

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian terdahulu digunakan untuk menempatkan hubungan antarkonstruk secara empiris, membandingkan hasil pengujian, dan menunjukkan ruang yang belum dijelaskan oleh penelitian sebelumnya. Kajian disusun dari tahun terbit terbaru menuju tahun yang lebih lama. Setiap penelitian dibaca berdasarkan tujuan, variabel, metode, hasil, serta kedekatannya dengan *fraud awareness*, literasi keuangan digital, kepercayaan pada *e-payment*, dan persepsi penipuan keuangan online.

1. Chen et al. (2026)

Chen et al. (2026) menelaah perilaku pencegahan penipuan daring dengan memusatkan perhatian pada empat konstruk, yaitu *online fraud susceptibility*, *threat awareness*, *anti-fraud self-efficacy*, dan *online scam prevention behavior*. *Protection Motivation Theory* digunakan untuk membedakan proses penilaian ancaman dari penilaian kemampuan menghadapi ancaman. *Threat awareness* menggambarkan sejauh mana seseorang menyadari keberadaan, tingkat bahaya, dan relevansi pribadi suatu penipuan, sedangkan *anti-fraud self-efficacy* menunjukkan keyakinan bahwa seseorang mampu mengenali, memeriksa, serta merespons informasi yang mencurigakan. Kerangka tersebut menempatkan kerentanan bukan sekadar sebagai pengalaman pernah tertipu, tetapi sebagai

struktur psikologis yang dapat memengaruhi cara individu membaca tanda bahaya dan memilih tindakan perlindungan.

Penelitian melibatkan 765 mahasiswa di Tiongkok melalui desain survei potong lintang. *Online fraud susceptibility* diukur melalui lima dimensi, yaitu dorongan memperoleh keuntungan moneter, pemrosesan informasi secara heuristik, preferensi terhadap risiko keuangan, pengetahuan antipenipuan, dan kerentanan terhadap pengaruh sosial. Hubungan antarkonstruk diuji menggunakan *structural equation modelling*, sedangkan *latent profile analysis* digunakan untuk mengidentifikasi kelompok responden berdasarkan pola kerentanannya. Penggunaan dua pendekatan analisis memungkinkan peneliti melihat hubungan rata-rata antarkonstruk sekaligus perbedaan karakteristik kelompok yang tidak selalu terlihat dari koefisien jalur saja.

Hasil pengujian memperlihatkan bahwa tingkat kerentanan yang lebih tinggi berkaitan dengan kesadaran ancaman, efikasi diri antipenipuan, dan perilaku pencegahan yang lebih rendah. *Threat awareness* serta *anti-fraud self-efficacy* berhubungan positif dengan perilaku pencegahan, tetapi hubungan antara kesadaran ancaman dan efikasi diri tidak terbukti secara statistik. Model menjelaskan 21,6% variasi *threat awareness*, 35,6% variasi *anti-fraud self-efficacy*, dan 75,1% variasi *online scam prevention behavior*. Tiga profil kerentanan juga ditemukan, yaitu kelompok rendah, sedang, dan tinggi, dengan kelompok berkerentanan rendah menunjukkan kesiapan pencegahan yang lebih baik.

Kedekatan penelitian tersebut dengan penelitian ini terdapat pada pembahasan kesadaran terhadap tanda penipuan dan respons pengguna ketika berhadapan dengan transaksi digital yang mencurigakan. *Fraud awareness* pada penelitian ini berhubungan dengan kemampuan mengenali modus, sedangkan persepsi penipuan keuangan online mencakup penilaian terhadap tingkat ancaman dan kecenderungan merespons risiko. Batas pembandingnya terletak pada populasi mahasiswa, penggunaan *Protection Motivation Theory*, serta penempatan perilaku pencegahan sebagai variabel terikat. Penelitian ini menggunakan pelaku UMKM pengguna *e-payment* dan menilai persepsi penipuan sebagai keluaran, sehingga temuan Chen et al. (2026) berfungsi memperjelas bahwa kesadaran perlu dibedakan dari kemampuan bertindak serta hasil penilaian risiko.

2. Aljaradat dan Shukla (2026)

Aljaradat dan Shukla (2026) mengembangkan model pembentukan kepercayaan dan perilaku penggunaan pembayaran digital dengan menggabungkan risiko keamanan siber yang dipersepsikan, pengaruh sosial, ekspektasi usaha, mekanisme penanganan pengaduan, kepercayaan, ekspektasi kinerja, dan perilaku penggunaan. Kepercayaan dipahami sebagai penilaian pengguna terhadap keterandalan dan keamanan sistem, bukan sekadar rasa nyaman ketika bertransaksi. Model tersebut juga memperhitungkan pengalaman kejahatan siber, usia, dan tingkat pendidikan sebagai kondisi yang dapat mengubah kekuatan hubungan antarkonstruksi. Fokus itu memberi gambaran bahwa kepercayaan terhadap pembayaran digital dibentuk oleh pengalaman,

kemudahan, dukungan sosial, dan kualitas perlindungan institusional secara bersamaan.

Data dikumpulkan pada 17 kota di sembilan negara bagian dan wilayah India Utara melalui teknik purposive sampling bertahap. Responden harus memiliki rekening bank aktif dan pernah menggunakan pembayaran digital. Sebanyak 850 respons terkumpul, lalu 732 respons dipertahankan setelah penyaringan terhadap kelengkapan jawaban, konsistensi, dan aktivitas transaksi. Instrumen disusun dalam bahasa Inggris dan Hindi, diuji melalui telaah ahli, uji keterbacaan, serta studi pendahuluan. Analisis *structural equation modelling* menunjukkan bahwa model mampu menjelaskan 44% variasi kepercayaan, 49% variasi ekspektasi kinerja, dan 67% variasi perilaku penggunaan. Risiko keamanan siber berhubungan negatif dengan kepercayaan, sedangkan pengaruh sosial dan ekspektasi usaha berhubungan positif dengan kepercayaan. Kepercayaan berhubungan positif dengan ekspektasi kinerja, tetapi pengaruh langsungnya terhadap perilaku penggunaan tidak terbukti secara statistik.

Relevansi penelitian tersebut terletak pada penjelasan mengenai proses terbentuknya kepercayaan pada *e-payment* melalui keamanan, kemudahan, dukungan sosial, dan kinerja penyedia layanan. Penelitian ini tidak menempatkan perilaku penggunaan sebagai variabel dependen, tetapi menguji kepercayaan terhadap persepsi penipuan keuangan online. Perbedaan tujuan itu membuat kepercayaan tidak dapat dipahami hanya sebagai pendorong penggunaan; kepercayaan juga perlu dilihat dari keyakinan terhadap perlindungan data, ketepatan layanan, transparansi informasi, dan penyelesaian pengaduan. Temuan

Aljaradat dan Shukla (2026) membantu membatasi konsep kepercayaan agar tidak berubah menjadi kepercayaan berlebihan yang menghilangkan kewaspadaan.

3. Widjanarko et al. (2025)

Widjanarko et al. (2025) menganalisis hubungan *digital financial literacy*, *financial stress*, *financial behavior*, dan *awareness of investment scam* pada 400 orang dewasa muda Indonesia berusia 20–40 tahun yang aktif menggunakan media sosial. *Theory of Planned Behavior* digunakan untuk menerangkan bagaimana pengetahuan keuangan digital dan kebiasaan keuangan membentuk penilaian terhadap risiko, sedangkan *Stress and Coping Theory* menjelaskan respons individu ketika menghadapi tekanan finansial. Penelitian memakai pendekatan kuantitatif asosiatif dan *PLS-SEM* melalui *SmartPLS*. *Digital financial literacy* mencakup kemampuan memahami layanan keuangan digital, menilai informasi, serta mengenali konsekuensi transaksi. *Financial behavior* ditempatkan sebagai variabel pemoderasi karena perilaku pengelolaan keuangan dapat menentukan apakah pengetahuan yang dimiliki benar-benar digunakan ketika individu menilai penawaran investasi yang mencurigakan.

