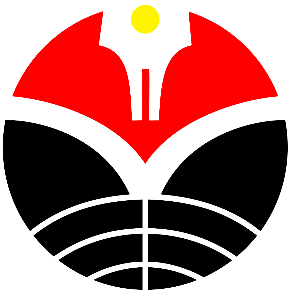
59/S/TEKKOM-KCBR/PK.03.08/14/AGUSTUS/2025

PENGEMBANGAN METODE KEAMANAN RESTFUL API BERBASIS JWT TOKEN GANDA DENGAN VARIASI *ONE TIME* TOKEN



SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar sarjana teknik
pada Program Studi Teknik Komputer

Oleh:
Johan Kristianto
2102635

PROGRAM STUDI S1 TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA
2025

HALAMAN HAK CIPTA

PENGEMBANGAN METODE KEAMANAN RESTFUL API BERBASIS JWT TOKEN GANDA DENGAN VARIASI *ONE TIME* TOKEN

Oleh
Johan Kristianto
2102635

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar sarjana teknik pada Program Studi Teknik Komputer

HALAMAN PENGESAHAN SKRIPSI

JOHAN KRISTIANTO

PENGEMBANGAN METODE KEAMANAN RESTFUL API BERBASIS JWT TOKEN GANDA DENGAN VARIASI ONE TIME TOKEN

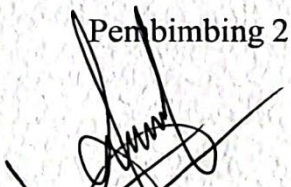
Disetujui dan disahkan oleh:

Pembimbing 1

Muhammad Taufik, S.Tr.Kom., M.T.I.

NIP. 920200819940117101

Pembimbing 2



Anugrah Adiwilaga, S.ST., M.T.

NIP. 920200819880813101

Mengetahui

Ketua Program Studi S-1 Teknik Komputer

Dr. Eng. Munawir, S.Kom., M.T.

NIP. 920200819851205101

PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Johan Kristianto

NIM : 2102635

Program Studi : Teknik Komputer

Judul Karya : Pengembangan Metode Keamanan RESTful API Berbasis JWT Token Ganda Dengan Variasi *One Time Token*.

Dengan ini menyatakan bahwa karya tulis ini merupakan hasil kerja saya sendiri, Saya menjamin bahwa seluruh isi karya ini, baik sebagian maupun keseluruhan, bukan merupakan plagiarisme dari karya orang lain, kecuali pada bagian yang telah dinyatakan dan disebutkan sumbernya dengan jelas.

Jika di kemudian hari ditemukan pelanggaran terhadap etika akademik atau unsur plagiarisme, saya bersedia menerima sanksi sesuai peraturan yang berlaku di Universitas Pendidikan Indonesia.

