p-ISSN : 2406-7733
e-ISSN : 2597-9922

# ANALISIS KEAMANAN DATA PADA PROSES PENARIKAN SALDO SHOPEEPAY UNTUK MENCEGAH AKSES TIDAK SAH

**Muhammad Dede Fitriawan[1], Abdul Muni[2]**
Program Studi Sistem Informasi Universitas Islam Indragiri
Jalan Provinsi Parit 1, Tembilahan Hulu, Riau, 29212
Email : dedeacc1122@gmail.com[1], abdulmuni@live.com[2]

**Abstrak** - Perkembangan teknologi finansial telah mendorong meningkatnya penggunaan dompet digital sebagai salah satu sarana transaksi yang praktis, cepat, dan efisien. ShopeePay merupakan salah satu layanan dompet digital yang banyak digunakan oleh masyarakat, khususnya mahasiswa, karena kemudahan akses dan fitur transaksi yang beragam, termasuk penarikan saldo. Namun, penggunaan layanan digital juga menghadapi berbagai ancaman keamanan, seperti akses tidak sah, pencurian akun, *phishing*, dan penyalahgunaan kode OTP. Penelitian ini bertujuan untuk menganalisis keamanan data pada proses penarikan saldo ShopeePay untuk mencegah akses tidak sah. Metode penelitian yang digunakan adalah kuantitatif deskriptif dengan teknik pengumpulan data melalui penyebaran kuesioner kepada mahasiswa Sistem Informasi FTIK angkatan 2023. Analisis data dilakukan menggunakan skala Likert untuk mengukur persepsi responden terhadap keamanan data, penggunaan autentikasi, efektivitas OTP (*One-Time Password*), serta potensi risiko akses tidak sah. Hasil penelitian menunjukkan bahwa mayoritas responden memiliki tingkat kepercayaan yang cukup baik terhadap sistem keamanan ShopeePay, terutama pada fitur PIN transaksi, autentikasi berlapis, dan OTP sebagai bentuk perlindungan akun. Meskipun demikian, masih terdapat kekhawatiran terkait ancaman *phishing*, kebocoran data pribadi, dan kurangnya kesadaran pengguna dalam menjaga kerahasiaan informasi akun. Penelitian ini menyimpulkan bahwa keamanan data pada ShopeePay tidak hanya bergantung pada teknologi yang diterapkan oleh penyedia layanan, tetapi juga dipengaruhi oleh perilaku pengguna dalam menerapkan keamanan digital. Oleh karena itu, diperlukan peningkatan edukasi keamanan siber dan penguatan sistem autentikasi untuk meminimalkan risiko akses tidak sah.

**Kata Kunci:** akses tidak sah, autentikasi, dompet digital, keamanan data, penarikan saldo, OTP, ShopeePay.

## I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi sistem pembayaran dari metode konvensional menuju transaksi digital berbasis elektronik. Salah satu bentuk inovasi tersebut adalah penggunaan dompet digital (*e-wallet*) yang semakin diminati masyarakat karena memberikan kemudahan, kecepatan, dan efisiensi dalam melakukan transaksi keuangan. Di Indonesia, peningkatan penggunaan *e-wallet* dipengaruhi oleh tingginya penetrasi internet, perkembangan teknologi finansial (*financial technology*), serta perubahan perilaku masyarakat menuju sistem pembayaran tanpa uang tunai (*cashless society*)(Febriani et al., 2025). ShopeePay merupakan salah satu layanan dompet digital yang banyak digunakan karena terintegrasi dengan platform perdagangan elektronik Shopee dan menyediakan berbagai fitur transaksi, termasuk pembayaran, transfer, dan penarikan saldo.

ShopeePay sebagai layanan keuangan digital memerlukan pengelolaan data pengguna dan transaksi secara aman untuk menjaga kepercayaan pengguna. Dalam sistem digital, data pribadi dan data transaksi merupakan aset penting yang harus dilindungi dari ancaman keamanan siber. Keamanan data menjadi aspek utama dalam sistem informasi karena berkaitan dengan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi (Amalina et al., 2021). Pada proses penarikan saldo, sistem ShopeePay melibatkan autentikasi akun, verifikasi identitas, serta pengiriman data transaksi melalui jaringan internet. Jika mekanisme keamanan tidak diterapkan secara optimal, maka risiko terjadinya akses tidak sah terhadap akun pengguna akan semakin tinggi.

Permasalahan keamanan pada dompet digital saat ini menjadi perhatian serius karena meningkatnya kasus pencurian akun, *phishing*, penyalahgunaan data pribadi, dan pembobolan transaksi digital. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, serangan siber terhadap layanan digital mengalami peningkatan signifikan, terutama pada sektor keuangan berbasis aplikasi (Candra & Irmeilyana, 2024). Akses tidak sah dapat terjadi akibat lemahnya autentikasi pengguna, penggunaan kata sandi yang mudah ditebak, kurangnya kesadaran keamanan digital, maupun kebocoran data pada sistem. Kondisi tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengambil alih akun dan melakukan transaksi tanpa izin pemilik akun.

