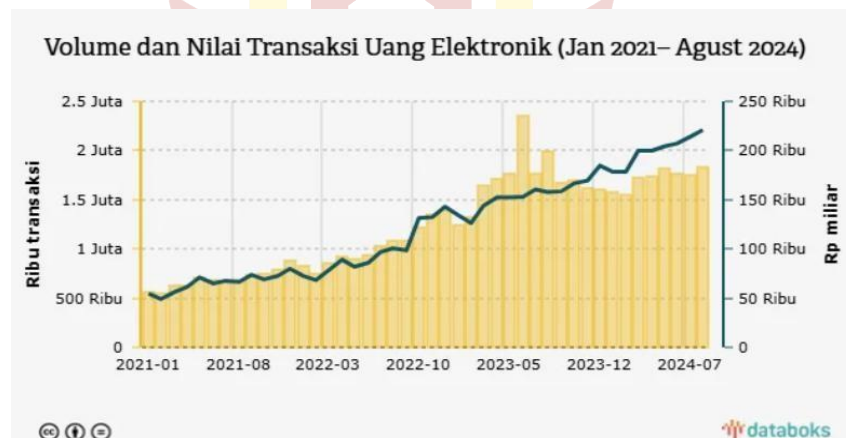


BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi digital telah membawa perubahan besar dalam cara masyarakat berinteraksi, berkomunikasi, dan bertransaksi. Salah satu perubahan yang paling terasa adalah hadirnya *financial technology* (fintech) di sektor keuangan, sebuah inovasi yang diterima masyarakat. Melalui layanan dompet digital berbasis (*e-wallet*), kini masyarakat bisa melakukan berbagai transaksi kapan saja dan di mana pun tanpa perlu membawa uang tunai. Besarnya adopsi layanan ini tercermin dari data Bank Indonesia (2021) yang mencatat nilai transaksi uang elektronik di Indonesia telah melampaui angka Rp400 triliun, dengan jumlah pengguna yang terus bertambah dari tahun ke tahun.



Gambar 1.1 Volume dan Nilai Transaksi Uang Elektronik

Angka tersebut menggambarkan adanya pergeseran perilaku masyarakat menuju sistem pembayaran digital yang lebih praktis, cepat, dan efisien. Salah satu aplikasi *e-wallet* yang banyak digunakan di Indonesia adalah DANA. Sejak diluncurkan, DANA menawarkan berbagai layanan pembayaran digital seperti pembelian pulsa, pembayaran tagihan, transfer antar pengguna, hingga pembayaran melalui QRIS di berbagai merchant. Inovasi ini membuat DANA semakin populer dan digunakan oleh berbagai kalangan masyarakat,

baik di kota besar maupun daerah.

Namun, meskipun jumlah pengguna terus bertambah, masih terdapat berbagai masalah yang berkaitan dengan keamanan sistem dan kepercayaan pengguna. Kekhawatiran mengenai kebocoran data, akses ilegal, serta penipuan online menimbulkan persepsi negatif terhadap layanan keuangan digital. Kepercayaan menjadi faktor penting yang menentukan keberhasilan suatu platform digital. Tanpa adanya rasa aman, pengguna akan cenderung enggan bertransaksi meskipun layanan tersebut menawarkan kemudahan. Hasil penelitian (Putri, dkk 2023) menunjukkan bahwa persepsi risiko, terutama yang berkaitan dengan keamanan, memiliki pengaruh negatif terhadap kepercayaan pengguna aplikasi DANA. Artinya, semakin tinggi risiko yang dirasakan, maka semakin rendah tingkat kepercayaan pengguna. Sementara itu, (Kinanti dan Rahmiati, 2022) menegaskan bahwa semakin tinggi persepsi keamanan suatu aplikasi, semakin besar pula rasa percaya pengguna untuk terus menggunakan layanan tersebut.

Dalam bidang sistem informasi, terdapat salah satu pendekatan teoritis yang sangat relevan untuk memahami bagaimana pengguna merespons risiko dan ancaman keamanan digital, yaitu *Protection Motivation Theory* (PMT). Teori yang diperkenalkan oleh (Rogers, 1983) ini menjelaskan proses pengambilan keputusan seseorang ketika menghadapi ancaman, apakah mereka akan mengambil tindakan untuk melindungi diri atau tidak. Proses tersebut melibatkan dua tahap penilaian kognitif, yakni *threat appraisal* yang berkaitan dengan seberapa serius dan rentan seseorang merasa terhadap ancaman yang ada, serta *coping appraisal* yang berkaitan dengan seberapa yakin seseorang bahwa dirinya mampu menghadapi ancaman tersebut secara efektif. Melalui kedua proses inilah variabel-variabel utama PMT seperti *perceived severity*, *perceived vulnerability*, *response efficacy*, dan *self-efficacy* bekerja dalam membentuk motivasi seseorang untuk mengambil tindakan perlindungan digital.

