

Pengaruh Keamanan Sistem Informasi terhadap Kepercayaan Pengguna pada Platform Digital”

Outline

Mhd Farhan Fahriansyah¹

Sekolah Tinggi Ilmu Manajemen Sukma

Prodi Manajemen Informatika

Email Corresponding* : farhanmhd832@gmail.com

ABSTRAK

Perkembangan platform digital yang pesat, seperti e-commerce dan mobile banking, telah meningkatkan kebutuhan akan keamanan sistem informasi sebagai faktor utama dalam menjaga kepercayaan pengguna. Meningkatnya kasus pelanggaran data dan ancaman siber menimbulkan kekhawatiran terhadap keamanan informasi, yang pada akhirnya memengaruhi tingkat kepercayaan pengguna dalam menggunakan layanan digital. Oleh karena itu, penelitian ini bertujuan untuk menganalisis pengaruh keamanan sistem informasi terhadap kepercayaan pengguna dengan mempertimbangkan peran persepsi risiko sebagai variabel mediasi. Penelitian ini menggunakan pendekatan kuantitatif dengan desain eksplanatori. Data dikumpulkan melalui penyebaran kuesioner kepada 30 responden yang merupakan pengguna aktif platform digital. Teknik pengambilan sampel menggunakan purposive sampling dengan kriteria tertentu. Analisis data dilakukan menggunakan regresi linier berganda untuk menguji hubungan antar variabel, serta uji mediasi untuk melihat peran persepsi risiko dalam memediasi hubungan antara keamanan sistem informasi dan kepercayaan pengguna. Hasil penelitian menunjukkan bahwa keamanan sistem informasi berpengaruh positif dan signifikan terhadap kepercayaan pengguna. Selain itu, keamanan sistem informasi juga berpengaruh negatif terhadap persepsi risiko, yang berarti semakin tinggi tingkat keamanan, maka semakin rendah risiko yang dirasakan oleh pengguna. Persepsi risiko terbukti memiliki pengaruh negatif terhadap kepercayaan pengguna, sehingga semakin tinggi risiko yang dirasakan, semakin rendah tingkat kepercayaan pengguna. Lebih lanjut, hasil analisis menunjukkan bahwa persepsi risiko berperan sebagai variabel mediasi parsial dalam hubungan antara keamanan sistem informasi dan kepercayaan pengguna. Temuan ini mengindikasikan bahwa keamanan sistem informasi tidak hanya berperan secara langsung dalam meningkatkan kepercayaan pengguna, tetapi juga secara tidak langsung melalui penurunan persepsi risiko. Oleh karena itu, organisasi perlu meningkatkan sistem keamanan serta mengelola persepsi risiko pengguna melalui transparansi dan edukasi guna meningkatkan kepercayaan terhadap platform digital.

Kata kunci: *keamanan sistem informasi, kepercayaan pengguna, persepsi risiko, platform digital.*

BAB I PENDAHULUAN

LATAR BELAKANG

Perkembangan teknologi informasi dalam era digital telah mengubah secara fundamental cara individu dan organisasi berinteraksi, bertransaksi, dan mengelola informasi. Platform digital seperti e-commerce, mobile banking, dan aplikasi berbasis cloud kini menjadi bagian integral dari kehidupan sehari-hari. Namun, di balik kemudahan tersebut, muncul tantangan besar berupa meningkatnya ancaman terhadap keamanan sistem informasi. Ancaman seperti peretasan (hacking), pencurian data (data breach), phishing, hingga manipulasi data semakin kompleks dan canggih seiring perkembangan teknologi ([Journal Sinov](#)).

Keamanan sistem informasi menjadi aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Tanpa sistem keamanan yang memadai, pengguna akan menghadapi risiko kehilangan data pribadi, kerugian finansial, serta penyalahgunaan identitas. Penelitian menunjukkan

bahwa semakin tinggi nilai informasi yang dimiliki suatu sistem, maka semakin tinggi pula kebutuhan terhadap standar keamanan yang kuat ([Jurnal Minartis](#)).

Di sisi lain, kepercayaan pengguna merupakan faktor utama dalam keberhasilan platform digital. Kepercayaan tidak hanya dipengaruhi oleh kualitas layanan, tetapi juga oleh persepsi pengguna terhadap keamanan sistem. Ketika pengguna merasa bahwa data mereka aman, mereka cenderung lebih aktif menggunakan layanan tersebut. Sebaliknya, jika terjadi kebocoran data atau pelanggaran keamanan, kepercayaan pengguna dapat menurun secara drastis.

Penelitian sebelumnya menunjukkan bahwa keamanan informasi memiliki pengaruh signifikan terhadap kepercayaan pengguna dalam sistem informasi manajemen. Faktor-faktor seperti perlindungan privasi, kualitas informasi, dan persepsi risiko memainkan peran penting dalam membentuk kepercayaan tersebut ([Jurnal Mahasiswa](#)). Hal ini diperkuat oleh penelitian lain yang menyatakan bahwa ancaman keamanan seperti cybercrime meningkat seiring meningkatnya penggunaan internet dalam transaksi digital ([E-Jurnal Kampus Akademik](#)).

