

Analisis Prioritas Risiko Penggunaan Aplikasi GOJEK Menggunakan Metode FMEA Pada Mahasiswa UIGM

Fauzan Azima¹, Nining Ariati², Anugrah Saputra³, M. Bimantara Sujana⁴, Muhammad Daffa⁵

¹⁻⁶ Sistem Informasi, Universitas Indo Global Mandiri

¹⁻⁷ Jalan Jend. Sudirman KM. 4 No. 629, 20 Ilir D. IV, Ilir Tim. I, Kota Palembang, Sumatera Selatan 30129, Indonesia

Email: zimazan15@gmail.com¹, nining@uigm.ac.id², anugerahsaputra16@gmail.com³, mbimantarasujana1@gmail.com⁴, muhammaddaffa7896@gmail.com⁵

Abstract

For students, the Gojek app is an instant and efficient way to carry out daily activities without having to leave the house. Although Gojek offers many conveniences for students, this application still has risks that can be detrimental to both users and service providers. The purpose of this study is to identify and analyze risks in the Gojek application using the Failure Mode and Effects Analysis (FMEA) method. Using this method, we can determine the level of risk management through a value called the risk priority number. This study uses a descriptive quantitative approach by collecting respondents of 100 students. Data collected through questionnaires were analyzed based on Severity, Occurrence, and Detection to obtain the Risk Priority Number (RPN) value. The results show that the highest risk is driver refusal to accept the location. Other high risks include GoPay refund failures, GoSend delays, and unilateral order cancellations. These results indicate that operational risks are the top priority, followed by security and financial aspects, so improvements are needed to improve service quality, system security, and transaction transparency. This study makes a meaningful contribution to understanding risk management in the Gojek application, by providing appropriate analysis based on real data for use in improving the Gojek application.

Key Words: Descriptive quantitative approach, FMEA, Gojek, Risk Priority Number, Students

Abstrak

Bagi kalangan mahasiswa, aplikasi Gojek merupakan cara instan serta efisien dalam beraktivitas sehari-hari tanpa perlu keluar ruangan. Meskipun Gojek banyak memberikan kemudahan bagi mahasiswa, aplikasi ini tetap mempunyai risiko yang dapat merugikan pengguna maupun penyedia layanan. Tujuan dari penelitian ini untuk mengidentifikasi dan menganalisis risiko pada aplikasi Gojek menggunakan metode Failure Mode and Effects Analysis (FMEA). Dengan menggunakan metode ini, kita dapat mengetahui tingkat penanganan risiko melalui nilai yang disebut risk priority number. penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan mengumpulkan responden sejumlah 100 mahasiswa. Data yang telah dikumpulkan melalui kuesioner dan dianalisis berdasarkan Severity, Occurrence, dan Detection untuk mendapatkan nilai Risk Priority Number (RPN). Hasil menunjukkan bahwa risiko tertinggi adalah penolakan driver terhadap lokasi. Risiko tinggi lainnya meliputi kegagalan refund GoPay, keterlambatan GoSend, dan pembatalan pesanan secara sepihak. Hasil ini menunjukkan bahwa risiko operasional menjadi prioritas utama, diikuti oleh aspek keamanan dan finansial, sehingga diperlukan perbaikan untuk meningkatkan kualitas layanan, keamanan sistem, dan transparansi transaksi. Penelitian ini menyumbangkan kontribusi yang bermakna dalam memahami pengelolaan risiko aplikasi Gojek, dengan memberikan analisis yang sesuai pada data yang nyata untuk digunakan dalam perbaikan aplikasi Gojek.

Kata Kunci: FMEA, Gojek, Mahasiswa, Pendekatan kuantitatif deskriptif, Risk Priority Number

Pendahuluan

Seiring dengan perkembangan zaman, teknologi informasi telah menjadi nafas kehidupan masyarakat dan memberikan dampak yang sangat signifikan dalam memenuhi kebutuhan sehari-hari. Di era digital saat ini, akses yang mudah dan cepat terhadap suatu layanan merupakan dua kunci utama dalam mewujudkan keberhasilan inovasi teknologi[1]. Kemajuan ini telah mendorong terjadinya transformasi

digital dalam berbagai sektor, termasuk ekonomi dan transportasi, yang mengubah pola konsumsi masyarakat menjadi lebih efisien.

Gojek hadir sebagai salah satu wujud nyata dari kemajuan teknologi informasi tersebut dengan konsep *super app* yang berhasil menyatukan berbagai layanan transportasi, logistik, pembayaran, dan jasa dalam satu platform integratif. Keberadaan aplikasi ini sukses menjadi solusi praktis yang mengubah cara pengguna berinteraksi dengan lingkungan sekitarnya, terutama dalam hal efisiensi waktu dan tenaga [2]. Sebagai platform layanan digital terbesar di Indonesia, gojek tidak hanya berperan sebagai penyedia layanan, tetapi juga sebagai inovasi baru yang mengubah masyarakat dalam memanfaatkan teknologi untuk kemudahan hidup [3].