Penelitian terdahulu juga mendukung relevansi PMT dalam konteks penggunaan fintech. (Gitareswara, Suratno, dan Lestari, 2025) menemukan bahwa kepercayaan, persepsi ancaman, serta efektivitas sistem berperan besar dalam menentukan intensi penggunaan aplikasi dompet digital seperti GoPay. Hasil tersebut memperkuat pandangan bahwa aspek keamanan tidak dapat dipisahkan dari faktor kepercayaan ketika membahas adopsi e-wallet di Indonesia. Berdasarkan hal tersebut, penerapan PMT pada penelitian mengenai aplikasi DANA menjadi penting untuk memahami lebih dalam perilaku keamanan digital pengguna.

Walaupun sudah ada beberapa penelitian mengenai e-wallet di Indonesia, masih terdapat sejumlah kesenjangan penelitian (research gap) yang membuat penelitian ini perlu dilakukan. Pertama, terdapat gap empiris, yaitu perbedaan fokus antara penelitian terdahulu dengan penelitian ini. Sebagian besar penelitian sebelumnya yang membahas aplikasi DANA hanya menyoroti aspek kepercayaan atau risiko keamanan (Mayasari dkk, 2025). Namun, sangat sedikit penelitian yang secara khusus meneliti motivasi pengguna dalam melindungi akun DANA dengan menggunakan pendekatan *Protection Motivation Theory* (PMT).

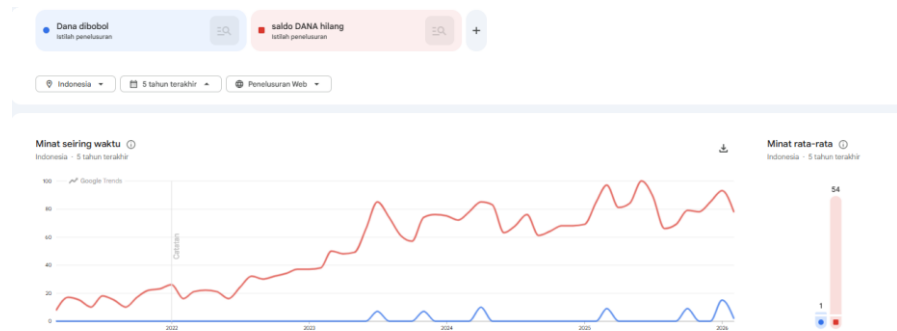
Kedua, terdapat gap teoritis, karena penelitian terdahulu lebih banyak menggunakan teori seperti TAM dan UTAUT untuk menjelaskan perilaku pengguna e-wallet, sebagaimana digunakan dalam studi tentang intensitas penggunaan e-wallet yang mengkombinasikan TAM dan UTAUT (Khofifah & Khordiyem, 2024). Padahal isu utama yang banyak muncul pada penggunaan aplikasi DANA adalah keamanan dan risiko penipuan digital, yang sebenarnya lebih tepat dijelaskan menggunakan PMT.

Ketiga, terdapat gap metode penelitian. Banyak penelitian sebelumnya menggunakan regresi linier atau SEM kovarian, sementara penelitian ini menggunakan SEM-PLS, yang lebih cocok

untuk model prediktif, sampel yang tidak terlalu besar, dan analisis dengan variabel laten yang memiliki indikator terbatas. Dalam konteks penelitian e-wallet, penelitian ini menerapkan *Technology Acceptance Model* (TAM) menggunakan SEM-PLS untuk menganalisis hubungan antara persepsi kemudahan, persepsi manfaat, sikap pengguna, dan minat penggunaan (Setiono, dkk 2022). Pendekatan ini memberikan hasil yang lebih akurat untuk memprediksi bagaimana faktor-faktor dalam PMT memengaruhi motivasi keamanan digital.

