The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4843

Desain Dan Pengembangan *Secure Integration Model* Pada Integrasi Layanan Melalui Mini Program: Studi Kasus *Mobile Banking* PT XYZ

Ghiant Masua Khols[1], Setiadi Yazid[2]
ghiant.masua@ui.ac.id[1], setiadi@cs.ui.ac.id[2]
[1,2] Universitas Indonesia

Informasi Artikel

Diterima : 15 Apr 2025
Direvisi : 22 Apr 2025
Disetujui : 30 Apr 2025

Kata Kunci

Mini Program, OAuth 2.0, Keamanan Data, Integrasi Layanan, Uji Penetrasi.

Abstrak

Penelitian ini mengembangkan *Secure Integration Model* berbasis OAuth 2.0, enkripsi AES-256, dan tokenisasi *Unique Code* untuk menyediakan integrasi yang aman antara *mobile banking* PT XYZ dan mitra melalui Mini Program. Tujuan utama penelitian ini adalah memungkinkan *seamless login* dan pembayaran pesanan nasabah menggunakan *virtual account* dengan tingkat keamanan yang tinggi. Model ini dirancang untuk memastikan bahwa hanya entitas yang terotorisasi yang dapat mengakses data sensitif melalui mekanisme autentikasi dan otorisasi yang kuat.

Pengembangan model ini menjadi solusi esensial dalam menyediakan integrasi layanan yang aman untuk akses data nasabah dan pembayaran melalui *virtual account* yang merupakan kebutuhan utama dalam integrasi antara PT XYZ dan mitra. Selain itu, model ini dirancang untuk menghadapi tantangan keamanan terkait perlindungan data nasabah serta mengatasi risiko serangan siber seperti pencurian data, manipulasi transaksi, dan penyalahgunaan kredensial. *Greybox penetration testing* diterapkan untuk mengidentifikasi potensi kerentanan pada *API Gateway*, autentikasi token, dan komunikasi antar sistem. Hasil pengujian menunjukkan bahwa integrasi menggunakan model ini memiliki tingkat kerentanan yang rendah dan telah sesuai dengan standar keamanan yang berlaku. Penerapannya diharapkan dapat meningkatkan keamanan, efisiensi, dan skalabilitas layanan digital PT XYZ.

Keywords

Mini Program, OAuth 2.0, Data Security, Service Integration, Penetration Testing.

Abstract

This research develops a Secure Integration Model based on OAuth 2.0, AES-256 encryption, and Unique Code tokenization to provide a secure integration between PT XYZ's mobile banking and its partners through the Mini Program. The primary objective of this study is to enable seamless login and customer order payments using virtual accounts with a high level of security. The model is designed to ensure that only authorized entities can access sensitive data through robust authentication and authorization mechanisms.

The development of this model serves as an essential solution to provide a secure service integration for accessing customer data and processing payments through virtual accounts, which is a critical requirement in the integration between PT XYZ and its partners. Additionally, this model addresses security challenges related to customer data protection and mitigates the risks of cyberattacks such as data theft, transaction manipulation, and credential misuse. Greybox penetration testing is applied to identify potential vulnerabilities in the API Gateway, token authentication, and inter-system communication. The testing results demonstrate that the integration using this model has low vulnerability and meets established security standards. Its implementation is expected to improve the security, efficiency, and scalability of PT XYZ's digital services.

A. Pendahuluan

Transformasi digital telah mengubah lanskap industri perbankan di Indonesia, didorong oleh meningkatnya penetrasi internet yang mencapai 79,50% pada tahun 2024 [1]. Masyarakat semakin bergantung pada layanan digital untuk memenuhi kebutuhan perbankan mereka, sehingga bank dituntut untuk mengadopsi teknologi inovatif guna meningkatkan daya saing serta efisiensi layanan. Salah satu strategi yang banyak diterapkan adalah integrasi layanan perbankan dengan platform digital yang memiliki ekosistem luas. PT XYZ, sebagai salah satu bank terbesar di Indonesia, melihat peluang besar dalam pemanfaatan ekosistem WeChat yang tidak hanya berfungsi sebagai aplikasi pesan instan, tetapi juga mencakup layanan pembayaran, e-commerce, dan berbagai fitur keuangan lainnya [2]. Konsep Mini Program yang diusung WeChat memungkinkan pengguna mengakses layanan tanpa harus mengunduh aplikasi tambahan, memberikan kemudahan akses dan interaksi yang lebih cepat.

Meskipun demikian, penggunaan teknologi ini menimbulkan tantangan dalam aspek keamanan informasi. Integrasi Mini Program dengan layanan perbankan melibatkan akses data nasabah oleh mitra serta transaksi pembayaran yang harus dilakukan dengan standar keamanan tinggi. Keamanan informasi menjadi prioritas utama untuk mencegah ancaman seperti peretasan dan kebocoran data yang dapat merugikan nasabah serta mengganggu reputasi bank. Selain itu, bank harus memastikan bahwa penggunaan Mini Program tetap mematuhi regulasi perbankan yang berlaku guna menjamin perlindungan data dan transaksi yang aman. *Secure Software Development* menjadi salah satu pendekatan yang dapat diterapkan untuk mengintegrasikan aspek keamanan sejak tahap awal pengembangan perangkat lunak [3], [4]. Melalui pendekatan ini, validasi input, enkripsi data, serta pengujian keamanan dapat diterapkan untuk mengidentifikasi potensi celah keamanan sebelum sistem diluncurkan.

Penelitian sebelumnya menunjukkan bahwa *Design Science Research* (DSR) dapat menjadi metodologi yang efektif dalam mengembangkan solusi inovatif dalam sistem informasi. DSR menekankan pengembangan dan evaluasi artefak yang dapat menyelesaikan masalah praktis serta memberikan kontribusi akademik [5]. Dalam konteks penelitian ini, DSR digunakan untuk merancang dan mengembangkan model integrasi yang aman bagi Mini Program pada platform mobile banking PT XYZ dalam integrasi data nasabah dan pembayaran. Model ini dikembangkan menggunakan pendekatan *Design Science Research* (DSR) untuk menjamin keamanan data, kontrol akses mitra, dan kepatuhan terhadap standar regulasi dalam transaksi pembayaran digital. Dengan menerapkan proses identifikasi, validasi, dan mitigasi kerentanan secara sistematis, pendekatan ini memastikan bahwa setiap integrasi diuji terhadap ancaman siber sebelum diterapkan. Penelitian menunjukkan bahwa metode ini efektif dalam mengurangi risiko eksploitasi melalui evaluasi berbasis bukti, pengujian penetrasi, dan iterasi perbaikan berkelanjutan [5]. Dengan demikian, model ini tidak hanya meningkatkan keamanan layanan perbankan digital, tetapi juga memperkuat kepercayaan nasabah terhadap perlindungan data dan integritas transaksi.

Selain itu, pengujian keamanan melalui uji penetrasi dalam integrasi layanan digital merupakan komponen penting dalam *Secure Integration Model* (SIM) yang dikembangkan dalam penelitian ini. Uji penetrasi digunakan untuk mengevaluasi

