

Digitalisasi perbankan syariah: Tantangan dalam menjaga keamanan data pribadi nasabah

Moh Zaky Fakhrezy

Program Studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang;
e-mail: mohzakyfakhrezy514@gmail.com

Kata Kunci:

keamanan data; perbankan syariah; digitalisasi; ancaman siber; perlindungan data pribadi

Keywords:

data security; Islamic banking; digitalization; cyber threats; personal data protection

ABSTRAK

Penelitian ini membahas tantangan yang dihadapi perbankan syariah dalam menjaga keamanan data pribadi nasabah pada era digitalisasi. Penelitian ini bertujuan untuk menganalisis berbagai ancaman terkait kebocoran data pribadi nasabah akibat digitalisasi layanan perbankan, serta upaya-upaya yang dilakukan bank syariah untuk memitigasi risiko tersebut. Studi kasus dilakukan terhadap bank-bank syariah di Indonesia dengan pendekatan kualitatif. Temuan menunjukkan bahwa ancaman keamanan data utama meliputi serangan siber, kelalaian karyawan, dan kesalahan pengelolaan data oleh bank. Untuk itu, bank syariah perlu menerapkan berbagai kebijakan dan teknologi keamanan data, serta melakukan sosialisasi

kepada nasabah. Hal ini bertujuan untuk mempertahankan kepercayaan nasabah dan memastikan kepatuhan terhadap peraturan perlindungan data pribadi.

ABSTRACT

This study examines the challenges faced by Islamic banking in maintaining the security of customers' personal data in the era of digitalization. This research aims to analyze various threats related to customer personal data leakage due to the digitalization of banking services, as well as efforts made by Islamic banks to mitigate these risks. A case study was conducted on Islamic banks in Indonesia using a qualitative approach. The findings show that the main data security threats include cyberattacks, employee negligence, and data mismanagement by banks. For this reason, Islamic banks need to implement various data security policies and technologies, as well as conduct socialization to customers. This aims to maintain customer trust and ensure compliance with personal data protection regulations.

Pendahuluan

Era digital telah membawa revolusi besar dalam kehidupan manusia, termasuk dalam sektor perbankan. Kemudahan akses dan layanan yang personalisasi menjadi tuntutan utama nasabah di era ini. Untuk menjawab tantangan tersebut, perbankan di Indonesia gencar melakukan transformasi digital. Proses ini tidak hanya sekadar memindahkan layanan konvensional ke platform digital, namun juga melibatkan perubahan mendasar dalam cara berpikir dan berbisnis. Dengan digitalisasi, bank tidak hanya dapat memangkas biaya operasional, tetapi juga menciptakan pengalaman



This is an open access article under the [CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/) license.

Copyright © 2023 by Author. Published by Universitas Islam Negeri Maulana Malik Ibrahim Malang.

perbankan yang lebih seamless dan sesuai dengan kebutuhan nasabah yang terus berkembang (A'yun et al., 2022).

Untuk menarik minat masyarakat, perbankan syariah harus mampu menciptakan layanan digital banking syariah yang tidak hanya praktis, tetapi juga memberikan rasa aman dan nyaman. Pemahaman terhadap kebutuhan dan ekspektasi nasabah menjadi kunci utama dalam membangun kepercayaan. Dengan demikian, nasabah akan merasa lebih yakin untuk menggunakan layanan digital banking syariah (Maghfiro & Budianto 2024).