Sering kali, bagi kalangan mahasiswa aplikasi Gojek merupakan Langkah strategis untuk memenuhi kebutuhan layanan yang instan dan mudah diakses karena desakan akademik, mobilitas antar kampus dan kos-kosan, waktu pengumpulan tugas yang semakin dekat (*deadline*), serta mahasiswa banyak yang hidupnya semua ingin praktis dan cepat [4]. Gojek menyajikan fitur-fitur seperti transportasi online, layanan antar makanan, pengiriman barang, sampai ada pembayaran digital yang sangat bermanfaat untuk efisiensi waktu dan tenaga. Keberadaan aplikasi Gojek menjadi daya tarik bagi mahasiswa dalam memenuhi kebutuhan sehari-hari karena memberikan kemudahan dan efisiensi dalam beraktivitas. [5].

Namun, ketergantungan pada platform digital juga menyimpan berbagai potensi risiko masalah di balik kemudahannya. Berdasarkan kenyataan di lapangan pengguna sering kali menemui berbagai risiko masalah muncul yang mengganggu pengalaman layanan. Pada aspek operasional layanan, contohnya adalah fenomena driver yang menolak untuk mengantarkan konsumennya hingga ke titik lokasi pasti (seperti menolak masuk gang sempit atau tempat yang sedang dalam kondisi ramai), pembatalan pesanan secara sepihak oleh driver, serta keterlambatan pada layanan pengiriman dokumen (GoSend) yang berdampak pada nilai akademik mahasiswa.

Ancaman tidak hanya pada aspek operasional saja, aspek keamanan dan finansial juga memiliki risiko masalah. Seperti, Modus penipuan yang mengatas namakan Customer Service (CS) Gojek untuk meminta kode OTP yang dimiliki pengguna yang dapat menyebabkan ancaman serius terhadap aset data [6]. Dalam konteks keamanan informasi, kerugian finansial dan pencurian data identitas merupakan dampak paling krusial yang harus diantisipasi oleh pengguna layanan berbasis digital [7]. Tidak hanya itu, masalah keuangan seperti kegagalan sistem dalam pengembalian saldo (*refund GoPay*) secara otomatis saat pesanan dibatalkan, serta pemotongan saldo yang tidak disengaja akibat fitur berlangganan, juga kerap menjadi keluhan bagi mahasiswa karena merugikan secara langsung. Namun, apabila serangkaian isu dan risiko ini tidak cepat dikelola dengan baik, maka secara bertahap akan berkurang juga kepercayaan, kepuasan dan rasa ketertarikan pengguna terhadap platform tersebut [8].

Diperlukan sebuah tindakan nyata dan terstruktur dalam mengatur risiko agar kegagalan layanan dapat ditekan seminimal mungkin. Metode Analisis Mode dan Efek Kegagalan (*Failure Mode and Effects Analysis / FMEA*) metode ini dipilih sebagai pendekatan utama dalam penelitian ini karena kapabilitasnya yang sangat komprehensif dalam mengidentifikasi potensi kegagalan. Melalui FMEA, setiap kemungkinan kegagalan akan dievaluasi berdasarkan tiga parameter krusial, yaitu *Severity* (tingkat keparahan dampak), *Occurrence* (frekuensi terjadinya kegagalan), dan *Detection* (kemampuan sistem dalam mendeteksi kegagalan [9]. Ketiga parameter ini akan menghasilkan sebuah nilai komposit yang disebut *Risk Priority Number* (RPN). Nilai RPN ini berfungsi sebagai tolak ukur objektif untuk menentukan prioritas penanganan risiko, di mana risiko dengan nilai RPN tertinggi menjadi fokus utama perbaikan [10].

Secara khusus, penelitian ini bertujuan untuk mengidentifikasi risiko-risiko utama yang umum pernah dialami mahasiswa saat memanfaatkan Gojek. Melalui penerapan analisis FMEA, diharapkan kajian ini dapat memberikan pemahaman tentang risiko utama yang perlu segera diatasi. Penelitian ini diharapkan hasilnya dapat memberikan saran dan kontribusi nyata kepada penyedia layanan untuk terus meningkatkan kualitas operasional serta keamanan sistem bagi para pengguna.

Metode Penelitian

Jenis dan Pendekatan Penelitian

Penelitian ini menerapkan pendekatan kuantitatif deskriptif. Pendekatan kuantitatif deskriptif dipilih karena studi ini bertujuan untuk menggambarkan, mengukur, dan mengkaji secara sistematis mengenai manajemen risiko pemanfaatan aplikasi Gojek di kalangan mahasiswa berdasarkan data numerik yang dikumpulkan. Pendekatan ini merupakan metode yang tepat untuk menganalisis variabel spesifik tanpa memberikan perlakuan atau intervensi khusus terhadap subjek penelitian [11]. Pendekatan ini tidak melakukan uji hipotesis, melainkan fokus pada deskripsi data berdasarkan perhitungan indeks tertentu untuk memetakan kondisi yang sebenarnya terjadi di lapangan [12].