hasil integrasi layanan digital yang dihasilkan oleh model, guna memastikan sistem benar-benar andal dan tahan terhadap serangan siber. Uji penetrasi merupakan metode evaluasi yang mensimulasikan serangan guna mengidentifikasi celah sebelum dapat dieksploitasi, dengan standar seperti *OWASP Top 10* digunakan untuk mendeteksi kelemahan kritis dalam aplikasi *web* dan *mobile* [6]. Proses ini mencakup *reconnaissance* untuk pengumpulan informasi, *scanning* guna mengidentifikasi area rentan, *exploitation* untuk menguji kelemahan, serta *reporting* dan *patching* sebagai langkah mitigasi [7]. Berbagai alat seperti Burp Suite Professional, OWASP ZAP, dan Arachni dapat digunakan untuk mendeteksi kerentanan seperti *SQL Injection* dan *Cross-Site Scripting* (XSS) [8]. Dari segi metode pengujian, *white box testing* memungkinkan analisis mendalam dengan akses penuh ke kode sumber, sementara *black box testing* menguji sistem dari perspektif pengguna tanpa akses ke kode. *Grey box testing* mengombinasikan keduanya untuk cakupan yang lebih luas dan efektif [9]. Pada tahap uji coba menggunakan uji penetrasi, tingkat keparahan setiap celah keamanan yang ditemukan dalam hasil integrasi diukur menggunakan *Common Vulnerability Scoring System* (CVSS) yang memberikan skor dari 0 hingga 10 berdasarkan dampaknya terhadap sistem. CVSS mengklasifikasikan tingkat kerentanan menjadi empat kategori, yaitu Low (0.1-3.9), *Medium* (4.0-6.9), *High* (7.0-8.9), dan *Critical* (9.0-10.0), sehingga membantu dalam menentukan prioritas mitigasi celah keamanan tersebut. Dampak dari kategori *Low* umumnya terbatas pada gangguan kecil tanpa risiko signifikan, kategori *Medium* dapat menyebabkan masalah fungsional tetapi tidak langsung mengancam sistem, kategori *High* berpotensi menyebabkan kebocoran data atau gangguan besar dalam operasi, sementara kategori *Critical* dapat menyebabkan eksploitasi penuh yang berakibat pada hilangnya integritas, kerahasiaan, dan ketersediaan sistem secara menyeluruh [9]. Rekomendasi keamanan dalam uji penetrasi mengacu pada *CIA Triad* (*Confidentiality, Integrity, Availability*) serta standar seperti *ISO/IEC 27001*, *OWASP Top 10* dan *NIST Cybersecurity Framework*. Integrasi prinsip keamanan dalam *Secure Software Development Lifecycle* (SDLC) memastikan keamanan diterapkan sejak tahap awal pengembangan, mengurangi risiko kerentanan di tahap akhir [6], [7].

Penelitian ini bertujuan untuk merancang dan mengembangkan *Secure Integration Model* (SIM) pada Mini Program. *Secure Integration Model* merupakan kerangka kerja sistematis yang terdiri dari berbagai fase untuk meninjau metode integrasi yang digunakan, mengidentifikasi kerentanan pada proses integrasi sistem digital, serta merumuskan langkah mitigasi yang tepat guna menjamin keamanan integrasi antar sistem [5]. Model ini memastikan bahwa setiap metode integrasi diuji terhadap potensi celah keamanan yang telah diidentifikasi, sehingga integrasi dapat berlangsung secara aman dan sesuai dengan regulasi yang berlaku. Dalam konteks ini, SIM dikembangkan khusus untuk mendukung *seamless integration* dalam akses data nasabah dan pembayaran melalui *virtual account*. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi industri perbankan dalam meningkatkan standar keamanan layanan digital serta menjadi referensi bagi pengembangan teknologi finansial yang lebih aman. Selain itu, penelitian ini juga memiliki manfaat akademik dengan memperkaya literatur mengenai keamanan integrasi layanan perbankan digital serta pemanfaatan metodologi DSR dalam

merancang dan mengoptimalkan sistem yang adaptif terhadap tantangan keamanan informasi.

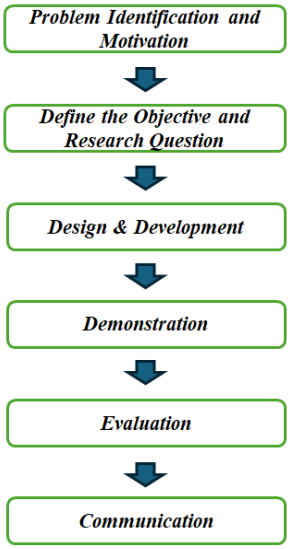
B. Metode Penelitian

Penelitian ini bersifat induktif dengan pendekatan kualitatif dan uji penetrasi sistem hasil integrasi [10]. Data dikumpulkan melalui wawancara, observasi, studi kasus, serta pengujian teknis untuk mengevaluasi keamanan integrasi layanan mini program. Metode ini memberikan pemahaman komprehensif dan applicable untuk organisasi lain dengan kondisi serupa [10].

Penelitian ini mengadopsi Design Science Research (DSR) untuk merancang dan mengevaluasi *secure integration model*. DSR dipilih karena kemampuannya menggabungkan desain artefak inovatif dengan evaluasi sistematis, memastikan relevansi praktis dan kontribusi teoretis [11]. Selain itu, DSR memungkinkan identifikasi dan mitigasi kerentanan secara sistematis, validasi keamanan melalui pengujian empiris, serta adaptasi terhadap ancaman siber dan regulasi yang terus berkembang, sehingga meningkatkan keandalan dan ketahanan sistem terhadap eksploitasi keamanan [5]. Langkah-langkah DSR mencakup:

1. *Problem Identification and Motivation*: Identifikasi masalah, skala dampak, dan manfaat solusi [5], [11].
2. *Define the Objectives for a Solution*: Perumusan tujuan solusi berdasarkan analisis masalah [5], [11].
3. *Design and Developmen*t: Pengembangan artefak berbasis model atau sistem yang menyelesaikan masalah [5], [11].
4. *Demonstration*: Pengujian artefak dalam skenario nyata atau simulasi [5], [11].
5. *Evaluation*: Analisis efektivitas artefak melalui uji coba dan simulasi [5], [11].
6. *Communication*: Dokumentasi dan penyebarluasan hasil penelitian [5], [11].

Berikut adalah ringkasan alur penelitian dalam bentuk gambar:



Gambar 1. Tahapan Penelitian

Instrumen penelitian dalam studi ini terdiri dari wawancara semi-terstruktur dan dokumen hasil uji penetrasi. Wawancara bertujuan untuk mengumpulkan data kualitatif yang mendalam, sementara uji penetrasi digunakan untuk mengidentifikasi dan mengevaluasi kerentanannya dalam sistem keamanan. Kedua

instrumen ini bekerja secara sinergis untuk memastikan validitas serta efektivitas desain integrasi sistem keamanan pada Mini Program di PT XYZ [12], [13], [14].

Wawancara dilakukan dengan pendekatan terbuka (*open-ended*), memberikan ruang bagi narasumber untuk menyampaikan pandangannya dengan bebas, namun tetap terarah sesuai panduan yang telah disiapkan. Fokus utama wawancara ini adalah untuk memahami metode integrasi data yang telah diterapkan pada *mobile banking* PT XYZ. Hasil dari wawancara ini menjadi landasan untuk merancang sistem keamanan yang lebih baik, dengan menggabungkan metode yang telah digunakan dan studi literatur yang relevan. Setelah desain sistem integrasi yang aman dirancang, focus group discussion (FGD) dilaksanakan bersama pakar untuk mengevaluasi dan menyempurnakan desain tersebut. FGD ini bertujuan untuk memastikan bahwa desain sistem yang diusulkan telah matang dan siap untuk diuji serta dikembangkan lebih lanjut [7], [8].

Selain wawancara dan FGD, uji penetrasi digunakan sebagai metode untuk mengidentifikasi celah-celah dalam sistem keamanan hasil integrasi. Uji penetrasi dilakukan dengan simulasi serangan oleh pihak ketiga yang bertindak sebagai peretas etis. Berbagai skenario serangan, seperti *SQL injection*, *cross-site scripting* (XSS), dan lainnya, diuji untuk menilai kerentanannya terhadap ancaman. Hasil dari uji penetrasi ini dianalisis secara menyeluruh untuk mengidentifikasi kelemahan dalam sistem dan memberikan rekomendasi perbaikan guna memperkuat ketahanan terhadap ancaman siber [15], [16], [17], [18], [19].

Metode pengumpulan data dalam penelitian ini dilakukan melalui wawancara untuk mendapatkan wawasan tentang protokol dan standar integrasi Mini Program yang aman, serta untuk memahami standar keamanan yang diterapkan. Narasumber wawancara terdiri dari para pakar dalam pengembangan produk digital yang memahami ISO 27001 dan *Digital Risk*. Setelah wawancara selesai, FGD dilakukan untuk mengevaluasi dan menyempurnakan desain sistem berdasarkan temuan awal. FGD ini bertujuan untuk memastikan bahwa model yang dihasilkan lebih aplikatif dan sesuai dengan standar keamanan yang berlaku [5], [20].

