Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue Desember, 2025 pp. 1982-1988 http://urj.uin-malang.ac.id/index.php/mij/index

Keamanan Digital di Era 4.0: Menangkal Serangan Siber di Lembaga Keuangan Syariah

Chandra Ray Daffandi[1]
program studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim
e-mail: ameerachandra99@gmail.com

Kata Kunci:
Keamanan Digital, Serangan Siber, Bank Syariah, Manajemen Risiko, keamanan data
Keywords:
Digital Security, Cyberattacks, Islamic Banking, Risk Management, data security

A B S T R A K

Era Revolusi Industri 4.0 menghadirkan kemajuan teknologi sekaligus tantangan baru berupa serangan siber terhadap lembaga keuangan syariah. Ancaman seperti phishing, malware, dan ransomware membahayakan data nasabah serta merusak kepercayaan publik. Studi ini mengulas bentuk serangan digital yang marak terjadi, dampaknya terhadap operasional perbankan syariah, serta upaya mitigasi yang dapat dilakukan. Pendekatan strategis mencakup penerapan enkripsi, autentikasi ganda, firewall, edukasi nasabah, serta penguatan manajemen risiko berbasis ISO 31000:2018. Kolaborasi dengan otoritas pengawas juga menjadi kunci dalam membangun sistem keamanan digital yang tangguh dan terpercaya. Serangan seperti phishing, malware, ransomware, hingga skimming telah terbukti mengancam keamanan data dan kepercayaan nasabah, sebagaimana tercermin dalam kasus serangan ransomware terhadap Bank Syariah Indonesia (BSI). Untuk mengatasi ancaman ini, diperlukan pendekatan keamanan digital yang komprehensif, mencakup penerapan teknologi enkripsi, autentikasi ganda, firewall, dan pemantauan sistem secara berkelanjutan

A B S T R A C T

The Industrial Revolution 4.0 era brings technological advancements along with new challenges such as cyberattacks on Islamic financial institutions. Threats like phishing, malware, and ransomware endanger customer data and damage public trust. This study explores common cyber threats, their impact on Islamic banking operations, and mitigation efforts. Strategic approaches include encryption, two-factor authentication, firewalls, customer education, and risk management based on ISO 31000:2018. Collaboration with regulatory authorities is also key to building a robust and trustworthy digital security system. Attacks such as phishing, malware, ransomware, and skimming have been proven to threaten data security and customer trust, as evidenced by the ransomware attack on Bank Syariah Indonesia (BSI). Addressing these threats requires a comprehensive digital security approach, including the implementation of encryption technology, dual authentication, firewalls, and continuous system monitoring.

Pendahuluan

Lembaga Keuangan Syariah adalah institusi keuangan yang menjalankan operasionalnya berdasarkan prinsip-prinsip Syariah Islam. Dalam kegiatannya, lembaga ini harus bebas dari unsur riba, gharar, dan maisir, karena unsur-unsur tersebut secara tegas dilarang dalam Al-Qur'an dan Hadis. Tujuan utama dari pendirian lembaga keuangan syariah adalah untuk menjalankan perintah Allah SWT dalam bidang ekonomi dan muamalah, serta membantu umat Islam terhindar dari praktik-praktik yang bertentangan dengan ajaran Islam. Pelaksanaan tujuan ini bukan hanya menjadi

tanggung jawab lembaga keuangan syariah semata, melainkan juga merupakan tanggung jawab bersama seluruh umat. Dalam praktiknya, kegiatan lembaga keuangan syariah—baik yang berbentuk bank maupun non-bank—diawasi oleh otoritas yang disebut Dewan Pengawas Syariah (Khikmatin & Setianingsih, 2021). Revolusi Industri 4.0 merupakan kemajuan teknologi yang membawa perubahan signifikan dalam sektor industri maupun kehidupan masyarakat secara luas. Era ini ditandai dengan hadirnya berbagai teknologi canggih seperti Internet of Things (IoT), kecerdasan buatan (AI), big data, komputasi awan, robotika, dan teknologi lainnya yang memungkinkan terciptanya sistem otomatisasi yang saling terhubung dan dapat diakses dari berbagai tempat. Meskipun kemajuan teknologi ini memberikan kemudahan dalam berbagai aktivitas manusia, sistem-sistem yang terintegrasi tersebut juga menghadirkan kerentanan terhadap serangan siber (Pertiwi et al., 2024).