Dalam upaya memberikan layanan yang lebih modern, bank syariah telah mengadopsi layanan perbankan digital. Akan tetapi, perkembangan teknologi juga membawa risiko baru, yaitu serangan siber. Serangan ini dapat mengakibatkan pencurian data pribadi, gangguan layanan, bahkan pencurian dana nasabah. Untuk melindungi nasabah dari risiko tersebut, pemerintah telah mengeluarkan Undang-Undang Perlindungan Konsumen. UUPK memberikan payung hukum bagi nasabah bank syariah. Salah satu hak yang dijamin adalah hak atas keamanan data pribadi. Bank berkewajiban menjaga keamanan sistemnya dan melindungi data nasabah dari ancaman siber. Selain itu, bank juga wajib memberikan informasi yang akurat dan terbuka kepada nasabah mengenai setiap gangguan layanan yang terjadi. Jika nasabah bank syariah mengalami kerugian akibat pelanggaran yang dilakukan oleh bank, misalnya pencurian data atau gangguan layanan, UUPK memberikan hak kepada nasabah untuk meminta ganti rugi. Besaran ganti rugi yang diberikan harus sesuai dengan kerugian yang dialami oleh nasabah (Marcelliana et al., 2023).

Metode Penelitian

Penelitian ini bertujuan untuk memahami secara mendalam tentang tantangan yang dihadapi oleh perbankan syariah dalam menjaga keamanan data pribadi nasabah di era digital. Studi kasus dilakukan pada Perbankan Syariah di Indonesia dengan menggunakan metode pendekatan kualitatif. Data dikumpulkan melalui penelitian terdahulu. Analisis data dilakukan secara tematik untuk mengidentifikasi tema-tema utama terkait tantangan keamanan data pribadi nasabah, kebijakan perlindungan data yang diterapkan, serta upaya yang dilakukan bank dalam mengatasi tantangan tersebut.

Penelitian ini diharapkan dapat memberikan kontribusi teoritis dan pengetahuan tentang adanya tantangan dalam menjaga keamanan data pribadi nasabah pada perbankan syariah. Temuan penelitian ini dapat membantu perbankan syariah khususnya di Indonesia untuk meningkatkan keamanan dan memberikan rasa aman serta nyaman kepada nasabah, sehingga nasabah akan merasa lebih yakin untuk menggunakan layanan digital banking syariah.

Pembahasan

Pengertian Digitalisasi Perbankan syariah

Perbankan digital merupakan inovasi di sektor keuangan yang memungkinkan nasabah mengakses layanan perbankan melalui teknologi digital, seperti aplikasi seluler atau situs web, tanpa perlu mengunjungi kantor cabang. Konsep ini mencakup berbagai

aktivitas, mulai dari transaksi keuangan hingga manajemen investasi, yang dapat dilakukan secara online. Dalam sistem ini, nasabah dapat melakukan beragam operasi perbankan seperti transfer dana, pembayaran tagihan, dan pembelian produk melalui perangkat yang terhubung internet. Selain itu, mereka juga dapat memeriksa saldo, melihat riwayat transaksi, dan mengakses informasi rekening secara real-time. Beberapa fitur unggulan perbankan digital meliputi kemampuan membuka rekening baru secara online, mengajukan pinjaman, serta berinvestasi dalam berbagai produk keuangan. Bank juga sering menyediakan materi edukasi keuangan melalui platform digital mereka. Keunggulan utama perbankan digital terletak pada aksesibilitas, fleksibilitas waktu, dan efisiensi biaya. Namun, tantangan seperti keamanan data dan kebutuhan akan pemahaman teknologi oleh pengguna juga sangat penting untuk diperhatikan (Junaedi et al., 2023).

Kemudahan yang ditawarkan pada digitalisasi perbankan telah menarik minat banyak nasabah. Ini sejalan dengan prinsip perbankan syariah. Namun, peningkatan penggunaan mobile banking juga membawa risiko kebocoran data yang dapat merusak kepercayaan nasabah (Kartika dan Segaf, 2022). Perbankan syariah merupakan sistem perbankan yang didesain untuk memberikan solusi keuangan yang sesuai dengan nilai-nilai agama dan etika. Seluruh operasionalnya, dari kebijakan internal hingga interaksi dengan nasabah, senantiasa berpedoman pada prinsip-prinsip syariah Islam yang telah teruji kebenarannya. Dengan mengadopsi prinsip bagi hasil, menghindari praktik riba, dan mengutamakan kepentingan masyarakat, perbankan syariah tidak hanya sekedar menawarkan produk dan jasa keuangan, tetapi juga berkontribusi dalam membangun masyarakat yang adil, sejahtera, dan bermartabat. Di Indonesia, perbankan syariah semakin tumbuh dan berkembang, menjadi pilihan bagi mereka yang menginginkan sistem keuangan yang lebih transparan, akuntabel, dan berorientasi pada kesejahteraan bersama (Ash-Shiddiqy, 2023).

