BAB II

LANDASAN TEORI

2.1 Tinjauan Teori

2.1.1 *Technology Acceptance Model* (TAM)

Technology Acceptance Model (TAM) diperkenalkan oleh Davis (1989) untuk menganalisis faktor-faktor yang memengaruhi penerimaan teknologi oleh individu. TAM menekankan dua konstruk utama, yaitu persepsi kegunaan (*perceived usefulness*) dan persepsi kemudahan penggunaan (*perceived ease of use*), dalam membentuk niat dan perilaku penggunaan teknologi baru. Sunaryanto (2025) dalam Jurnal Universitas Islam Indonesia mendefinisikan bahwa *Technology Acceptance Model* (TAM) menjelaskan bagaimana persepsi kemudahan dan persepsi kegunaan dapat memengaruhi niat seseorang dalam menerima dan menggunakan teknologi digital, di mana kedua variabel tersebut berperan penting dan menjadi prediktor utama dalam adopsi sistem baru. Keamanan merupakan faktor eksternal yang berpengaruh terhadap persepsi kemudahan dan kegunaan, yang pada akhirnya mendorong niat menggunakan teknologi (Widodo & Susanto 2024). Nugroho dan Sundari (2025) mengatakan bahwa kepercayaan terhadap keamanan sistem berkontribusi besar dalam membangun loyalitas pengguna, dan keamanan menjadi kriteria utama dalam keputusan penggunaan layanan finansial digital.

2.1.2 Keamanan Data pada *E-Wallet*

Di era serba digital seperti saat ini, *E-Wallet* menjadi salah satu pilihan pembayaran yang banyak dipakai karena praktis dan cepat. Meski begitu, kemudahan tersebut juga membuka celah munculnya berbagai risiko terkait keamanan data pribadi pengguna, terutama yang berkaitan dengan kejahatan siber. Pradana dan Nasution (2024)

menjelaskan bahwa informasi sensitif yang disimpan pengguna di aplikasi *E-Wallet*, seperti data diri dan detail finansial dapat menjadi sasaran empuk bagi pelaku *cybercrime*.

Menurut Manuhara (2025), "keamanan data pada aplikasi *E-Wallet* dapat diartikan sebagai serangkaian upaya menjaga kerahasiaan, integritas, serta ketersediaan data pengguna dari risiko pencurian, penyalahgunaan, atau akses tanpa izin melalui fitur enkripsi, autentikasi berlapis, serta kebijakan privasi yang jelas dan transparan". Nugroho & Sundari (2025) juga menegaskan bahwa kepercayaan pengguna terhadap perlindungan data menjadi penentu kepuasan dan loyalitas, di mana sistem keamanan yang kuat dan pengalaman tanpa insiden kebocoran data berdampak langsung pada peningkatan intensitas penggunaan *E-Wallet*, khususnya di kalangan Generasi Z. Dengan demikian, teori keamanan data pada *E-Wallet* menempatkan perlindungan dan transparansi sebagai komponen utama dalam membangun keberlanjutan ekosistem pembayaran digital berbasis aplikasi.

2.1.3 *Perceived Trust* (PT)

Perceived Trust berperan sebagai pondasi kritis yang mendorong intensi penggunaan jangka panjang serta loyalitas terhadap *E-Wallet*. Dalam layanan digital seperti ShopeePay, kepercayaan pengguna terbentuk bukan hanya dari pengalaman penggunaan, tetapi juga dari keandalan mekanisme teknologi yang digunakan untuk melindungi data. McKnight, Choudhury & Kacmar (2002) merumuskan *trust* di e-commerce sebagai konstruksi multidimensi yang memengaruhi niat bertransaksi "*initial consumer trust influences intentions to transact*" dan menekankan pentingnya mengukur kredibilitas, kemampuan, dan niat baik pelaku layanan. Gefen, Karahanna, dan Straub (2003) menambahkan bahwa kepercayaan merupakan prediktor kunci dalam

perilaku penggunaan sistem digital. Menurut Sari (2025), tingkat kepercayaan dipengaruhi oleh sejauh mana pengguna yakin aplikasi *E-Wallet* mampu menjaga dan melindungi data pribadi mereka, di mana kepercayaan pengguna meningkat ketika aplikasi secara aktif menginformasikan kebijakan privasi dan memberikan proteksi nyata terhadap data pengguna.

2.1.4 *Privacy Awareness* (PA)

Privacy Awareness merujuk pada tingkat pemahaman pengguna mengenai bagaimana data pribadi mereka dikumpulkan, diproses, disimpan, dan dibagikan oleh platform digital sesuai dengan kebijakan privasi yang tersedia. Kesadaran privasi semakin penting pada era digital karena pengguna seringkali tidak memahami bagaimana data pengguna dapat dimanfaatkan oleh penyedia layanan. Malhotra, Kim, dan Agarwal (2004) melalui konsep *Internet Users' Information Privacy Concerns* (IUIPC) menyatakan bahwa pemahaman pengguna tentang bagaimana privasi data dikelola menjadi aspek dasar yang memengaruhi munculnya persepsi risiko serta tingkat kepercayaan pengguna terhadap layanan digital. Pendekatan ini sejalan dengan teori *Contextual Integrity* oleh Nissenbaum (2004), yang menyatakan bahwa privasi bukan hanya tentang kerahasiaan data, tetapi tentang kesesuaian aliran informasi dengan norma kontekstual sehingga transparansi kebijakan privasi berperan penting dalam menciptakan rasa aman bagi pengguna.