Dampak dari permasalahan keamanan data tidak hanya merugikan pengguna secara finansial, tetapi juga menurunkan tingkat kepercayaan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

masyarakat terhadap layanan dompet digital. Pengguna yang menjadi korban akses tidak sah dapat mengalami kehilangan saldo, pencurian identitas, hingga penyalahgunaan data pribadi untuk tindakan kriminal lainnya. Selain itu, penyedia layanan juga dapat mengalami penurunan reputasi dan kepercayaan publik apabila sistem keamanan yang dimiliki dianggap tidak mampu melindungi data pengguna secara maksimal(Didin, 2025). Oleh karena itu, perlindungan data pada proses transaksi digital perlu menjadi prioritas utama dalam pengembangan sistem informasi keuangan.

Konsep keamanan data dalam sistem informasi meliputi beberapa mekanisme penting, seperti autentikasi, otorisasi, enkripsi, dan pengawasan sistem (*monitoring system*). Autentikasi digunakan untuk memastikan bahwa pengguna yang mengakses sistem merupakan pihak yang sah, sedangkan otorisasi berfungsi mengatur hak akses pengguna terhadap data tertentu. Selain itu, enkripsi digunakan untuk melindungi data agar tidak mudah dibaca oleh pihak yang tidak memiliki wewenang(Dan et al., 2026). Penerapan teknologi keamanan yang tepat dapat meminimalkan risiko pencurian data dan akses ilegal pada layanan dompet digital. Dalam konteks ShopeePay, keamanan sistem menjadi faktor penting untuk menjaga keberlangsungan layanan dan kenyamanan pengguna.

Penelitian terdahulu mengenai keamanan dompet digital telah banyak dilakukan. Penelitian oleh Rahmawati dan Putra menunjukkan bahwa keamanan autentikasi ganda (*two-factor authentication*) mampu meningkatkan perlindungan akun pengguna *e-wallet* dari ancaman akses ilegal (Cao et al., 2021). Penelitian lain oleh Saputra *et al.* menjelaskan bahwa faktor kesadaran pengguna terhadap keamanan digital memiliki pengaruh signifikan terhadap pencegahan kejahatan siber pada aplikasi keuangan digital (Ramadya Sari et al., 2022). Meskipun demikian, sebagian besar penelitian sebelumnya lebih berfokus pada keamanan transaksi digital secara umum dan belum secara khusus menganalisis keamanan data pada proses penarikan saldo ShopeePay, terutama pada lingkungan mahasiswa sebagai pengguna aktif teknologi digital. Dengan demikian, terdapat *research gap* yang menjadi dasar dilakukannya penelitian ini.

Urgensi penelitian ini terletak pada pentingnya meningkatkan perlindungan data pengguna terhadap ancaman akses tidak sah pada layanan dompet digital. Mahasiswa sebagai kelompok pengguna aktif teknologi finansial memiliki tingkat aktivitas transaksi digital yang tinggi sehingga rentan terhadap berbagai ancaman keamanan siber. Penelitian ini diharapkan dapat memberikan pemahaman mengenai potensi ancaman keamanan data pada proses penarikan saldo ShopeePay serta mekanisme perlindungan yang dapat diterapkan untuk meminimalkan risiko penyalahgunaan akun. Selain itu, hasil penelitian dapat menjadi bahan evaluasi bagi penyedia layanan dalam meningkatkan sistem keamanan aplikasi.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis keamanan data pada proses penarikan saldo ShopeePay guna mencegah akses tidak sah, khususnya pada mahasiswa Sistem Informasi FTIK Angkatan 2023. Penelitian ini dilakukan dengan pendekatan kuantitatif melalui penyebaran kuesioner untuk mengidentifikasi ancaman keamanan data serta mengevaluasi mekanisme perlindungan yang diterapkan. Solusi yang ditawarkan dalam penelitian ini meliputi peningkatan autentikasi pengguna, penguatan sistem enkripsi, serta edukasi keamanan digital bagi pengguna agar mampu mengurangi risiko akses ilegal pada akun dompet digital.

## II. TINJAUAN PUSTAKA

### 2.1 Basis Data

Basis data (*database*) merupakan kumpulan data yang terorganisir dan saling berhubungan sehingga dapat disimpan, dikelola, serta diakses dengan mudah menggunakan sistem komputer (Javaheri et al., 2024). Dalam sistem informasi, basis data digunakan untuk menyimpan berbagai informasi penting, seperti data pengguna, data transaksi, dan riwayat aktivitas sistem. Pengelolaan basis data yang baik dapat membantu meningkatkan efisiensi, keakuratan, dan keamanan informasi dalam suatu sistem digital.

Pada layanan dompet digital seperti ShopeePay, basis data memiliki peran penting dalam menyimpan informasi akun pengguna, saldo, riwayat transaksi, serta data autentikasi. Sistem basis data memungkinkan proses transaksi digital dilakukan secara cepat dan terstruktur. Namun, karena menyimpan data sensitif pengguna, basis data juga menjadi target ancaman keamanan siber seperti pencurian data, manipulasi informasi, dan akses tidak sah (Afrilia et al., 2025). Oleh karena itu, diperlukan mekanisme perlindungan basis data yang baik agar kerahasiaan dan integritas data tetap terjaga.

Keamanan basis data dilakukan melalui beberapa mekanisme, seperti autentikasi pengguna, otorisasi akses, enkripsi data, dan pencadangan (*backup*) sistem . Autentikasi digunakan untuk memastikan bahwa pengguna yang mengakses basis data merupakan pihak yang memiliki hak akses. Otorisasi berfungsi membatasi akses pengguna terhadap data tertentu, sedangkan enkripsi digunakan untuk melindungi data agar tidak mudah dibaca oleh pihak yang tidak berwenang. Dengan penerapan keamanan basis data

p-ISSN : 2406-7733
e-ISSN : 2597-9922

yang baik, risiko kebocoran data dan akses ilegal pada layanan dompet digital dapat diminimalkan.

