SISTEM KEAMANAN *WEB SERVICE* (RESTFUL API) PADA JSON WEB TOKEN UNTUK MENGUKURAUTHENTICATION DAN AUTHORIZATION DENGAN HASHING ALGORITMA HMAC SHA-512

TUGAS AKHIR

Disusun Oleh:

Amrina Rosyada

09011381621108

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

SISTEM KEAMANAN WEB SERVICE (RESTful API) PADA JSON WEB TOKEN UNTUK MENGUKUR AUTHENTICATION DAN AUTHORIZATION DENGAN HASHING ALGORITMA HMAC-SHA- 512

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

AMRINA ROSYADA
09011381621108

Palembang, Januari 2022

Pembimbing I,

Deris Stiawan,M.T.,Ph.D.
NIP. 197806172006041002

Pembimbing II,

Ahmad Heryanto,S.Kom.,M.T.
NIP. 198701222015041002

Mengetahui 5/1/22
Ketua Jurusan Sistem Komputer

Dr.Jr.Sukemi,M.T.
NIP. 19661203200604100

VALIDITY SHEET

WEB SERVICE SAFETY SYSTEM ON JSON WEB TOKEN FOR AUTHENTICATION AND AUTHORIZATION WITH HASHING ALGORITHM HMAC-SHA-512

FINAL PROJECT

Submitted to Computer of the Term Obtaining

Bachelor of Computer Engineering

By :

AMRINA ROSYADA

09011381621108

Palembang, Januari 2022

Final Project Advisor I	Final Project Advisor II
Deris Stiawan, Ph. D.	**Ahmad Heryanto, S.Kom.,M.T**
NIP.197806172006041002	**NIP.198701222015041002**

Acknowledge by,

The Head of Computer Systems Department,

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jumat

Tanggal : 16 Juli 2021

Tim Penguji :

1. **Ketua : Ahmad Zarkasih, S. T., M. T**

2. **Pembimbing I : Deris Stiawan, M.T., Ph.D.**

3. **Pembimbing II : Ahmad Heryanto, S.Kom., M.T.**

4. **Penguji : Huda Ubaya, M. T**

Mengetahui
Ketua Jurusan Sistem Komputer

Dr.Ir.H.Sukemi,M.T.
NIP. 196612032006041001

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Amrina Rosyada

NIM : 09011381621108

Judul : Sistem Keamanan Web Service (RESTful API) Pada JSON Web Token Untuk Mengukur *Authentication* dan *Authorization* Dengan Hasing Algoritma HMAC-SHA-512

Hasil pengecekan *Software Ithenticate / Turnitin* : 4%

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 25 Januari 2022

Amrina Rosyada

HALAMAN PERSETUJUAN SIMILARITY

Saya yang bertanda tangan di bawah ini

Nama	: Amrina Rosyada
Nim	: 09011281621108
Prodi	: Sistem Komputer
Fakultas	: Ilmu Komputer

Menyatakan bahwa benar hasil pengecekan similarity Skripsi/Tesis/Disertasi/Lap. Penelitian yang berjudul Sistem Keamanan Web Service (RESTful API) Pada JSON Web Token Untuk Mengukur Authentication dan Authorization Dengan Hashing Algoritma HMAC-SHA-512 adalah 4 %. Dicek oleh operator *:

1. Dosen Pembimbing
2. UPT Perpustakaan
3. Operatur Fakultas.....

Demikianlah surat keterangan ini saya buat dengan sebenarnya dan dapat saya pertanggung jawabkan.

Menyetujui,
Dosen Pembimbing I,

Deris Stiawan, M.T.,Ph.D.
NIP. 197806172006041002

Palembang, Januari 2022
Pembimbing II,

Ahmad Heryanto. S.Kom.,M.T.
NIP. 198701222015041002

Yang Menyatakan,

Amrina Rosyada
NIM. 09011381621108

*Lingkari salah satu jawaban tempat anda melakukan pengecekan Similarity

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala Karunia dan Rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul "**Sistem Keamanan Web Service (RESTful API) Pada JSON Web Token Untuk Mengukur Authentication dan Authorization Dengan Hashing Algoritma HMAC-SHA-512**".

