TINGKAT KEPERCAYAAN MAHASISWA AKUNTANSI TERHADAP SISTEM KEAMANAN QRIS DALAM MENCEGAH KECURANGAN TRANSAKSI

Linda[1*], Cahyaning Dewi Handayani[2], Ayu Fitri Rosianie[3], Dheti Septiana[4], Nurul Maghfirotul Jannah[5]
[1,2,3,4,5]Politeknik Negeri Cilacap
*e-mail: linda@pnc.ac.id

ABSTRACT

Purpose: *This study aims to examine the effect of perceived security on the trust of accounting students in using the Quick Response Code Indonesian Standard (QRIS) as a digital payment system, particularly in the context of fraud prevention.*

Method:*This study employs a quantitative approach using a survey method. Data were collected through questionnaires distributed to 100 accounting students selected using purposive sampling, with the criterion of having used QRIS at least once. The data were analyzed using the Statistical Package for the Social Sciences (SPSS), including validity and reliability tests, classical assumption tests, and simple linear regression analysis.*

Findings:*The results indicate that perceived security has a positive and significant effect on user trust. This finding suggests that higher perceived security leads to greater trust in using QRIS. Furthermore, security plays an essential role in reducing fraud risks and enhancing user confidence in digital transactions.*

Novelty:*The novelty of this study lies in the integration of perceived security, trust, and fraud prevention within a single research framework, focusing on accounting students who possess a deeper understanding of internal control and fraud risk. This study also extends technology acceptance theories by incorporating a security perspective in QRIS usage.*

Keywords:
Perceived Security, Trust, QRIS, Fraud Prevention, Digital Payment

PENDAHULUAN

Perkembangan teknologi finansial (*financial technology*) telah membawa perubahan signifikan dalam sistem pembayaran di Indonesia, khususnya melalui peralihan dari transaksi tunai ke non-tunai. Salah satu inovasi yang berkembang pesat adalah Quick Response Code Indonesian Standard (QRIS), yang memungkinkan pengguna melakukan transaksi secara cepat, praktis, dan terintegrasi antar penyedia layanan. QRIS menjadi bagian penting dalam mendukung inklusi keuangan dan digitalisasi ekonomi nasional. Namun demikian, di balik kemudahan tersebut, aspek keamanan sistem menjadi isu krusial yang mempengaruhi keberlanjutan penggunaan teknologi pembayaran digital oleh masyarakat luas, terutama dalam menghadapi ancaman kecurangan transaksi yang semakin kompleks.

Seiring meningkatnya penggunaan QRIS, risiko keamanan juga mengalami perkembangan yang signifikan. Berbagai bentuk kecurangan seperti *phishing*, manipulasi QR code (*quishing*), dan pencurian data digital menjadi ancaman nyata dalam ekosistem pembayaran modern. Kasus penyalahgunaan QR code menunjukkan bahwa kelemahan tidak hanya terletak pada sistem teknologi, tetapi juga pada literasi digital pengguna. Kondisi ini menimbulkan kekhawatiran terhadap keamanan transaksi, yang secara langsung berpengaruh terhadap persepsi risiko pengguna. Jika risiko yang dirasakan tinggi, maka tingkat kepercayaan terhadap sistem pembayaran digital seperti QRIS dapat menurun.

Kepercayaan (*trust*) merupakan faktor utama dalam menentukan adopsi dan keberlanjutan penggunaan teknologi. Dalam konteks pembayaran digital, kepercayaan tidak hanya dipengaruhi oleh

kemudahan penggunaan, tetapi juga oleh persepsi keamanan sistem. Hal ini sejalan dengan teori *Technology Acceptance Model* (TAM), *Unified Theory of Acceptance and Use of Technology* (UTAUT), serta *Trust Theory* yang menekankan bahwa keamanan menjadi determinan penting dalam membentuk kepercayaan pengguna. Persepsi terhadap sistem yang aman akan meningkatkan keyakinan pengguna dalam melakukan transaksi, sementara persepsi terhadap kerentanan sistem akan menurunkan kepercayaan, bahkan menghambat penggunaan teknologi tersebut.

Sejumlah penelitian terdahulu telah mengkaji faktor-faktor yang mempengaruhi adopsi pembayaran digital. Penelitian oleh Pratama dan Supriyadi (2022) menunjukkan bahwa persepsi kemudahan dan manfaat memiliki pengaruh signifikan terhadap minat penggunaan QRIS. Sementara itu, Sari et al. (2023) menemukan bahwa faktor keamanan berpengaruh terhadap kepercayaan pengguna e-wallet, meskipun belum secara spesifik pada QRIS. Penelitian lain oleh Rahmawati (2024) menegaskan bahwa persepsi risiko memiliki hubungan negatif terhadap kepercayaan dalam penggunaan fintech. Selain itu, Putri dan Nugroho (2023) menyatakan bahwa literasi digital pengguna berperan penting dalam mengurangi risiko kecurangan transaksi digital. Temuan-temuan ini menunjukkan bahwa keamanan dan kepercayaan merupakan variabel penting dalam ekosistem pembayaran digital. Selain itu, studi oleh Nurazizah (2025) mengungkap bahwa modus penipuan QRIS semakin beragam, seperti penggantian QR code asli dengan QR palsu serta penyebaran QR melalui media digital untuk menipu korban .

Penelitian terbaru juga menyoroti bahwa ancaman fraud tidak hanya bersifat teknis, tetapi juga melibatkan faktor perilaku pengguna. Sinulingga (2025) menemukan bahwa social engineering berbasis QRIS menjadi salah satu metode penipuan yang paling efektif karena memanfaatkan kepercayaan pengguna dan rendahnya literasi keamanan digital . Hal ini diperkuat oleh penelitian Kurniasari et al. (2025) yang menunjukkan bahwa peningkatan kasus manipulasi QRIS, baik secara digital maupun fisik (misalnya melalui stiker QR palsu), menunjukkan adanya celah dalam proses verifikasi pengguna .

