Jurnal INTEK (Informatika dan Teknologi Informasi)
Volume 9 Nomor 1, Mei 2026
eISSN: 2620 – 4924 | pISSN: 2620 – 4843 | Halaman: 27 – 37

Pengaruh Risiko Keamanan dan Performa Terhadap Persepsi Pengguna dalam Layanan e-Banking

Alya Dijayanti[1*], Fathia Kaila Azizah[2], Ahmad Bayu Saputra [3],
Faiz Purnomo Adi[4], Rangga Hapsendy Simarmata[5]

[1,2,3,4,5,6] Universitas Bina Sarana Informatika, Jakarta, 10450, Indonesia
dijayantialya4@gmail.com, fathiakaila12@gmail.com, ahmadbayu1555@gmail.com,
faizpurnomoadi8@gmail.com, rangga.hapsendy.simarmata@gmail.com

ABSTRAK
Transformasi digital pada sektor perbankan mendorong peningkatan penggunaan layanan e-banking, namun juga memunculkan risiko keamanan dan performa yang dapat memengaruhi persepsi serta kepercayaan nasabah. Penelitian ini menggunakan pendekatan kualitatif melalui studi literatur untuk mengevaluasi bagaimana dua jenis risiko tersebut membentuk pengalaman dan penilaian pengguna terhadap layanan keuangan digital. Hasil penelitian menunjukkan bahwa nasabah masih memiliki kekhawatiran terhadap ancaman seperti pencurian data, serangan malware, dan ketidakstabilan aplikasi, tetapi tingkat kepercayaan tetap tinggi ketika bank menyediakan mekanisme keamanan berlapis, menjaga keandalan sistem, serta memberikan edukasi terkait keamanan siber. Temuan ini menegaskan bahwa penguatan sistem keamanan dan peningkatan stabilitas layanan merupakan faktor kunci dalam membangun dan mempertahankan kepercayaan nasabah terhadap layanan e-banking.
Kata Kunci: E-Banking, Risiko Keamanan, Risiko Performa, Keamanan Siber

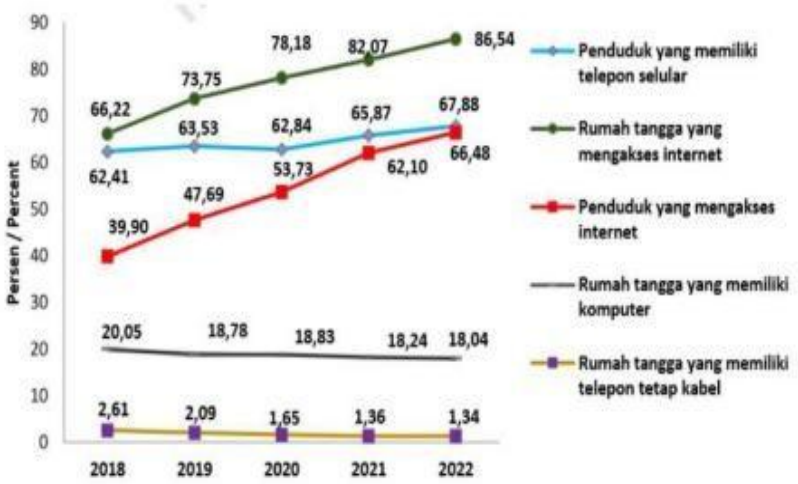
ABSTRACT
The rapid digital transformation in the banking sector has increased the adoption of e-banking services, yet it also introduces security and performance risks that may influence user perception and customer trust. Using a qualitative approach through literature review, this study examines how these two categories of risks shape user experiences and evaluations of digital financial services. The findings reveal that customers continue to express concerns regarding threats such as data theft, malware attacks, and system instability; however, trust remains relatively strong when banks implement layered security mechanisms, maintain system reliability, and provide adequate cybersecurity education. These results emphasize that strengthening security infrastructure and enhancing system performance are essential factors in building and sustaining customer trust in e-banking services.
Keywords: *E-Banking, Security Risk, Performance Risk, Cybersecurity.*

1. PENDAHULUAN

Pertumbuhan pesat teknologi informasi dan komunikasi (TIK) telah menciptakan transformasi yang signifikan dalam berbagai aspek kehidupan masyarakat, termasuk di Indonesia (Hutagaol et al., 2024). Dalam beberapa tahun terakhir, transformasi digital di Indonesia menunjukkan akselerasi yang sangat signifikan. Berdasarkan laporan Badan Pusat Statistik (BPS), kurun waktu 2018 hingga 2022 mencatat peningkatan tajam dalam pemanfaatan teknologi informasi dan komunikasi (TIK) oleh masyarakat. Tiga indikator yang mengalami pertumbuhan paling menonjol adalah persentase penduduk yang memiliki telepon seluler, jumlah rumah tangga yang terhubung dengan internet, dan proporsi penduduk

Jurnal INTEK (Informatika dan Teknologi Informasi)
Volume 9 Nomor 1, Mei 2026
eISSN: 2620 – 4924 | pISSN: 2620 – 4843 | Halaman: 27 – 37

yang aktif mengakses internet. Perkembangan ketiga indikator ini tergambarkan secara jelas pada Gambar 1.