Uji penetrasi dilakukan menggunakan teknik greybox, di mana penguji diberikan akses terbatas namun mendalam untuk mengidentifikasi celah keamanan dalam integrasi layanan melalui Mini Program pada mobile banking. Fokus utama uji ini adalah pada evaluasi hasil integrasi, terutama pada aliran data nasabah antara aplikasi mobile banking dan mitra, serta mekanisme pengiriman kode pembayaran yang menjadi komponen kritis dalam transaksi digital [7], [21], [22], [23], [24], [25], [26]. Hasil uji penetrasi terhadap sistem hasil integrasi disusun dalam laporan komprehensif yang mencakup skenario pengujian, temuan kerentanan, dan rekomendasi perbaikan untuk memperkuat sistem secara menyeluruh.

Dalam pengolahan data, wawancara dan FGD dianalisis dengan metode analisis tematik. Dimulai dengan transkripsi wawancara secara verbatim untuk memastikan akurasi informasi, kemudian dilakukan koding untuk mengidentifikasi kata kunci dan tema-tema utama yang relevan dengan tujuan penelitian. Temuan ini dibandingkan dengan hasil studi literatur untuk memastikan validitasnya sebelum digunakan dalam FGD untuk penyempurnaan model integrasi. Hasil dari FGD kemudian digunakan untuk memperkuat desain sistem yang lebih aplikatif dan aman [17], [22], [27].

Sementara itu, hasil uji penetrasi terhadap sistem hasil integrasi digunakan untuk mengevaluasi celah-celah dalam sistem, seperti kelemahan autentikasi, enkripsi data, dan perlindungan terhadap serangan siber. Temuan ini memberikan bukti empiris yang penting dalam merancang solusi keamanan yang lebih tangguh. Rekomendasi yang dihasilkan dari uji penetrasi ini akan digunakan untuk memperbaiki sistem dan memastikan bahwa integrasi layanan melalui Mini Program di PT XYZ dapat beroperasi dengan aman sesuai standar keamanan yang ditetapkan [6], [8], [28].

C. Hasil dan Pembahasan

Problem Identification and Motivation

PT XYZ menghadapi tantangan besar dalam mengintegrasikan layanan Mini Program yang dikembangkan oleh mitra dengan *mobile banking* mereka. Kebutuhan utama dari integrasi ini adalah memastikan adanya model layanan yang dapat mengakomodasi dua proses penting, yaitu penyediaan data nasabah dan pembayaran yang terintegrasi secara langsung ke *mobile banking* PT XYZ. Saat ini, proses integrasi tersebut belum memiliki standar yang efektif dalam mengelola akses mitra terhadap data nasabah maupun memastikan keamanan transaksi yang dilakukan. Ketidakefisienan dalam proses autentikasi, otorisasi, dan validasi akses menyebabkan potensi terjadinya akses tidak sah, kebocoran data sensitif, dan penyalahgunaan layanan. Selain itu, kurangnya pengelolaan yang tepat terhadap permintaan transaksi dari mitra dapat mengakibatkan terganggunya keandalan sistem dan pengalaman pengguna.

Ketiadaan model integrasi yang aman juga memperbesar risiko terhadap ancaman serangan yang dapat mengganggu ketersediaan layanan, terutama pada komunikasi data yang tidak terlindungi dengan baik. Infrastruktur yang tidak memiliki mekanisme pemantauan dan pengelolaan lalu lintas yang memadai menjadi celah potensial bagi penyusupan atau serangan yang dapat merugikan PT XYZ dan mitra. Oleh karena itu, diperlukan suatu model integrasi yang mampu mengelola seluruh proses secara aman, memastikan bahwa setiap permintaan akses atau transaksi telah terverifikasi dengan benar, serta memberikan perlindungan yang efektif terhadap data sensitif. Dengan demikian, integrasi layanan antara Mini Program mitra dan *mobile banking* PT XYZ dapat dilakukan secara aman, efisien, dan andal.

Define the Objectives for a Solution

PT XYZ menghadapi tantangan dalam mengintegrasikan layanan Mini Program dengan platform mobile banking yang mereka miliki. Kebutuhan utama dari integrasi ini adalah menyediakan akses data pengguna dan pembayaran secara aman tanpa mengorbankan konsistensi proses dan pengalaman pengguna. Saat ini, model integrasi yang diterapkan oleh PT XYZ mengandalkan protokol OAuth 2.0 untuk autentikasi dan enkripsi AES256 untuk melindungi komunikasi data. Model ini dirancang untuk mengamankan komunikasi antara aplikasi mobile banking, layanan PT XYZ, dan layanan mitra, dengan API Gateway sebagai lapisan perlindungan utama.

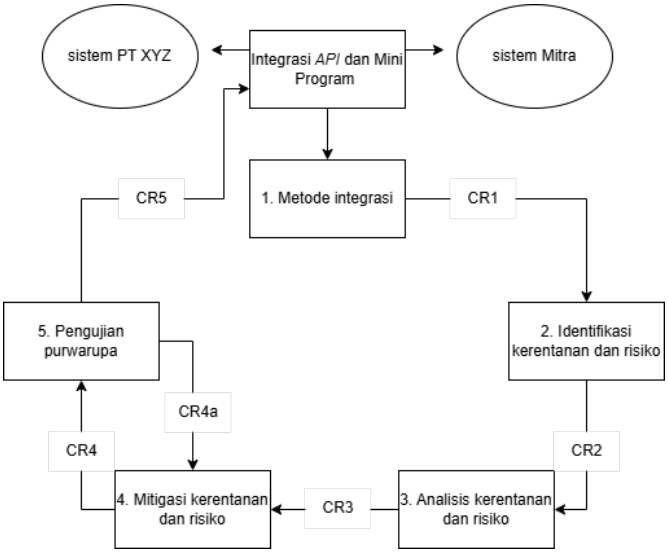
Namun, model integrasi yang diterapkan saat ini hanya cocok untuk integrasi berbasis *web* yang bersifat *webview*, di mana proses autentikasi OAuth 2.0 menghasilkan *URL web* yang kemudian dibuka melalui *webview* di dalam aplikasi *mobile banking*. Melalui mekanisme ini, pengguna diarahkan ke halaman *web* tertentu yang dikelola oleh mitra, di mana data nasabah yang terhubung dengan sesi autentikasi dapat diakses atau dikelola. Pendekatan ini bekerja dengan baik untuk aplikasi berbasis web, tetapi kurang cocok dengan Mini Program yang merupakan bagian dari aplikasi *mobile banking* dan membutuhkan proses integrasi yang lebih terstruktur serta aman tanpa mengandalkan *URL* yang dibuka melalui *webview*.

Perbedaan mendasar ini membuat pendekatan integrasi yang ada tidak efektif jika diterapkan pada Mini Program. Oleh karena itu, diperlukan suatu model integrasi baru yang mampu mengakomodasi kebutuhan komunikasi antara aplikasi mobile banking, server PT XYZ, dan server mitra dengan lebih aman dan efisien. Model integrasi yang diusulkan perlu mengatasi kelemahan yang ada dan memastikan bahwa seluruh proses autentikasi, otorisasi, dan akses data dapat dilakukan dengan validasi yang ketat dan perlindungan menyeluruh terhadap data yang dipertukarkan.

Design and Development

Secure Integration Model (SIM) untuk Mini Program merupakan kerangka kerja integrasi sistem yang dirancang untuk memastikan keamanan data dalam proses integrasi antara *mobile banking* PT XYZ dan mitra melalui penerapan mekanisme autentikasi, enkripsi, dan kontrol akses yang ketat. Model ini mengadopsi prinsip-prinsip keamanan yang mengacu pada standar OWASP serta menerapkan konsep secure by design untuk menjamin kerahasiaan, integritas, dan ketersediaan data. Selain itu, SIM dirancang untuk mengidentifikasi, memvalidasi, dan mengatasi potensi kerentanan melalui metode integrasi yang aman, mitigasi kerentanan yang efektif, dan proses pengujian yang menyeluruh, sehingga menciptakan komunikasi antar sistem yang aman dan andal.

