

BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Penelitian yang dilakukan oleh Wicaksana, N. N. (2019) tentang Penerapan Progressive Web Apps untuk Monitoring Status Service di Bengkel OS. Penelitian ini fokus pada penggunaan Progressive Web Apps (PWA) untuk memantau status service laptop di bengkel OS. Meskipun tidak secara langsung membahas JWT atau Golang, studi ini memberikan wawasan tentang pengembangan aplikasi web yang dapat memberikan dasar dalam implementasi sistem autentikasi berbasis JWT dengan pendekatan web.

Penelitian yang dilakukan oleh Daryanto, B., & Sari, E. (2020) tentang Implementasi JSON Web Token untuk Sistem Autentikasi Aplikasi Mobile Menggunakan Framework Golang. Artikel ini membahas penerapan JSON Web Token (JWT) dalam sistem autentikasi untuk aplikasi mobile dengan menggunakan framework Golang. Penelitian ini memberikan pemahaman yang mendalam tentang bagaimana JWT diimplementasikan dalam konteks aplikasi mobile dan menjelaskan mekanisme autentikasi dan otorisasi yang menggunakan JWT

Penelitian yang dilakukan oleh Santoso, D., & Pratama, Y. (2021) tentang Keamanan Autentikasi Berbasis JWT pada Aplikasi Web dengan Golang. Penelitian ini mengkaji aspek keamanan dalam implementasi JWT untuk aplikasi web yang

dikembangkan dengan Golang. Studi ini menyoroti berbagai teknik untuk melindungi token JWT dari serangan dan eksploitasi, serta memberikan rekomendasi praktis untuk meningkatkan keamanan sistem autentikasi berbasis JWT.

Penelitian yang dilakukan oleh Nugroho, S. (2022) tentang Optimalisasi Performansi JWT pada Aplikasi Backend Menggunakan Golang. Artikel ini mengeksplorasi cara-cara untuk mengoptimalkan performansi sistem autentikasi yang menggunakan JWT pada aplikasi backend dengan bahasa pemrograman Golang. Fokus utama dari penelitian ini adalah pada pengelolaan dan pemrosesan token JWT.

Penelitian oleh Fitriani, N., & Ramadhan, A. (2023) tentang Perbandingan Implementasi JWT dan OAuth2 dalam Sistem Autentikasi Aplikasi Berbasis Web dengan Golang. Penelitian ini membandingkan implementasi JWT dengan OAuth2 dalam konteks sistem autentikasi aplikasi berbasis web yang dikembangkan dengan Golang. Hasil dari studi ini memberikan wawasan tentang kelebihan dan kekurangan masing-masing metode autentikasi serta panduan dalam memilih solusi yang tepat berdasarkan kebutuhan aplikasi.

Tabel 2. 1 Tinjauan Pustaka

No.	Penulis	Judul	Metode	Hasil
1	Wicaksana, N. N. (2019)	Penerapan Progressive Web Apps untuk Monitoring Status Service di Bengkel OS	pengembangan perangkat lunak berbasis Progressive Web Apps (PWA)	Aplikasi PWA yang dikembangkan berhasil memudahkan pelanggan untuk memantau status pengerjaan service laptop mereka
2	Daryanto, B., & Sari, E. (2020)	Implementasi JSON Web Token untuk Sistem Autentikasi Aplikasi Mobile Menggunakan Framework Golang	eksperimen untuk mengimplementasikan JSON Web Token (JWT) dalam sistem autentikasi aplikasi mobile	Implementasi JWT dalam sistem autentikasi aplikasi mobile menggunakan Golang menunjukkan bahwa JWT dapat meningkatkan keamanan dan efisiensi autentikasi
3	Santoso, D., & Pratama, Y. (2021)	Keamanan Autentikasi Berbasis JWT pada Aplikasi Web dengan Golang	studi kasus untuk mengkaji keamanan implementasi JWT pada aplikasi web yang dikembangkan dengan Golang	menemukan bahwa implementasi JWT dengan praktik keamanan yang baik dapat mengurangi risiko serangan
4	Nugroho, S. (2022)	Optimalisasi Performansi JWT pada Aplikasi Backend Menggunakan Golang	metode eksperimen untuk mengoptimalkan performansi sistem autentikasi berbasis JWT pada aplikasi backend dengan Golang	dengan mengimplementasikan teknik-teknik optimasi tersebut, performa sistem autentikasi berbasis JWT dapat ditingkatkan secara signifikan
5	Fitriani, N., & Ramadhan, A. (2023)	Perbandingan Implementasi JWT dan OAuth2 dalam Sistem Autentikasi Aplikasi Berbasis Web dengan Golang	komparatif untuk membandingkan implementasi JWT dan OAuth2 dalam sistem autentikasi aplikasi web yang dikembangkan dengan Golang	menemukan bahwa JWT lebih mudah diimplementasikan dan memiliki performa yang lebih baik dibandingkan OAuth2. Namun, OAuth2 menawarkan fitur keamanan yang lebih komprehensif