Gambar 1. 1Pengguna TIK di Indonesia Tahun 2018-2022
(Badan Pusat Statistikmiskin, n.d.)

Persepsi keamanan yang dirasakan oleh para nasabah akan menghadirkan rasa percaya yang membuat mereka puas dan loyal terhadap sebuah produk [1]. Dalam konteks pengguna e-banking, nasabah yang mempunyai persepsi keamanan yang baik terhadap e-banking akan cenderung setia terhadap jasa keuangan tersebut. Tingginya jaminan keamanan layanan akan meningkatkan frekuensi penggunaan layanan tersebut [2]. Pernyataan ini diperkuat oleh Kusuma (2019) yang menemukan bahwasanya keamanan memengaruhi loyalitas pengguna mobile banking [2].

Di Indonesia, adopsi teknologi e-banking berada pada tahap permulaan yang memiliki prospek pengembangan yang besar. Peningkatan penggunaan internet yang didukung oleh tarif internet yang semakin terjangkau turut mendukung pengembangan ini. Meski adopsi e-banking berperan krusial dalam mendorong peningkatan pelayanan kepada nasabah, namun penggunaannya juga memiliki risiko yang sulit dihindari [3].

Inovasi ini tidak hanya ditujukan untuk menjawab kebutuhan nasabah modern yang menuntut kecepatan dan kenyamanan dalam bertransaksi, tetapi juga sebagai strategi untuk meningkatkan daya saing di tengah persaingan industri perbankan yang semakin kompetitif. Namun, keberhasilan adopsi layanan digital tersebut sangat bergantung pada kesiapan infrastruktur teknologi, keamanan sistem, kualitas sumber daya manusia [4], serta kemauan nasabah untuk beralih dari layanan konvensional ke layanan digital. Hal ini menunjukkan bahwa meskipun transformasi digital dalam dunia perbankan semakin pesat, tidak semua lapisan masyarakat dapat menikmati kemudahan dan efisiensi layanan tersebut secara setara [5].
Selain berfokus pada pemilihan bank untuk tempat berinvestasi atau menabung dan tingkat bunga atau keuntungan, nasabah di dunia perbankan kini juga mempertimbangkan

kecanggihan dan kelengkapan fitur dari produk perbankan. Hal ini dikarenakan para nasabah tidak hanya memperhitungkan value yang akan mereka peroleh, melainkan juga kualitas serta kemudahan untuk mendukung dan memperlancar proses transaksi [6]. Peningkatan penggunaan layanan digital di masyarakat mempermudah PT. Bank Negara Indonesia (Persero) TBK untuk mencatat pertumbuhan kinerja yang positif, seperti yang dipresentasikan pada Tabel 1.

Tabel 1. Jumlah Nasabah dan Penggunaan Mobile Bank

No	Uraian	2023	2024
1	Nasabah	62,9 Juta	64 Juta
2	Mobile Banking	16,2 Juta	16,9 Juta

Sumber: Laporan PT.Bank Negara Indonesia (2024)

Kendati demikian, perbankan digital yang tengah berkembang pesat kini turut menghadirkan sejumlah tantangan yang perlu diantisipasi, termasuk dalam aspek keamanan data. Kasus *cybercrime*, seperti peretasan sistem perbankan dan pembobolan data nasabah telah menurunkan kepercayaan masyarakat terhadap layanan digital. Keamanan yang lemah berpengaruh pada e-trust nasabah terhadap penggunaan layanan e-banking. Karenanya, sektor perbankan perlu memperkuat keamanan elektronik atau e-security guna meningkatkan kepercayaan nasabah [7].

Ada dua risiko yang dimana paling dominan adalah risiko keamanan (*security risk*) dan risiko performa (*performance risk*). Persepsi risiko secara khusus adalah penilaian evaluatif konsumen terhadap potensi kerugian kerahasiaan informasi pribadi, termasuk penyalahgunaan informasi yang berujung pada pencurian identitas. Sementara risiko adalah persepsi pelanggan terhadap ketidakpastian serta konsekuensi negatif dalam pembelian produk atau pemakaian jasa. Beberapa bentuk risiko yaitu jaminan keamanan, keadaan sistem keamanan, waktu yang terpakai, dan gangguan kinerja. Lebih lanjut, kepercayaan adalah tingkat keyakinan individu dalam mengandalkan produk atau layanan dari bank. Keberhasilan suatu bank dalam membangun persepsi nasabah ditentukan oleh kepercayaan nasabah terhadap layanan bank tersebut [8].

