

ANALISIS RISIKO DALAM DIGITALISASI PERBANKAN SYARIAH: TANTANGAN DAN SOLUSI

Amhar Maulana Harahap

Institut Agama Islam Padang Lawas
Jalan Kihajar Dewantara No.66, Huta Ibus, Kabupaten Padang Lawas
amharmaulana@gmail.com

Abstrak

Kemajuan teknologi informasi dan komunikasi (TIK) telah mendorong transformasi digital di sektor perbankan, termasuk perbankan syariah. Digitalisasi meningkatkan efisiensi operasional, mengurangi biaya layanan, dan memudahkan nasabah dalam mengakses layanan perbankan. Namun, transformasi ini juga menghadirkan tantangan signifikan, seperti risiko keamanan siber, kebocoran data, serangan ransomware, phishing, dan pencurian identitas. Perbankan syariah dituntut untuk menjaga kerahasiaan, integritas, dan ketersediaan data nasabah dengan menerapkan sistem teknologi informasi yang aman dan sesuai prinsip syariah. Tantangan lain termasuk rendahnya literasi digital nasabah, keterbatasan infrastruktur, dan kurangnya tenaga ahli di bidang teknologi digital. Penelitian ini bertujuan mengidentifikasi risiko digitalisasi perbankan syariah dan merumuskan strategi mitigasi, seperti peningkatan keamanan siber, penguatan infrastruktur teknologi, kolaborasi dengan fintech, dan pengembangan sumber daya manusia. Dengan langkah-langkah ini, diharapkan digitalisasi perbankan syariah dapat berjalan aman, efisien, dan sesuai prinsip syariah, memberikan manfaat optimal bagi seluruh pemangku kepentingan.

Kata kunci: Risiko, Digitalisasi, Perbankan Syariah, Tantangan, Solusi

Abstract

Advances in information and communication technology (ICT) have driven digital transformation in the banking sector, including Islamic banking. Digitalization enhances operational efficiency, reduces service costs, and facilitates customer access to banking services. However, this transformation also presents significant challenges, such as cybersecurity risks, data breaches, ransomware attacks, phishing, and identity theft. Islamic banking is required to maintain the confidentiality, integrity, and availability of customer data by implementing secure information technology systems that align with Sharia principles. Other challenges include low digital literacy among customers, infrastructure limitations, and a shortage of experts in digital technology. This study aims to identify the

risks associated with the digitalization of Islamic banking and formulate mitigation strategies, such as enhancing cybersecurity, strengthening technological infrastructure, collaborating with fintech, and developing human resources. Through these measures, it is hoped that the digitalization of Islamic banking can proceed securely, efficiently, and in accordance with Sharia principles, delivering optimal benefits to all stakeholders.

Keywords: Risk, Digitalisation, Islamic Banking, Challenges, Solutions

A. Pendahuluan

Kemajuan pesat dalam teknologi informasi dan komunikasi (TIK) telah mendorong berbagai perubahan di berbagai sektor, termasuk industri perbankan. Transformasi digital dalam perbankan telah meningkatkan efisiensi operasional, menekan biaya layanan, serta mempermudah nasabah dalam mengakses rekening mereka melalui platform digital. Namun, proses digitalisasi ini juga menghadirkan tantangan signifikan, seperti risiko kehilangan data, serangan ransomware dan malware, phishing, rekayasa sosial, pencurian identitas, serta ancaman siber lainnya. Oleh karena itu, perbankan syariah dituntut untuk menjaga kerahasiaan, integritas, dan ketersediaan data nasabah dengan menerapkan sistem teknologi informasi yang aman serta sesuai dengan prinsip syariah. Ancaman terhadap keamanan dan privasi informasi nasabah terus meningkat seiring dengan berkembangnya serangan siber dan semakin kompleksnya metode kejahatan digital (Zelyn Faizatul, 2023).

Bank-bank syariah di Indonesia perlu menyesuaikan prinsip mereka dengan teknologi digital guna meningkatkan efisiensi dan keamanan sistem. Meskipun demikian, mereka menghadapi berbagai tantangan, seperti keterbatasan informasi yang akurat, gangguan pada jaringan dan infrastruktur, serta lambatnya perkembangan dalam menciptakan sistem informasi yang aman. Oleh karena itu, diperlukan penelitian untuk mengevaluasi risiko yang terkait dengan digitalisasi perbankan syariah



serta mengidentifikasi solusi yang efektif (Fauzatul Laily Nisa & Krisna Reswara, 2024).