Dalam merancang *Secure Integration Model*, analisis risiko menjadi komponen fundamental yang diperlukan untuk memastikan bahwa seluruh potensi ancaman keamanan teridentifikasi dan diatasi melalui strategi mitigasi yang sesuai. Penerapan standar keamanan tanpa disertai proses analisis risiko yang komprehensif dapat menyebabkan kerentanan seperti validasi input yang tidak memadai, pengaturan izin yang keliru, serta penerapan enkripsi yang lemah sehingga berpotensi dieksploitasi oleh penyerang. Oleh karena itu, prinsip *Economy of Mechanism* dan *Fail-Safe Default* diterapkan dalam model ini untuk memastikan bahwa setiap mekanisme keamanan yang digunakan tetap sederhana, efektif, dan tidak menyisakan celah bagi potensi serangan.



Gambar 2. Relasi Komponen *Secure Integration Model*

Diagram menunjukkan relasi antar komponen utama dalam *Secure Integration Model* (SIM) untuk Mini Program, yang dirancang guna memastikan keamanan integrasi antara sistem PT XYZ dan sistem mitra. Proses diawali dengan penyusunan metode integrasi berdasarkan masukan dari kedua pihak (CR1 dan CR5), kemudian dilanjutkan dengan identifikasi dan analisis kerentanan serta risiko oleh mitra (CR2 dan CR3). Berdasarkan hasil analisis, dilakukan mitigasi untuk mengatasi kerentanan yang teridentifikasi (CR4), sebelum dilanjutkan ke tahap pengujian purwarupa (tahap 5) guna mengevaluasi efektivitas kontrol keamanan yang diterapkan. Jika hasil pengujian menunjukkan adanya kelemahan, proses kembali ke tahap mitigasi (CR4a). Namun, apabila pengujian berhasil dan sistem dinyatakan aman, maka integrasi dapat dilanjutkan, dan hal ini ditandai oleh CR5 sebagai keluaran akhir dari proses yang telah tervalidasi keamanannya.

PT XYZ mengadopsi standar keamanan internasional *OWASP ASVS 4.0.3* untuk aplikasi web dan *MASVS* untuk aplikasi mobile. Penggunaan standar ini memastikan aplikasi yang dikembangkan mematuhi regulasi industri dan mengidentifikasi risiko secara efektif. Rancangan hasil integrasi dari model ini juga akan diuji melalui uji penetrasi untuk memastikan keandalannya sebelum digunakan dalam lingkungan produksi.

Pada sisi autentikasi, PT XYZ menghadapi tantangan dalam mengintegrasikan mitra secara individual. Sebagai solusi, model autentikasi WeChat Mini Program yang berbasis *OpenID* dan *session key* dapat dijadikan referensi untuk meningkatkan efisiensi autentikasi dan memudahkan integrasi mitra.

Proses integrasi ini menerapkan enkripsi AES-256 dan mekanisme verifikasi data untuk memastikan keamanan transmisi antara aplikasi *mobile banking*, layanan PT XYZ, dan layanan mitra. *Secure Integration Model* yang diterapkan mencakup dua komponen integrasi: (1) Akses Data Nasabah yang diotorisasi melalui token OAuth 2.0 dengan *unique code*, dan (2) Pembayaran yang divalidasi menggunakan *User Token*, *Unique Code*, dan *Session ID*. Integrasi ini dirancang untuk menjamin keamanan, konsistensi, dan keandalan proses integrasi dengan standar keamanan yang ketat.

Agar penerapan *Secure Integration Model* ini efektif, diperlukan analisis risiko yang komprehensif untuk mengidentifikasi potensi ancaman yang dapat mengakibatkan kebocoran data nasabah, akses ilegal, dan ancaman terhadap infrastruktur utama. Langkah mitigasi yang diterapkan meliputi validasi akses yang ketat, pemantauan real-time, dan penguatan kebijakan keamanan dalam komunikasi data. Dengan pendekatan ini, *Secure Integration Model* diharapkan mampu menjaga keberlanjutan operasional, melindungi keamanan data, dan memastikan kepatuhan terhadap regulasi yang berlaku.

Tabel 1. Analisis Risiko

Kode Risiko	Dampak	Kerentanan	Likelihood (L)	Impact (I)	Tingkat Risiko
R1	Gangguan layanan menyebabkan downtime	Tidak ada mekanisme rate-limiting pada API Gateway untuk mencegah DoS/DDoS	3	4	Tinggi
R2	Kebocoran data sensitif	Konfigurasi API Gateway yang tidak aman menyebabkan eksposur data	3	5	Tinggi
R3	Manipulasi atau kegagalan autentikasi	Fungsi validasi unique code tidak memadai	2	3	Sedang
R4	Kredensial yang bocor meningkatkan risiko	Penyimpanan Credential tanpa kontrol akses	2	3	Sedang
R5	Penyalahgunaan token akses	Token akses tidak memiliki batas waktu atau validasi ulang	3	5	Tinggi
R6	Token yang sama dapat digunakan kembali tanpa validasi ulang	Tidak ada validasi token reuse	2	3	Sedang
R7	Komunikasi tidak aman dapat disadap	Sertifikat TLS/SSL tidak diperbarui tepat waktu	2	4	Sedang
R8	Gangguan layanan akibat kegagalan daya	Tidak ada backup daya listrik (UPS)	3	4	Tinggi
R9	Akses fisik tidak sah dapat menyebabkan kebocoran data	Keamanan fisik perangkat keras (*server*) tidak memadai	2	3	Sedang
R10	Layanan terganggu akibat kerusakan perangkat keras	Kerusakan perangkat keras akibat suhu atau kondisi lingkungan yang ekstrem	2	4	Sedang
R11	Data sensitif dapat disadap selama transfer	Tidak ada enkripsi *end-to-end* pada komunikasi data	3	4	Tinggi
R12	Protokol komunikasi tidak aman	Protokol komunikasi tidak aman	3	4	Tinggi
R13	Tidak dapat mendeteksi aktivitas mencurigakan	Tidak ada monitoring terhadap anomali trafik	2	4	Sedang
R14	Kelalaian mitra menyebabkan penyalahgunaan API	Kurangnya edukasi keamanan API	2	4	Sedang
R15	Data dapat diakses oleh pihak tidak sah	Tidak ada kebijakan kontrol akses yang memadai	2	4	Sedang
R16	Kredensial bocor meningkatkan risiko penyalahgunaan	Kelalaian dalam penyimpanan kredensial	2	4	Sedang

R17	Data nasabah dapat diakses oleh pihak tidak sah	Tidak ada kontrol akses ketat terhadap data nasabah	2	5	Sedang
R18	Aktivitas mencurigakan pada data tidak terdeteksi	Data sensitif tidak dimonitor untuk akses tidak sah	3	5	Tinggi
R19	Integrasi tidak divalidasi secara menyeluruh	Tidak ada validasi akses data antar sistem dalam integrasi	2	4	Sedang

Berdasarkan hasil analisis yang telah dilakukan, beberapa risiko dikategorikan dalam tingkat tinggi dan sedang, sehingga memerlukan langkah-langkah mitigasi yang tepat guna mengurangi potensi dampak negatif yang dapat terjadi serta memastikan keberlangsungan operasional sistem dan kepatuhan terhadap regulasi yang berlaku.

