SISTEM KEAMANAN WEB *SERVICE* (*RESTful* API) PADAJSON WEB TOKEN UNTUK MENGUKUR *AUTHENTICATION* DAN *AUTHORIZATION* DENGAN *HASHING* ALGORITMA RSA- SHA-512

TUGAS AKHIR

OLEH :

RESKY PANELYA ANNISA

09011381621088

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 RSA-SHA- 512

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

RESKY PANELYA ANNISA

09011381621088

Palembang, Januari 2022

Pembimbing I,

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

Pembimbing II,

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

Mengetahui 25/1/22
Ketua Jurusan Sistem Komputer

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

VALIDITY SHEET

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

FINAL PROJECT

Submitted to Computer of the Term Obtaining

Bachelor of Computer Engineering

By :

RESKY PANELYA ANNISA

09011381621088

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 :

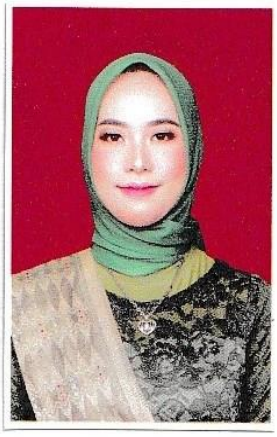
Nama : Resky Panelya Annisa

NIM : 09011381621088

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

Hasil pengecekan *Software Ithenticate / Turnitin* : 13%

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

ReskyPanelya Annisa

HALAMAN PERSETUJUAN SIMILARITY

Saya yang bertanda tangan di bawah ini

Nama : Resky Panelya Annisa
Nim : 09011281621088
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 RSA-SHA-512 adalah 13%. 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,

Resky Panelya Annisa
NIM. 09011381621088

*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 RSA-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 kesehatansehingga dapat menyelesaikan kerja praktik.
2. Kedua orang tua saya serta keluarga yang telah memberikandukungan, 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 AkademikPenulis 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 PembimbingII Tugas Akhir di Jurusan Sistem Komputer Universitas Sriwijaya.
8. Cresa, Nanda, Nia, dan Akbar yang selalu memberikan semangatdan 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

Resky Panelya Annisa
NIM. 09011381621088

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

Resky Panelya Annisa (09011381621088)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email: annisaecha16@gmail.com

Abstrak

Di zaman modern ini perkembangan internet semakin hari semakin meningkat baik dari segi teknologi dan dari penggunaannya, hal ini dapat membawa banyak hal positif bagi kehidupan manusia. Tentunya tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif juga bagi manusia. Keamanan Web Service masuk kedalam sepuluh kerentanan teratas dalam keamanan Application Programming Interface (API) Web Service yang kurang terlindungi menurut OWASP (The Open Web Application Security Project). Salah satu jenis dari web service adalah REST atau RESTful (Representational). Web Service API yang menggunakan REST disebut dengan RESTful API. Pada penelitian yang menggunakan JWT (Json Web Token) dengan algoritma HMAC SHA-256 yang masih umum digunakan, sehingga dapat menjadi kerentanan tersendiri bagi keamanan RESTful Web Service. Hasil sebuah penelitian menyatakan, perbandingan penerapan algoritma SHA-256 dan SHA-512 pada arsitektur intel 64-bit mengasilkan kinerja SHA-512 50% lebih baik dibandingkan dengan SHA-256.

Kata Kunci : *Web Service, Representational state transfer API (Restful API), Java Script Object Notation (JSON), Json web Token (JWT), Authentication, Authorization, RSA-SHA-512.*

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

Resky Panelya Annisa (09011381621088)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: annisaecha16@gmail.com

Abstract

In modern times, growing on the Internet in terms of technology and its use can bring many positive things to human life. Surely it cannot be denied that Internet technology has had a negative impact on people as well. Web service security tapped into the top ten vulnerability in the Application Programming Interface (API) web service less protected by OWASP (The Open Web Application Security Project). One kind of web service was REST or RESTful (Representational). Web service API using the rest called by RESTful API. On research using JWT (Json Web Token) with an HMAC SHA-256 algorithm still commonly used, and thus could be a unique security tailor for the restful web service. According to one study, a comparison of algorithm SHA-256 and SHA-512 algorithms in Intel 64-bit is better than SHA-512 percent with SHA-256.

