INTEGRASI BIOMETRIK PADA SISTEM OTENTIKASI OTP SEBAGAI TWO-FACTOR AUTHENTICATION PADA MULTIAPLIKASI

Muchamad Sandy [1)]

[1)] *Teknik Informatika Universitas Dian Nusantara Jakarta*
email : muchamad.sandy@dosen.undira.ac.id[1]

Abstraksi

Otentikasi berbasis One-Time Password (OTP) telah banyak digunakan sebagai metode keamanan dalam proses persetujuan dokumen digital, termasuk pada integrasi 3 aplikasi. Namun, meskipun OTP mampu memberikan lapisan keamanan tambahan dibandingkan autentikasi tunggal berbasis kredensial, metode ini masih memiliki kelemahan seperti potensi intersepsi maupun rekayasa sosial. Untuk memperkuat sistem yang sudah ada, penelitian ini mengusulkan integrasi biometrik sebagai faktor autentikasi tambahan, sehingga membentuk skema Two-Factor Authentication (2FA) yang lebih andal. Pengembangan sistem dilakukan menggunakan pendekatan Agile untuk memastikan fleksibilitas, adaptabilitas, serta pengembangan fungsionalitas yang cepat melalui iterasi singkat. Selain itu, desain responsif diterapkan agar sistem dapat diakses lintas perangkat. Temuan penelitian ini memberikan kontribusi pada pemahaman strategi penguatan autentikasi dengan kombinasi OTP dan biometrik dalam konteks persetujuan dokumen terdistribusi. Hasil pengujian menunjukkan bahwa pendekatan ini tidak hanya memperkuat aspek keamanan, tetapi juga meningkatkan efisiensi operasional serta pengalaman pengguna dalam mengakses dan menyetujui dokumen aplikasi integrasi multi aplikasi tersebut.

Kata Kunci **:** *biometrik, otp, agile , scrum, two-factor authentication*

Abstract

One-Time Password (OTP)-based authentication has been widely adopted as a security method for digital document approval processes, including in three-application integration. However, despite OTP providing an additional layer of security compared to single credential-based authentication, this method still has weaknesses such as potential interception and social engineering. To strengthen the existing system, this study proposes the integration of biometric as an additional authentication factor, thereby forming a more reliable Two-Factor Authentication (2FA) scheme. System development was carried out using an Agile approach to ensure flexibility, adaptability, and rapid functionality development through short iterations. Additionally, a responsive design was implemented so the system could be accessed across devices. The findings of this research contribute to the understanding of strategies for strengthening authentication through a combination of OTP and biometric in the context of distributed document approval. The test results show that this approach not only strengthens the security aspect but also improves operational efficiency and user experience in accessing and approving documents within the multi-application integration.

Keywords **:** *biometrik, otp, agile , scrum, two-factor authentication*

Pendahuluan

Dalam era digital saat ini, berbagai perusahaan di berbagai industri termasuk industri tambang batubara yang sudah memiliki dan mengimplementasikan integrasi multi aplikasi [1] sehingga penggunaan tersebut sangat membantu pengguna (*approver*) dalam kebutuhan operasional termasuk dalam proses persetujuan yang menjadi lebih efisien dan efektif sehingga aplikasi atau sistem informasi dengan menerapkan sistem tampilan antarmuka tunggal sebagai jembatan antara multi-aplikasi dengan OTP sebagai bagian keamanan [2].

Namun, seiring berjalannya waktu pada lingkup operasional perusahaan yang mengimplementasikan sistem informasi antarmuka tunggal mengalami beberapa kendala antara lain : informasi OTP yang dikirim terkadang masuk ke nomor yang tidak seharusnya terdaftar di sistem, nomor yang digunakan tidak dipegang langsung oleh yang bersangkutan (*approver*) , serta *social engineering malware* [3] saat *approver* untuk melakukan proses persetujuan di aplikasi antarmuka tunggal.

Menanggapi kendala tersebut, penelitian ini mengusulkan solusi untuk memperkuat sistem autentikasi yang ada. Berbagai studi telah mengeksplorasi pendekatan serupa, termasuk integrasi autentikasi tambahan dengan metode Agile [4], penerapan Two-Factor Authentication (2FA) [5][6], serta penggunaan biometrik seperti sidik jari [7][8][9] bersama OTP [10] untuk proses persetujuan. Mengambil inspirasi dari pendekatan ini, penelitian kami mengadopsi metodologi pengembangan Agile (Scrum) untuk memastikan fleksibilitas, efektivitas, dan adaptabilitas terhadap perubahan proses bisnis,

serta memfasilitasi keterlibatan aktif pengguna sepanjang siklus pengembangan.

Adapun tujuan utama penelitian ini adalah untuk mengembangkan dan mengimplementasikan sistem autentikasi 2FA yang mengintegrasikan biometrik (sidik jari) dengan OTP pada lingkungan multi-aplikasi. Diharapkan, sistem ini dapat memberikan kontribusi signifikan dalam meningkatkan keamanan, efisiensi, dan keandalan proses persetujuan dokumen, transaksi, atau operasional, sehingga mendukung tujuan strategis bisnis perusahaan.

