

ABSTRAK

PENGEMBANGAN PROTOTYPE SISTEM AUTENTIKASI DUA FAKTOR MENGGUNAKAN OTP WHATSAPP BERBASIS API FONNTE PADA PORTAL AKADEMIK UNIVERSITAS MUHAMMADIYAH BENGKULU (SIKAMU)

Nama: Ramadhan Ikhsan Perdana Putra Dani

NPM: 2155201089

Pembimbing: Harry Witriyono, S.P., M.Kom

Perkembangan teknologi informasi mendorong perguruan tinggi untuk meningkatkan keamanan system informasi akademik guna melindungi data mahasiswa dan dosen dari ancaman akses tidak sah. Portal Akademik Universitas Muhammadiyah Bengkulu (SIKAMU) sebagai pusat layanan akademik berbasis web memiliki resiko keamanan apabila hanya mengandalkan autentikasi satu faktor berupa username dan password. Penelitian ini bertujuan untuk mengembangkan prototype system autentikasi dua faktor (Two-Factor Authentication/2FA) menggunakan One Time Password (OTP) berbasis WhatsApp melalui API Fonnte sebagai lapisan keamanan tambahan pada SIKAMU. Metode penelitian yang digunakan adalah metode pengembangan sistem dengan pendekatan prototyping, yang meliputi tahap analisis kebutuhan, perancangan sistem, pembangunan prototype, serta pengujian sistem. Mekanisme 2FA dirancang dengan proses login awal menggunakan kredensial pengguna, kemudian sistem emngirimkan kode OTP yang dikirim bersifat unik, acak, dan memiliki batas waktu (time-based) sehingga meningkatkan keamanan proses autentikasi. Dengan demikian, penerapan 2FA berbasis WhatsApp menggunakan API Fonnte dapat menjadi solusi yang alternatif yang efektif dan efisien dalam meningkatkan keamanan akses pada sistem infromasi akademik SIKAMU.

Kata kunci: Autentikasi Dua Faktor, OTP, WhatsApp, API Fonnte, Keamanan Sistem Informasi, Portal Akademik.

ABSTRAK

DEVELOPMENT OF A PROTOTYPE OF A TWO-FACTOR AUTHENTICATION SYSTEM USING WHATSAPP OTP BASED ON FONNTE API ON THE ACADEMIC PORTAL OF MUHAMMADIYAH UNIVERSITY OF BENGKULU (SIKAMU)

Name: Ramadhan Ikhsan Perdana Putra Dani

Student ID: 2155201089

Supervisor: Harry Witriyono, S.P., M.Kom

The development of information technology encourages higher education institutions to enhance the security of academic information systems in order to protect student and lecturer data from unauthorized access. The Academic Portal of Universitas Muhammadiyah Bengkulu (SIKAMU), as a web-based academic service center, has security vulnerabilities if it relies solely on single-factor authentication in the form of a username and password. This study aims to develop a prototype of a Two-Factor Authentication (2FA) system using a One-Time Password (OTP) delivered via WhatsApp through the Fonnte API as an additional security layer for SIKAMU. The research method employed is a system development approach using the prototyping model, which includes requirements analysis, system design, prototype development, and system testing. The 2FA mechanism is designed by implementing an initial login process using user credentials, followed by the system sending a unique, randomly generated, and time-based OTP code to enhance authentication security. Therefore, the implementation of WhatsApp-based 2FA using the Fonnte API can serve as an effective and efficient alternative solution to improve access security in the SIKAMU academic information system.

Keywords: Two-Factor Authentication, OTP, WhatsApp, Fonnte API, Information System Security, Academic Portal.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi pada era digital saat ini mengalami kemajuan yang sangat pesat. Kemajuan tersebut telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, termasuk dalam bidang pendidikan. Perguruan tinggi sebagai institusi pendidikan dituntut untuk mampu beradaptasi dengan perkembangan teknologi guna meningkatkan kualitas layanan akademik yang diberikan kepada mahasiswa dan seluruh civitas akademika (Laudon & Laudon, 2020). Pemanfaatan teknologi informasi dalam dunia pendidikan telah mendorong terciptanya berbagai sistem berbasis digital yang mampu menggantikan proses manual menjadi lebih efisien dan efektif (O'Brien & Marakas, 2011). Salah satu bentuk implementasi teknologi tersebut adalah sistem informasi akademik yang digunakan untuk mengelola berbagai aktivitas akademik secara terintegrasi.

