BAB II

TINJAUAN LITERATUR

2.1 Penelitian Terkait

Penulis telah melakukan studi literature dan terdapat beberapa penelitian yang telah melakukan penelitian yang berkaitan dengan keamanan sistem informasi, autentikasi dua faktor (2FA), dan penggunaan *One-Time Password* (OTP). Berikut beberapa penelitian yang menjadi referensi penulis pada penelitian ini.

Penelitian yang dilakukan oleh (Cristian wt al., 2023) yang melakukan fokus penelitiannya menambahkan keamanan pada sistem autentikasi untuk melindungi sistem dan data pengguna dari akses tidak sah melalui metode kriptografi. Penelitian ini menggunakan algoritma RSA dengan Bahasa pemograman *Python* yang mempunyai kekurangan untuk implementasi kriptografi RSA pada autentikasi cenderung memerlukan beban komputasi yang lebih berat dan belum memanfaatkan media pesan instan seperti WhatsApp sebagai faktor kepemilikan perangkat secara *real-time.*

Penelitian yang dilakukan oleh (Riski & Mulyati, 2020) yang melakukan pengujian untuk mengetahui kinerja waktu pengiriman OTP. Penelitian ini menggunakan algoritma SHA-512 dengan metode *Waterfall Development* yang memiliki kekurangan dimana metode *Waterfall* kurang fleksibel untuk pengembangan sistem keamanan yang memerlukan literasi cepat, serta belum mengintegrasikan API pihak ketiga yang memudahkan pengiriman pesan otomatis seperti WhatsApp.

Penelitian yang dilakukan oleh (Hayat et al., 2022) yang melakukan penelitian menggunakan kode verifikasi satu kali kirim (OTP) dengan batasan waktu penggunaan maksimal 1 menit. Pengiriman kode OTP masih dilakukan melalui media *e-mail* yang memiliki risiko keterlambatan pengiriman (*delay*) yang lebih tinggi dan tingkat keamanan yang lebih rendah dibandingkan pesan WhatsApp yang terikat langsung pada nomor telepon pribadi pengguna.

Penelitian yang dilakukan oleh (Nasution e al., 2024) yang fokus penelitiannya adalah memberikan pedoman praktis dalam menerapkan verifikasi login yang aman untuk melindungi dari serangan *man-in-the-middle* (MITM). Menggunakan pengujian penetrasi untuk mengindentifikasi kerentanan memiliki kekurangan yang meskipun memiliki perlindungan terhadap MITM, penelitian ini tidak secara spesifik membahas integrasi dengan *gateway* pesan eksternal yang efisien untuk pengguna di lingkungan institusi pendidikan.

Penelitian yang dilakukan oleh (Alfarizi et al., 2024) yang melakukan fokus penelitian melakukan pengujian via *Mailtrap* API yang memiliki keterbatasan pada lingkungan pengujian *e-mail* dan belum diuji secara nyata pada integrasi *gateaway* pesan instan untuk pengguna akhir.

2.2 Metode *Prototyping*

Metode *Prototyping* merupakan salah satu pendekatan dalam pengembangan sistem yang menekankan pada pembuatan mode awal *(prototype)* sebagai representasi dari sistem yang akan dikembangkan. *Prototype* berfungsi sebagai gambaran awal sistem yang dapat diuji, dievaluasi, dan disempurnakan sebelum implementasi secara penuh (Pressman & Maxim, 2015). Pendekatan ini memungkinkan pengembang dan pengguna untuk berinteraksi langsung dengan model sistem sehingga kebutuhan sistem dapat di indentifikasi dan diperbaiki secara bertahap (Sommerville, 2016). Metode ini umumnya digunakan ketika kebutuhan sistem belum terdefinisi secara rinci atau ketika diperlukan validasi konsep sebelum sistem diterapkan secara permanen (Rosa & Shalahuddin, 2018).

Dalam konteks pengembangan sistem informasi, *prototyping* membantu meminimalkan risiko kesalahan desain serta meningkatkan kesesuaian sistem dengan kebutuhan pengguna melalui proses umpan balik *(feedback)* yang berulang (Sutabri, 2012). Pemilihan metode *prototyping* ini bertujuan untuk mengembangkan dan menguji model awal sistem autentikasi dua faktor, bukan langsung melakukan implementasi penuh pada sistem produksi. Selain itu, metode

ini memungkinkan evaluasi awal tahap efektivitas integrasi OTP berbasis WhatsApp menggunakan API Fonnte dalam meningkatkan keamanan login Portal Akademik SIKAMU.