Beberapa penelitian sebelumnya menunjukkan bahwa risiko yang dihadapi oleh bank syariah dalam proses digitalisasi cukup signifikan. Penelitian sebelumnya juga telah menunjukkan bahwa bank syariah telah mengembangkan mekanisme mitigasi risiko dan upaya pencegahan atas risiko yang timbul dari layanan mobile banking. Misalnya, penelitian tentang manajemen risiko layanan mobile banking telah menunjukkan bahwa bank syariah telah memiliki mekanisme mitigasi resiko yang efektif, seperti identifikasi risiko komprehensif, penggunaan teknologi keamanan mutakhir, pengawasan dan pemantauan aktif, serta pelatihan dan kesadaran keamanan yang terus-menerus (Oktaviani & Basyariah, 2022). Selain itu, penelitian tentang manajemen risiko perbankan syariah di era digital juga telah menunjukkan pentingnya implementasi sistem keamanan yang tepat dan kolaborasi dengan lembaga keamanan siber untuk mengurangi risiko serangan (bambang rianto rustam, 2018). penelitian yang dilakukan oleh Muneeza menyoroti adanya celah dalam penerapan teknologi digital yang sesuai dengan prinsip syariah, khususnya dalam hal transparansi dan akuntabilitas transaksi (Muneeza et al. 2020). Selain itu, Otoritas Jasa Keuangan (OJK) juga telah mengeluarkan beberapa kebijakan yang mendukung percepatan digitalisasi perbankan syariah melalui penerapan teknologi finansial yang aman dan sesuai dengan aturan syariah(Roadmap Pengembangan Perbankan Syariah Indonesia 2020-2025, 2021). Meskipun demikian, tantangan dalam hal regulasi dan infrastruktur masih menjadi penghambat utama dalam mewujudkan digitalisasi yang optimal di sektor ini.

Salah satu tantangan lain yang dihadapi perbankan syariah adalah rendahnya tingkat literasi digital di kalangan nasabah. Banyak nasabah masih mengandalkan layanan perbankan konvensional dan merasa ragu untuk beralih ke layanan digital. Kondisi ini memperumit proses



digitalisasi, karena bank perlu berinvestasi dalam edukasi dan pelatihan agar nasabah lebih memahami serta terbiasa dengan teknologi baru. Selain itu, bank syariah juga harus memastikan bahwa teknologi yang diterapkan mudah digunakan dan tidak menghambat aksesibilitas, terutama bagi nasabah di wilayah terpencil.

Penelitian ini bertujuan untuk mengidentifikasi berbagai risiko yang dihadapi bank syariah dalam proses digitalisasi serta merumuskan strategi atau solusi yang dapat diterapkan untuk mengurangi risiko tersebut. Dengan demikian, penelitian ini diharapkan dapat berkontribusi dalam pengembangan praktik perbankan syariah yang lebih efisien dan aman di era digital. Selain itu, hasil penelitian ini juga bertujuan memberikan rekomendasi kepada regulator dan industri perbankan syariah guna memperkuat infrastruktur teknologi serta memastikan kepatuhan terhadap prinsip-prinsip syariah dalam setiap aspek digitalisasi. Dengan langkah-langkah ini, diharapkan digitalisasi perbankan syariah dapat berjalan dengan aman, efisien, dan memberikan manfaat optimal bagi seluruh pemangku kepentingan.

B. Tinjauan Teoritis

1. Risiko Digitalisasi dalam Perbankan Syariah

Bank adalah perusahaan yang bergerak pada jenis usaha yang berhubungan dengan aktivitas keuangan dari masyarakat baik itu berupa tabungan, pengkreditan, deposito dan lainnya. Kemampuan bank dapat dilihat dari aspek permodalan, asset, majemen, rentabilitas, likuiditas, dan sensitifitas bank terhadap resiko pasar yang dimiliki oleh masing-masing bank.

Digitalisasi adalah konversi data kedalam format digital dengan adopsi teknologi (Marhamah & fauzi, 2021). Perbankan Digital adalah otomatisasi layanan perbankan tradisional. Perbankan digital memungkinkan nasabah bank untuk mengakses produk dan layanan perbankan melalui platform elektronik/online. Perbankan digital berarti



mendigitalkan semua operasi perbankan dan menggantikan kehadiran fisik bank dengan kehadiran online yang abadi, menghilangkan kebutuhan konsumen untuk mengunjungi cabang (Gultom & Rokan, 2022).

Analisis Risk (Risiko) yang dihadapi Bank Syariah Indonesia Dengan Adanya Digitalisasi Produk Perbankan. Aspek risk adalah berbagai risiko yang harus ditanggung Bank Syariah Indonesia karena adanya digitalisasi produk perbankan. Diagram dibawah ini menunjukkan paparan data dari cluster risk.



Gambar 1. Data cluster risk

Berdasarkan diagram diatas dapat kita ketahui bahwa indikator dari cluster risk itu ada 5 yaitu tingkat literasi masyarakat, safety, promosi, jaringan, dan hak privasi. Hak privasi menjadi indikator utama dalam cluster risk. Kurangnya perlindungan hak privasi. Karyawan bank bisa mengetahui tentang data nasabah dan dana yang tersimpan karena banyak dari mereka yang memiliki akses tersebut, sehingga apabila ada beberapa orang dari pihak bank yang memiliki niat buruk terhadap dana nasabah pasti akan di salah gunakan untuk kepentingan pihak karyawan bank itu sendiri.Safety menjadi indikator kedua dalam cluster, Dengan adanya digitalisasi rawan akan pembobolan dan keamanan. Pihak bank sering beranggapan hal tersebut terjadi karena nasabah lalai dan lupa pin akses.Tingkat literasi masyarakat menjadi indikator ketiga dalam cluster risk dengan Tingkat pengetahuan dan literasi masyarakat tentang sistem dan produk syariah juga masih minim. Untuk meningkatkan

pengetahuan tentang sistem dan produk perbankan syariah, maka bank perlu menjadikan kemajuan teknologi ini sebagaisarana literasi melalui digital. Jaringan menjadi indikator keempat dalam cluster risk dengan Kesulitan nasabah dalam pelayanan digitalisasi ini adalah susahnya mengakses aplikasi karena sistem jaringan yang terkadang tidak stabil. Promosi menjadi indikator kelima dalam cluster, Karena banyaknya bank yang telah lebih dulu menerapkan digitalisasi. Maka Bank Syariah Indonesia harus lebih gencar dalam melakukan promosi mengenai penggunaan digitalisasi beserta fungsinya (adhitya mahardhika dkk., 2021).