Hasil pengujian menunjukkan bahwa *digital financial literacy*, *financial stress*, dan *financial behavior* memengaruhi *awareness of investment scam*. *Financial behavior* memperkuat pengaruh literasi keuangan digital terhadap kesadaran penipuan dan mengurangi pengaruh tekanan keuangan terhadap kesadaran tersebut. Temuan ini menunjukkan bahwa pengetahuan tidak bekerja secara terpisah dari kebiasaan sehari-hari; kemampuan memahami risiko menjadi lebih efektif ketika disertai perilaku memeriksa informasi, mempertimbangkan

konsekuensi, dan mengendalikan keputusan keuangan. Persamaan dengan penelitian ini terdapat pada penggunaan literasi keuangan digital sebagai variabel penjelas, kesadaran penipuan sebagai keluaran yang berdekatan secara konseptual, konteks Indonesia, dan metode *PLS-SEM*. Perbedaannya terletak pada fokus penipuan investasi, penggunaan dewasa muda pengguna media sosial, serta keberadaan variabel tekanan dan perilaku keuangan. Penelitian ini mengarahkan pembahasan pada penipuan melalui *e-payment* yang dihadapi pelaku UMKM, sehingga cakupan risikonya meliputi transaksi, tautan palsu, penyalahgunaan data, dan manipulasi pembayaran.

4. Puri et al. (2025)

Puri et al. (2025) mengkaji faktor yang mendorong maupun menghambat perilaku aman ketika pengguna menghadapi penipuan keuangan digital pada sistem pembayaran digital. *Behavioral Reasoning Theory* digunakan untuk menerangkan bahwa keputusan tidak hanya dibentuk oleh alasan yang mendukung suatu tindakan, tetapi juga oleh alasan yang membuat seseorang enggan melakukan tindakan tersebut. Konstruk pendorong mencakup keyakinan, kepercayaan, efikasi diri, motivasi hedonis, norma injungtif, pusat kendali, dan efikasi respons. Hambatan dianalisis melalui kesadaran teknologi dan risiko yang dipersepsikan. Niat perilaku ditempatkan sebagai penghubung antara alasan yang dimiliki pengguna dan perilaku pencegahan yang benar-benar dilakukan.

Data diperoleh melalui kuesioner terstruktur kepada pengguna transaksi digital dan dianalisis dalam dua tahap. *Structural equation modelling* digunakan untuk menguji hubungan linear antarkonstruk dan menilai kesesuaian model

teoritis. Analisis neural network digunakan setelahnya untuk membaca urutan kepentingan relatif prediktor ketika hubungan yang terbentuk tidak sepenuhnya linear. Kombinasi SEM dan *artificial neural network* membuat penelitian tersebut tidak hanya menyatakan apakah suatu variabel berpengaruh, tetapi juga menunjukkan konstruk mana yang memiliki daya prediksi paling kuat terhadap perilaku aman.

Hasil penelitian memperlihatkan bahwa keyakinan, kepercayaan, efikasi diri, dan motivasi hedonis meningkatkan niat pengguna untuk mengambil langkah pencegahan. Niat perilaku menjadi prediktor paling kuat terhadap tindakan pencegahan, diikuti oleh motivasi hedonis, efikasi diri, norma injungtif, pusat kendali, kepercayaan, dan efikasi respons. Kesadaran teknologi dan hambatan risiko tidak menunjukkan pengaruh positif yang kuat. Pola tersebut memperlihatkan bahwa mengetahui keberadaan teknologi atau menyadari adanya risiko belum tentu cukup untuk menghasilkan perilaku perlindungan apabila pengguna tidak memiliki kepercayaan, keyakinan kemampuan, dan alasan yang mendorong tindakan.

Hubungan penelitian Puri et al. (2025) dengan penelitian ini berada pada konstruk kepercayaan, penipuan digital, dan respons terhadap transaksi yang berisiko. Kepercayaan pada penelitian ini diarahkan pada keyakinan terhadap keamanan, tanggung jawab, dan kemampuan penyedia *e-payment* menangani masalah. Arah positif hipotesis dapat diterangkan ketika kepercayaan tersebut membuat pengguna bersedia mengikuti notifikasi keamanan, melakukan verifikasi, dan menggunakan saluran pengaduan. Perbedaannya terletak pada

penggunaan *Behavioral Reasoning Theory*, keluaran berupa niat serta perilaku pencegahan, dan teknik *SEM-ANN*. Penelitian ini menempatkan persepsi penipuan keuangan online sebagai variabel dependen dan memakai *PLS-SEM*, sehingga temuan Puri et al. memberi dasar perilaku tanpa menyamakan persepsi risiko dengan tindakan aktual.

5. Pelawi et al. (2025)

Pelawi et al. (2025) menelaah kemungkinan individu menjadi korban penipuan melalui sudut pandang perilaku, bukan hanya karakteristik demografis. *Signal Detection Theory* digunakan untuk menjelaskan proses ketika seseorang harus membedakan sinyal penipuan dari informasi yang tampak normal di tengah ketidakpastian. Model penelitian memuat *fraud exposure* sebagai sumber paparan, *fraud victimization* sebagai akibat, *vigilance* sebagai variabel yang memperlemah hubungan paparan dan viktimisasi, serta *financial literacy* sebagai faktor yang meningkatkan kewaspadaan. Data survei berasal dari 671 responden Indonesia dan dianalisis menggunakan *PLS-SEM*.

Hasil pengujian menunjukkan bahwa paparan terhadap aktivitas penipuan meningkatkan kemungkinan viktimisasi. *Vigilance* memperlemah hubungan tersebut, yang berarti responden dengan kewaspadaan lebih tinggi lebih mampu mengenali tanda penipuan sebelum mengambil tindakan yang merugikan. *Financial literacy* berhubungan positif dengan *vigilance*, tetapi daya prediksinya relatif rendah. Temuan itu menunjukkan bahwa literasi memberikan dasar untuk memahami transaksi dan risiko, sedangkan kemampuan mendeteksi penipuan

tetap dipengaruhi oleh perhatian, pengalaman, kebiasaan memeriksa informasi, dan situasi saat keputusan dibuat.

Kedekatan penelitian Pelawi et al. (2025) dengan penelitian ini terlihat pada konteks Indonesia, penggunaan *PLS-SEM*, pembahasan literasi keuangan, dan perhatian terhadap kemampuan mengenali penipuan. Penelitian Pelawi mengukur pengalaman viktimisasi aktual serta menempatkan kewaspadaan sebagai pemoderasi, sedangkan penelitian ini mengukur persepsi penipuan dan memisahkan *fraud awareness* dari literasi keuangan digital. Pemisahan tersebut diperlukan karena pelaku UMKM dapat memahami produk keuangan digital tetapi belum tentu mengenali manipulasi sosial, pesan palsu, atau permintaan data rahasia. Temuan Pelawi et al. memberi dasar bahwa literasi dan kewaspadaan bekerja saling melengkapi, tetapi tidak dapat dipertukarkan sebagai konstruk yang sama.

6. Balakrishnan et al. (2025)

Balakrishnan et al. (2025) mengidentifikasi prediktor viktimisasi penipuan online dengan kerangka *personal, environmental, and behavioral* yang diturunkan dari *Social Cognitive Theory*. Penelitian dilakukan melalui dua tahap pada orang dewasa Malaysia. Studi pertama melibatkan 820 responden dan digunakan untuk menemukan struktur faktor melalui *exploratory factor analysis* serta menguji prediktor melalui *hierarchical binary logistic regression*. Studi kedua melibatkan 629 responden dan berfungsi memvalidasi model pada periode pengumpulan data yang berbeda. Lima faktor yang terbentuk ialah *self-awareness, safe practice, bank trust, overconfidence*, dan *social influence*. Penggunaan dua kumpulan data

memberi kekuatan pada penelitian karena hasil awal tidak langsung dianggap berlaku sebelum diuji kembali pada sampel lain.