Bandung, 20 Agustus 2025

Johan Kristianto

PENGEMBANGAN METODE KEAMANAN RESTFUL API BERBASIS JWT TOKEN GANDA DENGAN VARIASI *ONE TIME TOKEN*

Johan Kristianto
2102635

ABSTRAK

Di era digital yang semakin berkembang, sistem teknologi dan informasi yang aman sekaligus efisien merupakan salah satu prioritas utama di dalam bisnis dan perusahaan. RESTful API merupakan salah satu elemen penting di dalam sistem berbasis *enterprise*. Seiring dengan implementasi RESTful API yang semakin luas, serangan siber terhadap RESTful API juga semakin meningkat sehingga keamanan RESTful API yang optimal menjadi urgensi dalam menjaga akses RESTful API tersebut dari pihak-pihak luar yang tidak terautentikasi dan terotorisasi. Penelitian ini bertujuan untuk mengembangkan metode autentikasi dan otorisasi RESTful API berbasis JWT token ganda dengan variasi *one time token* serta menguji kinerjanya. Pada penelitian ini, metode yang akan digunakan adalah *design and development*. Selain itu metode autentikasi dan otorisasi yang dikembangkan diimplementasikan pada Aplikasi Product Management berbasis web sebagai pengujian. Penelitian ini menunjukkan hasil yang sesuai dari metode autentikasi dan otorisasi yang dikembangkan pada pengujian fungsionalitas dan ketahanan terhadap beberapa simulasi serangan pada uji penetrasi. Selain itu, pada pengujian beban, metode yang dikembangkan menunjukkan rentang nilai nilai 57 req/s hingga 283 ms pada *response time*, 3.5 req/sec hingga 17.3 req/sec pada *throughput*, dan rata-rata keseluruhan 0% pada pengujian beban. Hal ini mengindikasikan bahwa metode autentikasi dan otorisasi yang dikembangkan mampu menjaga akses RESTful API dari pengguna yang tidak terautentikasi dan terotorisasi serta memiliki daya tahan yang baik terhadap beban yang tinggi.

Kata Kunci: autentikasi, otorisasi, RESTful API, JWT, *One-time token*

DEVELOPMENT OF A JWT-BASED DUAL TOKEN SECURITY METHOD FOR RESTFUL APIs WITH ONE-TIME TOKEN VARIATION

Johan Kristianto

2102635

ABSTRACT

In the rapidly evolving digital era, secure and efficient information systems are among the top priorities for businesses and enterprises. RESTful APIs are a key component of enterprise-based systems. As the adoption of RESTful APIs becomes more widespread, cyberattacks targeting them have also increased, making optimal RESTful API security an urgent necessity to protect access from unauthenticated and unauthorized parties. This study aims to develop an authentication and authorization method for RESTful APIs based on dual JSON Web Tokens (JWT) with a one-time token variation and evaluating its performance*. The research adopts a design and development methodology, and the proposed method is implemented in web based product management application for testing purposes. The results indicate that the developed method meets expectations in both functionality testing and resilience against various simulated attacks in penetration testing. Furthermore, in load testing, the method demonstrated response times ranging from 57 req/s to 283 ms, throughput from 3.5 req/s to 17.3 req/s, and an average error rate of 0%. These findings suggest that the developed authentication and authorization method can effectively secure RESTful API access from unauthenticated and unauthorized users while maintaining high resilience under heavy load conditions.*

Keywords**:** *authentication, authorization, RESTful API, JWT, one-time token*

DAFTAR ISI

HALAMAN HAK CIPTA i
HALAMAN PENGESAHAN SKRIPSI ii
PERNYATAAN BEBAS PLAGIARISME iii
KATA PENGANTAR iv
ABSTRAK vi
ABSTRACT vii
DAFTAR ISI viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR PERSAMAAN xiii
DAFTAR LAMPIRAN xiv
BAB I PENDAHULUAN 1
1.1. Latar Belakang Penelitian 1
1.2. Rumusan Masalah Penelitian 4
1.3. Tujuan Penelitian 5
1.4. Manfaat Penelitian 5
1.4.1. Manfaat Teoritis 5
1.4.2. Manfaat Praktis 6
1.5. Ruang Lingkup Penelitian 6
1.6. Struktur Organisasi Skripsi 7
BAB II TINJAUAN PUSTAKA 8
2.1. Kajian Pustaka 8
2.1.1. Application Programming Interface (API) 8
2.1.1.1. Web API 8
2.1.1.2. Representational State Transfer (REST) dan RESTful API 8
2.1.2. Metode Keamanan RESTful API 15
2.1.2.1. Kriptografi Enkripsi Base64 (Base64 *encoding*) 15
2.1.2.2. Kriptografi *Hashing* HMAC SHA-256 18
2.1.2.3. Metode Keamanan Berbasis JWT 19
2.1.2.4. JWT dengan Mekanisme Token Ganda 21
2.1.2.5. Http-Only Cookies 22
2.1.3. Redis Cache 23

