

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

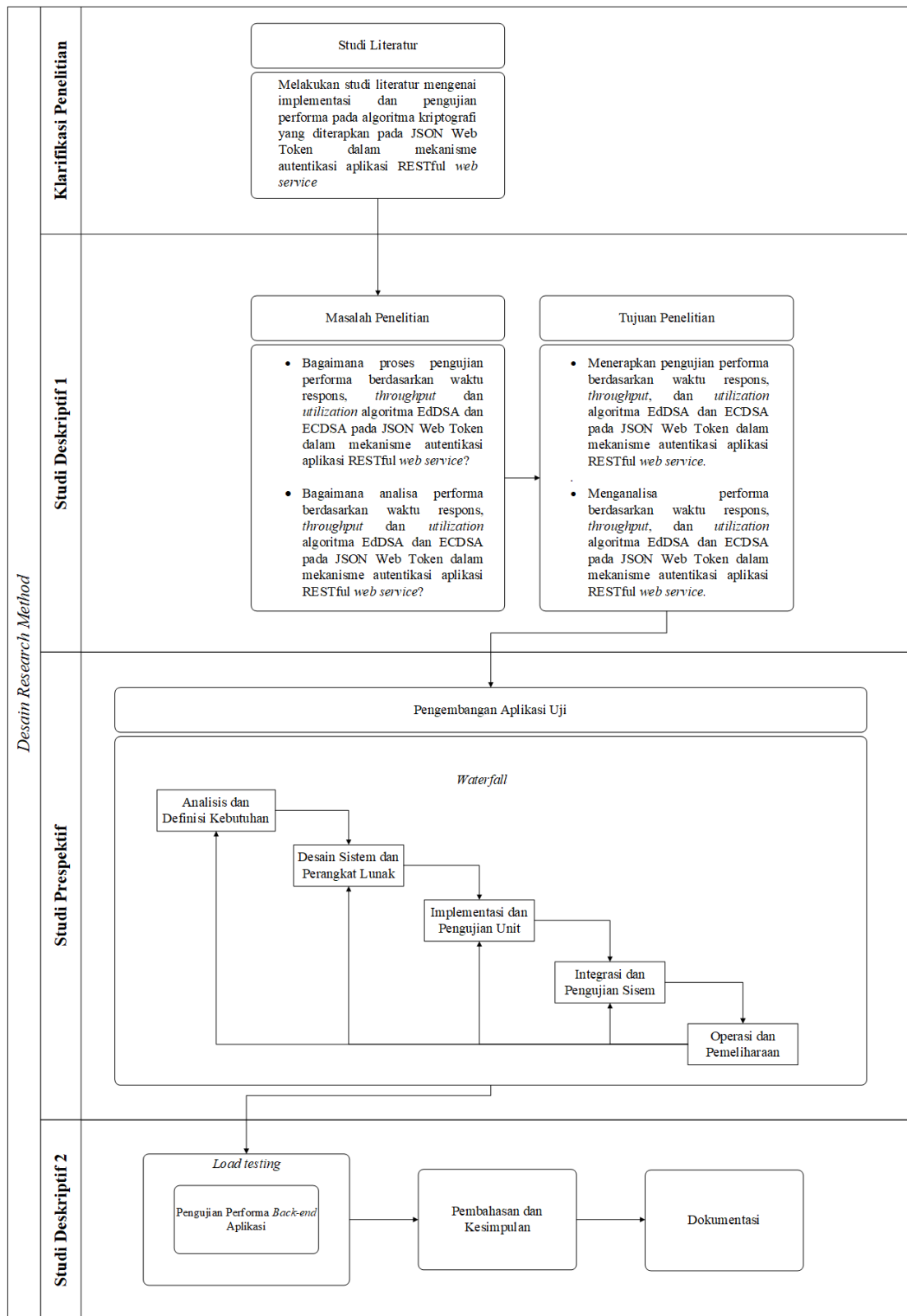
Penelitian akan diawali dengan pembuatan aplikasi RESTful *web service* WAFO yang merupakan aplikasi *E-Commerce* dengan mengimplementasikan mekanisme autentikasi JSON Web Token menggunakan algoritma EdDSA dan ECDSA. Penelitian ini akan menggunakan metode penelitian *Design Research Methodology* (DRM). Tujuan khusus dari DRM adalah sebagai sebuah kerangka kerja desain penelitian untuk membantu mengidentifikasi area penelitian dan mengembangkan argumentasi (lihat Blessing dan Chakrabati, 2009). Desain penelitian yang dibentuk dapat dilihat pada Gambar 3.1.