Pada tahapan pengembangan sistem yang meliputi inisialisasi perencanaan, pengumpulan kebutuhan pengguna terkait kendala proses bisnis, serta asesmen arsitektur aplikasi antarmuka tunggal. Asesmen ini penting untuk mengidentifikasi kebutuhan integrasi biometrik pada sistem OTP, mengingat potensi perbedaan platform, arsitektur, dan bahasa pemrograman antar aplikasi yang terintegrasi.

Untuk kontribusi utama pada penelitian ini adalah menyediakan strategi integrasi sistem yang efektif untuk memperkuat keamanan proses persetujuan dokumen, transaksi, atau operasional dalam lingkungan multi aplikasi. Dengan mengimplementasikan kombinasi biometrik dan OTP sebagai 2FA, sistem diharapkan tidak hanya menjadi lebih aman tetapi juga meningkatkan efisiensi dan mendukung tujuan strategis bisnis perusahaan. Tahapan awal pengembangan meliputi pengumpulan kebutuhan pengguna terkait kendala bisnis, serta asesmen arsitektur aplikasi antarmuka tunggal untuk mengidentifikasi kebutuhan integrasi biometrik pada sistem OTP, dengan mempertimbangkan perbedaan platform, arsitektur, dan bahasa pemrograman yang ada.

Tinjauan Pustaka

Metodologi Agile

Model Agile ini merupakan kelompok dalam metode untuk mengembangkan suatu software yang dilakukan secara duplikasi dan juga sistematis. Model Agile ini berisi beberapa metode yaitu antara lain Scrum, Crystal Clear, Extreme Programming (XP), Adaptive Software Development (ASD), Feature Driven Development (FDD), dan Metode Dynamic Systems Development (DSDM) Crystal, Lean Software Development dan lain-lain [4].

Metode agile Software Development merupakan proses iteratif dalam pembuatan sebuah perangkat lunak. Dalam prosesnya dalam pengembangan, agile juga dapat dikatakan sebagai metode pengembangan yang cepat dikarenakan proses utama dari metode pengembangan agile ini sendiri lebih berfokus kepada *design-code test once a day.*

Metodologi ini menempatkan empat pola pikir utama untuk menampilkan hasil produk dan juga bekerjasama dengan klien. Empat pola pikir utamanya yaitu dengan cara : 1) Individu dan interaksi akan lebih diprioritaskan dibandingkan dengan proses dan juga alat; 2) perangkat lunak sudah dapat berjalan dibandingkan dengan dokumentasi terperinci; 3) lebih kolaborasi dengan klien dibandingkan dengan kontrak negosiasi; 4) merespon terhadap perubahan – perubahan daripada mengikuti suatu rencana [11].

One Time Password (OTP)

One Time Password (OTP) adalah proses otentikasi dari server menggunakan kode dinamis setiap kali pengguna melakukan suatu tindakan yang diproses oleh server atau kode yang berubah setelah periode waktu tertentu serta kode yang dihasilkan secara unik dan tidak dapat digunakan kembali. Selain itu, kode OTP memiliki jangka waktu yang singkat karena dipengaruhi oleh faktor keamanan, jika kode OTP memiliki jangka waktu yang panjang atau bahkan tidak ada jangka waktu, maka kode tersebut rentan akan serangan seperti brute force yang sering digunakan untuk meretas password statis yang tidak memiliki jangka waktu penggunaan [12].

Algoritma RSA

Algoritma RSA merupakan salah satu metode kriptografi kunci publik yang sangat kuat. Algortima ini melibatkan pasangan kunci, yaitu kunci publik dan kunci privat [13]. Kunci publik digunakan untuk mengenkripsi pesan, sedanglan kunci pivat digunakan untuk mendekripsi pesan yang telah dienkripsi menggunakan kunci publik. Dengan menggunakan algoritma RSA sebagai metode autentikasi, sistem otentikasi dapat memastikan keamanan komunikasi dan melindungi informasi pengguna dengan efektif [10].

Biometrik

Biometrik merupakan bentuk pengukuran dan analisis karakteristik biologis atau perilaku individu. Karakteristik ini kemudian digunakan untuk mengidentifikasi atau memverifikasi identitas seseorang. Selain itu biometrik menawarkan sejumlah kelebihan yang signifikan dalam keamanan dan otentikasi. Salah satunya adalah tingkat keamanan yang tinggi karena biometrik menggunakan karakteristik unik individu, seperti sidik jari atau wajah, yang sulit untuk ditiru atau dicuri. Selain itu, penggunaan biometrik juga memungkinkan proses otentikasi yang cepat dan mudah, mengurangi kebutuhan untuk mengingat kata sandi atau membawa kartu akses.