2.3 *One Time Password* (OTP)

One Time Password (OTP) merupakan kode verifikasi yang dihasilkan secara unik dan hanya dapat digunakan satu kali dalam proses autentikasi. OTP dirancang untuk meningkatkan keamanan sistem dengan menambahkan lapisan verifikasi tambahan selain penggunaan *username* dan *password* (Kurniawan & Sari, 2019). Berbeda dengan *password* statis yang dapat digunakan berulang kali, OTP bersifat dinamis, acak, dan memiliki masa berlaku terbatas sehingga lebih aman terhadap risiko penyalahgunaan (Rahman & Utomo, 2018). Dalam sistem informasi berbasis web, OTP umumnya digunakan sebagai bagian dari mekanisme *Two-Factor Authentication* (2FA). Setelah pengguna berhasil memasukkan *usename* dan *password* yang valid, sistem akan menghasilkan kode OTP dan mengirimkannya ke media yang terdaftar, seperti SMS, *email*, atau aplikasi pesan instan. Pengguna kemudian diwajibkan memasukkan kode tersebut untuk menyelesaikan proses login. Berdasarkan mekanisme pembangkitannya, OTP dibedakan menjadi dua jenis utama, yaitu:

1. *HMAC-Based One Time Password* (HOTP)

   OTP yang dihasilkan berdasarkan penghitung *(counter)* atau jumlah permintaan autentikasi. Setiap kali proses autentikasi dilakukan, sistem akan menghasilkan kode baru berdasarkan nilai penghitung tersebut (Hidayat & Firmansyah, 2019). Metode ini menghasilkan kode yang berbeda setiap kali autentikasi dilakukan, namun tetap memerlukan sinkronasi antara server dan pengguna.

2. *Time-Based One Time Password* (TOTP)

   OTP yang dihasilkan berdasarkan waktu tertentu dan hanya berlaku dalam jangka waktu terbatas, misalnya 60 atau 120 detik. Setelah melewati batas waktu tersebut, kode akan otomatis kadaluwarsa dan tidak dapat digunakan kembali (Setiawan & Nugroho, 2021). Metode ini dinilai

lebih praktis dan aman karena memanfaatkan parameter waktu sebagai variabel pembentuk kode autentikasi.

Dalam penelitian ini, mekanisme OTP yang diterapkan bersifat *time-based* (TOTP), sehingga kode verifikasi hanya berlaku dalam periode waktu tertentu. Penerapan OTP pada Portal Akademik SIKAMU dilakukan melalui pengiriman kode verifikasi ke nomor WhatsApp pengguna menggunakan integrasi API Fonnte. Setelah pengguna memasukkan *username* dan *password* yang valid, sistem akan menghasilkan kode OTP secara acak (misalnya 6 digit numerik), kemudian menyimpan kode tersebut sementara di sistem beserta waktu kadaluwarsa, mengirimkan kode OTP ke nomor Whatsapp terdaftar melalui API Fonnte dan yang terakhir yaitu memverifikasi kesesuaian kode yang dimasukkan pengguna dengan kode yang tersimpan di sistem.

Hal ini secara signifikan meningkatkan tingkat keamanan autentikasi karena sistem memverifikasi dua faktor sekaligus, yaitu pengetahuan *(password)* dan kepemilikan perangkat komunikasi (WhatsApp). Secara keseluruhan, *One Time Password* (OTP) dalam penelitian ini berfungsi sebagai mekanisme pengamanan tambahan yang memperkuat proses autentikasi pada Portal Akademik SIKAMU. Penerapan OTP berbasis WhatsApp melaui API Fonnte diharapkan mampu meningkatkan perlindungan terhadap akses tidak sah serta menjaga kerahasiaan dan integritas data akademik secara lebih optimal (Wahyuni & Pratama, 2020).

2.4 *Application Programming Interface* (API) Fonnte

Application Programming Interface (API) merupakan sekumpulan aturan, protokol, dan mekanisme yang memungkinkan suatu aplikasi untuk berkomunikasi dan bertukar data dengan aplikasi atau layanan lainnya. API berfungsi sebagai penghubung *(interface)* antara sistem yang berbeda sehingga integrasi dapat dilakukan tanpa harus mengakses atau memodifikasi struktur internal masing-masing sistem secara langsung. Dalam pengembangan sistem berbasis web, API sering digunakan untuk mengintegrasikan layanan pihak ketiga, seperti layanan pembayaran, pengiriman email, maupun pengiriman pesan instan. Melalui API, sistem dapat mengirim dan menerima data secara otomatis

menggunakan metode komunikasi tertentu, umumnya berbasis protokol HTTP dengan format data seperti JSON.

