ANALISIS KEAMANAN *CALLBACK PAYMENT GATEWAY* TERHADAP *REPLAY ATTACK* DAN *WEBHOOK SPOOFING* MENGGUNAKAN PENDEKATAN *DEFENSE-IN-DEPTH* BERBASIS REDIS

SKRIPSI

Jibran Khairy Akram 2207421011

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

ANALISIS KEAMANAN *CALLBACK PAYMENT GATEWAY* TERHADAP *REPLAY ATTACK* DAN *WEBHOOK SPOOFING* MENGGUNAKAN PENDEKATAN *DEFENSE-IN-DEPTH* BERBASIS REDIS

SKRIPSI

Dibuat untuk Melengkapi Syarat – Syarat yang Diperlukan untuk Memperoleh
Diploma Empat Politeknik

Jibran Khairy Akram

2207421011

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama Mahasiswa : Jibran Khairy Akram

NIM : 2207421011

Jurusan/ProgramStudi Komputer/T.Multimedia dan Jaringan : T.Informatika dan

Judul Skripsi : Analisis Keamanan *Callback Payment Gateway* Terhadap *Replay Attack* dan *Webhook Spoofing* Menggunakan Pendekatan *Defense-in- Depth* Berbasis Redis

Menyatakan dengan sebenarnya bahwa skripsiini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok 9 Juni, 2026,

Yang membuat pernyataan

Jibran Khairy Akram

NIM. 2207421011

Skripsi diajukan oleh:

Nama	: Jibran Khairy Akram
NIM	: 2207421011
Program Studi	: Teknik Multimedia dan Jaringan
Judul Skripsi	: Analisis Keamanan *Callback Payment Gateway* Terhadap *Replay Attack* dan *Webhook Spoofing* Menggunakan Pendekatan *Defense-in-Depth*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari … , Tanggal … , Bulan …, Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I	Ayu Rosyida Zain, S.ST., M.T.	( )
Penguji I	Asep Kurniawan, S.Pd., M.Kom.	( )
Penguji II	Fachroni Arbi Murad, S.Kom., M.Kom.	( )
Penguji III	Iik Muhamad Malik Matin, S.Kom., M.T.	( )

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi berjudul "Analisis Keamanan *Callback Payment Gateway* Terhadap *Replay Attack* dan *Webhook Spoofing* Menggunakan Pendekatan Defense-in-Depth Berbasis Redis". Skripsi ini disusun untuk memenuhi salah satu syarat memperoleh gelar Diploma IV pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta.

Penulis menyadari bahwa penyusunan skripsi ini tidak lepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Orang tua dan seluruh keluarga tercinta, atas kasih sayang, doa, dan dukungan moril agar proses penyusunan skripsi penulis berjalan lancar, serta memberikan dukungan dalam menyelesaikan skripsi.
2. Ibu Ayu Rosyida Zain, S.ST., M.T., sebagai dosen pembimbing yang telah meluangkan waktu, membantu, mendukung dan memberikan masukan serta saran kepada penulis selama pengerjaan skripsi hingga selesai.
3. Bapak dan Ibu Dosen Jurusan Teknik Informatika dan Komputer, khususnya program studi Teknik Multimedia dan Jaringan, atas ilmu, motivasi, dan inspirasi yang telah diberikan.
4. Teman-teman seperjuangan penulis: Sahrul, Vito, Syifa, Raden, Abdan, Stepani, Audi, Rizki, Wibi, Dhea, Yoga, Rafli, dan Darma, serta rekan-rekan seprodi lainnya yang selalu memberikan dukungan, semangat, dan kebersamaan dalam suka maupun duka selama masa perkuliahan hingga skripsi ini selesai.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang. Semoga laporan ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang berkepentingan.

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini :

Nama Mahasiswa : Jibran Khairy Akram

NIM : 2207421011

Jurusan/ProgramStudi : T.Informatika dan Komputer/T.Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis Keamanan *Callback Payment Gateway* Terhadap *Replay Attack* dan *Webhook Spoofing* Menggunakan Pendekatan *Defense-in- Depth* Berbasis Redis

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok 9 Juni, 2026,

Yang m

Jibran Khairy Akram

NIM. 2207421011

Analisis Keamanan *Callback Payment Gateway* Terhadap *Replay Attack* dan *Webhook Spoofing* Menggunakan Pendekatan *Defense-in- Depth* Berbasis Redis