Brunotte, Specht, Chazette, dan Schneider (2022) menemukan bahwa penjelasan privasi yang jelas dan mudah dipahami (*privacy explanations*) secara signifikan meningkatkan kesadaran privasi dan kepercayaan pengguna. Penelitian ini menunjukkan bahwa *policy awareness* tidak hanya bergantung pada keberadaan kebijakan privasi, tetapi juga pada sejauh mana platform menyajikannya secara informatif

dan transparan. Penelitian lain yang dilakukan oleh Yuliana dan Pratiwi (2023) dalam konteks *fintech* di Indonesia menjelaskan bahwa semakin tinggi pemahaman pengguna tentang pengelolaan data pribadi, semakin tinggi pula persepsi keamanan (*perceived security*) yang mereka rasakan.

Dalam konteks *E-Wallet* seperti ShopeePay, *Privacy Awareness* berperan dalam membentuk persepsi keamanan dan kepercayaan, yang pada akhirnya mendorong loyalitas pengguna. Studi empiris *E-Wallet* Indonesia oleh Septiani et al. (2022) menunjukkan bahwa persepsi keamanan dan transparansi kebijakan privasi memiliki pengaruh positif terhadap loyalitas pengguna dompet digital. Pengguna yang memahami bagaimana data mereka diproses oleh aplikasi cenderung merasa lebih aman dan menunjukkan *continuance intention* serta loyalitas yang lebih tinggi. Dengan demikian, *Privacy Awareness* dapat dipandang sebagai variabel anteseden yang memengaruhi loyalitas pengguna ShopeePay secara langsung melalui peningkatan persepsi keamanan, maupun secara tidak langsung melalui pembentukan kepercayaan (*trust*) terhadap layanan.

2.1.5 *Institutional Surveillance* (IS)

Institutional Surveillance merupakan pengawasan oleh instansi atau regulator terhadap aktivitas transaksi di *E-Wallet*. *Institutional Surveillance* dalam layanan keuangan digital mencakup berbagai upaya pemantauan yang dilakukan oleh institusi keuangan maupun penyedia *e-payment* melalui proses pengumpulan dan pengolahan data transaksi para pengguna. Lyon (2007) menggambarkan pengawasan institusional sebagai aktivitas terstruktur untuk memperoleh serta memanfaatkan informasi individu guna mengatur risiko dan perilaku mereka. Sejalan dengan itu, Marx (2004) menyatakan bahwa bentuk pengawasan ini melibatkan pemanfaatan teknologi dan prosedur organisasi untuk

mengakses informasi yang dibutuhkan dalam rangka menjaga kontrol serta keamanan. Zuboff (2019) melalui teori *surveillance capitalism* menjelaskan bahwa perusahaan teknologi modern melakukan pengawasan menyeluruh terhadap aktivitas digital pengguna untuk mengekstraksi nilai ekonomi dari data perilaku yang terkumpul. Lyon (2021) menjelaskan bahwa pengawasan institusional tidak dapat dipisahkan dari aspek transparansi, karena meningkatnya praktik *surveillance* dapat menurunkan tingkat kepercayaan pengguna jika tidak disertai penjelasan yang jelas mengenai tujuan dan penggunaan data. Penerapan prinsip KYC (*Know Your Customer*) dan regulasi perlindungan konsumen dinilai penting untuk menekan risiko penyalahgunaan sistem serta meningkatkan kepercayaan pengguna terhadap pelaku *fintech*. Pengawasan institusional dan kepatuhan regulasi perlindungan konsumen sangat membantu meningkatkan *Perceived Trust* dan loyalitas pengguna digital wallet (Wongkar, 2024).

2.1.6 *Online Security Control Behavior* (OSCB)

Dalam layanan keuangan digital, terutama pada *E-Wallet* seperti ShopeePay, *Online Security Control Behavior* dipahami sebagai berbagai tindakan pengamanan yang dilakukan pengguna untuk melindungi data pribadi dan menjaga keamanan transaksi digital. Liang dan Xue (2010) menjelaskan bahwa perilaku kontrol keamanan online merupakan upaya aktif dari individu untuk mengelola serta mengurangi risiko ancaman digital melalui langkah-langkah perlindungan yang direncanakan. Penjelasan ini didukung oleh Herath dan Rao (2009) yang menyebutkan bahwa perilaku keamanan online merupakan bentuk kepatuhan pengguna terhadap aturan, kebijakan, dan prosedur keamanan yang disusun untuk mencegah terjadinya celah atau kerentanan sistem. Selain itu, Workman, Bommer, dan Straub (2008) juga menekankan bahwa perilaku kontrol keamanan online adalah tindakan pencegahan yang bertujuan meminimalkan potensi

penyalahgunaan, serangan siber, atau akses ilegal. Dalam konteks penggunaan *E-Wallet*, perilaku ini menjadi semakin penting karena meningkatnya risiko seperti phishing, penipuan OTP, dan pengambilalihan akun. Oleh sebab itu, penerapan langkah-langkah pengamanan oleh pengguna, misalnya menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan memeriksa aktivitas akun secara rutin merupakan wujud nyata *Online Security Control Behavior* yang membantu meningkatkan keamanan layanan ShopeePay maupun platform *E-Wallet* lainnya.