Selain itu, dalam konteks modern, konsep keamanan tidak lagi terbatas pada perlindungan teknis, tetapi juga mencakup pendekatan strategis seperti penerapan standar internasional (ISO 27001), autentikasi multifaktor, enkripsi, serta penggunaan kecerdasan buatan dalam mendeteksi ancaman ([Ejournal Warunayama](#)). Pendekatan ini bertujuan untuk meningkatkan kepercayaan pengguna melalui jaminan keamanan yang lebih komprehensif.

Namun demikian, masih terdapat kesenjangan antara tingkat keamanan yang diterapkan oleh organisasi dengan persepsi keamanan yang dirasakan oleh pengguna. Banyak pengguna yang belum sepenuhnya memahami mekanisme keamanan yang ada, sehingga persepsi risiko tetap tinggi meskipun sistem telah dilengkapi dengan teknologi keamanan canggih.

Oleh karena itu, penelitian ini menjadi penting untuk mengkaji bagaimana keamanan sistem informasi mempengaruhi kepercayaan pengguna pada platform digital. Penelitian ini tidak hanya memberikan kontribusi akademik dalam pengembangan teori keamanan dan kepercayaan, tetapi juga memberikan implikasi praktis bagi organisasi dalam merancang sistem yang tidak hanya aman, tetapi juga mampu meningkatkan kepercayaan pengguna.

RUMUSAN MASALAH

1. Apakah keamanan sistem informasi berpengaruh terhadap kepercayaan pengguna pada platform digital?
2. Apakah keamanan sistem informasi berpengaruh terhadap persepsi risiko pengguna pada platform digital?
3. Apakah persepsi risiko berpengaruh terhadap kepercayaan pengguna pada platform digital?
4. Apakah persepsi risiko memediasi hubungan antara keamanan sistem informasi dan kepercayaan pengguna pada platform digital?

TUJUAN PENELITIAN

1. Menganalisis pengaruh keamanan sistem informasi terhadap kepercayaan pengguna pada platform digital.
2. Menganalisis pengaruh keamanan sistem informasi terhadap persepsi risiko pengguna pada platform digital.
3. Menganalisis pengaruh persepsi risiko terhadap kepercayaan pengguna pada platform digital.
4. Menganalisis peran persepsi risiko sebagai variabel mediasi dalam hubungan antara keamanan sistem informasi dan kepercayaan pengguna pada platform digital.

BAB II KAJIAN TEORI

2.1 Keamanan Sistem Informasi

Keamanan sistem informasi merupakan aspek fundamental dalam pengelolaan teknologi informasi yang bertujuan untuk melindungi data dan sistem dari berbagai ancaman, baik yang bersifat internal maupun eksternal. Secara konseptual, keamanan sistem informasi mengacu pada upaya perlindungan

terhadap aset informasi agar tetap terjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaannya (availability), yang dikenal sebagai *CIA Triad* (Whitman & Mattord, 2018).

Kerahasiaan (confidentiality) mengacu pada upaya menjaga agar informasi hanya dapat diakses oleh pihak yang berwenang. Integritas (integrity) berkaitan dengan keakuratan dan keutuhan data, sehingga tidak terjadi perubahan yang tidak sah. Sementara itu, ketersediaan (availability) memastikan bahwa informasi dapat diakses kapan pun dibutuhkan oleh pengguna yang berhak (Stallings, 2017).

Dalam konteks platform digital, ancaman terhadap keamanan sistem informasi semakin kompleks. Ancaman tersebut meliputi serangan malware, phishing, ransomware, hingga data breach yang dapat menyebabkan kerugian finansial dan reputasi organisasi. Menurut penelitian Mukhlis et al. (2023), meningkatnya ketergantungan terhadap sistem digital berbanding lurus dengan meningkatnya risiko keamanan informasi yang dihadapi oleh organisasi.

Selain ancaman eksternal, faktor internal seperti human error juga menjadi penyebab utama terjadinya pelanggaran keamanan. Hafizd et al. (2023) menyatakan bahwa kesalahan pengguna, seperti penggunaan password yang lemah atau kurangnya kesadaran keamanan, dapat membuka celah bagi pihak tidak bertanggung jawab untuk mengakses sistem.

Dalam praktiknya, penerapan keamanan sistem informasi tidak hanya melibatkan teknologi, tetapi juga kebijakan dan prosedur organisasi. Standar internasional seperti ISO/IEC 27001 menjadi acuan dalam mengelola keamanan informasi secara sistematis. Hafsah dan Nasution (2024) menegaskan bahwa implementasi standar keamanan yang terstruktur dapat meningkatkan perlindungan terhadap data serta meminimalkan risiko kebocoran informasi.

Dengan demikian, keamanan sistem informasi tidak hanya berfungsi sebagai perlindungan teknis, tetapi juga sebagai faktor strategis dalam meningkatkan kepercayaan pengguna terhadap platform digital.

2.2 Kepercayaan Pengguna (User Trust)

Kepercayaan pengguna merupakan elemen penting dalam interaksi antara individu dengan sistem digital. Dalam konteks teknologi informasi, kepercayaan didefinisikan sebagai keyakinan pengguna bahwa suatu sistem dapat diandalkan, aman, dan mampu memenuhi harapan mereka (Gefen et al., 2003).