2.1.4. Bahasa Pemrograman Java 23
2.1.4.1. Spring Framework 24
2.1.5. Product Management 24
2.1.6. Penelitian Terkait 24
2.2. Kerangka Pemikiran 27
BAB III METODE PENELITIAN 28
3.1. Desain Penelitian 28
3.2. Identifikasi Masalah (*Identify the Problem*) 29
3.3. Identifikasi Tujuan (*Describe the Objectives*) 29
3.4. Pengembangan Metode dan Aplikasi Product Management Berbasis Web (*Design and Develop the Artifacts*) 30
3.4.1. Tahap Perencanaan (*Planning*) 30
3.4.2. Tahap Perancangan (*Design*) 31
3.4.3. Tahap Pengkodean (*Coding*) 40
3.4.4. Tahap Pengujian dan Pencarian *Bug* (*Testing and Debugging*) ... 41
3.5. Pengujian Metode dan Aplikasi (*Test the Artifacts*) 41
3.5.1. Pengujian Black Box (*Black Box Testing*) 41
3.5.2. Pengujian White Box (*White Box Testing*) 43
3.5.3. Pengujian Beban (*Load Testing*) 47
3.5.4. Pengujian Penetrasi (*Penetration Testing*) 49
3.5.5. Spesifikasi Lingkungan dan Infrastruktur Pengujian 50
3.6. Evaluasi Hasil Pengujian (*Evaluate Testing Result*) 51
3.7. Komunikasi Hasil Pengujian (*Communicate The Testing Result*) 52
BAB IV HASIL DAN PEMBAHASAN 53
4.1 Hasil Pengembangan Aplikasi *Product Management* 53
4.2 Hasil Pengembangan Metode Autentikasi dan Otorisasi 56
4.3 Hasil Pengujian Black Box (*Black Box Testing*) 59
4.4 Hasil Pengujian White Box (*White Box Testing*) 61
4.5 Hasil Pengujian Beban (*Load Testing*) 62
4.6 Hasil Pengujian Penetrasi (*Penetration Testing*) 66
4.7 Analisis Hasil Pengujian 72
BAB V KESIMPULAN DAN SARAN 74
5.1 Kesimpulan 74
5.2 Saran 74

DAFTAR PUSTAKA 75
LAMPIRAN 81

DAFTAR TABEL

Tabel 2.1 HTTP Method..... 12
Tabel 2.2 Klasifikasi kode status HTTP..... 14
Tabel 2.3 Penelitian terkait..... 25
Tabel 3.1 Format test case pengujian black-box..... 42
Tabel 3.2 Format Pengujian White Box..... 44
Tabel 3.3 Test plan skenario product manager..... 47
Tabel 3.4 Tabel test plan skenario finance manager..... 48
Tabel 3.5 Tabel test plan skenario marketing manager..... 48
Tabel 3.6 Format uji penetrasi..... 49
Tabel 3.7 Spesifikasi lingkungan pengujian..... 51
Tabel 4.1 Endpoint-endpoint di dalam API Web Service..... 53
Tabel 4.2 Hasil pengujian Black Box..... 59
Tabel 4.3 Hasil Pengujian White Box..... 62
Tabel 4.4 Hasil pengujian pertama dengan beban 1 thread..... 63
Tabel 4.5 Hasil pengujian pertama dengan beban 10 thread..... 63
Tabel 4.6 Hasil pengujian pertama dengan beban 100 thread..... 63
Tabel 4.7 Hasil pengujian kedua dengan 1 thread..... 64
Tabel 4.8 Hasil pengujian kedua dengan 10 thread..... 65
Tabel 4.9 Hasil pengujian kedua dengan 100 thread..... 65