ABSTRAK

Pertumbuhan transaksi digital memunculkan kerentanan pada arsitektur komunikasi asinkron, khususnya pada integrasi Payment Gateway. Permasalahan utama pada Website PsikoTest adalah rentannya jalur transmisi callback terhadap manipulasi logika bisnis (Webhook Spoofing) dan penggandaan transaksi akibat serangan serentak (Replay Attack) yang memicu kerugian finansial. Penelitian ini bertujuan menganalisis kerentanan tersebut dan mengimplementasikan arsitektur keamanan berlapis (Defense-in-Depth). Sistem dirancang menggunakan kriptografi HMAC-SHA256 pada lapisan jaringan, mekanisme Idempotency Key dan Rate Limiter berbasis Redis pada middleware, serta Database Absolute Lock pada persistensi. Pengujian dieksekusi menggunakan Apache JMeter. Hasil pengujian menunjukkan arsitektur berhasil mengisolasi 100% anomali muatan dan memblokir Webhook Spoofing dengan rata-rata latensi 65,2 ms. Pada simulasi konkurensi tinggi, sistem mencegat 99,00% muatan duplikat di tingkat memori dan memblokir 100% eksploitasi kedaluwarsa waktu di basis data. Pengujian beban puncak 10.000 threads mengonfirmasi sistem secure menekan latensi hingga 60,6% (5.369 ms) dibandingkan sistem rentan (13.632 ms), menjaga throughput pada 94,1 req/s, serta meredam Load Average di angka 1,67. Arsitektur ini terbukti beroperasi secara komplementer untuk mengamankan integritas transaksi dan mencegah kelumpuhan layanan.

Kata Kunci: Defense-in-Depth, HMAC-SHA256, Idempotency, Payment Gateway, Redis, Replay Attack, Webhook Spoofing.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Tren ancaman siber global pada sektor keuangan kini telah berevolusi dari serangan infrastruktur tradisional menuju serangan terhadap logika aplikasi (*Business Logic Abuse*), khususnya pada antarmuka pemrograman aplikasi (API). Laporan terbaru Salt Security (2025) mencatat bahwa 37% dari total masalah keamanan yang ditemukan pada API produksi adalah kategori kerentanan (*vulnerabilities*), yang membuka celah kritis bagi eksploitasi teknis dan manipulasi alur logika bisnis (*Business Logic Abuse*) untuk keuntungan finansial. Urgensi ini dipertegas oleh laporan Akamai (2024) yang menempatkan sektor jasa keuangan (*Financial Services*) sebagai target utama serangan global. Eskalasi ancaman ini diperburuk oleh serangan *Spoofing* yang menjadi risiko kritis pada API Fintech karena mengeksploitasi kelemahan autentikasi dengan menyamar sebagai entitas sah (Ranjan et al., 2022). Selain itu, teridentifikasi pula persistensi serangan *Replay Attack* yang mampu mengeksploitasi transmisi data valid namun minim verifikasi waktu atau *timestamp* (Obaidat et al., 2024). Kerentanan manipulasi transaksi ini terbukti fatal pada *Merchant Payment Platform*, di mana Al-Omari (2025) menyoroti bahwa celah tersebut sering dieksploitasi untuk merugikan integritas keuangan. Kondisi ini menjadikan pengamanan pada jalur komunikasi pembayaran digital (*Payment Gateway*) sangat krusial, mengingat serangan pada logika bisnis seringkali lolos dari deteksi keamanan standar karena lalu lintas datanya terlihat valid secara teknis namun manipulatif secara konteks.

Relevansi ancaman tersebut teramati secara nyata pada studi kasus Website PsikoTest yang dikelola oleh PT Sudami Jaya Medika. Berdasarkan hasil observasi dan analisis kebutuhan sistem, proses pembayaran token tes psikologi sebelumnya masih dilakukan melalui mekanisme konvensional yang mewajibkan pengguna mengirimkan bukti transfer secara manual. Mekanisme ini teridentifikasi memiliki kelemahan signifikan berupa inefisiensi operasional akibat antrean verifikasi yang menghambat kecepatan layanan. Untuk mengatasi kendala

kalabilitas tersebut, sistem beralih mengadopsi pembayaran otomatis (*cashless*) berbasis *Webhook*. Namun, transisi teknologi ini justru membuka permukaan serangan (*attack surface*) baru yang jauh lebih kompleks. Tanpa adanya validasi kriptografis yang memadai, sistem otomatis ini menjadi sangat rentan terhadap manipulasi alur data, khususnya ancaman *Webhook Spoofing* dan *Replay Attack* yang dapat memvalidasi transaksi ilegal secara *real-time* tanpa interaksi admin.