Risiko keamanan ini sering muncul ketika nasabah melakukan transaksi, dan informasi sensitif dapat dilihat oleh pihak tertentu, seperti teller bank dan pegawai toko. Tingkat keamanan bank menjadi tolak ukur bagi nasabah yang menggunakan m-banking dan internet banking [9].

Risiko keamanan muncul dari potensi ancaman seperti pencurian data, *phishing*, *malware*, peretasan akun, maupun kebocoran informasi pribadi. Tingginya angka kejahatan siber di sektor finansial menimbulkan kekhawatiran bagi nasabah, terutama karena transaksi e-banking melibatkan data sensitif dan akses langsung ke rekening keuangan [5], [2]. Persepsi resiko sangat mempengaruhi tingkat kepercayaan. Semakin kecil persepsi resiko dari suatu individu maka semakin besar tingkat kepercayaannya, begitupun sebaliknya. Jika resiko itu meningkat dari sekedar informasi sampai padakeputusan pembelian produk (transaksi), resiko diasosiasikan dengan kepercayaan [10]. Oleh karena itu, penting bagi

pihak bank untuk mengetahui bagaimana para nasabah mengapresiasi layanan E-Banking agar dapat membantu menemukan rencana strategis dan meningkatkan pangsa pasar [11].

Dengan adanya antisipasi dan jaminan dari bank terkait risiko tersebut, diharapkan dapat melahirkan sikap kepercayaan dari para nasabah untuk mencoba fasilitas internet banking. Sehingga nasabah dapat menerima manfaatnya. Persepsi nasabah akan manfaat dan kemudahan yang ditimbulkan dari pemakaian internet banking akan menentukan sikap nasabah dalam penggunaan layanan internet banking. Sikap nasabah dalam menerima internet banking bisa ditunjukkan dengan intensi pemakaian layanan internet banking [12].

Melihat semakin tingginya penggunaan e-banking di Indonesia, serta meningkatnya kasus kejahatan siber dan gangguan sistem digital, maka perlu dilakukan penelitian mengenai bagaimana risiko keamanan dan risiko performa memengaruhi persepsi pengguna dalam penggunaan layanan e-banking [7]. Penelitian ini diharapkan dapat memberikan pemahaman bagi pihak perbankan dalam meningkatkan kualitas layanan serta memberikan kepercayaan dan kenyamanan kepada nasabah.

Menilai dari popularitas yang sekarang, online banking akan terus popular dan digunakan di masa yang akan datang. Individual dan pelaku bisnis yang sebelumnya menolak untuk mengadopsi online banking sebagai alat komersial, sekarang tidak akan mempunyai banyak pilihan lagi. Kecepatan sistem online dalam melakukan transaksi akan mengalahkan metode tradisional sepenuhnya [13].

2. METODE

Jenis penelitian yang digunakan pada penelitian ini adalah metode kualitatif. Dipilihnya penelitian kualitatif ini di harapkan akan memberikan ruang bagi peneliti untuk memahami konteks nyata yang dialami pengguna dalam menggunakan layanan e-Banking, sehingga data yang diperoleh tidak terbatas pada angka statistik, melainkan berupa pengalaman, interpretasi, dan persepsi personal pengguna. Penelitian ini berfokus pada bagaimana pengguna menilai tingkat keamanan, kenyamanan, dan keandalan layanan berdasarkan interaksi langsung mereka dengan sistem perbankan digital. Oleh karena itu, pendekatan kualitatif mampu menangkap emosi, pendapat, dan gambaran nyata mengenai rasa aman atau rasa cemas pengguna ketika bertransaksi secara digital.

Dalam penelitian kualitatif, peneliti merupakan instrumen kunci (*key instrument*), sehingga keterlibatan peneliti secara langsung dalam proses pengumpulan dan analisis data sangat penting. Peneliti melakukan pencarian, seleksi, interpretasi, dan pemaknaan data melalui sumber-sumber literatur ilmiah dan dokumen yang relevan. Analisis dilakukan secara induktif, yaitu dari temuan khusus menuju pola dan kesimpulan umum. Dengan cara ini, penelitian dapat menghasilkan pemahaman yang mendalam mengenai hubungan antara risiko keamanan, risiko performa, dan persepsi pengguna layanan e-Banking.
Penelitian ini juga menggunakan analisis tematik, yaitu teknik analisis yang mengelompokkan data berdasarkan tema-tema penting yang muncul dari hasil kajian literatur. Tema yang diidentifikasi di antaranya:

1. Bagaimana pengguna menginterpretasikan risiko pencurian data, phishing, scam?
2. Apakah performa berkaitan dengan persepsi profesionalisme bank?
3. Bagaimana kombinasi rasa aman di barengi performa sistem memengaruhi persepsi?
4. Bagaimana bank seharusnya merespon kekhawatiran pengguna?