Identifikasi awal mode kegagalan dilakukan melalui tiga tahapan, yaitu studi literatur terhadap penelitian sebelumnya mengenai risiko layanan transportasi online, observasi terhadap pengalaman penggunaan aplikasi Gojek di kalangan mahasiswa, serta diskusi dengan beberapa pengguna aktif untuk memverifikasi relevansi setiap risiko. Hasil identifikasi tersebut menghasilkan tujuh mode kegagalan yang kemudian dijadikan indikator dalam kuesioner.

Tahapan Penelitian

Untuk memastikan metodologi berjalan secara sistematis, penelitian ini dilaksanakan melalui tahapan-tahapan berikut:



Gambar 1 Tahapan Penelitian

Populasi dan Sample Penelitian

Penelitian ini hanya melibatkan 100 mahasiswa Universitas Indo Global Mandiri menggunakan teknik purposive sampling sehingga hasil penelitian belum dapat digeneralisasikan kepada seluruh pengguna aplikasi Gojek di Indonesia yang memiliki karakteristik berbeda [13].

Penelitian ini berfokus pada pengalaman pengguna mahasiswa UIGM sebagai kelompok pengguna yang memiliki karakteristik mobilitas, kebutuhan akademik, dan penggunaan layanan digital tertentu. Penelitian selanjutnya disarankan melibatkan responden dari berbagai perguruan tinggi, wilayah, kelompok pekerjaan, dan jumlah sampel yang lebih besar agar hasil penelitian lebih representatif..

Teknik Pengumpulan Data

Data dalam penelitian ini dikumpulkan menggunakan kuesioner yang disebarakan secara daring dan door to door. Kuesioner dirancang berdasarkan identifikasi awal risiko yang telah diklasifikasikan ke dalam tiga domain utama: aspek operasional, keamanan, dan finansial. Kuesioner disusun menggunakan skala Likert yang memiliki reliabilitas dan validitas tinggi dalam mengukur persepsi responden [14]. Responden diminta untuk menilai setiap pernyataan risiko menggunakan skala Likert 1 sampai 5 yang kemudian dikonversikan ke dalam parameter FMEA [15].

Konversi Skala Likert ke Parameter FMEA Standar (1–10)

Standar FMEA menggunakan skala 1–10 yang umumnya diisi oleh para ahli Teknik. Karena penelitian ini menggunakan data persepsi pengguna melalui kuesioner skala Likert 1–5, maka diperlukan metode transformasi linier untuk mengkonversi nilai rata-rata Likert ke dalam skala FMEA 1–10 tanpa mengubah proporsi jarak antar nilai [10].

Rumus konversi yang digunakan adalah:

$$\text{Nilai FMEA} = [(\text{Nilai Rata-rata Likert} - 1) \times 2,25] + 1$$

Berdasarkan rumus tersebut, dirancang tabel konversi acuan sebagai berikut:

Tabel 1 Nilai Konversi Skala Likert

Rentang Nilai Rata-Rata Likert	Konversi Skala Fmea (1-10)	Kategori Severity (S)	Kategori Occurrence (O)	Kategori Detection (D)
1,00 – 1,44	1,00 – 2,00	Sangat Rendah	Sangat Jarang	Sangat Mudah Dideteksi
1,45 – 1,89	2,01 – 4,00	Rendah	Jarang	Mudah Dideteksi
1,90 – 2,33	4,01 – 5,00	Cukup Rendah	Cukup Jarang	Cukup Mudah Dideteksi
2,34 – 2,78	5,01 – 6,00	Sedang	Sedang	Sedang Sulit Dideteksi
2,79 – 3,22	6,01 – 7,00	Tinggi	Sering	Sulit Dideteksi
3,23 – 3,67	7,01 – 8,00	Sangat Tinggi	Sangat Sering	Sangat Sulit Dideteksi
3,68 – 5,00	8,01 – 10,00	Kritis/Hampir Pasti	Hampir Pasti Terjadi	Sangat Kritis/Tidak Terdeteksi

Kategorisasi Nilai RPN (Skala 1-10)

Pendekatan yang diterapkan dalam penelitian ini adalah Analisis Modus Kegagalan dan Dampaknya (FMEA) yang disesuaikan dengan instrumen kuesioner menggunakan skala Likert 1-10. Ada tiga parameter utama dalam evaluasi FMEA yang diajukan kepada responden, yaitu: Severity (S) yang menilai tingkat keparahan dampak dari kegagalan, Occurrence (O) yang menghitung frekuensi terjadinya kegagalan, dan Detection (D) yang menilai kemampuan sistem dalam mendeteksi kegagalan. Nilai S, O, dan D untuk setiap kategori risiko selanjutnya dihitung berdasarkan nilai rata-rata (mean) dari semua jawaban responden [10]. Setelah ketiga parameter didapatkan, langkah berikutnya ialah menghitung nilai Risk Priority Number (RPN) dengan rumus:

$$RPN = S \times O \times D$$

Nilai RPN yang dihasilkan kemudian dikategorikan untuk menentukan level risiko, di mana semakin tinggi nilai RPN, semakin prioritas risiko tersebut memerlukan penanganan.