Dalam penelitian ini, API yang digunakan adalah API Fonnte. Fonnte merupakan layanan penyedia WhatsApp *Gateaway* berbasis API yang memungkinkan sistem untuk mengirimkan pesan WhatsApp secara otomatis melalui integrasi dengan aplikasi berbasis web. API Fonnte menyediakan *endpoint* yang dapat diakses oleh sistem menggunakan token autentikasi tertentu untuk menjamin keamanan komunikasi antara sistem dan layanan Fonnte (Fonnte, 2024). Penggunaan API Fonnte sebagai media pengirim OTP mendukung penerapan autentikasi dua faktor yang lebih kuat dibandingkan metode *single-factor authentication* (Pratama & Putra, 2020). Dengan adanya integrasi ini, sistem tidak hanya memverifikasi pengetahuan pengguna terhadap *password*, tetapi juga memastikan bahwa pengguna memiliki akses terhadap nomor WhatsApp yang terdaftar sebagai faktor kepemilikan *(something you have)* (Putri & Santoso, 2021). Dengan demikian, API Fonnte berperan sebagai komponen pendukung utama dalam penelitian ini.

2.5 WhatsApp sebagai media pengirim OTP

WhatsApp merupakan aplikasi pesan instan berbasis internet banyak digunakan oleh masyarakat Indonesia. Tingginya tingkat penggunaan WhatsApp menjadikannya salah satu media komunikasi digital yang paling efektif dan mudah diakses oleh berbagai kalangan (APJII, 2023). WhatsApp tidak hanya berfungsi sebagai sarana komunikasi personal, tetapi juga dapat dimanfaatkan sebagai media pengiriman pesan otomatis mealui integritas *Application Programming Interface* (API). Penelitian ini menggunakan WhatsApp sebagai media pengiriman *One Time Password* (OTP) pada proses autentikasi dua faktor (*Two-Factor Authentication*/2FA) di Portal Akademik Universitas Muhammadiyah Bengkulu (SIKAMU).

Pemilihan WhatsApp sebagai media pengiriman OTP didasarkan pada beberapa pertimbangan teknis dan praktis. Sebagian besar mahasiswa dan dosen telah menggunakan WhatsApp sebagai aplikasi komunikasi utama, hal ini

memudahkan proses implementasi karena pengguna tidak perlu menginstal aplikasi tambahan atau perangkat khusus untuk menerima kode verifikasi (Sari & Wijaya, 2021). Pengiriman pesan melalui WhatsApp relatif cepat dan *real-time* selama pengguna terhubung ke jaringan internet, dan penggunaan WhatsApp lebih fleksibel dibandingkan SMS *gateway* yang bergantung pada operator seluler dan biaya pengiriman pesan. Secara teknis, pengiriman OTP melalui WhatsApp dalam penelitian ini dilakukan dengan memanfaatkan layanan API Fonnte sebagai penghubung antara sistem portal akademik dan layanan WhatsApp. Integrasi API memungkinkan sistem portal akademik untuk mengirimkan pesan secara otomatis ke nomor WhatsApp pengguna yang telah terdaftar (Fauzi & Santoso, 2022).

Proses pengiriman dilakukan setelah pengguna berhasil melewati tahap autentikasi pertama (*username* dan *password*), sistem kemudian menghasilkan kode OTP yang bersifat unik dan *time-based* lalu mengirimkannya melalui WhatsApp sebagai faktor verifikasi kedua. Penggunaan WhatsApp sebagai media pengiriman OTP memberikan beberapa keuntungan dalam konteks keamanan sistem informasi seperti verifikasi kepemiliki perangkat, pengiriman *real-time*, kemudahan akses, dan efisiensi implementasi (Putri & Santoso, 2021). Pemanfaatan WhatsApp sebagai media pengiriman kode OTP merupakan bagian dari pengembangan *prototype* sistem autentikasi dua faktor pada Portal Akademik SIKAMU yang bertujuan untuk menambahkan lapisan keamanan tambahan yang efektif, mudah diimplementasikan, serta sesuai dengan kebutuhan dan karakteristik pengguna di lingkungan perguruan tinggi.