Hasil kedua studi secara konsisten menunjukkan bahwa *overconfidence* dan *social influence* meningkatkan kemungkinan viktimisasi penipuan online. Jenis kelamin juga menjadi prediktor pada studi kedua, dengan responden perempuan menunjukkan risiko lebih tinggi pada sampel tersebut. *Self-awareness*, *safe practice*, dan *bank trust* tidak menjadi prediktor langsung setelah variabel lain diperhitungkan, walaupun sebagian besar responden menyatakan telah mengetahui isu privasi digital. Temuan ini memperlihatkan adanya jarak antara merasa sadar dan benar-benar mampu menghindari manipulasi. Persamaan dengan penelitian ini terletak pada pembahasan kesadaran, kepercayaan terhadap lembaga atau sistem keuangan, dan risiko penipuan. Perbedaannya terdapat pada variabel dependen berupa viktimisasi, metode regresi logistik, serta responden Malaysia. Penelitian ini menguji persepsi penipuan pada pelaku UMKM pengguna *e-payment* dan memaknai kepercayaan sebagai keyakinan rasional terhadap keamanan serta mekanisme perlindungan, bukan *overconfidence* terhadap kemampuan pribadi.

7. Kraiwanit et al. (2025)

Kraiwanit et al. (2025) menganalisis faktor yang memprediksi pengalaman penipuan digital pada masyarakat Thailand sebagai salah satu ekonomi berkembang dengan penggunaan layanan digital yang cepat. Variabel penelitian mencakup karakteristik demografis, pola penggunaan teknologi, jenis perangkat dan sistem operasi, intensitas media sosial, manfaat transaksi digital yang

dipersepsikan, fitur keamanan digital yang dipersepsikan, serta pengalaman penipuan. Variabel dependen dibentuk secara biner berdasarkan pernah atau tidaknya responden mengalami penipuan digital. Pendekatan tersebut memungkinkan penelitian membandingkan kontribusi faktor sosial, ekonomi, dan teknologi terhadap peluang viktimisasi.

Survei dilakukan terhadap 1.200 responden dan dianalisis menggunakan regresi logistik biner. Instrumen melalui proses validasi isi serta uji coba kepada 30 partisipan sebelum pengumpulan data utama. Reliabilitas skala mencapai nilai Cronbach's alpha 0,896. Sebanyak 70,3% responden melaporkan pernah mengalami penipuan digital, menunjukkan tingginya paparan pada sampel penelitian. Seluruh variabel yang telah ditetapkan secara teoritis dimasukkan ke dalam model tanpa seleksi otomatis agar hasil tetap mencerminkan kerangka konseptual yang dirancang.

Usia yang lebih tinggi, pendapatan yang lebih besar, status mahasiswa, penggunaan perangkat portabel, dan keterlibatan media sosial meningkatkan peluang viktimisasi. Pengguna *iOS* menunjukkan peluang yang lebih rendah dibandingkan kelompok pembandingan, sedangkan durasi penggunaan internet tidak terbukti sebagai prediktor utama. Temuan yang menonjol ialah persepsi keamanan digital yang lebih kuat justru berkaitan dengan risiko penipuan yang lebih tinggi. Pola tersebut menunjukkan kemungkinan *security confidence paradox*, yaitu rasa aman terhadap kata sandi, autentikasi, atau peringatan penipuan dapat membuat sebagian pengguna mengurangi pemeriksaan kritis terhadap transaksi.

Kaitan dengan penelitian ini muncul pada penggunaan transaksi digital, perhatian terhadap keamanan, dan kemungkinan kepercayaan yang tidak disertai kewaspadaan. Perbedaan utamanya ialah penelitian Kraiwanit et al. (2025) menggunakan banyak prediktor demografis dan teknologi untuk menjelaskan viktimisasi aktual, sedangkan penelitian ini memusatkan model pada *fraud awareness*, literasi keuangan digital, serta kepercayaan pada *e-payment* untuk menjelaskan persepsi penipuan. Temuan paradoks keamanan menjadi pembatas konseptual agar kepercayaan pada *e-payment* tidak diartikan sebagai keyakinan tanpa evaluasi. Kepercayaan yang sehat perlu didasarkan pada pemahaman fitur, kemampuan membaca peringatan, dan kesediaan melakukan verifikasi.

8. Umar dan Dalimunthe (2024)

Umar dan Dalimunthe (2024) menguji pengaruh *financial literacy* dan *digital literacy* terhadap *investment scam awareness* dengan *cybercrime awareness* sebagai variabel mediasi. Penelitian melibatkan 288 mahasiswa dari perguruan tinggi yang tersebar di 38 provinsi Indonesia. Data diperoleh melalui kuesioner daring dan dianalisis menggunakan *SEM-PLS*. Pemisahan literasi keuangan dan literasi digital memungkinkan peneliti melihat apakah pemahaman terhadap konsep keuangan serta kemampuan menggunakan dan mengevaluasi teknologi memiliki jalur yang berbeda menuju kesadaran penipuan investasi.

Hasil penelitian menunjukkan bahwa *financial literacy* dan *digital literacy* memiliki pengaruh tidak langsung terhadap *investment scam awareness* melalui *cybercrime awareness*. Pengetahuan keuangan maupun kemampuan digital baru membentuk kesadaran penipuan ketika keduanya membantu responden mengenali

cara kerja ancaman siber, tanda manipulasi, dan potensi penyalahgunaan informasi. Pengaruh literasi keuangan juga berbeda antara mahasiswa dengan latar belakang pendidikan ekonomi dan nonekonomi. Perbedaan tersebut memperlihatkan bahwa pengetahuan formal dapat memengaruhi cara individu mengolah informasi keuangan, tetapi pengalaman dan paparan digital tetap diperlukan agar penilaian risiko menjadi lebih tajam.

Persamaan dengan penelitian ini terdapat pada konteks Indonesia, penggunaan data primer, *SEM-PLS*, serta keterkaitan literasi dengan kesadaran penipuan. Penelitian Umar dan Dalimunthe memisahkan *financial literacy* dan *digital literacy*, sedangkan penelitian ini menggabungkannya sebagai literasi keuangan digital yang mencakup pengetahuan produk, penggunaan teknologi, perlindungan data, dan pengelolaan risiko. Responden mahasiswa serta fokus penipuan investasi juga berbeda dari pelaku UMKM pengguna *e-payment*. Temuan penelitian ini tetap relevan karena menunjukkan bahwa kemampuan finansial dan digital tidak otomatis menghasilkan persepsi ancaman tanpa adanya proses pengenalan terhadap kejahatan siber.

9. Kubilay et al. (2023)

Kubilay et al. (2023) mengembangkan ukuran *scam identification ability* menggunakan pesan SMS penipuan dan pesan resmi yang benar-benar beredar di Kenya. Sebanyak 1.000 responden mengikuti survei daring dan diminta mengklasifikasikan 12 pesan sebagai penipuan atau bukan penipuan, disertai penilaian keyakinan atas setiap jawaban. Enam pesan pertama digunakan untuk mengukur kemampuan awal. Separuh responden kemudian menerima edukasi

singkat mengenai ciri umum penipuan, seperti kesalahan bahasa, pengirim tidak dikenal, tautan pendek, serta permintaan PIN atau kata sandi, sebelum mengklasifikasikan enam pesan berikutnya. Desain eksperimen tersebut mengukur ketepatan, bukan sekadar rasa waspada, karena responden dapat melakukan dua jenis kesalahan: gagal mengenali penipuan atau salah menilai pesan asli sebagai penipuan.