Selama penulisan dan penyusunan Tugas Akhir, penulis mendapatkan begitu banyak bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Penulis menyampaikan ucapan terima kasih sebesar-besarnya kepada:

1. Allah SWT. atas nikmat kehidupan, kesempatan, serta kesehatan sehingga dapat menyelesaikan kerja praktik.
2. Kedua orang tua saya serta keluarga yang telah memberikan dukungan, semangat dan kepercayaan.
3. Bapak Jaidan Jauhari, S.pd., M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Program Studi Sistem Komputer Universitas Sriwijaya.
5. Bapak Ahmad Fali Oklilas, M.T. sebagai Pembimbing Akademik Penulis di Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Universitas Sriwijaya.
7. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Universitas Sriwijaya.
8. Nova, Rini, dan miftahuljannah yang selalu memberikan semangat dan dorongannya.
9. Seluruh teman-teman seperjuangan Angkatan 2016 Bukit Jurusan Sistem Komputer

Penulis menyadari bahwa dalam penulisan laporan Tugas Akhir masih banyak terdapat kekurangan dan kesalahan, untuk itu penulis memohon maaf serta dengan rendah hati menerima kritik dan saran sebagai evaluasi bagi pribadi penulis dimasa mendatang. Tentu penulis berharap apa yang di tulis dalam laporan Tugas Akhir ini memiliki manfaat bagi pembacanya.

Palembang, Januari 2022

Penulis

Amrina Rosyada

NIM. 09011381621108

SISTEM KEAMANAN WEB SERVICE (RESTFUL API) PADA JSON WEB TOKEN UNTUK MENGUKUR AUTHENTICATION DAN AUTHORIZATION DENGAN HASHING ALGORITMA HMAC SHA-512

Amrina Rosyada (0901181621108)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : Amrina2304@gmail.com

Abstrak

Di dalam perkembangan bisnis, web service sungguh sangat dibutuhkan dalam integrasi sistem karena tidak melihat platform, arsitektur maupun bahasa pemrograman yang digunakan oleh sumber berbeda. Keamanan web service ada didalam sepuluh kerentanan teratas dalam *keamanan Application Programming Interface* (API) Web Service yang kurang terlindungi menurut *The Open Web Application Security Project* (OWASP). Dalam pemanfaatan teknologi informasi yang begitu pesat saat ini, dapat mempermudah penyampaian informasi yang akurat dan tepat dari satu pihak ke pihak yang lain. Internet merupakan sarana yang baik untuk melakukan hal tersebut. Salah satu teknologi yang memanfaatkan internet untuk memberikan informasi dan pertukaran data adalah web service . Sedangkan REST, memiliki 2 format pengiriman data, yaitu dalam format XML dan format JSON. Di mana perbandingan performa dari keduanya, web service dengan basis JSON memiliki performa yang lebih baik. Keamanan pada ReST Technology mencakup data serta seluruh komunikasi untuk melindungi kerahasiaan dan integrasi data. Salah satu solusi yang paling efektif dan terdistribusi adalah menggunakan JWT (JSON Web Token) untuk pengamanan secara *stateless*.

Kata Kunci :*Web Service, Representational state transfer API (Restful API), Javascript Object Nonation (JSON), Json web token (JWT), Authentication, Atuhorization,* HMAC-SHA-512.

WEB SERVICE SAFETY SYSTEM ON JSON WEB TOKEN FOR AUTHENTICATION AND AUTHORIZATION WITH HASHING ALGORITHM HMAC-SHA-512

Amrina Rosyada (09011381621108)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email :Amrina2304@gmail.com

Abstract

In the growing business, the web service is desperately needed inside systems integration because it doesn't see the platform, architecture or programming language.Used by different sources. Web service security is in ten.The top vulnerability in the security application programming interface (fire) web.The underprotected service according to the open web application security project(OWASP). In today's rapid use of information technology, May make it easier to convey accurate and accurate information from one side to the other side. The Internet is a good tool for doing this. One of the technologies that USES the Internet to provide information and the data exchange is a web service. By rest, it has a 2nd form of delivery data, which is in XML format and Json format. Where the performance comparisons are from both: web service with a json base has better performance. Security at the rest technology includes data as well as all communication for protecting secrecy and integration of data. One of the most effective and effective solutions distributed is using the JWT (JSON Web Token) for safekeeping stateless.