Flavián, Guinalíu, dan Gurrea (2006) menjelaskan bahwa keamanan yang dirasakan merujuk pada persepsi konsumen mengenai tingkat perlindungan terhadap berbagai ancaman dan risiko dalam lingkungan online, sehingga menggambarkan keyakinan pengguna bahwa suatu platform digital memiliki mekanisme keamanan yang memadai. Sejalan dengan itu, Kim, Ferrin, dan Rao (2008) menyatakan bahwa keamanan yang dirasakan merupakan sejauh mana konsumen meyakini bahwa penggunaan suatu sistem online aman dari potensi ancaman, menegaskan perannya dalam membangun kepercayaan serta mendorong niat penggunaan layanan digital. Konsep *perceived security* ini berkaitan erat dengan variabel *Online Security Control Behavior*, yaitu perilaku pengguna dalam mengawasi, mengelola, dan menjaga keamanan aktivitas digital mereka. Kedua variabel tersebut memiliki makna yang sejenis karena sama-sama menitikberatkan pada penilaian individu terhadap perlindungan dan keamanan informasi digital.

2.1.7 *E-Payment Continuance Intention* (EPCI)

Dalam layanan pembayaran digital, *E-Payment Continuance Intention* mengacu pada niat pengguna untuk terus memakai suatu layanan pembayaran elektronik setelah mereka mencobanya pada penggunaan awal. Bhattacherjee (2001) menjelaskan bahwa

continuance intention adalah keinginan individu untuk tetap menggunakan sebuah sistem informasi yang dibentuk dari hasil evaluasi pengalaman penggunaan sebelumnya. Zhou (2013) kemudian memperluas definisi ini dalam konteks *mobile payment* dengan menyatakan bahwa *continuance intention* merupakan niat pengguna untuk melanjutkan penggunaan layanan setelah tahap adopsi awal, di mana niat tersebut dipengaruhi oleh persepsi manfaat, keamanan, dan tingkat kepuasan. Selain itu, Susanto, Chang, dan Ha (2016) menegaskan bahwa dalam industri *fintech*, *continuance intention* mencerminkan keinginan pengguna untuk terus memanfaatkan layanan pembayaran elektronik ketika mereka merasa memperoleh manfaat serta memiliki kepercayaan yang cukup terhadap layanan tersebut. Penelitian oleh Ofori, Osei, dan Boateng (2022) juga menunjukkan bahwa niat pengguna untuk terus menggunakan *E-Wallet* dipengaruhi oleh faktor seperti persepsi keamanan, kenyamanan, dan keandalan. Dengan demikian, *E-Payment Continuance Intention* dapat dipahami sebagai komitmen psikologis pengguna untuk tetap menggunakan layanan pembayaran digital secara konsisten, yang terbentuk dari pengalaman penggunaan, persepsi kualitas layanan, dan keyakinan terhadap keamanan sistem.

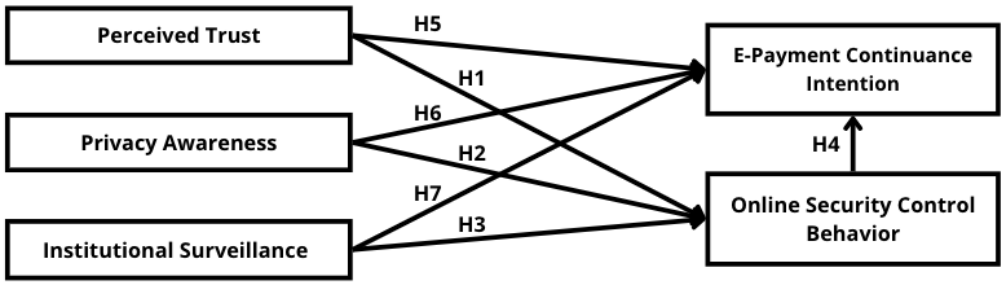
Dalam kerangka teori penelitian ini, *Online Security Control Behavior* pada *E-Wallet* ShopeePay ditempatkan sebagai variabel anteseden bagi *continuance intention*. Model yang diusulkan menggambarkan bahwa keamanan data memengaruhi kepuasan pengguna, yang kemudian mendorong niat berlanjut dan akhirnya meningkatkan loyalitas. Karena itu, peningkatan fitur keamanan seperti enkripsi, autentikasi multi-faktor, dan perlindungan data, sekaligus mempertahankan kepuasan pengguna, merupakan strategi utama bagi ShopeePay untuk memperkuat loyalitas penggunanya dalam jangka panjang.