3.1.1. Klarifikasi Penelitian

Studi literatur dilakukan sebagai tahap awal guna mendapatkan pemahaman mengenai masalah yang akan diangkat menjadi topik penelitian. Dalam hal ini penulis mengidentifikasi permasalahan terkait algoritma kriptografi pada JWT yang digunakan dalam mekanisme autentikasi salah satunya pada aplikasi RESTful *web service*. Sumber penelitian terkait juga teori-teori dari berbagai sumber seperti jurnal, dokumen internet serta buku dijadikan sebagai sumber rujukan dalam mengidentifikasi masalah dari topik yang diangkat dan agar penelitian menjadi terarah.

3.1.2. Studi Deskriptif 1

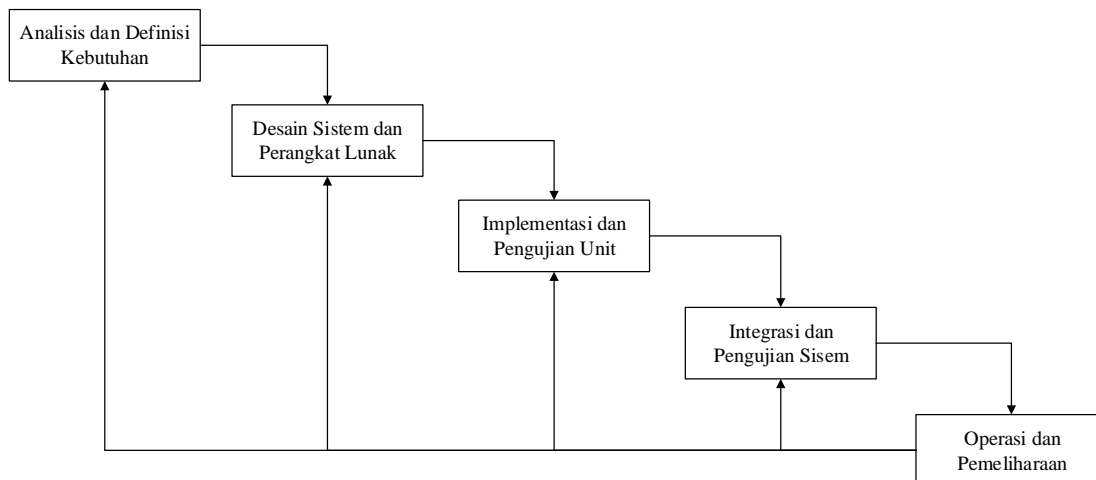
Tahapan berikutnya adalah merumuskan masalah dan tujuan berdasarkan proses yang telah dilakukan pada tahap awal. Hasil dari kajian dari berbagai sumber yang telah dilakukan kemudian dijadikan dasar untuk membuat sebuah rumusan masalah dan tujuan dari penelitian yang akan dilakukan. Rumusan masalah dan tujuan nantinya digunakan sebagai landasan dalam merancang solusi yang akan dilakukan pada penelitian ini.



Gambar 3.1 Desain Penelitian

3.1.3. Studi Prespektif

Tahap ini merupakan proses pengembangan aplikasi uji berdasarkan masalah dan tujuan yang telah dirumuskan pada tahap studi deskriptif 1. Aplikasi uji yang akan dikembangkan berupa RESTful *web service E-Commerce* dengan nama WAFO. Aplikasi menerapkan konsep bisnis *online to offline*. Pengembangan aplikasi uji disesuaikan dengan model fitur sistem *E-Commerce* (Rodas-Silva dkk., 2019). Aplikasi tersebut akan mengimplementasikan mekanisme autentikasi JWT menggunakan algoritma EdDSA dan ECDSA. Guna pengembangan aplikasi dapat berjalan dengan baik, digunakan model pengembangan perangkat lunak yaitu *waterfall* (lihat Sommerville, 2011). Model tersebut memiliki beberapa tahapan yang dapat dilihat pada gambar 3.2



Gambar 3.2 Model *Waterfall*

Berikut merupakan penjelasan dari tahap-tahap model *waterfall*:

1. Analisis dan definisi kebutuhan

Melakukan analisis kebutuhan perangkat lunak mengenai aplikasi *E-Commerce* berbasis RESTful *web service* yang akan dibuat mencakup kebutuhan fungsional dan non-fungsional dalam pengembangan aplikasi. Batasan-batasan aplikasi juga didefinisikan pada tahap ini.