Kemampuan awal responden rata-rata mencapai 71% dari seluruh pesan, dengan tingkat ketepatan 74% untuk pesan penipuan dan 66% untuk pesan asli. Edukasi singkat tidak meningkatkan *scam identification ability* secara rata-rata. Responden menjadi lebih baik dalam mengenali pesan penipuan, tetapi juga lebih sering menganggap pesan asli sebagai penipuan. Temuan tersebut menunjukkan bahwa kewaspadaan yang terlalu umum dapat menghasilkan *overcaution* dan menurunkan ketepatan penilaian. Penelitian ini memiliki kedekatan pada variabel persepsi penipuan keuangan online, khususnya penilaian ancaman dan kemampuan memeriksa transaksi mencurigakan. Perbedaannya berada pada desain eksperimen, penggunaan SMS Kenya, dan pengukuran klasifikasi pesan. Penelitian ini menggunakan survei pelaku UMKM untuk menilai persepsi terhadap risiko *e-payment*, sehingga hasil Kubilay et al. (2023) membantu menegaskan bahwa persepsi yang baik bukan hanya tinggi atau rendah, tetapi juga realistis dan didasarkan pada kemampuan membedakan transaksi aman dari transaksi berbahaya.

10. DeLiema dan Mottola (2023)

DeLiema, Li, dan Mottola (2023) mengidentifikasi faktor yang berhubungan dengan respons terhadap penawaran penipuan dan kemungkinan kehilangan uang setelah individu merespons. Data berasal dari 1.375 konsumen Amerika Serikat dan Kanada yang sebelumnya melaporkan pengalaman penipuan kepada organisasi pengaduan konsumen di Amerika Utara. Penelitian membedakan empat kategori, yaitu *opportunity-based scams*, *threat-based scams*, *consumer purchase scams*, dan *phishing scams*. Pemisahan ini penting karena strategi pelaku, tekanan psikologis, serta bentuk kerugian pada setiap jenis penipuan tidak sama.

Dua tahapan hasil dianalisis secara terpisah. Tahap pertama menilai apakah konsumen merespons atau mengabaikan penawaran penipuan. Tahap kedua menilai apakah konsumen yang merespons kemudian mengalami kerugian finansial. Variabel penjelas meliputi pengetahuan awal tentang penipuan, literasi keuangan, kesulitan finansial, kesepian, pendidikan, pendapatan, jenis kelamin, ras, dan karakteristik demografis lain. Perbedaan tahapan tersebut menghindari anggapan bahwa seluruh orang yang merespons pasti menjadi korban, karena sebagian individu dapat menghentikan interaksi sebelum menyerahkan uang atau informasi.

Hasil penelitian menunjukkan bahwa peluang merespons dan peluang kehilangan uang berbeda menurut jenis penipuan. *Consumer purchase scams* memiliki peluang viktimisasi paling tinggi, sedangkan *threat-based scams* dan *phishing* lebih jarang memperoleh respons dibandingkan *opportunity-based*

scams. Faktor risiko juga tidak seragam pada setiap kategori. Pengetahuan mengenai modus penipuan sebelum seseorang menjadi sasaran menjadi faktor perlindungan pada hampir seluruh jenis penipuan. Literasi keuangan, tekanan finansial, dan karakteristik individu menunjukkan hubungan yang berbeda-beda, sehingga tidak terdapat satu profil korban yang dapat menjelaskan seluruh bentuk penipuan.

Kedekatan dengan penelitian ini terletak pada *fraud awareness* dan literasi keuangan sebagai dasar untuk menilai risiko sebelum kerugian terjadi. Penelitian DeLiema et al. (2023) berfokus pada respons serta viktimisasi konsumen di Amerika Utara, sedangkan penelitian ini menilai persepsi penipuan keuangan online pada pelaku UMKM pengguna *e-payment* di Indonesia. Perbedaan tersebut memperlihatkan ruang penelitian pada tahap sebelum viktimisasi, yaitu ketika pelaku usaha membentuk penilaian atas ancaman berdasarkan kesadaran modus, literasi keuangan digital, dan kepercayaan terhadap sistem pembayaran. Penggunaan persepsi sebagai variabel dependen memungkinkan penelitian ini membaca kesiapan kognitif pengguna tanpa mensyaratkan responden pernah mengalami kerugian.

11. Ravikumar et al. (2022)

Ravikumar et al. (2022) mengembangkan dan memvalidasi skala Literasi Keuangan Digital pada orang dewasa pengguna layanan keuangan digital di India. Penelitian tersebut berangkat dari belum adanya kesepakatan mengenai dimensi yang dapat menggambarkan Literasi Keuangan Digital secara utuh. Literasi Keuangan Digital dipahami sebagai konstruk multidimensi yang menggabungkan

pengetahuan keuangan, kemampuan menggunakan teknologi, pemahaman terhadap layanan keuangan digital, pengenalan risiko, perlindungan pengguna, serta kemampuan menerapkan pengetahuan ketika mengambil keputusan keuangan (Ravikumar et al., 2022).

Penelitian menggunakan rancangan deskriptif dan korelasional dengan pendekatan survei *cross-sectional*. Populasinya adalah orang dewasa pengguna layanan keuangan digital di Bangalore, India. Kuesioner disebarluaskan melalui Google Form kepada 828 orang dan memperoleh 391 respons. Sebanyak 387 respons dinyatakan lengkap, lalu 384 respons pertama yang memenuhi persyaratan dipakai sebagai sampel penelitian. Penentuan jumlah sampel mengacu pada formula Krejcie dan Morgan, sedangkan instrumen penelitian menggunakan skala Likert untuk mengukur 47 pernyataan yang dikembangkan dari berbagai dimensi Literasi Keuangan Digital (Ravikumar et al., 2022).

Proses pengembangan instrumen dilakukan melalui penelaahan literatur, penilaian ahli, studi pendahuluan, dan pengujian reliabilitas. Nilai Cronbach's Alpha keseluruhan skala mencapai 0,923. Data utama dianalisis menggunakan *Exploratory Factor Analysis*, *parallel analysis*, dan *Confirmatory Factor Analysis*. Nilai KMO sebesar 0,838 serta hasil Bartlett's Test yang berada di bawah 0,05 menunjukkan bahwa data memenuhi persyaratan analisis faktor. Dua belas faktor yang dipertahankan mampu menjelaskan 70,87% variasi pada skala Literasi Keuangan Digital (Ravikumar et al., 2022).

Dua belas faktor yang terbentuk mencakup kualitas layanan keuangan digital, pengetahuan mengenai layanan dan penyedia keuangan digital, kesadaran

serta pengendalian risiko keuangan digital, pengetahuan digital, penerapan pengetahuan dan keterampilan, kecakapan digital, kemauan menggunakan pengetahuan, kesadaran keamanan digital, sikap keuangan positif, pengetahuan keuangan berdasarkan norma gender, perilaku keuangan rasional, dan pengetahuan keuangan. Hasil CFA menunjukkan tingkat kesesuaian model yang dapat diterima. Tingkat Literasi Keuangan Digital secara umum berbeda menurut tingkat pendidikan, sedangkan beberapa dimensi tertentu juga menunjukkan perbedaan berdasarkan usia, status perkawinan, dan pendapatan responden (Ravikumar et al., 2022).

Penelitian Ravikumar et al. menjadi dasar pengukuran Literasi Keuangan Digital pada penelitian ini, terutama melalui dimensi pengetahuan layanan keuangan digital, kesadaran risiko keuangan digital, pengendalian risiko, dan pengetahuan mengenai hak pengguna. Perbedaan objek terlihat pada penggunaan orang dewasa pengguna seluruh layanan keuangan digital di India, sedangkan penelitian ini membatasi responden pada pelaku UMKM yang menggunakan *e-payment* untuk kegiatan usaha. Ravikumar et al. juga berfokus pada pembentukan dan validasi skala, bukan menguji pengaruh Literasi Keuangan Digital terhadap Persepsi Penipuan Keuangan Online. Ruang tersebut ditempatkan sebagai salah satu pembeda penelitian ini.