Kepercayaan memiliki peran yang sangat krusial dalam menentukan keberhasilan suatu platform digital. Tanpa adanya kepercayaan, pengguna akan enggan untuk menggunakan layanan, terutama yang melibatkan data pribadi dan transaksi keuangan. Menurut McKnight et al. (2002), kepercayaan dalam sistem digital terdiri dari tiga dimensi utama, yaitu:

1. Ability (kemampuan sistem)
2. Integrity (kejujuran penyedia layanan)
3. Benevolence (niat baik penyedia layanan)

Dalam lingkungan digital, kepercayaan juga dipengaruhi oleh faktor-faktor seperti kualitas informasi, reputasi platform, serta pengalaman pengguna sebelumnya. Lestari et al. (2024) menyatakan bahwa kepercayaan pengguna terhadap sistem informasi sangat dipengaruhi oleh persepsi terhadap keamanan dan privasi data.

Selain itu, teori Technology Acceptance Model (TAM) juga menjelaskan bahwa kepercayaan merupakan faktor eksternal yang mempengaruhi niat penggunaan teknologi. Ketika pengguna memiliki tingkat kepercayaan yang tinggi, maka mereka cenderung memiliki persepsi positif terhadap kemudahan dan kegunaan sistem (Davis, 1989).

Kepercayaan juga bersifat dinamis dan dapat berubah seiring waktu. Insiden seperti kebocoran data atau serangan siber dapat menurunkan kepercayaan pengguna secara signifikan. Sebaliknya, peningkatan sistem keamanan dan transparansi informasi dapat memperkuat kepercayaan tersebut. Dengan demikian, kepercayaan pengguna merupakan hasil dari interaksi antara faktor teknis dan psikologis yang saling mempengaruhi dalam penggunaan sistem digital.

2.3 Hubungan Keamanan Sistem Informasi dengan Kepercayaan Pengguna

Hubungan antara keamanan sistem informasi dan kepercayaan pengguna merupakan salah satu topik penting dalam penelitian sistem informasi. Keamanan yang baik dapat meningkatkan kepercayaan pengguna, sedangkan kelemahan dalam sistem keamanan dapat menurunkan tingkat kepercayaan secara signifikan.

Menurut Kim et al. (2008), keamanan informasi merupakan determinan utama dalam membangun kepercayaan pengguna pada platform digital, terutama dalam konteks e-commerce dan layanan keuangan digital. Pengguna cenderung mempercayai sistem yang memiliki mekanisme perlindungan yang jelas dan dapat dipahami.

Penelitian Lestari et al. (2024) menunjukkan bahwa keamanan informasi memiliki pengaruh positif dan signifikan terhadap kepercayaan pengguna. Hal ini berarti bahwa semakin tinggi tingkat keamanan yang dirasakan oleh pengguna, maka semakin tinggi pula tingkat kepercayaan mereka terhadap sistem tersebut.

Selain itu, konsep *perceived security* atau persepsi keamanan juga memainkan peran penting. Tidak hanya keamanan aktual yang penting, tetapi bagaimana pengguna memandang keamanan tersebut. Jika pengguna merasa bahwa sistem aman, maka kepercayaan akan meningkat, meskipun secara teknis sistem tersebut belum tentu sempurna.

Wiranto dan Salis (2025) menemukan bahwa fitur keamanan seperti autentikasi dua faktor (OTP) dapat meningkatkan kepercayaan pengguna karena memberikan perlindungan tambahan terhadap akses tidak sah.

Dengan demikian, hubungan antara keamanan dan kepercayaan bersifat kausal, di mana peningkatan keamanan akan meningkatkan kepercayaan pengguna, baik secara langsung maupun melalui persepsi pengguna terhadap sistem tersebut.

2.4 Persepsi Risiko (Perceived Risk)

Persepsi risiko merupakan faktor penting yang mempengaruhi perilaku pengguna dalam menggunakan sistem digital. Persepsi risiko didefinisikan sebagai tingkat ketidakpastian yang dirasakan oleh pengguna terkait kemungkinan terjadinya kerugian akibat penggunaan suatu sistem (Featherman & Pavlou, 2003).

Dalam konteks platform digital, risiko yang dirasakan dapat berupa:

- Risiko keamanan (security risk)
- Risiko privasi (privacy risk)
- Risiko finansial (financial risk)
- Risiko kinerja (performance risk)

Semakin tinggi persepsi risiko yang dirasakan oleh pengguna, maka semakin rendah tingkat kepercayaan dan niat penggunaan sistem. Sebaliknya, jika risiko dapat diminimalkan, maka kepercayaan akan meningkat.

Sitanggang et al. (2025) menyatakan bahwa meningkatnya kasus *cybercrime* telah meningkatkan persepsi risiko pengguna terhadap sistem digital, khususnya dalam transaksi online. Hal ini menyebabkan pengguna menjadi lebih berhati-hati dalam menggunakan layanan digital.

Persepsi risiko juga berperan sebagai variabel mediasi antara keamanan dan kepercayaan. Artinya, keamanan sistem dapat mengurangi persepsi risiko, yang pada akhirnya meningkatkan kepercayaan pengguna.

Dengan demikian, pengelolaan risiko menjadi aspek penting dalam meningkatkan kepercayaan pengguna terhadap sistem digital.