Melalui proses analisis ini, penelitian dapat memetakan pola yang berkaitan dengan bagaimana kedua jenis risiko tersebut membentuk persepsi pengguna terhadap kualitas layanan secara keseluruhan.

Hasil akhir metode kualitatif ini diharapkan tidak hanya memberikan gambaran deskriptif mengenai persepsi pengguna, tetapi juga memberikan kontribusi berupa rekomendasi bagi bank, pengembang aplikasi, dan regulator untuk meningkatkan keamanan serta performa layanan e-Banking. Dengan demikian, penelitian ini tidak hanya berfungsi sebagai kajian akademik tetapi juga berpotensi menjadi bahan evaluasi strategis untuk meningkatkan kepuasan dan kepercayaan pelanggan dalam ekosistem perbankan digital.

3. HASIL DAN PEMBAHASAN

3.1. Risiko Keamanan dan Kerangka Regulasi Perlindungan Data

Risiko keamanan menjadi perhatian utama bagi pengguna ketika mengakses layanan e-banking. Dalam penelitian ini, sebagian besar informan menunjukkan kekhawatiran terhadap potensi pencurian data, phishing, dan akses ilegal pada akun perbankan mereka. Kekhawatiran tersebut sejalan dengan temuan Almaiah et al. (2023), yang menjelaskan bahwa *perceived security* secara langsung memengaruhi tingkat persepsi risiko serta kepercayaan pengguna dalam aplikasi mobile banking. Hal ini menunjukkan bahwa persepsi keamanan bukan hanya respon emosional, tetapi merupakan refleksi dari ancaman nyata yang terus berkembang dalam ekosistem digital perbankan.

Di sisi lain, beberapa responden juga mengaitkan keamanan dengan kemampuan bank dalam melindungi data pribadi nasabah. Perspektif ini relevan dengan penelitian Hutagaol et al. [14] yang menemukan bahwa tingginya kesadaran pengguna terhadap ancaman siber berbanding lurus dengan meningkatnya tuntutan terhadap keamanan data pada layanan digital. Pengguna semakin menyadari bahwa data pribadi memiliki nilai strategis dan harus dilindungi melalui mekanisme yang transparan dan dapat diverifikasi.

Kekhawatiran tersebut berdiri di atas landasan hukum yang kuat. Dalam konteks regulasi nasional, bank berkewajiban menjaga kerahasiaan, integritas, dan ketersediaan data nasabah sebagaimana dijelaskan dalam kerangka hukum perlindungan data pribadi dan pedoman penyelenggaraan teknologi informasi pada bank umum. Regulasi tersebut mewajibkan bank menerapkan pengendalian akses, melakukan pelaporan insiden keamanan, serta memastikan arsitektur keamanan yang memadai untuk mencegah kebocoran atau penyalahgunaan data pribadi. Temuan kualitatif penelitian ini menunjukkan bahwa pengguna secara intuitif memahami pentingnya kewajiban hukum ini, sehingga membentuk persepsi bahwa keamanan bukan sekadar fitur teknis, tetapi merupakan indikator profesionalisme dan kepatuhan bank terhadap standar nasional.

Selain itu, persepsi risiko juga dipengaruhi oleh transparansi bank dalam menangani ancaman keamanan. Pengguna dalam penelitian ini menunjukkan tingkat kepercayaan yang lebih tinggi ketika bank dinilai responsif terhadap insiden digital dan mampu memberikan edukasi keamanan kepada nasabah. Temuan ini menguatkan studi [15], yang menegaskan bahwa risiko keamanan memiliki efek negatif terhadap kepercayaan pengguna, kecuali jika diimbangi dengan sistem perlindungan dan komunikasi yang efektif. Dengan demikian, aspek perilaku organisasi bank berperan penting dalam membentuk persepsi risiko pengguna.

Dalam konteks peningkatan keamanan e-banking, literatur terbaru menunjukkan bahwa indikator keamanan seperti autentikasi berlapis, enkripsi, dan deteksi aktivitas anomali secara signifikan memperkuat persepsi keandalan sistem (Pramesti & Damayanthi, 2024). Hasil penelitian ini memperlihatkan pola serupa, di mana responden yang menyadari keberadaan fitur-fitur keamanan cenderung memiliki persepsi risiko lebih rendah dan tingkat kepercayaan yang lebih tinggi. Hal ini menunjukkan bahwa pemahaman pengguna terhadap mekanisme keamanan berkontribusi pada pembentukan persepsi positif terhadap layanan digital.