Dalam beberapa penelitian, *continuance intention* juga diposisikan sebagai indikator dari loyalitas pengguna. Loyalitas dalam layanan digital tidak hanya diukur dari preferensi atau sikap positif, tetapi juga dari perilaku penggunaan yang berulang dan berkelanjutan. Loyalitas dalam konteks layanan digital tidak hanya mencakup sikap positif atau preferensi terhadap aplikasi, tetapi juga diwujudkan melalui penggunaan yang konsisten dan berkelanjutan. Beberapa studi menunjukkan bahwa ketika pengguna memiliki niat kuat untuk melanjutkan penggunaan *E-Wallet*, mereka cenderung lebih terikat, puas, dan memperlihatkan loyalitas jangka panjang. Rhamdhani (2020) menemukan bahwa *continuance intention* mempunyai pengaruh signifikan terhadap loyalitas pengguna mobile banking, dimana konsistensi penggunaan dipengaruhi oleh kepercayaan dan rasa aman dalam layanan digital yang digunakan. Hal serupa ditegaskan oleh Ansori dan Nugroho (2024) yang menunjukkan bahwa kepercayaan pengguna dan persepsi keamanan berdampak langsung pada *continuance usage intention* dalam aplikasi pembayaran digital di Indonesia. Dengan demikian, pada penelitian mengenai keamanan data *E-Wallet* ShopeePay, *E-Payment Continuance Intention* dapat diposisikan sebagai variabel dependen sekaligus indikator kuat untuk mengukur tingkat loyalitas pengguna, karena pengguna yang berniat melanjutkan penggunaan cenderung memiliki rasa aman, puas, dan percaya terhadap sistem pengelolaan data dalam platform tersebut.

2.2 Model Penelitian

Pada penelitian ini, peneliti menggunakan model penelitian yang digunakan oleh penelitian sebelumnya yang berjudul "*Digital Literacy, Online Security Behaviors and E-Payment Intention*" yang ditulis oleh Nguyen et al. (2024).

Berdasarkan model penelitian pada jurnal utama, peneliti menyesuaikan model penelitian sesuai dengan objek yang ingin diteliti dengan didukung oleh jurnal pendukung yang berjudul "*E-Payment Continuance Intention: Evidence from Vietnam*" yang ditulis oleh Nguyen dan Pham (2025). Adapun model penelitian yang dibentuk dan telah disesuaikan sebagai berikut:



Gambar 2. 1 Model Penelitian

Sumber: Modifikasi model dari penelitian Nguyen et al. (2024) dan Nguyen dan Pham (2025)

H1: *Perceived Trust* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

H2: *Privacy Awareness* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

H3: *Institutional Surveillance* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

H4: *Online Security Control Behavior* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

H5: *Perceived Trust* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

H6: *Privacy Awareness* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

H7: *Institutional Surveillance* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

2.3 Hipotesis

Berdasarkan model penelitian yang digunakan pada penelitian ini, berikut merupakan hipotesis pada penelitian ini.

2.3.1 Hubungan antara *Perceived Trust* dengan *Online Security Control Behavior*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Perceived Trust* memiliki pengaruh terhadap *Online Security Control Behavior*. Penelitian ini menelaah pengaruh *Perceived Trust* terhadap *Online Security Control Behavior* pengguna pada platform digital. Tingkat kepercayaan yang tinggi diyakini mendorong pengguna untuk lebih proaktif memanfaatkan fitur keamanan bawaan, mengikuti saran proteksi, serta menerima edukasi keamanan melalui notifikasi atau tips perlindungan akun (Gulati, 2024; Saxena, 2024; Zhang, 2023). Dengan demikian, kepercayaan yang seimbang tidak hanya meningkatkan kepatuhan terhadap protokol keamanan, tetapi juga memotivasi tindakan preventif seperti penggantian kata sandi secara rutin dan pengaktifan autentikasi dua faktor. Namun, literatur juga menunjukkan bahwa kepercayaan yang berlebihan dapat menimbulkan efek paradoks. Pengguna yang terlalu yakin pada platform cenderung mengalami risk compensation, menurunkan kewaspadaan pribadi, mengabaikan proteksi tambahan, serta mengurangi kecenderungan melaporkan insiden keamanan (Saveljeva, 2025; Prastyanti, 2024). Dengan demikian, *Perceived Trust* memiliki dampak ganda terhadap perilaku kontrol keamanan online, yaitu mampu memperkuat praktik proteksi yang tepat sekaligus berpotensi melemahkan kewaspadaan pengguna jika tidak seimbang. Temuan ini menjadi dasar bagi perumusan enam hipotesis penelitian yang mencerminkan efek positif dan negatif trust terhadap perilaku keamanan digital.

H1: *Perceived Trust* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

2.3.2 Hubungan antara *Privacy Awareness* dengan *Online Security Control Behavior*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Privacy Awareness* memiliki pengaruh positif terhadap *Online Security Control Behavior*. Penelitian yang dilakukan oleh Nguyen et al. (2024) menghasilkan pernyataan bahwa *Privacy Awareness* memiliki pengaruh positif terhadap *Online Security Control Behavior*. Penelitian ini berhipotesis bahwa *Privacy Awareness* atau kesadaran individu terhadap privasi memiliki pengaruh yang kompleks terhadap *Online Security Control Behavior* dalam lingkungan digital. Secara positif, tingkat kesadaran privasi yang tinggi diyakini mendorong pengguna untuk aktif menerapkan tindakan protektif, seperti mengaktifkan fitur keamanan dan pengaturan privasi, sehingga meningkatkan kontrol keamanan daring (Zhang et al., 2023). Selain itu, pengguna dengan tingkat *Privacy Awareness* tinggi cenderung merasakan rasa aman yang lebih besar saat berinteraksi dengan layanan digital, karena keyakinan bahwa data mereka dihargai dan dilindungi (Liu et al., 2024). Kesadaran privasi juga diharapkan dapat memperkuat kepercayaan pengguna terhadap sistem keamanan, sehingga mendukung konsistensi perilaku protektif jangka panjang (Zhang et al., 2023).