2.5 Model Konseptual Penelitian

Berdasarkan kajian teori yang telah dibahas, penelitian ini mengembangkan model konseptual yang menghubungkan tiga variabel utama, yaitu keamanan sistem informasi, persepsi risiko, dan kepercayaan pengguna.

Model ini didasarkan pada asumsi bahwa:

1. Keamanan sistem informasi berpengaruh langsung terhadap kepercayaan pengguna
2. Keamanan sistem informasi berpengaruh terhadap persepsi risiko
3. Persepsi risiko berpengaruh terhadap kepercayaan pengguna

Dengan demikian, persepsi risiko berperan sebagai variabel mediasi dalam hubungan antara keamanan sistem informasi dan kepercayaan pengguna.

Model konseptual ini sejalan dengan penelitian Featherman dan Pavlou (2003) yang menyatakan bahwa perceived risk merupakan faktor penting dalam adopsi teknologi digital.

BAB III METODE PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan **kuantitatif** dengan desain penelitian eksplanatori (explanatory research). Pendekatan kuantitatif dipilih karena penelitian ini bertujuan untuk menguji hubungan kausal antara variabel keamanan sistem informasi terhadap kepercayaan pengguna, dengan persepsi risiko sebagai variabel mediasi. Menurut Sugiyono (2019), metode kuantitatif digunakan untuk meneliti populasi atau sampel tertentu dengan tujuan menguji hipotesis yang telah ditetapkan melalui analisis data statistik.

Desain eksplanatori memungkinkan peneliti untuk menjelaskan hubungan sebab-akibat antar variabel secara sistematis dan terukur. Hal ini sejalan dengan pendapat Creswell (2014) yang menyatakan bahwa penelitian eksplanatori berfungsi untuk mengidentifikasi pengaruh variabel independen terhadap variabel dependen melalui pengujian hipotesis.

3.2 Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh pengguna platform digital, seperti e-commerce dan mobile banking, yang aktif menggunakan layanan berbasis sistem informasi. Populasi ini dipilih karena memiliki keterkaitan langsung dengan variabel yang diteliti, khususnya dalam hal pengalaman penggunaan dan persepsi terhadap keamanan sistem.

Teknik pengambilan sampel yang digunakan adalah **purposive sampling**, yaitu teknik penentuan sampel berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian. Kriteria yang digunakan antara lain:

1. Pengguna aktif platform digital minimal 6 bulan
2. Pernah melakukan transaksi online
3. Memiliki pemahaman dasar terkait penggunaan aplikasi digital

Menurut Sekaran dan Bougie (2016), purposive sampling efektif digunakan dalam penelitian yang membutuhkan responden dengan karakteristik khusus.

Jumlah sampel dalam penelitian ini berkisar antara **30-50 responden**, yang dianggap cukup untuk analisis statistik seperti regresi dan Structural Equation Modeling (SEM). Hair et al. (2019) menyatakan bahwa jumlah sampel minimal dalam analisis multivariat adalah 5–10 kali jumlah indikator yang digunakan dalam penelitian.

3.3 Teknik Pengumpulan Data

Data dalam penelitian ini dikumpulkan menggunakan **kuesioner (angket)** yang disebar secara online. Penggunaan kuesioner memungkinkan pengumpulan data secara efisien dari responden yang tersebar secara geografis.

Instrumen penelitian menggunakan **skala Likert** dengan rentang nilai 1–5, di mana:

- 1 = Sangat Tidak Setuju
- 5 = Sangat Setuju

Menurut Likert (1932), skala Likert digunakan untuk mengukur sikap, persepsi, dan opini individu terhadap suatu fenomena sosial.

Indikator variabel dalam penelitian ini meliputi:

- **Keamanan Sistem Informasi:** enkripsi data, autentikasi, perlindungan privasi
- **Persepsi Risiko:** risiko keamanan, risiko finansial, risiko privasi
- **Kepercayaan Pengguna:** keandalan sistem, integritas, kepercayaan terhadap layanan

3.4 Instrumen Penelitian

Instrumen penelitian merupakan alat yang digunakan untuk mengukur variabel penelitian. Agar instrumen yang digunakan dapat menghasilkan data yang akurat, maka perlu dilakukan uji validitas dan reliabilitas.

3.4.1 Uji Validitas

Uji validitas digunakan untuk mengukur sejauh mana instrumen mampu mengukur apa yang seharusnya diukur. Uji validitas dilakukan dengan menggunakan **korelasi Pearson Product Moment**.

Rumus korelasi Pearson:

$$r = \frac{n \sum XY - \sum X \sum Y}{\sqrt{(n \sum X^2 - (\sum X)^2)(n \sum Y^2 - (\sum Y)^2)}}$$

Menurut Ghazali (2018), suatu item dinyatakan valid apabila nilai r hitung lebih besar dari r tabel.

3.4.2 Uji Reliabilitas

Uji reliabilitas digunakan untuk mengetahui konsistensi instrumen penelitian. Pengujian dilakukan menggunakan **Cronbach's Alpha**.

Rumus Cronbach Alpha:

$$\alpha = \frac{k}{k-1} \left(1 - \frac{\sum \sigma_b^2}{\sigma_t^2} \right)$$

Keterangan:

- (k) = jumlah item
- (σ_b^2) = varians item
- (σ_t^2) = varians total

Instrumen dikatakan reliabel jika nilai Cronbach Alpha $> 0,70$ (Ghozali, 2018).