Secara keseluruhan, hasil temuan ini mengindikasikan bahwa risiko keamanan dalam e-banking tidak hanya dipahami sebagai ancaman teknis, tetapi juga sebagai indikator kredibilitas lembaga perbankan. Persepsi keamanan terbentuk melalui kombinasi antara pengalaman pengguna, edukasi bank, serta kepatuhan bank terhadap regulasi perlindungan data yang berlaku. Jika bank mampu menunjukkan komitmen terhadap perlindungan data pribadi dan pengelolaan risiko yang efektif, maka persepsi risiko pengguna dapat ditekan, sehingga kepercayaan dan niat berkelanjutan untuk menggunakan layanan e-banking dapat meningkat secara signifikan.

Pasal-pasal yang mencakup poin-poin di atas meliputi:

- UU ITE Pasal 30 - Akses Ilegal
- UU ITE Pasal 35 - Manipulasi Informasi Elektronik
- UU ITE Pasal 32 ayat (1–2) - melarang pengambilan atau memindahkan data elektronik milik orang lain.
- UU Perbankan Pasal 40 - Rahasia Bank
- UU ITE Pasal 33 - Gangguan Sistem Elektronik
- UU ITE Pasal 32 ayat (1) - Melarang merusak, mengacaukan, dan menghentikan sistem elektronik
- UU ITE Pasal 28 ayat (1) - Dilarang menyebarkan informasi menyesatkan yang merugikan konsumen.
- UU Perbankan Pasal 40 – Rahasia Bank

3.2. Performa Sistem dan Standar Layanan Digital Perbankan

Performa sistem—termasuk ketersediaan layanan (*availability*), kecepatan proses transaksi, dan konsistensi respons aplikasi—menjadi indikator utama yang digunakan pengguna untuk menilai profesionalisme dan kualitas layanan bank digital. Studi kasus dan penelitian lokal menunjukkan bahwa ketidakstabilan aplikasi (misal latency tinggi, kegagalan transaksi, *downtime*) secara konsisten menurunkan kepuasan dan kepercayaan pengguna, sedangkan ketersediaan fitur dan responsifitas sistem meningkatkan kenyamanan dan niat penggunaan kembali.

Secara regulatif, POJK No.11/POJK.03/2022 mengamanatkan tata kelola penyelenggaraan Teknologi Informasi oleh bank umum yang mencakup kewajiban menjaga kontinuitas layanan, manajemen risiko TI, serta mekanisme pelaporan insiden. POJK mengatur

ketentuan pelaporan notifikasi awal insiden TI paling lambat 1x24 jam dan laporan lengkap paling lambat 5 hari kerja (diatur pada ketentuan pelaporan dan sanksi terkait pelaporan insiden), serta mewajibkan bank melakukan penilaian tingkat maturitas digital minimal sekali tiap tahun (Pasal tentang pelaporan insiden dan Pasal 66 mengenai penilaian maturitas digital). Implementasi kewajiban ini secara langsung menuntut bank untuk menjaga indikator performa teknis agar tidak melanggar ketentuan pengawasan OJK.

Dari perspektif perlindungan data, UU No.27 Tahun 2022 tentang Perlindungan Data Pribadi mempertegas bahwa pengendali data wajib menjamin keamanan pemrosesan data (Pasal 35) dan melakukan pemberitahuan apabila terjadi kegagalan pelindungan data; Pasal 46 mewajibkan pemberitahuan tertulis kepada subjek data paling lambat 3×24 jam bila terjadi kegagalan perlindungan yang berdampak signifikan. Karena data keuangan dikategorikan sebagai data pribadi spesifik yang memerlukan perlindungan lebih tinggi (Pasal 4 ayat (2)), maka desain performa sistem (mis. redundansi, *disaster recovery*, pemulihan layanan) juga menjadi bagian dari kewajiban kepatuhan hukum—bukan sekadar aspek teknis internal.

Implikasinya, perbaikan performa tidak hanya meningkatkan kepuasan pengguna tetapi juga memenuhi kewajiban tata kelola dan pelaporan menurut OJK; oleh karena itu rekomendasi teknis yang sering muncul dalam literatur lokal mencakup penerapan SLA/SLI, monitoring real-time, loadbalancing, uji beban berkala, dan rencana pemulihan bencana (disaster recovery plan) yang terdokumentasi. Langkah-langkah ini selaras dengan ketentuan POJK terkait arsitektur TI, audit internal TI, dan pelaporan realisasi penyelenggaraan TI kepada OJK (sebagai bagian intelektual dan operasional yang mengikat secara regulatif).