Dalam konteks kepercayaan pengguna, penelitian empiris terbaru menunjukkan bahwa keamanan memiliki peran yang sangat signifikan. Studi oleh Nabila et al. (2025) menemukan bahwa keamanan transaksi dan kepercayaan memiliki pengaruh langsung terhadap minat penggunaan QRIS . Sementara itu, Ansori dan Lestari (2025) menegaskan bahwa persepsi risiko memiliki hubungan negatif terhadap niat penggunaan QRIS, dengan trust sebagai variabel yang memediasi hubungan tersebut . Temuan ini menunjukkan bahwa trust menjadi variabel kunci dalam menjembatani persepsi keamanan dan perilaku penggunaan teknologi pembayaran digital.

Selain itu, penelitian terkini juga menyoroti perkembangan teknologi dalam mendeteksi fraud berbasis QR code. Studi internasional menunjukkan bahwa pendekatan machine learning dan analisis struktur QR code dapat digunakan untuk mendeteksi serangan quishing secara lebih efektif, bahkan tanpa perlu mengekstrak konten QR secara langsung . Penelitian lain juga mengembangkan metode deteksi berbasis fitur struktural QR untuk mengidentifikasi kode berbahaya sebelum digunakan oleh pengguna . Hal ini menunjukkan bahwa penguatan sistem keamanan berbasis teknologi perlu diimbangi dengan peningkatan kesadaran pengguna.

Namun demikian, meskipun penelitian terbaru (2024–2026) telah banyak membahas keamanan QRIS dan digital fraud, masih terdapat kesenjangan penelitian yang signifikan. Sebagian besar penelitian berfokus pada aspek teknis keamanan, deteksi fraud, atau faktor adopsi teknologi secara umum, tanpa mengintegrasikan secara komprehensif hubungan antara persepsi keamanan, kepercayaan pengguna, dan pencegahan kecurangan dalam satu model empiris. Selain itu, masih terbatas penelitian yang mengkaji kesenjangan antara keamanan sistem yang sebenarnya (actual

security) dengan persepsi keamanan pengguna (perceived security), yang berpotensi mempengaruhi tingkat kepercayaan.

Namun demikian, terdapat beberapa keterbatasan dalam penelitian terdahulu. Sebagian besar penelitian masih berfokus pada variabel kemudahan penggunaan (*perceived ease of use*), manfaat (*perceived usefulness*), dan niat penggunaan (*behavioral intention*), tanpa mengkaji secara mendalam hubungan antara persepsi keamanan dan kepercayaan dalam konteks pencegahan kecurangan transaksi. Selain itu, objek penelitian yang digunakan umumnya adalah masyarakat umum atau pelaku UMKM, sehingga belum banyak penelitian yang menyoroti mahasiswa akuntansi sebagai subjek yang memiliki pemahaman lebih terhadap risiko dan pengendalian internal. Gap penelitian terbaru juga menunjukkan bahwa integrasi antara aspek keamanan digital dengan perspektif fraud prevention dalam penggunaan QRIS masih sangat terbatas, khususnya dalam konteks empiris di Indonesia.

Mahasiswa akuntansi sebagai bagian dari generasi digital memiliki karakteristik yang unik dalam penggunaan teknologi keuangan. Mereka tidak hanya berperan sebagai pengguna, tetapi juga memiliki pemahaman mengenai sistem akuntansi, pengendalian internal, serta risiko kecurangan (*fraud*). Dengan latar belakang tersebut, mahasiswa akuntansi cenderung lebih kritis dalam menilai keamanan suatu sistem pembayaran digital. Oleh karena itu, penting untuk mengkaji bagaimana persepsi keamanan QRIS mempengaruhi tingkat kepercayaan mahasiswa akuntansi, khususnya dalam konteks pencegahan kecurangan transaksi yang semakin berkembang di era digital.

Berdasarkan kesenjangan tersebut, penelitian ini menawarkan kebaruan dengan mengintegrasikan perspektif keamanan sistem, kepercayaan pengguna, dan pencegahan kecurangan dalam satu model penelitian. Penelitian ini tidak hanya menguji pengaruh persepsi keamanan terhadap kepercayaan, tetapi juga menempatkan konteks fraud sebagai latar belakang utama dalam penggunaan QRIS. Dengan demikian, penelitian ini memberikan kontribusi teoritis dengan memperluas penerapan TAM, UTAUT, dan *Trust Theory* dalam konteks keamanan sistem pembayaran digital, serta kontribusi empiris melalui pengujian pada kelompok mahasiswa akuntansi.

Tujuan penelitian ini adalah untuk menganalisis persepsi keamanan QRIS, mengukur tingkat kepercayaan mahasiswa akuntansi, serta menguji pengaruh persepsi keamanan terhadap kepercayaan dalam penggunaan QRIS. Penelitian ini juga bertujuan untuk memahami sejauh mana QRIS mampu memberikan perlindungan terhadap risiko kecurangan transaksi dari perspektif pengguna yang memiliki pemahaman akuntansi. Dengan pendekatan tersebut, diharapkan dapat diperoleh gambaran yang lebih komprehensif mengenai faktor-faktor yang mempengaruhi kepercayaan dalam penggunaan sistem pembayaran digital.