Perbankan merupakan industry yang harus responsive terhadap berbagai risiko fundamental yang dapat mempengaruhi kinerjanya (Kurniawan, Rahayu, & Wibowo, 2021). Menurut Vaidyula & Kavala (2018) Manajemen risiko pada industry perbankan menjadi sorotan, terutama setelah terjadinya gejolak yang terjadi belakangan ini, yang memberikan dampak yang sangat buruk terhadap eksistensi sektor perbankan sebagai industry yang layak. Tidak hanya perbankan, bahkan berbagai instansi pemerintahpun telah menyadari akibat atau dampak dari tidak efektifnya pengelolaan risiko pada bank, oleh karena itu telah ditetapkan beberapa peraturan untuk mengendalikan risiko-risiko yang timbul dalam bisnis industry perbankan. Beberapa resiko yang menjadi perhatian serius adalah terkait kebocoran data nasabah serta adanya berbagai serangan siber yang sering terjadi. Risiko kebocoran data nasabah merupakan risiko yang muncul karena adanya pengunggahan data pribadi yang bersifat sensitive, seperti NIK dan NPWP. Risiko ini adalah salah satu bentuk beretasan atau kegagalan system keamanan (Gumilang, 2023).

Kebocoran data juga terjadi dari pihak pelaku usaha jasa keuangan dengan cara menjual data konsumen, memberikan data pada pihak ketiga, system aplikasi perlindungan data mudah diretas hacker. Sedangkan, Serangan siber adalah serangan yang dilakukan oleh network computer atau telekomunikasi terhadap network komputer atau



telekomunikasi yang lain seperti website, sistem komputer, dan computer individu. Risiko serangan siber merupakan upaya yang dilakukan oleh individu atau kelompok untuk menyusup, merusak, memanipulasi, atau mengakses sistem komputer atau jaringan secara ilegal atau tanpa izin (Legowo dkk., 2023). Berikut adalah risiko perbankan digital yang dikutip dari keterangan OJK dan menjadi sejumlah resiko perbankan di era digital:

a) Risiko Perlindungan Data Pribadi

Tantangan yang pertama pada perbankan era digital adalah rawannya perlindungan data pribadi. Seperti yang diketahui, untuk mendaftarkan diri dan melakukan registrasi pada aplikasi perbankan digital, diperlukan identitas data nasabah yang valid. Data nasabah ini wajib untuk terlindungi dengan baik agar tidak bocor dan disalahgunakan.

b) Risiko Strategis Investasi di Bidang IT

Perkembangan digital tentu memerlukan investasi di bidang IT yang bertujuan untuk mengembangkan sumber daya agar dapat mencapai tujuan yang diharapkan. Namun, hal ini memerlukan strategi yang tepat dan terukur agar investasi dapat mencapai potensi maksimalnya dan tidak menimbulkan kerugian.

c) Risiko Serangan Siber

Serangan siber adalah salah satu tantangan besar dalam perkembangan perbankan digital di Indonesia. Sebuah organisasi yang menaungi teknologi perkembangan perbankan digital sudah selayaknya mampu menghalau serangan siber dengan teknologi yang terbaru.

d) Kesiapan Organisasi

Penting bagi sebuah organisasi untuk memiliki sumber daya suportif serta memiliki pemahaman industri yang mendalam agar tantangan perbankan di era digital dapat teratas dengan baik.

e) Risiko Kebocoran Data Nasabah

Pihak bank perlu menjaga keamanan data nasabah guna menghindari kebocoran data. Dari sisi nasabah, mereka pun harus selalu berhati-hati dan melindungi data diri mereka sebaik mungkin.

f) Penyalahgunaan Teknologi

Penting untuk memahami bagaimana cara kerja sebuah aplikasi atau layanan digital perbankan *online* agar menghindari penipuan yang memanfaatkan perkembangan teknologi. Oleh karena itu, nasabah perlu menjaga data pribadi, misalnya *password*, *pin*, dan *One Time Password* (OTP) untuk mencegah oknum yang tidak bertanggung jawab dalam memanfaatkan data tersebut.

g) Risiko Penggunaan Pihak Ketiga

Risiko penyalahgunaan data dari pihak ketiga juga menjadi salah satu tantangan perbankan di era digital. Namun, berkat regulasi dan pengawasan yang ketat, risiko ini dapat diatasi sedini mungkin.

h) Infrastruktur Jaringan Komunikasi

Tantangan perbankan di era digital selanjutnya adalah belum tersebarluasnya jaringan komunikasi secara merata pada setiap daerah. Hal ini disebabkan sebagian besar daerah di Indonesia belum memiliki infrastruktur perkembangan teknologi yang mendukung.

i) Regulasi Perbankan dari Pemerintah

Dari sisi pemerintah, mereka juga perlu untuk selalu meninjau dan mengakomodasi pengembangan layanan berbasis digital secara cepat. Pengembangan regulasi yang baikterkait produk dan kelembagaan dapat mendukung industri perbankan, khususnya sebagai upaya percepatan transformasi digital perbankan (*9 Tantangan Perbankan di Era Digital dan Cara BRI API Meresponnya*, 2022).