Untuk mengatasi ancaman Webhook Spoofing dan Replay Attack, berbagai penelitian telah mengusulkan mekanisme keamanan berbasis verifikasi integritas data dan validasi waktu transaksi. Salah satu pendekatan yang banyak digunakan adalah algoritma HMAC-SHA256 yang terbukti efektif dalam menjamin keaslian dan integritas data yang dikirimkan melalui API. Selain itu, validasi berbasis timestamp juga umum diterapkan untuk membatasi rentang waktu validitas suatu permintaan sehingga dapat mengurangi risiko serangan Replay Attack.

Meskipun demikian, implementasi mekanisme tersebut masih memiliki sejumlah keterbatasan. Penggunaan HMAC-SHA256 sering kali menghadapi kendala latensi ketika proses verifikasi masih bergantung pada basis data relasional (Hendra et al., 2025). Di sisi lain, strategi validasi berbasis timestamp dinilai belum sepenuhnya efektif dalam menangani duplikasi event secara presisi pada kondisi jaringan yang tidak stabil (Wang, 2024). Selain itu, pemanfaatan teknologi Redis pada penelitian terdahulu masih lebih banyak difokuskan pada optimasi performa sistem dan belum dieksplorasi secara maksimal sebagai lapisan keamanan (security layer) untuk mencegah serangan berbasis logika aplikasi (Joshi, 2024). Keterbatasan tersebut menunjukkan masih adanya kesenjangan penelitian dalam pengembangan mekanisme pertahanan yang tidak hanya aman, tetapi juga mampu merespons ancaman secara real-time dengan tetap mempertahankan performa sistem.

Untuk menjawab tantangan tersebut, penelitian ini mengusulkan strategi mitigasi *Defense-in-Depth* yang mengintegrasikan dua lapisan pertahanan vital. Lapisan pertama menggunakan verifikasi HMAC-SHA256 sebagai standar otentikasi data, sedangkan lapisan kedua diperkuat dengan mekanisme Idempotency Key berbasis Redis. Mekanisme ini berfungsi sebagai penanda unik untuk mendeteksi dan

memblokir eksekusi ulang pada transaksi yang sama secara otomatis. Fungsi validasi ini menjadi krusial karena arsitektur asinkron rentan terhadap anomali *Race Condition*, yang terbukti menyebabkan 54% pelanggaran semantik serius berupa pencatatan ganda (*Duplicate Entries*) yang merugikan integritas keuangan (Qiu et al.,2022). Risiko ini diperparah oleh *bottleneck* basis data relasional yang memiliki waktu respons lambat hingga 980 ms (Iurchenko, 2025). Sebaliknya, pemanfaatan operasi atomik pada Redis terbukti mampu memangkas waktu respons signifikan menjadi 78 ms dan meningkatkan *throughput* sebesar 40% (Joshi, 2024), sehingga efektif memitigasi serangan duplikasi secara *real-time* sekaligus menutupi kelemahan strategi terdahulu.

Berdasarkan akumulasi kerentanan protokol dan risiko inefisiensi basis data tersebut, penelitian ini bertujuan untuk menganalisis efektivitas strategi *Defense-in-Depth* dalam memitigasi serangan *Replay Attack* dan *Webhook Spoofing* pada studi kasus Website PsikoTest. Urgensi ini didorong oleh risiko finansial nyata berupa *Double Spending* akibat mekanisme *retry* otomatis dari *Payment Gateway* yang gagal ditangani oleh validasi konvensional. Melalui integrasi verifikasi HMAC-SHA256 dan mekanisme Idempotency Key berbasis Redis, penelitian ini diharapkan dapat menghadirkan solusi keamanan yang tidak hanya menjamin integritas transaksi secara presisi, tetapi juga mempertahankan performa sistem yang tinggi sesuai tuntutan ekosistem pembayaran digital modern.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana menerapkan mekanisme pertahanan berlapis (*defense-in- depth*) yang mengintegrasikan validasi *Idempotency Key* berbasis Redis dan Verifikasi HMAC-SHA256 pada modul *callback* sistem eksisting Payment Gateway di Website PsikoTest?