2.6 *Two-Factor Authentication* (2FA)

Two-Factor Authentication (2FA) merupakan salah satu metode autentikasi yang digunakan untuk meningkatkan keamanan sistem dengan cara menambahkan lapisan verifikasi tambahan selain penggunaan password. Dalam sistem autentikasi tradisional, pengguna hanya diminta untuk memasukkan *username* dan *password* sebagai syarat untuk mengakses suatu sistem. Namun, pendekatan ini memiliki berbagai kelemahan karena *password* dapat dengan mudah ditebak, dicuri melalui serangan *phishing*, atau dibobol menggunakan

teknik *bruce force*. Kondisi tersebut menjadikan sistem berbasis *single-factor authentication* semakin rentan terhadap ancaman keamanan. Untuk mengatasi permasalahan tersebut, dikembangkan metode *Two-Factor Authentication* yang mengharuskan pengguna untuk melewati dua tahap verifikasi sebelum mendapatkan akses ke dalam sistem. Metode ini bekerja dengan mengkombinasikan dua jenis faktor autentikasi yang berbeda, sehingga meskipun salah satu faktor berhasil diketahui oleh pihak yang tidak berwenang, akses ke sistem tetap dapat dicegah karena masih memerlukan faktor kedua yang lebih sulit untuk diperoleh.

Penerapan *Two-Factor Authentication* memberikan berbagai keuntungan dalam meningkatkan keamanan sistem. Salah satu keunggulan utamanya adalah kemampuannya dalam mengurangi risiko pencurian akun akibat kebocoran *password*. Selain itu, metode ini juga memberikan perlindungan tambahan terhadap berbagai jenis serangan siber, seperti *phishing* dan *bruce force*, karena penyerang tidak hanya membutuhkan *password* tetapi juga akses ke perangkat pengguna. Dengan demikian, tingkat keamanan sistem secara keseluruhan menjadi lebih tinggi dibandingkan dengan metode authentikasi konvensional. Seiring dengan perkembangan teknologi keamanan, *Two-Factor Authentication* saat ini tidak lagi dianggap sebagai satu-satunya indikator keamanan yang kuat. Hal ini dikarenakan tidak semua implementasi 2FA memiliki tingkat keamanan yang sama. Oleh karena itu, diperlukan suatu standar yang dapat digunakan untuk mengevaluasi kekuatan autentikasi secara lebih menyeluruh. Salah satu yang digunakan adalah NIST SP 800-63B yang memperkenalkan *Authenticator Assurance Level* (AAL). Melalui pendekatan ini, sistem autentikasi tidak hanya dinilai berdasarkan jumlah faktor yang digunakan berdasarkan kualitas, metode, dan tingkat keamanannya.

2.7 NIST SP 800-63B

NIST SP 800-63B merupakan bagian dari standar *Digital Identity Guidelines* yang dikembangkan oleh *National Institute of Standards and Technology* (NIST), sebuah lembaga resmi di Amerika Serikat yang berfokus

pada pengembangan standar teknologi dan keamanan informasi. Standar ini dirancang untuk memberikan pedoman dalam proses autentikasi digital, khususnya dalam memastikan bahwa identitas pengguna dapat diverifikasi secara aman, andal, dan sesuai dengan tingkat risiko yang dihadapi oleh suatu sistem. Berbeda dengan pendekatan tradisional yang hanya menekankan pengguna satu atau dua faktor autentikasi, NIST SP 800-63B mengadopsi pendekatan yang lebih komprehensif dengan mempertimbangkan berbagai aspek keamanan, seperti jenis *authenticator* yang digunakan, cara pengelolaannya, serta ketahanan terhadap serangan. Standar ini menekankan bahwa keamanan autentikasi tidak hanya ditentukan oleh jumlah faktor yang digunakan, tetapi juga oleh kualitas dan implementasi dari faktor tersebut.

Salah satu konsep utama yang diperkenalkan dalam NIST SP 800-63B adalah *Authentikator Assurance Level* (AAL), yaitu tingkat jaminan keamanan autentikasi yang digunakan untuk mengklasifikasikan seberapa kuat suatu sistem dalam memverifikasi identitas pengguna. Melalui konsep ini, sistem autentikasi tidak hanya dinilai secara umum, tetapi dikategorikan ke dalam tingkat tertentu berdasarkan karakteristik dan kekuatan *autentikator* yang digunakan. Selain itu, NIST SP 800-63B juga memberikan perhatian khusus tehadap jenis-jenis *autentikator* yang digunakan dalam sistem. NIST SP 800-63B juga menekankan pentingnya perlindungan terhadap berbagai jenis serangan yang umum terjadi dalam sistem autentikasi. Oleh karena itu, standar ini direkomendasikan penggunaan mekanisme seperti *One-Time Password* (OTP) yang memiliki masa berlaku terbatas, serta penerapan sistem yang mampu mendeteksi dan mencegah penggunaan ulang autentikasi.