2. Tantangan Digitalisasi

Otoritas Jasa Keuangan (OJK) menyebut perbankan Indonesia menghadapi setidaknya tiga tantangan dalam layanan perbankan digital. yakni, mengevaluasi percobaan layanan perbankan digital (BI) Bank Indonesia dari sisi sistem informasi perbankan, kesiapan jaringan, edukasi



dan pengamanan konsumen. Beberapa tantangan ekonomi digital terhadap kemajuan perbankan, seperti bidang keamanan dan keamanan. Seiring dengan kecanggihan teknologi pencurian di ranah digital, kecanggihan teknologi keamanan pun semakin maju. Salah satu kejahatan yang paling umum adalah peniruan identitas dan phishing. Phishing adalah pencurian informasi sensitif milik orang lain, seperti nama, alamat rumah, dan nomor telepon, yang digunakan untuk menjebol akun pelanggan. Semua ini dilakukan oleh pengguna yang tidak bertanggung jawab itu sendiri. Misalnya, timbulnya kejahatan baru, seperti bahaya peretasan situs web untuk mencuri informasi perusahaan, dan penyebaran penipuan berkedok bisnis online (Tambunan & Nasution, 2023).

Tantangan Perbankan Syariah di Era Digitalisasi adalah sebagai berikut:

- a) Sumber Daya Manusia. Komponen utama dalam mengintegrasikan operasional keuangan digital adalah sumber daya manusia. Topik hangat tentang sumber daya manusia juga muncul sehubungan dengan keuangan Islam. Agar sektor keuangan syariah tumbuh di era digitalisasi, perbankan syariah harus memiliki SDM yang berkualitas sehingga mampu mengelola sistem perbankan syariah dan siap menghadapi masalah yang ditimbulkan oleh kemajuan teknologi.
- b) Cyber Security. Keberadaan IKD di industri perbankan syariah menjadikan cyber security sebagai topik yang menonjol. Perbankan syariah harus meningkatkan pengetahuan tentang cyber security karena meningkatnya ancaman kejahatan siber. Untuk memiliki proses pengambilan keputusan, perbankan syariah diharus mempunyai hubungan antara ekonomi dengan pasar. Hal ini dilakukan agar dapat mengidentifikasi masalah dan menentukan cara mengatasinya. Menurut Al-Alawi dan Al-Bassam (2019), kepatuhan keamanan, dedikasi, anggaran, manajemen, dan



keamanan merupakan elemen penting dalam menghindari kejahatan dunia maya.

- c) *Consume Protection Risk* yang dihadapi bank dan nasabah tidak diragukan lagi telah meningkat karena adanya inovasi keuangan digital. Sebagai salah satu bentuk pertahanan Muhammad Ash-Shiddiqy. terhadap risiko yang mungkin terjadi, perlindungan bagi nasabah diberikan saat mengimplementasikan layanan perbankan digital. Untuk meraih kepercayaan masyarakat, perlindungan konsumen harus berjalan seiring dengan menghadirkan sektor perbankan syariah yang memiliki reputasi tinggi (Setyowati, Abubakar, dan Rodliah, 2017).
- d) Adanya keterputusan nyata antara inklusi keuangan dan literasi keuangan di masyarakat karena kurangnya literasi keuangan di era digital kontemporer. Dengan demikian, salah satu kesulitan yang dihadapi perbankan syariah adalah hal tersebut (Putri, Damayanti, dan Rahadi, 2022).
- e) Kurangnya Pemahaman Teknologi Syariah. Banyak pelaku industri yang masih kurang memahami bagaimana mengintegrasikan teknologi dengan prinsip syariah. Hal ini menimbulkan kesulitan dalam menciptakan produk digital yang sesuai dengan aturan syariah.

Tantangan-tantangan di atas yang ditimbulkan oleh perkembangan digital di perbankan syariah tentu akan dijawab dengan beberapa strategi antara lain dengan pemilihan SDM yang ketat untuk mengisi komponen struktural dan pengetatan keamanan dunia maya, yang menawarkan perlindungan data-data nasabah yang ketat, dan dengan menungkatkan literasi publik yang ada (Muhammad Ash Shiddiqy, 2023).