DAFTAR GAMBAR

Gambar 2.1 Endpoint RESTful API....11
Gambar 2.2 Headers pada RESTful API.... 13
Gambar 2.3 Body pada RESTful API dengan format JSON 13
Gambar 2.4 Response body pada RESTful API 15
Gambar 2.5 Proses Base64 encoding pada pesan “hello”.... 17
Gambar 2.6 Struktur proses pada algoritma HMAC (Ravilla, 2015) 18
Gambar 2.7 Metode keamanan berbasis JWT dengan mekanisme token ganda .. 22
Gambar 3.1 alur metode design and development (Ellis & Levy, 2010).... 28
Gambar 3.2 Diagram flowchart proses registrasi.... 32
Gambar 3.3 Flowchart mekanisme token ganda dan *one time* token.... 34
Gambar 3.4 Use case diagram aplikasi *product management* berbasis web.... 36
Gambar 3.5 Desain ERD untuk API service product management 39
Gambar 3.6 Sequence diagram metode autentikasi dan otorisasi.... 39
Gambar 4.1 Dashboard Product Manager.... 55
Gambar 4.2 Dashboard Finance Manager.... 55
Gambar 4.3 Dashboard Marketing Manager.... 55
Gambar 4.4 Kode program pengecekan dan validasi access token 56
Gambar 4.5 Kode program token blacklist 57
Gambar 4.6 Kode program refresh token.... 57
Gambar 4.7 Access token dan Refresh token.... 58
Gambar 4.8 Kode program SecurityConfig 58
Gambar 4.9 Hasil output *unit testing* 62
Gambar 4.10 Hasil pengamatan dengan Wireshark 66
Gambar 4.11 Request body untuk endpoint Update Project Overview 67
Gambar 4.12 Hasil pengamatan Request Body dengan Wireshark.... 68
Gambar 4.13 Hasil decoding pada token JWT menggunakan JWT.IO 69
Gambar 4.14 Token palsu yang dibuat menggunakan JWT.IO.... 70
Gambar 4.15 Proses intercepting menggunakan Burpsuite 71
Gambar 4.16 Response server setelah pengujian.... 71

DAFTAR PERSAMAAN

Persamaan HMAC SHA-256 (1) 19
Persamaan *signature* JWT (2) 21

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian 81
Lampiran 2 Kode program Application Config 81
Lampiran 3 Kode program Security Config..... 82
Lampiran 4 Kode program JwtAuthenticationFilter Middleware..... 83
Lampiran 5 Kode program AuthenticationService 86
Lampiran 6 Kode Program JwtUtilities 88
Lampiran 7 Hasil Pengujian API..... 91
Lampiran 8 Hasil Pengujian Load Testing metode autentikasi dan otorisasi yang dikembangkan 99
Lampiran 9 Hasil Load Testing Metode Autentikasi dan otorisasi pada penelitian terdahulu..... 100
Lampiran 10 Hasil Pengujian Black Box..... 101

DAFTAR PUSTAKA

Abhishek, P., Ravipati, P., Vigneswari, S., & Posonia, A. (2019). Product Management System. *Journal of Computational and Theoretical Nanoscience*, *16*(8). 3311-3315, doi: https://doi.org/10.1166/jctn.2019.8183.

Alonso, F. S. (2015). *Development of RESTful API* (Bachelor's Thesis, Turku University Of Applied Sciences). Turku university applied sciences THESIS. https://core.ac.uk/download/pdf/38126503.pdf

Astowo, U. B., & Sujarwo, A. (2023). Penerapan JSON Web Token sebagai Strategi Pengamanan Data pada Aplikasi MultiMasjid. *Innovative: Journal Of Social Science Research*, *3*(6). 5279-5292. doi: https://j-innovative.org/index.php/Innovative/article/view/6908

Azeez, N. A., & Chinazo, O. J. (2018). ACHIEVING DATA AUTHENTICATION WITH HMAC-SHA256 ALGORITHM. *Computer Science & Telecommunications*, *54*(2). 34-43, diakses dari https://www.researchgate.net/publication/332182220

Bollinger, D. (2021). *Analyzing cookies compliance with the GDPR* (Master's thesis, ETH Zurich). Siwss Federal Institute Of Technology Zurich.