Namun, terdapat beberapa kekurangan yang perlu diperhatikan. Salah satunya adalah biometrik rentan terhadap hilangnya privasi, karena karakteristik biometrik yang sensitif harus disimpan dalam basis data. Ada pula potensi untuk kesalahan dalam pengenalan biometrik, baik karena kesalahan teknis dalam pemindaian atau karena karakteristik biometrik individu dapat berubah seiring waktu. Oleh sebab itu, penting untuk mempertimbangkan dan mengelola risiko ini dengan cermat dalam penerapan teknologi biometrik.

Saat ini ada berbagai jenis penggunaan sistem biometrik yang umum digunakan, antara lain : sidik

jari, pengenalan wajah, mata serta suara. Untuk penelitian ini menggunakan biometrik Sidik Jari, yang menjadi salah satu jenis biometrik yang paling umum digunakan atau implementasi serta perangkat pendukung yang memadai [7][14]

Two-Factor Authentication (2FA)

Multi-factor authentication (2FA), adalah sebuah metode otentikasi elektronik yang mana menggunakan proses persetujuan pengguna komputer untuk memperoleh akses ke halaman situs web atau aplikasi secara sukses dengan penyerahan bukti. Metode yang digunakan pada 2FA tergolong rapi dan efektif untuk proses masuk pengguna, perolehan bukti atau faktor dapat diinput dengan sandi tertentu untuk dicocokkan dengan halaman situs web atau aplikasi yang dituju. 2FA umumnya sangat digantungkan kepada keawetan penjagaan keamanan dokumen penting, seperti informasi identitas pribadi, detail, maupun aset finansial [15].

Penelitian Terdahulu

Untuk memetakan posisi penelitian ini dan memastikan keterbaruan temuan, dilakukan tinjauan terhadap lima penelitian relevan yang berfokus pada manajemen identitas, keamanan akses, dan metodologi pengembangan sistem. Perbandingan antara penelitian terdahulu dengan penelitian ini disajikan dalam Tabel 1.

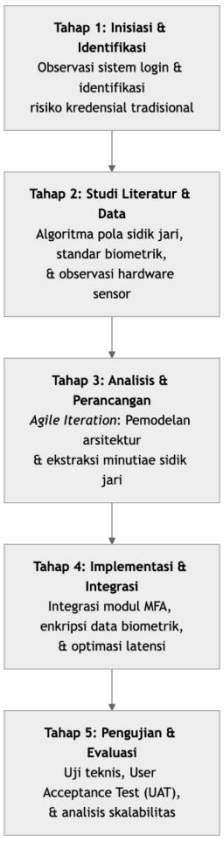
Tabel 1. Penelitian terdahulu

#	Penulis, Judul Paper	Fokus Penelitian	Metode Teknologi	Perbandingan dengan Penelitian
1	A. I. A. Mashudi and A. Prihantoro, "Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication," *J-Informatics Comput. Sci.*, vol. 6, no. 03, pp. 630–638, 2025	Konsep keamanan dengan menggunakan 2FA	2FA	Penelitian sudah implementasi 2FA terkait keamanan akses namun belum menggunakan biometrik
2	Amirullah, H. H., Eviyanti, A., & Sumarno, S. (2024). Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android. *SMATIKA JURNAL: STIKI Informatika Jurnal*, 14(01), 23–32.	Implementasi metode keamanan dengan biometrik sidik jari	AES Enkripsi	Hasil penelitian ini menunjukkan terkait implementasi biometrik sidik jari pada aplikasi
3	Miftahul Jannah, Muhamad Faris Hidayat, Mutia Agustiyani, Pandu Wira Buana, & Fenny Purwani. (2024). Implementasi Autentikasi Biometrik Untuk Meningkatkan Keamanan Dan Privasi Pengguna Dompet Digital.	Implementasi autentikasi biometrik	Biometrik, Enkripsi AES	Hasil penelitian ini berhasil menerapkan peningkatan keamanan terhadap proses transaksi
4	Cahyadi, I. H., Hidayatullah, M. A., & Ramdan, S. N. (n.d.). Perancangan Sistem Otentikasi Berbasis One Time Password (Otp) Dengan Algoritma Rsa Sebagai Metode Autentikasi.	Integrasi keamanan dengan OTP	OTP, RSA Algoritma	Sistem otentikasi berbasis One Time Password (OTP) merupakan metode keamanan yang melibatkan penggunaan kata sandi sekali pakai yang berlaku hanya untuk satu sesi otentikasi, sehingga menjadi salah satu metode keamanan yang tinggi

Penelitian ini membantu mengatasi masalah keamanan yang terkait dengan integrasi sistem yang sering dihadapi perusahaan. Studi ini menunjukkan bagaimana keamanan dengan 2FA dapat terintegrasi dengan mudah pada tampilan multi-aplikasi dengan menggunakan teknik seperti biometrik sidik jari dan otentikasi dengan OTP. Meningkatkan efisiensi operasional dan pengalaman pengguna sekaligus meningkatkan keamanan sistem adalah keunggulan utamanya. Penelitian ini menunjukkan bahwa ada metode praktis yang dapat digunakan perusahaan untuk mencapai tujuan bisnisnya secara lebih efisien.