Tabel 2 Kategori Level Risiko

Rentang Nilai RPN	Level Risiko	Prioritas Penanganan
1 – 150	Rendah	Risiko dapat diterima, tidak memerlukan tindakan segera
151 – 250	Sedang	Perlu pemantauan dan perbaikan rutin
251 – 350	Tinggi	Memerlukan tindakan perbaikan prioritas
351 – 1000	Sangat Tinggi	Memerlukan intervensi segera dan mendasar

Hasil dan Pembahasan

A. Identifikasi Aset Kritis

Identifikasi awal mode kegagalan dilakukan melalui studi literatur, observasi pengalaman penggunaan aplikasi Gojek di kalangan mahasiswa, dan diskusi eksploratif dengan pengguna aktif. Proses ini dilakukan untuk memastikan bahwa risiko yang dipilih memiliki relevansi dengan pengalaman pengguna. Risiko yang muncul dari ketiga tahap tersebut dikelompokkan ke dalam aspek operasional, keamanan, dan finansial. Selanjutnya, tujuh risiko yang paling relevan dijadikan indikator dalam instrumen kuesioner.

Berikut merupakan tabel dari hasil identifikasi aset kritis:

Tabel 3 Identifikasi Aset

No.	Kategori	Aset
1.	Aset Finansial	Saldo GoPay dan cashflow keuangan pribadi mahasiswa
2.	Aset Waktu dan Akademik	Waktu istirahat, jadwal kuliah, dan tenggat (deadline) pengumpulan tugas/dokumen
3.	Aset Data dan Identitas Digital	Data pribadi (KTP, Nomor HP), Kode OTP, dan Riwayat Transaksi
4.	Aset Kenyamanan Fisik	Lokasi pengantaran tepat di titik tujuan tanpa perlu berjalan kaki jauh

B. Identifikasi Risiko

Berdasarkan aset kritis di atas, risiko diidentifikasi melalui potensi kegagalan sistem dan layanan yang dirasakan oleh mahasiswa. Risiko dikelompokkan menjadi tiga domain utama yaitu:

Tabel 4 Identifikasi Risiko

No.	Jenis Risiko	Risiko
1.	Aspek Finansial	Kegagalan sistem dalam mengembalikan dana (Refund GoPay) secara langsung saat pesanan batal
2.		Pemotongan saldo otomatis akibat tidak sengaja mengklik fitur berlangganan
3.	Aspek Keamanan	Penipuan yang mengatasnamakan CS Gojek untuk meminta kode OTP
4.		Penyalahgunaan data dan penumpukan tagihan akibat meminjamkan akun kepada teman

5.	Aspek Operasional	Driver menolak untuk mengantarkan sampai ke lokasi pasti (menolak masuk gang)
6.		Driver batalkan pesanan secara sepihak
7.		Terjadi keterlambatan pada layanan pengiriman dokumen (GoSend)

C. Menentukan Nilai Severity, Occurrence dan Detection

Berdasarkan hasil survei dari pernyataan kuesioner yang telah dilakukan, berikut adalah hasil dari penentuan tingkat *severity*, *occurrence* dan *detection* untuk setiap potensi kegagalan yang tercantum dalam tabel berikut.

Tabel 5 Nilai SOD

No.	Aset	Identifikasi Risiko	Severity	Occurrence	Detection
1.	Finansial	Kegagalan sistem dalam mengembalikan dana (Refund GoPay) secara langsung saat pesanan batal	5,75	5,91	6,31
2.		Pemotongan saldo otomatis akibat tidak sengaja mengklik fitur berlangganan	5,18	5,41	5,34
3.	Keamanan	Penipuan yang mengatasnamakan CS Gojek untuk meminta kode OTP	6,71	6,49	4,67
4.		Penyalahgunaan data dan penumpukan tagihan akibat meminjamkan akun kepada teman	6,11	5,82	5,46
5.	Operasional	Driver menolak untuk mengantarkan sampai ke lokasi pasti (menolak masuk gang)	6,90	7,46	6,65
6.		Driver batalkan pesanan secara sepihak	6,24	6,11	5,43
7.		Terjadi keterlambatan pada layanan pengiriman dokumen (GoSend)	6,00	6,87	5,18

D. Hasil Dari RPN

Setelah nilai Severity (S), Occurrence (O), dan Detection (D) diperoleh, ketiga parameter tersebut dikalikan untuk menghasilkan nilai *Risk Priority Number* (RPN). Penentuan prioritas risiko didasarkan pada nilai RPN tertinggi, yang mengindikasikan kombinasi dampak yang paling parah, frekuensi yang sering, dan kemampuan deteksi yang paling rendah. Berikut ini adalah tabel yang menyajikan peringkat

risiko, nilai RPN, tingkat risiko, serta rekomendasi tindak lanjut yang diperlukan untuk meningkatkan kualitas layanan aplikasi Gojek.