2. Bagaimana hasil analisis efektivitas mitigasi serangan Replay Attack dan Webhook Spoofing setelah penerapan mekanisme pertahanan berlapis

(*defense-in-depth*) tersebut dibandingkan dengan kondisi sistem sebelumnya yang hanya mengandalkan validasi basis data konvensional?

3. Bagaimana dampak penggunaan penyimpanan data berbasis *memory* (*In-Memory Data Store*) Redis terhadap kinerja sistem (latensi dan throughput) saat menghadapi kondisi *high concurrency*?

1.3 Batasan Masalah

Penelitian ini difokuskan pada analisis keamanan untuk memitigasi serangan *Replay Attack* dan *Webhook Spoofing* pada *callback Payment Gateway* Website PsikoTest, dengan menerapkan pendekatan Defense-in-Depth yang mengintegrasikan verifikasi HMAC-SHA256 dan mekanisme Idempotency Key berbasis Redis. Adapun batasan masalah dalam penelitian ini adalah:

1. Analisis terbatas pada dua jenis serangan spesifik, yaitu *Replay Attack* (pengiriman ulang paket transaksi valid) dan *Webhook Spoofing* (pemalsuan identitas server pengirim), dengan target operasi pada *endpoint callback* pembayaran.

2. Solusi keamanan diterapkan menggunakan pendekatan *Defense-in- Depth* yang hanya mencakup dua lapisan pertahanan: verifikasi validitas pengirim menggunakan HMAC-SHA256 dan pencegahan duplikasi data menggunakan Idempotency Key berbasis Redis.

3. Lingkungan pengujian diimplementasikan pada layanan awan *Virtual Private Server* (VPS) bersistem operasi Ubuntu Server yang telah dilengkapi dengan nama domain dan sertifikat SSL/HTTPS terenkripsi. Simulasi *callback* pembayaran dikirimkan langsung dari simulator Tripay menuju *endpoint* publik VPS.

4. Perangkat lunak (*tools*) yang digunakan meliputi Postman untuk validasi fungsional API, Burp Suite untuk simulasi serangan penetrasi (*Replay Attack* dan *Spoofing*), serta Apache JMeter untuk pengujian beban (*stress test*) dan konkurensi sistem.

4. Sistem yang diuji dan diimplementasikan berbasis Node.js (Next.js) dengan basis data MySQL dan Redis, tidak mencakup perbandingan dengan basis data NoSQL atau bahasa pemrograman lain.

5. Konfigurasi Redis Difokuskan pada penggunaan Operasi Atomik (*Atomic Operations*) dan manajemen *Time-To-Live* (TTL) agar kunci idempotensi kadaluarsa secara otomatis demi efisiensi *memory*.

6. Analisis efektivitas sistem dibatasi pada parameter keberhasilan pencegahan *double spending*, deteksi *payload* palsu, serta kinerja sistem (*latency* dan *throughput*), tanpa melakukan analisis kriptanalisis mendalam terhadap algoritma SHA-256.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun Tujuan penelitian ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan mekanisme pertahanan berlapis (*defense-in-depth*) yang mengintegrasikan *Idempotency Key* berbasis Redis dan verifikasi HMAC-SHA256 pada arsitektur *callback* Payment Gateway di Website PsikoTest.
2. Menganalisis efektivitas sistem dalam memitigasi serangan *Replay Attack* dan *Webhook Spoofing* dengan membandingkan tingkat keberhasilan serangan pada sistem yang diusulkan terhadap sistem validasi basis data konvensional.
3. Mengevaluasi dampak penggunaan penyimpanan data berbasis memori (*In-Memory Data Store*) Redis terhadap performa sistem, khususnya pada parameter latensi (*response time*) dan *throughput* saat menangani lalu lintas transaksi yang tinggi (*high concurrency*).