12. Sleiman et al. (2021)

Sleiman et al. (2021) menganalisis faktor-faktor yang membentuk kepercayaan dan penerimaan sistem pembayaran seluler pada pengguna Alipay dan WeChat Pay di Tiongkok. Kerangka penelitian dikembangkan dari

Technology Acceptance Model dengan memasukkan keamanan, reputasi, pengawasan pemerintah, kepercayaan, risiko, mobilitas, norma subjektif, kesenangan, kemudahan penggunaan, kegunaan, dan niat perilaku. Kepercayaan diukur sebagai keyakinan bahwa layanan pembayaran seluler memiliki kompetensi dalam menangani transaksi, memberikan layanan yang andal, dan dapat dipercaya saat digunakan (Sleiman et al., 2021).

Survei daring diberikan kepada pengguna yang memiliki pengalaman menggunakan Alipay atau WeChat Pay di Kota Xi'an. Penelitian memperoleh 373 kuesioner yang layak dianalisis setelah melalui pengumpulan data selama sekitar tiga bulan. Sebelum penyebaran utama, instrumen diuji kepada 50 pengguna untuk memeriksa validitas dan reliabilitas item. Empat pernyataan dihapus dan beberapa item diperbaiki berdasarkan hasil uji awal serta masukan dari dua ahli. Jawaban diukur menggunakan skala Likert lima poin, mulai dari Sangat Tidak Setuju sampai Sangat Setuju. Analisis dilakukan melalui EFA, CFA, analisis jalur, dan SEM, disertai pengujian reliabilitas menggunakan Cronbach's Alpha, Composite Reliability, dan Average Variance Extracted (Sleiman et al., 2021).

Hasil penelitian menunjukkan bahwa pengawasan pemerintah menjadi faktor terkuat yang meningkatkan kepercayaan pada pembayaran seluler, dengan koefisien jalur sebesar 0,934. Reputasi dan keamanan juga berpengaruh positif terhadap kepercayaan, masing-masing dengan koefisien 0,592 dan 0,472. Kepercayaan selanjutnya berpengaruh positif terhadap persepsi kegunaan layanan. Risiko yang dipersepsikan berpengaruh negatif terhadap niat menggunakan pembayaran seluler, sedangkan kegunaan, kemudahan,

kesenangan, dan pengawasan pemerintah meningkatkan niat perilaku pengguna. Hasil tersebut menunjukkan bahwa kepercayaan terhadap pembayaran digital tidak hanya dibentuk oleh kemampuan teknis sistem, tetapi juga oleh reputasi penyedia dan keberadaan perlindungan kelembagaan (Sleiman et al., 2021).

Keterkaitan penelitian Sleiman et al. dengan penelitian ini terdapat pada penggunaan TAM, pembahasan kepercayaan, dan objek berupa sistem pembayaran digital. Tiga item *perceived trust* digunakan sebagai dasar pengembangan instrumen Kepercayaan pada *E-Payment*. Perbedaannya terdapat pada posisi variabel dan tujuan pengujian. Sleiman et al. menempatkan kepercayaan sebagai konstruk yang dibentuk oleh keamanan, reputasi, pengawasan pemerintah, dan mobilitas serta menghubungkannya dengan kegunaan layanan. Penelitian ini menempatkan Kepercayaan pada *E-Payment* sebagai variabel independen yang diuji terhadap Persepsi Penipuan Keuangan Online pada pelaku UMKM di Indonesia.

13. Williams dan Joinson (2020)

Williams dan Joinson (2020) mengembangkan dan memvalidasi instrumen berbasis *Protection Motivation Theory* untuk mengukur persepsi pengguna terhadap ancaman *phishing* dan kecenderungan mencari informasi perlindungan. Konstruk yang diuji meliputi kemampuan mengenali *phishing*, persepsi keseriusan, persepsi kerentanan, efikasi diri, biaya respons, dan efikasi respons. Persepsi keseriusan menjelaskan penilaian mengenai beratnya konsekuensi ketika menjadi korban, sedangkan persepsi kerentanan menunjukkan penilaian individu mengenai kemungkinan serta risiko dirinya menjadi sasaran *phishing*.

Pengembangan instrumen dilakukan melalui dua studi. Studi pertama melibatkan 150 respons yang layak dianalisis dan menggunakan analisis faktor eksploratori untuk memperoleh susunan item akhir. Studi kedua melibatkan 157 responden dan menerapkan analisis faktor konfirmatori terhadap instrumen yang telah disempurnakan. Hasil validasi menghasilkan 22 item pada enam konstruk dengan konsistensi internal yang memadai. Subskala persepsi keseriusan memiliki Cronbach's Alpha sebesar 0,86, sedangkan subskala persepsi kerentanan mencapai 0,90. Pengujian lanjutan juga menggunakan kuis klasifikasi surel untuk membandingkan persepsi pengguna dengan kemampuan aktual mengenali *phishing*.

Hasil penelitian menunjukkan bahwa persepsi keseriusan berhubungan positif dengan niat untuk mengikuti perkembangan informasi mengenai teknik *phishing*, sedangkan persepsi kerentanan menunjukkan hubungan negatif dengan niat tersebut. Seluruh konstruk berbasis PMT tidak terbukti memprediksi kemampuan aktual membedakan surel *phishing* dan surel asli. Kedekatan penelitian Williams dan Joinson dengan penelitian ini terletak pada penggunaan persepsi keseriusan dan persepsi kerentanan sebagai dasar pengukuran Persepsi Penipuan Keuangan Online. Perbedaannya terdapat pada objek *phishing* melalui surel, responden umum di Inggris, Amerika Serikat, dan Kanada, serta keluaran berupa niat mencari informasi dan kemampuan klasifikasi. Penelitian ini mengadaptasi kedua dimensi tersebut pada transaksi *e-payment* pelaku UMKM di Indonesia.

Tabel 2.1 Matriks Research GAP

No.	Penelitian	Tahun	<i>Fraud Awareness</i>	Literasi Keuangan Digital	Kepercayaan pada E-Payment	Persepsi Penipuan Keuangan Online
1	Chen et al.	2026	S+			S+
2	Aljaradat & Shukla	2026			TS	
3	Widjanarko et al.	2025		S+		S+
4	Puri et al.	2025			S+	
5	Pelawi et al.	2025	S-	S+		
6	Balakrishnan et al.	2025	TS		TS	
7	Kraiwanit et al.	2025				
8	Umar & Dalimunthe	2024	S+	S+		S+
9	Kubilay et al.	2023	TS			TS
10	DeLiema & Mottola	2023	S-	S-		
11	Ravikumar et al.	2022		S+		
12	Sleiman et al.	2021			S+	
13	Williams & Joinson	2020				S+ / S- / TS

Keterangan: S+ = Signifikan Positif; S- = Signifikan Negatif; TS = Tidak Signifikan; kolom kosong = variabel tidak diuji. Pada Williams dan Joinson (2020), kode S+ / S- / TS menunjukkan hasil yang berbeda menurut dimensi persepsi dan keluaran pengujian.

2.2 Landasan Teori

2.2.1 *Theory of Planned Behavior*

Theory of Planned Behavior (TPB) menjelaskan bahwa perilaku seseorang tidak muncul secara tiba-tiba, melainkan didahului oleh niat yang terbentuk dari sikap terhadap perilaku, norma subjektif, dan kontrol perilaku yang dipersepsikan. Sikap bersumber dari keyakinan mengenai manfaat atau konsekuensi yang mungkin timbul ketika suatu tindakan dilakukan. Norma subjektif menggambarkan penilaian terhadap dukungan atau tekanan sosial, sedangkan kontrol perilaku menunjukkan keyakinan seseorang mengenai kemampuan, kesempatan, dan sumber daya yang tersedia untuk melakukan tindakan tersebut. Ketiga unsur itu bekerja melalui kumpulan keyakinan yang

spesifik terhadap perilaku yang sedang dinilai sehingga penerapan TPB harus selalu disesuaikan dengan objek dan situasi keputusan yang diteliti (Ajzen, 1991).