Borman, R. I., Priandika, A. T., & Edison, A. R. (2020). Implementasi metode pengembangan sistem Extreme Programming (XP) pada aplikasi investasi peternakan. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, *8*(3). 272-277, doi: 10.26418/justin.v8i3.40273

Bucko, A., Vishi, K., Krasniqi, B., & Rexha, B. (2023). Enhancing jwt authentication and authorization in web applications based on user behavior history. *Computers*, *12*(4), 78. doi: https://doi.org/10.3390/computers12040078.

Busro, S. A. B. C., Firliana, R., Muzzaki, M. N., Wardani, A. S., Khalid, M. I., Gamas, A. W. M., & Setiawan, H. (2022). Rancangan Pembuatan API Website Data Tanaman Obat Dan Langka Kabupaten Kediri. *Bulletin of Information Technology (BIT)*, *3*(4), 255-260. doi: https://doi.org/10.47065/bit.v3i4.373

Cahyono, S. A. B., Sucipto, S., & Firliana, R. (2023). Implementasi Otentikasi Website Node JS Express Menggunakan Passport. *JSITIK: Jurnal Sistem Informasi dan Teknologi Informasi Komputer*, *2*(1), 33-40. doi: https://doi.org/10.53624/jsitik.v2i1.309

Compagna, L., Jonker, H., Krochewski, J., Krumnow, B., & Sahin, M. (2021, September). A preliminary study on the adoption and effectiveness of SameSite cookies as a CSRF defence. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 49–59). IEEE. doi: https://doi.org/10.1109/EuroSPW54576.2021.00012

Darmawan, I., Mansyur, M. U., Imam, K. Z., Syahdan, M., & Fawaid, A. (2023). Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem

Informasi Akademik. *Jurnal Informasi dan Teknologi*, *5*(2). 120-128. doi: 10.37034/jidt.v5i1.368.

Ellis, T. J., & Levy, Y. (2010, June). A guide for novice researchers: Design and development research methods. In Proceedings of Informing Science & IT Education Conference (InSITE) (pp. 107–117). Informing Science Institute. doi: https://www.informingscience.org/Publications/1435

Fahrezi, A., Salam, F. N., Ibrahim, G. M., Syaiful, R. R., & Saifudin, A. (2022). Pengujian Black Box Testing pada Aplikasi Inventori Barang Berbasis Web di PT. AINO Indonesia. *LOGIC: Jurnal Ilmu Komputer dan Pendidikan*, *1*(1), 1-5. doi: https://journal.mediapublikasi.id/index.php/logic/article/view/1262

Gokhale, S., Turcotte, A., & Tip, F. (2021). Automatic migration from synchronous to asynchronous JavaScript APIs. *Proceedings of the ACM on Programming Languages*, *5*(OOPSLA), 1-27, doi: https://doi.org/10.1016/j.jpdc.2025.105130

Habibullah, K. M. Y., Witriyono, H., Wibowo, S. H., & Imanullah, M. (2024). Implementasi Proteksi Session Pada Menu Dan Module Program Alternatif Pengamanan Aplikasi Sim Dprd Kota Bengkulu. *Jurnal Komputer, Informasi dan Teknologi*, *4*(1), 10-10, doi: https://doi.org/10.53697/jkomitek.v4i1.1803

Hadi, S., & Fachri, F. (2025). Implementasi Rancang Bangun Aplikasi Kriptografi Berbasis Web Menggunakan Metode Enkripsi Base-64. *Jati (Jurnal Mahasiswa Teknik Informatika)*, 9(2), 2026-2031, doi: https://mail.ejournal.itn.ac.id/index.php/jati/article/view/12789

