ANALISIS PERBANDINGAN PERFORMA ALGORITMA EDDSA DAN ECDSA PADA JSON WEB TOKEN DALAM MEKANISME AUTENTIKASI RESTFUL *WEB SERVICE*

SKRIPSI

diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana komputer pada Program Studi Rekayasa Perangkat Lunak

Oleh

Fajar Nashirul Haq

1903751

UNIVERSITAS PENDIDIKAN INDONESIA

KAMPUS UPI DI CIBIRU

PROGRAM STUDI REKAYASA PERANGKAT LUNAK

2023

ANALISIS PERBANDINGAN PERFORMA ALGORITMA EDDSA DAN ECDSA PADA JSON WEB TOKEN DALAM MEKANISME AUTENTIKASI RESTFUL *WEB SERVICE*

Oleh

Fajar Nashirul Haq

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Komputer Program Studi Rekayasa Perangkat Lunak

HALAMAN PENGESAHAN

Fajar Nashirul Haq

ANALISIS PERBANDINGAN PERFORMA ALGORITMA EDDSA DAN ECDSA PADA JSON WEB TOKEN DALAM MEKANISME AUTENTIKASI RESTFUL *WEB SERVICE*

disetujui dan disahkan oleh pembimbing:

Pembimbing I

Dian Anggraini, S.ST., M.T.

NIP. 920190219930526201

Pembimbing II

Raditya Muhammad, S.T., M.T.

NIP 920190219920507101

Mengetahui,

Ketua Program Studi Rekayasa Perangkat Lunak

Mochamad Iqbal Ardimansyah, S.T., M.Kom.

NIP 920190219910328101

PERNYATAAN KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi dengan judul "Analisis Perbandingan Performa Algoritma EdDSA Dan ECDSA Pada Json Web Token Dalam Mekanisme Autentikasi *Web Service*" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, 03 Agustus 2023

Fajar Nashirul Haq

NIM 1903751

HALAMAN UCAPAN TERIMAKASIH

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Perbandingan Performa Algoritma EdDSA Dan ECDSA Pada Json Web Token Dalam Mekanisme Autentikasi *Web Service*" tepat pada waktunya. Pada kesempatan ini, penulis mengucapkan terima kasih kepada seluruh pihak yang selalu mendukung sehingga skripsi ini dapat terselesaikan. Dalam hal ini, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Solehuddin, M.Pd., MA., selaku Rektor Universitas Pendidikan Indonesia.
2. Bapak Prof. Dr. Deni Darmawan, S.Pd., M.Si., MCE., selaku Direktur Universitas Pendidikan Indonesia Kampus Cibiru.
3. Bapak M. Iqbal Ardimansyah, S.T., M.Kom., selaku dosen pembimbing akademik dan kepala program studi Rekayasa Perangkat Lunak yang telah banyak membantu segala bentuk administrasi penulis selama menjalani perkuliahan.
4. Ibu Dian Anggraini, S.ST., M.T., selaku dosen pembimbing skripsi pertama yang telah meluangkan banyak waktu untuk mengarahkan penelitian penulis.
5. Bapak Raditya Muhammad, S.T., M.Kom., selaku dosen pembimbing skripsi kedua yang telah memberikan masukan selama penyusunan penelitian penulis.
6. Seluruh dosen RPL yang telah memberikan banyak sekali ilmu selama penulis menjalani perkuliahan.
7. Kedua orang tua yang selalu mendukung dan mendoakan dari setiap kesulitan yang penulis hadapi.
8. Semua anggota keluarga yang telah memberikan dukungan kepada penulis selama kuliah hingga menyelesaikan skripsi ini.
9. Sahabat-sahabat MA yang telah membersamai dalam perjuangan untuk terus menjadi lebih baik.
10. Teman seperjuangan pada grup WhatsApp yang selalu membersamai dan berkeluh kesah dalam perjuangan semasa kuliah dari awal sampai akhir.