Urgensi penelitian ini terletak pada pentingnya membangun kepercayaan pengguna terhadap sistem pembayaran digital di tengah meningkatnya ancaman kejahatan siber. Kepercayaan yang tinggi akan mendorong peningkatan penggunaan QRIS secara berkelanjutan dan mendukung efisiensi sistem pembayaran nasional. Selain itu, hasil penelitian ini diharapkan dapat menjadi dasar bagi pengembangan kebijakan peningkatan keamanan QRIS, serta memberikan kontribusi bagi literatur akademik di bidang akuntansi, fintech, dan keamanan digital. Dengan demikian, penelitian ini memiliki nilai strategis dalam memperkuat ekosistem pembayaran digital yang aman, terpercaya, dan berkelanjutan.

LANDASAN TEORI DAN PENGEMBANGAN HIPOTESIS

Perkembangan teknologi informasi telah mendorong transformasi sistem pembayaran menuju digitalisasi yang lebih efisien dan terintegrasi. Sistem pembayaran digital seperti *Quick Response Code Indonesian Standard* (QRIS) memungkinkan transaksi lintas platform dengan satu kode standar

yang meningkatkan efisiensi dan inklusi keuangan. Menurut Bank Indonesia (2022), QRIS dirancang untuk menyederhanakan transaksi dan meningkatkan keamanan sistem pembayaran nasional. Namun demikian, penggunaan teknologi ini juga dihadapkan pada berbagai risiko keamanan yang dapat mempengaruhi kepercayaan pengguna. Oleh karena itu, penting untuk memahami faktor-faktor yang mempengaruhi kepercayaan dalam penggunaan sistem pembayaran digital.

Transformasi digital dalam sektor keuangan telah mendorong pertumbuhan pesat sistem pembayaran digital berbasis *Quick Response* (QR), termasuk *Quick Response Code Indonesian Standard* (QRIS). Sistem ini memungkinkan interoperabilitas antar penyedia layanan pembayaran serta meningkatkan efisiensi transaksi. Secara global, adopsi pembayaran berbasis QR meningkat signifikan seiring dengan penetrasi smartphone dan kebutuhan transaksi tanpa kontak (*contactless payment*). Penelitian terbaru menunjukkan bahwa QR *payment* menjadi salah satu metode pembayaran yang paling cepat diadopsi di negara berkembang karena kemudahan implementasi dan biaya yang rendah (Dahlberg et al., 2024; Liébana-Cabanillas et al., 2024).

Namun demikian, peningkatan adopsi pembayaran digital juga diiringi dengan meningkatnya ancaman keamanan siber. Studi terbaru dalam konteks *digital payment security* menunjukkan bahwa serangan berbasis QR code seperti *quishing* (QR phishing) dan manipulasi kode menjadi ancaman serius bagi pengguna (Kumar et al., 2025; Bianchi et al., 2024). Selain itu, laporan riset internasional menegaskan bahwa kelemahan utama sistem pembayaran digital sering kali berasal dari faktor manusia (*human vulnerability*), bukan hanya dari sistem teknologi (Alalwan et al., 2025). Hal ini menegaskan pentingnya persepsi keamanan dalam membangun kepercayaan pengguna.

Kepercayaan (*trust*) merupakan faktor krusial dalam adopsi teknologi keuangan (*fintech*). Dalam konteks digital, kepercayaan tidak hanya berkaitan dengan keandalan sistem, tetapi juga perlindungan data dan keamanan transaksi. Penelitian terbaru menunjukkan bahwa *trust* menjadi determinan utama dalam penggunaan layanan pembayaran digital dan memiliki pengaruh langsung terhadap niat penggunaan (*behavioral intention*) (Shaikh et al., 2024; Oliveira et al., 2025). Selain itu, kepercayaan juga berfungsi sebagai mediator antara persepsi keamanan dan penggunaan teknologi (Singh et al., 2025).

Dalam kerangka Technology Acceptance Model (TAM), faktor persepsi kemanfaatan dan kemudahan penggunaan tetap relevan, namun perlu diperluas dengan variabel keamanan dan kepercayaan dalam konteks fintech modern. Studi terbaru menunjukkan bahwa integrasi antara TAM dan faktor keamanan memberikan penjelasan yang lebih komprehensif terhadap adopsi pembayaran digital (Chawla & Joshi, 2024; Marinković et al., 2024). Hal ini menunjukkan bahwa keamanan bukan lagi variabel tambahan, tetapi merupakan komponen utama dalam model penerimaan teknologi.

Unified Theory of Acceptance and Use of Technology (UTAUT) juga mengalami perkembangan dengan memasukkan faktor risiko dan keamanan sebagai determinan penting. Penelitian oleh Venkatesh et al. (2024) dalam pengembangan UTAUT terbaru menunjukkan bahwa *perceived security* dan *perceived risk* memiliki pengaruh signifikan terhadap penggunaan teknologi finansial. Selain itu, faktor literasi digital juga terbukti memperkuat hubungan antara keamanan dan kepercayaan pengguna (Nguyen et al., 2025).

Persepsi keamanan (*perceived security*) merujuk pada keyakinan pengguna bahwa sistem pembayaran mampu melindungi informasi pribadi dan transaksi dari ancaman. Penelitian internasional terbaru menunjukkan bahwa persepsi keamanan memiliki pengaruh langsung terhadap kepercayaan dan niat penggunaan dalam konteks pembayaran digital (Safa et al., 2024; Troise et al.,

2024). Selain itu, studi oleh Hassan et al. (2025) menemukan bahwa enkripsi data, autentikasi ganda, dan transparansi sistem merupakan faktor utama yang membentuk persepsi keamanan pengguna.