Keamanan siber dalam dunia keuangan merupakan isu yang semakin penting seiring pesatnya perkembangan teknologi. Berbagai studi menunjukkan bahwa sektor ini menjadi salah satu sasaran utama para pelaku kejahatan siber, karena menyimpan data pribadi nasabah dan aset keuangan dalam jumlah besar. Keberlangsungan operasional serta kepercayaan masyarakat terhadap lembaga keuangan sangat bergantung pada ketangguhan sistem keamanannya. Serangan seperti phishing, malware, hingga Distributed Denial of Service (DDoS) terus mengintai, berpotensi mengganggu layanan, mencuri data penting, dan menimbulkan kerugian finansial yang besar. Bank syariah pun tidak luput dari ancaman ini, sehingga diperlukan upaya serius untuk menerapkan strategi keamanan digital yang kuat, canggih, dan adaptif demi melindungi nasabah serta menjaga kepercayaan public (Restika & Sonita, 2023).

Pembahasan

Kemajuan teknologi informasi membawa serta tantangan baru bagi perbankan syariah dalam bentuk kejahatan siber. Serangan seperti phishing, malware, ransomware, dan pencurian identitas bukan hanya dapat merusak data nasabah, tetapi juga mengganggu layanan dan menurunkan kepercayaan masyarakat. Para pelaku memanfaatkan celah keamanan serta minimnya pemahaman pengguna tentang risiko digital. Dalam kondisi ini, bank syariah dihadapkan pada tanggung jawab besar untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelolanya. Jika perlindungan terhadap data pribadi tidak memadai, dampaknya bisa sangat merugikan, termasuk pada reputasi lembaga. Oleh karena itu, dibutuhkan pendekatan keamanan yang menyeluruh dan berlapis, mulai dari penggunaan teknologi enkripsi, pemantauan sistem secara rutin, peningkatan kapasitas staf, hingga pemberian edukasi yang berkelanjutan kepada nasabah agar mereka juga menjadi bagian dari sistem perlindungan tersebut (Lubis et al., 2025).

Di era digital saat ini, bank syariah dihadapkan pada berbagai risiko yang semakin kompleks, seperti kebocoran data, serangan siber, dan penipuan berbasis elektronik. Risiko-risiko tersebut tidak bisa diabaikan dan perlu ditangani secara menyeluruh melalui langkah-langkah identifikasi, evaluasi, pengendalian, dan pemantauan risiko yang dilakukan secara berkesinambungan. Kejahatan siber menjadi ancaman nyata karena mampu merusak integritas sistem dan mengikis kepercayaan nasabah. Untuk itu, bank

syariah harus memanfaatkan teknologi terkini guna melindungi data, membekali karyawan dengan pemahaman tentang keamanan digital, serta memberikan edukasi yang jelas dan mudah dipahami kepada nasabah. Pendekatan manajemen risiko yang merujuk pada ISO 31000:2018 dapat membantu bank dalam mengenali potensi risiko teknologi informasi, menganalisis dampaknya, dan menetapkan langkah mitigasi melalui kebijakan keamanan yang tegas. Membangun budaya organisasi yang peka terhadap risiko, serta dukungan penuh dari manajemen puncak, sangat penting dalam melawan ancaman siber. Di samping itu, sistem pengelolaan data yang kuat dan mekanisme pelaporan risiko yang transparan juga berperan besar dalam meminimalkan dampak yang ditimbulkan oleh serangan siber (Widyaningsih et al., 2024).