Di sisi lain, pengaruh negatif juga mungkin muncul. *Privacy Awareness* yang berlebihan dapat menimbulkan kecemasan terhadap ancaman privasi, sehingga menurunkan kenyamanan dan menghambat penerapan tindakan protektif secara efektif(Wang et al., 2023). Selain itu, tanpa dukungan literasi digital atau kemampuan teknis, kesadaran privasi saja tidak cukup untuk mendorong perilaku keamanan yang

konsisten (Smith & Jones, 2023). Penelitian lain mengandalkan persepsi privasi sebagai satu-satunya indikator keamanan dapat membuat pengguna merasa "sudah aman" dan mengabaikan langkah protektif tambahan, yang secara paradoks menurunkan efektivitas *Online Security Control Behavior* (Nguyen et al., 2022).

H2: *Privacy Awareness* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

2.3.3 Hubungan antara *Institutional Surveillance* dengan *Online Security Control Behavior*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Institutional Surveillance* memiliki pengaruh terhadap *Online Security Control Behavior*. Penelitian yang dilakukan oleh Nguyen et al. (2024) menghasilkan pernyataan bahwa *Institutional Surveillance* memiliki pengaruh positif terhadap *Online Security Control Behavior*. Penelitian lain juga menghasilkan pengaruh pengawasan institusional secara positif yang diterapkan sebagai bagian dari budaya keamanan organisasi diyakini dapat meningkatkan kesadaran individu akan pentingnya perlindungan keamanan serta mendorong penerapan tindakan protektif, seperti autentikasi ganda dan pengelolaan kata sandi yang aman, sehingga memperkuat perilaku kontrol keamanan (Smith & Johnson, 2024). Selain itu, institusi yang secara konsisten melakukan monitoring dan audit dapat meningkatkan kepatuhan terhadap prosedur keamanan serta pelaporan insiden, sehingga memperkuat keseluruhan perilaku keamanan pengguna (Brown et al., 2025).

Di sisi lain, pengawasan institusional juga berpotensi menimbulkan efek negatif. Tingginya tingkat penerimaan terhadap pengawasan dapat menciptakan *false sense of security*, di mana pengguna merasa sistem sudah sepenuhnya aman sehingga mengurangi motivasi untuk menjaga kontrol keamanan sendiri (Smith & Johnson, 2024). Selain itu, penerapan

Institutional Surveillance tanpa dukungan pelatihan, komunikasi, dan komitmen manajemen yang jelas dapat menimbulkan complacency atau kepercayaan berlebihan terhadap sistem, meningkatkan risiko kesalahan manusia dan pelanggaran keamanan (Brown et al., 2025). Intensitas pengawasan yang tinggi tanpa melibatkan pengguna juga berpotensi menimbulkan resistensi atau kecurigaan, menurunkan rasa kepemilikan terhadap keamanan digital, dan berdampak negatif pada perilaku kontrol keamanan jangka panjang (Davis, 2024).

H3: *Institutional Surveillance* berpengaruh positif terhadap *Online Security Control Behavior* pada aplikasi *E-Wallet* Shopeepay

2.3.4 Hubungan antara *Online Security Control Behavior* dengan *E-Payment Continuance Intention*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Online Security Control Behavior* memiliki pengaruh terhadap *E-Payment Continuance Intention*. Penelitian yang dilakukan oleh Nguyen et al. (2024) menghasilkan pernyataan bahwa perceived security memiliki pengaruh positif terhadap *E-Payment Continuance Intention*. Dalam penelitian Shanmugavel et al. (2024) hasil penelitiannya mengungkapkan bahwa perceived security yang memiliki makna yang sama dengan *Online Security Control Behavior* memiliki pengaruh positif terhadap continuance intention to use digital wallet, sejalan dengan hasil penelitian dari Nursjanti et al. (2024) memberikan banyak bukti bahwa persepsi keamanan patut mendapat pertimbangan yang lebih besar karena hal ini secara signifikan memengaruhi niat generasi Z untuk terus menggunakan dompet elektronik. Dalam penelitian Ying dan Mohammed (2021) memiliki pengaruh positif antara persepsi keamanan dengan niat menggunakan kembali di mana semakin besar privasi dan keamanan, maka semakin besar pula niat untuk terus menerus menggunakan *E-Wallet*. Namun, terdapat beberapa penelitian sebelumnya yang menemukan bahwa

terdapat hubungan yang tidak sejalan antara persepsi keamanan dengan niat konsumen untuk menggunakan teknologi dan layanan tertentu (Nguyen dan Tran, 2022; Umam dan Puspawati, 2024; Visakha dan Keni, 2022)