Keywords : Web Service, Representational state transfer API (Restful API), Javascript Object Nonation (JSON), Json web token (JWT), Authentication, Atuhorization, HMAC-SHA-512.

DAFTAR ISI

HALAMAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di dalam perkembangan bisnis, *web service* sungguh sangat dibutuhkan dalam integrasi sistem karena tidak melihat platform, arsitektur maupun bahasa pemrograman yang digunakan oleh sumber berbeda. Keamanan *web service* ada didalam sepuluh kerentanan teratas dalam keamanan *Application Programming Interface* (API*) Web Service* yang kurang terlindungi menurut *The Open Web Application Security Project* (OWASP) [1]. Dalam pemanfaatan teknologi informasi yang begitu pesat saat ini, dapat mempermudah penyampaian informasi yang akurat dan tepat dari satu pihak ke pihak yang lain. Internet merupakan sarana yang baik untuk melakukan hal tersebut. Salah satu teknologi yang memanfaatkan internet untuk memberikan informasi dan pertukaran data adalah web service .Sedangkan REST, memiliki 2 format pengiriman data, yaitu dalam format XML dan format JSON. Di mana perbandingan performa dari keduanya, web service dengan basis JSON memiliki performa yang lebih baik [2]. Keamanan pada ReST *Technology* mencakup data serta seluruh komunikasi untuk melindungi kerahasiaan dan integrasi data [3]. Salah satu solusi yang paling efektif dan terdistribusi adalah menggunakan JWT (*JSON Web Token*) untuk pengamanan secara stateless [4].

Situs web biasanya ditempatkan pada server web. Sebuah server web umumnya telah dilengkapi dengan perangkat-perangkat lunak khusus untuk menangani pengaturan nama ranah, serta menangani layanan atas protokol HTTP yang disebut sebagai Server HTTP, seperti Apache HTTP Server, atau *Internet Information Services* (IIS) [5]. Penggunaan otentikasi berbasis token menggunakan JWT telah diselidiki oleh[6] yang menghasilkan otentikasi berbasis token menggunakan JWT lebih baik dari yang lain dilihat dari Mekanisme otentikasi, Mekanisme kontrol akses, struktur token *Compact* & *stateless*, Ganda otentikasi atau dukungan

SSO, dan skalabilitas kontrol akses. Salah satu mekanisme hashing yang digunakan pada JWT adalah HMAC-SHA. JWT menstandarisasikan HMAC-SHA sebagai algoritma hashing untuk pengamanannya. Selanjutnya terkait penelitian terkait kemanan REST API menggunakaan JWT seperti dalam studi[7] yang membandingkan kinerja JWT dengan satu dan beberapa token di satu atau beberapaserver.

Hasil menunjukkan bahwa sistem yang diusulkan memiliki kinerja yang lebih buruk daripada yang menggunakan token tunggal. Oleh karena itu dari penelitian ini, kita akan menerapkan HMAC SHA-512 dengan menggunakan *Express Node* JS sebagai RESTful API dan dijalankan dalam sistem operasi berbasis Linux (Ubuntu 18.04)[7]. Dari penelitian ini diharapkan hasil perbandingan dengan algoritma HMAC SHA-512 dapat lebih baik dalam mengamankan *Web Service* yang dibangun. Alasan utama penerapan algoritma ini dibandingkan standarisasi seperti HMAC SHA-256/512 adalah untuk menguji hasil dan performa dari algoritma..

1.2 Tujuan

Tujuan dari penelitian yang dilakukan adalah untuk menerapkan membandingkan dan membuktikan beberapa permasalahan penelitian, antara lain :

1. Mengimplemtasikan RESTful API dengan Node-JS pada aplikasi berbasis web
2. Membandingkan hasil penerapan algoritma HMAC SHA-512 dengan HMAC SHA-256.
3. Token yang dihasilkan pada HMAC- 512 lebih panjang, dengan data *size* yang lebih besar, Walaupun membawa data yang sama besar jika dibandingkan dengan algoritma HMAC-SHA-256, HMAC-SHA-512 tetap lebih cepat dalam execution time. Supaya dapat membuktikan bahwa hasil dari penelitian ini jauh lebih baik dari Algoritma sebelumnya , dan diterapkan pada sistem yang menggunakan JSON Web Token untuk pengamanan *web service.*

1.3 Manfaat

Adapun manfaat yang didapatkan dalam penelitian ini adalah :

1. Dapat mengetahui cara kerja dengan menerapkan sistem keamanan *web service* yang menggunakan JSON Web Token (JWT) yang mengimplementasikan RESTful API.
2. Dapat dikendalikan dengan sistem keamanan dengan menggunakan algoritma HMAC-SHA-512
3. Dapat meningkatkan kualitas keamanan aplikasi berbasis web dengan menerapkan JSON Web Token (JWT).