Berbagai bentuk kejahatan siber di Indonesia dapat dikaitkan dengan ketentuan hukum pidana yang berlaku, baik yang tercantum dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun dalam peraturan di luar KUHP, seperti yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 yang telah diperbarui melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Namun demikian, masih terdapat perbedaan mendasar antara konsep hukum pidana konvensional dengan karakteristik unik dari kejahatan siber. Dalam konteks sektor jasa keuangan dan perbankan, kejahatan siber umumnya terbagi menjadi dua jenis utama. Pertama adalah sosial engineering, yaitu manipulasi psikologis terhadap seseorang dengan tujuan memperoleh informasi tertentu melalui cara yang tampak wajar atau tidak mencurigakan—seperti melalui percakapan langsung atau panggilan telepon—sehingga korban tidak menyadari bahwa ia sedang ditipu. Kedua adalah skimming, yaitu pencurian informasi secara ilegal dengan cara menyalin data yang tersimpan pada strip magnetik kartu debit atau kredit. Skimming sering terjadi saat nasabah melakukan transaksi di mesin ATM. Untuk melancarkan aksi ini, pelaku biasanya menggunakan tiga alat utama: skimmer, kamera tersembunyi (hidden camera), dan keypad palsu. Skimmer dipasang di slot kartu pada mesin ATM dan berfungsi untuk merekam data dari strip magnetik kartu saat dimasukkan. Kamera tersembunyi dan keypad palsu digunakan untuk merekam gerakan jari korban saat memasukkan PIN, sehingga pelaku dapat memperoleh akses penuh terhadap rekening korban. Kejahatan semacam ini menunjukkan pentingnya kewaspadaan serta perlindungan sistem dan data di sektor keuangan (Prasetyo, 2024).

Insiden serangan ransomware oleh kelompok LockBit 3.0 yang terjadi pada Mei 2023 menjadi pelajaran penting bagi dunia perbankan, khususnya dalam mengungkap kelemahan sistem keamanan siber Bank Syariah Indonesia (BSI). Serangan ini menyebabkan gangguan operasional yang cukup besar dan menimbulkan kekhawatiran di kalangan nasabah. Dampaknya tidak hanya terasa secara finansial, tetapi juga mencoreng reputasi bank, bahkan berisiko memicu aksi penarikan dana secara besar-besaran yang bisa membahayakan kondisi likuiditas (Sari et al., 2024). Sebagai respons atas insiden yang berdampak pada citra perusahaan, Bank Syariah Indonesia (BSI) telah mengambil berbagai langkah strategis untuk mengatasi krisis sekaligus memulihkan kepercayaan publik. BSI merespons dugaan serangan siber dengan cepat melalui komunikasi yang terbuka dan tepat sasaran, termasuk merilis pernyataan resmi dan siaran pers guna menenangkan nasabah serta menunjukkan komitmen terhadap transparansi dan perbaikan. Dalam upaya memperkuat sistem keamanannya, BSI

melakukan pembaruan teknologi seperti pengembangan server baru, peningkatan sistem enkripsi data, pembaruan gateway, dan penerapan sistem otentikasi ganda (double authentication). Langkah-langkah ini mencerminkan keseriusan BSI dalam menjaga keamanan data nasabah dan membangun kembali citra sebagai lembaga keuangan yang terus berbenah, khususnya dalam hal perlindungan digital. Sebagai wujud kepedulian terhadap nasabah yang terdampak, BSI juga meluncurkan program "Pesta Hadiah" serta layanan "Weekend Banking" sebagai bentuk apresiasi sekaligus untuk memperkuat hubungan emosional antara bank dan nasabah. Namun demikian, tantangan tetap ada. Salah satunya adalah belum tersedianya sistem yang mampu mengukur sejauh mana nasabah memahami, mendukung, dan menyetujui kebijakan serta langkah penanggulangan krisis yang diterapkan. Hal ini menyulitkan proses evaluasi terhadap efektivitas strategi yang dijalankan. Selain itu, kebutuhan akan komunikasi yang lebih terbuka, dua arah, dan empatik dengan nasabah menjadi hal penting yang harus ditingkatkan agar kualitas layanan terus membaik dan kepercayaan dapat dipulihkan secara menyeluruh. Untuk menghadapi ancaman semacam ini, diperlukan strategi manajemen risiko yang kokoh serta kesadaran bersama dari seluruh pihak. Edukasi kepada nasabah tentang pentingnya menjaga keamanan data pribadi, pemanfaatan teknologi mutakhir seperti blockchain, serta penerapan autentikasi multi-faktor menjadi langkah penting dalam membentengi sistem dari serangan siber. Selain itu, peran audit internal yang konsisten dan kolaborasi erat dengan lembaga pengawas seperti OJK, BSSN, dan Bank Indonesia sangat penting untuk memperkuat sistem pertahanan digital dan membangun kembali kepercayaan Masyarakat (Maulana & Nasrulloh, 2024).