Dalam penelitian ini, NIST SP 800-63B digunakan sebagai dasar untuk mengevaluasi sistem authentikasi yang dikembangkan. Pendekatan yang digunakan adalah dengan mengidentifikasi jenis *autentikator* yang digunakan dalam sistem, kemudian memetakan karakteristiknya ke dalam kategori *Autheticator Assurance Level*. Dengan demikian, hasil evaluasi yang diperoleh tidak hanya menunjukkan apakah sistem telah menggunakan metode autentikasi

tertentu, tetapi juga memberikan gambaran yang lebih jelas mengenai tingkat keamanan yang dimiliki oleh sistem tersebut.

2.8 *Authenticator Assurance Level* (AAL)

Authenticator Assurance Level merupakan konsep yang diperkenalkan standar NIST SP 800-63B sebagai kerangka untuk mengklasifikasikan tingkat jaminan keamanan dalam proses autentikasi digital. Konsep ini digunakan untuk menilai seberapa kuat suatu sistem dalam memverifikasi identitas pengguna berdasarkan jenis *autentikator* yang digunakan, serta bagaimana *autentikator* tersebut diimplementasikan dalam sistem. Dengan adanya AAL, proses evaluasi keamanan tidak lagi bersifat umum atau sekadar melihat jumlah faktor autentikasi, melainkan dilakukan secara lebih terstruktur dan terukur. Secara umum, *Authenticator Assurance* dibagi ke dalam tiga tingkat yang menunjukkan peningkatan kekuatan keamanan secara bertahap. Tingkat pertama menggambarkan sistem autentikasi yang paling dasar, di mana proses verifikasi identitas hanya bergantung pada satu jenis *autentikator*. Pada tingkat ini, keamanan sistem relatif terbatas karena hanya terdapat satu lapisan perlindungan yang dapat menjadi titik lemah apabila berhasil ditembus. Tingkat ini biasanya digunakan pada sistem yang tidak memiliki risiko tinggi terhadap kebocoran data atau penyalahgunaan akses. Pada tingkat ini hanya menggunakan *username* dan *password* hingga tidak ada persyaratan khusus untuk perangkat *autentikator* (NIST SP 800-63B, 2017).

Tingkat berikutnya menunjukkan peningkatan keamanan melalui penggunaan lebih dari satu faktor autentikasi. Pada tingkat ini, sistem diharuskan mengkombinasikan dua jenis *autentikator* yang berbeda, sehingga proses verifikasi menjadi lebih kuat. Selain itu, *autentikator* yang digunakan juga harus memiliki ketahanan terhadap serangan umum, seperti serangan *replay* atau pencurian *kredensial.* Dengan adanya dua lapisan autentikasi yang saling melengkapi, risiko akses tidak sah dapat diminalkan secara signifikan (NIST SP 800-63B, 2017). Tingkat tertinggi dalam AAL menggambarkan sistem autentikasi dengan tingkat keamanan yang sangat kuat. Pada tingkat ini, penggunaan

autentikator berbasis perangkat keras menjadi salah satu syarat utama. *Autentikator* jenis ini dirancang untuk memberikan perlindungan yang lebih tinggi karena tidak mudah direplikasi atau disalahgunakan oleh pihak lain. Selain itu, proses autentikasi pada tingkat ini juga biasanya melibatkan mekanisme tambahan yang memastikan bahwa interaksi antara pengguna dan sistem benar-benar aman dari gangguan pihak ketiga (NIST SP 800-63B, 2017).

Penerapan konsep *Authenticator Assurance Level* dalam suatu sistem memberikan manfaat yang signifikan, terutama dalam hal evaluasi dan peningkatan keamanan. Dengan menggunakan AAL, pengembang sistem dapat mengidentifikasi posisi keamanan sistem yang mereka bangun, serta menentukan langkah-langkah yang di perlukan untuk meningkatkan tingkat keamanan tersebut. Dalam konteks penelitian ini, AAL digunakan sebagai pendekatan utama untuk megevaluasi sistem autentikasi yang dikembangkan. Proses evaluasi dilakukan dengan menganalisis jenis *autentikator* yang digunakan, kemudian menilai kesesuaiannya dengan kriteria yang ditetapkan dalam masing-masing tingkat AAL. Dengan pendekatan ini, hasil penelitian tidak hanya menunjukkan apakah sistem telah menggunakan mekanisme autentikasi tertentu, tetapi juga memberikan gambaran yang lebih mendalam mengenai tingkat keamanan yang dimiliki oleh sistem tersebut.