Tabel 6 Hasil Dari RPN

Rank	Identifikasi Risiko	S	O	D	Nilai RPN	Level
1.	Driver menolak untuk mengantarkan sampai ke lokasi pasti (menolak masuk gang)	6,90	7,46	6,65	341,81	Tinggi
2.	Kegagalan sistem dalam mengembalikan dana (Refund GoPay) secara langsung saat pesanan batal	5,75	5,91	6,31	214,16	Sedang
3.	Terjadi keterlambatan pada layanan pengiriman dokumen (GoSend)	6,00	6,87	5,18	213,63	Sedang
4.	Driver batalkan pesanan secara sepihak	6,24	6,11	5,43	207,12	Sedang
5.	Penipuan yang mengatasnamakan CS Gojek untuk meminta kode OTP	6,71	6,49	4,67	203,41	Sedang
6.	Penyalahgunaan data dan penumpukan tagihan akibat meminjamkan akun kepada teman	6,11	5,82	5,46	193,73	Sedang
7.	Pemotongan saldo otomatis akibat tidak sengaja mengklik fitur berlangganan	5,18	5,41	5,34	149,86	Rendah

E. Analisis Hasil Perhitungan RPN

Berdasarkan hasil perhitungan yang telah dilakukan, nilai Risk Priority Number (RPN) pada skala FMEA 1–10 berkisar antara 149,86 hingga 341,81. Mengacu pada tabel ambang batas RPN yang telah ditetapkan (Tabel Kategorisasi RPN), hanya satu risiko yang masuk kategori "Tinggi", lima risiko berada pada kategori "Sedang", dan satu risiko berada pada kategori "Rendah". Hasil analisis menunjukkan bahwa risiko dengan prioritas tertinggi tetap didominasi oleh masalah pada aspek operasional layanan, sementara aspek keamanan dan finansial menempati posisi menengah hingga rendah. Berikut adalah analisis mendalam berdasarkan urutan prioritas risiko:

1. Prioritas Utama (Risiko Tinggi)

Risiko dengan nilai RPN tertinggi, yakni sebesar 341,81, yaitu "Driver menolak untuk mengantarkan sampai ke lokasi pasti (menolak masuk gang)".

a) Analisis Faktor:

Tingginya nilai RPN ini terutama dipengaruhi oleh nilai Occurrence (O) hasil konversi sebesar 7,46, yang merupakan nilai tertinggi di antara seluruh parameter. Hal ini mengindikasikan bahwa fenomena driver menolak untuk masuk ke lokasi yang sulit dijangkau (seperti gang sempit) adalah kejadian yang sangat sering terjadi dan menjadi keluhan di kalangan mahasiswa.

b) Dampak:

Nilai Severity (S) hasil konversi sebesar 6,90 menunjukkan dampak yang signifikan terhadap kenyamanan fisik dan waktu mahasiswa, di mana mereka terpaksa harus berjalan kaki atau mencari transportasi lain untuk menempuh sisa jalan.

c) Sistem Deteksi:

Nilai Detection (D) hasil konversi sebesar 6,65 mengindikasikan bahwa sistem aplikasi belum memiliki mekanisme efektif untuk mendeteksi atau mencegah penolakan ini secara real-time, sehingga konflik sering terjadi di lapangan.

2. Prioritas Sedang

Lima risiko masuk dalam kategori "Sedang" dengan rentang nilai RPN antara 193,73 hingga 214,16, menandakan bahwa masalah-masalah ini memerlukan pemantauan serta perbaikan rutin, meskipun urgensinya tidak sekritis risiko pada kategori "Tinggi".

a) **Kegagalan Refund GoPay (RPN 214,16):**

Risiko ini memiliki nilai Occurrence (O) hasil konversi tertinggi kedua yaitu 5,91, menunjukkan bahwa kegagalan refund cukup sering terjadi, baik akibat keterlambatan proses dari sistem maupun kendala dalam verifikasi transaksi. Dampaknya tergolong krusial karena dapat mengganggu aktivitas atau kebutuhan pengguna yang bersifat mendesak.

b) **Keterlambatan Pengiriman Dokumen (RPN 213,63):**

Nilai Occurrence (O) sebesar 6,87 menunjukkan bahwa keterlambatan pengiriman cukup sering dialami oleh responden. Nilai Severity (S) sebesar 6,00 menunjukkan bahwa keterlambatan tersebut dapat memberikan dampak yang cukup signifikan, terutama apabila dokumen berkaitan dengan pengumpulan tugas, administrasi, atau kebutuhan akademik yang memiliki batas waktu. Sementara itu, nilai Detection (D) sebesar 5,18 menunjukkan bahwa pengguna masih memiliki kemampuan sedang untuk memantau status pengiriman melalui aplikasi, tetapi sistem belum sepenuhnya mampu mencegah keterlambatan sebelum terjadi.

c) **Pembatalan Pesanan Sepihak (RPN 207,12):**

Risiko ini memiliki nilai hasil konversi yang relatif merata pada seluruh parameter (S: 6,24; O: 6,11; D: 5,43), menunjukkan bahwa perilaku driver yang membatalkan pesanan merupakan masalah operasional yang cukup seimbang antara frekuensi kejadian dan dampaknya terhadap waktu pengguna.