Keempat, terdapat gap populasi dan geografis. Sebagian besar penelitian sebelumnya dilakukan di wilayah kota besar di Pulau Jawa atau menggunakan populasi umum seperti mahasiswa seluruh Indonesia. Penelitian ini berfokus pada pengguna aktif aplikasi DANA di Kota Padang, yang memiliki karakteristik penggunaan layanan digital yang berbeda dibandingkan kota-kota besar lainnya. Minimnya penelitian tentang keamanan digital e-wallet di luar Jawa membuat penelitian ini memberikan perspektif baru mengenai perilaku keamanan pengguna di wilayah dengan perkembangan digital yang sedang bertumbuh.

Dengan adanya keempat celah penelitian yang telah diidentifikasi, penelitian ini hadir untuk mengisi ruang yang belum banyak dijamah yaitu mengkaji secara khusus bagaimana variabel-variabel dalam PMT membentuk motivasi keamanan digital pengguna aplikasi DANA di Kota Padang.



Gambar 1.2 Data Google Trends

Data google trends menunjukkan bahwa pencarian dengan kata kunci “Saldo Dana Hilang” mengalami tren peningkatan dalam lima tahun terakhir dengan rata-rata indeks 54. Hal ini menunjukkan tingginya perhatian dan kekhawatiran masyarakat terhadap potensi risiko kehilangan saldo aplikasi DANA.

Berdasarkan kesenjangan penelitian yang diuraikan, penelitian ini bertujuan untuk menganalisis hubungan antar variabel *Protection Motivation Theory* (PMT) terhadap motivasi keamanan digital pengguna aplikasi DANA. Secara spesifik, penelitian ini menelaah bagaimana konstruk *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost* membentuk motivasi pengguna dalam menjaga keamanan akun mereka dari ancaman digital. Fokus penelitian diarahkan pada pengguna aplikasi DANA di kota padang guna memperoleh gambaran perilaku keamanan digital dalam konteks wilayah yang masih relatif jarang dikaji.

Urgensi penelitian ini semakin tinggi karena e-wallet tidak hanya memudahkan transaksi individu, tetapi juga mendukung upaya pemerintah dalam meningkatkan literasi keuangan digital serta mendorong terciptanya masyarakat tanpa uang tunai.

B. Rumusan Masalah

Bagaimana hubungan antara variabel *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost* terhadap motivasi keamanan digital pengguna aplikasi DANA di kota Padang?

C. Batasan Masalah

Berdasarkan rumusan masalah diatas, maka didapatkanlah batasan masalah dalam penelitian ini, yaitu:

1. Penelitian ini hanya berfokus pada pengguna aplikasi DANA, dengan lama penggunaan minimal kurang lebih 6 bulan hingga lebih dari 2 tahun. Penelitian ini tidak membahas aspek keamanan sistem aplikasi DANA, melainkan hanya meneliti persepsi dan motivasi pengguna dalam melindungi akun DANA berdasarkan pendekatan *Protection Motivation Theory* (PMT). Selain itu, penelitian ini bersifat *cross-sectional*, yaitu pengambilan data dilakukan pada satu waktu tertentu.
2. Variabel yang dianalisis dibatasi pada faktor-faktor dalam Protection Motivation Theory (PMT), yaitu *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost*.
3. Responden penelitian dibatasi pada masyarakat yang berdomisili di wilayah kota padang.

D. Tujuan Penelitian

Tujuan penelitian ini adalah menganalisis hubungan antara *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost* terhadap motivasi keamanan digital pengguna aplikasi DANA di Kota Padang.

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, sebagai berikut:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat memperkuat penerapan *Protection Motivation Theory* (PMT) dalam konteks keamanan e-wallet, khususnya pada penggunaan aplikasi DANA. Hasil penelitian ini memberikan kontribusi mengenai peran *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost* dalam membentuk motivasi keamanan digital pengguna. Dengan demikian, penelitian ini dapat menjadi rujukan bagi pengembangan model PMT pada studi keamanan digital di bidang sistem informasi dan teknologi keuangan.

2. Manfaat Praktis

Bagi pengembang aplikasi DANA, hasil penelitian digunakan sebagai dasar dalam perancangan dan pengembangan fitur keamanan, seperti penguatan autentikasi, pengaturan notifikasi risiko, serta penyajian informasi keamanan yang lebih mudah dipahami pengguna. Selain itu, temuan penelitian ini juga dapat dimanfaatkan untuk menyusun strategi edukasi keamanan digital yang lebih tepat sasaran, sesuai dengan tingkat persepsi risiko dan kemampuan pengguna dalam melindungi akun mereka.