2. Desain sistem dan perangkat lunak

Tahap ini mengubah kebutuhan perangkat lunak dari tahapan analisis ke dalam bentuk rancangan agar dapat diimplementasikan menjadi program aplikasi ada tahap

selanjutnya. Desain perangkat lunak melibatkan identifikasi dan deksripsi abstraksi perangkat lunak yang fundamental serta hubungan antara mereka.

3. Implementasi dan pengujian unit

Rancangan desain yang telah dibuat selanjutnya diimplementasikan dalam bentuk kode unit program aplikasi. Tahap ini akan membuat kode program *E-Commerce* berbasis RESTful *web service* yang mengimplementasikan mekanisme autentikasi JWT menggunakan algoritma EdDSA dan algoritma ECDSA. Pengujian unit akan memverifikasi bahwa setiap unit program telah memenuhi spesifikasinya.

4. Integrasi dan pengujian sistem

Unit-unit program pada tahap sebelumnya diintegrasikan dan diuji sebagai sebuah sistem lengkap untuk memastikan bahwa kebutuhan perangkat lunak telah terpenuhi.

5. Operasi dan pemeliharaan

Sistem dijalankan dan digunakan secara praktis. Pemeliharaan melibatkan perbaikan kesalahan yang tidak ditemukan pada tahap sebelumnya, peningkatan implementasi unit sistem, dan penyempurnaan layanan sistem seiring dengan penemuan kebutuhan baru.

3.1.4. Studi Deskriptif 2

Tahap terakhir guna mendapatkan tujuan dari penelitian yang dilakukan, diperlukan proses identifikasi terhadap aplikasi uji yang telah dikembangkan. Proses identifikasi berupa pengujian performa dengan metrik waktu respons, *throughput* dan *utilization* terhadap aplikasi uji yang diimplementasikan mekanisme autentikasi JWT dengan algoritma EdDSA dan mekanisme autentikasi JWT dengan algoritma ECDSA. Pengujian akan dilakukan menggunakan aplikasi JMeter. Hasil pengujian akan dianalisis untuk mengetahui perbedaan performa antara keduanya.

Selanjutnya dari hasil tersebut akan ditarik kesimpulan serta pemaparan kelebihan dan kekurangan dari penelitian yang dilakukan. Pada bagian kesimpulan tercantum jawaban dari rumusan masalah yang telah dibentuk. Selain itu peneliti juga memberikan saran terhadap peneliti selanjutnya agar penelitian dapat ditingkatkan lagi. Tahap akhir adalah dilakukan penyusunan skripsi.

3.2 Alat dan Bahan

3.2.1 Alat Penelitian

Alat yang digunakan dalam penelitian ini terdiri dari perangkat keras dan perangkat lunak. Adapun perangkat keras yang digunakan penulis:

1. Laptop prosesor AMD A8
2. RAM 12 GB DDR4
3. SSD 225 GB + HDD 500 GB

Perangkat lunak yang dibutuhkan dalam penelitian yang dilakukan adalah sebagai berikut:

1. Visual Studio Code
2. Node.js
3. Express
4. Node Package Manager (NPM)
5. Jose
6. Crypto
7. MongoDB
8. Midtrans
9. Microsoft Excel
10. Cloudinary
11. JMeter
12. Postman

