BAB II

TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Berikut merupakan hasil penelitian terdahulu berdasarkan penelitian yang sudah dilakukan oleh peneliti sebelumnya, ditunjukan pada Tabel 2.1.

Tabel 2.1 Hasil Penelitian Terdahulu

NO	Persamaan Penelitian	Perbedaan Penelitian
1.	Penelitian yang dilakukan oleh (Christian et al., 2023) dan (Cahyadi et al., 2023) terdapat tambahan keamanan pada sistem autentikasi untuk melindungi sistem dan data pengguna dari akses yang tidak sah.	Penelitian yang dilakukan oleh (Christian et al., 2023) menggunakan Algoritma RSA dengan menggunakan metode kriptografi dan penelitian yang dilakukan oleh (Cahyadi et al., 2023) menggunakan algoritma RSA dengan menggunakan bahasa pemrograman Phyton.
2.	Penelitian yang dilakukan oleh (Rizki & Mulyati, 2020) menggunakan pengujian untuk mengetahui kinerja waktu pengiriman OTP dan penelitian yang dilakukan oleh (Hayat et al., 2022) menggunakan kode verifikasi satu kali kirim dan apabila kode verifikasi dimasukan lebih dari satu menit setelah diterima, kode tersebut tidak berlaku.	Penelitian yang dilakukan oleh (Rizki & Mulyati, 2020) menggunakan algoritma SHA-512 dengan menerapkan metode *waterfall development* untuk pengembangan sistem dan penelitian yang dilakukan oleh (Hayat et al., 2022) menggunakan algoritma SHA-256 untuk mengenkripsi data pengguna dan pengiriman kode OTP dapat dikirimkan melalui e-mail.
3.	Penelitian yang dilakukan oleh (Erawan, 2020) mengembangkan sebuah aplikasi web untuk melindungi file data pribadi dan penelitian yang dilakukan oleh (Patidar et al., 2022) menambahkan keamanan autentikasi tambahan setelah proses login.	Penelitian yang dilakukan oleh (Erawan, 2020) menggunakan algoritma *One Time Pad* sebagai proses enkripsi untuk menggunakan password dan penelitian yang dilakukan oleh (Patidar et al., 2022) menggunakan metode *One Time Pad* dengan menggunakan kode QR sebagai autentikasi tambahan yang

		diimplementasikan pada aplikasi GYM.
4	Penelitian yang dilakukan oleh (Nasution et al., 2024) memberikan pedoman praktis kepada pengembang untuk menerapkan verifikasi login yang lebih aman dan efektif ke dalam aplikasi.	Penelitian yang dilakukan oleh (Nasution et al., 2024) menggunakan pengujian penetrasi untuk mengidentifikasi potensi kerentanan dalam sistem dan mendapatkan hasil sistem tersebut memiliki tingkat keamanan yang baik dengan mekanisme perlindungan terhadap serangan man-in-the-middle (MITM).
5	Penelitian yang dilakukan oleh (Alfarizi et al., 2024) berdasarkan pengujian yang telah dilakukan tidak ditemukan kode OTP yang sama yang menunjukan bahwa pengiriman OTP menghasilkan nilai yang benar-benar berbeda.	Penelitian yang dilakukan oleh (Alfarizi et al., 2024) menggunakan metode agile sebagai pengembangan pada aplikasi dan menggunakan *mailtrap* API yang dirancang untuk pengujian e-mail dalam pengembangan perangkat lunak.

B. LANDASAN TEORI

Landasan teori merupakan bagian dari penelitian yang berisi teori-teori dan konsep dasar yang mendasari pembuatan skripsi ini yang bertujuan untuk memberikan panduan dalam menyusun hipotesis, menguatkan penelitian, dan membantu menentukan metode penelitian. Dengan demikian landasan teori berfungsi sebagai landasan yang menjelaskan konsep-konsep utama atau teori-teori yang akan digunakan dalam penelitian.

1. *One Time Password* (OTP)

One Time Password (OTP), yang menggunakan kode yang dibuat secara acak dan hanya berlaku untuk satu sesi *login* atau transaksi, telah digunakan secara luas sebagai metode autentikasi kedua kode. dengan

tujuan untuk membuktikan keaslian seseorang dalam menggunakan suatu sistem (Setiawan et al., 2020). OTP biasanya dikirimkan melalui saluran komunikasi yang aman, seperti SMS, email, atau aplikasi *messenger*, untuk memastikan bahwa hanya pengguna yang memiliki akses ke saluran tersebut yang dapat menerima dan menggunakan kode verifikasi. Implementasi OTP sering kali digunakan sebagai bagian dari autentikasi dua faktor (2FA), yang mengharuskan pengguna untuk memasukkan kode OTP setelah memasukkan kata sandi, sehingga meningkatkan lapisan perlindungan terhadap akun pengguna dari ancaman peretasan atau pencurian data karena dengan menggunakan OTP dapat mengatasi keamanan *login* karena kode ini hanya berlaku dalam waktu yang terbatas dan tidak bisa digunakan kembali.