Sistem informasi akademik berperan penting dalam mendukung kegiatan operasional perguruan tinggi, seperti pengolahan data mahasiswa, dosen, jadwal perkuliahan, nilai akademik, hingga administrasi lainnya (O'Brien & Marakas, 2011). Dengan adanya sistem ini, proses pengelolaan data menjadi lebih terstruktur, cepat, dan mudah diakses oleh pengguna. Portal akademik merupakan bagian dari sistem informasi akademik yang menjadi sarana utama bagi pengguna dalam mengakses berbagai layanan akademik. Melalui portal akademik, mahasiswa dan dosen dapat melakukan berbagai aktivitas seperti pengisian Kartu Rencana Studi (KRS), melihat jadwal perkuliahan, mengakses nilai, dan memperoleh informasi penting lainnya secara online. Penggunaan portal akademik memberikan banyak manfaat, terutama dalam meningkatkan efisiensi waktu dan kemudahan akses informasi. Pengguna tidak lagi harus datang langsung ke kampus untuk mengurus administrasi akademik, karena semua dapat dilakukan secara daring melalui sistem yang telah disediakan. Namun demikian, di balik kemudahan yang ditawarkan, penggunaan sistem informasi akademik

juga memiliki berbagai risiko, terutama yang berkaitan dengan keamanan data dan akses pengguna (Whitman & Mattord, 2018). Sistem yang tidak memiliki perlindungan yang kuat berpotensi menjadi target serangan oleh pihak yang tidak bertanggung jawab.

Ancaman keamanan yang sering terjadi pada sistem informasi akademik antara lain adalah pencurian akun, peretasan sistem, serta akses tidak sah terhadap data pengguna. Hal ini dapat terjadi apabila sistem hanya mengandalkan metode autentikasi sederhana seperti *username* dan *password* tanpa adanya lapisan keamanan tambahan. Penggunaan *username* dan *password* sebagai satu-satunya metode autentikasi memiliki kelemahan, terutama jika pengguna menggunakan *password* yang lemah atau mudah ditebak (Stallings, 2017). Selain itu, risiko pencurian data melalui teknik seperti *phishing* dan *keylogging* juga dapat mengancam keamanan akun pengguna (Whitman & Mattord, 2018)). Oleh karena itu, diperlukan suatu mekanisme keamanan tambahan yang mampu meningkatkan perlindungan terhadap sistem informasi akademik. Salah satu metode yang dapat diterapkan adalah autentikasi dua faktor atau *Two-Factor Authentication* (2FA). Autentikasi dua faktor merupakan metode keamanan yang mengharuskan pengguna untuk melewati dua tahap verifikasi sebelum mendapatkan akses ke sistem (Aloul et al., 2009). Metode ini menggabungkan dua jenis autentikasi, yaitu sesuatu yang diketahui pengguna (seperti *password*) dan sesuatu yang dimiliki pengguna (seperti kode verifikasi).

Dengan penerapan autentikasi dua faktor, tingkat keamanan sistem dapat meningkat secara signifikan. Hal ini dikarenakan meskipun *password* pengguna diketahui oleh pihak lain, akses ke sistem tetap tidak dapat dilakukan tanpa melalui tahap verifikasi kedua. Salah satu bentuk implementasi autentikasi dua faktor adalah penggunaan *One Time Password* (OTP). OTP merupakan kode verifikasi yang bersifat unik dan hanya berlaku dalam jangka waktu tertentu, sehingga tidak dapat digunakan kembali (M'Raihi et al., 2011). Penggunaan OTP sebagai faktor kedua dalam autentikasi dinilai efektif dalam mencegah akses ilegal ke dalam sistem (Aloul et al., 2009). Kode OTP yang dikirimkan secara *real-time* kepada pengguna memastikan bahwa hanya pengguna yang memiliki

akses ke perangkat tertentu yang dapat melakukan login. Media pengiriman OTP dapat dilakukan melalui berbagai platform, seperti SMS, email, maupun aplikasi pesan instan. Dalam perkembangannya, penggunaan aplikasi pesan instan menjadi pilihan yang lebih populer karena dinilai lebih cepat, praktis, dan mudah diakses. WhatsApp merupakan salah satu aplikasi pesan instan yang paling banyak digunakan oleh masyarakat saat ini (Statista, 2024). Dengan tingkat penggunaan yang tinggi, WhatsApp menjadi media yang efektif untuk menyampaikan informasi, termasuk dalam pengiriman kode OTP.

Pemanfaatan WhatsApp sebagai media pengiriman OTP dapat dilakukan melalui integrasi dengan *Application Programming Interface* (API). Salah satu layanan API yang dapat digunakan adalah Fonnte, yang memungkinkan sistem untuk mengirim pesan WhatsApp secara otomatis (Fonnte, 2024). API Fonnte menyediakan layanan pengiriman pesan berbasis WhatsApp yang dapat diintegrasikan dengan berbagai sistem informasi. Dengan menggunakan API ini, pengiriman kode OTP dapat dilakukan secara cepat, otomatis, dan *real-time* kepada pengguna (Fonnte, 2024). Penggunaan API Fonnte dalam sistem autentikasi memberikan kemudahan bagi pengembang dalam mengimplementasikan fitur keamanan tambahan. Selain itu, pengguna juga akan mendapatkan pengalaman yang lebih praktis dalam menerima kode verifikasi. Universitas Muhammadiyah Bengkulu sebagai salah satu perguruan tinggi yang telah memanfaatkan sistem informasi akademik melalui portal SIKAMU perlu memperhatikan aspek keamanan sistem yang digunakan. Hal ini penting untuk melindungi data akademik dari potensi ancaman yang dapat merugikan pengguna (Whitman & Mattord, 2018).