d) **Penipuan OTP (RPN 203,41):**

Menariknya, risiko ini memiliki nilai Severity (S) hasil konversi tertinggi kedua (6,71) setelah penolakan driver. Ini menandakan bahwa meskipun frekuensinya (O: 6,49) tidak setinggi masalah operasional, dampak yang ditimbulkan berpotensi sangat parah (ancaman kebocoran data dan identitas), sehingga sistem keamanan tetap perlu diperkuat meskipun nilai RPN-nya berada pada kategori "Sedang".

e) **Penyalahgunaan Data Akun (RPN 193,73):**

Risiko ini memiliki nilai hasil konversi yang relatif merata pada ketiga parameter (S: 6,11; O: 5,82; D: 5,46). Nilai Occurrence menunjukkan bahwa kebiasaan meminjamkan akun Gojek kepada teman masih cukup sering terjadi di kalangan mahasiswa, yang berpotensi menyebabkan penyalahgunaan data pribadi dan kerugian finansial.

3. Prioritas Rendah

Dua risiko pada aspek keamanan berikut juga berada pada kategori "Rendah", namun tetap memerlukan perhatian karena berkaitan langsung dengan keamanan data pengguna.

a) **Pemotongan Saldo Otomatis (RPN 149,86):**

Risiko ini berada di peringkat terendah dengan kategori "Rendah", tepat di ambang batas kategori "Sedang". Nilai Severity, Occurrence, dan Detection hasil konversi berada di kisaran angka 5, yang mengindikasikan bahwa masalah ini lebih bersifat ketidaknyamanan minor (UI/UX) dan jarang menimbulkan kerugian besar dibandingkan risiko lainnya.

F. Mitigasi Risiko

Berdasarkan hasil analisis nilai Risk Priority Number (RPN), strategi mitigasi risiko dirancang untuk menurunkan tingkat keparahan (Severity), frekuensi kejadian (Occurrence), dan meningkatkan kemampuan deteksi (Detection). Fokus utama penanganan ditujukan pada risiko dengan kategori "Sangat Tinggi" dan "Tinggi".

Berikut adalah rekomendasi mitigasi untuk setiap risiko:

Tabel 7 Mitigasi Risiko

Rank	Identifikasi Risiko	Nilai RPN	Level	Rekomendasi Tindakan
1.	Driver menolak untuk mengantar sampai ke lokasi pasti (menolak masuk gang)	341,81	Tinggi	- Fitur Lokasi Presisi: Mengembangkan fitur <i>pinpoint</i> lokasi dan unggah foto lokasi agar driver mengetahui kondisi jalan sebelum mengambil order. - Kebijakan Driver: Penerapan sistem penalti atau pengurangan insentif bagi driver yang menolak tanpa alasan valid, serta <i>reward</i> bagi driver yang melayani rute sulit.
2.	Kegagalan sistem dalam mengembalikan dana (Refund GoPay) secara langsung saat pesanan batal	214,16	Sedang	- Audit Sistem: Evaluasi dan perbaikan <i>gateway</i> transaksi untuk memastikan proses refund otomatis berjalan instan. - Transparansi: Menambahkan menu "Cek Status Refund" secara <i>real-time</i> di aplikasi untuk mengurangi kecemasan pengguna. - SLA Refund: Menetapkan kebijakan pengembalian dana maksimal 1x24 jam dengan notifikasi yang jelas.
3.	Terjadi keterlambatan pada layanan pengiriman dokumen (GoSend)	213,63	Sedang	- Estimasi Waktu Real-time: Penyempurnaan algoritma estimasi waktu dengan mempertimbangkan data lalu lintas terkini. - Label Prioritas: Menambahkan opsi "Urgent/Dokumen" agar sistem memprioritaskan alokasi driver tercepat. - Kompensasi: Pemberian voucher kompensasi otomatis

				jika terjadi keterlambatan melebihi batas toleransi.
4.	Driver membatalkan pesanan secara sepihak	207,12	Sedang	• Sistem Penalti: Algoritma pendeteksi pola pembatalan (suspend sementara bagi pelanggar). • Proteksi Pengguna: Fitur "Re-book Otomatis" yang mencari driver pengganti dengan harga yang sama atau subsidi harga jika pembatalan terjadi saat peak hour.
5.	Penipuan yang mengatasnamakan CS Gojek untuk meminta kode OTP	203,41	Sedang	• Edukasi Keamanan: Menampilkan <i>banner</i> peringatan hard-coded di aplikasi: "Gojek tidak pernah meminta OTP/Password via telepon/WA". • Notifikasi Sistem: Mengirim <i>alert</i> peringatan instan saat akun mendeteksi percobaan login atau permintaan OTP mencurigakan.
6.	Penyalahgunaan data dan penumpukan tagihan akibat meminjamkan akun kepada teman	193,73	Sedang	• Multi-Factor Authentication (MFA): Mewajibkan verifikasi wajah (<i>Face ID</i>) atau sidik jari untuk transaksi di atas nominal tertentu. • Edukasi Pengguna: Sosialisasi melalui <i>email</i> atau <i>newsletter</i> tentang bahaya meminjamkan akun pribadi.
7.	Pemotongan saldo otomatis akibat tidak sengaja mengklik fitur berlangganan	149,86	Rendah	• UI/UX Design: Penerapan <i>Double Confirmation</i> (Konfirmasi ganda) sebelum transaksi berlangganan diproses. • Kemudahan Akses: Menyediakan tombol "Batalkan Langganan" yang mudah ditemukan di pengaturan akun tanpa ribet.