Tantangan Keamanan Data Pribadi Nasabah

Ancaman kebocoran data semakin nyata dan meluas ke berbagai sektor, termasuk industri perbankan. Kebocoran data pribadi nasabah, seperti nomor rekening, informasi kartu kredit, dan data identitas, bukan hanya sekedar masalah privasi, tetapi juga dapat menimbulkan kerugian finansial yang besar dan merusak kepercayaan masyarakat terhadap lembaga perbankan. Serangan siber, kesalahan dalam pengelolaan data, atau bahkan kelalaian karyawan dapat menjadi penyebab utama terjadinya kebocoran data. Akibatnya, nasabah berisiko mengalami pencurian identitas, penipuan, dan penyalahgunaan data pribadi untuk tujuan kejahatan. Selain itu, kebocoran data juga dapat memicu krisis kepercayaan yang berdampak negatif pada reputasi lembaga perbankan (Putri et al., 2023).

Data nasabah merupakan aset yang sangat berharga dan harus dijaga kerahasiaannya. Semakin maraknya penggunaan layanan perbankan digital menuntut adanya perlindungan data yang lebih kuat. Penerapan regulasi internasional tentang perlindungan data pribadi nasabah sudah menjadi keharusan. Ketiadaan regulasi akan membuka celah bagi terjadinya pelanggaran privasi dan kebocoran data pribadi. Pertumbuhan pesat ekonomi digital di Indonesia juga diiringi dengan meningkatnya

risiko kebocoran data. Kasus-kasus kebocoran data dalam beberapa tahun terakhir menunjukkan betapa seriusnya ancaman ini (Arfaizar et al., 2023).

Mengingat pentingnya data nasabah, perbankan syariah wajib menerapkan prinsip kehati-hatian yang tinggi dalam menjaga kerahasiaan data para nasabahnya. Pasalnya, data nasabah yang bocor akan dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, sehingga berpotensi merugikan baik institusi maupun para nasabahnya. Dalam era digital seperti sekarang, keamanan data menjadi isu krusial yang tidak boleh diabaikan (Ulhaq & Al Fajar, 2022).

Upaya Mitigasi Risiko Keamanan Data Pribadi Nasabah

Di era digital, perlindungan data pribadi nasabah perbankan semakin mendesak. Meningkatnya kejahatan siber seperti penipuan online dan pencurian identitas mengharuskan masyarakat dan perbankan untuk lebih waspada. Penggunaan kata sandi yang kuat, verifikasi informasi, dan pembaruan perangkat lunak secara berkala adalah langkah-langkah penting untuk melindungi data pribadi (Yunita et al., 2023). Dengan program edukasi dan sosialisasi yang berkelanjutan, kita dapat memberdayakan masyarakat dengan pengetahuan dan keterampilan yang diperlukan untuk melindungi data pribadi mereka di era digital. Melalui pemahaman yang mendalam tentang ancaman siber dan praktik keamanan digital yang baik, masyarakat dapat secara aktif mencegah terjadinya penyalahgunaan data pribadi dan meminimalisir risiko menjadi korban kejahatan siber (Hidayah & Kartini, 2017).