Setiap risiko yang telah teridentifikasi membutuhkan strategi mitigasi yang sesuai agar dampaknya dapat dikendalikan secara efektif. Oleh karena itu, diperlukan penerapan langkah-langkah mitigasi yang tepat untuk menjaga keamanan sistem serta memastikan bahwa operasional tetap berjalan dengan optimal. Berikut adalah beberapa upaya mitigasi yang dapat diterapkan:

Tabel 2: Mitigasi Risiko

Kode Risiko (R)	**Mitigasi Risiko**
R1	Penerapan mekanisme *rate-limiting* pada API Gateway untuk mencegah serangan DoS/DDoS
R2	Enkripsi data sensitif selama transmisi dan transfer menggunakan protokol TLS 1.3 atau lebih baru
R3	Penguatan validasi token dengan algoritma hashing yang aman dan pembaruan periodik token
R4	Pengetatan akses data dengan prinsip least privilege dan audit berkala
R5	Membatasi waktu berlaku token untuk menghindari penggunaan yang tidak sah
R6	Deteksi otomatis penggunaan ulang token (*token reuse*) dan pembatalan token yang lama
R7	Monitoring otomatis untuk memperbarui sertifikat TLS/SSL sebelum masa berlaku habis
R8	Penyediaan backup daya listrik (UPS) untuk memastikan layanan tetap berjalan selama pemadaman sesuai SOP yang sudah ada
R9	Penguatan keamanan fisik dengan CCTV, kontrol akses biometrik, dan audit fisik berkala sesuai SOP yang sudah ada
R10	Penambahan sistem pendinginan dan sensor untuk mendeteksi suhu ekstrem sesuai SOP yang sudah ada
R11	Penerapan enkripsi *end-to-end* untuk melindungi data selama transfer (HTTPS)
R12	Pemantauan protokol komunikasi secara rutin untuk memastikan keamanan protokol
R13	Integrasi alat monitoring lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan secara real-time sesuai SOP yang sudah ada
R14	Menerapkan kontrak SLA (*Service Level Agreement*) yang mencakup tanggung jawab keamanan API bagi mitra
R15	Penerapan scoped tokens untuk membatasi akses mitra hanya pada data yang relevan, serta monitoring real-time API
R16	Menggunakan token OAuth dengan waktu berlaku singkat, serta enkripsi saat transit
R17	Audit berkala terhadap akses data nasabah untuk memastikan kepatuhan kontrol akses
R18	Mengaktifkan *audit log* dan pemantauan rutin untuk mendeteksi aktivitas mencurigakan pada data sensitif

R19	Memvalidasi integrasi layanan dengan pengujian API rutin untuk memastikan komunikasi dan ketersediaan data

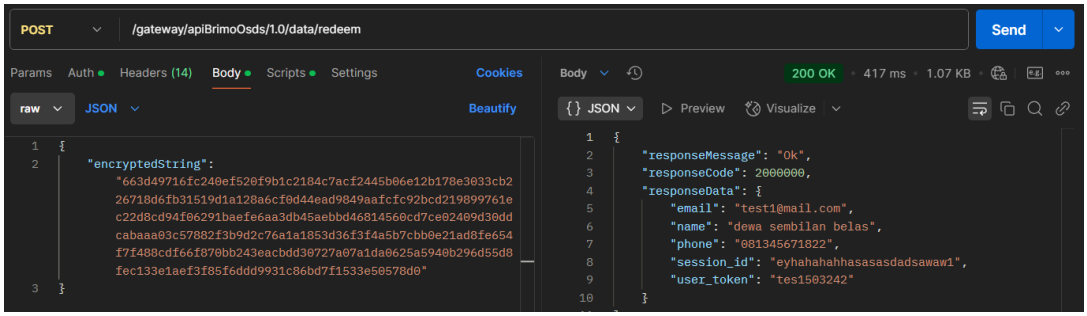
Langkah mitigasi yang diterapkan bertujuan untuk mengurangi dampak potensi ancaman, meningkatkan keandalan sistem, dan memastikan kepatuhan terhadap regulasi yang berlaku. *Penetration testing* dan kontrol yang efektif menjadi bagian integral dari strategi mitigasi risiko ini. Proses ini membantu organisasi menjaga keberlanjutan operasional, perlindungan data, dan kepercayaan pemangku kepentingan, serta memastikan bahwa setiap perubahan aplikasi aman dan sesuai dengan standar yang ditetapkan.

Setelah dilakukan perancangan dan juga analisis risiko dari rancangan model integrasi, maka perlu divalidasi dan diverifikasi oleh pakar ahli untuk memastikan bahwa desainnya memenuhi standar keamanan, keakuratan, dan efisiensi yang diharapkan. Para pakar memberikan umpan balik konstruktif, termasuk rekomendasi untuk menambahkan mekanisme validasi menggunakan *Hash-based Message Authentication Code* (HMAC) dan membatasi akses *Mobile Banking* PT XYZ hanya kepada alamat IP yang terdaftar. Langkah-langkah ini bertujuan untuk memperkuat keamanan dengan mencegah akses tidak sah dan memastikan integritas data selama transmisi.

Setelah mempertimbangkan rancangan tersebut, para pakar sepakat untuk melanjutkan ke tahap pengembangan purwarupa dengan fokus pada penerapan HMAC untuk verifikasi integritas dan keaslian data. Sistem juga akan dilengkapi dengan pembatasan akses berbasis alamat *IP* yang terdaftar, pengawasan rutin untuk mendeteksi potensi ancaman, serta protokol rotasi kunci enkripsi secara berkala guna menjaga validitas mekanisme keamanan. Pendekatan ini bertujuan untuk menciptakan integrasi yang lebih aman, handal, dan sesuai dengan kebutuhan operasional PT XYZ dalam menghadapi ancaman keamanan siber yang terus berkembang.

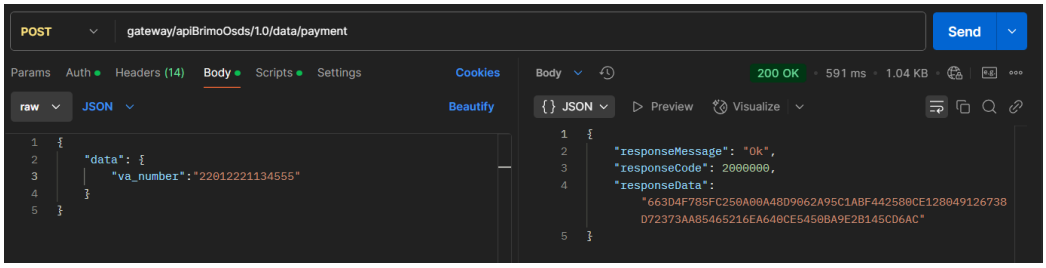
Pengembangan *Secure Integration Model* ini juga mencakup penerapan autentikasi aman berbasis OAuth 2.0, enkripsi data, validasi input, manajemen rahasia, API Gateway, serta teknologi container seperti Kubernetes. Pendekatan "shift left security" dan pemantauan real-time diterapkan untuk mendeteksi kerentanan dan ancaman sejak tahap awal pengembangan, menjaga integritas dan keandalan sistem. Selain itu, penerapan prinsip-prinsip pengkodean aman sesuai dengan *OWASP Secure Coding Practices* dan pengelolaan *secret variable* menjadi langkah penting dalam mengurangi risiko eksploitasi serta memastikan bahwa model integrasi ini dapat memenuhi standar keamanan modern secara menyeluruh.

Dalam penelitian ini, Integrasi Layanan Akses Data Nasabah yang Aman berbasis *Unique Code* menunjukkan hasil yang sukses dengan pengujian API pada endpoint /gateway/apiBrimoOsds/1.0/data/redeem, yang memastikan enkripsi dan autentikasi token. Respons yang diperoleh dengan kode status 200 OK dan waktu pemrosesan optimal menunjukkan bahwa model ini aman dan efisien dalam mengelola permintaan data nasabah.



Gambar 3. Hasil Pengembangan Integrasi Akses Data Nasabah

Penelitian ini mengembangkan Integrasi Layanan Pembayaran Aman untuk menghasilkan *Unique Code* pembayaran, yang menjaga keamanan transaksi melalui Mini Program. Integrasi Layanan ini memproses nomor *virtual account* (VA) untuk menghasilkan *Unique Code* terenkripsi, memastikan bahwa hanya pihak berwenang yang dapat menggunakannya. Keberhasilan respons dengan kode status 200 OK dan waktu pemrosesan optimal menunjukkan efisiensi model dalam mengelola permintaan pembayaran. Hasil pengembangan model ini membuktikan bahwa model dapat diterapkan untuk sistem pembayaran dengan menggunakan *Unique Code* seperti yang ditunjukkan pada Gambar 4.



Gambar 4. Hasil Pengembangan Integrasi Pembayaran

Demonstration

Pengujian keamanan sistem secara umum merupakan bagian dari *Secure Integration Model* (SIM) yang dikembangkan dalam penelitian ini, dan dilakukan untuk mengevaluasi hasil integrasi antara aplikasi *mobile banking* dan Mini Program mitra. Pengujian ini melibatkan simulasi serangan guna mengidentifikasi potensi kerentanan, baik pada API maupun fitur-fitur yang menggunakan Mini Program. Proses ini divalidasi dengan metode standar seperti *Penetration Testing Execution Standard* (PTES) dan diikuti dengan penerapan langkah mitigasi seperti validasi input dan enkripsi untuk mengatasi kelemahan yang ditemukan. Pengujian ulang dilakukan untuk memastikan kerentanan telah berhasil diatasi, sehingga sistem dapat beroperasi dengan aman dan andal [5].