3.3. Integrasi Keamanan dan Performa dalam Pembentukan Persepsi Pengguna

Integrasi antara keamanan dan performa sistem menjadi faktor krusial dalam membentuk persepsi pengguna terhadap layanan e-banking. Pengguna tidak hanya mengevaluasi keamanan dari sisi teknis seperti enkripsi, autentikasi, dan perlindungan terhadap akses ilegal, tetapi juga menilai performa layanan melalui kecepatan transaksi, kestabilan aplikasi, dan minimnya gangguan operasional. Ketika kedua aspek ini berjalan selaras, persepsi pengguna terhadap kualitas layanan meningkat signifikan. Kerangka regulatif nasional juga memperkuat pentingnya integrasi ini.

POJK No.11/POJK.03/2022 Pasal 36 menegaskan kewajiban bank memastikan ketersediaan dan keandalan layanan TI, sedangkan Pasal 48–51 mengatur manajemen serta pelaporan insiden yang berdampak langsung terhadap transparansi dan kepercayaan pengguna. Dari sisi perlindungan data, UU No.27 Tahun 2022 Pasal 35 mengamanatkan kewajiban pengendali data untuk menjaga keamanan pemrosesan data pribadi, yang berarti kegagalan performa sistem juga dapat memicu risiko terhadap keamanan data.
Regulasi Bank Indonesia melalui PBI 22/23/2020 menekankan kelancaran, kontinuitas, dan reliabilitas sistem pembayaran digital sebagai standar layanan. Dengan demikian, persepsi positif pengguna tidak hanya bergantung pada seberapa aman suatu sistem, tetapi juga pada sejauh mana performa teknis mendukung pengalaman digital yang cepat, stabil, dan dapat dipercaya. Integrasi keamanan dan performa inilah yang akhirnya menciptakan persepsi bahwa layanan e-banking profesional, modern, dan layak digunakan secara berkelanjutan.

Di Indonesia sendiri keamanan dan performa layanan e-banking memiliki landasan regulatif yang kuat. POJK No.11/2022 menegaskan kewajiban bank menjaga keandalan dan keamanan layanan TI melalui Pasal 11, Pasal 36, serta ketentuan manajemen insiden pada Pasal 48–51. Perlindungan data nasabah diperkuat melalui UU PDP 2022, khususnya Pasal 4, Pasal 20, Pasal 35, dan Pasal 46 mengenai kewajiban keamanan dan pelaporan insiden.

Regulasi Bank Indonesia seperti PBI 22/23/2020 dan PBI 19/12/2017 mengatur keandalan sistem pembayaran, kelancaran layanan, transparansi risiko, serta penanganan keluhan pengguna. BSSN melalui Peraturan No.4/2021 menambah kerangka manajemen insiden siber. Seluruh ketentuan ini membentuk fondasi nasional bagi kepercayaan dan persepsi positif pengguna terhadap layanan e-banking.

Untuk menghadapi ancaman *cyber crime* yang semakin kompleks, bank menerapkan berbagai strategi *cyber security*. Hasil pembahasan menunjukkan bahwa semakin kuat tingkat keamanan siber yang diterapkan bank, semakin rendah kerentanan terhadap serangan. Pengaruh *cyber security* terlihat pada beberapa aspek berikut:

a. Peningkatan Perlindungan Data dan Sistem
   Penerapan enkripsi, firewall, sistem deteksi intruksi (IDS/IPS), dan penguatan autentikasi dua faktor (2FA/OTP) terbukti efektif menurunkan peluang serangan berhasil. Bank yang menerapkan standar keamanan tinggi menunjukkan tingkat insiden yang lebih rendah.
b. Deteksi dan Respons Insiden yang Lebih Cepat
   Adanya tim khusus keamanan siber (*security operation center*/SOC) serta penggunaan teknologi monitoring real-time membantu bank mendeteksi aktivitas mencurigakan sejak dini. Respons cepat dapat mengurangi dampak kerugian dan mencegah serangan yang lebih luas.
c. Meningkatkan Kesadaran Nasabah
   Bagian dari *cyber security* adalah edukasi nasabah. Bank yang secara aktif memberikan edukasi mengenai bahaya phishing, penipuan, dan pentingnya menjaga kerahasiaan OTP terbukti memiliki tingkat kasus kejahatan siber yang lebih rendah.
d. Meningkatkan Kepercayaan Pengguna terhadap Layanan Digital
   Ketika bank menerapkan standar keamanan yang kuat dan transparan, nasabah merasa lebih aman dalam menggunakan layanan *internet banking* dan *mobile banking*. Ini berdampak positif terhadap kepuasan dan loyalitas nasabah.