H4: *Online Security Control Behavior* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

2.3.5 Hubungan antara *Perceived Trust* dengan *E-Payment Continuance Intention*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Perceived Trust* memiliki pengaruh terhadap *E-Payment Continuance Intention*. Penelitian yang dilakukan oleh Nguyen dan Pham (2025) menghasilkan pernyataan bahwa *Perceived Trust* berpengaruh positif terhadap *continuance intention to use e-payment*, sejalan dengan penelitian yang dilakukan oleh Nguyen dan Tran (2022). Dalam penelitian lain yang mendukung dilakukan oleh Nursjanti et al. (2024) mengatakan bahwa kepercayaan terhadap pelayanan lebih diutamakan dalam penggunaan kembali dibandingkan dan menjadi faktor penting. Namun, terdapat beberapa penelitian sebelumnya yang menemukan bahwa terdapat hubungan yang tidak sejalan antara kepercayaan dengan niat konsumen untuk menggunakan teknologi dan layanan tertentu (Hafizh et al., 2024; Wahyudi et al., 2025; Ankadhitra et al., 2023)

H5: *Perceived Trust* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

2.3.6 Hubungan antara *Privacy Awareness* dengan *E-Payment Continuance Intention*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Privacy Awareness* memiliki pengaruh terhadap *E-Payment Continuance Intention*. Penelitian yang dilakukan oleh Nguyen et al.

(2024) menghasilkan pernyataan bahwa *Privacy Awareness* memiliki pengaruh positif terhadap *E-Payment Continuance Intention*, sejalan dengan penelitian yang dilakukan oleh Riache dan Pradana (2023) mengatakan bahwa apabila kesadaran privasi meningkat, maka niat untuk menggunakan kembali akan semakin meningkat. Dalam penelitian Darmiasih dan Setiawan (2021) menghasilkan bahwa privasi memiliki pengaruh positif terhadap niat penggunaan kembali sehingga jika pengguna merasa data rahasia termasuk informasi pribadinya terlindungi, maka akan meningkatkan kepercayaan diri pengguna dalam melakukan transaksi menggunakan aplikasi *E-Wallet*. Namun, terdapat beberapa penelitian sebelumnya yang menemukan bahwa terdapat hubungan yang tidak sejalan antara kesadaran privasi dengan niat konsumen untuk menggunakan teknologi dan layanan tertentu (Mahuri dan Arief, 2024; Ariningsih et al., 2022; Sinulingga et al., 2024)

H6: *Privacy Awareness* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

2.3.7 Hubungan antara *Institutional Surveillance* dengan *E-Payment Continuance Intention*

Berdasarkan penelitian yang pernah dilakukan oleh para peneliti sebelumnya, *Institutional Surveillance* memiliki pengaruh terhadap *E-Payment Continuance Intention*. Penelitian yang dilakukan oleh Triwijaya dan Puspitasari (2023) menyatakan bahwa faktor keamanan merupakan determinan utama dalam meningkatkan niat penggunaan berkelanjutan, sehingga menunjukkan bahwa *Institutional Surveillance* dapat memperkuat *perceived security*. Selain itu, pemahaman pengguna terhadap keberadaan regulasi dan mekanisme pengawasan yang jelas juga dapat memperkuat kepercayaan terhadap institusi penyedia layanan dan hal ini sejalan dengan penelitian yang dilakukan oleh Lestari et al. (2023) yang menemukan bahwa *trust* berkontribusi positif terhadap *continuance*

intention dalam konteks e-payment. Ditambah lagi, Utami et al. (2023) menegaskan bahwa transparansi dan reliabilitas sistem yang umumnya diasosiasikan dengan pengawasan institusional berpengaruh positif terhadap minat untuk menggunakan *fintech* secara berkelanjutan. Dengan demikian, hasil penelitian mengatakan bahwa *Institutional Surveillance* mampu meningkatkan *perceived security*, *trust*, dan *system reliability* yang pada akhirnya mendukung *continuance intention*.

Di sisi lain, *Institutional Surveillance* juga berpotensi menimbulkan dampak negatif sesuai dengan hasil penelitian yang dilakukan oleh Cloarec et al. (2024) menunjukkan bahwa pengguna merasakan *privacy cynicism* ketika merasa tidak memiliki kontrol atas data mereka yang kemudian menurunkan keinginan untuk terus menggunakan layanan. Sejalan dengan penelitian yang dilakukan oleh Ningtias et al. (2022) mengatakan bahwa keberadaan pengawasan institusional dapat meningkatkan *perceived risk*, yang menemukan bahwa persepsi risiko merupakan hambatan signifikan terhadap niat penggunaan berkelanjutan layanan digital. Dalam penelitian lain yang dilakukan oleh Munzel et al. (2025) menyoroti bahwa transparansi mengenai pengawasan institusional tidak selalu meningkatkan rasa aman, karena dapat memicu kekhawatiran terhadap potensi penyalahgunaan data pada akhirnya menekan *continuance usage*. Dengan demikian, mendukung hipotesis negatif yang menyatakan bahwa *Institutional Surveillance* dapat meningkatkan *privacy concerns*, *perceived risk*, dan *privacy cynicism*, yang ketiganya berpotensi menurunkan keberlanjutan penggunaan e-payment.