PT XYZ bekerja sama dengan perusahaan keamanan siber terkemuka yang memiliki spesialisasi dalam uji penetrasi dan pengujian keamanan aplikasi. Vendor ini berpengalaman dalam membantu organisasi mengidentifikasi dan memitigasi risiko keamanan digital, khususnya di sektor perbankan dan keuangan. Mereka menawarkan layanan pengujian keamanan aplikasi web dan mobile, uji penetrasi dengan pendekatan standar global, serta simulasi serangan komprehensif (*Red Teaming*). Kolaborasi ini memungkinkan PT XYZ untuk melindungi data sensitif,

memastikan kepatuhan terhadap standar keamanan industri, dan meningkatkan kepercayaan pelanggan serta mitra.

Sebagai bagian dari model untuk memitigasi risiko, PT XYZ melaksanakan uji penetrasi terhadap hasil model integrasi menggunakan dua pendekatan yang saling melengkapi: pengujian langsung terhadap API dan pengujian pada fitur hasil integrasi Mini Program. Pengujian API bertujuan mengidentifikasi kerentanan terkait autentikasi, otorisasi, dan pertukaran data, sedangkan pengujian Mini Program fokus pada integritas proses integrasi dan potensi kerentanan pada fungsi inti seperti otentikasi pengguna dan transaksi. Hasil pengujian ini diharapkan memberikan wawasan berbasis data tentang risiko keamanan dan rekomendasi teknis untuk mengurangi ancaman serta meningkatkan ketahanan sistem PT XYZ.

Pengujian pada API mengidentifikasi kerentanan dengan skor 3.1 berdasarkan cvss sehingga temuan ini dinyatakan terdapat pada tingkat kerentanan rendah (*low)*, termasuk penerapan kriptografi yang rentan, di mana penggunaan AES-GCM dengan *nonce* statis per pengguna berpotensi dieksploitasi dalam kondisi tertentu. Rekomendasi perbaikan yang disarankan adalah penerapan *nonce* unik atau kombinasi AES dengan HMAC-SHA. Selain itu, ditemukan validasi input data yang tidak memadai dalam konversi JSON ke XML, yang dapat membuka peluang injeksi XML. Untuk mengurangi kerentanan sistem, sistem disarankan membuat objek JSON baru guna mencegah manipulasi data.

Pengujian terhadap Fitur X dan Fitur Y mengungkapkan kerentanan keamanan signifikan. Fitur X merupakan aplikasi pengelolaan pembayaran menggunakan pemindai tangan berbasis kecerdasan buatan dengan *liveness detection*, dan Fitur Y yang mengelola iuran secara digital rentan terhadap *Authenticated SQL Injection*, memungkinkan akses tidak sah ke data sensitif. Rekomendasi yang disarankan adalah penggunaan *parameterized queries*. Selain itu, kurangnya pembatasan sumber daya (*Lack of Resources & Rate Limiting*) berpotensi mengganggu ketersediaan layanan, sehingga perlu diterapkan rate limiting untuk menjaga performa sistem.

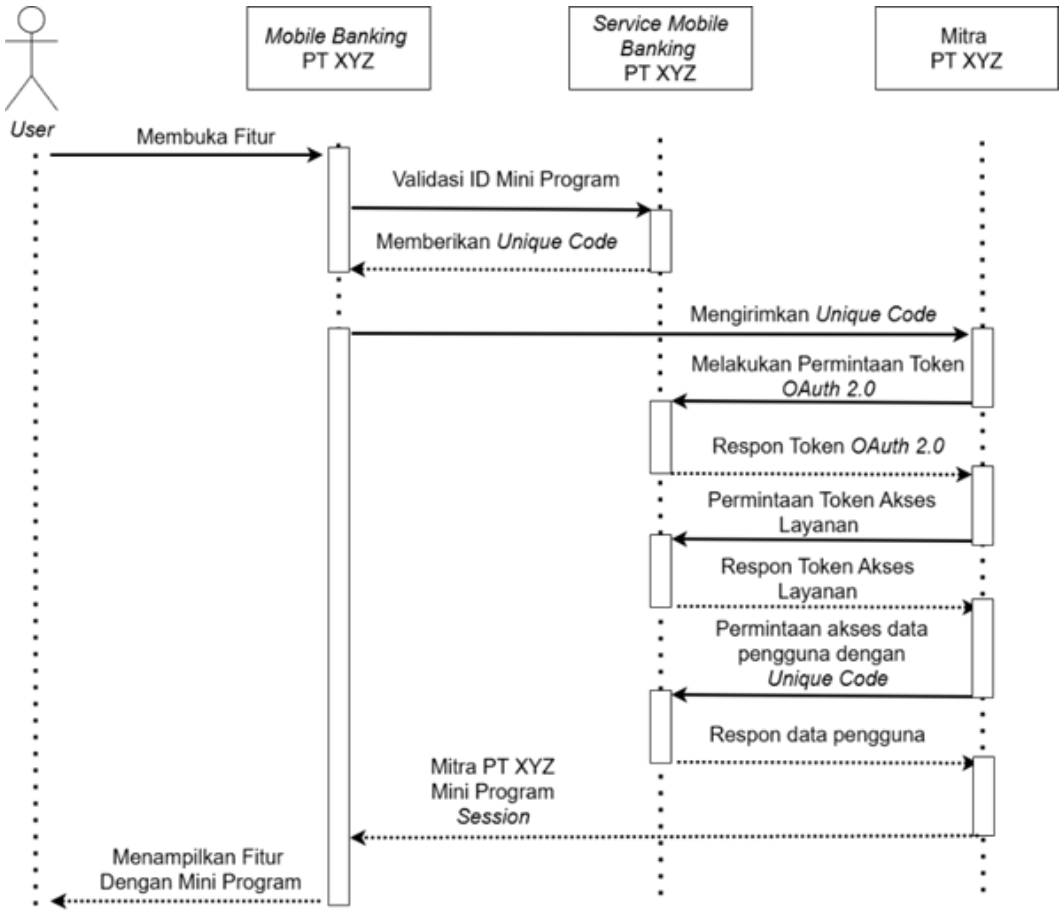
Evaluation of Secure Integration Model

Hasil uji penetrasi pada tahap uji coba *Secure Integration Model* oleh tim Keamanan Informasi mengidentifikasi dua kerentanan dengan tingkat kategori rendah dalam pengujian pada *Application Programming Interface*. Meskipun dampaknya terbatas, temuan ini ditangani untuk mencegah potensi eksploitasi di masa depan. Pengujian integrasi dengan Mini Program dan pengujian *end-to-end* menunjukkan penerapan *Secure Integration Model* efektif dalam mengurangi temuan kerentanan terkait pertukaran data nasabah dengan mitra dan juga pembayaran melalui Mini Program. Setelah perbaikan dan uji penetrasi ulang, kerentanan tertutup, memastikan keamanan sistem tetap terjaga. Tim Keamanan Informasi memberikan persetujuan untuk melanjutkan pengembangan, dengan catatan bahwa mitigasi akan terus dipantau dan disesuaikan dengan standar keamanan yang berkembang.

Selain hasil uji teknis, diskusi terfokus (FGD) yang melibatkan para pakar menyimpulkan bahwa rancangan dan hasil pengembangan *Secure Integration Model* telah optimal dan memenuhi kebutuhan mini program pada *mobile banking* PT XYZ. Evaluasi menunjukkan bahwa tidak ada kerentanan di atas kategori rendah dalam pengujian langsung terhadap *API*, sehingga model ini layak untuk diterapkan. Para

pakar menekankan pentingnya pemantauan berkala, pendampingan teknis oleh tim PT XYZ, serta uji penetrasi setiap kali integrasi melalui Mini Program untuk mengidentifikasi potensi kerentanan. Langkah-langkah ini penting untuk memastikan model tetap relevan dan aman dalam jangka panjang.