**2.2 ShopeePay**

ShopeePay merupakan layanan dompet digital yang dikembangkan oleh platform perdagangan elektronik Shopee untuk mendukung transaksi pembayaran digital. ShopeePay memungkinkan pengguna melakukan berbagai aktivitas transaksi seperti pembayaran belanja daring, transfer saldo, pembayaran tagihan, pembelian pulsa, dan penarikan saldo (Zikri et al., 2026). Keberadaan ShopeePay memberikan kemudahan bagi pengguna dalam melakukan transaksi secara cepat tanpa menggunakan uang tunai.

ShopeePay memiliki beberapa fitur utama, antara lain pengisian saldo (*top up*), transfer saldo antar pengguna, pembayaran menggunakan kode QRIS, serta penarikan saldo ke rekening bank. Pada proses penarikan saldo, pengguna harus melakukan verifikasi akun melalui PIN atau kode OTP sebagai bentuk autentikasi keamanan (Hapsari & Pambayun, 2023). Sistem keamanan tersebut bertujuan untuk memastikan bahwa transaksi dilakukan oleh pemilik akun yang sah dan mencegah terjadinya akses ilegal terhadap akun pengguna.

**2.3 Keamanan Data**

Keamanan data merupakan upaya perlindungan terhadap data dan informasi agar terhindar dari ancaman, kerusakan, maupun akses oleh pihak yang tidak berwenang. Dalam sistem informasi, keamanan data memiliki tiga prinsip utama yang dikenal sebagai *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad) (Ovo & Dana, 2021).*Confidentiality* berkaitan dengan kerahasiaan data agar hanya dapat diakses oleh pihak yang memiliki hak akses. *Integrity* berhubungan dengan keutuhan dan keakuratan data agar tidak mengalami perubahan tanpa izin. Sementara itu, *Availability* memastikan bahwa data dan sistem dapat diakses ketika dibutuhkan oleh pengguna yang sah (Febriani et al., 2025). Penerapan keamanan data menjadi sangat penting dalam layanan dompet digital karena sistem menyimpan informasi pribadi dan data transaksi pengguna yang bersifat sensitif.

**2.4 Sistem Informasi**

Sistem informasi merupakan sistem yang digunakan untuk mengelola data transaksi menjadi informasi yang berguna bagi pengguna maupun organisasi (Fauziah & Retnoningsih, 2020). Sistem informasi terdiri dari beberapa komponen, seperti perangkat keras (*hardware*), perangkat lunak (*software*), basis data, prosedur, dan pengguna yang saling berhubungan dalam mengolah data menjadi informasi yang dibutuhkan.

Dalam layanan dompet digital seperti ShopeePay, sistem informasi digunakan untuk memproses transaksi pengguna, menyimpan data akun, mengelola saldo, serta melakukan verifikasi transaksi secara otomatis (Nizatsary et al., 2022). Sistem ini memungkinkan pengguna melakukan aktivitas pembayaran, transfer, dan penarikan saldo secara cepat dan efisien melalui aplikasi digital.

Keamanan sistem informasi menjadi aspek penting dalam layanan keuangan digital karena sistem menyimpan data pribadi dan transaksi pengguna yang bersifat sensitif. Jika sistem informasi tidak memiliki perlindungan keamanan yang baik, maka dapat terjadi ancaman seperti akses tidak sah, pencurian data, dan manipulasi transaksi (Trout & Betts, 1988). Oleh karena itu, diperlukan mekanisme keamanan seperti autentikasi, otorisasi, dan enkripsi data untuk menjaga keamanan informasi pada sistem dompet digital.

**2.5 Penelitian Terdahulu**

Penelitian terdahulu digunakan sebagai dasar dan referensi dalam mendukung penelitian yang dilakukan. Berdasarkan berbagai penelitian terkait keamanan data dan dompet digital, dapat diketahui bahwa aspek keamanan merupakan faktor penting yang memengaruhi kepercayaan, kepuasan, serta keberlanjutan penggunaan layanan fintech, termasuk ShopeePay. Berbagai mekanisme keamanan seperti autentikasi pengguna, enkripsi data, dan perlindungan transaksi terbukti berperan dalam mengurangi risiko akses tidak sah serta meningkatkan rasa aman pengguna dalam melakukan transaksi digital. Selain itu, persepsi pengguna terhadap tingkat keamanan suatu layanan juga menjadi salah satu faktor yang memengaruhi minat dan loyalitas dalam menggunakan dompet digital.