Pembentukan niat pada TPB dimulai ketika individu menilai informasi yang diterimanya, menghubungkan informasi tersebut dengan pengalaman, lalu memperkirakan akibat dari pilihan yang akan diambil. Kontrol perilaku yang dipersepsikan tidak hanya berperan melalui niat, tetapi juga dapat berkaitan langsung dengan tindakan apabila penilaian kemampuan individu sesuai dengan kendali aktual yang dimilikinya. Perkembangan kajian TPB memperlihatkan bahwa unsur tambahan dapat digunakan selama posisi konseptualnya jelas dan tidak menghilangkan hubungan antara keyakinan, penilaian, niat, dan tindakan. Kerangka ini membuat TPB dapat digunakan untuk membaca keputusan pada lingkungan digital yang memiliki perubahan cepat, informasi yang tidak selalu lengkap, serta tingkat risiko yang berbeda-beda (Bosnjak et al., 2020).

Fraud awareness ditempatkan sebagai keyakinan dan pengetahuan mengenai keberadaan modus, tanda bahaya, serta konsekuensi penipuan yang membentuk sikap waspada saat menggunakan layanan pembayaran digital. Pengguna yang memahami pola permintaan kode OTP, tautan palsu, penyamaran identitas, dan manipulasi komunikasi memiliki dasar yang lebih kuat untuk menilai bahwa transaksi tertentu mengandung ancaman. Literasi keuangan digital berkaitan dengan kontrol perilaku yang dipersepsikan karena pengetahuan mengenai cara kerja layanan, pengamanan akun, pemeriksaan informasi, dan prosedur pengaduan membuat pengguna merasa lebih mampu

mengendalikan keputusan transaksi. Norma subjektif tidak dijadikan variabel tersendiri, tetapi pengaruh lingkungan tetap dapat muncul melalui edukasi penyedia layanan, pengalaman komunitas usaha, dan informasi mengenai kasus penipuan yang beredar.

Fungsi TPB pada penelitian ini terletak pada penjelasan mengenai cara pengetahuan, keyakinan, dan kemampuan pengguna membentuk penilaian terhadap ancaman penipuan keuangan online. Variabel dependen tidak diarahkan untuk mengukur perilaku aktual atau pengalaman menjadi korban, melainkan persepsi mengenai kemungkinan, keseriusan, dan konsekuensi penipuan. TPB digunakan untuk menerangkan proses kognitif yang mendahului kehati-hatian, sehingga hubungan *fraud awareness* dan literasi keuangan digital dengan persepsi penipuan dapat dipahami sebagai hasil dari pembentukan sikap serta kontrol atas keputusan transaksi. Pemakaian teori dibatasi pada unsur yang berhubungan dengan model agar penjelasan tidak bergeser menjadi pengujian lengkap terhadap niat dan perilaku yang tidak ditempatkan sebagai konstruk penelitian.

2.2.2 Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) menjelaskan penerimaan teknologi melalui keyakinan mengenai kegunaan dan kemudahan penggunaan. *Perceived usefulness* menggambarkan tingkat kepercayaan bahwa suatu teknologi membantu pengguna menyelesaikan pekerjaan atau transaksi dengan lebih efektif, sedangkan *perceived ease of use* menunjukkan penilaian bahwa teknologi dapat dipelajari dan digunakan tanpa usaha yang berlebihan. Kedua

keyakinan tersebut memengaruhi sikap, niat, dan keputusan untuk menggunakan teknologi. Perkembangan penelitian TAM menunjukkan bahwa model ini tetap banyak digunakan karena mampu menjelaskan penerimaan teknologi sekaligus dapat disesuaikan dengan karakter sistem yang diteliti (Musa et al., 2024).

Layanan *e-payment* memiliki karakter yang berbeda dari teknologi umum karena transaksi melibatkan nilai finansial, penyimpanan data pribadi, ketepatan pemrosesan, serta ketergantungan pada penyedia layanan. Penilaian terhadap kegunaan dan kemudahan belum cukup untuk menerangkan respons pengguna ketika terdapat risiko kebocoran data atau penipuan. Kepercayaan berkembang sebagai keyakinan bahwa penyedia memiliki kemampuan teknis, integritas, transparansi, dan mekanisme perlindungan yang dapat diandalkan. Risiko keamanan siber, pengalaman pengguna, kinerja sistem, serta penanganan pengaduan ikut membentuk kualitas kepercayaan tersebut, sehingga kepercayaan seharusnya dibaca sebagai hasil evaluasi terhadap sistem dan lembaga, bukan sekadar rasa nyaman ketika bertransaksi (Aljaradat & Shukla, 2026).

TAM digunakan untuk menjelaskan posisi kepercayaan pada *e-payment* sebagai keyakinan pengguna terhadap teknologi pembayaran yang diterima dan digunakan. Arah positif terhadap persepsi penipuan dipahami melalui kepercayaan yang berbasis informasi keamanan, peringatan sistem, perlindungan data, dan tanggung jawab penyedia. Pengguna yang mempercayai mekanisme tersebut cenderung memperhatikan notifikasi, mengikuti prosedur verifikasi, dan menggunakan saluran pelaporan ketika menemukan aktivitas

mencurigakan. Kepercayaan yang dimaksud berbeda dari kepercayaan tanpa evaluasi; dasar utamanya terletak pada kemampuan sistem membantu pengguna mengenali dan menangani ancaman. Temuan mengenai perilaku aman pada transaksi digital memberikan dasar bahwa kepercayaan dapat mendorong tindakan perlindungan ketika didukung efikasi diri dan informasi yang memadai (Puri et al., 2025).

2.2.3 *Fraud Awareness*

Fraud awareness merupakan kesadaran individu mengenai keberadaan, bentuk, pola, dan akibat penipuan disertai kemampuan mengenali tanda awal yang menunjukkan adanya manipulasi. Konstruk ini mencakup pengetahuan tentang modus, perhatian terhadap informasi yang tidak wajar, kewaspadaan saat menerima permintaan transaksi, dan kesiapan melakukan pencegahan. Kesadaran tidak cukup diukur dari pengakuan bahwa penipuan dapat terjadi karena seseorang dapat mengetahui adanya ancaman tanpa mampu menentukan ciri yang harus diperiksa. Pengetahuan ancaman perlu diikuti kemampuan menghubungkan pola komunikasi, identitas pengirim, tautan, permintaan data, serta tekanan waktu dengan kemungkinan penipuan. Kajian Chen et al. (2026) memperlihatkan bahwa kesadaran ancaman dan efikasi diri antipenipuan berhubungan dengan perilaku pencegahan, sedangkan kerentanan yang lebih tinggi berkaitan dengan kesadaran dan perlindungan yang lebih rendah.

Posisi *fraud awareness* dibedakan dari persepsi penipuan keuangan online. *Fraud awareness* menjelaskan bekal pengetahuan dan kewaspadaan yang dimiliki pengguna sebelum menilai suatu ancaman, sedangkan persepsi

penipuan menggambarkan hasil penilaian mengenai kemungkinan, keseriusan, dan konsekuensi ancaman pada transaksi digital. Individu yang memahami modus penyamaran, *phishing*, rekayasa sosial, aplikasi palsu, serta penyalahgunaan data mempunyai kerangka pembandingan ketika menghadapi pesan atau transaksi mencurigakan. Pengetahuan mengenai penipuan juga berfungsi sebagai faktor pelindung karena membantu individu menahan respons spontan dan melakukan pemeriksaan sebelum mengambil keputusan (Koning et al., 2024).