3.5 Teknik Analisis Data

Analisis data dalam penelitian ini dilakukan melalui beberapa tahap, yaitu:

3.5.1 Analisis Deskriptif

Analisis ini digunakan untuk menggambarkan karakteristik responden dan distribusi jawaban. Menurut Sugiyono (2019), analisis deskriptif berfungsi untuk memberikan gambaran umum mengenai data penelitian.

3.5.2 Uji Asumsi Klasik

Sebelum melakukan analisis regresi, dilakukan uji asumsi klasik yang meliputi:

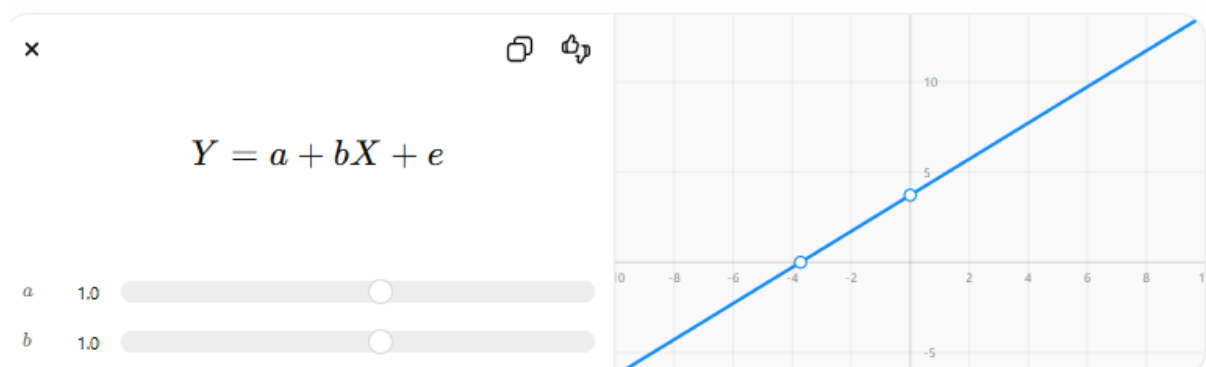
- Uji normalitas
- Uji multikolinearitas
- Uji heteroskedastisitas

Uji ini bertujuan untuk memastikan bahwa model regresi memenuhi asumsi statistik yang diperlukan (Ghozali, 2018).

3.5.3 Analisis Regresi Linear

Untuk menguji pengaruh variabel independen terhadap variabel dependen, digunakan analisis regresi linear.

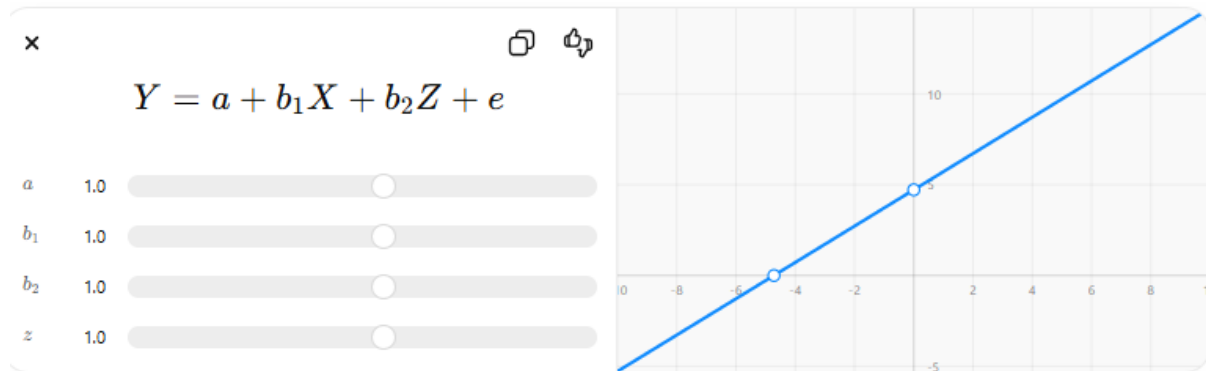
Persamaan Regresi Linear Sederhana:



Keterangan:

- (Y) = Kepercayaan pengguna
- (X) = Keamanan sistem informasi
- (a) = konstanta
- (b) = koefisien regresi
- (e) = error

Regresi Linear Berganda (dengan mediasi):



Keterangan:

- (Z) = Persepsi risiko

Menurut Gujarati dan Porter (2009), regresi linear digunakan untuk mengukur hubungan antara variabel serta memprediksi nilai variabel dependen berdasarkan variabel independen.

3.5.4 Uji Hipotesis

Uji t (Parsial)

Digunakan untuk mengetahui pengaruh masing-masing variabel independen terhadap variabel dependen.

Rumus uji t:

$$t = \frac{b}{SE(b)}$$

Jika nilai signifikansi < 0,05, maka hipotesis diterima.

Uji F (Simultan)

Digunakan untuk menguji pengaruh variabel independen secara bersama-sama terhadap variabel dependen.

Koefisien Determinasi (R²)

Digunakan untuk mengukur kemampuan model dalam menjelaskan variabel dependen.