3. Solusi Digitalisasi

Bank Digital berpeluang memenuhi kebutuhan dan ekspektasi konsumen akan layanan yang cepat dan sesuai dengan kebutuhan. Peluang ini semakin terbuka lebar di masa pandemi yang berdampak



terhadap perilaku masyarakat yang lebih banyak menggunakan teknologi digital dalam memenuhi kebutuhannya. Perkembangan positif terlihat pada peningkatan preferensi dan akseptasi masyarakat terhadap penggunaan platform dan instrumen keuangan digital, seperti e-commerce untuk pemenuhan kebutuhan sehari-hari (Mawarni, dkk. 2021).

Secara umum, penguatan regulasi diperlukan untuk menjawab tantangan yang harus dihadapi oleh Bank Digital untuk memenuhi persyaratan yang diatur dalam Pasal 24 POJK Bank Umum, yaitu:

- a) memiliki model bisnis dengan penggunaan teknologi yang inovatif dan aman dalam melayani kebutuhan nasabah;
- b) memiliki kemampuan untuk mengelola model bisnis perbankan digital yang prudent dan berkesinambungan;
- c) memiliki manajemen risiko yang memadai;
- d) memenuhi aspek tata kelola termasuk pemenuhan direksi yang mempunyai kompetensi di bidang teknologi informasi dan kompetensi lain sesuai dengan ketentuan OJK mengenai penilaian kemampuan dan kepatutan bagi pihak utama Lembaga keuangan;
- e) menjalankan perlindungan terhadap keamanan data nasabah;
- f) memberikan upaya yang kontributif terhadap pengembangan ekosistem keuangan digital dan/atau inklusi keuangan.

Keenam syarat yang wajib dipenuhi oleh Bank Digital tersebut berimplikasi terhadap regulasi yang sudah ada. Beberapa isu hukum strategis yang perlu dielaborasi ke dalam regulasi yaitu keamanan data nasabah, perlindungan konsumen Bank Digital dan manajemen risiko teknologi informasi (Abubakar & Handayani, 2022).

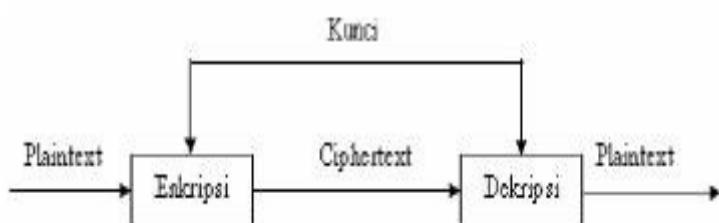
Berikut merupakan jenis sistem keamanan yang dipakai dalam internet banking menurut Lewis dan Thygerson yaitu sebagai berikut:

a. Cryptography System

Sistem dimana menggunakan berbagai angka yang sering disebut dengan key. Sistem memiliki fungsi melakukan pengenalan terhadap seorang nasabah dan melindungi semua informasi finansial nasabah.



Metode ini disebut metode kata sandi. Ada dua jenis enkripsi: enkripsi simetris dan enkripsi asimetris. Sistem ini menggunakan kode kunci yang sama untuk penerima dan pengirim pesan. Kerugian dari enkripsi simetris adalah kuncinya harus dikirim ke penerima, sehingga seseorang dapat melakukan intervensi di sepanjang proses tersebut. Sistem enkripsi asimetris juga memiliki kelemahan yaitu menambahkan lebih banyak kode akan memperlambat transfer data(Della Fitri dkk., 2024).



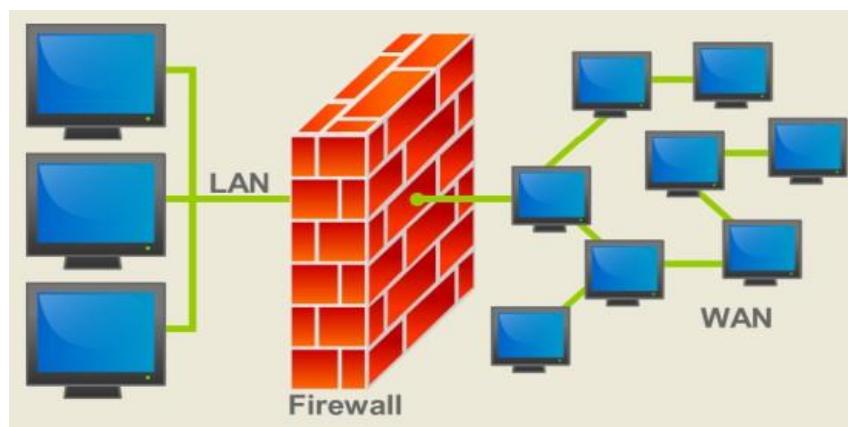
Gambar 2. Cryptography system

b) Firewall System

Sistem ini berfungsi untuk melakukan pencegahan terhadap pihak-pihak yang tidak mendapat izin dalam memasuki area yang dilindungi atau diproteksi dalam unit pusat kerja suatu perusahaan. Firewall system tidak dapat mencegah adanya virus dan ini murni kendala internal organisasi. Ada beberapa fungsi Firewall diantaranya:

- Mengontrol dan mengawasi paket data yang mengalir di jaringan Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.
- Melakukan autentifikasi terhadap akses.

- Aplikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.
- Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini Memungkinkan membantu sebagai pendekripsi dini akan penjebohan jaringan (Kominfo, 2022).