2. Application Programming Interface (API)

API merupakan alat yang memungkinkan aplikasi dan perangkat lunak untuk saling bertukar data, fitur dan fungsionalitas. API menyederhanakan dan mempercepat pengembangan aplikasi dan perangkat lunak dengan memungkinkan pengembang untuk mengintegrasikan data, layanan, dan kapabilitas dari aplikasi lain, alih-alih mengembangkannya dari awal (Goodwin, 2024). Arsitektur API biasanya dijelaskan dalam kaitanya dengan klien dan *server* Aplikasi yang mengirimkan permintaan disebut sebagai klien dan aplikasi yang mengirimkan respons disebut sebagai *server*. API dapat berupa *web* API, yang memungkinkan komunikasi antar sistem melalui protokol HTTP, atau *library* API, yang memungkinkan

interaksi langsung antara program dengan pustaka perangkat lunak tertentu. Dengan menggunakan API dapat mempercepat pembangunan aplikasi, menghemat waktu, serta memanfaatkan layanan dan fungsi yang telah ada tanpa harus membuatnya dari awal. Dalam konteks layanan seperti WhatsApp API, API memungkinkan untuk mengirim pesan otomatis, termasuk kode OTP, kepada pengguna, yang meningkatkan keamanan dan pengalaman pengguna dalam aplikasi.

3. WhatsApp Sebagai Platform Pengiriman OTP

WhatsApp merupakan aplikasi komunikasi yang memungkinkan *user* dapat berkomunikasi secara langsung baik dengan pesan teks, panggilan suara maupun vidio dan menjadikan WhatsApp menjadi aplikasi yang paling banyak digunakan di dunia. Saat ini, WhatsApp dilaporkan memiliki lebih dari 2 miliar pengguna aktif bulanan di seluruh dunia, termasuk 94,3 juta di Indonesia, dan menduduki peringkat sebagai aplikasi perpesanan seluler terpopuler di dunia (Backlinko, 2024). Salah satu keunggulan utama WhatsApp adalah kemampuannya untuk beroperasi menggunakan koneksi internet (Wi-Fi atau data seluler), sehingga mengurangi biaya komunikasi dibandingkan dengan SMS atau panggilan telepon tradisional. WhatsApp juga dikenal dengan fitur enkripsi end-to-end yang memastikan bahwa pesan yang dikirim hanya dapat dibaca oleh pengirim dan penerima, memberikan tingkat keamanan yang tinggi. WhatsApp juga memungkinkan untuk dengan mudah mengintegrasikan API ke dalam aplikasi atau layanan yang sudah ada dengan menggunakan

WhatsApp Bussines API, tanpa perlu membangun infrastuktur baru dari awal. Karena popularitasnya yang besar dan infrastruktur pengiriman pesannya yang cepat, WhatsApp adalah platform terbaik untuk pengiriman OTP.

4. **Integrasi API WhatsApp**

Integrasi API WhatsApp memungkinkan pengembang untuk menambahkan fitur WhatsApp ke dalam aplikasi atau sistem yang sedang dikembangkan. Hal ini sangat berguna bagi bisnis dan organisasi untuk meningkatkan interaksi dengan pelanggan. Dengan menggunakan API WhatsApp, sistem yang terintegrasi dapat langsung terhubung dengan aplikasi *messenger* dari *platform mobile* maupun *web* (Izzah, 2021). Integrasi API WhatsApp dapat dilakukan salah satunya dengan menggunakan layanan pihak ketiga yang menyediakan API WhatsApp seperti WhatsApp *Bussines* API atau Twilio.

5. **Fonnte**

Fonnte merupakan layanan pihak ketiga penyedia API WhatsApp, namun tidak berjalan diatas *official* API WhatsApp seperti Twillio atau WhatsApp *Bussines* API. Fonnte menggunakan WhatsApp *web* untuk melakukan otomatisasi pengiriman dan membalas pesan whatsapp baik menggunakan API maupun *webhook* (*webhook* sama fungsinya seperti *autoreply* untuk membalas pesan secara otomatis). Fonnte juga menawarkan berbagai layanan berupa mengirim notifikasi aktivitas secara otomatis, mengirim

balasan pesan WhatsApp secara otomatis, mengirim pesan *reminder* secara otomatis, mengirim tagihan melalui pesan WhatsApp, mengirim informasi terbaru secara otomatis, dan mengirim OTP untuk keamanan.

6. Implementasi Sistem OTP

Implementasi sistem OTP bertujuan untuk meningkatkan tingkat keamanan dengan menambahkan lapisan autentikasi tambahan di luar kata sandi. Implementasi sistem verifikasi *login* menggunakan OTP melalui WhatsApp terdiri dari beberapa komponen utama, yaitu *backend server*, WhatsApp API, dan antarmuka pengguna dengan *endpoint* untuk *login* dan *request* OTP. Implementasi OTP dapat dilakukan dengan mengintegrasikan layanan API pihak ketiga yang memudahkan untuk mengirim OTP kepada pengguna secara otomatis.

7. PHP

PHP adalah bahasa pemrograman yang berasal dari kata *Hypertext Preprocessor*. Bahasa pemrograman ini menggunakan sistem *server side* yang merupakan jenis bahasa pemrograman yang nantinya *script* atau program tersebut akan dijalankan atau diproses oleh *server*. PHP dapat digunakan secara gratis dan bersifat *open source* yang dirilis dalam lisensi PHP license, sedikit berbeda dengan lisensi GNU *General Public License* (GPL) yang biasa digunakan untuk proyek *open source* (Noviana, 2022).