Meskipun demikian, sebagian besar penelitian terdahulu masih berfokus pada keamanan layanan dompet digital secara umum, pengaruh persepsi keamanan terhadap perilaku pengguna, atau penerapan teknologi keamanan pada sistem fintech. Penelitian yang secara khusus menganalisis keamanan data pada proses penarikan saldo ShopeePay sebagai upaya mencegah akses tidak sah, terutama pada kalangan mahasiswa sebagai pengguna aktif layanan dompet digital, masih relatif terbatas. Oleh karena itu, penelitian ini dilakukan untuk mengisi kesenjangan penelitian (*research gap*) tersebut dengan menganalisis aspek keamanan data pada proses penarikan saldo ShopeePay serta mengidentifikasi peran mekanisme keamanan dalam meminimalkan risiko akses tidak sah.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

## III. METODE PENELITIAN

### 3.1 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode kuantitatif dengan pendekatan deskriptif. Penelitian kuantitatif digunakan untuk memperoleh data dalam bentuk angka yang kemudian dianalisis menggunakan teknik statistik sederhana guna mengetahui tingkat keamanan data pada proses penarikan saldo ShopeePay. Pendekatan deskriptif bertujuan untuk menggambarkan kondisi keamanan data serta potensi akses tidak sah yang terjadi pada penggunaan layanan dompet digital ShopeePay. Penelitian ini difokuskan pada mahasiswa Sistem Informasi FTIK angkatan 2023 sebagai objek penelitian karena mahasiswa merupakan salah satu kelompok pengguna aktif layanan dompet digital dalam aktivitas transaksi sehari-hari.

### 3.2 Lokasi dan Waktu Penelitian

Penelitian dilaksanakan pada Program Studi Sistem Informasi Fakultas Teknologi Informasi dan Komunikasi (FTIK) terhadap mahasiswa angkatan 2023 yang menggunakan aplikasi ShopeePay. Waktu penelitian dilakukan pada semester genap tahun akademik 2025/2026, dimulai dari tahap penyusunan instrumen penelitian, pengumpulan data, pengolahan data, hingga penyusunan laporan penelitian.

### 3.3 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini terdiri dari beberapa metode, yaitu:

1. Kuesioner
   Kuesioner digunakan sebagai instrumen utama dalam pengumpulan data. Penyebaran kuesioner dilakukan secara daring menggunakan Google Form kepada mahasiswa Sistem Informasi FTIK angkatan 2023. Kuesioner berisi pernyataan terkait penggunaan ShopeePay, keamanan data, risiko akses tidak sah, dan tingkat kepercayaan pengguna terhadap sistem keamanan ShopeePay.
2. Studi Literatur
   Studi literatur dilakukan dengan mengumpulkan referensi dari jurnal ilmiah, buku, artikel, dan penelitian terdahulu yang berkaitan dengan keamanan data, dompet digital, dan keamanan transaksi digital. Studi literatur digunakan sebagai dasar teori dan pendukung dalam penelitian.

### 3.4 Instrumen Penelitian

Instrumen penelitian yang digunakan berupa daftar pernyataan tertutup berdasarkan skala Likert. Pernyataan dalam kuesioner disusun berdasarkan indikator penelitian yang meliputi:

1. Penggunaan ShopeePay
2. Keamanan data
3. Risiko akses tidak sah
4. Kepercayaan pengguna terhadap sistem keamanan

Instrumen penelitian dibuat untuk mengetahui persepsi responden terhadap keamanan data pada proses penarikan saldo ShopeePay.

### 3.5 Skala Pengukuran

Penelitian ini menggunakan skala Likert sebagai alat ukur untuk mengetahui tingkat persetujuan responden terhadap setiap pernyataan yang diberikan. Adapun kategori jawaban pada skala Likert dapat dilihat pada Tabel 1.

Tabel 1. Skala Likert

| No | Kategori Jawaban | Skor |
|---|---|---|
| 1 | Sangat Setuju (SS) | 5 |
| 2 | Setuju (S) | 4 |
| 3 | Netral (N) | 3 |
| 4 | Tidak Setuju (TS) | 2 |
| 5 | Sangat Tidak Setuju (STS) | 1 |

### 3.6 Teknik Analisis Data

Data yang diperoleh dari hasil kuesioner dianalisis menggunakan teknik analisis deskriptif kuantitatif. Analisis dilakukan dengan menghitung hasil persentase jawaban responden pada setiap indikator penelitian. Data kemudian disajikan dalam bentuk tabel dan uraian deskriptif untuk memberikan gambaran mengenai tingkat keamanan data pada proses penarikan saldo ShopeePay. Tahapan analisis data dalam penelitian ini meliputi:

1. Pengumpulan data hasil kuesioner
2. Pengelompokan data berdasarkan indikator penelitian
3. Perhitungan skor jawaban responden
4. Analisis persentase hasil kuesioner
5. Penarikan kesimpulan berdasarkan hasil analisis data

### 3.7 Tahapan Penelitian

Tahapan penelitian yang dilakukan dalam penelitian ini terdiri dari beberapa langkah sebagai berikut:

1. Identifikasi Masalah
   Menentukan permasalahan terkait keamanan data pada proses penarikan saldo ShopeePay.
2. Studi Literatur
   Mengumpulkan referensi yang berkaitan dengan keamanan data, sistem informasi, dan dompet digital.
3. Penyusunan Instrumen Penelitian
   Menyusun kuesioner berdasarkan variabel dan indikator penelitian.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

4. Pengumpulan Data
   Menyebarkan kuesioner kepada responden penelitian yaitu mahasiswa Sistem Informasi FTIK angkatan 2023.
5. Analisis Data
   Mengolah dan menganalisis data hasil penelitian menggunakan metode deskriptif kuantitatif.
6. Penarikan Kesimpulan
   Menyimpulkan hasil penelitian serta memberikan rekomendasi terkait peningkatan keamanan data pada proses penarikan saldo ShopeePay untuk mencegah akses tidak sah.