Kesimpulan

Berdasarkan analisis data yang diperoleh dari 100 responden mahasiswa Universitas Indo Global Mandiri (UGM) menggunakan metode Failure Mode and Effects Analysis (FMEA), penelitian ini berhasil mengidentifikasi dan memetakan berbagai risiko yang dihadapi pengguna dalam memanfaatkan aplikasi Gojek. Setelah nilai Severity, Occurrence, dan Detection dikonversi dari skala Likert (1–5) ke skala standar FMEA (1–10), hasil perhitungan Risk Priority Number (RPN) menunjukkan bahwa risiko dengan prioritas tertinggi atau kategori "Tinggi" adalah driver menolak untuk mengantar sampai ke lokasi pasti seperti menolak masuk ke gang sempit, dengan nilai RPN

sebesar 341,81 dari rentang maksimum 1000. Nilai ini dipengaruhi oleh tingginya frekuensi kejadian (Occurrence) serta dampak yang signifikan terhadap kenyamanan fisik dan waktu pengguna, mengindikasikan bahwa sistem deteksi dini aplikasi belum optimal dalam menangani konflik rute secara real-time.

Selain risiko utama tersebut, penelitian juga menemukan lima risiko lain yang masuk dalam kategori "Sedang" dengan rentang nilai RPN antara 193,73 hingga 214,16, yaitu keterlambatan pada layanan pengiriman dokumen (GoSend), kegagalan sistem dalam mengembalikan dana (Refund GoPay), pembatalan pesanan secara sepihak oleh driver, penipuan yang mengatasnamakan CS Gojek, dan penyalahgunaan data akun. Satu risiko, yaitu pemotongan saldo otomatis, berada pada kategori "Rendah" dengan RPN 149,86. Temuan ini menggarisbawahi bahwa meskipun aspek keamanan siber dan finansial seperti penipuan OTP memiliki tingkat keparahan (Severity) yang relatif tinggi, frekuensi kejadiannya masih lebih rendah dibandingkan hambatan operasional sehari-hari. Secara keseluruhan, temuan penelitian menegaskan bahwa masalah operasional layanan menjadi tantangan terbesar bagi mahasiswa, di mana ketidakpastian waktu dan lokasi berdampak langsung pada aktivitas akademik dan produktivitas mereka, sehingga memerlukan intervensi sistem yang cepat dan terukur.

Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan karena melibatkan 100 responden yang seluruhnya merupakan mahasiswa Universitas Indo Global Mandiri dengan teknik purposive sampling. Oleh karena itu, hasil penelitian belum dapat digeneralisasikan untuk seluruh pengguna aplikasi Gojek di Indonesia. Selain itu, penilaian Severity, Occurrence, dan Detection masih didasarkan pada persepsi pengguna, sehingga belum sepenuhnya menggambarkan data operasional aktual dari penyedia layanan. Penelitian selanjutnya disarankan melibatkan responden dari berbagai perguruan tinggi, wilayah, dan kelompok pekerjaan, menggunakan jumlah sampel yang lebih besar, serta mengombinasikan data persepsi pengguna dengan data keluhan atau data operasional layanan agar prioritas risiko yang dihasilkan lebih komprehensif dan representatif.

Saran

Upaya perbaikan kualitas layanan harus difokuskan pada penanganan risiko operasional yang menjadi keluhan utama pengguna, dimulai dari pengembangan teknologi *pinpoint* lokasi yang lebih presisi, agar driver dapat mempertimbangkan sebelum menerima pesanan. Untuk meminimalisir penolakan lokasi oleh driver, perlu diterapkan kebijakan insentif ganda berupa bonus bagi driver yang melayani rute sulit serta sistem penalti ketat bagi yang membatalkan tanpa alasan valid, guna menciptakan kesepadan layanan yang adil.

Di sisi lain, perbaikan infrastruktur transaksi keuangan sangat mendesak untuk dilakukan dengan menyempurnakan algoritma gateway pembayaran agar proses refund GoPay dapat berjalan secara instan dan otomatis tanpa intervensi manual, dilengkapi dengan fitur transparansi "Cek Status Refund" real-time di dashboard aplikasi. Untuk mengantisipasi keterlambatan pengiriman dokumen yang krusial bagi mahasiswa, sistem perlu mengintegrasikan data lalu lintas terkini untuk estimasi waktu yang lebih akurat serta menambahkan fitur label prioritas "Urgent" dengan mekanisme kompensasi otomatis jika terjadi keterlambatan.

