KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.2, No.1 Januari 2025
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 01-11
DOI : https://doi.org/10.61722/jinu.v2i1.3075

IMPLEMENTASI TEKNOLOGI UNTUK PENGUATAN KEAMANAN DATA PRIBADI NASABAH DALAM SEKTOR PERBANKAN

Syakira Edriamarsha Firdaus
syakiramrsha@students.unnes.ac.id
Ilmu Hukum, Universitas Negeri Semarang, Indonesia
Syarifaatul Hidayah
hidayahsari109@students.unnes.ac.id
Ilmu Hukum, Universitas Negeri Semarang, Indonesia
Herjuno Putro
herjunputro@students.unnes.ac.id
Ilmu Hukum, Universitas Negeri Semarang, Indonesia

ABSTRACT *Rapid technological developments have brought major transformation in the banking sector, especially in the aspect of digitalization of services. However, this progress is accompanied by big challenges, especially regarding the security of customers' personal data which is vulnerable to cyber threats. This article discusses various technologies used by banks to protect customer data, such as data encryption, fintech technology, and the implementation of cloud-based security systems. Apart from that, this article also discusses regulations governing personal data protection in Indonesia, such as Law no. 27 of 2022, as well as Financial Services Authority (OJK) regulations. The research method used is normative juridical with a conceptual and technological approach. Even though various technologies have been implemented, various challenges remain. Therefore, the banking sector also needs to continue to improve its security system. This effort is expected to create a safer banking system and increase public trust in digital banking services.*
Keywords*: Banking, Security, and Technology.*

ABSTRAK Perkembangan teknologi yang pesat telah membawa transformasi besar di sektor perbankan, terutama dalam aspek digitalisasi layanan. Namun, kemajuan ini diiringi dengan tantangan besar, khususnya terkait keamanan data pribadi nasabah yang rentan terhadap ancaman siber. Artikel ini membahas berbagai teknologi yang digunakan perbankan untuk melindungi data nasabah, seperti enkripsi data, teknologi fintech, serta penerapan sistem keamanan berbasis cloud. Selain itu, dalam artikel ini dibahas juga mengenai regulasi yang mengatur perlindungan data pribadi di Indonesia, seperti UU No. 27 Tahun 2022, serta peraturan Otoritas Jasa Keuangan (OJK). Metode penelitian yang digunakan yaitu yuridis normatif dengan pendekatan konseptual dan teknologis. Meskipun berbagai teknologi telah diimplementasikan, namun berbagai tantangan tetap ada. Oleh karena itu, sektor perbankan juga perlu untuk terus meningkatkan sistem keamanannya. Upaya ini diharapkan dapat menciptakan sistem perbankan yang lebih aman dan meningkatkan kepercayaan masyarakat terhadap layanan digital perbankan.
Kata Kunci: Perbankan, Keamanan, dan Teknologi.

PENDAHULUAN

Pada era kini, manusia hidup dalam periode globalisasi dan era modern, dimana segala hal berkembang dengan sangat cepat dan tak terbendung. Perkembangan kehidupan manusia yang tadinya bergerak lamban, berkat pemikiran manusia yang semakin maju dan peradaban budaya mendukung terjadinya kemajuan khususnya di

Received Oktober 30, 2024; Revised November 30, 2024; Januari 01, 2025
* Syakira Edriamarsha Firdaus, *syakiramrsha@students.unnes.ac.id*

sektor teknologi[1]. Perkembangan teknologi diawali dengan adanya internet yang mendukung manusia untuk berinteraksi dengan sesama tanpa memandang jarak dan waktu. Semua orang dapat terhubung hanya dari balik layar komputer ataupun gawai.

Perkembangan internet telah menyebar ke berbagai aspek kehidupan manusia termasuk ekonomi khususnya di sektor perbankan. Bank sebagai subjek penting dalam menggerakkan perekonomian suatu negara karena menjadi penyelenggara sistem pembayaran dan sumber utama kredit dalam mencari modal sebagai stimulus bisnis dan sebagai tempat yang aman untuk menyimpan uang[2]. Sehingga dalam perkembangnya, bank harus mengikuti kemajuan teknologi ditandai dengan adanya *internet banking* dipelopori oleh salah satu bank swasta nasional pada medio 1999 lalu diikuti oleh 7 bank Indonesia seperti Bank Lippo, BCA, Bank Bali, BII, Bank Universal, Bank Niaga dan Citibank[3].