Gambar 3. Firewall system

Ada beberapa aspek keamanan komputer wajib diperhatikan dan mempunyai beberapa lingkup penting, dimana menurut Lewis dan Thygerson 9 dalam 4, yaitu:

- a) Privacy & Confidentiality Aspek ini menekankan pada usaha dalam menjaga kerahasiaan data dan informasi dan pihak lain tidak boleh mengaksesnya. Sedangkan privacy lebih menekankan pada data-data privat, contohnya data tentang nasabah perbankan.
- b) Integrity Aspek integrity memprioritaskan keamanan data atau informasi agar tidak bisa diakses selain tanpa seizin pemilik.
- c) Authentication Aspek yang menekankan mengenai otorisitas suatu data atau informasi, termasuk didalamnya pihak yang memberi data atau mengaksesnya tersebut merupakan pihak yang memiliki ijin akses atau pemilik sah.

- d) Availability Aspek yang berkaitan dengan ketersediaan informasi ketika dibutuhkan (Dianta & Zusrony, 2019).

Dalam era digitalisasi perbankan, keamanan data menjadi salah satu aspek yang paling krusial untuk diperhatikan. Untuk memastikan perlindungan data nasabah, bank perlu menerapkan teknologi enkripsi yang kuat dalam semua transaksi digital. Enkripsi ini berfungsi untuk mengamankan informasi sensitif, seperti nomor rekening dan data pribadi, sehingga hanya pihak yang berwenang yang dapat mengaksesnya. Selain itu, penerapan sistem autentikasi multi-faktor (MFA) juga sangat penting. Dengan MFA, nasabah harus melewati beberapa lapisan verifikasi sebelum dapat mengakses akun mereka, yang secara signifikan mengurangi risiko akses tidak sah dan pencurian identitas.

Selain teknologi enkripsi dan autentikasi multi-faktor, bank juga harus melakukan audit keamanan secara berkala untuk mengidentifikasi dan mengatasi potensi celah keamanan dalam sistem mereka. Pelatihan dan edukasi bagi karyawan serta nasabah mengenai praktik keamanan siber yang baik juga merupakan langkah penting dalam menjaga keamanan data. Bank dapat mengadakan seminar atau workshop tentang cara mengenali phishing, penggunaan kata sandi yang kuat, dan tindakan pencegahan lainnya. Dengan kombinasi teknologi canggih dan kesadaran akan keamanan di kalangan pengguna, digitalisasi perbankan dapat berlangsung dengan lebih aman dan efisien, memberikan kepercayaan kepada nasabah untuk menggunakan layanan perbankan digital tanpa rasa khawatir.

C. Metode Penelitian

Penelitian ini menerapkan metode kualitatif dengan pendekatan studi kepustakaan, yang melibatkan pemikiran serta pendapat para ahli di



bidang teknologi informasi, ekonomi syariah, perbankan syariah, dan perkembangan digital. Selanjutnya, penelitian ini dilakukan dengan menganalisis berbagai literatur, seperti jurnal penelitian, buku, artikel, serta karya ilmiah lainnya yang berkaitan dengan risiko digitalisasi perbankan, tantangan, dan solusi dalam digitalisasi perbankan syariah. Pada tahap akhir, penelitian ini disimpulkan melalui analisis dan interpretasi berbagai sumber yang telah dieksplorasi, diidentifikasi, serta diklasifikasikan menggunakan metode deskriptif.

D. Hasil dan Pembahasan

Digitalisasi telah membawa perubahan besar dalam industri perbankan, termasuk sektor perbankan syariah. Transformasi ini bertujuan untuk meningkatkan efisiensi operasional, memperluas aksesibilitas nasabah, serta meningkatkan daya saing dengan perbankan konvensional. Namun, di balik berbagai manfaatnya, digitalisasi juga menghadirkan sejumlah risiko yang perlu dianalisis guna menjaga prinsip syariah serta stabilitas lembaga keuangan.

Penelitian ini berfokus pada analisis risiko yang dihadapi perbankan syariah dalam proses digitalisasi serta mengusulkan solusi untuk mengurangi risiko tersebut. Beberapa risiko utama dalam digitalisasi perbankan meliputi:

- Risiko Perlindungan Data Pribadi.** Untuk mendaftar dan menggunakan layanan perbankan digital, nasabah harus menyediakan identitas serta data pribadi yang valid. Oleh karena itu, perlindungan data menjadi aspek krusial guna mencegah kebocoran serta penyalahgunaan informasi pribadi.
- Risiko Strategis dalam Investasi Teknologi.** Pengembangan infrastruktur IT memerlukan investasi besar agar bank dapat mengoptimalkan sumber daya dan mencapai tujuan strategis yang diharapkan.



3. **Risiko Serangan Siber.** Ancaman serangan siber menjadi tantangan utama dalam perbankan digital di Indonesia. Bank syariah harus menerapkan sistem keamanan yang ketat untuk melindungi sistem serta data nasabah dari potensi serangan.
4. **Risiko Kebocoran Data Nasabah.** Keamanan data nasabah harus dijaga secara optimal oleh pihak bank guna menghindari kebocoran informasi. Selain itu, nasabah juga perlu meningkatkan kewaspadaan serta menjaga data pribadi mereka agar tidak disalahgunakan. Kebocoran data masih menjadi salah satu risiko paling sering terjadi dalam era digital perbankan.