Keywords : *Web Service, Representational state transfer API (Restful API), Java Script Object Notation (JSON), Json web Token (JWT), Authentication, Authorization, RSA-SHA-512.*

DAFTAR ISI

Halaman

BAB III METODOLOGI PENELITIAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di zaman modern ini perkembangan internet semakin hari semakin meningkat baik dari segi teknologi dan dari penggunaannya, hal ini dapat membawa banyak hal positif bagi kehidupan manusia. Tentunya yang bersifat positif semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi internet ini. Tentunya tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif juga bagi manusia. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan. Kini dapat dilakukan dengan menggunakan media komputer secara *online* dengan risiko tertangkap dengan sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru. Banyaknya dampak negatif yang timbul dan berkembang, membuat suatu paradigma bahwa tidak ada perangkat yang aman jika terhubung pada sebuah jaringan [1].

Komputasi terdistribusi adalah teknologi informasi yang melakukan komputasi pada banyak mesin. Komputasi terdistribusi ditemukan setelah adanya teknologi *web*. Maksud dari teknologi ini adalah *Web Service* [2]. *Web service* merupakan sebuah perangkat lunak atau *software* digunakan sebagai jembatan yang memungkinkan berbagai sistem dapat berkomunikasi tanpa terpengaruh dengan perbedaan *platform*, arsitektur maupun bahasa pemrograman yang digunakan dari sumber yang berbeda [3]. Keamanan *Web Service* masuk kedalam sepuluh kerentanan teratas dalam keamanan *Application Programming Interface* (API) *Web Service* yang kurang terlindungi menurut *OWASP (The Open Web Application Security Project)* [4].

Authentication merupakan proses untuk memastikan suatu pengenalan atau memastikan suatu pengakuan. Jadi pada *authentication* ini akan memastikan siapakah sebenarnya yang telah berinteraksi dengan sistem. Sistem

authentication berbasis token memungkinkan pengguna memasukkan kredensial mereka untuk menerima token yang memungkinkan mereka mengakses sumber daya tertentu - tanpa menggunakan kredensial mereka. Setelah token mereka diperoleh, pengguna dapat menawarkan token - yang menawar akses ke sumber daya tertentu untuk jangka waktu tertentu - ke situs jarak jauh. Dengan kata lain itu menambahkan satu tingkat tipuan untuk otentikasi daripada harus mengesahkan dengan nama pengguna dan kata sandi untuk setiap sumber daya yang dilindungi, pengguna mengotentikasi itu berarti sekali (dalam sesi durasi terbatas), memperoleh token terbatas waktu secara timbal balik, dan menggunakan token itu untuk autentikasi tambahan sepanjang sesi. Sedangkan *authorization* adalah proses selanjutnya setelah *authentication* berhasil. Sistem akan memberikan akses sesuai kebijakan yang sudah ditentukan sebelumnya.Di sini sistem akan memberikan batasan akses yang akan diberikan kepada karyawan yang sudah login tersebut. Tentu saja sebelumnya sudah ada rancangan pembatasan akses untuk mencegah terjadinya fraud atau kecurangan dalam perusahaan.

Salah satu jenis dari *web service* adalah *REST* atau *RESTful* (*Representational*). *REST* sendiri memungkinkan *system request* dapat mengakses dan memanipulasi teks yang direpresentasikan dari sebuah *Web Service*. *Web Service API* yang menggunakan *REST* disebut dengan *RESTful API*. Tidak seperti jenis *Web Service* lainnya, *RESTful API* tidak memiliki standar yang resmi untuk notasinya dikarenakan *REST* merupakan sebuah arsitektur. Dengan berbagai implementasi, *REST* menemukan notasi yang biasa digunakan, seperti *HTTP, URI, JSON, dan XML*. Dalam penggunaannya, *REST API* terbukti lebih cepat dalam transfer data daripada metode lain yang serupa, dalam hal ini *SOAP (SympleObject Access Protocol)*. Tidak seperti SOAP, tidak ada notasistandar resmi untuk*RESTful API*. Hal ini dikarenakan *REST* merupakan arsitektur, sedangkan *SOAP* adalah protocol [5].