## IV. HASIL DAN PEMBAHASAN

### 4.1 Hasil Penelitian

Penelitian ini dilakukan terhadap mahasiswa Sistem Informasi FTIK Angkatan 2023 dengan jumlah responden sebanyak 36 responden. Data penelitian diperoleh melalui penyebaran kuesioner secara daring menggunakan Google Form. Kuesioner disusun berdasarkan variabel penelitian yang meliputi penggunaan ShopeePay, keamanan data, risiko akses tidak sah, autentikasi keamanan, dan kepercayaan pengguna terhadap sistem keamanan ShopeePay.Berdasarkan hasil pengumpulan data, sebagian besar responden merupakan pengguna aktif ShopeePay yang telah menggunakan fitur transaksi digital dan penarikan saldo. Selain itu, penelitian juga didukung dengan observasi langsung terhadap penggunaan ShopeePay pada transaksi digital di merchant retail sebagai dokumentasi penelitian. Hasil penelitian menunjukkan bahwa responden memiliki persepsi yang cukup baik terhadap keamanan sistem ShopeePay, meskipun masih terdapat kekhawatiran terkait potensi akses tidak sah pada akun dompet digital.

### 4.2 Dokumentasi Penelitian




Gambar 1. Dokumentasi Penggunaan ShopeePay pada Merchant Retail

Gambar 1 menunjukkan aktivitas pengguna saat melakukan transaksi digital menggunakan layanan ShopeePay pada merchant retail modern. Pada proses transaksi tersebut, pengguna menggunakan perangkat pribadi untuk melakukan autentikasi transaksi melalui aplikasi ShopeePay sebelum pembayaran diproses oleh sistem kasir merchant. Penggunaan ShopeePay dalam transaksi digital memberikan kemudahan dan efisiensi karena transaksi dapat dilakukan secara cepat tanpa menggunakan uang tunai. Namun demikian, proses transaksi digital juga memerlukan sistem keamanan yang baik untuk melindungi data pengguna dari ancaman akses tidak sah. Berdasarkan hasil observasi, sistem keamanan ShopeePay menerapkan mekanisme autentikasi melalui penggunaan PIN dan kode OTP (*One Time Password*) untuk memverifikasi identitas pengguna. Penggunaan OTP bertujuan untuk memastikan bahwa transaksi dilakukan oleh pemilik akun yang sah sehingga dapat meminimalkan risiko penyalahgunaan akun digital.Selain itu, observasi menunjukkan bahwa pengguna harus menjaga kerahasiaan kode OTP dan data akun agar tidak disalahgunakan oleh pihak lain. Risiko pencurian akun dapat terjadi apabila pengguna memberikan kode OTP kepada pihak yang tidak bertanggung jawab. Oleh karena itu, kesadaran pengguna terhadap keamanan digital menjadi faktor penting dalam menjaga keamanan transaksi dompet digital.Dokumentasi penelitian ini mendukung hasil kuesioner yang menunjukkan bahwa fitur autentikasi seperti OTP dan PIN dianggap mampu membantu mencegah akses tidak sah pada akun ShopeePay.

### 4.3 Analisis Hasil Kuesioner

#### 4.3.1 Variabel Penggunaan ShopeePay

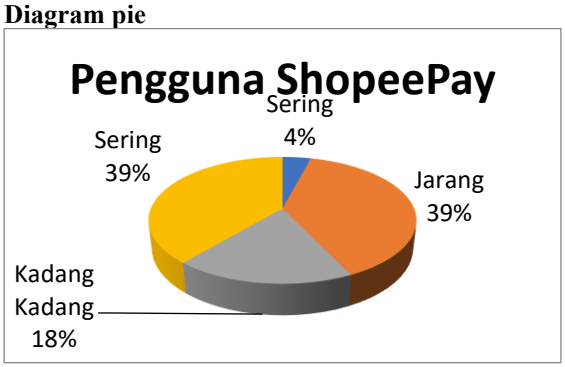
Tabel 2. Intensitas Penggunaan ShopeePay

| Jawaban | Jumlah | Persentase |
|---|---|---|
| Jarang | 19 | 52,8% |
| Kadang-kadang | 9 | 25% |
| Sangat Sering | 6 | 16,7% |
| Sering | 2 | 5,5% |

Berdasarkan tabel 2, mayoritas responden menyatakan jarang menggunakan ShopeePay untuk transaksi digital, yaitu sebanyak 52,8%. Sebanyak 25% responden menggunakan ShopeePay kadang-kadang, sedangkan 16,7% responden menggunakan ShopeePay sangat sering.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

**Diagram pie**




Gambar 2. Frekuensi Penggunaan ShopeePay oleh Responden (diagram pie)

- Sangat sering : 18%
- Sering : 4%
- Kadang-kadang : 39%
- Jarang : 39%

Berdasarkan Gambar 2, kategori "Jarang" dan "Kadang-kadang" memiliki persentase tertinggi, masing-masing sebesar 39%. Sementara itu, kategori "Sering" hanya sebesar 4%. Hasil ini menunjukkan bahwa sebagian besar responden belum menggunakan ShopeePay secara intensif dalam aktivitas sehari-hari. Kondisi tersebut dapat dipengaruhi oleh penggunaan dompet digital lain maupun perbedaan kebiasaan transaksi setiap responden.

**Variabel Keamanan Data**

Variabel keamanan data digunakan untuk mengetahui tingkat persepsi pengguna terhadap keamanan proses penarikan saldo pada aplikasi ShopeePay.