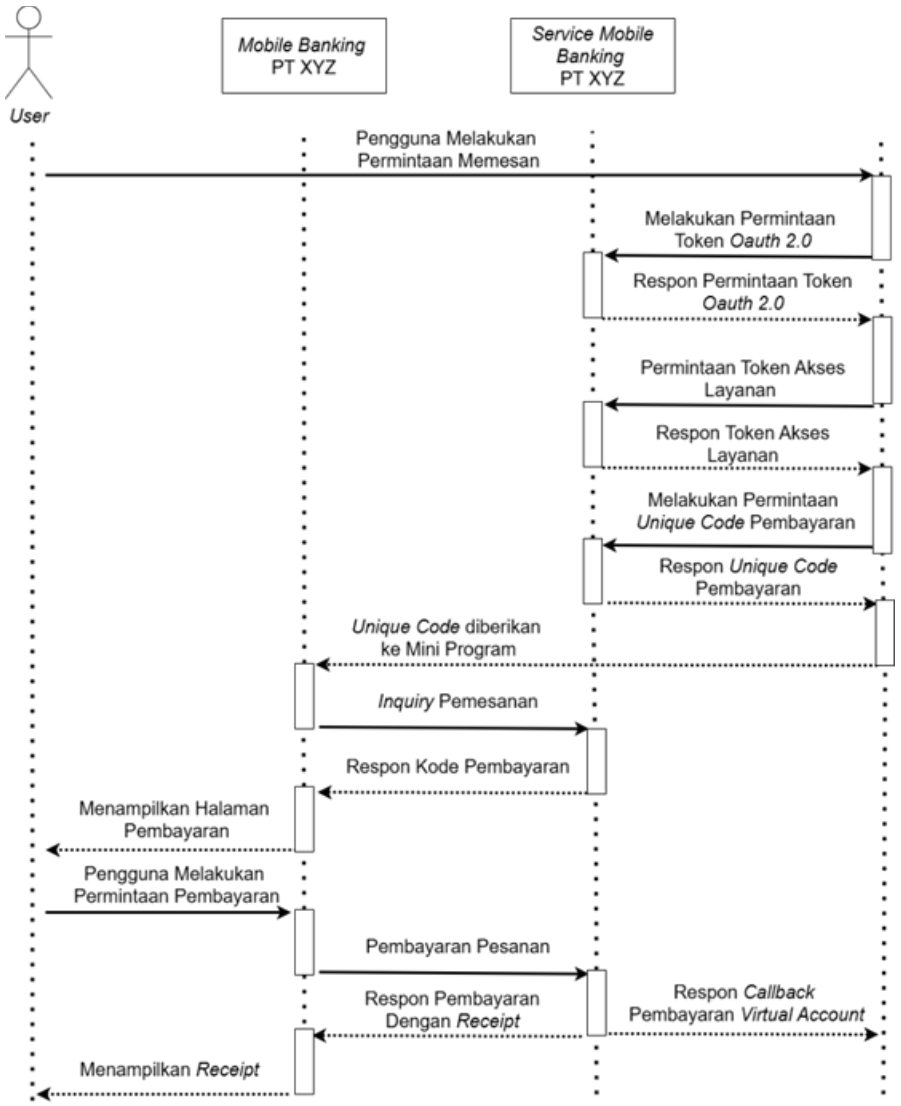
Integrasi Layanan Akses Data Nasabah Melalui Mini Program



Gambar 5. Model Integrasi Layanan Akses Data Nasabah

Proses integrasi akses data nasabah melalui Mini Program dirancang untuk memastikan keamanan dan kerahasiaan data nasabah, selaras dengan alur komunikasi yang ditetapkan dalam arsitektur sistem. Proses ini dimulai ketika pengguna mengakses fitur melalui *Mobile Banking* PT XYZ, yang kemudian mengajukan permintaan verifikasi ke layanan mobile banking. Setelah memvalidasi ID Mini Program, sistem akan mengembalikan kode unik (*unique code*) yang telah dienkripsi menggunakan algoritma AES-256 dengan format yang dioptimalkan untuk menyertakan hanya informasi yang relevan, guna meminimalkan risiko kebocoran data. Mini Program kemudian menggunakan fungsi khusus untuk menerima kode unik tersebut, meneruskannya ke layanan mitra guna memproses data, melakukan sinkronisasi akun, serta mengirimkan hasil sinkronisasi kembali ke Mini Program. Dengan penerapan standar keamanan yang ketat serta pengelolaan data yang efisien, PT XYZ menjamin integrasi layanan yang aman serta menjaga kerahasiaan dan integritas data nasabah di setiap tahap proses.

Integrasi Layanan Pembayaran Melalui Mini Program



Gambar 6. Model Integrasi Layanan Pembayaran *Virtual Account*

Dalam proses pembayaran, integrasi layanan melibatkan pengiriman data transaksi dari mitra PT XYZ ke sistem *mobile banking*. Data yang dikirim mencakup kode pembayaran *virtual account* yang setelah diterima dan diproses oleh sistem PT XYZ, menghasilkan *unique code* pembayaran. *Unique code* ini kemudian digunakan sebagai parameter untuk mengaktifkan fungsi pembayaran pada *Mini Program*, yang selanjutnya mengarahkan pengguna ke halaman pembayaran dalam aplikasi *mobile banking* PT XYZ. Dengan mekanisme ini, proses pembayaran dapat berlangsung secara aman, terintegrasi, dan sesuai dengan ekosistem *mobile banking* PT XYZ.

Keamanan dalam integrasi layanan ini menjadi aspek krusial dalam melindungi data nasabah selama pertukaran informasi dan transaksi pembayaran *virtual account*. Hasil penelitian menunjukkan bahwa *Secure Integration Model* pada akses data nasabah dan pembayaran *virtual account* melalui *Mini Program* efektif dalam menjaga keamanan informasi melalui penerapan OAuth 2.0*, unique code, user*

token, dan *session ID* yang mengamankan akses layanan. Pengujian penetrasi mengonfirmasi efektivitas *rate-limiting* pada *API Gateway* dalam mencegah serangan *DoS/DDoS*, sementara enkripsi AES-256 melindungi data sensitif, *token rotation* mencegah penyalahgunaan token, dan TLS 1.3 menjaga keamanan data selama transmisi. Selain itu, penelitian ini menyoroti pentingnya uji penetrasi dalam mengevaluasi kerentanan sistem, terutama dalam integrasi dengan mitra, di mana ditemukan celah keamanan dengan tingkat risiko sedang hingga tinggi. Oleh karena itu, uji penetrasi harus menjadi bagian dari kebijakan keamanan berkelanjutan guna mengidentifikasi dan memitigasi risiko secara proaktif. Dengan penerapan proteksi *API Gateway*, validasi akses berbasis token, serta enkripsi yang kuat, *Secure Integration Model* yang dikembangkan tidak hanya meningkatkan ketahanan sistem terhadap ancaman keamanan dalam ekosistem *Mini Program*, tetapi juga memastikan perlindungan optimal terhadap data nasabah.

D. Simpulan

Penelitian ini telah mengembangkan Model Integrasi Layanan yang Aman pada Platform Mini Program dengan menerapkan pendekatan *Design Science Research* (DSR) dan prinsip *Secure Software Development* (SSD). Model ini memastikan keamanan informasi dengan mengintegrasikan mekanisme perlindungan sejak tahap awal pengembangan (*Security by Design*), mencakup autentikasi berbasis OAuth 2.0, validasi transaksi dengan *Unique Code*, serta enkripsi menggunakan TLS dan AES-256. Selain itu, *API Gateway* diterapkan dengan fitur *rate-limiting*, *IP whitelisting*, dan validasi permintaan untuk mencegah akses tidak sah dan serangan *brute-force*.