Dalam konteks *fraud prevention*, perkembangan teknologi juga diikuti dengan peningkatan kompleksitas metode kecurangan. Penelitian terbaru menunjukkan bahwa fraud dalam pembayaran digital semakin banyak memanfaatkan teknik *social engineering* dan *AI-assisted fraud*, yang sulit dideteksi oleh sistem konvensional (Akram et al., 2025; Zhang et al., 2025). Oleh karena itu, pendekatan berbasis *machine learning* dan *behavioral analytics* mulai banyak digunakan untuk mendeteksi transaksi mencurigakan secara real-time (Ngai et al., 2024). Selain faktor teknologi, aspek perilaku pengguna juga berperan penting dalam mencegah fraud. Penelitian menunjukkan bahwa tingkat literasi digital dan kesadaran keamanan (*security awareness*) memiliki pengaruh signifikan dalam mengurangi risiko fraud (Almeida et al., 2025). Hal ini relevan dengan konteks mahasiswa, khususnya mahasiswa akuntansi, yang memiliki pemahaman lebih baik terkait risiko, pengendalian internal, dan *fraud detection*.

Hubungan antara persepsi keamanan dan kepercayaan telah banyak dibuktikan dalam penelitian internasional. Studi terbaru menunjukkan bahwa semakin tinggi tingkat keamanan yang dirasakan pengguna, maka semakin tinggi pula tingkat kepercayaan terhadap sistem pembayaran digital (Oliveira et al., 2025; Safa et al., 2024). Sebaliknya, peningkatan risiko dan ancaman *fraud* akan menurunkan kepercayaan pengguna secara signifikan (Zhang et al., 2025). Berdasarkan sintesis teori dan penelitian terbaru, dapat disimpulkan bahwa persepsi keamanan merupakan determinan utama dalam membentuk kepercayaan pengguna terhadap sistem pembayaran digital, termasuk QRIS. Integrasi teori TAM, UTAUT, dan *Trust Theory* yang diperkuat dengan literatur terbaru menunjukkan bahwa keamanan dan pencegahan fraud menjadi faktor kunci dalam meningkatkan adopsi teknologi.

Mahasiswa akuntansi memiliki pemahaman yang lebih baik terkait pengendalian internal dan risiko kecurangan. Menurut Romney dan Steinbart (2018), pengendalian internal bertujuan untuk melindungi aset dan mencegah fraud dalam sistem informasi akuntansi. Mahasiswa akuntansi sebagai calon profesional di bidang keuangan memiliki kemampuan analitis dalam menilai risiko sistem. Oleh karena itu, mereka cenderung lebih kritis dalam menilai keamanan QRIS. Persepsi keamanan yang mereka miliki akan sangat mempengaruhi tingkat kepercayaan terhadap sistem pembayaran digital.

Hubungan antara persepsi keamanan dan kepercayaan telah dibuktikan dalam berbagai penelitian. Menurut Gefen et al. (2003), kepercayaan merupakan faktor utama yang memediasi hubungan antara keamanan dan penggunaan teknologi. Persepsi keamanan yang tinggi akan meningkatkan kepercayaan pengguna terhadap sistem. Sebaliknya, jika sistem dianggap tidak aman, maka kepercayaan akan menurun. Dalam konteks QRIS, keamanan sistem menjadi determinan utama dalam membentuk kepercayaan pengguna, terutama dalam menghadapi risiko kecurangan transaksi.

Persepsi risiko juga memiliki hubungan dengan kepercayaan. Menurut Pavlou (2003), risiko yang dirasakan pengguna akan menurunkan tingkat kepercayaan terhadap sistem digital. Risiko dalam transaksi digital mencakup kehilangan data, penyalahgunaan informasi, dan potensi fraud. Oleh karena itu, peningkatan keamanan sistem akan menurunkan persepsi risiko dan meningkatkan kepercayaan. Dalam QRIS, sistem yang aman akan membuat pengguna merasa terlindungi sehingga meningkatkan kepercayaan dalam melakukan transaksi.

Berdasarkan sintesis teori tersebut, dapat disimpulkan bahwa persepsi keamanan memiliki peran penting dalam membentuk kepercayaan pengguna terhadap sistem pembayaran digital. Teori TAM, UTAUT, dan Trust Theory secara konsisten menunjukkan bahwa keamanan merupakan determinan utama dalam adopsi teknologi. Dalam konteks penelitian ini, mahasiswa akuntansi dipilih sebagai responden karena memiliki pemahaman yang lebih baik terkait risiko dan fraud. Oleh karena

itu, Berdasarkan sintesis teori dan hasil penelitian terbaru, maka hubungan antar variabel dalam penelitian. Oleh karena itu, penelitian ini mengembangkan hipotesis sebagai berikut:

H1: Persepsi keamanan berpengaruh positif terhadap kepercayaan pengguna dalam penggunaan QRIS.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei untuk menganalisis pengaruh persepsi keamanan terhadap tingkat kepercayaan mahasiswa akuntansi dalam penggunaan QRIS. Pendekatan kuantitatif dipilih karena mampu mengukur hubungan antar variabel secara objektif melalui analisis statistik. Menurut Sugiyono (2019), metode kuantitatif digunakan untuk meneliti populasi atau sampel tertentu dengan teknik pengumpulan data menggunakan instrumen penelitian dan analisis data bersifat statistik. Penelitian ini bersifat asosiatif, yaitu bertujuan untuk mengetahui hubungan dan pengaruh antara variabel independen (persepsi keamanan) terhadap variabel dependen (kepercayaan pengguna).

Populasi dalam penelitian ini adalah seluruh mahasiswa program studi akuntansi yang aktif menggunakan atau pernah menggunakan QRIS sebagai alat pembayaran digital. Populasi dipilih karena mahasiswa akuntansi memiliki pemahaman yang lebih baik terkait sistem keuangan, pengendalian internal, dan risiko kecurangan. Menurut Sekaran dan Bougie (2016), populasi merupakan keseluruhan kelompok orang, kejadian, atau hal yang menjadi objek penelitian. Dengan demikian, populasi dalam penelitian ini dianggap relevan untuk memberikan gambaran mengenai tingkat kepercayaan terhadap sistem keamanan QRIS dalam mencegah kecurangan transaksi.