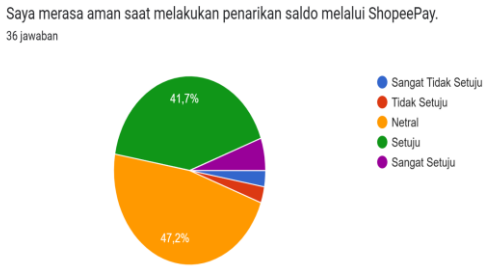
Tabel 3. Keamanan Penarikan Saldo ShopeePay

| Jawaban | Jumlah | Persentase |
|---|---|---|
| Sangat Tidak Setuju | 1 | 2,8% |
| Tidak Setuju | 1 | 2,8% |
| Netral | 17 | 47,2% |
| Setuju | 15 | 41,7% |
| Sangat Setuju | 2 | 5,5% |
| Total | **36** | **100%** |

**Analisis Tabel 3 Keamanan Penarikan Saldo ShopeePay**

Berdasarkan Tabel 3, hasil jawaban responden mengenai keamanan penarikan saldo pada ShopeePay menunjukkan bahwa sebagian besar responden memberikan tanggapan positif terhadap sistem keamanan yang diterapkan. Sebanyak 15 responden (41,7%) menyatakan setuju dan 2 responden (5,5%) menyatakan sangat setuju bahwa proses penarikan saldo ShopeePay memiliki sistem keamanan yang baik.Sementara itu, terdapat 17 responden (47,2%) yang memberikan jawaban netral. Hal ini menunjukkan bahwa masih ada pengguna yang belum sepenuhnya memahami atau merasakan secara langsung efektivitas keamanan pada proses penarikan saldo. Jawaban netral juga dapat dipengaruhi oleh kurangnya pengalaman responden terkait kendala keamanan ataupun minimnya pengetahuan mengenai fitur perlindungan akun seperti kode OTP, verifikasi identitas, dan autentikasi akun.Di sisi lain, hanya 1 responden (2,8%) yang menyatakan tidak setuju dan 1 responden (2,8%) yang menyatakan sangat tidak setuju. Persentase yang kecil ini menunjukkan bahwa sebagian besar pengguna merasa sistem keamanan ShopeePay sudah cukup mampu melindungi akun dari akses tidak sah.Hasil penelitian ini menunjukkan bahwa sistem keamanan pada proses penarikan saldo ShopeePay dinilai cukup baik oleh mahasiswa. Adanya fitur keamanan seperti One Time Password (OTP), verifikasi PIN, dan autentikasi login menjadi faktor penting dalam meningkatkan rasa aman pengguna saat melakukan transaksi digital. Namun, tingginya jawaban netral menunjukkan bahwa edukasi mengenai keamanan digital masih perlu ditingkatkan agar pengguna lebih memahami pentingnya menjaga kerahasiaan data akun dan kode verifikasi.

**Diagram Pie**




Gambar 3. Diagram Persepsi Keamanan Penarikan Saldo pada Aplikasi ShopeePay

- Netral = 47,2%
- Setuju = 41,7%
- Sangat Setuju = 5,5%
- Tidak Setuju = 2,8%
- Sangat Tidak Setuju = 2,8%

**Analisis Hasil**

Berdasarkan hasil penelitian, mayoritas responden memberikan jawaban netral terhadap keamanan penarikan saldo ShopeePay dengan persentase sebesar 47,2%. Sebanyak 41,7% responden menyatakan setuju bahwa ShopeePay aman digunakan dalam proses penarikan saldo digital.Hasil tersebut menunjukkan bahwa sebagian besar pengguna memiliki tingkat kepercayaan yang cukup baik terhadap sistem keamanan ShopeePay. Namun demikian, masih terdapat responden yang merasa ragu terhadap keamanan transaksi digital

p-ISSN : 2406-7733
e-ISSN : 2597-9922

karena adanya risiko pencurian akun dan kebocoran data pribadi.

### 4.2 Analisis Hasil Data

Hasil penelitian menunjukkan bahwa sebagian besar responden memiliki tingkat kepercayaan yang cukup baik terhadap keamanan transaksi digital ShopeePay. Hal ini terlihat dari dominasi jawaban netral dan setuju terhadap keamanan proses penarikan saldo. Namun demikian, tingginya jumlah responden yang memilih kategori **netral** menunjukkan masih adanya keraguan terhadap efektivitas perlindungan data yang diterapkan. Keraguan tersebut kemungkinan disebabkan oleh beberapa faktor, antara lain:

1. Meningkatnya kasus phishing dan pencurian OTP
   Banyak pengguna khawatir terhadap modus penipuan digital yang meminta kode verifikasi.
2. Kurangnya pemahaman keamanan digital
   Sebagian pengguna belum memahami pentingnya menjaga PIN, password, dan OTP secara rahasia.
3. Ancaman akses tidak sah terhadap akun
   Risiko seperti *login* dari perangkat asing, *malware*, atau kebocoran data dapat menyebabkan pengambilalihan akun.

Secara umum, sistem keamanan ShopeePay telah memberikan perlindungan dasar yang baik, tetapi masih diperlukan edukasi pengguna agar keamanan tersebut dapat berjalan secara optimal.