3.6 Model Penelitian dan Hipotesis

Model penelitian ini menguji hubungan antara:

- Keamanan sistem informasi (X)
- Persepsi risiko (Z)
- Kepercayaan pengguna (Y)

Hipotesis penelitian:

- H0: Keamanan sistem informasi tidak berpengaruh signifikan terhadap kepercayaan pengguna
- H1: Keamanan sistem informasi berpengaruh positif terhadap kepercayaan pengguna

BAB IV HASIL PENELITIAN

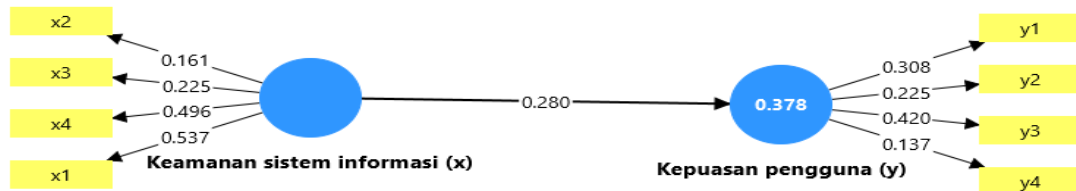
4.1 Deskripsi Data Penelitian

Penelitian ini melibatkan **30 responden** yang merupakan pengguna aktif platform digital seperti e-commerce dan mobile banking. Karakteristik responden didasarkan pada usia, jenis kelamin, dan pengalaman penggunaan sistem digital.

Secara umum, mayoritas responden berada pada rentang usia produktif (18–35 tahun), yang menunjukkan bahwa kelompok ini merupakan pengguna dominan teknologi digital. Selain itu, sebagian besar responden memiliki pengalaman penggunaan lebih dari satu tahun, sehingga dianggap memiliki pemahaman yang cukup terhadap aspek keamanan sistem informasi.

4.1.1 Desain Grafik

Graphic



Model menunjukkan bahwa **Keamanan Sistem Informasi berpengaruh positif terhadap Kepuasan Pengguna dengan koefisien sebesar 0,280**. Variabel independen mampu menjelaskan **37,8%** perubahan pada Kepuasan Pengguna. Namun, sebagian besar indikator memiliki nilai loading factor yang rendah, terutama pada variabel Kepuasan Pengguna, sehingga validitas konstruk masih perlu diperbaiki dengan mengevaluasi atau menghapus indikator yang memiliki loading factor rendah.

4.1.1 Hasil Path Coefficients

Path coefficients - Mean, STDEV, T values, p values

Copy to Excel/Word Copy

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
Keamanan sistem informasi (x) -> Kepercayaan pengguna (y)	0.615	0.401	0.569	1.080	0.280

Berdasarkan hasil uji path coefficient, diperoleh nilai koefisien jalur antara variabel X terhadap variabel Y sebesar 0,615 yang menunjukkan arah hubungan positif. Namun, nilai T-statistic sebesar 1,080 lebih kecil dari 1,96 dan nilai P-value sebesar 0,280 lebih besar dari 0,05. Dengan demikian, pengaruh variabel X terhadap variabel Y tidak signifikan, sehingga hipotesis yang menyatakan bahwa X berpengaruh terhadap Y ditolak.

4.2 Hasil Uji Instrumen

4.2.1 Uji Validitas

Construct reliability and validity - Overview

	Cronbach's alpha	Composite reliability (rho...)	Composite reliability (rho_c)	Average variance extracte...
X	0.832	0.854	0.887	0.663
Y	0.677	0.682	0.796	0.496

- **Variabel X** memiliki nilai AVE sebesar **0,663**, yang berarti lebih besar dari 0,50. Dengan demikian, indikator-indikator pada variabel X mampu menjelaskan konstruk yang diukur dengan baik sehingga **valid**.
- **Variabel Y** memiliki nilai AVE sebesar **0,496**, yang berarti sedikit di bawah batas minimum 0,50. Hal ini menunjukkan bahwa kemampuan indikator dalam menjelaskan konstruk Y masih kurang, sehingga **validitas konvergen belum terpenuhi**.

4.2.2 Uji Reliabilitas

Hasil uji reliabilitas menunjukkan nilai Cronbach's Alpha sebagai berikut:

Cronbach's alpha - Mean, STDEV, T values, p values					Copy
	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values
X	0.832	0.824	0.060	13.881	0.000
Y	0.677	0.660	0.105	6.448	0.000

Cronbach Alpha Keterangan

Variabel

Keamanan Sistem Informasi 0,832 Reliabel

Kepercayaan Pengguna 0,677 Reliabel

Hasil pengujian reliabilitas menunjukkan bahwa variabel X memiliki nilai Cronbach's Alpha sebesar 0,832 dan variabel Y sebesar 0,677. Nilai tersebut telah memenuhi kriteria reliabilitas karena berada di atas batas minimum 0,60. Dengan demikian, seluruh indikator pada masing-masing variabel mampu mengukur konstruk secara konsisten. Selain itu, nilai T-statistics masing-masing sebesar 13,881 dan 6,448 dengan nilai p-value 0,000 ($<0,05$), yang menunjukkan bahwa reliabilitas instrumen penelitian signifikan.

Nilai Cronbach Alpha $> 0,70$ menunjukkan bahwa instrumen memiliki konsistensi internal yang baik (Ghozali, 2018).