Tabel 2.1 Tinjauan Pustaka (Lanjutan)

No.	Penulisan	Judul	Metode	Hasil
1	Musa, K. A. (2024)	Sistem Autentikasi Berbasis JWT (JSON Web Token) Menggunakan Bahasa Pemrograman Golang	studi kasus untuk mengkaji keamanan implementasi JWT pada sistem transaksi online yang dikembangkan dengan Golang	Implementasi dari sitem autentikasi berbasis token dapat mengurangi beban server dan juga mengamankan data pengguna

Pada tabel 2.1 Penelitian-penelitian yang dibahas memberikan landasan teori dan praktik yang kuat untuk pengembangan sistem autentikasi berbasis JWT menggunakan Golang. Penelitian tersebut dapat menjadi acuan pembejaraan untuk menerapkan teknologi JWT pada situs penjualan tiket *online*. Perbedaan dari penelitian diatas dengan penelitian yang penulis gunakan yaitu studi kasus pada sistem autentikasi berbasis JWT (JSON Web Token) menggunakan bahasa pemrograman Golang.

2.2 Dasar Teori

2.2.1 Golang

Golang, atau Go, adalah bahasa pemrograman yang dikembangkan oleh Google dan dirancang untuk memenuhi kebutuhan pengembangan perangkat lunak yang cepat dan efisien. Diperkenalkan pada tahun 2009 oleh Robert Griesemer, Rob Pike, dan Ken Thompson, Go mengedepankan kecepatan kompilasi yang tinggi, pengelolaan memori otomatis melalui garbage collection, dan dukungan untuk concurrency dengan menggunakan goroutine dan channel. Go memiliki sintaksis

yang sederhana dan mudah dipahami, menjadikannya pilihan populer untuk pengembangan aplikasi backend, layanan microservices, dan sistem yang membutuhkan performa tinggi. Banyak perusahaan besar seperti Google, Dropbox, dan Docker menggunakan Golang untuk mendukung infrastruktur dan aplikasi mereka, berkat kemampuannya yang handal dalam mengelola skala besar dan kompleksitas sistem (Go Programming Language. (n.d.). *Go programming language*. Retrieved December 3, 2024, from <https://golang.org/>)

2.2.2 Autentikasi

Autentikasi adalah mekanisme yang digunakan untuk memastikan bahwa individu atau sistem yang mengakses suatu layanan adalah pihak yang sah, sering kali dengan memverifikasi kredensial yang diberikan, seperti nama pengguna dan kata sandi. Selain itu, autentikasi dapat mencakup penggunaan metode lain seperti token keamanan atau otentikasi dua faktor (2FA) untuk meningkatkan tingkat keamanan. Autentikasi sering kali diikuti oleh otorisasi, yaitu proses yang menentukan tingkat akses atau izin yang diberikan kepada pengguna setelah berhasil terautentikasi. Proses autentikasi sangat penting untuk melindungi data sensitif dan mencegah akses yang tidak sah dalam sistem yang lebih besar (Techopedia. (2024). *Authentication*. Retrieved December 3, 2024, from <https://www.techopedia.com/definition/5625/authentication>).

2.2.3 Web Service

Web service adalah sebuah sistem atau teknologi yang memungkinkan aplikasi untuk berkomunikasi dan berinteraksi dengan aplikasi lain melalui internet,

tanpa memandang bahasa pemrograman yang digunakan. Teknologi ini mendukung akses melalui berbagai protokol standar, seperti HTTP, SMTP, atau FTP, sehingga memudahkan integrasi antar sistem. Web service bekerja dengan cara menerima permintaan dari aplikasi klien, memprosesnya, dan mengirimkan respon dalam format standar seperti XML atau JSON. Contoh penerapan web service dapat ditemukan pada aplikasi cuaca, layanan peta, dan platform e-commerce yang menggunakan layanan pembayaran online. Dengan kemampuannya untuk menghubungkan aplikasi secara efisien, web service menjadi salah satu fondasi penting dalam pengembangan aplikasi modern. (Dewaweb. 2024. "Apa Itu Web Service?" Retrieved December 19, 2024, from <https://www.dewaweb.com/blog/apa-itu-web-service/>.)