Portal akademik SIKAMU saat ini telah digunakan untuk berbagai keperluan akademik, namun masih memiliki potensi untuk dikembangkan, khususnya dalam meningkatkan sistem keamanan autentikasi pengguna. Peningkatan ini diperlukan untuk mengurangi risiko penyalahgunaan akun dan akses tidak sah (Stallings, 2017). Berdasarkan kondisi tersebut, diperlukan suatu solusi yang mampu meningkatkan keamanan sistem tanpa mengurangi kenyamanan pengguna. Salah satu solusi yang dapat diterapkan adalah dengan

mengintegrasikan autentikasi dua faktor menggunakan OTP berbasis WhatsApp (Aloul et al., 2009). Pengembangan sistem autentikasi dua faktor ini diharapkan mampu memberikan lapisan keamanan tambahan pada proses login pengguna. Dengan demikian, sistem akan menjadi lebih aman dan mampu melindungi data pengguna dari ancaman yang ada (M'Raihi et al., 2011).

Selain itu, penggunaan WhatsApp sebagai media pengiriman OTP juga memberikan kemudahan bagi pengguna karena tidak memerlukan aplikasi tambahan. Pengguna hanya perlu memiliki akses ke WhatsApp untuk menerima kode verifikasi. Dengan adanya integrasi antara sistem akademik dan API Fonnte, proses pengiriman OTP dapat dilakukan secara otomatis dan efisien (Fonnte, 2024). Hal ini juga mendukung peningkatan kualitas layanan sistem informasi akademik secara keseluruhan (Laudon & Laudon, 2020). Pengembangan sistem dilakukan menggunakan metode *prototyping* sehingga implementasi difokuskan pada pembuatan dan pengujian model awal sistem sebelum diterapkan pada lingkungan produksi. Oleh karena itu, proses pengujian dilakukan pada lingkungan *localhost*, karena pada tahap ini penelitian bertujuan untuk membuktikan keberhasilan integrasi mekanisme autentikasi dua faktor, bukan melakukan implementasi penuh pada server operasional SIKAMU. Penggunaan *localhost* tidak mempengaruhi kinerja API Fonnte, karena komunikasi antara sistem dan server fonnte dilakukan melalui jaringan internet menggunakan protokol HTTP. Selama komputer pengembang terhubung ke internet dan token API yang digunakan masih aktif, proses pengiriman OTP melalui WhatsApp tetap dapat berjalan sebagaimana mestinya.

Penelitian ini belum menggunakan server *hosting* karena implementasi pada server produksi memerlukan izin institusi, konfigurasi server, pengamanan jaringan, domain, serta sertifikat keamanan (SSL) yang berada di luar ruang lingkup penelitian. Oleh sebab itu, lingkungan *localhost* dipilih sebagai media pengembangan dan pengujian yang aman, terkendali, serta sesuai dengan karakteristik metode *prototyping*. Hasil pengujian pada lingkungan tersebut telah mampu menunjukkan bahwa mekanisme autentikasi dua faktor dapat berjalan sesuai kebutuhan sistem dan berpotensi untuk diterapkan pada lingkungan

produksi di masa mendatang. Penggunaan layanan API Fonnte juga mengharuskan perangkat WhatsApp terlebih dahulu dihubungkan dengan server Fonnte melalui halaman *md.fonnte.com* dengan melakukan pemindaian QR code menggunakan aplikasi WhatsApp. Proses ini merupakan mekanisme autentikasi perangkat yang memungkinkan server Fonnte memperoleh izin untuk mengirimkan pesan WhatsApp secara otomatis melalui akun yang telah terhubung. Tanpa proses pemindaian QR code tersebut, layanan API tidak dapat mengirimkan kode OTP kepada pengguna karena akun WhatsApp belum terhubung dengan server *gateway*.

