International, Journal of Islamic Business Management (IJMBS), Vol. 4 (4) 2025
E-ISSN : 2963-2218 Hal. 52-56

PERAN SOFTWARE CYBER SECURITY DALAM MENJAGA KEPERCAYAAN NASABAH PADA TRANSAKSI DIGITAL BSI

Dwi Adinda Putri[1], Nur Aisyah[2], Sabhi Febrian[3], Nurbaiti[4]
Universitas Islam Negeri Sumatera Utara
[1]dwiadindaputrii@gmail.com, [2]aisyahsmara@gmail.com, [3]sabhifebrian06@gmail.com,
[4]nurbaiti@uinsu.ac.id

Menerima:
10/12/2025

Diterima:
11/12/2025

Menerbitkan:
12/12/2025

Abstrak
Penelitian ini bertujuan menganalisis peran dan dampak persepsi nasabah terhadap *software* keamanan siber yang diterapkan oleh Bank Syariah Indonesia (BSI) dalam membangun kepercayaan (*E-Trust*), khususnya dalam konteks kewajiban *Amanah* Syariah. Menggunakan metodologi kualitatif melalui Netnography dan Analisis Konten terhadap ulasan pengguna BSI Mobile dan dokumen resmi bank, penelitian ini menemukan bahwa *software* keamanan BSI memiliki peran ganda yang volatil. Kegagalan fungsional *software* autentikasi *frontend* (Biometrik/OTP) secara langsung merusak Keyakinan Struktural dan Kapabilitas bank, sementara *E-Trust* sangat sensitif terhadap ketersediaan sistem (*Availability*), di mana *downtime* dianggap melanggar prinsip Amanah. BSI juga dinilai kurang transparan dalam mengkomunikasikan *tujuan perlindungan software*. Disimpulkan bahwa *software* keamanan adalah pilar *E-Trust* BSI, namun kegagalan fungsional sekecil apa pun mengikis kepercayaan. Saran utama adalah memprioritaskan optimalisasi *usability software frontend* untuk menjaga *e-trust* nasabah.

Kata Kunci: Cybersecurity, Kepercayaan Nasabah, BSI

PENDAHULUAN

Layanan digital telah menjadi tulang punggung transaksi finansial modern, dengan menawarkan kemudahan akses, kecepatan, dan efesiensi yang tak tertandingi dalam bertransaksi. Transformasi digital kini telah bergeser dari sekadar fitur tambahan menjadi kebutuhan inti bagi bank agar tetap relevan dan kompetitif. Di Indonesia, dampak perubahan digital ini sangat signifikan, khususnya dalam industri perbankan syariah. PT Bank Syariah Indonesia Tbk (BSI), yang merupakan gabungan dari bank-bank syariah milik negara dan kini menjadi bank syariah terbesar di negeri ini, menjadikan layanan digital sebagai tulang punggung operasional utamanya. BSI meluncurkan aplikasi mobile banking mereka, Byond by BSI untuk melayani jutaan nasabah. Adopsi masif layanan ini menunjukkan komitmen BSI dalam memimpin inklusi keuangan syariah digital. Meningkatnya adopsi teknologi finansial ini secara eksponensial juga berbanding lurus dengan peningkatan risiko ancaman siber (Priyadi, 2023). Dalam konteks transaksi digital, isu keamanan bukan hanya masalh teknis, tetapi merupakan fondasi psikologis yang membangun kepercayaan nasabah (*Customer Trust*). Aspek ini menjadi semakin vital bagi perbankan Syariah. Hal ini mengingat landasan utama dalam prinsip Muamalat adalah amanah (kepercayaan) dan maslahah (manfaat untuk umum) (Shubhie, 2025). Menurut (Putri et al., 2023), serangan digital seperti phishing, malware, dan insiden kebocoran data memiliki potensi besar untuk merusak citra bank, mengakibatkan kerugian materi, dan yang paling kritis, melenyapkan kepercayaan nasabah yang selama ini susah payah dipertahankan.