Pentingnya Keamanan Siber

Di tengah pesatnya pertumbuhan layanan fintech dan mobile banking, keamanan siber menjadi hal yang sangat krusial untuk diperhatikan. Ancaman kejahatan siber terus meningkat dan dapat membahayakan kepercayaan pengguna serta stabilitas sistem keuangan digital. Serangan ini sering kali disebabkan oleh berbagai faktor internal, seperti lemahnya sistem pengamanan, kurangnya pembaruan perangkat lunak, keterbatasan kompetensi sumber daya manusia, hingga kelalaian pengguna dalam menjaga data pribadinya. Sementara dari sisi eksternal, risiko datang dari serangan malware, belum matangnya regulasi yang mengatur, serta pemanfaatan teknologi canggih oleh pelaku kejahatan. Untuk menghadapi tantangan ini, dibutuhkan langkah-langkah konkret seperti penerapan firewall yang andal, pemanfaatan teknologi blockchain, penguatan manajemen risiko, dan peningkatan infrastruktur jaringan. Selain itu, pembentukan tim khusus yang fokus pada keamanan siber, kejelasan regulasi yang mengatur perlindungan data dan transaksi digital, serta edukasi berkelanjutan kepada pengguna juga sangat penting. Perlu disadari bahwa keamanan siber bukan sekadar isu teknis, melainkan fondasi utama yang menopang integritas sistem serta membangun kepercayaan masyarakat terhadap layanan keuangan berbasis digital (Azizah et al., 2024).

Risiko teknologi informasi yang muncul saat ini menjadi tantangan serius bagi bank syariah dalam menjaga keamanan sistem perbankan serta melindungi data dan informasi nasabah. Untuk menghadapi tantangan tersebut, dibutuhkan penerapan

sistem keamanan yang menyeluruh dan tepat sasaran. Langkah pertama yang krusial adalah melakukan identifikasi dan evaluasi terhadap berbagai potensi risiko. Dengan analisis risiko yang menyeluruh, bank syariah dapat mengenali ancaman yang mungkin terjadi serta mengetahui titik-titik kerentanan dalam sistem mereka. Hal ini memungkinkan perumusan strategi keamanan yang lebih terarah dan penentuan skala prioritas untuk melindungi aset-aset penting. Langkah selanjutnya adalah memanfaatkan teknologi keamanan terkini. Penggunaan perlindungan seperti firewall yang tangguh, sistem pendeteksi intrusi, enkripsi data, serta solusi anti-malware dan anti-phishing menjadi sangat penting untuk menangkal berbagai bentuk serangan siber. Tak kalah penting, penerapan autentikasi dua faktor, kontrol akses yang ketat, dan pemantauan jaringan secara real-time juga perlu dilakukan guna meminimalkan risiko kebocoran atau penyalahgunaan data. Selain itu, pengawasan aktif terhadap sistem harus menjadi bagian dari rutinitas operasional. Bank syariah memerlukan mekanisme pemantauan yang berjalan terus-menerus agar bisa segera mengenali adanya aktivitas mencurigakan atau upaya serangan. Respons cepat terhadap insiden akan membantu meminimalkan dampak negatif yang mungkin ditimbulkan. Terakhir, namun tak kalah penting, adalah aspek pelatihan dan peningkatan kesadaran keamanan. Memberikan edukasi secara berkala kepada karyawan, serta mengajak nasabah untuk lebih paham tentang pentingnya menjaga data pribadi, merupakan langkah strategis untuk menciptakan budaya sadar keamanan. Dengan begitu, semua pihak dapat berperan aktif dalam menjaga sistem tetap aman dan andal (Faizal et al., 2023).

Kejahatan siber memiliki dampak besar terhadap tingkat kepercayaan masyarakat terhadap layanan perbankan syariah. Di tengah kemajuan teknologi digital yang mempermudah akses layanan keuangan, muncul pula ancaman baru yang meresahkan, seperti serangan ransomware. Salah satu contoh nyata adalah insiden yang menimpa Bank Syariah Indonesia (BSI), yang menunjukkan bagaimana serangan siber dapat melemahkan sistem keamanan, mengganggu layanan perbankan, dan menimbulkan kekhawatiran di kalangan nasabah. Dalam konteks ini, kejahatan dunia maya menjadi salah satu faktor utama yang memengaruhi persepsi dan rasa aman masyarakat terhadap layanan bank. Oleh karena itu, keamanan digital bukan hanya menjadi kebutuhan teknis, tetapi juga fondasi penting dalam membangun dan mempertahankan kepercayaan publik. Untuk menjaga kredibilitas, bank syariah perlu terus meningkatkan sistem keamanannya, aktif memberikan edukasi kepada nasabah mengenai cara mencegah kejahatan siber, serta menjaga transparansi dalam menyampaikan informasi terkait insiden dan langkah penanganannya untuk meningkatkan kepercayaan Masyarakat (Zudyaten et al., 2016).