Metode Penelitian

Alur Penelitian



Gambar 2. Alur Penelitian

Penelitian ini dilaksanakan melalui serangkaian tahapan sistematis yang dirancang untuk menjawab tantangan kerentanan pada mekanisme autentikasi konvensional berbasis teks. Alur penelitian secara komprehensif dipetakan ke dalam lima fase utama sebagai berikut:

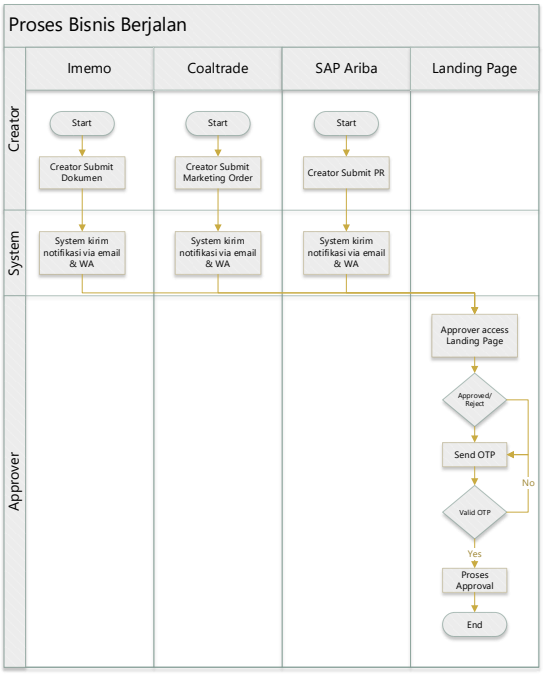
1. Tahap Inisiasi dan Identifikasi Masalah: Langkah awal dimulai dengan observasi terhadap efektivitas sistem login yang ada dan identifikasi risiko keamanan pada manajemen kredensial tradisional. Pada tahap ini, dilakukan perumusan masalah mengenai urgensi penerapan autentikasi biometrik (sidik jari) sebagai metode verifikasi identitas yang unik dan sulit dipalsukan.
2. Tahap Studi Literatur dan Pengumpulan Data: Proses berlanjut pada pengumpulan referensi akademik terkait algoritma pengenalan pola sidik jari, dan standar keamanan biometrik. Secara paralel, dilakukan observasi terhadap perangkat keras sensor sidik jari dan pemetaan kebutuhan fungsional terkait proses registrasi (enrollment) serta verifikasi pengguna.
3. Tahap Analisis dan Perancangan (Agile Iteration): Mengacu pada metodologi Agile, dilakukan analisis terhadap sistem berjalan dan perancangan arsitektur keamanan yang mengintegrasikan data biometrik. Tahap ini mencakup pemodelan alur ekstraksi minutiae sidik jari.
4. Tahap Implementasi dan Integrasi: Pada fase ini, modul pemindai sidik jari diintegrasikan ke dalam ekosistem aplikasi sebagai faktor autentikasi utama atau tambahan (MFA). Proses pengembangan dilakukan secara iteratif untuk memastikan bahwa data biometrik diproses dengan latensi rendah dan tersimpan secara aman dalam modul enkripsi, sehingga integrasi identitas tetap terjaga tanpa mengorbankan privasi pengguna.
5. Tahap Pengujian, Evaluasi, dan Penarikan Kesimpulan: Tahap akhir melibatkan pengujian teknis terhadap uji penerimaan pengguna melalui User Acceptance Test (UAT). Hasil pengujian dievaluasi untuk memastikan bahwa solusi biometrik yang dibangun telah meningkatkan level keamanan akses secara signifikan, yang diakhiri dengan penyusunan kesimpulan dan rekomendasi pengembangan terkait skalabilitas sistem identitas biometrik.

Metode Pengumpulan Data

Pada penelitian ini menggunakan teknik pengumpulan data observasi, wawancara serta studi literatur yang meliputi observasi, yang dilakukan dengan pengamatan serta melakukan uji coba pada aplikasi yang akan diintegrasikan pada *environment development*, termasuk dengan bahasa pemrograman yang digunakan pada aplikasi tersebut. Kemudian proses wawancara yang dilakukan dengan pengguna (*creator & approver*) melalui proses diskusi internal yang dibantu oleh tim *Business Partner* yang merujuk pada hasil observasi yang dilakukan sebelumnya. Serta studi literatur dilakukan dengan mencari informasi teori penelitian dari berbagai sumber termasuk jurnal.