Hindra, F., & Ali, H. (2023). Peran Teknologi Informasi, Sumber Daya Manusia Dan Komunikasi Terhadap Implementasi Enterprise Information System (EIS). *Jurnal Ekonomi Manajemen Sistem Informasi*, *5*(1), 18-27. Diakses dari https://search.ebscohost.com/login.aspx

International Business Machines Corporation (IBM)**.** (2021, 14 Oktober). *Java*. IBM Think. Diakses 12 Juni 2025, dari https://www.ibm.com/think/topics/java

International Organization for Standardization. (1989). *Open Systems International Organization for Standardization. (1989). Open systems interconnection: Security architecture (ISO 7498-2).* ISO. Diakses dari https://www.iso.org/standard/14256.html

Kim, S. H., & Huarng, K. H. (2011). Winning strategies for innovation and high-technology products management. *Journal of Business Research*, *64*(11), 1147-1150. Diakses dari https://www.sciencedirect.com/science/article/abs/pii/S0148296311002001

Khodayari, S., & Pellegrino, G. (2022, May). The state of the samesite: Studying the usage, effectiveness, and adequacy of samesite cookies. In 2022 IEEE symposium on security and privacy (SP) (pp. 1590-1607). IEEE. doi: doi: 10.1109/SP46214.2022.9833637

Lamothe, M., Guéhéneuc, Y. G., & Shang, W. (2020). A systematic review of API evolution literature. *ACM Computing Surveys (CSUR)*, *54*(8), 1-36. doi: https://doi.org/10.1145/3470133

Laipaka, R. (2022). Penerapan JWT untuk Authentication dan Authorization pada Laravel 9 menggunakan Thunder Client. In *Seminar Nasional Corisindo*. doi: https://corisindo.stikom-bali.ac.id/penelitian/index.php/semnas/article/view/91

Lisgiani, R., & Nurmajid, S. (2022). Implementasi autentikasi dari sisi backend pada arsitektur microservices menggunakan Express JS. *Infotronik: Jurnal Teknologi Informasi dan Elektronika, 7*(1), 27–32. doi: https://journal.mediapublikasi.id/index.php/logic/article/view/1262

Madhiyono, M., Kosasi, S., & David, D. (2021). Implementasi JWT, Fingerprint dan Algoritma Haversine Dalam Aplikasi Presensi Mahasiswa. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, *10*(3), 328-333, doi: https://doi.org/10.32736/sisfokom.v10i3.1292

Masse, M. (2011). *REST API design rulebook*. USA: O'Reilly Media.

Matias, M., Ferreira, E., Mateus-Coelho, N., Ribeiro, O., & Ferreira, L. (2024). Evaluating effectiveness and security in microservices architecture. *Procedia Computer Science, 237*, 626–636, doi: https://doi.org/10.1016/j.procs.2024.05.148

Melyani, R. I., Rosita, R., & Aji, S. (2023). Pengembangan Sistem Informasi Penggajian Berbasis Web Menggunakan Framework Laravel dengan Metode Agile Software Development. *Jurnal Sistem Informasi Akuntansi (JASIKA)*, *3*(1), 31-36. doi: https://doi.org/10.31294/jasika.v3i01.2195

Nugroho, A. Y. (2015). Pembuatan aplikasi kriptografi algoritma base64 menggunakan PHP untuk mengamankan data teks. In *Seminar Nasional Informatika (SemnasIF)* (pp. 134–139). doi: https://d1wqtxts1xzle7.cloudfront.net/62240494/255-63

Nugroho, T. A., Hadiana, A. I., & Anggoro, S. (2023). Keamanan Berbasis Service Oriented Architecture Menggunakan Oauth 2.0 dan Json Web Token. *IJESPG (International Journal of Engineering, Economic, Social Politic and Government)*, *1*(3), 229-236. doi: https://ijespgjournal.org/index.php/ijespg/article/view/56