2.2.4 JWT

JWT (JSON Web Token) adalah format token yang digunakan untuk pertukaran data terverifikasi antara dua pihak, seringkali digunakan untuk autentikasi dalam aplikasi web. JWT menyimpan informasi dalam bentuk yang terkodekan, yang dapat dipastikan keasliannya dengan menggunakan signature. Struktur JWT terdiri dari tiga bagian utama: header, payload, dan signature. Header biasanya berisi informasi tentang algoritma yang digunakan untuk menandatangani token, sedangkan payload berisi klaim yang dapat mencakup informasi pengguna atau data lainnya. Signature digunakan untuk memastikan bahwa token tidak diubah setelah dibuat. Keunggulan JWT adalah kemampuannya untuk bekerja secara stateless, yang memungkinkan server untuk tidak perlu menyimpan informasi sesi, karena semua informasi ada dalam token yang dikirim bersama setiap permintaan

(Auth0. (2024). *What is JSON Web Token (JWT)?* Retrieved December 3, 2024, from <https://auth0.com/learn/json-web-tokens>).

2.2.5 Backend

Backend adalah bagian dari aplikasi yang menangani pemrosesan data, logika bisnis, dan interaksi dengan database. Ini mencakup semua komponen yang berjalan di server, seperti server web, database, dan aplikasi pemrograman yang mengelola dan menyajikan data ke frontend. Backend bertugas untuk mengelola permintaan yang datang dari pengguna atau frontend, memprosesnya, dan mengirimkan respons kembali. Teknologi backend sering mencakup berbagai bahasa pemrograman seperti Java, Python, Node.js, serta database SQL dan NoSQL seperti MySQL, PostgreSQL, dan MongoDB (MDN Web Docs. (2024). *Backend web development*. Retrieved December 3, 2024, from <https://developer.mozilla.org/en-US/docs/Learn/Server-side>).

2.2.6 PostgreSQL

PostgreSQL adalah sistem manajemen basis data relasional (RDBMS) sumber terbuka yang dikenal karena kestabilannya, skalabilitasnya, dan kepatuhannya terhadap standar SQL. Dikembangkan pertama kali pada tahun 1986 di Universitas California, Berkeley, PostgreSQL mendukung berbagai fitur canggih, seperti transaksi ACID, integritas data, dan kemampuan untuk menjalankan kueri kompleks. PostgreSQL juga mendukung berbagai tipe data, termasuk data geospasial, JSON, dan XML, serta memungkinkan pengembangan aplikasi yang membutuhkan pengolahan data dalam jumlah besar. Sebagai sistem

yang sangat fleksibel, PostgreSQL digunakan di berbagai industri untuk mengelola dan menyimpan data dalam aplikasi web, layanan cloud, dan aplikasi besar lainnya (PostgreSQL Global Development Group. (2024). *What is PostgreSQL?* Retrieved December 3, 2024, from <https://www.postgresql.org/about/>)

2.2.7 Postman

Postman adalah alat pengujian dan pengembangan API yang memungkinkan pengguna untuk membuat, mengelola, dan menguji API dengan mudah. Alat ini mempermudah pengembang dalam mengirimkan permintaan API dan memeriksa responsnya tanpa perlu menulis kode secara manual. Dengan Postman, pengembang dapat mengatur berbagai jenis permintaan seperti GET, POST, PUT, dan DELETE, serta menambahkan header, parameter, dan body untuk menguji berbagai skenario. Postman juga menyediakan kemampuan untuk mengorganisasi permintaan dalam koleksi, membuat skrip pengujian, dan menghasilkan dokumentasi API secara otomatis, menjadikannya alat yang sangat berguna dalam pengembangan aplikasi berbasis API (Guru99. (2024). *What is Postman? Postman Tutorial for Beginners*. Retrieved December 3, 2024, from <https://www.guru99.com/postman-tutorial.html>).