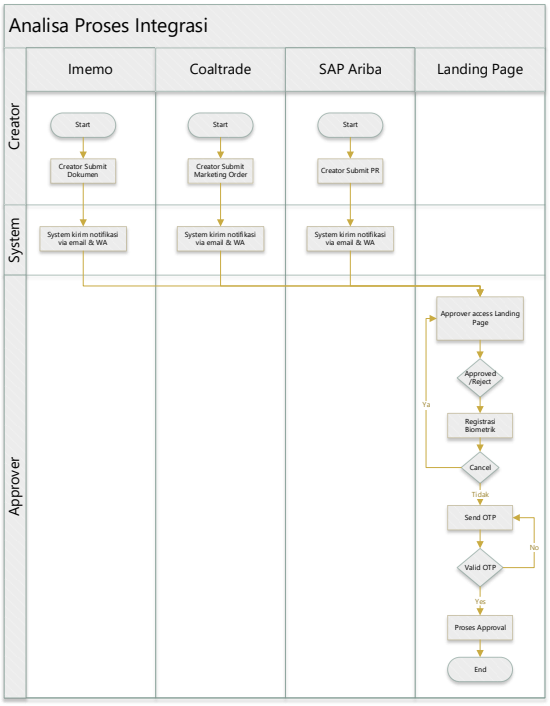
Analisis Sistem Berjalan

Berdasarkan hasil dari data proses analisis yang dilakukan pada tahap sebelumnya yang sudah dipelajari dan dievaluasi dari berbagai permasalahan yang ada untuk kebutuhan untuk implementasi integrasi tiga aplikasi utama dengan tampilan antarmuka tunggal yang dimodelkan dengan flowchart yang digunakan untuk menyederhanakan terkait masalah pada proses bisnis saat ini yang merujuk pada flowmap dibawah ini



Gambar 3. Proses Bisnis Berjalan

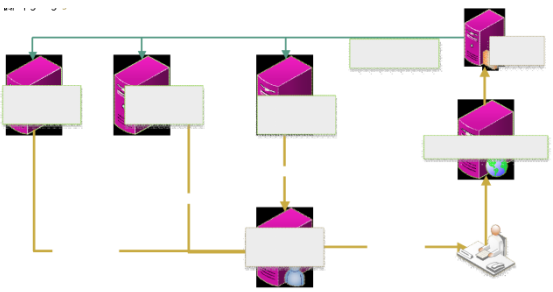
Pada tahap analisis sistem berjalan dilakukan untuk memahami dan mengevaluasi proses bisnis yang ada serta mengidentifikasi permasalahan yang muncul dalam implementasi integrasi multi-aplikasi dengan autentikasi OTP. Saat ini, alur proses persetujuan dimulai ketika pengguna menerima notifikasi email yang berisi token. Pengguna kemudian mengakses halaman arahan (landing page) untuk memulai proses persetujuan. Dari halaman ini, pengguna dapat langsung mengakses aplikasi-aplikasi terintegrasi melalui menu utama, memungkinkan persetujuan dokumen secara efisien dan terstruktur tanpa perlu berpindah aplikasi. Meskipun demikian, seperti yang diuraikan pada bagian Pendahuluan, sistem ini masih memiliki kerentanan keamanan.



Gambar 4. Analisa Proses Integrasi

Untuk proses pengembangan integrasi dengan biometrik pada otentikasi OTP saat *approver* melakukan proses persetujuan maka setelah menampilkan informasi OTP, *approver* harus melakukan validasi biometrik dengan menggunakan sidik jari untuk melakukan pengiriman notifikasi OTP, sehingga kode tersebut hanya dikirimkan sesuai dengan hasil registrasi sidik jari *approver*, selain itu, biometrik ini hanya bisa pada saat user akses di browser yang sama, jika sudah berpindah browser harus registrasi biometrik kembali.

Selain itu untuk proses persetujuan menggunakan otentikasi dengan OTP untuk menjaga keamanan terhadap data yang dilakukan persetujuan, sehingga tidak akan terjadi proses persetujuan tanpa ada validasi dari pihak yang melakukan persetujuan tersebut.



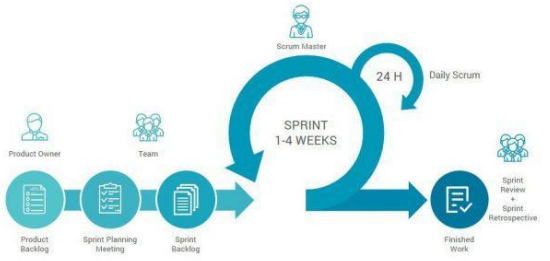
Gambar 5. Arsitektur Sistem

Untuk model arsitektur sistem yang digunakan dalam integrasi antarmuka tunggal pada otentikasi OTP dengan biometrik sidik jari adalah **client-server**, yang digambarkan dengan jelas pada diagram di atas.

Sistem ini terdiri dari beberapa komponen yang berkomunikasi satu sama lain melalui permintaan (*request*) dan balasan (*response*). Serta aplikasi ini akan dikembangkan dengan menggunakan Node JS sebagai bahasa pemrograman sebagai halaman arahan (*landing page*) antarmuka tunggal yang mengimplementasi otentikasi OTP dan biometrik serta MySQL dan Mongodb sebagai basis data untuk menyimpan data biometrik tersebut.