11. Seluruh teman-teman kuliah yang telah memberikan dukungan serta berbagi ilmu yang bermanfaat.
12. Semua orang yang pernah datang dan pergi di kehidupan penulis, yang telah memberikan banyak pelajaran yang begitu berharga.

Ucapan terima kasih penulis persembahkan kepada semua yang telah membantu penulis dalam melakukan penelitian sekaligus penyusunan skripsi ini hingga selesai, semoga kita semua selalu dalam ridho dan lindungan-Nya. Semoga semua kebaikan yang telah diberikan mendapat balasan yang setimpal dari Allah SWT. Aamiin.

Bandung, 03 Agustus 2023

Fajar Nashirul Haq

ANALISIS PERBANDINGAN PERFORMA ALGORITMA EDDSA DAN ECDSA PADA JSON WEB TOKEN DALAM MEKANISME AUTENTIKASI RESTFUL *WEB SERVICE*

ABSTRAK

Autentikasi sangat penting dalam menjaga keamanan sistem dari akses yang tidak berwenang. Autentikasi berbasis token adalah salah satu konsep yang digunakan, dan salah satu implementasi yang dapat diterapkan adalah JSON Web Token (JWT). JWT dalam mekanismenya mencakup proses kriptografi dengan algoritma-algoritma terntentu, seperti algoritma tanda tangan maupun *hash*. Namun, algoritma-algoritma kriptografi tanda tangan yang umum digunakan dalam JWT, seperti HMAC (*Hash Message-based Authentication Code*), RSA (*Rivest Shamir Adleman*), dan ECDSA (*Elliptic Curve Digital Signature Algorithm*) memiliki kekurangan dalam aspek keamanan dan performa komputasi. Penelitian ini menganalisis performa algoritma tanda tangan *Edwards-Curve Digital Signature Algorithm* (EdDSA) sebagai algoritma alternatif JWT dengan melakukan perbandingan terhadap algoritma ECDSA. Pengujian dilakukan pada aplikasi RESTful *web service E-Commerce* dengan nama WAFO. Pengujian dilakukan dalam dua tahap, yaitu generasi token dan verifikasi token, serta membandingkan EdDSA dan ECDSA pada tiga tingkatan beban pengguna: 50, 150, dan 250 pengguna. Parameter atau metrik yang digunakan berupa waktu respons, *throughput* dan *utilization* (CPU dan memori). Dari hasil pengujian, EdDSA menunjukkan beberapa keunggulan pada parameter waktu respons, penggunaan CPU, dan penggunaan memori, terutama pada beban 50 pengguna pada masing-masing tahap uji. Selisih waktu respons masing-masing sebesar 6,34% dan 0,16%, perbedaan penggunaan CPU masing-masing adalah 5,67% dan 1,84%, sementara perbedaan penggunaan memori adalah 0,11% dan 0,21%. Sementara itu, pada *throughput*, EdDSA hanya unggul pada beban 150 pengguna pada kedua tahap, dengan selisih sebesar 0,49% dan 0,10%. Dari hasil pengujian ini, EdDSA menunjukkan performa yang kompetitif dan memiliki beberapa keunggulan dibandingkan dengan ECDSA.

Kata kunci: JSON Web Token (JWT), EdDSA, ECDSA, RESTful *Web Service*, Pengujian Performa

COMPARISON ANALYSIS OF EDDSA AND ECDSA ALGORITHM PERFORMANCE ON JSON WEB TOKEN IN RESTFUL WEB SERVICE AUTHENTICATION MECHANISM