Pasal-pasal yang mencakup poin-poin di atas meliputi:

- UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022) Pasal 35–36
- UU Perbankan Pasal 40 - Bank wajib menjaga kerahasiaan data nasabah.
- POJK Sistem Elektronik Perbankan (POJK No. 38/POJK.03/2016)
- UU PDP Pasal 46 - Pengendali data wajib melaporkan insiden kebocoran data sesegera mungkin.
- POJK Perlindungan Konsumen (POJK 6/POJK.07/2022)
- UU ITE Pasal 36 - Tindakan ilegal yang menyebabkan kerugian bagi pengguna dikenakan sanksi lebih berat.
- UU Perbankan Pasal 47 - Pegawai bank yang membocorkan data rahasia dapat dipidana.

- UU PDP Pasal 51 - Jika bank gagal melindungi data maka mendapat sanksi administratif dan pidana

3.4. Pengaruh Risiko terhadap Kepercayaan dan Niat Penggunaan

Risiko keamanan dan risiko performa terbukti memiliki pengaruh langsung terhadap tingkat kepercayaan (*trust*) dan niat penggunaan ulang layanan e-banking. Ketika pengguna menghadapi potensi ancaman seperti pencurian data, akses ilegal, atau serangan siber, persepsi risiko meningkat dan trust terhadap bank menurun. Kondisi ini diperkuat oleh temuan regulatif yang menempatkan keamanan dan performa sebagai kewajiban hukum. POJK No.11/POJK.03/2022 Pasal 36 mewajibkan bank memastikan keandalan layanan TI, sementara Pasal 48 dan 51 mengatur manajemen serta pelaporan insiden sebagai bentuk transparansi dan akuntabilitas kepada pengguna.

Dari perspektif perlindungan data, UU No.27 Tahun 2022 (UU PDP) Pasal 35 dan Pasal 46 memperjelas kewajiban bank untuk menjaga keamanan data pribadi serta memberikan notifikasi insiden kepada nasabah dalam batas waktu tertentu. Ketentuan ini berfungsi sebagai jaminan legal yang memperkuat persepsi pengguna bahwa hak-hak digital mereka dilindungi secara formal. Di sisi performa, standar kelancaran transaksi dan reliabilitas sistem yang diatur dalam PBI No.22/23/2020 menjadi indikator yang memengaruhi niat penggunaan ulang; gangguan layanan yang sering terjadi dapat menurunkan persepsi profesionalisme bank dan menghambat adopsi berkelanjutan. Dengan demikian, semakin rendah persepsi risiko dan semakin kuat bukti kepatuhan bank terhadap regulasi keamanan dan performa, semakin tinggi pula kepercayaan dan niat pengguna untuk terus memanfaatkan layanan e-banking.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa persepsi pengguna terhadap layanan e-banking sangat dipengaruhi oleh dua faktor utama, yaitu risiko keamanan dan risiko performa sistem. Risiko keamanan, yang mencakup kekhawatiran terhadap pencurian data, serangan siber, akses ilegal, dan pelanggaran privasi, terbukti memiliki pengaruh signifikan terhadap tingkat kepercayaan pengguna. Ketika pengguna merasa bahwa data pribadinya tidak terlindungi, persepsi risiko meningkat dan trust terhadap bank menurun. Hal ini sejalan dengan ketentuan dalam POJK No.11/POJK.03/2022 serta UU No.27/2022 tentang Perlindungan Data Pribadi yang menekankan kewajiban bank menjaga keandalan, keamanan, dan akuntabilitas pemrosesan data pribadi.

Selain keamanan, risiko performa juga memberikan kontribusi penting terhadap pembentukan persepsi pengguna. Kestabilan aplikasi, kecepatan transaksi, reliabilitas server, dan minimnya gangguan operasional menjadi indikator utama penilaian pengguna terhadap profesionalisme layanan digital bank. Sistem yang lambat atau sering mengalami error menurunkan persepsi kualitas layanan dan berdampak pada berkurangnya niat penggunaan ulang. Regulasi Bank Indonesia, khususnya PBI No.22/23/2020 dan PBI No.19/12/2017, memperkuat standar performa layanan digital melalui kewajiban kelancaran transaksi, kontinuitas operasional, serta transparansi informasi risiko kepada konsumen.