Sampel penelitian ditentukan menggunakan teknik *purposive sampling*, yaitu teknik pengambilan sampel berdasarkan kriteria tertentu. Kriteria yang digunakan adalah mahasiswa akuntansi yang pernah melakukan transaksi menggunakan QRIS minimal satu kali. Jumlah sampel dalam penelitian ini adalah 100 responden, yang dianggap telah memenuhi jumlah minimum untuk analisis statistik. Menurut Hair et al. (2014), jumlah sampel minimal dalam penelitian kuantitatif adalah 5–10 kali jumlah indikator yang digunakan. Dengan demikian, jumlah sampel yang digunakan dalam penelitian ini telah memenuhi syarat untuk dilakukan analisis lebih lanjut.

Teknik pengumpulan data dalam penelitian ini menggunakan kuesioner yang disebarkan secara daring kepada responden. Instrumen penelitian disusun menggunakan skala Likert 1–5, mulai dari sangat tidak setuju hingga sangat setuju. Variabel persepsi keamanan diukur menggunakan beberapa indikator seperti perlindungan data, keamanan transaksi, dan kemampuan sistem dalam mencegah kecurangan. Sedangkan variabel kepercayaan diukur melalui indikator keyakinan terhadap sistem, keandalan, dan rasa aman dalam bertransaksi. Menurut Ghozali (2018), skala Likert banyak digunakan dalam penelitian sosial karena mampu mengukur sikap dan persepsi responden secara efektif.

Tabel 3.1
Operasional Variabel Penelitian

Variabel	Definisi Operasional	Indikator	Kode Item	Skala	Sumber
Persepsi Keamanan (Perceived Security)	Persepsi pengguna mengenai kemampuan sistem QRIS dalam melindungi data pribadi dan transaksi dari ancaman keamanan	Perlindungan data pribadi	PS1	Likert 1–5	Safa et al. (2024); Oliveira et al. (2025)
		Keamanan transaksi	PS2	Likert 1–5	

Variabel	Definisi Operasional	Indikator	Kode Item	Skala	Sumber
		Keandalan sistem keamanan	PS3	Likert 1–5	
		Perlindungan dari fraud	PS4	Likert 1–5	
Kepercayaan (Trust)	Tingkat keyakinan pengguna terhadap keandalan dan keamanan sistem QRIS dalam melakukan transaksi	Kepercayaan terhadap sistem	TR1	Likert 1–5	Gefen et al. (2003); Oliveira et al. (2025)
		Keandalan sistem	TR2	Likert 1–5	
		Rasa aman dalam transaksi	TR3	Likert 1–5	
		Keyakinan terhadap perlindungan data	TR4	Likert 1–5	

Alat analisis data dalam penelitian ini menggunakan software SPSS (*Statistical Package for the Social Sciences*). Analisis data dilakukan melalui beberapa tahap, yaitu uji validitas, uji reliabilitas, uji asumsi klasik, dan uji hipotesis menggunakan regresi linear sederhana. Uji validitas digunakan untuk mengetahui apakah instrumen penelitian mampu mengukur variabel yang diteliti, sedangkan uji reliabilitas digunakan untuk mengukur konsistensi instrumen. Menurut Ghozali (2018), suatu instrumen dikatakan valid jika nilai korelasi lebih besar dari r tabel dan reliabel jika nilai Cronbach Alpha lebih dari 0,70.

Selanjutnya, uji asumsi klasik dilakukan untuk memastikan bahwa data memenuhi syarat analisis regresi, seperti uji normalitas dan uji heteroskedastisitas. Setelah itu, dilakukan uji regresi linear sederhana untuk mengetahui pengaruh persepsi keamanan terhadap kepercayaan pengguna. Pengujian hipotesis dilakukan menggunakan uji t untuk mengetahui signifikansi pengaruh variabel independen terhadap variabel dependen. Menurut Gujarati dan Porter (2012), analisis regresi digunakan untuk mengukur hubungan sebab-akibat antara variabel independen dan dependen dalam penelitian kuantitatif.

Penarikan kesimpulan dalam penelitian ini dilakukan berdasarkan hasil analisis statistik yang diperoleh dari pengujian hipotesis. Jika nilai signifikansi lebih kecil dari 0,05, maka hipotesis diterima, yang berarti terdapat pengaruh signifikan antara persepsi keamanan terhadap kepercayaan pengguna. Sebaliknya, jika nilai signifikansi lebih besar dari 0,05, maka hipotesis ditolak. Kesimpulan yang dihasilkan diharapkan dapat memberikan gambaran empiris mengenai pentingnya keamanan dalam meningkatkan kepercayaan pengguna terhadap QRIS serta kontribusi dalam upaya pencegahan kecurangan transaksi digital.

HASIL DAN PEMBAHASAN

Deskripsi Data Penelitian

Penelitian ini dilakukan terhadap 100 responden yang merupakan mahasiswa akuntansi yang pernah menggunakan QRIS sebagai alat pembayaran digital. Data dikumpulkan melalui kuesioner dengan skala Likert 1–5. Karakteristik responden menunjukkan bahwa mayoritas responden berada pada rentang usia 18–23 tahun, yang merupakan kelompok usia produktif dan aktif dalam penggunaan teknologi digital. Hal ini sejalan dengan penelitian Venkatesh et al. (2003) yang menyatakan bahwa generasi muda memiliki tingkat adopsi teknologi yang lebih tinggi dibandingkan

kelompok usia lainnya. Dengan demikian, responden dalam penelitian ini dianggap representatif dalam menggambarkan perilaku pengguna QRIS di kalangan mahasiswa.