Kesimpulan

Di era Revolusi Industri 4.0, lembaga keuangan syariah menghadapi tantangan serius dalam bentuk serangan siber yang semakin canggih dan kompleks. Kemajuan teknologi digital seperti IoT, AI, dan big data membuka peluang efisiensi tetapi juga memperbesar risiko keamanan informasi. Serangan seperti phishing, malware, ransomware, hingga skimming telah terbukti mengancam keamanan data dan kepercayaan nasabah, sebagaimana tercermin dalam kasus serangan ransomware terhadap Bank Syariah

Indonesia (BSI). Untuk mengatasi ancaman ini, diperlukan pendekatan keamanan digital yang komprehensif, mencakup penerapan teknologi enkripsi, autentikasi ganda, firewall, dan pemantauan sistem secara berkelanjutan. Selain itu, penting juga bagi lembaga keuangan syariah untuk mengedukasi nasabah, meningkatkan kapasitas SDM internal, serta membangun budaya sadar keamanan yang kuat. Strategi manajemen risiko yang mengacu pada standar internasional seperti ISO 31000:2018 dan kerja sama erat dengan lembaga pengawas seperti OJK dan BSSN menjadi kunci dalam menciptakan sistem pertahanan digital yang tangguh.

Daftar Pustaka

Azizah, S., Ula, Z. N., Mutiara, D., Prameswari, M. P., Ekonomi, F., Islam, U., Abdurrahman, N. K. H., & Pekalongan, W. (2024). *Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile : Studi literatur mengenai cybercrime dan mitigasinya kehidupan , aplikasi keuangan mobile telah menjadi salah satu inovasi terkemuka yang bisnis dalam mengakses dan mengelola keuangan s*. *17*(April), 221–237.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Khikmatin, A., & Setianingsih, P. (2021). Analisis peluang dan tantangan lembaga keuangan syariah dalam upaya meningkatkan daya saing terhadap lembaga keuangan konvensional di indonesia. *Al-Iqtishod: Jurnal Ekonomi Syariah*, *3*(1), 49–62.

Lubis, A. M., Jelita, G., Okta, S., & Wirya, V. (2025). *Tantangan dan Keamanan Teknologi Informasi pada Manajemen Bank Syariah*. *1*.

Maulana, B. R., & Nasrulloh, N. (2024). *Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber Bagus*.

Pertiwi, N. A. S., Umardiyah, F., Mansyur, M. N., Munir, M., Sapiâ, I., Sholichah, A., & Fudlah, T. N. (2024). Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4.0. *Jumat Informatika: Jurnal Pengabdian Masyarakat*, *5*(1), 49–55.

Prasetyo, Y. D. (2024). *STRATEGI PENERAPAN MANAJEMEN RISIKO UNTUK MENCEGAH KEJAHATAN SIBER DI MOBILE BANKING PADA BANK PEMBANGUNAN DAERAH YOGYAKARTA KANTOR CABANG SYARIAH*.

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah: Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25–36.

Sari, S. K., Anggryani, L., Hidayat, R., & Marzuki, S. N. (2024). *TANTANGAN DAN SOLUSI DALAM PENGAWASAN RISIKO DI PERBANKAN SYARIAH PADA ERA CYBER: TINJAUAN LITERATUR BANK SYARIAH INDONESIA Surya*. 6(1), 195–222. https://doi.org/10.1201/9781032622408-13

Widyaningsih, B., Ashlihah, & Afan, T. I. (2024). Peran Manajemen Resiko Dalam Meningkatkan Ketahanan Bank Syariah Di Era Digital. *Jurnal Masharif Al-Syariah …*, 9(204), 1459–1470. https://journal.um-surabaya.ac.id/Mas/article/view/22933

Zudyaten, Septianingsih, R., & Busyro, W. (2016). *PENGARUH CYBER CRIME TERHADAP TINGKAT KEPERCAYAAN MASYARAKAT DALAM BERTRANSAKSI DI BANK SYARIAH KOTA PEKANBARU*. *7*(1), 1–23.