2.2.4 Literasi Keuangan Digital

Literasi keuangan digital merupakan kemampuan menggabungkan pengetahuan keuangan, keterampilan menggunakan teknologi, dan pertimbangan keamanan ketika mengambil keputusan melalui layanan digital. Kemampuan tersebut tidak berhenti pada penguasaan fitur aplikasi, tetapi meliputi pemahaman biaya, hak dan kewajiban pengguna, perlindungan data, autentikasi, kredibilitas penyedia, serta konsekuensi transaksi. Perkembangan layanan keuangan membuat pengguna perlu memahami produk sekaligus lingkungan digital tempat produk tersebut diakses. Literasi keuangan pada era digital karena itu memuat dimensi kognitif, teknis, dan perilaku yang saling melengkapi (Koskelainen et al., 2023).

Pengguna yang memiliki literasi keuangan digital mampu membaca informasi transaksi, membandingkan layanan, menilai kewajaran permintaan, dan menentukan langkah ketika terjadi kesalahan atau indikasi penipuan. Keterampilan keamanan terlihat melalui penggunaan kata sandi yang kuat,

perlindungan PIN dan OTP, pembaruan aplikasi, pemeriksaan alamat situs, serta pemanfaatan autentikasi tambahan. Pengetahuan mengenai prosedur pengaduan juga menjadi bagian dari literasi karena perlindungan tidak hanya dilakukan sebelum transaksi, tetapi mencakup tindakan setelah muncul aktivitas mencurigakan. Hubungan antara pengetahuan dan praktik tersebut membedakan literasi yang bersifat fungsional dari kemampuan memakai aplikasi secara rutin (Setiawan et al., 2022).

Literasi keuangan digital membentuk persepsi penipuan melalui kemampuan mengolah informasi risiko secara lebih terarah. Pengguna yang memahami cara kerja pembayaran digital dapat mengenali perbedaan antara gangguan teknis, kesalahan transaksi, dan pola yang mengarah pada penipuan. Penilaian risiko menjadi lebih realistis karena tidak semata-mata didasarkan pada rasa takut atau pengalaman orang lain. Penelitian pada pengguna di Indonesia menunjukkan bahwa literasi keuangan digital berkaitan dengan peningkatan kesadaran terhadap penipuan, sedangkan perilaku keuangan memperkuat kemampuan tersebut. Temuan ini menunjukkan bahwa pengetahuan akan lebih efektif ketika diterapkan melalui kebiasaan memeriksa dan mengendalikan transaksi (Widjanarko et al., 2025).

Posisi literasi keuangan digital pada TPB berhubungan dengan kontrol perilaku yang dipersepsikan. Pengetahuan mengenai fitur, risiko, keamanan, serta prosedur penanganan masalah memberi pengguna keyakinan bahwa dirinya mampu mengendalikan transaksi dan menentukan respons yang tepat. Literasi tidak disamakan dengan *fraud awareness* karena ruang lingkupnya lebih

luas, sedangkan kesadaran penipuan secara khusus berpusat pada pengenalan modus dan tanda ancaman. Kedua konstruk dapat saling menguatkan, tetapi tetap diukur melalui indikator yang berbeda agar pengaruh masing-masing terhadap persepsi penipuan dapat dianalisis secara terpisah (Isaia et al., 2024).

2.2.5 Kepercayaan pada *E-Payment*

Kepercayaan pada *e-payment* merupakan keyakinan pengguna bahwa sistem dan penyedia layanan mempunyai kemampuan, integritas, serta tanggung jawab untuk memproses transaksi secara akurat dan melindungi kepentingan pengguna. Kemampuan berkaitan dengan kualitas teknologi, kestabilan layanan, enkripsi, dan ketepatan pemrosesan. Integritas tampak pada konsistensi antara informasi yang diberikan dengan tindakan penyedia, sedangkan tanggung jawab berkaitan dengan perlindungan data, penanganan gangguan, dan penyelesaian pengaduan. Kepercayaan dapat terbentuk dari pengalaman langsung maupun penilaian terhadap reputasi dan mekanisme institusional yang tersedia (Alrawad et al., 2023).

Pembentukan kepercayaan pada pembayaran digital dipengaruhi oleh penilaian terhadap risiko keamanan siber, manfaat layanan, kemudahan penggunaan, pengaruh sosial, dan kualitas penanganan pengaduan. Mekanisme penyelesaian masalah memberi sinyal bahwa penyedia tidak hanya menyediakan sarana transaksi, tetapi juga mempunyai prosedur ketika pengguna menghadapi kesalahan atau dugaan penipuan. Transparansi mengenai keamanan, notifikasi aktivitas, batas tanggung jawab, dan langkah pemulihan membuat pengguna mempunyai dasar yang lebih objektif untuk menilai perlindungan sistem.

Kepercayaan yang lahir dari informasi tersebut berbeda dari sikap terlalu percaya karena tetap memberi ruang bagi pemeriksaan dan kewaspadaan (Aljaradat & Shukla, 2026).

Hubungan positif antara kepercayaan pada *e-payment* dan persepsi penipuan diarahkan pada kepercayaan yang mendukung penggunaan fitur keamanan dan respons preventif. Pengguna yang yakin bahwa penyedia akan memberikan peringatan, membantu verifikasi, dan menindaklanjuti laporan cenderung lebih siap mengenali serta merespons aktivitas mencurigakan. Rasa percaya tidak dimaknai sebagai anggapan bahwa sistem bebas risiko, melainkan keyakinan bahwa sistem menyediakan sarana untuk memahami dan menangani risiko. Penelitian mengenai perilaku aman pada transaksi digital menunjukkan bahwa kepercayaan bersama efikasi diri dan keyakinan perlindungan dapat mendorong niat melakukan pencegahan penipuan (Puri et al., 2025).

2.2.6 Persepsi Penipuan Keuangan Online

Persepsi penipuan keuangan online merupakan penilaian individu mengenai tingkat kerentanan dirinya terhadap penipuan dan keseriusan konsekuensi yang mungkin timbul. Williams dan Joinson (2020) membagi penilaian ancaman menjadi *perceived vulnerability* dan *perceived severity*. *Perceived vulnerability* menunjukkan kemungkinan atau risiko seseorang menjadi korban, sedangkan *perceived severity* menunjukkan beratnya dampak kehilangan data, pencurian identitas, dan kerugian setelah penipuan terjadi. Kedua dimensi tersebut disesuaikan dengan penggunaan *e-payment* oleh pelaku UMKM, sehingga

persepsi tidak diartikan sebagai pengalaman viktimisasi, tetapi sebagai penilaian atas kemungkinan dan dampak ancaman sebelum kerugian terjadi.