Komitmen BSI dalam menghadapi tantangan ini diwujudkan melalui alokasi sumber daya yang signifikan; BSI, misalnya, telah melaporkan peningkatan investasi pada infrastruktur keamanan siber sebesar Rp1,5 triliun pada tahun fiskal 2024 untuk memperkuat *Security Operations Center* (SOC) dan *Fraud Detection System* (FDS). Dengan demikian, perangkat lunak keamanan siber termasuk *Multi-Factor Authentication* (MFA), sistem pendeteksi kecurangan (*fraud*), dan teknologi enkripsi yang telah diterapkan oleh BSI memegang peranan yang sangat menentukan. Aplikasi keamanan ini berfungsi sebagai benteng pertahanan utama BSI untuk melindungi keutuhan data dan mengamankan setiap transaksi. Kualitas dan efektivitas dari software keamanan tersebut akan tercermin secara langsung pada pengalaman yang dirasakan nasabah ketika bertransaksi melalui saluran digital BSI. Meskipun sudah banyak penelitian mengenai adopsi teknologi di bank syariah atau manajemen risiko siber secara garis besar, masih jarang ditemukan studi yang secara spesifik meneliti bagaimana implementasi software keamanan oleh BSI memengaruhi persepsi keamanan, yang kemudian berujung pada tingkat kepercayaan nasabah. Mengingat BSI adalah bank Syariah yang sangat menjunjung tinggi prinsip amanah (kepercayaan), diperlukan adanya pemahaman yang komprehensif tentang hubungan sebab-akibat antara performa sistem keamanan berbasis perangkat lunak dengan e-trust (kepercayaan digital) nasabah mereka.

TINJAUAN PUSTAKA

Keamanan Siber (*Cybersecurity*) dan Software Keamanan

Cybersecurity berasal dari gabungan dua kata, yaitu *cyber* yang berarti dunia maya atau internet, dan *security* yang berarti keamanan. Dengan demikian, secara sederhana, *cybersecurity* dapat diartikan sebagai keamanan siber. Keamanan siber memiliki fungsi dan peran penting dalam mendeteksi, memperbaiki, serta meminimalkan risiko terjadinya ancaman (*cyber threat*) maupun serangan siber Selain itu, *cybersecurity* juga mencakup segala upaya untuk melindungi berbagai komponen dalam sistem siber, termasuk perangkat keras (*hardware*), perangkat lunak (*software*), data atau informasi, serta infrastruktur yang digunakan. Keamanan siber memiliki sifat yang harus proaktif, tidak hanya sebatas reaktif (menunggu dan menanggapi serangan). Dalam praktiknya, perangkat lunak keamanan merupakan perwujudan teknis dari seluruh strategi pengamanan. Perangkat ini melibatkan *software* yang bekerja di balik layar (*backend*), seperti *Security Information and Event Management* (SIEM) dan *Intrusion Detection Systems* (IDS), serta *software* di bagian antarmuka (*frontend*) yang berinteraksi langsung dengan nasabah, contohnya *Multi-Factor Authentication* (MFA) dan Biometrik. Salah satu software paling penting di perbankan adalah FDS. FDS menggunakan algoritma *machine learning* untuk menganalisis pola transaksi *real-time* dan mengidentifikasi anomali yang mengindikasikan aktivitas penipuan. Keakuratan dan kecepatan FDS secara langsung memengaruhi trust nasabah dan kerugian bank (Ismanda & Silitonga, 2025).

Kepercayaan Nasabah (*Customer Trust*)

Implementasi *software* keamanan yang berhasil dan efektif pada dasarnya bertujuan untuk mencapai kepercayaan sebagai hasil akhir. Dalam konteks digital, karena nasabah sering tidak memiliki kontak pribadi dengan penyedia jasa, kepercayaan mereka lebih bergantung pada Keyakinan Struktural yakni, anggapan nasabah terhadap mekanisme jaminan dan keselamatan yang disediakan oleh sistem. Apabila software keamanan BSI Mobile mengalami gangguan (contohnya, biometrik merespon lambat atau notifikasi OTP tidak terkirim), hal ini secara langsung

mencederai Keyakinan Struktural nasabah. Kegagalan tersebut akan merusak pandangan nasabah terhadap Kapabilitas teknis bank, yang pada akhirnya dapat mendorong nasabah untuk berpindah layanan (switching behavior) seperti yang disoroti oleh (Astuti, 2023).