Sejak hadirnya *internet banking* di Indonesia, semakin memudahkan nasabah dalam menyelesaikan urusan perbankan dalam hitungan menit, kapanpun dan dimanapun. Walaupun *internet banking* menawarkan kemudahan dan kenyamanan di dalam bertransaksi baik dalam melakukan pengiriman uang antar bank serta pembayaran, namun mempengaruhi munculnya bentuk-bentuk kejahatan baru melalui cybercrime. Dalam layanan *internet banking*, data pribadi dapat dicuri jika gawai nasabah dimanfaatkan orang lain karena dipinjam, dicuri, atau hilang. Tidak hanya itu, ancaman juga dapat timbul di dunia digital atau yang lebih sering disebut dengan cybercrime dengan hanya memanfaatkan kode ataupunk link yang dikirimkan. Bentuk-bentuk kejahatan digital dalam sektor perbankan sudah banyak terjadi dan merugikan banyak orang bahkan mengancam keamanan nasional.

Dikarenakan sudah banyaknya terjadinya kejahatan di sektor perbankan diperlukan perlindungan data nasabah dengan lebih ketat. Data yang dimaksudkan seperti data pribadi baik dari nama, npwp, hingga nomor induk kependudukan nasabah. Lalu nomor rekening, informasi keuangan, data kredit, kode OTP, dank ode CVV/CVC. Keamanan data merupakan aspek yang sangat penting dalam *internet banking* di karena

[1]Arum, S., Kaltsum, D., & Muslichah, I, Artikel Hasil Penelitian Mobile Banking. 01(02), 31– 46, 2022, https://journal.uii.ac.id/selma/index

[2] Muhammad Akbar Suharbi dan Hendro Margono, "Kebutuhan transformasi bank digital Indonesia di era revolusi industri 4.0", Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan Volume 4, Number 10, hlm. 4750, 2022

[3] Direktorat Penelitan dan Pengaturan Perbankan Bank Indonesia, "Internet Banking di Indonesia," Bank Indonesia

informasi yang dikumpulkan sangatlah sensitif dan dapat digunakan oleh pihak luar untuk melakukan kejahatan keuangan.

Selain itu perlindungan data merupakan hak asasi manusia yang bersifat fundamental dan telah diakui oleh beberapa negara perlindungan data sebagai hak konstitusional atau dalam bentuk *"habeas data",* yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya. Sehingga sektor perbankan harus melakukan penguatan teknologi dalam melindungi data nasabah tidak hanya sebagai bentuk tanggung jawab dan implementasi dari Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi, namun juga menjaga integritas dan kepercayaan masyarakat terhadap sistem perbankan secara keseluruhan

METODE

Metode penelitian yang digunakan dalam artikel ini adalah metode yuridis normatif dengan pendekatan konseptual dan teknologis. Data diperoleh yaitu dari bahan hukum primer seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan peraturan-peraturan OJK, serta bahan sekunder berupa jurnal, artikel, dan laporan penelitian yang relevan. Analisis yang dilakukan yaitu secara deskriptif yang bertujuan untuk memberikan gambaran mengenai penerapan teknologi keamanan dalam sektor perbankan dan efektivitasnya dalam melindungi data pribadi nasabah.

HASIL DAN PEMBAHASAN

A.Teknologi Saat ini Yang Digunakan Oleh Bank dalam Melindungi Data Pribadi Nasabah

Saat ini, masyarakat hidup dalam dua era yang saling mempengaruhi: era globalisasi dan era modern, di mana keduanya ditandai oleh perkembangan teknologi yang pesat. Perkembangan ini juga berdampak besar pada sektor keuangan, termasuk perbankan, yang terus berinovasi untuk memenuhi kebutuhan masyarakat modern. Saat ini, sektor perbankan menghadapi tantangan besar dalam melindungi data pribadi nasabah dari ancaman kebocoran dan serangan siber. Oleh karena itu, berbagai teknologi modern telah diimplementasikan untuk memastikan keamanan data nasabah, baik yang tersimpan di sistem internal maupun yang digunakan dalam transaksi.