3.2.2 Bahan Penelitian

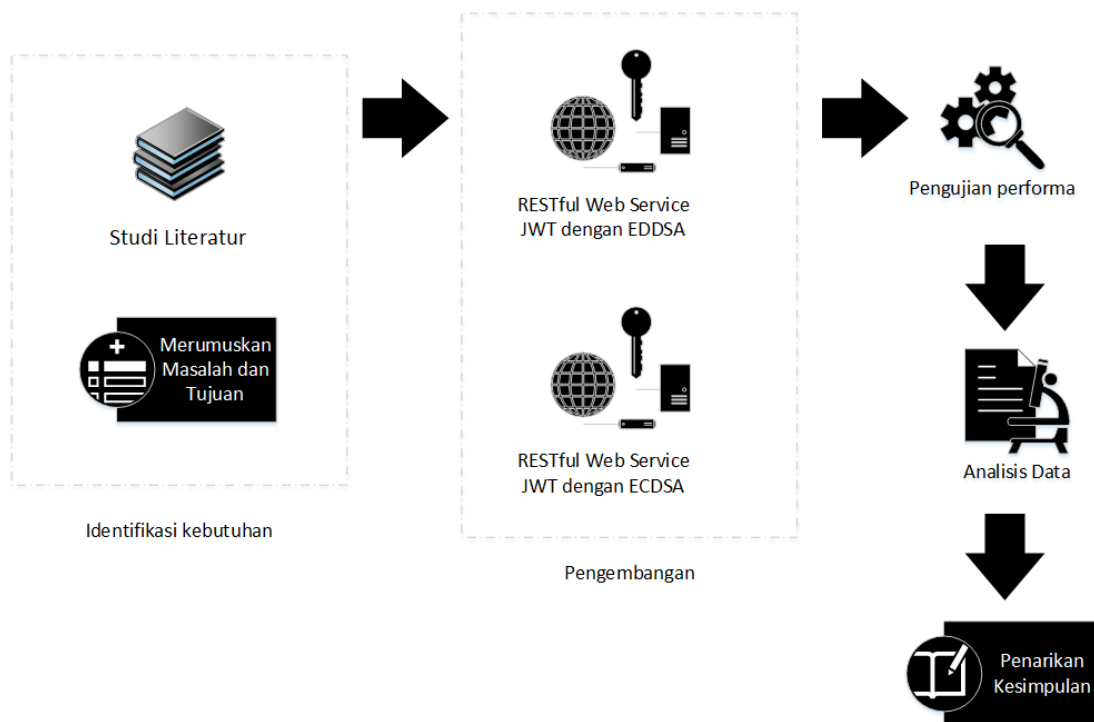
Bahan penelitian berupa jurnal, buku elektronik, dokumen internet, artikel dan lain sebagainya yang berhubungan dengan penelitian sebagai penunjang penulis dalam memahami penelitian serta membangun aplikasi dan melakukan pengujian.

3.3 Instrumen Penelitian

Instrumen penelitian yang akan digunakan pada penelitian ini adalah alat berupa aplikasi JMeter. Aplikasi JMeter dapat digunakan untuk menguji performa sebuah aplikasi RESTful *web service* yang dapat menganalisis berbagai parameter performa (Lenka dkk., 2018). Parameter atau metrik pengujian performa pada penelitian kali ini mengacu pada metrik pengujian performa yaitu berupa waktu respons, *throughput*, dan *utilization* (Wang dan Wu, 2019). Proses pengujian dilakukan pada waktu generasi token JWT dan verifikasi token JWT yang didasari pada penelitian yang dilakukan oleh Rahmatulloh dkk. (2019), dan Alkhulaifi dan El-Alfy (2020).

3.4 Prosedur Penelitian

Prosedur penelitian akan dilakukan berdasarkan desain penelitian yang telah dijabarkan sebelumnya. Adapun secara garis besar penelitian yang akan dilakukan dapat dilihat pada gambar 3.3 berikut.



Gambar 3.3 Prosedur Penelitian

3.5 Analisis Data

Penelitian dirancang untuk dapat mengambil nilai dari parameter pengujian performa yaitu waktu respons, *throughput* dan *utilization* (CPU dan memori). Nilai parameter akan diambil dari aplikasi uji saat menerapkan mekanisme JWT dengan algoritma EdDSA dan ECDSA. Adapun jenis kurva yang digunakan untuk EdDSA adalah Ed25519 dan ECDSA adalah NIST P-256 + SHA 256 (ES256). Kedua jenis kurva tersebut dipilih berdasarkan level atau tingkat keamanan yang sama (lihat NIST.SP.800-152).

Pengujian akan dilakukan pada lingkungan lokal agar menjaga proses pengujian dari variabel-variabel lain seperti masalah koneksi dan lain sebagainya. Penelitian dilakukan pada dua tahap yaitu saat generasi token JWT dan verifikasi token JWT. Metode pengujian yang akan digunakan adalah *load testing* dengan memberikan beban secara bertahap terhadap aplikasi uji. Setiap nilai parameter yang didapatkan akan dibandingkan rata-ratanya pada setiap tahap.