Lebih jauh, peningkatan lapisan keamanan sistem wajib dilakukan dengan mengimplementasikan *Multi-Factor Authentication* (MFA) seperti verifikasi wajah atau sidik jari untuk setiap transaksi sensitif, serta menampilkan *banner* peringatan permanen mengenai larangan memberikan kode OTP kepada pihak manapun sebagai langkah preventif terhadap penipuan. Akhirnya, pengguna sebagai individu juga perlu meningkatkan literasi digital pribadi dengan lebih teliti memeriksa konfirmasi ganda sebelum berlangganan fitur layanan serta menjaga kerahasiaan akun untuk menghindari penyalahgunaan data dan kerugian finansial yang tidak perlu.

Daftar Pustaka

- [1] M. J. P. Perdana and H. Prasetyo, “Pengaruh Kecepatan Layanan dan Ketersediaan Layanan Digital terhadap Kepuasan Masyarakat di BPKAD Kota Yogyakarta,” vol. 8, no. 3, 2025.
- [2] D. A. Rabbani and F. U. Najicha, “Pengaruh Perkembangan Teknologi terhadap Kehidupan dan Interaksi Sosial Masyarakat Indonesia,” 2023.
- [3] J. A. Sari and B. A. Diana, “Dampak Transformasi Digitalisasi terhadap Perubahan Perilaku Masyarakat Pedesaan,” *J. Pemerintah. dan Polit.*, vol. 9, no. 2, pp. 88–96, Jun. 2024, doi: 10.36982/jpg.v9i2.3896.
- [4] S. Nurhayati, S. Nurbayani, and A. Dahliyana, “Pengaruh fitur go-food pada aplikasi go-jek terhadap gaya hidup mahasiswa di era digital”.
- [5] D. F. Siregar, R. D. Putra, and Y. Apriliza, “Pengaruh Kemudahan Penggunaan Dan Keamanan Terhadap Minat Menggunakan Gojek Dengan Tingkat Kepercayaan Sebagai Variabel Moderasi,” vol. 9, no. 5, 2024.
- [6] A. Almadira, Y. Pratama, and F. Purwani, “Melindungi Data Di Dunia Digital: Peran Statigis Enkripsi Dalam Keamanan Data,” 2024.
- [7] B. S. Deva and R. Jayadi, “Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro,” *JATI*, vol. 12, no. 2, pp. 106–117, Sep. 2022, doi: 10.34010/jati.v12i2.6829.
- [8] D. Putri Sekti Ari and L. Hanum, “Pengaruh Kualitas Pelayanan Website Djp Terhadap Kepuasan Pengguna Dengan Modifikasi E Govqual,” *jbisfia*, vol. 15, no. 01, pp. 104–111, Jan. 2021, doi: 10.21776/ub.profit.2021.015.01.11.
- [9] A. Chakhrit, N. E. H. Benharkat, I. H. M. Guetarni, A. Guedri, and M. Chennoufi, “A literature review of risk assessment approaches in failure mode and effects analysis,” *International Journal of Quality & Reliability Management*, vol. 42, no. 9, pp. 2415–2454, Sep. 2025, doi: 10.1108/IJQRM-01-2025-0042.
- [10] F. S. Nevada, E. B. Utomo, Z. Darojah, and E. Kusumawati, “Perhitungan Risk Priority Number Menggunakan Metode Failure Mode and Effect Analysis pada Modular Production System,” 2024.
- [11] M. Irfan Syahroni, “Prosedur Penelitian Kuantitatif,” *Jurnal Al Musthafa*, vol. 2, no. 3, pp. 43–56, Sep. 2022, doi: 10.62552/ejam.v2i3.50.
- [12] A. Syahri, L. Efriyanti, S. Zakir, and M. Imamuddin, “Pengaruh Penggunaan Chat Gpt Terhadap Pola Pikir Mahasiswa Dalam Mata Kuliah Metodologi Penelitian: Studi Penelitian Kuantitatif,” *JIPTI*, vol. 5, no. 1, pp. 135–143, Apr. 2024, doi: 10.52060/jipti.v5i1.1910.
- [13] Sugiyono, *Metode penelitian kuantitatif kualitatif dan r&d*, Ed.2, cet. 29. 2022.

- [14] B. Antoro, “KESALAHAN SISTEMATIS Penggunaan Skala Likert Dalam Penelitian: Analisis Systematic Literature Review,” *JMSH*, vol. 2, no. 2, pp. 63–81, Oct. 2025, doi: 10.70585/jmsh.v2i2.163.
- [15] Suciati Rahayu Widyastuti, “Pengembangan Skala Likert Untuk Mengukur Sikap Terhadap Penerapan Penilaian Autentik Siswa Sekolah Menengah Pertama,” *JEAS*, vol. 3, no. 02, pp. 57–75, Sep. 2022, doi: 10.52188/ja.v3i02.393.