Salah satu inovasi tersebut adalah layanan mobile banking atau sering disebut M-banking. M-banking merupakan layanan perbankan yang memanfaatkan perangkat seluler, terutama ponsel pintar, untuk menyediakan akses mudah dan cepat ke berbagai transaksi perbankan. Melalui aplikasi M-banking, bank menawarkan kemudahan bagi nasabah untuk mengelola akun mereka kapan saja dan di mana saja. Layanan ini mencakup berbagai aktivitas, seperti memeriksa saldo, melakukan transfer dana, hingga pembayaran tagihan. Dengan teknologi ini, transaksi perbankan menjadi lebih efisien, aman, dan nyaman[4]. Keunggulan utama M-banking terletak pada fleksibilitasnya. Dengan hanya menggunakan telepon seluler yang terhubung ke internet, nasabah dapat menjalankan berbagai kebutuhan keuangan tanpa harus mengunjungi kantor cabang bank atau mesin ATM. Layanan ini tidak hanya mempermudah kehidupan sehari-hari, tetapi juga mempercepat proses transaksi di tengah gaya hidup modern yang serba cepat.

Salah satu teknologi utama yang digunakan bank untuk melindungi data nasabah adalah enkripsi data. Teknologi ini dirancang untuk memastikan bahwa data yang dikirimkan atau disimpan di sistem perbankan hanya dapat diakses oleh pihak yang berwenang. Proses enkripsi mengubah informasi menjadi kode yang sulit dipahami tanpa kunci dekripsi yang sesuai. Dengan demikian, meskipun data jatuh ke tangan pihak yang tidak bertanggung jawab, data tersebut tetap tidak dapat dibaca atau dimanfaatkan. Pada umumnya bank menggunakan algoritma enkripsi canggih seperti Advanced Encryption Standard (AES) untuk memberikan perlindungan tingkat tinggi[5]. Teknologi ini tidak hanya diterapkan pada komunikasi data antar server, tetapi juga pada aplikasi mobile dan internet banking, sehingga keamanan data nasabah tetap terjaga di berbagai titik akses. Implementasi enkripsi yang kuat menjadi fondasi penting dalam upaya bank menjaga kepercayaan nasabah di era digital yang semakin rentan terhadap ancaman keamanan.

Tidak hanya terbatas pada teknologi tersebut, terdapat juga teknologi fintech yang digunakan oleh perbankan untuk melindungi data nasabah. Perkembangan teknologi finansial (fintech) telah menghadirkan perubahan besar dalam cara layanan keuangan dijalankan di seluruh dunia. Dengan mengintegrasikan teknologi canggih ke dalam sektor keuangan, fintech berhasil menciptakan solusi inovatif yang lebih efisien, inklusif, dan

[4] Fasa, M. I., & Susanto, I. (2024). ANALISIS PERAN KEAMANAN DATA DALAM MENINGKATKAN KEPUASAN NASABAH PADA PENGGUNAAN MOBILE BANKING. *Jurnal Media Akademik (JMA)*, *2*(11).
[5] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, *2*(01), 163-171.

mudah diakses oleh masyarakat. Namun, transformasi ini juga membawa tantangan baru, terutama dalam hal perlindungan data nasabah. Platform fintech mengumpulkan berbagai data pribadi, seperti identitas, informasi keuangan, hingga pola transaksi pengguna. Data-data ini menjadi target yang mudah bagi kejahatan siber, termasuk pencurian identitas dan penyalahgunaan data untuk kepentingan ilegal. sehingga terdapat juga tantangan keamanan data dalam fintech[6].

Di Indonesia, Otoritas Jasa Keuangan (OJK) telah merancang regulasi untuk mengawasi operasional fintech, seperti yang tercantum dalam Peraturan OJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Regulasi ini mencakup panduan operasional, perlindungan konsumen, dan kewajiban untuk menjaga keamanan data. Namun, tantangan masih ada, seperti kurangnya pemahaman di kalangan pelaku industri tentang pentingnya keamanan data, serta minimnya infrastruktur untuk mendukung pengawasan yang optimal. Mengamankan data pelanggan di bidang fintech bukan hanya tanggung jawab penyedia layanan, namun juga memerlukan dukungan peraturan yang kuat dan kesadaran pengguna yaitu dengan menggabungkan teknologi canggih, regulasi yang adaptif sehingga, fintech dapat menciptakan sistem keuangan yang aman dan inovatif

Selain itu, banyak bank telah mengadopsi teknologi autentikasi multi-faktor (Multi-Factor Authentication/MFA). Sistem ini mewajibkan nasabah untuk melewati lebih dari satu lapisan keamanan, seperti kombinasi kata sandi, kode OTP yang dikirim ke ponsel, atau bahkan autentikasi biometrik seperti sidik jari atau pengenalan wajah. Hal ini mencegah akses tidak sah ke akun nasabah meskipun kata sandi mereka berhasil dicuri. Terdapat juga adanya teknologi blockchain yang juga mulai diterapkan dalam sistem perbankan, terutama untuk memastikan transparansi dan keamanan dalam pengelolaan data. Blockchain menciptakan catatan transaksi yang tidak dapat diubah, sehingga mempersulit pihak tidak bertanggung jawab untuk memanipulasi data nasabah. Di samping itu, bank menerapkan sistem firewall canggih dan sistem deteksi serta pencegahan intrusi (IDS/IPS) untuk melindungi jaringan mereka dari serangan siber eksternal. Firewall bertindak sebagai penghalang pertama, sementara IDS/IPS memonitor dan memblokir aktivitas mencurigakan secara real-time.