Metode Perancangan Sistem

Untuk Metodologi pengembangan integrasi pada penelitian ini penulis menggunakan metode *Agile* yang melakukan pengembangan perangkat lunak dengan menggunakan beberapa tahapan antara lain : analisa kebutuhan, desain sistem, pengujian dan implementasi secara iteratif dengan metode *sprint* setiap iterasi sehingga mampu mencapai hasil yang maksimal, untuk tahapan dari metode tersebut bisa di lihat pada gambar dibawah ini :



Gambar 6. Agile Framework

Metode Pengujian Sistem

Untuk pengujian akan menggunakan metode *Blackbox* dan *User Acceptance Test* (UAT) di mana sistem akan diuji dengan memperhatikan fungsi yang akan berjalan kemudian ketika diserahkan kepada pengguna, pengguna dapat memberikan umpan balik terkait sistem yang ada.

Blackbox Testing

Proses ini dimulai dengan melakukan proses input data yang dilakukan oleh tim QA berdasarkan *test case* yang sudah dibuat yang kemudian jika ada umpan balik maka akan diproses oleh tim *development*, sehingga sistem akan berjalan dengan sesuai dengan harapan.

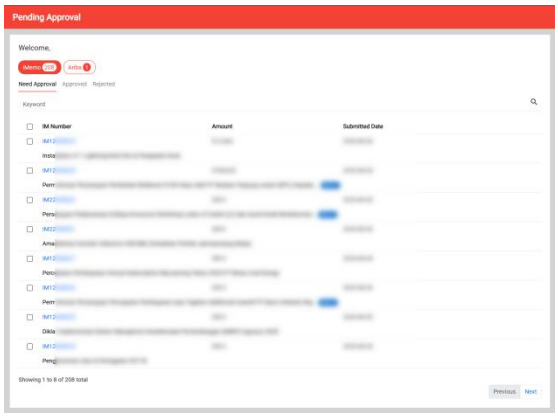
User Acceptance Test

Proses ini dimulai merujuk pada hasil Blackbox Testing terhadap sistem yang sudah dapat digunakan, serta diberikan kepada pengguna untuk dilakukan proses pengoperasian sesuai dengan proses bisnis yang sudah direncanakan. Pengguna akan diminta untuk memberikan umpan balik terkait kelayakan sistem berdasarkan *test case* sebelumnya.

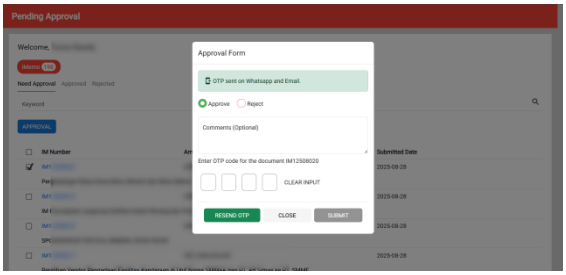
Hasil dan Pembahasan

Implementasi

Berdasarkan hasil analisis, perancangan dan pengembangan aplikasi dengan menggunakan metode Agile (Scrum), berhasil mengembangkan dan mengimplementasi integrasi otentikasi OTP dengan biometrik sidik jari pada halaman antarmuka tunggal. Tampilan antarmuka tunggal yang terintegrasi dengan OTP dan biometrik sidik jari ini dapat dilihat pada gambar di bawah ini, yang menunjukkan pengguna saat mengakses halaman antarmuka tunggal serta saat akan melakukan proses persetujuan.



Gambar 7. Tampilan Antarmuka



Gambar 8. Input OTP

Pengujian

Blackbox Testing

Setelah melakukan pengujian *black box* untuk memastikan seluruh fungsionalitas aplikasi berjalan dengan benar sesuai spesifikasi. Pengujian ini mencakup validasi setiap fitur utama, seperti akses masuk halaman antarmuka tunggal, pencarian data, proses persetujuan pada setiap aplikasi pada bagian antarmuka tunggal. Tabel 2 adalah daftar *test case* yang digunakan pada *blackbox testing.*

Tabel 2. Testcase Blackbox

Test Case ID	Test Case Title	Pre-requisite	Test Steps	Expected Result
TC-NEG-01	Persetujuan Gagal Karena OTP Salah	Approver login, ada transaksi menunggu persetujuan	1. Pilih transaksi di salah satu tab 2. Klik Setujui 3. Masukkan OTP salah 4. Coba	Sistem menolak persetujuan, muncul error OTP tidak valid, transaksi tetap menunggu

			verifikasi sidik jari	
TC-NEG-02	Persetujuan Gagal Karena Sidik Jari Tidak Cocok	Approver login, ada transaksi menunggu persetujuan	1. Pilih transaksi 2. Klik Setujui 3. Masukkan OTP benar 4. Verifikasi sidik jari salah	Sistem menolak persetujuan, muncul error Sidik jari tidak cocok, transaksi tetap menunggu
TC-NEG-03	Persetujuan Gagal Karena OTP Kadaluarsa	Approver login, ada transaksi menunggu persetujuan	1. Pilih transaksi 2. Klik Setujui 3. Masukkan OTP kadaluarsa 4. Verifikasi sidik jari	Sistem menolak persetujuan, muncul error OTP kadaluarsa, transaksi tetap menunggu

UAT (User Acceptance Testing)
Setelah pengujian internal selesai, proses dilanjutkan dengan **UAT** untuk memvalidasi aplikasi langsung dengan pengguna. Pengujian ini dilakukan untuk memastikan aplikasi tidak hanya berfungsi dengan baik, tetapi juga memenuhi kebutuhan bisnis dan alur kerja pengguna. Hasilnya menjadi dasar untuk persetujuan akhir sebelum aplikasi diluncurkan.

