UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Rancang Bangun Library Web Token Untuk Enkripsi HTTP Data Menggunakan Eksklusif-OR (XOR)

Oleh:

Bagus Dwi Kurniawan,

Mochamad Alfan Rosid

Progam Studi Informatika

Universitas Muhammadiyah Sidoarjo

April, 2023

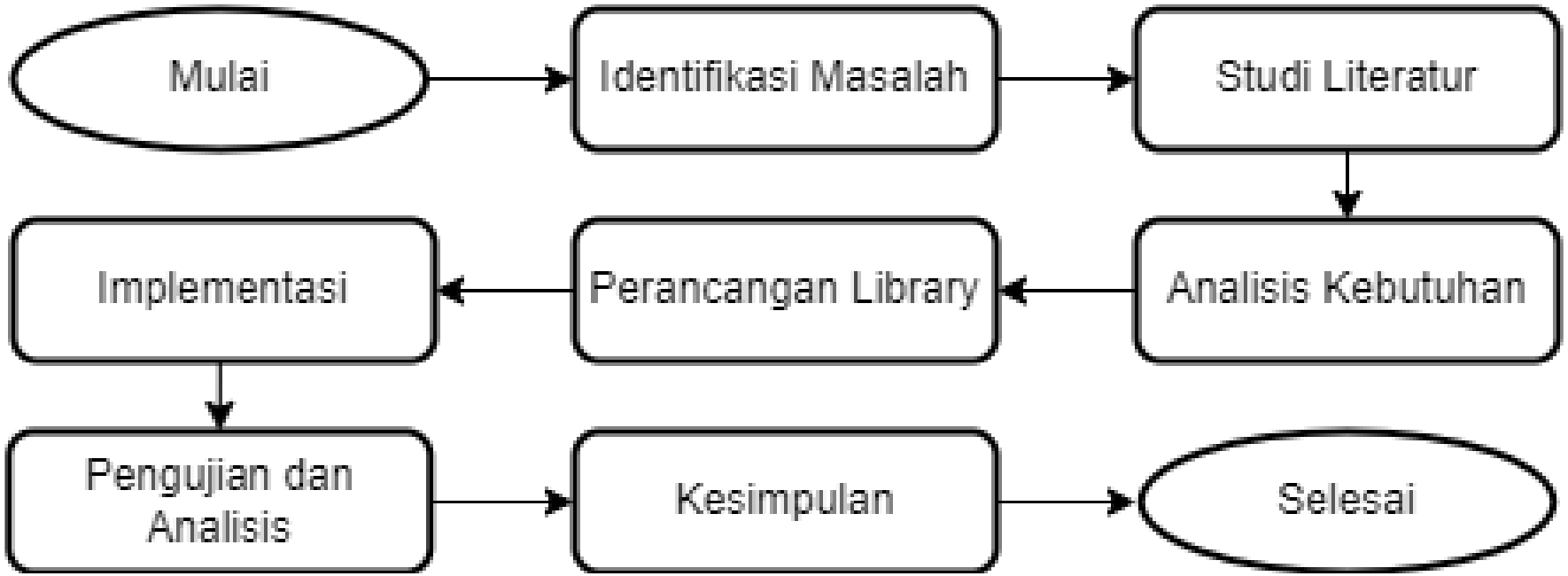
Pendahuluan

Meningatnya peretasan data akhir ini khususnya di Indonesia menjadi suatu masalah yang menakutkan. Karena data adalah suatu hal yang sensitif. Mengamankan data khususnya pada pertukaran data diperlukan pengamanan dengan cara mengengkripsi. Ada permasalahan yang dialami ketika tanpa adanya mekanisme token tanda tangan digital. server memerlukan penyimpanan yang lebih besar, tidak mendukung arsitektur aplikasi yang terdistribusi.

Pertanyaan Penelitian (Rumusan Masalah)

- Bagaimana cara menerapkan algoritma XOR pada pertukaran http data?
- Bagaimana menjaga integritas Token yang telah dibuat?
- Apakah program ini dapat menjadi alternatif untuk membantu para pengembang (*developer*) dalam melakukan pengamanan pertukaran http data?