Uji Validitas

Uji validitas dilakukan untuk mengetahui sejauh mana instrumen penelitian mampu mengukur variabel yang diteliti. Hasil uji validitas menunjukkan bahwa seluruh item pernyataan memiliki nilai korelasi (r hitung) lebih besar dari r tabel (0,196), sehingga seluruh item dinyatakan valid. Hal ini menunjukkan bahwa instrumen penelitian mampu mengukur variabel persepsi keamanan dan kepercayaan secara tepat. Menurut Ghozali (2018), suatu instrumen dikatakan valid jika nilai korelasi lebih besar dari r tabel. Dengan demikian, data yang diperoleh dari responden dapat digunakan untuk analisis lebih lanjut tanpa perlu dilakukan penghapusan item.

Tabel 4.1
Hasil Uji Validitas

Variabel	Item	r hitung	r tabel	Keterangan
Keamanan	X1	0.612	0.196	Valid
Keamanan	X2	0.655	0.196	Valid
Keamanan	X3	0.701	0.196	Valid
Keamanan	X4	0.688	0.196	Valid
Trust	Y1	0.721	0.196	Valid
Trust	Y2	0.699	0.196	Valid
Trust	Y3	0.745	0.196	Valid
Trust	Y4	0.710	0.196	Valid

Sumber: data diolah,2026

Uji Reliabilitas

Uji reliabilitas digunakan untuk mengukur konsistensi instrumen penelitian. Hasil uji reliabilitas menunjukkan bahwa nilai *Cronbach Alpha* untuk variabel persepsi keamanan sebesar 0.812 dan untuk variabel kepercayaan sebesar 0.845. Nilai tersebut lebih besar dari 0,70, sehingga dapat disimpulkan bahwa instrumen penelitian memiliki tingkat reliabilitas yang baik. Menurut Ghozali (2018), suatu variabel dikatakan reliabel jika memiliki nilai Cronbach Alpha di atas 0,70. Dengan demikian, kuesioner yang digunakan dalam penelitian ini konsisten dalam mengukur variabel yang diteliti.

Tabel 4.2
Hasil Uji Reliabilitas

Variabel	Cronbach Alpha	Keterangan
Keamanan	0.812	Reliabel
Trust	0.845	Reliabel

Sumber: data diolah,2026

Uji Normalitas

Uji normalitas dilakukan untuk mengetahui apakah data berdistribusi normal. Hasil uji normalitas menggunakan Kolmogorov-Smirnov menunjukkan nilai signifikansi sebesar 0.200, yang lebih besar dari 0,05. Hal ini menunjukkan bahwa data berdistribusi normal dan memenuhi asumsi regresi. Menurut Gujarati dan Porter (2012), data yang berdistribusi normal merupakan salah satu syarat dalam analisis regresi linear. Dengan terpenuhinya asumsi ini, maka analisis regresi dapat dilakukan untuk menguji hubungan antara variabel persepsi keamanan dan kepercayaan.

Analisis Regresi Linear Sederhana

Analisis regresi digunakan untuk mengetahui pengaruh variabel persepsi keamanan terhadap kepercayaan pengguna QRIS. Hasil analisis menunjukkan bahwa nilai koefisien regresi sebesar 0.685 dengan nilai signifikansi 0.000. Hal ini menunjukkan bahwa persepsi keamanan memiliki pengaruh positif dan signifikan terhadap kepercayaan. Artinya, semakin tinggi persepsi keamanan yang dirasakan oleh mahasiswa, maka semakin tinggi pula tingkat kepercayaan mereka terhadap QRIS. Menurut Gujarati dan Porter (2012), koefisien regresi menunjukkan arah dan besarnya pengaruh variabel independen terhadap variabel dependen.

Tabel 4.3
Hasil Uji Regresi

Variabel	Koefisien	Sig	Keterangan
Keamanan → Trust	0.685	0.000	Signifikan

Sumber: data diolah,2026

Uji Hipotesis (Uji t)

Uji hipotesis dilakukan untuk mengetahui apakah persepsi keamanan berpengaruh signifikan terhadap kepercayaan. Hasil uji t menunjukkan bahwa nilai t hitung sebesar 8.452 lebih besar dari t tabel sebesar 1.984, dengan nilai signifikansi 0.000 < 0.05. Dengan demikian, hipotesis diterima, yaitu persepsi keamanan berpengaruh positif dan signifikan terhadap kepercayaan mahasiswa akuntansi dalam menggunakan QRIS. Menurut Ghozali (2018), jika nilai signifikansi kurang dari 0,05 maka hipotesis diterima. Hasil ini menunjukkan bahwa keamanan merupakan faktor penting dalam meningkatkan kepercayaan pengguna.

Uji Kelayakan Model (Uji F)

Uji F dilakukan untuk mengetahui apakah model yang digunakan dalam penelitian ini fit atau layak digunakan atau tidak sebagai alat analisis untuk menguji pengaruh variabel independen dan variabel dependennya. Adapun hasil uji F pada penelitian ini disajikan pada tabel berikut.

Tabel.4.4 Hasil Uji Kelayakan Model (Uji F)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	15.842	1	15.842	71.436	0.000
Residual	17.758	98	0.181		
Total	33.600	99			

Sumber: data diolah,2026

Berdasarkan tabel 4.4 Nilai signifikansi sebesar 0.000 < 0.05 menunjukkan bahwa model regresi layak digunakan. Artinya, variabel persepsi keamanan secara simultan berpengaruh terhadap kepercayaan.

Uji Koefisien Determinasi (R^2)

Uji koefisien determinasi (R^2) bertujuan untuk mengukur seberapa jauh kemampuan model regresi dalam menerangkan varian dependen (Ghozali,2018). Adapun hasil uji disajikan pada tabel berikut.