1.4.2 Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Memberikan kontribusi terhadap pengembangan studi di bidang keamanan web (*Web Security*), khususnya dalam implementasi strategi *Defense in Depth* untuk mengamankan arsitektur *Event- Driven* dan *Webhook* pada sistem pembayaran digital.
2. Menawarkan solusi keamanan komprehensif yang mampu menutup celah kerentanan logika bisnis (*Business Logic Abuse*) seperti manipulasi saldo ganda (*Double Spending*) tanpa mengorbankan kecepatan pemrosesan
3. Memungkinkan pengembang sistem untuk menerapkan proteksi integritas data tingkat tinggi yang efisien menggunakan perangkat lunak *open source* (Redis), tanpa bergantung pada peningkatan spesifikasi perangkat keras basis data yang memakan biaya tinggi.
4. Menjadi referensi dalam pengembangan penelitian lanjutan terkait optimasi keamanan infrastruktur *Microservices* dan integrasi pola *Idempotency* pada sistem transaksi *real-time*.
5. Memberikan panduan implementatif bagi praktisi IT dan *Backend Developer* dalam membangun mekanisme validasi *callback* yang efisien dan resisten terhadap ancaman pengulangan paket data.
6. Memberikan dasar bagi Website PsikoTest (Klinik Yuliarpan Medika) untuk meningkatkan standar keamanan operasional pada layanan transaksi digital, sehingga integritas data keuangan perusahaan dan kepercayaan pengguna dapat terjaga.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari 5 bab, yaitu:

1. BAB I PENDAHULUAN

   Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan,

manfaat, dan sistematika penulisan.

2. BAB II TINJAUAN PUSTAKA

Berisi teori-teori yang mendukung penelitian dan ulasan penelitian terdahulu berdasarkan studi literatur.

3. BAB III METODOLOGI PENELITIAN

Menjelaskan rancangan penelitian, objek penelitian, dan tahapan penelitian.

4. BAB IV HASIL DAN PEMBAHASAN

Berisi realisasi rancangan penelitian, yaitu identifikasi kebutuhan, pembuatan model, pengujian, implementasi model ke aplikasi web, dan analisa data yang didapat dari pengujian.

5. BAB V PENUTUP

Berisi kesimpulan penelitian dan saran untuk pengembangan lebih lanjut.

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk menganalisis dan memitigasi kerentanan pada *callback Payment Gateway* Website PsikoTest terhadap serangan *Replay Attack* dan *Webhook Spoofing*. Permasalahan utama yang ingin diselesaikan adalah rentannya arsitektur asinkron terhadap manipulasi logika bisnis dan penggandaan transaksi (*Double Spending*) akibat ketiadaan mekanisme validasi kriptografis dan penanganan konkurensi data.

Berdasarkan hasil perancangan dan serangkaian pengujian komparatif yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

1. Mekanisme pertahanan berlapis (*Defense-in-Depth*) berhasil dirancang dan diimplementasikan secara komprehensif menggunakan verifikasi kriptografi HMAC-SHA256 pada lapisan pertama, mekanisme *Idempotency Key* berbasis Redis pada lapisan kedua, serta didukung *Database Absolute Lock*. Pengujian pra-validasi (*Buffer Mismatch*) menunjukkan bahwa sistem secara mutlak (100%) mampu mengisolasi empat variasi anomali format muatan secara presisi (karakter pendek, *over-length*, *integer*, dan simbol) dengan memotong siklus eksekusi di awal melalui respons HTTP 400 *Bad Request*, menjaga stabilitas *runtime* aplikasi.

2. Sistem terbukti sangat efektif dalam memitigasi serangan pemalsuan identitas dan eksploitasi logika. Pada pengujian *Webhook Spoofing*, lapisan HMAC berhasil mendeteksi dan menolak 100% modifikasi *payload* ilegal dengan waktu respons yang sangat efisien (rata-rata 65,2 ms), melindungi integritas basis data dari manipulasi sepihak. Pada skenario *Replay Attack*, algoritma *fail-fast* Redis beroperasi secara presisi dengan memproses 1 transaksi sah dan seketika memblokir 99 *request* duplikat pesaing di tingkat memori RAM (penolakan 99,00%). Lebih lanjut, pertahanan lapis ketiga (*Database Lock*) sukses memblokir eksploitasi jeda waktu secara mutlak (100%) sesaat setelah kunci memori Redis kedaluwarsa (*TTL Expiry* > 60 detik).

3. Penggunaan *In-Memory Data Store* (Redis) memberikan dampak positif yang sangat signifikan terhadap efisiensi dan stabilitas server saat menghadapi uji tegangan tinggi (*Load & Stress Testing*). Berkat mekanisme penolakan instan oleh *Rate Limiter* dan *Idempotency*, pada beban puncak 10.000 *threads*, sistem *secure* mampu menekan rata-rata latensi hingga 60,6% lebih rendah (5.369 ms) dibandingkan sistem rentan (13.632 ms). Server terbukti sukses mempertahankan *throughput* yang konstan di kisaran 94,1 req/s dan meredam *Load Average* di angka 1,67. Hal ini menghindarkan infrastruktur dari antrean *bottleneck* basis data dan kelumpuhan layanan (*Resource Exhaustion*) yang terjadi pada arsitektur konvensional.