Hasil penelitian menunjukkan bahwa model ini efektif dalam menjaga kerahasiaan, integritas, dan ketersediaan layanan, serta melindungi komunikasi dan data sensitif melalui penerapan berbagai strategi keamanan, termasuk kontrol akses berbasis token, manajemen identitas dan akses (IAM), serta pemantauan sistem secara *real-time*. Pengujian keamanan melalui penetration testing menunjukkan bahwa hasil integrasi dari model ini mampu mengurangi risiko serangan *DoS/DDoS* dengan penerapan rate-limiting pada *API Gateway*, sementara enkripsi AES-256 memastikan perlindungan terhadap data sensitif. Selain itu, mekanisme *token rotation* terbukti mengurangi potensi reuse token, serta validasi berbasis *Unique Code* efektif dalam mencegah *replay attack* dan penyalahgunaan akses.

Salah satu temuan penting dalam penelitian ini adalah bahwa uji penetrasi menjadi aspek esensial dalam mengevaluasi dan mengidentifikasi potensi kerentanan sistem, terutama dalam integrasi dengan mitra, di mana sebagian besar potensi kerentanan sistem berada pada tahap autentikasi dan akses layanan. Oleh karena itu, uji penetrasi harus dilakukan setiap kali melakukan integrasi dengan mitra untuk memastikan sistem tetap aman dari eksploitasi dan risiko keamanan yang berkembang.

Sebagai hasil penelitian ini, model yang dikembangkan akan menjadi standar keamanan dalam integrasi layanan akses data nasabah dan pembayaran *virtual account* melalui Mini Program. Standar ini mencakup autentikasi, otorisasi, validasi input, dan enkripsi untuk memastikan setiap proses integrasi dengan mitra memenuhi prinsip keamanan yang ketat. Untuk meningkatkan kualitas dan

keberlanjutan model ini beberapa langkah strategis perlu diterapkan termasuk pelatihan keamanan bagi tim internal dan mitra, pengujian penetrasi rutin, serta kajian terhadap model integrasi modern yang aman. Dengan penerapan model ini, sistem Mini Program dapat beroperasi dengan tingkat keamanan yang tinggi, memastikan perlindungan optimal terhadap data nasabah.

E. Referensi

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, "Survei Penetrasi Internet Indonesia 2024," 2024. Accessed: Aug. 28, 2024. [Online]. Available: https://survei.apjii.or.id/

[2] M. Schreieck, A. Ou, and H. Krcmar, "Mini-App Ecosystems," *Business and Information Systems Engineering*, vol. 65, no. 1, pp. 85–93, Feb. 2023, doi: 10.1007/s12599-022-00773-9.

[3] M. Humayun, N. Z. Jhanjhi, M. F. Almufareh, and M. I. Khalil, "Security Threat and Vulnerability Assessment and Measurement in Secure Software Development," *Computers, Materials and Continua*, vol. 71, no. 2, pp. 5039–5059, 2022, doi: 10.32604/cmc.2022.019289.

[4] A. Ramirez, A. Aiello, and S. J. Lincke, "A survey and comparison of secure software development standards," in *13th CMI Conference on Cybersecurity and Privacy - Digital Transformation - Potentials and Challenges, CMI 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/CMI51275.2020.9322704.

[5] P. Shigwedha and F. B. Shava, "Designing A Secure Integration Model for EGovernance Platforms," in *2021 3rd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/IMITEC52926.2021.9714556.

[6] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, May 2020. doi: 10.1088/1757-899X/846/1/012036.

[7] P. S. S. Kiran Gandikota, D. Valluri, S. B. Mundru, G. K. Yanala, and S. Sushaini, "Web Application Security through Comprehensive Vulnerability Assessment," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 168–182. doi: 10.1016/j.procs.2023.12.072.

[8] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," *Electronics (Switzerland)*, vol. 11, no. 19, Oct. 2022, doi: 10.3390/electronics11192991.

[9] S. Margareth *et al.*, "Uji Penetration Testing Web Server XYZ, Menggunakan Metode OWASP TOP 10 dan CVSS," *CENTIVE*, vol. 4, no. 1, pp. 1173–1183, 2024.

[10] B. Ding and X. Ferràs Hernández, "Case study as a methodological foundation for Technology Roadmapping (TRM): Literature review and future research agenda," *Journal of Engineering and Technology Management - JET-M*, vol. 67, Jan. 2023, doi: 10.1016/j.jengtecman.2023.101731.

[11] T. A. Henriques and H. O'Neill, "Design science research with focus groups – a pragmatic meta-model," *International Journal of Managing Projects in*

Business, vol. 16, no. 1, pp. 119–140, Mar. 2023, doi: 10.1108/IJMPB-01-2020-0015.

[12] Tencent Cloud, "SDK Introduction." Accessed: Feb. 07, 2025. [Online]. Available: https://www.tencentcloud.com/document/product/1219/61257

[13] D. Ritter, F. Nordvall Forsberg, and S. Rinderle-Ma, "Responsible composition and optimization of integration processes under correctness preserving guarantees," *Inf Syst*, vol. 124, Sep. 2024, doi: 10.1016/j.is.2024.102400.

[14] D. Ritter, S. Rinderle-Ma, M. Montali, and A. Rivkin, "Formal foundations for responsible application integration," *Inf Syst*, vol. 101, Nov. 2021, doi: 10.1016/j.is.2019.101439.

[15] H. Dong, X. Zhang, D. Kong, and B. Zhang, "Analysis and Design of Garbage Classification System Based on Wechat Mini Program," in *CIBDA 2022*, 2022.

[16] Y. Zhang, B. Turkistani, A. Y. Yang, C. Zuo, and Z. Lin, "A Measurement Study of Wechat Mini-Apps," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 5, no. 2, Jun. 2021, doi: 10.1145/3460081.

[17] Z. Yuyan, "Design and Implementation of Mini Programs that Integrate Foreign Trade English Video Learning Resources," in *2023 International Conference on Network, Multimedia and Information Technology, NMITCON 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/NMITCON58196.2023.10276242.

[18] Y. Wang and H. Qi, "Design and Implementation of Experiment Online Teaching Platform for Oil and Gas Storage and Transportation Based on WeChat Mini-Program," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 22, pp. 152–166, Nov. 2023, doi: 10.3991/ijet.v18i22.42235.

[19] A. Srivastava, N. Singh, and K. Suhail, "Major Software Security Risks in Banking Industry: Design Phase Perspective," in *Proceedings of 2023 3rd International Conference on Innovative Practices in Technology and Management, ICIPTM 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICIPTM57143.2023.10118067.

[20] I. U. Haq and T. A. Khan, "Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review," 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3088229.

[21] D. Mortágua, A. Zúquete, and P. Salvador, "Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0," *Computer Networks*, vol. 244, May 2024, doi: 10.1016/j.comnet.2024.110337.

[22] X. Li, J. Xu, Z. Zhang, X. Lan, and Y. Wang, "Modular Security Analysis of OAuth 2.0 in the Three-Party Setting," in *Proceedings - 5th IEEE European Symposium on Security and Privacy, Euro S and P 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 276–293. doi: 10.1109/EuroSP48549.2020.00025.

[23] S. Kostoudas, O. Markovskyi, N. Doukas, and N. Bardis, "Secure and Encrypted Communication System on Mobile Devices," in *Proceedings of the 2022 IEEE 12th International Conference on Dependable Systems, Services and Technologies, DESSERT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/DESSERT58054.2022.10018747.

[24] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," Jan. 2009. doi: 10.1016/j.infsof.2008.09.009.

[25] L. Khakim, M. Mukhlisin, and A. Suharjono, "Security system design for cloud computing by using the combination of AES256 and MD5 algorithm," in *IOP Conference Series: Materials Science and Engineering*, Institute of Physics Publishing, Jan. 2020. doi: 10.1088/1757-899X/732/1/012044.

[26] G. G. Kagombe, R. W. Mwangi, and J. M. Wafula, "Achieving Standard Software Security in Agile Developments," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2021, pp. 24–33. doi: 10.1145/3484399.3484403.

[27] P. V. Torres-Carrión, C. S. González-González, S. Aciar, and G. Rodríguez-Morales, "Methodology for systematic literature review applied to engineering and education," in *2018 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, 2018, pp. 1364–1373.

[28] J. R. Almeida, A. Zúquete, A. Pazos, and J. L. Oliveira, "A federated authentication schema among multiple identity providers," *Heliyon*, vol. 10, no. 7, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28560.