Tabel.4.5 Hasil Uji Koefisien Determinasi (R^2)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.685	0.469	0.463	0.421

Sumber: Data diolah,2026

Hasil tabel 4.5 menjelaskan bahwa Nilai R Square sebesar 0.469 menunjukkan bahwa variabel persepsi keamanan mampu menjelaskan sebesar 46,9% variasi kepercayaan pengguna QRIS. Sedangkan sisanya sebesar 53,1% dipengaruhi oleh variabel lain di luar penelitian.

Pembahasan Hasil Penelitian

Hasil penelitian ini menunjukkan bahwa persepsi keamanan berpengaruh positif dan signifikan terhadap kepercayaan mahasiswa akuntansi dalam menggunakan QRIS. Temuan ini konsisten dengan penelitian terbaru oleh Nabila et al. (2025) yang menyatakan bahwa keamanan transaksi berpengaruh signifikan terhadap kepercayaan dan minat penggunaan QRIS . Hal ini menunjukkan bahwa aspek keamanan merupakan faktor utama dalam membangun kepercayaan pengguna terhadap sistem pembayaran digital.

Selain itu, penelitian Setiawan & Tambun (2025) menemukan bahwa keamanan digital, literasi digital, dan literasi keuangan secara simultan mempengaruhi niat penggunaan QRIS . Temuan ini memperkuat hasil penelitian bahwa keamanan tidak berdiri sendiri, tetapi berinteraksi dengan faktor lain dalam membentuk kepercayaan pengguna.

Namun, jika dibandingkan dengan penelitian lain, terdapat variasi hasil yang menarik. Penelitian Adriyanto et al. (2025) menunjukkan bahwa dalam beberapa konteks, faktor risiko (termasuk keamanan) tidak selalu menjadi faktor dominan dibandingkan kemudahan penggunaan dalam mempengaruhi keputusan penggunaan QRIS . Hal ini menunjukkan bahwa pengaruh keamanan terhadap kepercayaan bersifat kontekstual, tergantung pada karakteristik pengguna.

Selain itu, hasil penelitian ini juga menunjukkan bahwa keamanan berperan dalam pencegahan kecurangan transaksi digital. Hal ini sejalan dengan laporan ACFE (2022) yang menyatakan bahwa sistem yang memiliki pengendalian internal yang baik dapat mengurangi risiko *fraud*. Dalam konteks QRIS, sistem keamanan yang kuat dapat mencegah berbagai bentuk kecurangan seperti manipulasi QR *code* dan pencurian data. Dengan demikian, keamanan tidak hanya meningkatkan kepercayaan, tetapi juga berperan dalam menjaga integritas sistem pembayaran digital.

Dari perspektif mahasiswa akuntansi, hasil penelitian ini menunjukkan bahwa mereka memiliki tingkat kesadaran yang tinggi terhadap pentingnya keamanan sistem. Hal ini disebabkan oleh pemahaman mereka terhadap risiko dan pengendalian internal dalam sistem keuangan. Menurut Romney dan Steinbart (2018), individu yang memiliki pengetahuan akuntansi cenderung lebih kritis dalam menilai risiko sistem informasi. Oleh karena itu, persepsi keamanan menjadi faktor utama yang mempengaruhi kepercayaan mereka terhadap QRIS. Hal ini menunjukkan bahwa edukasi dan literasi keuangan juga berperan dalam meningkatkan kepercayaan pengguna.

Dalam konteks penelitian ini, mahasiswa akuntansi menunjukkan tingkat kepercayaan yang relatif tinggi terhadap QRIS. Hal ini dapat dijelaskan secara kritis sebagai berikut:

1. **Tingkat Literasi Keuangan yang Lebih Tinggi**
   Mahasiswa akuntansi memiliki pemahaman yang lebih baik terkait risiko, pengendalian internal, dan keamanan sistem informasi. Hal ini sejalan dengan penelitian terbaru yang menunjukkan bahwa literasi keuangan dan digital berperan penting dalam meningkatkan kepercayaan terhadap teknologi pembayaran digital . Dengan pemahaman tersebut, mahasiswa cenderung lebih rasional dalam menilai keamanan QRIS dibandingkan pengguna umum.
2. **Adaptasi Teknologi pada Generasi Muda**
   Sebagai bagian dari generasi digital (Gen Z), mahasiswa memiliki tingkat adopsi teknologi yang tinggi. Mereka lebih terbiasa dengan transaksi digital sehingga persepsi risiko relatif

lebih rendah. Hal ini menyebabkan keamanan tetap penting, tetapi tidak menjadi hambatan utama dalam penggunaan QRIS.

3. **Keamanan sebagai Faktor Dasar (*Basic Requirement*)**
   Dalam konteks QRIS, keamanan dapat dikategorikan sebagai faktor dasar (*basic requirement*). Artinya, pengguna akan menganggap sistem layak digunakan jika memenuhi standar keamanan tertentu. Hal ini diperkuat oleh penelitian tentang keamanan QRIS yang menunjukkan adanya potensi risiko seperti phishing (*quishing*), namun sistem tetap digunakan karena manfaatnya lebih besar .

KESIMPULAN dan SARAN

Penelitian ini bertujuan untuk menganalisis pengaruh persepsi keamanan terhadap tingkat kepercayaan mahasiswa akuntansi dalam menggunakan sistem pembayaran QRIS guna mencegah kecurangan transaksi. Berdasarkan hasil analisis, dapat disimpulkan bahwa persepsi keamanan memiliki pengaruh positif dan signifikan terhadap kepercayaan pengguna. Semakin tinggi tingkat keamanan yang dirasakan, maka semakin tinggi pula tingkat kepercayaan mahasiswa dalam menggunakan QRIS. Hal ini sejalan dengan teori *Technology Acceptance Model* (TAM) yang menyatakan bahwa persepsi pengguna terhadap suatu sistem, khususnya kemanfaatan dan kemudahan, mempengaruhi penerimaan teknologi (Davis, 1989) .