5.2 Saran

Beberapa saran yang dapat dilakukan pada penelitian dan pengembangan selanjutnya, antara lain:

1. Sistem keamanan dapat dikembangkan lebih lanjut dengan mengimplementasikan mekanisme *Message Broker* (seperti Apache Kafka atau RabbitMQ) untuk mengelola antrean pembaruan data secara asinkron (*queueing*) apabila aplikasi dihadapkan pada lalu lintas *enterprise* berskala besar.

2. Perlu dipertimbangkan pengujian stabilitas dan penerapan arsitektur *Redis Cluster* atau *Redis Sentinel* guna meningkatkan ketersediaan layanan (*High Availability*) dan skalabilitas manajemen kunci memori jika API diimplementasikan secara terdistribusi pada beberapa *server*.

3. Sistem pemantauan (*monitoring*) pada terminal aplikasi dapat diintegrasikan dengan fitur notifikasi otomatis (*Alerting System*) berbasis *bot* Telegram atau surel (*email*) untuk memberikan peringatan *real-time* kepada administrator ketika terdeteksi indikasi anomali masif, seperti serangan DDoS atau pemalsuan *signature*.

4. Eksplorasi lebih lanjut dapat difokuskan dengan membandingkan performa efisiensi algoritma enkripsi asimetris (seperti RSA atau ECDSA) sebagai pendamping/alternatif HMAC-SHA256 untuk meminimalisasi risiko penyebaran

Private Key tunggal, dengan catatan penyedia layanan *Payment Gateway* telah mendukung adopsi protokol tersebut.

DAFTAR PUSTAKA

Akuma (2024) 'Navigating the Rising Tide: Attack Trends in Financial Services', *State of the Internet / Security*, 10(5), pp. 1–36.

Al-Omari, A. H. (2025) 'Penetration Testing of a Merchant Payment Platform; Systemic Vulnerabilities and Compliance-Centric Mitigation', *2025 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1–6. doi:https://doi.org/10.1109/ICIT64950.2025.11049241.

Aulia, B. W. et al. (2023) 'Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital', *JUSTINFO (Jurnal Sistem Informasi dan Teknologi Informasi)*, 1(1), pp. 9–18.

Baihaqie, M. R. (2021) 'Analisis dan Perancangan Sistem Pembayaran Pajak dan Retribusi Daerah secara Non-Tunai dengan Menggunakan Layanan Payment Gateway', in *Seminar Nasional Sistem Informasi (SEMNASIF)*. Yogyakarta, pp. 101–119.

Chaudhari, B. and Verma, S. C. G. (2024) 'Achieving High-Speed Data Consistency in Financial Microservices Platforms Using NoSQL Technologies', *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 4(2), pp. 751–758.

Hendra, H. et al. (2025) 'Memperkuat Autentikasi dan Integritas Data REST-API Menggunakan Token HMAC SHA-256', *Jurnal Minfo Polgan*, 13(2), pp. 2189–2196.

Turchenko, A. (2025) 'Optimization of Microservices Architecture Performance in High-Load Systems', *The American Journal of Engineering and Technology*, pp. 123–131.

Joshi, P. K. (2024) 'Redis Cache Optimization for Payment Gateways in the Cloud', *IJETCSIT*, 4(1), pp. 28–3

Kurniawan, A., Nursyabani, N. and Matin, I. M. M. (2025) 'Analisis Keamanan Website Kota Depok Menggunakan Metode Vulnerability Assesment', *Jurnal Multinetics*, 11(1), pp. 62–73.

Mahadik, D. et al. (2025) 'To Study Webhooks for an Event-Driven Integration Mechanism', *Alochana Journal*, 14(11), pp. 35–39.

Obaida, M. A. et al. (2024) 'Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions', *Big Data and Cognitive Computing*, 8(12), p. 174.

Qiu, Z. et al. (2022) 'A Deep Study of the Effects and Fixes of Server-Side Request Races in Web Applications', in *19th International Conference on Mining Software Repositories (MSR '22)*. Pittsburgh, PA, USA: ACM, pp. 744–756.

Rainita, N. P. A. et al. (2023) 'Analisis Perbandingan Vulnerability Scanning Pada Website DVWA Menggunakan OWASP Nikto Dan Burpsuite', *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, 3(2), pp. 89–97

Ranjan, P. et al. (2022) 'Threat Modeling and Risk Assessment of APIs in Fintech Applications', *ESP Journal of Engineering & Technology Advancements*, 2(2), pp. 44–61.