1.4 Rumusan Masalah

Dari beberapa penelitian yang dilakukan sebelumnya adalah:

1 Apa yang akan dilakukan pada algoritma HMAC SHA-256 dan di-jalankan pada arsitektur 64 bit?

2 Apakah penelitian dengan menerapkan algoritma HMAC SHA-512 sudah benar?

3 Bagaimana hasil penerapan sistem dengan menggunakan JSON Web Token untuk pengamanan *web service* ?

1.5 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah :

1. RESTful API yang dibangun menggunakan NodeJS, karena pertimbangan flexsibilitas dan penerapan algoritma kompatibel di platform ini.
2. Sistem operasi yang digunakan berbasis linux Ubuntu 18.04 LTS 64 bit.
3. Metode algoritma dilakukan pada localhost dengan melakukan pengujian *authentication, authorization* dan pengaksesan enpoint lain.

1.6 Metodologi Penelitian

Agar tujuan penelitian ini dapat tercapai berikut merupakan tahapan penelitian:

1. Studi Pustaka atau Literatur

   Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk diangkat sebagai penelitian, dengan membaca banyak artikel atau makalahpenelitian yang berhubungan langsung dengan tugas akhir yang dibahas.

2. Perancangan Sistem

   Tahap ini membahas mengenai proses bagaimana membangun system dengan menggunakan metode atau pendekatan tertentu, Apa saja perangkat keras atau perangkat lunak yang digunakan, kemudian bagaimana proses instalasi dan konfigurasi sistem, selanjutnya bagaimana pula penerapan metode pada penelitian tugas akhir.

3. Pengujian

   Tahap ini merupakan tahap lanjutan dari proses perancangan yang telah dilakukan. Dengan melakukan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat secara konsep dan teknis.

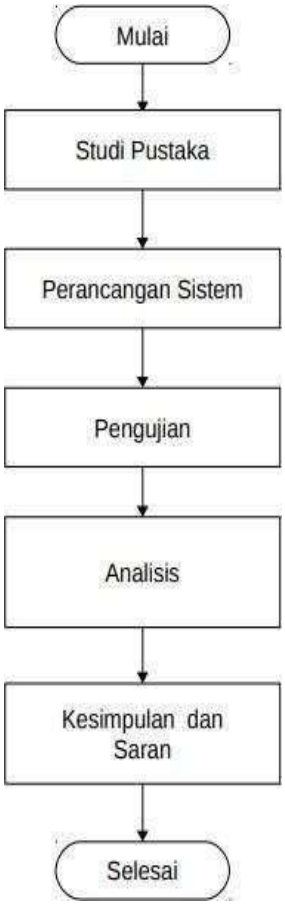
4. Analisis

   Data yang diperoleh dari proses pengujian, kemudian dianalisis berdasarkan pendekatan tertentu, mengingat data yang diperoleh berupa data kuantitatif maka diolah berdasarkan pendekatan tersebut, selanjutnya dilakukan analisis sehingga didapatkan data yang objektif.

5. Kesimpulan dan Saran

   Pada tahap ini akan dirumuskan suatu kesimpulan berdasarkan permasalahan, studi pustaka, metodologi penelitian dan analisis hasil pengujian. Kemudian beberapa saran yang dapat dijadikan landasan untuk penelitian lanjutan.Pada gambar 1.1 berikut, ditampilkan metodologi penelitian secara visual dalam bentuk diagram alir, yang

merepresentasikan proses pelaksanaan penelitian



Gambar 1.1. Diagram Alir Metodologi Penelitian

1.7 Sistematika Penulisan

Untuk lebih memudahkan dalam proses penyusunan tugas akhir dan memperjelas konten dari tiap bab, maka dibuat suatu sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan dan Batasan Masalah, kemudian Metodologi Penelitian, dan yang terakhir mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitian terkait mengenai penelitian terkait Authentication dan Authorization process dengan JWT menggunakan Algoritma HMAC-SHA-512

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang hasil penelitian yang dilakukan, serta menjawab setiap tujuan yang hendak dicapai seperti yang tercantum pada BAB 1 (Pendahuluan).