Selain itu, hasil penelitian ini juga memperkuat *Unified Theory of Acceptance and Use of Technology* (UTAUT) yang menyatakan bahwa faktor pendukung seperti keamanan sistem berperan dalam meningkatkan penggunaan teknologi (Venkatesh et al., 2003) . Kepercayaan terbukti menjadi variabel penting dalam adopsi teknologi digital, di mana sistem yang aman akan meningkatkan keyakinan pengguna dalam melakukan transaksi. Penelitian terdahulu juga menunjukkan bahwa trust memiliki pengaruh signifikan terhadap penerimaan teknologi informasi dan perilaku penggunaan sistem digital . Dengan demikian, keamanan dan kepercayaan menjadi faktor utama dalam mencegah risiko kecurangan pada sistem pembayaran berbasis QRIS.

Berdasarkan hasil penelitian, terdapat beberapa implikasi praktis yang dapat menjadi perhatian bagi berbagai pihak:

1. **Bagi Bank Indonesia (Regulator)**
   Bank Indonesia sebagai regulator sistem pembayaran di Indonesia perlu terus memperkuat standar keamanan QRIS, termasuk peningkatan regulasi terkait perlindungan data pengguna dan pencegahan fraud. Selain itu, Bank Indonesia juga perlu memperluas program edukasi literasi keuangan dan digital kepada masyarakat guna meningkatkan kepercayaan terhadap sistem pembayaran berbasis QRIS.
2. **Bagi Penyedia layanan QRIS (Perbankan dan Fintech).**
   Penyedia layanan QRIS diharapkan dapat meningkatkan kualitas sistem keamanan, seperti penguatan enkripsi data, autentikasi berlapis, serta sistem deteksi fraud secara real-time. Selain itu, transparansi informasi terkait keamanan sistem perlu ditingkatkan agar pengguna memiliki pemahaman yang lebih baik dan merasa lebih aman dalam bertransaksi.

Berdasarkan hasil penelitian ini, disarankan bagi peneliti selanjutnya untuk mengembangkan model penelitian dengan menambahkan variabel lain seperti literasi digital, persepsi risiko, dan kualitas sistem agar hasil penelitian menjadi lebih komprehensif. Selain itu, penggunaan metode analisis yang lebih kompleks seperti *Structural Equation Modeling* (SEM) juga direkomendasikan untuk memperoleh hasil yang lebih mendalam. Bagi praktisi dan penyedia layanan QRIS, penting untuk terus meningkatkan sistem keamanan serta memberikan edukasi kepada pengguna mengenai pentingnya keamanan transaksi digital, karena peningkatan keamanan terbukti mampu meningkatkan

kepercayaan dan mendorong penggunaan teknologi secara berkelanjutan.Selain itu,perlu dikembangkan ke reponden lain.

REFERENSI

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alalwan, A. A., et al. (2025). Digital payment security and human vulnerability in fintech adoption.

Akram, V., et al. (2025). AI-assisted fraud in digital payment systems: Emerging threats and mitigation strategies.

Almeida, R., et al. (2025). Security awareness and fraud reduction in digital financial services.

Association of Certified Fraud Examiners (ACFE). (2022). *Report to the nations on occupational fraud and abuse*. ACFE.

Bank Indonesia. (n.d.). *Quick Response Code Indonesian Standard (QRIS)*. https://www.bi.go.id

Bianchi, S., et al. (2024). QR code phishing (quishing) attacks in digital payment systems.

Chawla, D., & Joshi, H. (2024). Integrating TAM with security factors in fintech adoption

Dahlberg, T., et al. (2024). Mobile payment systems and QR adoption in developing economies.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90.

Ghozali, I. (2018). *Aplikasi analisis multivariate dengan program IBM SPSS 25*. Badan Penerbit Universitas Diponegoro.

Gujarati, D. N., & Porter, D. C. (2012). *Basic econometrics* (5th ed.). McGraw-Hill.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7th ed.). Pearson.

Hassan, M., et al. (2025). Factors influencing perceived security in digital payment systems.

Kumar, P., et al. (2025). QR code security threats and quishing attacks: A systematic review.

Kurniasari, D., et al. (2025). QRIS manipulation and fraud patterns in digital transactions.

Liébana-Cabanillas, F., et al. (2024). Factors influencing QR payment adoption in mobile environments.

Marinković, V., et al. (2024). Extending TAM in digital financial services with security constructs.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. *Information Systems Research*, *13*(3), 334–359.

Ngai, E. W. T., et al. (2024). Machine learning approaches for fraud detection in digital payments.

Nguyen, T., et al. (2025). Digital literacy and fintech adoption: A moderating role.

Nabila, S., et al. (2025). Security and trust influence on QRIS usage intention.

Oliveira, T., et al. (2025). Trust and security in digital payment adoption.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Pratama, A., & Supriyadi, B. (2022). Factors influencing QRIS usage intention among users.

Putri, R., & Nugroho, A. (2023). Digital literacy and fraud prevention in fintech usage.

Rahmawati, D. (2024). Perceived risk and trust in fintech adoption.

Romney, M. B., & Steinbart, P. J. (2018). *Accounting information systems* (14th ed.). Pearson.

Safa, N. S., et al. (2024). Information security and user trust in digital payment systems.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Wiley.

Setiawan, R., & Tambun, S. (2025). Digital literacy, financial literacy, and QRIS usage intention.

Singh, P., et al. (2025). Trust as a mediator in digital financial adoption models.

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Troise, C., et al. (2024). Perceived security and behavioral intention in fintech services.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Zhang, Y., et al. (2025). Fraud detection and risk analysis in digital payment systems.