Salt Security (2025) *State of API Security Report, Q1 2025*. Palo Alto: Salt Security.

Shrikant, S. B. (2025) 'Enhancing Retry Policies for Webhook Delivery in Fintech Platforms', *IEEE*, pp. 1–6.

Taofik, I. et al. (2023) 'Implementasi JSON Web Token (JWT) untuk Authentication Data pada Aplikasi Bayeue Dengan Algoritma HMAC SHA-256', *Jurnal Tekno Kompak*, 17(1), pp. 1–6.

Uskono, B. M. et al. (2024) 'Analisis Keamanan Aplikasi Fintech di Indonesia: Studi Kasus OVO, GoPay, ShopeePay dan Dana', *Jurnal JIFORTY (Jurnal Ilmiah Informatika dan Teknologi)*, 5(2), pp. 177–186

Wang, Y. (2024) 'Optimizing Payment Systems with Microservices and Event- Driven Architecture: The Case of Mollie Platform', *Journal of Industrial Engineering and Applied Science*, 2(1), pp. 56–67.

Zanah, A. S. et al. (2025) 'Deteksi Dini Fraud pada Layanan Keuangan Digital Menggunakan Metode Random Forest', *Indonesian Journal on Data Science*, 3(2), pp. 97–107.

DAFTAR RIWAYAT HIDUP

Jibran Khairy Akram di Jakarta pada tanggal 29 April 2004. Penulis mulai menempuh pendidikan dasar di SDN Harapan Baru II Kota Bekasi pada tahun 2010. Setelah itu, penulis melanjutkan pendidikan ke SMPN 44 Kota Bekasi pada tahun 2016. Pada tahun 2019, penulis melanjutkan pendidikan menengah kejuruan di SMKN 5 Kota Bekasi. Setelah menyelesaikan pendidikan menengah kejuruan, penulis melanjutkan pendidikan tinggi pada tahun 2022 di Politeknik Negeri Jakarta, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan Jaringan.

LAMPIRAN

Tempat: Daring (Online)

Tanggal Wawancara: 15 Januari 2026

Narasumber: Pihak Klinik Yuliarpan Medika (dr. piet)

Lampiran 1 Tabel Wawancara

No	Pertanyaan	Jawaban
1	Apa kendala terbesar yang dokter rasakan dengan sistem pemesanan tes psikotes lewat WhatsApp yang berjalan sekarang?	Kendala utamanya adalah inefisiensi operasional. Admin diharuskan melayani pesan satu per satu, kemudian memeriksa mutasi rekening secara manual untuk mencocokkan bukti transfer. Proses ini seringkali membuat admin kewalahan ketika volume pendaftar meningkat, serta menimbulkan risiko bukti transfer terlewat atau terselip.
2	Solusi seperti apa yang diharapkan dari pengembangan website baru tersebut?	Solusi utama yang diharapkan adalah implementasi fitur pembayaran non-tunai (*cashless*) yang terotomatisasi. Pengguna dapat melakukan pembayaran melalui *Payment Gateway* dan status transaksi terverifikasi secara langsung (*real-time*) oleh sistem, sehingga meniadakan kebutuhan validasi bukti transfer manual ke admin. Tujuannya adalah untuk mewujudkan otomatisasi penuh pada proses transaksi.

No	Pertanyaan	Jawaban
3.	Mengingat sistem akan berjalan secara otomatis tanpa verifikasi manual admin, apakah terdapat kekhawatiran khusus terkait validitas pembayaran?	Kekhawatiran utama terletak pada aspek keamanan validasi. Berbeda dengan mekanisme manual di mana admin dapat memeriksa mutasi bank secara langsung, sistem otomatis memiliki risiko manipulasi data di mana status pembayaran dapat dipalsukan seolah-olah telah lunas. Oleh karena itu, sistem yang dikembangkan harus memiliki mekanisme yang mampu menjamin otentikasi dan keaslian setiap notifikasi pembayaran yang masuk.
4.	Bagaimana harapan dokter jika nanti terjadi gangguan jaringan saat user melakukan pembayaran?	Prioritas utamanya adalah mencegah kerugian finansial maupun operasional. Sistem harus menjamin tidak terjadi duplikasi pencatatan di mana satu kali pembayaran tercatat dua kali, atau sebaliknya. Akurasi dan presisi data keuangan sangat krusial karena berdampak langsung pada pendapatan perusahaan.