Berdasarkan penjelasan diatas, maka diharapkan penelitian ini dapat menghasilkan perbandingan yang lebih baik pada algoritma *RSA-SHA-512* dalam mengamankan *Web Service* yang akan dibangun, ada juga alasan utama penerapan algoritma ini dibandingkan dengan standarisasi seperti *RSA-256/512* adalah untuk

menguji hasil dan performa dari algoritma ini. Kelebihan dari *RSA* adalah tingkat keamaan algoritma terletak pada kesulitan memfaktorkan bilangan yang besar menjadi faktor-faktor prima[6].

1.2 Tujuan

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

1. Menerapkan metode *RESTful API* pada *Node JS.*
2. Membandingkan hasil dari pengimplementasian dari algoritma *RSA- SHA-512* dengan algoritma sebelumnya *RSA-SHA-256*.
3. Mendapatkan hasil yang lebih baik, untuk diterapkan pada sistem yang menggunakan *JWT* (*JSON Web Token*) untuk otorisasi dan otetinkasi pada sebuah *Web Service*.

1.3 Manfaat

Adapun manfaat yang didapatkan dalam penelitian ini adalah:

1. Dapat membangun *RESTful API* dengan *Node JS*.
2. Membangun systempengamanan *API* yang lebih aman, dengan menerapkan algoritma *RSA-SHA-512*.
3. Dapat membangun *Authentication* dan *Authorization* pada sebuah *Web Service*

1.4 Rumusan Masalah

Dari beberapa penelitian yang dilakukan sebelumnya ialah:

1. Bagaimana mengimplementasikan *RESTful API* dengan *Node JS* ?
2. Bagaimana hasil perbandingan dari penerapan algoritma *RSA-SHA-512* dengan *RSA-SHA-256*
3. Bagaimana hasil yang didapatkan sistemdengan menggunakan JWT (*Json Web Token)* untuk pengamanan *Web Servive* ?

1.5 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah:

1. *RESTful API* yang dibangun menggunakan *Node JS/Express*, karena pertimbangan *fleksibilitas* dan penerapan algoritma lebih baik berjalan di platform ini.
2. Sistem operasi yang digunakan berbasis *linux* dengan kode distribusi *Ubuntu 18.04 LTS* (64-bit)
3. Adapun algoritma yang dilibatkan dalam penelitian ini tidak keluar dari *RSA-SHA-256* dan *RSA-SHA-512*.

1.6 Metodologi Penelitian

Metodologi penelitan dalam tugas akhir ini memiliki beberapa tahapan, yaitu:

1. Studi Pustaka / Literatur

Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk diangkat sebagai penelitian, dengan membaca banyak artikel atau makalah penelitian 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.

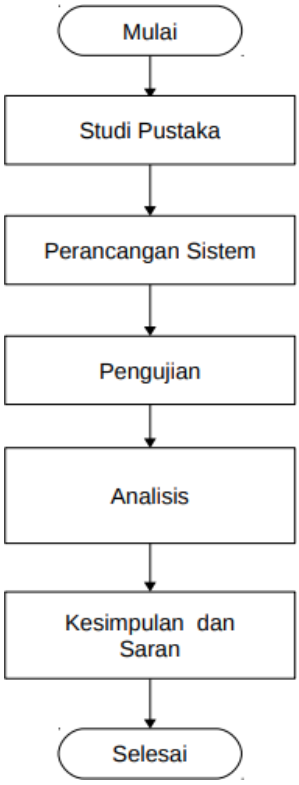
4. Analisis

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 dibawah ini, ditampilkan metodologi penelitian secara visual dalam bentuk diagram alir, yang merepresentasikan proses pelaksanaan penelitian:



Gambar 1.1. Diagram Alur Metodologi Penelitia

1.7 Sistematika Penulisan

Untuk lebih memudahkan dalam proses penyusunan tugas akhir dan memperjelas topik dari setiap bab, maka dibuat suatu sistematika penulisansebagaiberikut:

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 membahasa teori dasar seperti *Web Service*, API, HTTP, *Authentication*, *Authorization*, JSON, JWT, Algoritma RSA-SHA-256, Algoritma RSA-SHA-512, NodeJS, Ubuntu18.04LTS, dan MySQL yang berkaitan langsung pada penelitian.

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] F. widya Putra, "Analisis Keamanan Website Dari Serangan Sql Injection Menggunakan Web Application Firewall," 2018.

[2] Edy, Ferdiansyah, W. Pramusinto, and S. Waluyo, "Pengamanan Restful API menggunakan JWT untuk Aplikasi Sales Order," vol. 3, no. 2, pp. 106–112, 2019.

[3] R. S. Galih and F. Salamun, "Implementasi Web Service pada Aplikasi Mobile untuk Mendukung Sistem Informasi di Bandung N-Max Community," pp. 8–9, 2018.

[4] 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.

[5] B. Satria, A. Kusyanti, and W. Yahya, "Implementasi Algoritme Blake2s pada JSON Web Token (JWT) sebagai Algoritme Hashing untuk Mekanisme Autentikasi Layanan REST-API," vol. 2, no. 12, pp. 6269–6276, 2018.

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

[7] 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*, pp. 47–53, 2017.

[8] 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.

[9] W. M. Quinn *et al.*, "System and Method For Achieving Highly Scalable Real-Time Collaboration Application Using HTTP," vol. 1, no. 19, 2008.

[10] G. Tyson *et al.*, “Exploring HTTP header manipulation In-the-wild,” pp. 451–458, 2017.

[11] A. Setiawan and A. I. Purnamasari, “Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk Otentikasi Aplikasi Batik Kita,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, pp. 4–10, 2020.

[12] R. Choirudin and A. Adil, “Implementasi Rest Api Web Service dalam Membangun Aplikasi Multiplatform untuk Usaha Jasa,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 18, no. 2, pp. 284–293, 2019.

[13] Sunardi, I. Riadi, and P. A. Raharja, “Analisis Application Programming Interface Pada Mobile E-Voting Menggunakan Metode Test-Driven Development,” *(Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 20, no. 2, p. 87, 2019.

[14] A. Banati, E. Kail, K. Karoczkai, and M. Kozlovszky, “Authentication and Authorization Orchestrator For Microservice-Based Software Architectures,” no. May, pp. 1180–1184, 2018.

[15] 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.

[16] T. Bray, J. Paoli, and C. M. S. McQueen, “Extensible Markup Language (XML) 1.0,” *Wirtschaftsinformatik*, vol. 41, no. 3, pp. 274– 276, 1999, doi: 10.1007/BF03254940.

[17] A. W. Appel, *Verification of A Cryptographic Primitive: SHA-256*, vol. 2015-June. 2015.

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

[19] K. Saravanan, G. Abraham, K. Ventakasubramanian, and K. Borasia,

"Securing Web Services Using XML Signature and XML Encryption," no. September, 2013.

[20] H. Sembiring, F. Y. Manik, and T. Zaidah, "Penerapan Algoritma Secure Hash Algorithm (SHA) Keamanan Pada Citra," *Media Inf. Anal. dan Sist.*, vol. 4, no. 1, pp. 33–36, 2019.

[21] H. Agung and Ferry, "Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature," vol. 3, no. 1, pp. 34–45, 2016.

[22] Antares, "Postman." https://www.postman.com/.

[23] Insomnia, "Insomnia REST API." https://insomnia.rest/.