Temuan penelitian ini juga menegaskan bahwa kepercayaan merupakan variabel kunci yang memediasi pengaruh risiko keamanan dan performa terhadap niat penggunaan e-banking. Semakin rendah persepsi risiko dan semakin tinggi kepatuhan bank terhadap regulasi keamanan serta standar operasional digital, semakin positif persepsi pengguna terhadap kualitas layanan. Integrasi kedua aspek—keamanan dan performa—menjadi fondasi utama pembentukan persepsi pengguna bahwa e-banking adalah layanan yang aman, andal, dan layak digunakan secara berkelanjutan.

Dengan demikian, penelitian ini menyimpulkan bahwa penguatan sistem keamanan, peningkatan kualitas performa, peningkatan kesadaran risiko digital, serta kepatuhan terhadap regulasi nasional merupakan strategi utama untuk meningkatkan kepercayaan dan mendorong adopsi e-banking. Bank perlu mengintegrasikan aspek teknis, operasional, dan tata kelola risiko secara holistik agar mampu membangun pengalaman digital yang aman, stabil, dan sesuai dengan ekspektasi masyarakat di era transformasi digital.

DAFTAR PUSTAKA

[1] Afghani, M. F., dan Yulianti, E. (2017). *Persepsi Risiko serta Kesadaran Nasabah Terhadap Adopsi e-Banking di BRI Surabaya*. Volume *6* Nomor 1, Halaman 113–128. https://doi.org/10.14414/jbb.v6i1.

[2] Akuntansi, J., Ramadhani, S., Arita, E. (2025). *Pengaruh E-Banking dan Mobile Banking Terhadap Kinerja Keuangan pada Perbankan Konvensional di Kota Padang*. Volume *2* Nomor 1, Halaman 206–216.

[3] Aurora, M. D., Ramadhany, A. A., Richmayati, M., Akuntansi, M., Ekonomi, F., Sina, U. I. (2025). *Keamanan Terhadap Tingkat Transaksi Nasabah Menggunakan Mobile Banking PT. Bank Negara Indonesia (Persero), Tbk. Wilayah Batam*. Volume *3* Nomor 2, Halaman 87–104.

[4] Bertransaksi, M., dan Secara, U. (2015). *No Title*.

[5] Hutagaol, B. J., Sitorus, R. S., Hutagaol, N. (2024). *Identifikasi Tingkat Kesadaran Pengguna Mobile Banking Terhadap Ancaman Cybercrime*. Volume *7* Nomor 3. https://doi.org/10.32493/jtsi.v7i3.41639

[6] Ilmiah, M., dan Vol, S. (2020). *No Title*. Volume *18 Nomor* 4.

[7] Juli, V. N., Saputra, A. T., Awka, A. M., & Ghoni, A. (2024). *Pengaruh Persepsi Kemudahan, Manfaat dan Risiko Terhadap Minat Mahasiswa Menggunakan Mobile Banking dan E-Wallet (Studi Kasus IAIN Syekh Nurjati Cirebon)*. Volume *3* Nomor 1.

[8] Kasus, S., Nasabah, P., BNI, E. B. (2022). *1, 2 1, 2*. Volume *1 Nomor* 8, Halaman 1665–1672.

[9] Kemanfaatan, P. P., Fitur, D. A. N., Terhadap, L. (2015). *Minat Penggunaan Berulang E-Banking*.

[10] Kepercayaan, P., dan Fauziah, A. (n.d.). *E-Banking (Survei pada Nasabah BRI Syariah di Kota Palu)*. Volume *3 Nomor* 1.

[11] Pengguna, N., Literasi, E. P., Ayu, N., Dewi, S. (2025). *Dampak E-Security dan Risk Perception Terhadap E-Trust*. Volume *23* Nomor 2.

[12] Permana, K. K., Eprianto, I., Fauzi, A., Minarny, T., Fajriansyah, D. N. (2024). *Pengaruh Keamanan Data Pribadi Terhadap Kepercayaan Pengguna di Era Tranformasi Digital : Studi Kasus pada Aplikasi Mobile Banking*. Volume *1 Nomor* 1, Halaman 37–46.

[13] Syariah, J. E., dan Ekonomi, F. (2021). *Analisis Pengaruh Kepercayaan Nasabah Terhadap Risiko Menggunakan Layanan E-Banking*. Halaman 28–38.

[14] Tanuwijaya, A., dan Arifin, A. Z. (2023). *Persepsi Risiko Pada Penggunaan M-Banking Dalam*. Volume *11 Nomor* 2, Halaman 165–180.

[15] Yudha, H. N., Prof, J., dan Sh, S. (2015). *Analisis Pengaruh Persepsi Nasabah Bank Terhadap Internet Banking Adoption (Studi pada Nasabah Perbankan yang Menggunakan Internet Banking di Kota Surakarta)*. Volume *4*, Halaman 1–15.