Bank Syariah Indonesia

Bank Syariah Indonesia (BSI) didirikan secara resmi pada 1 Februari 2021, sebagai hasil penggabungan (merger) tiga Bank Umum Syariah (BUS) milik Himbara (Himpunan Bank Milik Negara): PT Bank BRI syariah Tbk, PT Bank Syariah Mandiri, dan PT Bank BNI Syariah. Penggabungan ini menghasilkan pembentukan entitas bank Syariah terbesar di Indonesia, baik dari sisi aset maupun luasnya jaringan. Oleh karena itu, peran BSI menjadi amat penting karena bank ini merepresentasikan penggabungan kekuatan perbankan Syariah di tingkat nasional dalam rangka menghadapi persaingan, baik di dalam negeri maupun di kancah global (Hisam, 2023). Sejak pembentukannya, BSI menempatkan transformasi digital sebagai pilar strategi utama. Hal ini diwujudkan melalui pengandalan pada kanal-kanal elektronik, yang paling utama adalah aplikasi mobile banking. BSI Mobile (Byond by BSI) berfungsi sebagai antarmuka utama bagi nasabah untuk mengakses layanan bank. Kualitas kinerja dari software BSI Mobile ini khususnya dari aspek kecepatan bertransaksi, kemudahan penggunaan (usability), serta fitur keamanan frontend (seperti penggunaan login biometrik dan OTP) secara langsung menjadi indikator mutu layanan digital (E-Service Quality) yang ditawarkan oleh BSI.

METODOLOGI

Metode Penelitian

Penelitian ini menggunakan metode enelitian Kualitatif Deskriptif. Penelitian ini bertujuan untuk mendeskripsikan, menginterpretasikan, dan memahami fenomena sentimen dan pengalaman nasabah terkait aspek keamanan software BSI Mobile. Penelitian ini juga menggunakan pendekatan penelitian Netnography. Netnography digunakan untuk mempelajari perilaku dan pengalaman nasabah (sebagai komunitas *online*) yang terekspresikan melalui teks di ruang digital.

Data

Penelitian ini menggunakan dua jenis data utama:

1. Data Primer Digital (Netnography)

   Teks yang berasal dari ulasan nasabah yang merefleksikan pengalaman langsung mereka terkait fungsionalitas dan kegagalan software keamanan BSI Mobile.

2. Data Sekunder Dokumen

   Dokumen resmi yang digunakan sebagai pembanding untuk narasi keamanan BSI. Sumber data diambil dari laporan tahunan BSI (bagian *Risk management* dan IT *Governance*), halaman resmi *website* BSI terkait keamanan dan privasi data, dan *Press Release* BSI mengenai peningkatan fitur keamanan *software.*

Teknik Analisis Data

Data kualitatif yang terkumpul (teks ulasan dan konten dokumen) akan dianalisis menggunakan Analisis Tematik (Thematic Analysis) enam fase yang diadaptasi dari Braun & Clarke (2006).

HASIL DAN ANALISIS

Hasil

Analisis tematik kualitatif terhadap ulasan nasabah (Netnography) serta dokumen resmi BSI mengungkap tiga poin utama mengenai kontribusi perangkat lunak keamanan BSI terhadap pembentukan E-Trust:

1. **Kesenjangan Kinerja Frontend**
   Terdapat perbedaan antara pernyataan BSI mengenai keandalan sistem keamanan pada sisi backend (seperti pemenuhan standar ISO) dan pengalaman nyata yang dirasakan nasabah melalui perangkat lunak yang mereka gunakan setiap hari. Fitur penting, seperti autentikasi biometrik dan OTP, kerap mengalami kegagalan atau keterlambatan, dan kondisi ini diterjemahkan oleh nasabah sebagai keterbatasan kemampuan teknis bank.
2. **Kepercayaan yang Bergantung pada Ketersediaan Sistem**
   Tingkat kepercayaan nasabah sangat ditentukan oleh konsistensi ketersediaan layanan (*Availability*) yang bergantung pada perangkat lunak. Keluhan terkait gangguan layanan yang muncul tanpa peringatan menjadi sumber sentimen negatif paling kuat, karena dipandang sebagai kegagalan BSI dalam memenuhi Amanah kepercayaan yang bersifat syariah untuk menjaga akses nasabah terhadap dana mereka.
3. **Ambiguitas dalam Komunikasi**
   Mekanisme keamanan perangkat lunak, seperti pemblokiran otomatis pada akun, sering dipahami sebagai hambatan layanan alih-alih perlindungan. Hal ini disebabkan ketidakmampuan BSI menjelaskan alasan di balik tindakan sistem tersebut, sehingga menurunkan persepsi nasabah terhadap unsur Keikhlasan (*Benevolence*) bank