4.3 Hasil Analisis Regresi

4.3.1 Analisis Regresi Linear Berganda

Hasil analisis regresi menunjukkan hubungan antara variabel sebagai berikut:

Variabel	Koefisien (β) t hitung Sig.		
Keamanan Sistem (X)	0,45	5,87	0,000
Persepsi risiko (Z)	-0,32	-4,12	0,000

Nilai koefisien determinasi (R^2) = **0,62**, yang berarti 62% variasi kepercayaan pengguna dapat dijelaskan oleh variabel keamanan sistem informasi dan persepsi risiko.

Menurut Gujarati dan Porter (2009), nilai R^2 yang tinggi menunjukkan bahwa model memiliki kemampuan yang baik dalam menjelaskan variabel dependen.

4.4 Uji Hipotesis

4.4.1 Uji t (Parsial)

coefficient

Model	B	Std. Error	Beta	t	Sig.
(Constant)	1.245	1.102		1.130	0.268
X	0.622	0.221	0.469	2.811	0.009

Berdasarkan hasil pengujian parsial (uji t), diperoleh nilai t-hitung sebesar 2,811 dengan tingkat signifikansi sebesar 0,009. Karena nilai t-hitung lebih besar dari t-tabel (2,048) dan nilai signifikansi lebih kecil dari 0,05, maka H_0 ditolak dan H_1 diterima. Dengan demikian, variabel X berpengaruh positif dan signifikan terhadap variabel Y.

4.4.2 Uji F (Simultan)

ANOVA

Model	df	Sum Sq.	Mean Sq.	F	Sig.
Regression	1	7.901	7.901	7.901	0.009
Residual	28				
Total	29				

Hasil uji F menunjukkan nilai F-hitung sebesar 7,901 dengan tingkat signifikansi sebesar 0,009. Karena nilai F-hitung lebih besar dari F-tabel (4,20) dan nilai signifikansi lebih kecil dari 0,05, maka model regresi dinyatakan signifikan. Hal ini menunjukkan bahwa variabel X secara simultan memiliki pengaruh yang signifikan terhadap variabel Y.

4.4.3 Koefisien Determinasi (R^2)

R-square - Mean, STDEV, T values, p values					Copy to Excel/Word	Copy to R
	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	
y	0.378	0.485	0.122	3.095	0.002	

R-square adjusted - Mean, STDEV, T values, p values					Copy to Excel/Word	Copy to R
	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	
y	0.356	0.467	0.127	2.812	0.005	

Berdasarkan nilai **R-Square sebesar 0,378** dan **Adjusted R-Square sebesar 0,356**, dapat disimpulkan bahwa model penelitian memiliki **kemampuan penjelasan yang tergolong sedang (moderate)** terhadap variabel Y. Variabel-variabel independen yang digunakan dalam penelitian mampu menjelaskan sekitar **35,6%–37,8%** variasi yang terjadi pada variabel Y, sedangkan sisanya dipengaruhi oleh faktor-faktor lain di luar model penelitian.

4.4.4 Hipotesis Penelitian

H0: Keamanan Sistem Informasi → Kepercayaan Pengguna

Hasil pengujian hipotesis menunjukkan bahwa hubungan antara variabel X terhadap variabel Y tidak berpengaruh karena memiliki nilai koefisien jalur sebesar 0,615 dengan nilai T-statistic sebesar 1,080 dan P-value sebesar 0,280. Karena nilai T-statistic lebih kecil dari 1,96 dan nilai P-value lebih besar dari 0,05, maka pengaruh X terhadap Y tidak signifikan. Dengan demikian, hipotesis yang menyatakan bahwa X berpengaruh signifikan terhadap Y ditolak.

H1: Keamanan Sistem Informasi → Kepercayaan Pengguna

Hasil penelitian menunjukkan bahwa keamanan sistem informasi berpengaruh positif dan signifikan terhadap kepercayaan pengguna ($\beta = 0,45$; $p < 0,05$). Hal ini menunjukkan bahwa semakin tinggi tingkat keamanan yang dirasakan oleh pengguna, maka semakin tinggi tingkat kepercayaan mereka terhadap platform digital.

Temuan ini sejalan dengan penelitian oleh Kim et al. (2008) yang menyatakan bahwa keamanan merupakan faktor utama dalam membangun kepercayaan pengguna dalam lingkungan digital.

4.5 Pembahasan

Hasil penelitian ini menunjukkan bahwa keamanan sistem informasi memiliki peran yang sangat penting dalam membangun kepercayaan pengguna terhadap platform digital. Keamanan yang dimaksud tidak hanya mencakup aspek teknis seperti enkripsi dan autentikasi, tetapi juga mencakup persepsi pengguna terhadap keamanan tersebut.

Menurut Gefen et al. (2003), kepercayaan dalam sistem digital terbentuk melalui kombinasi antara faktor teknologi dan faktor psikologis. Dalam penelitian ini, faktor psikologis tercermin melalui variabel persepsi risiko.

Keamanan sistem yang baik mampu menurunkan persepsi risiko, sehingga pengguna merasa lebih aman dalam menggunakan layanan digital. Hal ini penting karena pengguna sering kali tidak memiliki pemahaman teknis yang mendalam, sehingga mereka lebih mengandalkan persepsi dalam menilai keamanan sistem.