OWASP. (2023). *OWASP Top 10 API Security Risks – 2023*. OWASP API Security. [Online] Diakses dari https://owasp.org/API-Security/editions/2023/en/0x11-t10/

Pranoto, S., Sutiono, S., & Nasution, D. (2024). Penerapan UML Dalam Perancangan Sistem Informasi Pelaporan Dan Evaluasi Pembangunan Pada Bagian Administrasi Pembangunan Sekretariat Daerah Kota Tebing Tinggi. *Surplus: Jurnal Ekonomi dan Bisnis*, *2*(2), 384-401. Diakses dari https://yptb.org/index.php/sur/article/view/866

Praniffa, A. C., Syahri, A., Sandes, F., Fariha, U., Giansyah, Q. A., & Hamzah, M. L. (2023). Pengujian Black Box Dan White Box Sistem Informasi Parkir Berbasis Web Black Box and White Box Testing of Web-Based Parking Information System. *J. Test. dan Implementasi Sist. Inf*, *1*(1), 1-16. doi: https://doi.org/10.55583/jtisi.v1i1.321

Prasetyo, S. E. (2024). Evaluasi Kerentanan Insecure Direct Object Reference pada Aplikasi Pendaftaran Sidang Universitas XYZ. *Journal of Applied Computer Science and Technology*, *5*(2), 165-171. doi: https://doi.org/10.52158/jacost.v5i2.873

Pratama, Arie & Linawati, Linawati & Sastra, Nyoman Putra. (2018). Token-based Single Sign-on with JWT as Information System Dashboard for Government. *Telkomnika (Telecommunication Computing Electronics and Control)*. *16*. 1745-1751. doi: 10.12928/TELKOMNIKA.v16i4.8388.

Purnama, S., Kamal, M., & Yadila, A. B. (2023). Application of RESTful Method with JWT Security and Haversine Algorithm on Web Service-Based Teacher Attendance System. *International Transactions on Artificial Intelligence*, *2*(1), 33-39. doi: https://doi.org/10.33050/italic.v2i1.400

Ramadhan, I. N., Saraswati, G., & ini berlisensi di bawah Creative, K. (2024). Penerapan database redis sebagai optimalisasi pemrosesan kueri data pengguna aplikasi siresma berbasis laravel: Implementation of the redis database as optimization of user. *Technomedia Journal*, *8*(3), 394-406. Diakses dari https://ijc.ilearning.co/index.php/TMJ/article/download/2152/786

Rasyada, N. (2022). SHA-512 Algorithm on Json Web Token for Restful Web Service-Based Authentication. *Journal of Applied Data Sciences*, *3*(1), 33-43. doi: https://doi.org/10.47738/jads.v3i1.51

Richey, R. C., & Klein, J. D. (2007). *Design and development research: Methods, strategies, and issues*. New York: Routledge.

Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Dinamik*, *10*(3). 160-167.

Senapartha, I. K. D. (2021). Implementasi Single Sign-On Menggunakan Google Identity, REST dan OAuth 2.0 Berbasis Scrum. *Jurnal Teknik Informatika dan Sistem Informasi*, *7*(2), 307-320. doi: https://doi.org/10.28932/jutisi.v7i2.3437

Setiawan, A., & Purnamasari, A. I. (2020). Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk Otentikasi Aplikasi BatikKita. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(6), 1036-1045. Diakses dari http://jurnal.iaii.or.id

Shikhverdiyev, I., Babayev, E., Rahimli, C., Rahimli, N., & Aslanova, H. (2024). Secure authentication in e-government 2.0: a comparative analysis of traditional session-based and modern jwt-based authentication. *International*

Science Journal of Engineering & Agriculture, *3*(6), 117-129. doi: https://doi.org/10.46299/j.isjea.20240306.12