### 4.3 Pembahasan Berdasarkan Teori Keamanan Data

**a. Autentikasi (Authentication)**

Autentikasi merupakan proses verifikasi identitas pengguna sebelum sistem memberikan akses. Dalam ShopeePay, autentikasi dilakukan melalui beberapa mekanisme:

- *Username* dan *Password*
- PIN transaksi
- OTP (*One-Time Password*)

PIN digunakan sebagai lapisan keamanan utama ketika pengguna melakukan penarikan saldo, sedangkan OTP digunakan untuk memastikan bahwa transaksi benar-benar dilakukan oleh pemilik akun. Menurut teori keamanan sistem informasi, autentikasi termasuk bagian penting dalam menjaga kerahasiaan (*confidentiality*) agar data hanya dapat diakses oleh pihak yang berwenang.

**b. OTP (*One-Time Password*)**

OTP adalah kode unik yang dikirim melalui SMS atau email dan hanya berlaku untuk satu sesi transaksi. Fungsi OTP antara lain:

- Memverifikasi identitas pengguna secara *real-time*
- Mencegah akses oleh pihak yang mengetahui *password* tetapi tidak memiliki perangkat pengguna
- Menambah lapisan keamanan (*two-factor authentication*)

Walaupun efektif, OTP tetap memiliki kelemahan jika pengguna:

- Membagikan kode kepada orang lain
- Menjadi korban phishing
- Menginstal aplikasi berbahaya yang dapat membaca SMS

Karena itu, efektivitas OTP sangat bergantung pada kesadaran keamanan pengguna**.**

**c. Enkripsi Data (Data Encryption)**

Enkripsi adalah proses mengubah data menjadi bentuk kode yang tidak dapat dibaca tanpa kunci dekripsi.
Pada transaksi digital ShopeePay, enkripsi digunakan untuk:

- Melindungi data akun pengguna
- Mengamankan nomor rekening tujuan
- Menjaga informasi saldo dan histori transaksi
- Mencegah penyadapan data selama transmisi internet

Enkripsi mendukung prinsip *integrity* dan *confidentiality*, karena membantu menjaga data tetap utuh dan rahasia.

**d. Risiko Akses Tidak Sah (*Unauthorized Access*)**

Akses tidak sah adalah kondisi ketika seseorang memperoleh akses ke akun tanpa izin pemiliknya.

**Analisis Risiko Akses Tidak Sah**

Tabel 4. Beberapa risiko utama yang teridentifikasi

| Risiko | Dampak |
|---|---|
| Phishing OTP | Pengambilalihan akun |
| Password lemah | Login ilegal |
| Malware pada perangkat | Pencurian data |
| SIM Swap | Penyalahgunaan OTP |
| Kebocoran data pribadi | Identitas dicuri |

Risiko terbesar berasal dari *human error*, bukan semata-mata kelemahan sistem. Oleh karena itu, edukasi keamanan digital sangat diperlukan.

### 4.4 Kaitan dengan Kasus ShopeePay

ShopeePay sebagai dompet digital memiliki sistem keamanan yang cukup kuat melalui:

- Verifikasi OTP
- PIN transaksi
- Deteksi aktivitas mencurigakan
- *Logout* otomatis
- Notifikasi transaksi *real-time*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Namun, beberapa kasus kehilangan saldo ShopeePay di Indonesia menunjukkan bahwa ancaman terbesar sering berasal dari:

1. Pengguna memberikan OTP kepada penipu
2. Akun login pada perangkat publik
3. *Password* yang sama digunakan di banyak platform
4. Kurangnya aktivasi fitur keamanan tambahan

Hasil penelitian ini menunjukkan bahwa mahasiswa sebagai pengguna aktif teknologi masih memiliki kekhawatiran terhadap keamanan data, terutama pada proses penarikan saldo karena melibatkan akses langsung ke dana. Hal ini memperkuat teori bahwa keamanan sistem digital tidak hanya bergantung pada teknologi, tetapi juga pada perilaku pengguna**.**

## V. KESIMPULAN DAN SARAN

### 5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai analisis keamanan data pada proses penarikan saldo ShopeePay untuk mencegah akses tidak sah, dapat disimpulkan bahwa:

1. Sistem keamanan pada proses penarikan saldo ShopeePay secara umum telah memberikan perlindungan yang cukup baik terhadap data dan transaksi pengguna, yang ditunjukkan oleh mayoritas responden memberikan tanggapan netral (47,2%) dan setuju (41,7%) terhadap keamanan layanan tersebut.
2. Mekanisme keamanan seperti penggunaan PIN, password, OTP (*One-Time Password*), dan autentikasi berlapis berperan dalam mendukung pencegahan akses tidak sah serta meningkatkan keamanan transaksi digital.
3. Penerapan enkripsi data menjadi salah satu komponen penting dalam menjaga kerahasiaan dan integritas informasi pengguna selama proses transaksi digital berlangsung.
4. Hasil penelitian menunjukkan bahwa masih terdapat kekhawatiran pengguna terhadap berbagai risiko keamanan, seperti phishing, pencurian OTP, penggunaan password yang lemah, malware, dan kebocoran data pribadi yang berpotensi menyebabkan akses tidak sah.
5. Keamanan data pada proses penarikan saldo ShopeePay tidak hanya dipengaruhi oleh mekanisme keamanan yang diterapkan oleh sistem, tetapi juga oleh perilaku dan tingkat kesadaran pengguna dalam menjaga keamanan akun dan informasi pribadinya.
6. Tujuan penelitian untuk menganalisis keamanan data pada proses penarikan saldo ShopeePay dalam upaya mencegah akses tidak sah telah tercapai, dengan menunjukkan bahwa efektivitas keamanan layanan dipengaruhi oleh kombinasi antara penerapan teknologi keamanan dan kesadaran pengguna.