Pembahasan
Berdasarkan hasil penelitian termasuk dengan analisa tentang kebutuhan metode serta kesimpulan bahwa pengembangan dengan Agile dapat melakukan adaptasi, sehingga dapat menyesuaikan *timeline* dalam pengembangan sistem di integrasi multi aplikasi. Selain itu, kemampuan inspeksi dapat secara rutin memberikan *reminder* setiap anggota tim untuk menyelesaikan *timeline* dalam pengembangan sistem. Transparansi saat pengembangan dapat membantu setiap pihak yang terlibat termasuk manajemen untuk pertimbangan dalam memberikan *task* / *product backlog*. Metode *Agile* mengadaptasi segala variasi dalam waktu pengembangan sistem termasuk lingkup pembaruan maupun perubahan yang berasal dari *feedback* pengguna.
Sistem informasi integrasi otentikasi OTP dengan biometrik sidik jari bertujuan meningkatkan keamanan user (approver) didalam proses bisnis serta operasional saat melakukan persetujuan atau review dokumen, sehingga berdasarkan menghasilkan integrasi otentikasi dengan konsep 2FA yang dapat meningkatkan keamanan proses bisnis serta operasional di dalam lingkup perusahaan.

Penerapan Metode Agile
Pengembangan sistem ini mengadopsi metode *Agile Framework* untuk memastikan proyek dapat diselesaikan dengan cepat dan fleksibel. Dengan timeline yang singkat, metode ini menjadi pilihan yang ideal. Metode ini secara signifikan mempercepat waktu pengembangan, memungkinkan sistem dapat diselesaikan dalam periode yang jauh lebih singkat dibandingkan dengan metode tradisional.

Pengujian Sistem
Untuk menjamin kualitas dan fungsionalitas sistem yang dikembangkan, dilakukan dua jenis pengujian:

- **Black-box Testing:** Pengujian ini dilakukan untuk memverifikasi fungsionalitas sistem secara keseluruhan tanpa melihat kode internal. Tujuannya adalah memastikan bahwa fitur-fitur yang dirancang, seperti integrasi data antar aplikasi iMemo, SAP Ariba dan Coaltrade, berfungsi dengan benar sesuai dengan spesifikasi.
- **User Acceptance Test (UAT):** Setelah fungsionalitas terjamin, UAT dilakukan dengan melibatkan pengguna akhir. Pengujian ini bertujuan untuk memastikan sistem dapat diterima dan digunakan dengan baik oleh pengguna. UAT ini sangat krusial untuk memastikan bahwa sistem integrasi ini benar-benar memenuhi ekspektasi dan kebutuhan bisnis mereka.

Pengujian ini memastikan bahwa sistem yang dihasilkan dipastikan berfungsi serta dapat memberikan hasil yang optimal.

Kesimpulan dan Saran

Penelitian ini berhasil mengimplementasikan sistem informasi pada aplikasi antarmuka tunggal yang mengintegrasikan mekanisme One-Time Password (OTP) dan autentikasi biometrik sidik jari. Penerapan Agile Framework terbukti menjadi faktor krusial dalam mempercepat siklus pengembangan sistem di tengah batasan waktu yang ketat, sekaligus memastikan keselarasan antara fungsionalitas teknis dan strategi bisnis. Keberhasilan integrasi ini didorong oleh struktur peran yang jelas dan komunikasi iteratif yang memungkinkan adaptasi cepat terhadap perubahan kebutuhan. Hasil pengujian menunjukkan bahwa penggabungan dua faktor autentikasi ini tidak hanya memperkuat lapisan keamanan akses, tetapi juga memberikan efisiensi operasional yang signifikan serta nilai tambah instan bagi pengguna akhir melalui antarmuka yang terpusat.
Meskipun sistem telah berhasil diimplementasikan, penelitian selanjutnya disarankan untuk mengeksplorasi skalabilitas sistem pada infrastruktur cloud yang lebih luas guna meminimalkan *latency* saat terjadi lonjakan permintaan autentikasi biometrik. Selain itu, perlu dilakukan analisis mendalam mengenai pemulihan akun (*account recovery*) jika terjadi kegagalan pada perangkat keras sensor sidik jari. Pengembangan lebih lanjut juga dapat mempertimbangkan integrasi algoritma kecerdasan buatan untuk mendeteksi anomali

perilaku pengguna sebagai lapisan keamanan tambahan di luar metode biometrik yang sudah ada.