Selain risiko digitalisasi, perbankan syariah juga menghadapi berbagai tantangan dalam beradaptasi dengan era digital agar tetap kompetitif dengan perbankan konvensional maupun lembaga keuangan lainnya. Tantangan tersebut mencakup:

- **Sumber Daya Manusia (SDM)** – Kurangnya tenaga ahli di bidang teknologi digital dan keamanan siber.
- **Keamanan Siber (Cybersecurity)** – Meningkatnya ancaman kejahatan siber yang menargetkan sistem perbankan.
- **Perlindungan Konsumen** – Nasabah perlu diberikan edukasi mengenai keamanan transaksi digital dan hak-hak mereka.
- **Kurangnya Pemahaman Teknologi Syariah** – Rendahnya literasi digital dan pemahaman terhadap konsep perbankan syariah dalam ekosistem digital.

Strategi dan Solusi untuk Mitigasi Risiko serta Menghadapi Tantangan Digitalisasi Perbankan Syariah

1. Meningkatkan Keamanan Siber

- Menggunakan teknologi canggih seperti enkripsi data, autentikasi dua faktor (2FA), serta sistem deteksi ancaman berbasis kecerdasan buatan (AI) untuk mencegah dan mendeteksi serangan siber lebih awal.

2. Penguatan Infrastruktur Teknologi



- Meningkatkan fleksibilitas dan kapasitas sistem IT tanpa harus mengeluarkan biaya besar untuk infrastruktur fisik.

3. Kolaborasi dengan Perusahaan Fintech

- Menjalin kerja sama dengan perusahaan fintech guna mempercepat pengembangan layanan digital tanpa harus membangun ekosistem digital dari nol.

4. Pemanfaatan Big Data dan AI

- Menerapkan teknologi big data serta kecerdasan buatan untuk menganalisis data secara real-time, meningkatkan efisiensi operasional, serta memberikan layanan yang lebih personal bagi nasabah.

5. Pengembangan Sumber Daya Manusia (SDM)

- Melatih karyawan dalam bidang teknologi digital, keamanan siber, dan fintech melalui pelatihan internal, sertifikasi eksternal, atau kemitraan dengan institusi pendidikan.
- Merekrut tenaga ahli di bidang IT, data science, serta keamanan siber yang memiliki pemahaman mendalam terkait teknologi perbankan digital.

6. Menciptakan Budaya Inovasi

- Mendorong inovasi dalam organisasi dengan memberikan ruang bagi karyawan untuk bereksperimen dengan ide-ide baru serta belajar dari setiap kegagalan sebagai bagian dari proses pengembangan.

Dengan menerapkan strategi ini, diharapkan perbankan syariah dapat mengatasi tantangan digitalisasi secara efektif, menjaga keamanan serta kepatuhan terhadap prinsip syariah, dan meningkatkan daya saing di era perbankan digital.



E. Kesimpulan

Digitalisasi dalam perbankan syariah membuka peluang besar untuk meningkatkan efisiensi operasional, inovasi produk, serta memperluas akses layanan bagi nasabah. Namun, di balik manfaat tersebut, terdapat berbagai risiko yang harus diantisipasi oleh bank syariah. Beberapa risiko utama dalam digitalisasi perbankan syariah mencakup risiko kepatuhan, keamanan siber, teknologi, dan operasional, yang berpotensi mengganggu stabilitas serta kepercayaan nasabah. Kompleksitas tantangan ini semakin meningkat akibat keterbatasan infrastruktur teknologi, regulasi yang belum sepenuhnya matang, serta kurangnya tenaga profesional yang memiliki keahlian dalam teknologi digital berbasis syariah.

Untuk menghadapi risiko dan tantangan tersebut, perbankan syariah perlu menerapkan berbagai strategi. Pertama, meningkatkan keamanan siber serta memastikan kepatuhan terhadap prinsip syariah melalui penerapan teknologi yang lebih canggih dan pembaruan regulasi secara berkala. Kedua, perbankan syariah harus terus berinovasi dengan memperkuat infrastruktur teknologi, mengadopsi teknologi cloud computing, serta menjalin kerja sama dengan fintech syariah guna mempercepat proses transformasi digital. Selain itu, peningkatan literasi dan pelatihan bagi sumber daya manusia di bidang teknologi finansial berbasis syariah juga menjadi langkah krusial agar bank tetap kompetitif dalam industri yang terus berkembang.

Secara keseluruhan, digitalisasi merupakan langkah yang tidak dapat dihindari bagi perbankan syariah agar dapat bertahan dan bersaing di era modern. Namun, keberhasilan transformasi digital ini sangat bergantung pada kemampuan bank dalam mengelola risiko secara proaktif, mengikuti perkembangan teknologi, serta memperkuat regulasi dan tata kelola. Dengan strategi yang tepat, digitalisasi dapat menjadi solusi bagi bank syariah untuk meningkatkan kualitas layanan,



memperluas pangsa pasar, serta tetap berpegang pada prinsip-prinsip syariah yang menjadi dasar operasionalnya.