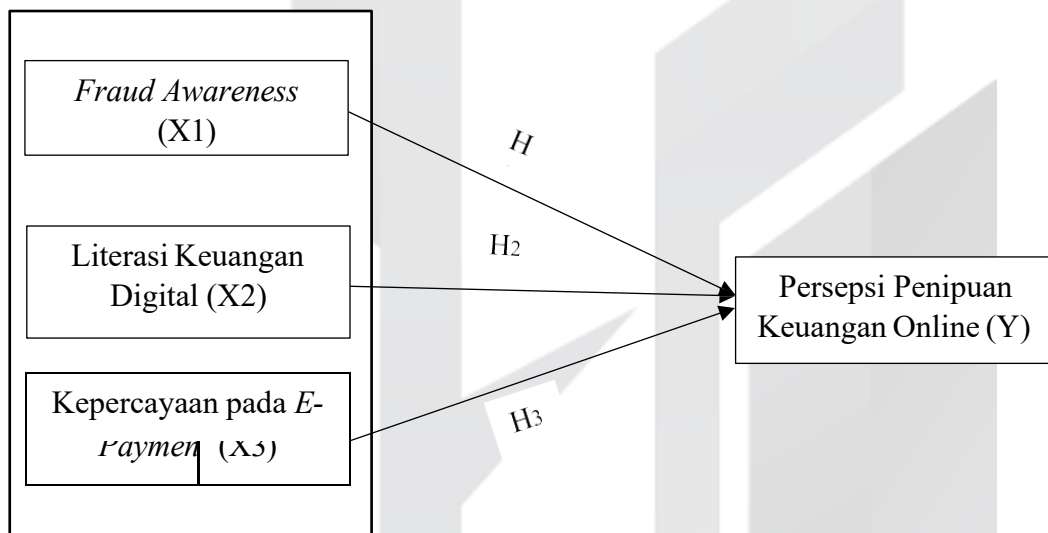
Variabel ini dibedakan dari pengalaman menjadi korban dan kemampuan identifikasi yang berdiri sendiri. Viktimisasi menunjukkan kejadian aktual, sedangkan persepsi merekam cara individu memahami ancaman sebelum atau ketika transaksi berlangsung. Kemampuan mengidentifikasi pesan penipuan menjadi salah satu dasar penilaian, tetapi persepsi juga mencakup kemungkinan kerugian, tingkat ancaman, dan respons yang dianggap tepat. Kubilay et al. (2023) menunjukkan bahwa kemampuan membedakan pesan penipuan dan pesan asli perlu dinilai secara hati-hati karena peningkatan kewaspadaan dapat disertai kesalahan menganggap pesan yang sah sebagai penipuan. Pengukuran persepsi pada penelitian ini diarahkan pada penilaian risiko, ancaman, konsekuensi, verifikasi, dan pelaporan aktivitas mencurigakan.

2.3 Kerangka Berfikir

Kerangka berfikir menggambarkan hubungan antara *fraud awareness*, literasi keuangan digital, kepercayaan pada *e-payment*, dan persepsi penipuan keuangan online. Hubungan tersebut dibangun dari TPB untuk menjelaskan pembentukan keyakinan, sikap waspada, dan kontrol perilaku, serta TAM untuk menjelaskan penerimaan teknologi dan pembentukan kepercayaan terhadap sistem pembayaran digital.

Fraud awareness diperkirakan meningkatkan persepsi penipuan karena pengetahuan mengenai modus dan tanda bahaya membuat individu lebih peka dalam menilai ancaman. Literasi keuangan digital diperkirakan meningkatkan

persepsi penipuan melalui kemampuan memahami layanan, mengevaluasi keamanan, dan menentukan tindakan ketika muncul transaksi mencurigakan. Kepercayaan pada *e-payment* diperkirakan berpengaruh positif ketika kepercayaan dibentuk oleh transparansi, perlindungan, notifikasi keamanan, dan mekanisme pengaduan yang mendorong pengguna memperhatikan serta merespons risiko penipuan.



Gambar 2.1 Kerangka Berfikir

Sumber: Diolah peneliti.

Pada kerangka berfikir di atas, variabel dependen (Y) adalah Persepsi Penipuan Keuangan Online. Variabel Independen terdiri dari beberapa, yaitu *Fraud Awareness* (X1), Literasi Keuangan Digital (X2), dan Kepercayaan pada *E-Payment* (X3).

2.4 Hipotesis Penelitian

Hipotesis merupakan dugaan sementara atau jawaban sementara atas rumusan masalah yang diajukan dalam bentuk pertanyaan penelitian. Hipotesis

ini disusun berdasarkan teori yang relevan, hasil pengamatan, atau temuan dari penelitian sebelumnya, namun belum dibuktikan secara empiris melalui data di lapangan. Oleh karena itu, hipotesis diajukan setelah peneliti menyusun landasan teori dan kerangka berpikir, sehingga menjadi bagian penting dalam proses penelitian kuantitatif secara keseluruhan (Sugiyono, 2023).

2.4.1 Pengaruh *Fraud Awareness* terhadap Persepsi Penipuan Keuangan Online

Fraud awareness menggambarkan kemampuan mengenali pola, komunikasi, dan permintaan transaksi yang berpotensi menipu. Pengetahuan tersebut membentuk keyakinan mengenai konsekuensi transaksi dan membuat pengguna lebih peka terhadap kemungkinan terjadinya kerugian. Semakin tinggi kesadaran terhadap modus penipuan, semakin terarah pula penilaian individu terhadap tingkat ancaman pada transaksi *e-payment*.

TPB menerangkan hubungan tersebut melalui *behavioral beliefs* dan sikap terhadap perilaku. Informasi mengenai modus dan konsekuensi penipuan membentuk keyakinan bahwa verifikasi dan kehati-hatian diperlukan sebelum transaksi dilanjutkan. Chen et al. (2026) menemukan bahwa kesadaran ancaman berhubungan positif dengan perilaku pencegahan penipuan online. Temuan tersebut mendukung dugaan bahwa peningkatan *fraud awareness* akan diikuti oleh persepsi yang lebih tinggi dan lebih tepat terhadap penipuan keuangan online.

H1: *Fraud Awareness* berpengaruh positif terhadap persepsi penipuan keuangan online.

2.4.2 Pengaruh Literasi Keuangan Digital terhadap Persepsi Penipuan Keuangan Online

Literasi keuangan digital memberikan pengetahuan mengenai fungsi layanan, keamanan akun, perlindungan data, serta prosedur yang harus ditempuh ketika muncul transaksi tidak sah. Pengguna yang memahami unsur tersebut mempunyai dasar yang lebih kuat untuk membedakan transaksi wajar dan mencurigakan, sehingga penilaiannya terhadap risiko penipuan menjadi lebih terarah.

TPB menjelaskan literasi keuangan digital melalui kontrol perilaku yang dipersepsikan. Pengetahuan dan keterampilan meningkatkan keyakinan individu bahwa dirinya mampu memeriksa kredibilitas platform, menjaga akses akun, dan mengambil tindakan ketika menemukan ancaman. Widjanarko et al. (2025) membuktikan bahwa literasi keuangan digital memengaruhi kesadaran penipuan investasi pada responden Indonesia. Kemampuan menguasai aspek keuangan dan digital diperkirakan meningkatkan persepsi terhadap penipuan keuangan online.

H2: Literasi keuangan digital berpengaruh positif terhadap persepsi penipuan keuangan online.

2.4.3 Pengaruh Kepercayaan pada E-Payment terhadap Persepsi Penipuan Keuangan Online

Kepercayaan pada *e-payment* dipandang sebagai keyakinan terhadap integritas, kemampuan teknis, perlindungan data, transparansi, serta tanggung jawab penyedia layanan. Kepercayaan yang terbentuk dari unsur tersebut

membuat informasi keamanan, peringatan transaksi, dan prosedur pengaduan dipandang kredibel oleh pengguna. Pengguna yang mempercayai mekanisme perlindungan cenderung lebih bersedia mengikuti verifikasi, memperhatikan notifikasi, dan menyampaikan laporan ketika menemukan aktivitas yang tidak wajar.

TAM menerangkan bahwa keyakinan terhadap kegunaan, kemudahan, dan keandalan sistem membentuk penerimaan serta cara pengguna berinteraksi dengan teknologi. Aljaradat dan Shukla (2026) menunjukkan bahwa pembentukan kepercayaan pada pembayaran digital berkaitan dengan risiko keamanan, ekspektasi kinerja, kemudahan, dan penanganan pengaduan. Puri et al. (2025) menemukan bahwa kepercayaan meningkatkan niat pengguna untuk melakukan tindakan pencegahan terhadap penipuan keuangan digital. Kepercayaan yang berbasis keamanan dan akuntabilitas diperkirakan meningkatkan perhatian pengguna terhadap ancaman, sehingga persepsi penipuan keuangan online menjadi lebih kuat dan terarah.

H3: Kepercayaan pada *E-Payment* berpengaruh positif terhadap persepsi penipuan keuangan online.