H7: *Institutional Surveillance* berpengaruh positif terhadap *E-Payment Continuance Intention* pada aplikasi *E-Wallet* Shopeepay

2.4 Penelitian Terdahulu

Untuk memperkuat hipotesis dalam penelitian ini, penulis mengacu pada sejumlah studi terdahulu yang relevan dengan variabel-variabel dalam kerangka penelitian. Variabel-variabel tersebut menjelaskan hubungan antarhipotesis sesuai dengan model penelitian yang diterapkan dalam studi ini.

Model penelitian terdahulu yang digunakan oleh peneliti adalah penelitian dari Nguyen et al. (2024) sebagai jurnal utama dalam penelitian ini. Dalam penelitian terdahulu Nguyen et al. (2024), ditemukan bahwa *E-Payment Continuance Intention* dipengaruhi oleh variabel *Technical Familiarity*, *Privacy and Policy Awareness*, *Institutional Surveillance*, dan *Online Security Control*. Selain itu, peneliti juga menggunakan penelitian dari Nguyen dan Pham (2025), ditemukan bahwa *E-Payment Continuance Intention* dipengaruhi oleh *Perceived Trust* sebagai jurnal pendukung dari penelitian ini.

Tabel 2.1 Penelitian Terdahulu

Tabel 2.1 Penelitian Terdahulu

No.	Peneliti	Judul Literatur	Temuan Inti
1.	Thu Thuy Nguyen, Thi Ngoc Hoai Tran, Thi Huyen My Do, Thi Khanh Linh Dinh, Thi Uyen Nhi Nguyen, Tran Minh Khue Dang (2024)	Digital Literacy, Online Security Behaviors and E-Payment Intention	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai acuan utama, juga digunakan sebagai referensi dalam penelitian ini, seperti variabel *Privacy Awareness*, *Institutional Surveillance*, *Online Security Control Behavior*, dan *E-Payment Continuance Intention*.
2.	Thanh D. Nguyen dan Yen Binh Pham (2025)	*E-Payment Continuance Intention*: Evidence from Vietnam	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai acuan pendukung, juga digunakan sebagai referensi dalam penelitian ini, seperti variabel *Perceived Trust*.
3.	Gulati, S. (2024)	Trust Models and Theories in Human–Computer Interaction	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai implikasi trust terbentuk terhadap perilaku pengguna
4.	Saxena, C. (2024)	Mediating Role Of Trust and Privacy Concerns Between Web Assurance and Purchase Intention	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai bentuk acuan mengenai peran trust dalam memediasi respons pengguna terhadap mekanisme keamanan dan assurance.
5.	Zhang, W. (2023)	Data Security, Customer Trust and Intention for Adoption (SAGE)	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai acuan mengenai keterkaitan antara keamanan data, trust, dan adopsi perilaku.
6.	Saveljeva, J.	Trust and Risk Management	Penelitian ini dijadikan sebagai

	(2025)	Interplay: A Review in the Digital Context	acuan bagi peneliti sebagai acuan mengenai tinjauan yang menguraikan paradoks trust vs. risk management (termasuk risk compensation)
7.	Prastyanti, R.A. (2024)	Establishing Consumer Trust Through Data Protection Law	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai kajian hubungan antara kebijakan perlindungan data, kepercayaan konsumen, dan implikasi praktik keamanan.
8.	Zhou, S., & Liu, Y. (2023)	*Effects of Perceived Privacy Risk and Disclosure Benefits on the Online Privacy Protection Behaviors among Chinese Teens.*	Penelitian ini dijadikan sebagai acuan bagi peneliti sebagai pendukung bahwa persepsi terhadap risiko privasi (perceived privacy risk) memiliki *efek positif signifikan* terhadap "online privacy protection behaviors"
9.	Zhang, Y. et al. (2024)	*Impact of perceived privacy and security in the TAM model. (Dalam artikel: Impact of perceived privacy and security in the TAM model, 2024)*	Penelitian ini dijadikan sebagai acuan bagi peneliti dalam mendukung hipotesis bahwa perceived privacy dapat meningkatkan perceived security atau sense of security pengguna.
10.	Leschanowsky, A., Rech, S., Popp, B., & Bäckström, T. (2024)	*Evaluating Privacy, Security, and Trust Perceptions in Conversational AI: A Systematic Review*	Penelitian ini dijadikan sebagai acuan bagi peneliti dalam mendukung hipotesis negatif bahwa awareness tinggi tidak selalu menjamin proteksi efektif, bahkan bisa menyebabkan kelalaian atau paradoks privasi.
11.	Septiari, E. D. (2025)	*The Paradox of Customer Privacy Concern in Social Media. Review of Integrative Business and Economics Research*	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung hipotesis negatif bahwa awareness tinggi tidak selalu menjamin proteksi efektif,