DAFTAR PUSTAKA

[1] A.Rahmatulloh, H. Sulastri, and R. Nugroho, “Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 7, no. 2, 2018.

[2] A. Aziz, Wiharto, and B. Wicaksono, “Pemanfaatan Web Service Moodle Berbasis REST-JSON untuk Membangun Moodle Online Learning Extension berbasis Android,” *J. Itsmart*, vol. 2, no. 2, pp. 1–6, 2013.

[3] P. F. Tanaem, D. Manongga, and A. Iriani, “RESTFul Web Service Untuk Sistem Pencatatan Transaksi Studi Kasus PT . XYZ,” vol. 2, no. April, 2016.

[4] R. Gunawan and A. Rahmatulloh, “JSON Web Token (JWT) untuk Authentication pada Interoperabilitas Arsitektur berbasis RESTful Web Service,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 74, 2019

[5] S. M. Intani and F. Salsabila, “Sejarah Web Service dan Cara Penggunaannya,” *Sej. Web Serv. Dan Pengguna.*, no. March, pp. 1–3, 2020.

[6] O. Ethelbert, F. F. Moghaddam, P. Wieder, and R. Yahyapour, “A JSON token- based authentication and access management schema for cloud SaaS applications,” *Proc. - 2017 IEEE 5th Int. Conf. Futur. Internet Things Cloud, FiCloud 2017*, vol. 2017- Janua, pp. 47–53, 2017

[7] K. V. Kanmani and P. S. Smitha, “Survey on Restful Web Services Using Open Authorization (Oauth),” *IOSR J. Comput. Eng.*, vol. 15, no. 4, pp. 53–56, 2013

[8] Aradea., “Implementasi Web-Service Untuk Pembangunan Sistem

Kartu Rencana Studi (KRS) Online," no. 1693–9670, 2006.

[9] A. Rahmatulloh, R. Gunawan, and F. M. S. Nursuwars, "Performance comparison of signed algorithms on JSON Web Token," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 550, no. 1, 2019.

[10] L. Petkova, "HTTP Security Headers," no. March 2019, 2020

[11] R. Jumadi, "Simple Object Access Protocol Pada Situs Web Periklanan," 2011.

[12] K. Beznosov, D. J. Flinn, S. Kawamoto, and B. Hartman, "Introduction to Web services and their security," *Inf. Secur. Tech. Rep.*, vol. 10, no. 1, pp. 2–14, 2005.

[13] A. B. Warsito, A. Ananda, and D. Triyanjaya, "Penerapan Data JSON Untuk Mendukung Pengembangan Aplikasi Pada Perguruan Tinggi Dengan Teknik RESTful Dan Web Service," *Technomedia J.*, vol. 2, no. 1, pp. 26–36, 2017.

[14] H. Sy and Rismayani, "Monitoring Absensi Harian Kepegawaian Pada Instansi Pemerintahan Kota Makassar Berbasis," *Semin. Nas. Inform.*, pp. 236– 239, 2015.

[15] A. Kusumawaty, "Aplikasi Pemesanan Makanan Pada Restoran Berbasis Android dan PHP Menggunakan Protokol JSON," *Univ. Gunadarma*, pp. 1–8, 2012.

[16] Wahabi, M. Jones, N. Sakimura, and J. Bradley, "Penggunaan Hashing dalam JSON Web Token (JWT) untuk Sistem Autentikasi Pengguna," 2018.

[17] N. Triyana and A. Eka, "Analisis dns amplification attack," vol. 1, pp. 17–22, 2017..

[18] W. Hardi, "Evaluasi Aplikasi Domain Name Server (DNS) sebagai Search Engine untuk Pencarian Nama Domain Best Universities dan Top Leading Banks di Indonesia," *Online J.*, 2007.