### 5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat diberikan adalah sebagai berikut:

1. Pengguna ShopeePay diharapkan dapat meningkatkan kesadaran terhadap keamanan digital dengan menjaga kerahasiaan PIN, password, dan kode OTP serta lebih berhati-hati terhadap berbagai bentuk penipuan digital.
2. Pihak penyedia layanan ShopeePay diharapkan terus meningkatkan mekanisme keamanan dan memberikan edukasi kepada pengguna mengenai pentingnya menjaga keamanan akun serta data pribadi.
3. Penelitian selanjutnya disarankan untuk menggunakan jumlah responden yang lebih banyak dan melibatkan populasi yang lebih beragam sehingga hasil penelitian dapat memberikan gambaran yang lebih luas mengenai keamanan layanan dompet digital.
4. Penelitian berikutnya dapat mengembangkan kajian pada aspek keamanan transaksi digital lainnya, seperti efektivitas autentikasi multifaktor, perlindungan data pribadi, dan faktor perilaku pengguna dalam mencegah akses tidak sah pada layanan dompet digital.

## DAFTAR PUSTAKA

Afrilia, V., Zulaihati, S., & Kismayanti Respati, D. (2025). Ekopedia : Jurnal Ilmiah Ekonomi. *Jurnal Ilmiah Ekonomi*, *1*(2), 450–458.

Amalina, D., Jaelani, E., & Rosidin, U. (2021). Legal Protection of Personal Data of Shopeepay Later Loan Users. *Antara*, *2*(1), 25–30. https://doi.org/10.15575/vh.v6i1.26742

Candra, stefanie fortuna, & Irmeilyana. (2024). Jurnal Penelitian Sains. *Jurnal Penelitian Sains*, *26*(1), 30–39. https://doi.org/10.23917/saintek.v2i1.13562

Cao, L., Yang, Q., & Yu, P. S. (2021). Data science and AI in FinTech: an overview. *International Journal of Data Science and Analytics*, *12*(2), 81–99. https://doi.org/10.1007/s41060-021-00278-w

Dan, D., Di, S., & Tangerang, K. (2026). Analisis Persepsi Keamanan Data Dan Kepuasan Pelanggan Terhadap Penggunaan Dompet Digital. *15*, 2340–2351. https://doi.org/10.34127/jrlab.v15i2.2168

Didin, D. (2025). The Effect of Brand Awareness and Perceived Quality on User Loyalty Through Satisfaction as a Mediating Variable. *Journal Research of Social Science, Economics, and Management*, *5*(3), 34–50. https://doi.org/10.59141/jrssem.v5i3.1157

Fauziah, N. F., & Retnoningsih, E. (2020). *Sistem*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

*Informasi Penelitian dan Pengabdian kepada Masyarakat Berbasis Web*. *4*(2), 183–192.

Febriani, D. S., Safitri, E. M., & Wulansari, A. (2025). Pengguna Fintech Paylater Pada Aplikasi Shopeepay Menggunakan Utaut2. *ILTEK : Jurnal Teknologi*, *20*(1), 82–90.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 1–42. https://doi.org/10.1016/j.eswa.2023.122697

Mulyani, S. (2024). Pengaruh E- Security Dan Service Quality Terhadap Ecustomer Loyalty Dengan Kepuasan Pelanggan Aplikasi Dana Sebagai Variabel Moderasi Ditinjau Dalam Perspektif Etika Bisnis Islam (Vol. 1).

Nizatsary, R. N., Seta, H. B., & Wahyono, B. T. (2022). Penerapan Keamanan Data Siswa Menggunakan International Data Encryption Algorithm (Idea) Dan Rivest Shamir Adleman (Rsa). *Informatik : Jurnal Ilmu Komputer*, *18*(2), 152. https://doi.org/10.52958/iftk.v18i2.4665

Ovo, K., & Dana, S. (2021). *Analisis Keamanan Aplikasi Fintech di Indonesia : Studi*. *2*(1), 177–186.

Prena, G. Das, & Dewi, N. K. S. G. (2023). Pengaruh Kemudahan Penggunaan, Gaya Hidup, Persepsi Keamanan Dan Kepercayaan Terhadap Minat Menggunakan Shopeepay. *WACANA EKONOMI (Jurnal Ekonomi, Bisnis Dan Akuntansi)*, *22*(2), 142–155. https://doi.org/10.22225/we.22.2.2023.142-155

Ramadya Sari, L., Anggraini, R., Sri Kencanawati, M., & Sularto, L. (2022). Dampak Keamanan, Manfaat, Kepercayaan, Promosi, serta Kemudahan pada Keputusan Pemanfaatan Dompet Elektronik Shopeepay. *Metik Jurnal*, *6*(1), 59–69. https://doi.org/10.47002/metik.v6i1.335

Trout, J. E., & Betts, C. P. (1988). Security Engineering. *Military Engineer*, *80*(522), 368–371. https://doi.org/10.4018/978-1-59140-911-3.ch011

Zikri, M., Hakim, A., Simatupang, R. A., Uhur, M., & Saragih, A. (2026). *Analisis Kepuasan dan Loyalitas Pengguna ShopeePay di Indonesia*. *2*(1), 82–89.