			bahkan bisa menyebabkan kelalaian atau paradoks privasi.
12.	Smith, A., & Johnson, B. (2024)	*Institutional Surveillance and User Security Perception in Digital Payment Systems*	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif *Institutional Surveillance* terhadap perceived security & trust.
13.	Brown, C., Miller, R., & Tan, J. (2025)	*Privacy Concerns and Over-Surveillance: Impacts on Digital Payment Continuance Intention*	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung tiga pengaruh negatif *Institutional Surveillance* terhadap perceived privacy, user anxiety, kenyamanan bertransaksi.
14.	Davis, L. (2024)	*Balancing Security and Privacy in Fintech Platforms: Effects on User Retention*	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk menjelaskan moderasi keseimbangan antara keamanan dan privasi.
15.	Shanmugavel et al. (2024)	Assessing Continuance Intention to Use Digital Wallet- A Dual-Factor Approach Using UTAUT2 and Updated IS Success Model	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara perceived security terhadap *E-Payment Continuance Intention*.
16.	Nursjanti et al. (2024)	Examining the Determinants of Gen Z's Continuance Intention towards *E-Wallet*s	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara perceived security terhadap continuance intention dan *Perceived Trust* terhadap continuance intention dan pengaruh positif *Perceived Trust* terhadap continuance intention.

17.	Ying dan Mohammed (2021)	Understanding the Factors That Influence Consumer Continuous Intention to Use *E-Wallet* In Malaysia	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara privacy and security terhadap continuous intention
18.	Nguyen dan Tran (2022)	E-Payment Continuance Usage the Roles of *Perceived Trust* and Perceived Security	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived security terhadap e-payment continuance usage dan pengaruh positif antara *Perceived Trust* terhadap e-payment continuance usage.
19.	Umam dan Puspawati (2024)	Continuance Use Intention in the use of *E-Wallet*s by using the Expectation Confirmation Model through E-Satisfaction	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived security terhadap continuance use intention
20.	Visakha dan Keni (2022)	The Impact of Security and Perceived Ease of Use on Reuse Intention of *E-Wallet* Users in Jakarta: The Mediating Role of E-Satisfaction	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived security terhadap reuse intention
21.	Nguyen dan Pham (2025)	*E-Payment Continuance Intention* Evidence from Vietnam	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara *Perceived Trust* terhadap continuance intention
22.	Hafizh et al. (2024)	Factors Affecting Continuance Intention Towards Adoption of Linkaja Mobile Payment	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Perceived Trust* terhadap e-payment continuance usage.

23.	Wahyudi et al. (2025)	The Determinants in The Adoption of Banking Application Technology	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Perceived Trust* terhadap e-payment continuance usage.
24.	Ankadhitra et al. (2023)	Usage Analysis of Mobile Payment System to Consumer Continuance Intention in Jabodetabek	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Perceived Trust* terhadap e-payment continuance usage.
25.	Riache dan Pradana (2022)	The Effect of Perceived Privacy, Security, and Trust on the Continuance Intention to Use Social Networking Services (A Study on Meta's Social Networks)	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara perceived privacy terhadap continuance use intention.
26.	Darmiasih dan Setiawan (2021)	Continuance Usage Intention and Its Antecedents on Using Ovo Ewallet Application in Denpasar	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara perceived privacy terhadap continuance usage intention.
27.	Mahuri dan Arief (2024)	The Factors Affecting Continuance Intention of ChatGPT as an AI Chatbot in Indonesia	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived privacy terhadap continuance intention.
28.	Ariningsih et al. (2022)	Intention to Use *E-Wallet* dilihat dari Perceived Usefulness, Perceived Ease of Use, Perceived Security,dan Trust	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived privacy terhadap intention to use *E-Wallet*.
29.	Sinulingga et al. (2024)	A Study Intention, Implementation and Adoption of *E-Wallet* in Indonesia	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara perceived privacy terhadap

			adoption and use of *E-Wallet*.
30.	Triwijaya dan Puspitasari (2023)	Teknologi Sistem Informasi Akuntansi dalam Minat Penggunaan Layanan Pembayaran Digital.	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara institutional terhadap intention to use.
31.	Lestari et al. (2023)	Pengaruh E-Payment Trust terhadap Minat Transaksi pada E-Marketplace Menggunakan Framework TAM 3	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara *Institutional Surveillance* terhadap continuance intention melalui trust.
32.	Utami et al. (2023)	Pengaruh Privasi, Keamanan, Keandalan, dan Transparansi Terhadap Minat Penggunaan Payment *Fintech* UMKM.	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh positif antara *Institutional Surveillance* terhadap continuance intention
33.	Cloarec et al. (2024)	*Transformative Privacy Calculus: Conceptualizing the Personalization-Privacy Paradox.*	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Institutional Surveillance* terhadap continuance intention melalui privacy cynicism.
34.	Ningtias et al. (2022)	Pengaruh Kepercayaan dan Keamanan Layanan Digital Payment terhadap Keputusan Bertransaksi Online.	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Institutional Surveillance* terhadap continuance intention melalui meningkatnya perceived risk.
35.	Munzel et al. (2025)	Unravelling the Effects of Privacy Policies on Information Disclosure: Insights from E-Commerce Consumer Behavior.	Penelitian ini dijadikan sebagai acuan bagi peneliti untuk mendukung pengaruh negatif antara *Institutional Surveillance* terhadap continuance intention.