Daftar Pustaka

[1] A. M. Asmiddin, "Perancangan Dan Implementasi Sistem Informasi Pemesanan Tiket Kapal Wanci – Lasalimu Dengan Integrasi Multiplatform Dan Layanan Seluler Design and Implementation of the Wanci – Lasalimu Ship Ticket Booking Information System With Multiplatfrom Integration," vol. 13, no. 2, pp. 28–36, 2024.

[2] S. Wibawa, S. Suryanto, and R. Ningsih, "Perlindungan Data Digital Dengan Time-Based One-Time Password (TOTP)," *INSANtek*, vol. 5, no. 1, pp. 30–36, 2024.

[3] D. Fajariandono, W. W. Sitorus, E. Desianto, F. Aer, A. Rahim, and Y. A. Pramata, "Upaya Risk Management Dalam Mengatasi Penipuan Modus Social Engineering Melalui Smartphone," *EKOMA J. Ekon. Manajemen, Akunt.*, vol. 3, no. 3, pp. 752–759, 2024.

[4] Nico Abrarsyah Atallah and Mardi Mardi, "Penggunaan Metode Agile Scrum Pada Perancangan Sistem Informasi Surat Izin Penelitian di BAKESBANGPOL Lombok Tengah," *Neptunus J. Ilmu Komput. Dan Teknol. Inf.*, vol. 2, no. 3, pp. 371–384, 2024, doi: 10.61132/neptunus.v2i3.276.

[5] I. G. Arianto, W. Witanti, and H. Ashaury, "Sistem Keamanan Otentikasi Pengguna Pada Modul Single Sign On Menggunakan OAuth 2.0 dan One Time Password," *J. Ilmu Komput. dan Teknol.*, vol. 6, no. 1, pp. 25–31, 2025, doi: 10.35960/ikomti.v6i1.1768.

[6] A. I. A. Mashudi and A. Prihanto, "Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication," *J. Informatics Comput. Sci.*, vol. 6, no. 03, pp. 630–638, 2025.

[7] Miftahul Jannah, Muhamad Faris Hidayat, Mutiara Agustiyyani, Pandu Wira Buana, and Fenny Purwani, "Implementasi Autentikasi Biometrik Untuk Meningkatkan Keamanan Dan Privasi Pengguna Dompet Digital," *J. Sci. Res. Dev.*, vol. 6, no. 2, pp. 531–539, 2024, doi: 10.56670/jsrd.v6i2.606.

[8] F. Y. Nadhotul Sufi, D. K. Putri, and D. S. Senapan, "Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review," *Semin. Nas. Akunt. dan Call Pap.*, vol. 3, no. 1, pp. 19–29, 2023, doi: 10.33005/senapan.v3i1.281.

[9] H. H. Amirullah, A. Eviyanti, and S. Sumarno, "Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android," *SMATIKA J. STIKI Inform. J.*, vol. 14, no. 01, pp. 23–32, 2024.

[10] I. H. Cahyadi, M. A. Hidayatullah, and S. N. Ramdan, "Perancangan Sistem Otentikasi Berbasis One Time Passworsd (Otp) Dengan Algoritma Rsa Sebagai Metode Autentikasi: Implementasi …," *Jurnal.Umj.Ac.Id*, pp. 8–13.

[11] M. Informatika and U. A. Yogyakarta, "METODE AGILE SCRUM DALAM PEMBUATAN APLIKASI PERMOHONAN INFORMASI E-PPID BAWASLU Abstraksi Bawaslu Sleman merupakan lembaga yang bertugas mengawasi jalannya pemilihan umum . Seperti informasi yang tersedia tidak tertata dengan baik . Seiring berjalannya wa," vol. 5, no. 1, 2023.

[12] S. Kacung, C. Pamungkas Putra Bagyana, and D. Cahyono, "Analisis Sentimen Terhadap Layanan Samsat Digital Nasional (Signal) Menggunakan Metode Svm," *J. Mnemon.*, vol. 7, no. 1, pp. 118–122, 2024, doi: 10.36040/mnemonic.v7i1.9557.

[13] M. S. D. Dairi, M. S. Asih, and others, "Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan," *J. Ilmu Komput. dan Sist. Inf.*, vol. 2, no. 1, pp. 98–107, 2023.

[14] M. K. Nursyarif, A. Arbansyah, and M. T. Sumadi, "Sistem Keamanan Berbasis Sidik Jari pada Prodi TI Universitas Muhammadiyah Kalimantan Timur," *J. Inform. Polinema*, vol. 11, no. 1, pp. 19–28, 2024.

[15] F. Mossal, S. Achmady, and Z. Khalid, "Perancangan Sistem Pengamanan Dokumen Menggunakan Algoritma Time-Based One Time Password (TOTP) Pada Two-Factor Authentation (2FA) Berbasis Web Design of a Document Security System Using the Time-Based One-Time Password (TOTP) Algorithm in Web-Based Two-F," vol. 3, no. 2, pp. 31–36, 2022.