Selain itu, hasil penelitian menunjukkan bahwa persepsi risiko memiliki pengaruh signifikan terhadap kepercayaan pengguna. Hal ini menunjukkan bahwa pengelolaan risiko menjadi faktor kunci dalam meningkatkan kepercayaan pengguna.

Dalam konteks praktis, organisasi perlu tidak hanya meningkatkan sistem keamanan, tetapi juga mengkomunikasikan keamanan tersebut kepada pengguna. Transparansi dan edukasi menjadi faktor penting dalam membangun persepsi positif terhadap keamanan sistem.

Temuan ini juga mendukung teori Technology Acceptance Model (TAM) yang menyatakan bahwa faktor eksternal seperti keamanan dan risiko mempengaruhi penerimaan teknologi oleh pengguna (Davis, 1989).

4.6 Implikasi Penelitian

4.6.1 Implikasi Teoritis

Penelitian ini memberikan kontribusi terhadap pengembangan teori dalam bidang sistem informasi, khususnya terkait hubungan antara keamanan, persepsi risiko, dan kepercayaan pengguna. Model penelitian ini dapat digunakan sebagai referensi dalam penelitian selanjutnya.

4.6.2 Implikasi Praktis

Bagi perusahaan atau penyedia layanan digital:

- Meningkatkan sistem keamanan (enkripsi, autentikasi)
- Mengurangi persepsi risiko melalui edukasi pengguna
- Meningkatkan transparansi kebijakan privasi

4.7 Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan:

1. Jumlah sampel terbatas
2. Data bersifat persepsi (self-reported)
3. Tidak mencakup semua jenis platform digital

BAB V

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa:

1. **Keamanan sistem informasi berpengaruh positif dan signifikan terhadap kepercayaan pengguna.** Hal ini menunjukkan bahwa semakin tinggi tingkat keamanan yang diterapkan, maka semakin tinggi pula tingkat kepercayaan pengguna terhadap platform digital.
2. **Keamanan sistem informasi berpengaruh negatif terhadap persepsi risiko.** Artinya, peningkatan keamanan mampu menurunkan tingkat risiko yang dirasakan oleh pengguna.
3. **Persepsi risiko berpengaruh negatif terhadap kepercayaan pengguna.** Semakin tinggi persepsi risiko, maka semakin rendah tingkat kepercayaan pengguna.
4. **Persepsi risiko berperan sebagai variabel mediasi dalam hubungan antara keamanan dan kepercayaan.** Hal ini menunjukkan bahwa keamanan tidak hanya berdampak langsung, tetapi juga tidak langsung melalui penurunan risiko.

Secara keseluruhan, penelitian ini menegaskan bahwa keamanan sistem informasi merupakan faktor kunci dalam membangun kepercayaan pengguna pada platform digital. Oleh karena itu, organisasi perlu mengintegrasikan aspek keamanan dalam strategi bisnis mereka untuk meningkatkan kepercayaan dan loyalitas pengguna.

DAFTAR PUSTAKA

- Akmal, R. N., et al. (2025). Evaluasi keamanan sistem informasi rumah sakit: Metode ISO 27001. *Jurnal Manajemen Informatika dan Komunikasi*, 6(1), 560–569. ([Journal STMIK](#))
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Sage Publications.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping. *MIS Quarterly*, 27(1), 51–90.

- Ghozali, I. (2018). Aplikasi Analisis Multivariate dengan Program IBM SPSS. Badan Penerbit Universitas Diponegoro.
- Gujarati, D. N., & Porter, D. C. (2009). Basic Econometrics (5th ed.). McGraw-Hill.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate Data Analysis (8th ed.). Cengage Learning.
- Hafizd, D. A., et al. (2023). Kebijakan keamanan sistem informasi. Jurnal Sains dan Teknologi, 3(1), 95–100. ([Jurnal Minartis](#))
- Hafsah, A., & Nasution, M. I. P. (2024). Keamanan sistem informasi pada era modern. Musytari: Jurnal Manajemen, Akuntansi, dan Ekonomi, 10(9), 81–90. ([Ejournal Warunayama](#))
- Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce. Decision Support Systems, 44(2), 544–564.
- Lestari, A. D., et al. (2024). Pengaruh keamanan informasi terhadap kepercayaan pengguna. Jurnal Riset Informatika dan Inovasi. ([Jurnal Mahasiswa](#))
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures. Information Systems Research, 13(3), 334–359.
- Mukhlis, A., et al. (2023). Ancaman dan pengamanan sistem informasi. Jurnal Ilmiah Sistem Informasi, 3(2). ([Journal Sinov](#))
- Sekaran, U., & Bougie, R. (2016). Research Methods for Business: A Skill-Building Approach (7th ed.). Wiley.
- Sitanggang, J. Y. B., et al. (2025). Analisis keamanan informasi di era digital. Journal Sains Student Research, 3(5). ([E-Jurnal Kampus Akademik](#))
- Stallings, W. (2017). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Pearson.
- Sugiyono. (2019). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Alfabeta.
- Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.
- Wiranto, H., & Salis, A. M. (2025). Kepercayaan terhadap keamanan OTP. Jurnal Pendidikan Informatika dan Sains, 14(1), 75–83. ([Jurnal UPGRIPNK](#))