Untuk mempertahankan kepercayaan nasabah dan melindungi kerahasiaan data pribadi, perbankan syariah wajib menerapkan langkah-langkah keamanan data yang komprehensif. Dalam hal ini, perbankan syariah perlu:

- 1) Kebijakan Keamanan yang Kuat: Untuk melindungi data pribadi nasabah, bank syariah wajib menyusun kebijakan keamanan data yang jelas dan komprehensif. Kebijakan ini harus mencakup langkah-langkah terperinci dalam mengelola data nasabah, mulai dari pengumpulan hingga penyimpanan, serta memastikan kepatuhan terhadap seluruh regulasi yang berlaku, termasuk POJK (Maisah et al., 2023).
- 2) Teknologi Keamanan: Untuk mengamankan data nasabah, perbankan syariah mengandalkan teknologi canggih seperti enkripsi data dan sistem deteksi intrusi. Enkripsi berfungsi untuk mengacak data sehingga hanya pihak yang berwenang dapat membacanya, sedangkan sistem deteksi intrusi berperan sebagai penjaga yang selalu siaga untuk mencegah akses tidak sah (Suryawijaya, 2023).
- 3) Edukasi Nasabah: Edukasi mengenai keamanan data pribadi merupakan bagian penting dari layanan yang diberikan oleh bank syariah. Nasabah harus diberitahu tentang bahaya membagi informasi pribadi secara sembarangan, seperti nomor identitas dan PIN, serta pentingnya menjaga kerahasiaan data tersebut. Sebagai tambahan, nasabah juga perlu didorong untuk secara berkala mengganti kata sandi untuk meningkatkan keamanan akun mereka (Cahyono et al., 2024).
- 4) Penilaian dan Manajemen Risiko: Melalui penilaian risiko yang dilakukan secara berkala, bank mampu mendeteksi dini potensi ancaman terhadap keamanan data.

Hal ini memungkinkan bank untuk mengambil langkah-langkah pencegahan yang tepat, seperti memperbarui sistem keamanan dan memberikan edukasi kepada karyawan (Pratama, 2018).

- 5) Respons Terhadap Insiden: Untuk memastikan perlindungan optimal terhadap data nasabah, perbankan syariah perlu memiliki protokol penanganan insiden keamanan yang detail. Protokol ini mencakup langkah-langkah untuk mencegah, mendeteksi, dan merespon insiden keamanan dengan cepat, serta mekanisme untuk meminimalkan dampak negatif terhadap nasabah (Asakdiyah et al., 2024).

Dengan mengintegrasikan berbagai langkah keamanan siber, mulai dari teknologi canggih hingga pelatihan karyawan, bank syariah dapat membangun pertahanan yang kuat terhadap ancaman siber. Hal ini tidak hanya melindungi data pribadi nasabah, tetapi juga memastikan kelancaran operasional bank dan kepatuhan terhadap regulasi yang berlaku.

Kesimpulan dan Saran

Jurnal ini membahas mengenai tantangan yang dihadapi perbankan syariah dalam menjaga keamanan data pribadi nasabah di era digital. Digitalisasi layanan perbankan memudahkan nasabah namun juga meningkatkan risiko kebocoran data. Data nasabah merupakan aset penting yang perlu dijaga kerahasiaannya. Ancaman serangan siber, kesalahan pengelolaan data, bahkan kelalaian karyawan dapat merugikan nasabah dan merusak reputasi bank. Oleh karena itu, perbankan syariah perlu menerapkan berbagai upaya untuk menjaga keamanan data, seperti kebijakan dan teknologi yang memadai serta edukasi kepada nasabah dan karyawan. Bank juga harus melakukan penilaian risiko secara berkala.

Berdasarkan pembahasan di atas, penulis menyarankan agar perbankan syariah dapat meningkatkan upaya keamanan data nasabah dengan: 1) memperbaharui kebijakan dan teknologi keamanan data secara berkala seiring perkembangan ancaman siber; 2) meningkatkan literasi digital nasabah melalui berbagai program edukasi yang terstruktur; dan 3) melakukan audit keamanan secara rutin untuk memastikan sistem keamanan telah memadai. Dengan berbagai langkah perbaikan secara berkelanjutan, diharapkan perbankan syariah dapat terus melindungi hak nasabah dan mempertahankan kepercayaan masyarakat di era digital.