ABSTRACT

Authentication is crucial in safeguarding systems from unauthorized access. Token-based authentication is one of the utilized concepts, with JSON Web Token (JWT) being a viable implementation. In its mechanism, JWT encompasses cryptographic processes involving specific algorithms, such as signature and hash algorithms. However, the commonly used cryptographic signature algorithms within JWTs, like HMAC (Hash Message-based Authentication Code), RSA (Rivest Shamir Adleman), and ECDSA (Elliptic Curve Digital Signature Algorithm), have limitations in terms of security and computational performance. This research analyzes the performance of the Edwards-Curve Digital Signature Algorithm (EdDSA) as an alternative JWT signature algorithm by conducting a comparison against the ECDSA algorithm. Testing was performed on the E-Commerce RESTful web service application named WAFO. The testing took place in two phases, namely token generation and token verification, and compared EdDSA and ECDSA across three user load levels: 50, 150, and 250 users. The parameters or metrics utilized consisted of response time, throughput, and utilization (CPU and memory). From the test results, EdDSA exhibited several advantages in the parameters of response time, CPU usage, and memory usage, particularly at a user load of 50 for each test phase. The respective response time differences were 6.34% and 0.16%, with CPU usage differences of 5.67% and 1.84%, while memory usage differences were 0.11% and 0.21%. Meanwhile, in terms of throughput, EdDSA only excelled at a user load of 150 in both phases, with differences of 0.49% and 0.10%. Based on these test results, EdDSA demonstrated competitive performance and various advantages over ECDSA.

Keywords: **JSON Web Token (JWT), EdDSA, ECDSA, RESTful** ***Web Service, Performance Testing***

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Aggarwal, S., & Kumar, N. (2021). Digital Signatures. In *Advances in Computers*, *121*(1), 95-107.

Aldya, A. P., Rahmatulloh, A., & Arifin, M. N. (2019). Stateless Authentication with JSON Web Tokens using RSA-512 Algorithm. *Jurnal Infotel*, *11*(2), 36.

Alkhulaifi, A., & El-Alfy, E. S. M. (2020). Exploring Lattice-based Post-Quantum Signature for JWT Authentication: Review and Case Study. *IEEE Vehicular Technology Conference*, *1*(1), 1–5.

Barenghi, A., Bertoni, G., Palomba, A., & Susella, R. (2011). A Novel Fault Attack Against ECDSA. *2011 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2011*, (1), 161–166.

Bhuiyan, T., Begum, A., Rahman, S., & Hadid, I. (2018). API Vulnerabilities: Current Status and Dependencies. *International Journal of Engineering and Technology (UAE)*, *7*(2), 9–13.

Edy, E., Ferdiansyah, F., Pramusinto, W., & Waluyo, S. (2019). Pengamanan Restful API Menggunakan JWT Untuk Aplikasi Sales Order. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *3*(2), 106–112.

Ehsan, A., Abuhaliqa, M. A. M. E., Catal, C., & Mishra, D. (2022). RESTful API Testing Methodologies: Rationale, Challenges, and Solution Directions. *Applied Sciences (Switzerland)*, *12*(9), 1-16.

Emadinia, T., Moghaddam, F. F., Wieder, P., Dabbaghi, S., & Yahyapour, R. (2019). An Updateable Token-Based Schema for Authentication and Access Management in Clouds. *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, *1*(1), 50–56.

Felício, D., Simão, J., & Datia, N. (2023). RapiTest : Continuous Black-Box Black of RESTful RESTful Web APIs RapiTest : Continuous. *Procedia Computer Science*, *219*(2022), 537–545.

Gunawan, R., dan Rahmatulloh, A. (2019). JSON Web Token (JWT) untuk Authentication Pada Interoperabilitas Arsitektur Berbasis RESTful Web Service.

Jurnal Edukasi dan Penelitian Informatika (JEPIN), *5*(1), 74-79.

Gupta, P., Sinha, A., Kr. Srivastava, P., Perti, A., & Singh, A. K. (2021). Security Implementations in Iot Using Digital Signature. *Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2020*. *661*, 523-535.

Haekal, M., & Eliyani. (2016). Token-based Authentication Using JSON Web Token on SIKASIR RESTful Web Service. *2016 International Conference on Informatics and Computing, ICIC 2016*, *1*(1), 175–179.

He, X., & Yang, X. (2017). Authentication and Authorization of End User in Microservice Architecture. *Journal of Physics: Conference Series*, *910*(1), 1-9.

