Proyek Siswa Kelas X Sma," Jurnal Ilmu Budaya, pp. 353-366, 2017.

[13] L. Tahmidaten and W. Krismanto, "Permasalahan Budaya Membaca di Indonesia (Studi Pustaka Tentang Problematika & Solusinya)," Jurnal Pendidikan dan Kebudayaan, pp. 22-33, 2020.