Analisis

Temuan ini menegaskan bahwa perangkat lunak keamanan BSI memegang dua peran yang bersifat fluktuatif. Pertama, perangkat lunak menjadi sumber utama kerentanan psikologis bagi nasabah. Ketidakandalan fungsi pada sisi frontend secara langsung melemahkan Keyakinan Struktural (McKnight & Chervany, 2001). Nasabah menilai kualitas keamanan BSI melalui kestabilan antarmuka yang mereka gunakan sehari-hari, bukan melalui sertifikasi teknis yang tidak tampak. Kedua, hasil penelitian menunjukkan bahwa gangguan pada perangkat lunak BSI tidak hanya merupakan persoalan teknis, tetapi juga memiliki dimensi etis. Ketidaktersediaan layanan dipersepsikan sebagai bentuk kelalaian terhadap amanah sehingga dampaknya terhadap E-Trust menjadi lebih besar dibandingkan konteks perbankan konvensional.
Untuk mempertahankan *e-trust*, BSI perlu mengutamakan peningkatan aspek usability pada perangkat lunak keamanan di sisi frontend (Biometrik/OTP) serta memperkuat keterbukaan dalam komunikasi agar nasabah memahami bahwa tindakan sistem dirancang untuk melindungi mereka.

Kesimpulan

Penelitian ini menyimpulkan bahwa peran perangkat lunak keamanan siber dalam mempertahankan kepercayaan (*E-Trust*) nasabah BSI bersifat dualistik dan

sangat mudah terganggu. Tingkat kepercayaan nasabah bergantung pada performa software yang mereka amati secara langsung; kegagalan pada fitur frontend seperti Biometrik dan OTP segera melemahkan Keyakinan Struktural terhadap kemampuan teknis bank. Selain itu, E-Trust menunjukkan sensitivitas tinggi terhadap aspek ketersediaan layanan (*Availability*) yang ditopang oleh *software*, di mana terjadinya downtime dipandang sebagai pelanggaran serius terhadap prinsip Amanah dalam perspektif syariah. Di samping itu, BSI perlu memperbaiki keterbukaan dalam menjelaskan mekanisme software keamanannya karena saat ini kompleksitas sistem tersebut sering dipersepsikan sebagai hambatan layanan, bukan sebagai bentuk proteksi. Secara keseluruhan, guna mempertahankan *E-Trust*, perangkat lunak keamanan BSI harus beroperasi dengan stabil, andal, dan disertai komunikasi yang transparan.

REFERENSI

Astuti, A. R. T. (2023). The effect of E-Service Quality on E-loyalty is mediated by E-Trust at Bank Syariah Indonesia. *YMER*, *22*(3), 1279–1294.

Hisam, M. (2023). Tinjauan kinerja Bank Syariah Indonesia (BSI): Perkuat aset dan visi misi yang efektif. *Currency (Jurnal Ekonomi Dan Perbankan Syariah)*, *2*(1), 202–221.

Ismanda, R. S., & Silitonga, M. T. A. (2025). Deteksi Hybrid Anomali Transaksi Digital dengan Optimasi Isolation Forest-K-Means untuk Peningkatan Keamanan Finansial. *Innovative: Journal Of Social Science Research*, *5*(3), 5749–5765.

Priyadi, W. (2023). Cara sitasi: Wiwit Priyadi. 2023. Analisis Cyber Security Pada Pengguna Mobile Banking Di Indonesia. *Bina Insani ICT Journal*, *10*(1), 92–103.

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173–181.

Shubhie, H. M. (2025). *FIQIH MUAMALAT*. Uwais Inspirasi Indonesia.