Shofiana, D. A., Mardiansyah, S. S., Parabi, M. I., & Syarif, A. (2024). Implementasi REST API Menggunakan JSON WEB Token (JWT) Pada Sistem Monitoring KPI Berbasis Mobile di PT Industri Kereta API (Persero). *Jurnal Komputasi*, 12(2), 101-111. doi: https://doi.org/10.23960/komputasi.v12i2.272

Sianturi, E. M. P., Sandy, R. R., & Najaf, A. R. E. (2023, November). Rancang bangun REST API aplikasi Blues untuk mempermudah bisnis food & beverage. In *Prosiding Seminar Nasional Teknologi dan Sistem Informasi* (pp. 68–77). doi: https://doi.org/10.33005/sitasi.v3i1.445

Singh, S., & Dandotiya, M. (2023). An Efficient Approach for Mitigating Insecure Direct Object Reference (IDOR) Bug Bounty Method. *Int J Res Appl Sci Eng Technol*, *11*(6), 1803-1813. Diakses dari https://www.researchgate.net/profile/Monika-Dandotiya/publication/371962685

Sugara, V. I., & Sriyasa, I. W. (2024). Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP). *Indonesian Journal of Computer Science*, *13*(2), 3315-3327. doi: https://doi.org/10.33022/ijcs.v13i2.3736

Sunaringtyas, S. U., & Prayoga, D. S. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On. *Edu Komputika Journal*, *8*(1), 48-56. Diakses dari https://www.researchgate.net/publication/361065465

Utami, K. S., Sastra, N. P., & Wiharta, D. M. (2021). Pengembangan Metode Autentikasi pada Sistem Presensi Berbasis Aplikasi Mobile. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(4), 615-623. doi: https://doi.org/10.29207/resti.v5i4.3110

Wagito, W., & Nuryono, A. (2025). Pengembangan Sistem Backup berbasis Backup Flow Microservice Dan GRPC Menggunakan Cloud Computing. *JIKO (Jurnal Informatika dan Komputer)*, *9*(1), 204-211. doi: https://doi.org/10.29207/resti.v5i4.3110

Wijayanti, Y., Emanuel, A. W., Hidayat, A. T., & Widodo, T. (2024). Perancangan Arsitektur Enterprise Sistem Informasi Pengelolaan Kerja Praktik dan Tugas Akhir menggunakan TOGAF. *Jurnal Janitra Informatika dan Sistem Informasi*, *4*(1), 47-53. doi: https://doi.org/10.59395/janitra.v4i1.182

Winanda, M., Defrianti, S., Nabila, W., Rikarni, R., & Alfarizhi, H. (2025). Implementasi Fungsi Hash dalam Kriptografi Modern untuk Enkripsi Data Satu Arah. *JIKUM: Jurnal Ilmu Komputer*, *1*(1), 17-21. Winanda, M., Defrianti, S., Nabila, W., Rikarni, R., & Alfarizhi, H. (2025). Implementasi Fungsi Hash dalam Kriptografi Modern untuk Enkripsi Data Satu Arah. *JIKUM: Jurnal Ilmu Komputer*, *1*(1), 17-21. doi: https://doi.org/10.62671/jikum.vxix.xxxx

Wu, X., & Zhu, H. (2016). Formalization and analysis of the REST architecture from the process algebra perspective. *Future Gener. Comput. Syst.*, 56, 153-168. doi: https://doi.org/10.1016/j.future.2015.09.007

Yolanda, S., & Neneng, N. (2021). Rancang Bangun Sistem Informasi untuk Perhitungan Biaya Sewa Kontainer Pada PT Java Sarana Mitra Sejati. *Jurnal Ilmiah Sistem Informasi Akuntansi*, *1*(1), 24-34. Diakses dari https://www.academia.edu/download/90925195/314.pdf

Yuricha, Y., & Phan, I. K. (2023). Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud: The Implementation of Role Based Access Control in a Cloud-Based Supply Chain Management System. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *3*(2), 339-348. doi: https://doi.org/10.57152/malcom.v3i2.1259