No	Pertanyaan	Jawaban
5.	Apakah nantinya admin masih bersedia melakukan pengecekan manual jika ada selisih data antara uang di bank dan status di website?	Harapannya, proses rekonsiliasi manual tidak lagi diperlukan. Tujuan utama otomatisasi sistem adalah untuk mengurangi beban kerja administratif. Oleh karena itu, sistem diharapkan dapat menjamin konsistensi data yang mutlak; apabila status di website tercatat 'Lunas', maka dana harus dipastikan telah masuk dengan nominal yang tepat, tanpa adanya selisih data.

Lampiran 2 Dokumentasi Wawancara

Lampiran 3 Surat Pengantar Observasi

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
Jalan Prof. Dr. G. A.Siwabessy, Kampus UI, Depok 16425
Telepon (021) 7270036, Hunting, Fax (021) 7270034
Laman: http://www.pnj.ac.id Posel: humas@pnj.ac.id

Nomor : 70/DST/PL3.A.9/B/KM.07.00/2026 19 Januari 2026
Perihal : Permohonan Izin Observasi

Kepada Yth.
dr. Piet Y, MARS, FISQua dan Untung Suprihadi, S.Kom., M.Pd.
Dokter Klinik Yuliarpan Medika
Jalan Raya Setu No.149, Cibuntu, Kecamatan Cibitung, Kabupaten Bekasi, Jawa Barat 17520

Dengan hormat,
Sehubungan dengan mata kuliah Skripsi yang dilaksanakan pada semester 8 (delapan) Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta. Dengan ini kami mohon kesediaan Bapak/Ibu agar dapat mengizinkan mahasiswa kami untuk melakukan observasi di **Klinik Yuliarpan Medika** dengan judul penelitian "Analisis Mitigasi Serangan Replay Attack dan Webhook Spoofing pada Callback Payment Gateway Website PsikoTest Menggunakan Mekanisme Idempotency Key Berbasis Redis dan Verifikasi HMAC".

Tugas mata kuliah ini bertujuan untuk menambah wawasan terkait dengan aplikasi teori yang sudah dipelajari di Kampus dengan kondisi lapangan sebagai wadah pembelajaran dan penambah informasi mengenai mata kuliah tersebut. Adapun berikut adalah nama mahasiswa kami:

No.	Nama dan Nim	Semester/ Program Studi	Nomor Telepon dan Email	Tujuan Observasi
1	Jibran Khairy Akram 2207421011	8 / Teknik Multimedia dan Jaringan	085966250075 jibran.khairy.akram.tik22@mhsw.pnj.ac.id	Ingin mengetahui data-data penunjang dan wawancara untuk Skripsi

Demikian surat ini kami buat, atas perhatian dan kerjasama Bapak/Ibu kami ucapkan terima kasih.

Ketua Jurusan,

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

Tembusan :
1. Direktur;
2. Wakil Direktur Bidang Akademik;
3. Kepala Bagian Keuangan dan Umum
4. Kasubbag. Umum Politeknik Negeri Jakarta.

Lampiran 4 Surat Izin Perusahaan Uji Coba Sistem

KLINIK YULIARPAN MEDIKA

Dokter Umum
Dokter Gigi
Bidan
Laboratorium
Medical Check Up

Jl. Raya Setu No.149, Cibuntu, Kec. Cibitung, Kabupaten Bekasi, Jawa Barat 17520

SURAT KETERANGAN PENGGUNAAN DAN UJI COBA SISTEM

Yang bertanda tangan di bawah ini:

Nama : dr. Piet Y, MARS, FISQua.

Jabatan : Dokter

Instansi : Klinik Yuliarpan Medika

Dengan ini menerangkan bahwa sistem/aplikasi berbasis web "Psychotest Website" telah diimplementasikan, digunakan, dan diuji coba di lingkungan Klinik Yuliarpan Medika.

Berdasarkan hasil penggunaan dan uji coba yang telah dilakukan, sistem dapat digunakan untuk mendukung kegiatan operasional dan masih dalam tahap pengembangan serta penyempurnaan lebih lanjut, khususnya pada aspek keamanan sistem dan data.

Demikian surat keterangan ini dibuat untuk digunakan sebagaimana mestinya.

Bekasi, 4 Mei 2026

dr. Piet Y, MARS, FISQua