Daftar Pustaka

- Arfaizar, J., Ayu, N., Riyanto, F., YUSDANI, Y., & Muliadi, S. (2023). Dinamika kontemporer dalam transaksi perbankan syariah dan problematikanya. *Wadiah*, 7 (2), 163–191. <https://doi.org/10.30762/wadiah.v7i2.327>.
- Asakdiyah, S., Rachmiani., Musafir., & Hasim. (2024). Dampak reputasi, responsifitas, pemberian hadiah, dan rekomendasi terhadap nasabah yang berpindah dari BSI ke bank konvensional. *Jurnal EMT KITA*, 8(1), 263–272. <https://doi.org/10.35870/emt.v8i1.1707>.
- Ash-Shiddiqy, M. (2023). Analisis perbandingan kinerja keuangan bank syariah dan bank konvensional. *Risalah iqtisadiyah: Journal of Sharia Economics*, 2(2), 18-25.

- Cahyono, D., Fahrudin, R., & Sinclair, A. (2024). Pentingnya edukasi dalam mengatasi keamanan data mobile banking di Indonesia. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 3(1), 81-89.
- Hidayah, A. N., & Kartini, I. A. (2017). Peranan bank syariah dalam sosialisasi dan edukasi masyarakat tentang kemanfaatan produk dan jasa perbankan syariah. *Kosmik Hukum*, 16(1), 74-86.
- Kartika, G., & Segaf, S. (2022). Kombinasi peran model TAM dan CARTER terhadap optimalisasi kepuasan nasabah mobile syariah banking di masa pandemi Covid-19. *Jurnal Manajerial*, 9(02), 152-167.
<https://doi.org/10.30587/jurnalmanajerial.v9i02.3969>.
- Maghfiro, N., & Budianto, E. W. H. (2024). Determinan minat menggunakan layanan digital banking syariah pada generasi z di Kota Malang. *Jurnal Dimensi*, 13(2), 352-363.
- Maisah, M., Sari, S. P., Sudiarni, S., & Ompusunggu, H. P. (2023). Analisis hukum terhadap perlindungan data pribadi nasabah dalam layanan perbankan digital di Indonesia. *Aufklarung: Jurnal Pendidikan, Sosial dan Humaniora*, 3(3), 285-290.
- Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., ... & Bayhaqi, T. A. R. (2023). Penerapan perlindungan konsumen terhadap nasabah PT. Bank Syariah Indonesia dalam kasus kebocoran data nasabah. *Depositi: Jurnal Publikasi Ilmu Hukum*, 1(2), 180-194.
- Pratama, R. (2018). Penerapan manajemen risiko pada perbankan syariah: Studi kasus pada Bank Muamalat & Bank Syariah Mandiri cabang Kota Ternate. *Jurnal Mitra Manajemen*, 2(6), 597-609. <https://doi.org/10.52160/ejmm.v2i6.162>.
- 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. <https://doi.org/10.61722/jiem.v1i4.331>.
- Suryawijaya, T. W. E. (2023). Memperkuat keamanan data melalui teknologi blockchain: mengeksplorasi implementasi sukses dalam transformasi digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55-68.
<https://doi.org/10.21787/jskp.2.2023.55-68>.
- Ulhaq, M. Z., & Al Fajar, M. R. (2022). Peluang dan tantangan bank syariah di era digital. *J-Esa (Jurnal Ekonomi Syariah)*, 5(1), 49-61.
<http://ejournal.iaimbima.ac.id/index.php/jesa>.
- Yunita, A. R., Sari, S. P., Putri, F. E., Felissia, D. S., Fadhilana, Y. R., & Arizzal, N. Z. (2023, November). Hukum perdata nasional di era digital: Tantangan dan peluang dalam perlindungan data pribadi. In *Proceeding of Conference on Law and Social Studies*, 4(1).