REFERENCE

- 9 *Tantangan Perbankan Di Era Digital Dan Cara Briapi Meresponnya*. (2022.). Diambil 25 September 2024, Dari <Https://Developers.Bri.Co.Id/Id/News/9-Tantangan-Perbankan-Di-Era-Digital-Dan-Cara-Briapi-Meresponnya>
- Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. *Masalah-Masalah Hukum*, 51(3), 259–270. <Https://Doi.Org/10.14710/Mmh.51.3.2022.259-270>
- Bagaspati Adibrata Cahyolaksono, Adhitya Mahardhika, & Mochamad Ismail Zakaria. (2021). Usulan Kebijakan Pencegahan Resiko Perbankan Di Era Digital. *E-Bisma: Enterpreneurship Bisnis Manajemen Akuntansi*.
- Bambang Rianto Rustam. (2018). *Manajemen Risiko Perbankan Syariah Di Era Digital: Konsep Dan Penerapan Di Indonesia*. <Https://Inlisite.Uin-Suska.Ac.Id/Opac/Detail-Opac?Id=28868>
- Della Fitri, Edy Soesanto, & Winny Winny. (2024). Implementasi Nilai-Nilai Kebangsaan Yang Bersumber Uud 1945 Dan Nkri Dalam Mengacu Peran Manajemen Sekuriti Menunjang Keamanan Data Nasabah Di Era Digital Pada Pt Bank Rakyat Indonesia. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, 2(2), 84–105. <Https://Doi.Org/10.47861/Sammajiva.V2i2.986>
- Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. *Intensif: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, 3(1), 1. <Https://Doi.Org/10.29407/Intensif.V3i1.12125>
- Fauzatul Laily Nisa & Krisna Reswara. (2024). Analisis Perkembangan Dan Tantangan Bank Syariah Dalam Persaingan Dengan Bank Konvensional Di Pasar Keuangan Modern. *Jurnal Ekonomi Dan Pembangunan Indonesia*, 2(3), 120–125. <Https://Doi.Org/10.61132/Jepi.V2i2.601>
- Gultom, M. S. D., & Rokan, M. K. (2022). Problematika Perbankan Syariah: Solusi Dan Strategi Digitaliasasi Dalam Meningkatkan Kualitas Produk Dan Layanan Perbankan Di Bank Sumut Kantor Cabang Syariah Medan. *Alexandria (Journal Of Economics, Business, & Entrepreneurship)*, 3(1), 14–20. <Https://Doi.Org/10.29303/Alexandria.V3i1.175>
- Gumilang. (2023). *Pengaruh Terpaan Berita Online Kebocoran Data Digital Oleh Hacker Bjorka Terhadap Kecemasan Gen Z (Survei Pada Mahasiswa Universitas Lampung)*.
- Kominfo. (2022, Februari 1). *Diskominfo*. Diskominfo. <Https://Kominfo.Kotabogor.Go.Id/>



- Legowo, M. B., Romauli, A. S., Kamalia, A. S., & Diska, A. (2023). Manajemen Resiko Kebocoran Data Nasabah Dan Serangan Siber Menggunakan Nist-Risk Management Framework. *Prosiding Seminar Nasional*, 3, 144–151.
- Marhamah, & Fauzi. (2021). Jurnalisme Di Era Digital. *Journal Of Islamic Communication And Media Studies*, 1(1).
- Mawarni, Fasa, & Suharto. (2021). Penerapan Digital Banking Bank Syariah Sebagai Upaya Customer Retention Pada Masa Covid-19. *Jurnal Pemikiran Dan Penelitian Ekonomi Islam*, 2(9).
- Muhammad Ash Shiddiqy. (2023). Analisis Peluang Dan Tantangan Perbankan Syariah Di Era Digital. *Jasie (Jurnal Of Aswaja And Islamic Economics)*, 2(1).
- Muhazzab Alief Faizal, & Zelyn Faizatul. (2023). *View Of Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini*. <Https://Journal.Uiad.Ac.Id/Index.Php/Asy-Syariyah/Article/View/2022/962>
- Muneeza, Arshad, & Azeez. (2020). Shariah Governance Framework For Islamic Banks: The Case Of Malaysia. *Journal Of Islamic Accounting And Businnes Research*.
- Oktaviani, S., & Basyariah, N. (2022). Analisis Manajemen Risiko Layanan Mobile Banking Pada Bank Syariah. *Jurnal Manajemen Dan Penelitian Akuntansi*, 15(1), 29–34. <Https://Doi.Org/10.58431/Jumpa.V15i1.183>
- Roadmap Pengembangan Perbankan Syariah Indonesia 2020-2025.* (2021.). Diambil 25 September 2024, Dari <Https://Ojk.Go.Id/Id/Kanal/Syariah/Berita-Dan-Kegiatan/Publikasi/Pages/Roadmap-Pengembangan-Perbankan-Syariah-Indonesia-2020-2025.Aspx>
- Tambunan, R. T., & Nasution, M. I. P. (2023). Tantangan Dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi Di Era 4.0. *Sci-Tech Journal*, 2(2), Article 2. <Https://Doi.Org/10.56709/Stj.V2i2.75>