Metode


Mulai
Identifikasi Masalah
Studi Literatur
Analisis Kebutuhan
Perancangan Library
Implementasi
Pengujian dan Analisis
Kesimpulan
Selesai

Hasil

Tabel 4. Pengujian Kecepatan 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
XORJWT	0.0024	0.0049	0.00779	0.01151	0.01732	0.02440	0.03196	0.05537	0.06822	0.08102	0.11131	0.11802	0.14634	0.16840	0.19138
	0.0043	0.0061	0.00903	0.01177	0.01483	0.01963	0.02476	0.04214	0.05329	0.07727	0.12204	0.11229	0.12382	0.15652	0.16656

Tabel 5. Pengujian Kecepatan 2

	50	60	70	80	90	100
XOR	0.00253	0.00258	0.00284	0.00318	0.00309	0.00324
JWT	0.00420	0.00438	0.00448	0.00416	0.00488	0.00493

Pembahasan

Kesimpulan dari kedua pengujian yang dilakukan memperlihatkan bahwa operasi XOR dan BLAKE2b lebih efisien dalam kondisi field dan panjang data yang lebih kecil. Ini dikarenakan algoritma hash BLAKE2b menghasilkan hasil hash dengan ukuran yang lebih kecil.

Manfaat Penelitian

Dari penelitian ini ada manfaat yang bisa di ambil adalah sebagai berikut:

- 1. Dapat dijadikan sebagai bahan referensi dalam melakukan pengamanan saat pertukaran data dari client ke server ataupun sebaliknya dan mempermudah jalannya pengembangan aplikasi dari sisi keamanan.
- 2. Memberikan alternatif algoritma yang aman, cepat dalam performance dan efektif dalam menjaga keamanan data pada proses transfer data yang sensitif dan penting
- 3. Menambah pengetahuan dan pemahaman tentang teknik XOR serta BLAKE2b dalam keamanan data.

Profile Validator

Nikko Enggaliano Pratama

Sertifikasi

- Certified Red Team Professional
- Certified AppSec Practitioner (CAP)
- Penetration Testing, Incident Response and Forensics
- Certified Network Security Specialist
- Certified Secure Computer User
- OffSec Certified Professional (OSCP)

Referensi

- [1] M. Betty Yel and M. K. M Nasution, “Keamanan Informasi Data Pribadi Pada Media Sosial,” *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, [Online]. Available: http://jurnal.kaputama.ac.id/index.php/JIK/article/view/768.
- [2] F. P. Nugroho, R. W. Abdullah, S. Wulandari, and Hanafi, “Keamanan Big Data di Era Digital di Indonesia,” *J. Inf.*, vol. 5, no. 1, pp. 28–34, 2019.
- [3] R. Rosdiana, “Sekuritas Sistem Dengan Kriptografi,” *Al-Khwarizmi J. Pendidik. Mat. dan Ilmu Pengetah. Alam*, vol. 3, no. 1, 2018, doi: 10.24256/jpmipa.v3i1.216.
- [4] Suparyanto dan Rosad, “IMPLEMENTASI ALGORITMA AES DAN ALGORITMA XOR PADA APLIKASI ENKRIPSI DAN DEKRIPSI TEKS BERBASIS ANDROID,” *Suparyanto dan Rosad*, vol. 5, no. 3, pp. 248–253, 2020.
- [5] A. R. Pratama, M. H. H. Ichsan, and A. Kusyanti, “Implementasi Algoritme AES Pada Pengiriman Data Sensor DHT11 Menggunakan Protokol Komunikasi HTTP,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 4, pp. 3781–3789, 2019.
- [6] C. Mainka, V. Mladenov, T. Guenther, and J. Schwenk, “Automatic recognition, processing and attacking of single sign-on protocols with burp suite,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. 251, pp. 117–131, 2015.
- [7] V. M. Deshpande, M. K. Nair, and D. Shah, “Major Web Application Threats for Data Privacy & Security-Detection, Analysis and Mitigation Strategies,” *Accepted*, vol. 7, no. 10, pp. 182–198, 2017, [Online]. Available: www.ijsrst.com.
- [8] N. F. Sitorus, A. Kusyanti, and A. Bhawiyuga, “Implementasi Autentikasi Berbasis Token Menggunakan Platform Agnostic Security Tokens (PASETO) Sebagai Mekanisme Autentikansi RESTful API,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 11, pp. 3947–3955, 2020, [Online]. Available: http://j-ptiik.ub.ac.id.
- [9] V. Ganesh and B. V. H. Sandilya, “Implementation of SIMD Instruction Set Extension for BLAKE2,” *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, 2019, doi: 10.1109/ICCCNT45670.2019.8944835.


UMSIDA
DARI SINI PENCERAHAN BERSEMI