Hendayun, M., Ginanjar, A., & Ihsan, Y. (2023). Analysis Of Application Performance Testing Using Load Testing And Stress Testing Methods In Api Service. *Jurnal Sisfotek Global*, *13*(1), 28–34.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36–63.

Josias, N., & Eugène, G. S. (2020). Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm. *Proceedings of CARI*, *October 2020*.

Kaur, R., & Kaur, A. (2012). Digital signature. *2012 International Conference on Computing Sciences*, 295–301.

Lawi, A., dan Panggabean, B. L. E. (2021). Evaluating GraphQL and REST API Services Performance in a Massive and Intensive Accessible Information System. *Computers 2021*, *10*, 138.

Lee, S., Jo, J. Y., dan Kim, Y. (2015). A Method for secure RESTful web service. *2015 IEEE/ACIS 14th International Conference on Computer and Information Science, ICIS 2015 - Proceedings*, 77–81.

Lenka, R. K., Mamgain, S., Kumar, S., & Barik, R. K. (2018). Performance Analysis of Automated Testing Tools: JMeter and TestComplete. *Proceedings - IEEE 2018 International Conference on Advances in Computing, Communication Control and Networking, ICACCCN 2018*, 399–407.

Neumann, A., Laranjeiro, N., & Bernardino, J. (2021). An Analysis of Public REST

Web Service APIs. *IEEE Transactions on Services Computing*, *14*(4), 957–970.

Pezoa, F., Reutter, J. L., Suarez, F., Ugarte, M., & Vrgoč, D. (2016). Foundations of JSON Schema. *25th International World Wide Web Conference, WWW 2016*, 263–273.

Rahmatulloh, A., Gunawan, R., dan Nursuwars, F. M. S. (2019). Performance comparison of signed algorithms on JSON Web Token. *IOP Conference Series: Materials Science and Engineering*, *550*(1).

Rahmatulloh, A., Sulastri, H., dan Nugroho, R. (2018). Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, *7*(2).

Ramdani, F. C., Rahmatulloh, A., Shofa, R. N., Nomor, J. S., Tasikmalaya, J., & Barat, I. (2023). Implementasi JSON Web Tokenpada Authenticationdengan Algoritma HMAC SHA-256. *SISTEMASI:Jurnal Sistem Informasi Volume 12*, *Nomor 1*, *Januari 2023: 194-205*, *12*(1), 2540–9719.

Rodas-Silva, J., Galindo, J. A., Garcia-Gutierrez, J., dan Benavides, D. (2019). Selection of Software Product Line Implementation Components Using Recommender Systems: An Application to Wordpress. *IEEE Access*, *7*, 69226–69245.

Sabir, B. E., Youssfi, M., Bouattane, O., dan Allali, H. (2019). Authentication and load balancing scheme based on JSON Token for Multi-Agent Systems. *Procedia Computer Science*, *148*, 562–570.

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), 4–10.

Steward, S., Callaghan, J., dan Rea, T. (1999). The eCommerce Revolution. *BT technology journal*, *17*(2), 124–123.

Tijms, A., Bais, T., & Keil, W. (2022). The Definitive Guide to Security in Jakarta EE. In *The Definitive Guide to Security in Jakarta EE*.

Toradmalle, D., Singh, R., Shastri, H., Naik, N., dan Panchidi, V. (2019). Prominence of ECDSA over RSA digital signature algorithm. *Proceedings of the International*

Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018, 253–257.

Varchola, M., Drutarovsky, M., Repka, M., dan Zajac, P. (2016). Side channel attack on multiprecision multiplier used in protected ECDSA implementation. *2015 International Conference on ReConFigurable Computing and FPGAs, ReConFig 2015*.

Wang, J., & Wu, J. (2019). Research on performance automation testing technology based on JMeter. *Proceedings - 2019 International Conference on Robots and Intelligent System, ICRIS 2019*, 55–58.