Pada penelitian ini digunakan layanan Fonnte versi gratis (*free*) karena seluruh fitur utama yang diperlukan untuk pengembangan *prototype* telah tersedia, seperti penyediaan token API, integrasi WhatsApp *gateway*, dan pengiriman pesan OTP secara otomatis. Meskipun demikian, layanan versi gratis memiliki beberapa keterbatasan antara lain perangkat WhatsApp harus tetap aktif dan terhubung ke internet, adanya pembatasan penggunaan layanan, serta belum tersedianya jaminan kualitas layanan (*Service Level Agreement*) sebagaimana pada layanan berbayar. Keterbatasan tersebut tidak memengaruhi tujuan penelitian karena fokus utama penelitian ini adalah membuktikan keberhasilan implementasi autentikasi dua faktor berbasis OTP menggunakan API Fonnte pada Portal Akademik SIKAMU, bukan mengevaluasi performa layanan *gateway* dalam skala produksi. Berdasarkan uraian tersebut, maka penelitian ini difokuskan pada pengembangan *prototype* sistem autentikasi dua faktor menggunakan OTP berbasis WhatsApp melalui API Fonnte pada portal akademik SIKAMU. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan sistem informasi akademik serta menjadi referensi bagi pengembangan sistem serupa di masa yang akan datang (Whitman & Mattord, 2018).

1.2 Pertanyaan Penelitian

Dari uraian di atas muncul pertanyaan seperti bagaimana merancang sistem autentikasi dua faktor menggunakan OTP berbasis WhatsApp pada Portal Akademik SIKAMU, bagaimana mengintegrasikan API Fonnte dalam mekanisme pengiriman dan validasi OTP, serta bagaimana hasil pengujian prototype sistem autentikasi dua faktor dalam meningkatkan keamanan proses login pada SIKAMU?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk :

- a) Merancang dan mengembangkan prototype sistem autentikasi dua faktor menggunakan OTP berbasis WhatsApp pada Portal Akademik SIKAMU.
- b) Mengintegrasikan API Fonnte sebagai media pengiriman OTP secara otomatis dan terstruktur.
- c) Melakukan pengujian sistem untuk mengetahui efektivitas penerapan autentikasi dua faktor dalam meningkatkan keamanan proses login.

1.4 Kerangka Kerja Penelitian

No	Tahap Penelitian	Penjelasan
1.	Identifikasi Masalah	Tahap ini bertujuan untuk mengidentifikasi permasalahan yang terdapat pada sistem autentikasi Portal Akademik SIKAMU. Sistem yang masih menggunakan satu faktor autentikasi dinilai memiliki risiko keamanan, sehingga diperlukan pengembangan sistem autentikasi dua faktor

No	Tahap Penelitian	Penjelasan
		(2FA).
2.	Studi Literatur (2FA, OTP, WhatsApp API, Fonnte)	Pada tahap ini dilakukan pengumpulan dan kajian referensi berupa jurnal ilmiah, buku, dan dokumentasi teknis yang berkaitan dengan konsep <i>Two-Factor Authentication</i> (2FA), <i>One Time Password</i> (OTP), WhatsApp API, serta layanan API Fonnte sebagai media pengiriman OTP.
3.	Analisis Kebutuhan Sistem	Tahap ini dilakukan untuk menentukan kebutuhan sistem yang akan dikembangkan, meliputi kebutuhan fungsional seperti proses pengiriman dan verifikasi OTP, serta kebutuhan non-fungsional seperti keamanan, kecepatan, dan keandalan sistem.
4.	Perancangan Sistem Autentikasi Dua Faktor	Pada tahap perancangan, dibuat desain alur autentikasi dua faktor, arsitektur sistem, serta rancangan integrasi antara Portal Akademik SIKAMU dengan layanan WhatsApp API melalui Fonnte. Perancangan ini

No	Tahap Penelitian	Penjelasan
		bertujuan agar sistem mudah digunakan dan aman.
5.	Implementasi OTP WhatsApp Berbasis API Fonnte	Tahap ini merupakan penerapan hasil perancangan ke dalam bentuk prototype sistem. Implementasi meliputi pembuatan modul pengiriman OTP melalui WhatsApp menggunakan API Fonnte dan mekanisme validasi OTP saat proses login pengguna.
6.	Pengujian Sistem (<i>Black Box Testing</i>)	Pengujian sistem dilakukan menggunakan metode <i>black box testing</i> dengan fokus pada pengujian fungsi sistem, seperti login pengguna, pengiriman OTP, verifikasi OTP, serta penanganan kesalahan untuk memastikan sistem berjalan sesuai kebutuhan.
7.	Evaluasi Kinerja 2FA	Evaluasi dilakukan untuk mengukur kinerja sistem autentikasi dua faktor berdasarkan NIST AAL. Hasil evaluasi digunakan untuk menilai efektivitas dan

No	Tahap Penelitian	Penjelasan
		keandalan sistem yang dikembangkan.
8.	Kesimpulan dan Rekomendasi	Tahap akhir penelitian berupa penarikan kesimpulan berdasarkan hasil pengujian dan evaluasi sistem. Selain itu, diberikan rekomendasi untuk pengembangan sistem lebih lanjut agar keamanan dan performa sistem dapat ditingkatkan.

Tabel 1.1 Kerangka Kerja Penelitian