[6] Fahri, A. A. R., & Melda, M. (2023). Perbandingan Regulasi Teknologi Finansial (Fintech) Terhadap Perlindungan Data Nasabah Di Indonesia Dengan Filipina dan Uni Eropa. *Indonesian Journal of Management Studies*, *1*(3), 7-13.

Langkah-langkah tersebut juga dilengkapi dengan penerapan *Cloud Security* bagi bank yang mulai memanfaatkan layanan komputasi awan. Sistem keamanan berbasis cloud memungkinkan data untuk disimpan dengan tingkat enkripsi tinggi dan akses yang sangat terbatas, sehingga meningkatkan efisiensi sekaligus keamanan. Keamanan data yang disimpan dalam sistem komputasi awan sangat bergantung pada langkah-langkah perlindungan yang diterapkan oleh penyedia layanan cloud. Jika penyedia layanan tidak menerapkan pengamanan yang memadai, risiko terhadap keamanan data akan meningkat. Bahkan jika langkah pengamanan dianggap sudah cukup baik, potensi risiko tetap ada karena data pengguna tidak tersimpan secara lokal di perangkat milik mereka, melainkan di server milik pihak penyedia layanan. Hal ini menimbulkan kekhawatiran, terutama terkait aksesibilitas dan potensi kebocoran data yang disebabkan oleh celah keamanan pada infrastruktur penyedia cloud[7].

Secara keseluruhan, berbagai teknologi tersebut saling melengkapi untuk memberikan perlindungan yang menyeluruh terhadap data pribadi nasabah. Namun, tantangan tetap muncul, terutama dalam menghadapi ancaman baru yang terus berkembang. Oleh karena itu, bank juga harus secara konsisten memperbarui sistem keamanannya agar dapat menjaga data nasabah tetap terlindungi dengan aman dan optimal.

B. Tantangan Yang Dihadapi Oleh Bank dalam Menerapkan Teknologi Untuk Menjaga Keamanan Data Pribadi

Perbankan sebagai sektor yang berperan penting dalam jalur perekonomia dan memiliki kendali dalam pengelolaan data nasabah melakukan segala hal yang mereka bisa untuk melindungi data pribadi nasabah mereka sehingga diharapkan tidak akan terjadi keadaan yang tidak diinginkan seperi pembobolan data, pencurian, ataupun hal lainnya. Meskipun, perbankan telah melakukan segala upaya dalam menjaga keamanan data pribadi nasabah, tetap ada tantangan yang dihadapi dalam tersebut. Adapun hal-hal yang menjadi tantangan Perbankan dalam menjaga keamanan data pribadi nasabah sebagai berikut:

1. Memperoleh dan Menjaga Persetujuan Data Nasabah

[7] Alim, Z. (2016). Meningkatkan Keamanan Data Cloud Computing menggunakan Algoritma Vigenere Cipher Modifikasi. *Jurnal TIMES*, *5*(1), 23-27.

Kurnia Rosyada selaku Senior Vice President (SVP) Enterprise Data Analytics Bank Mandiri, mengungkapkan tantangan pertama yang dihadapi dalam menjaga data pribadi nasabah adalah memperoleh izin atau consent dari nasabah untuk menyimpan data pribadi mereka dikarenakan adanya data yang bersifat wajib atau *mandatory* dan opsional. Kadang kala nasabah tidak mau memberikan persetujuan dalam penyimpanan data ini padahal penting bagi perbankan dalam memperoleh izin dari nasabah tersebut agar mereka bisa melacak perubahan izin dari nasabah. Persetujuan ini juga akan mempengaruhi perbankan dalam menjaga atau *maintaining* yang berkaitan dengan permintaan nasabah dalam beberapa hal, seperti meminta akses data, meminta dilakukan penyetopan data yang diproses, dan meminta untuk dilakukan penghapusan[8].

2. Ancaman Kejahatan Digital

Kejahatan digital atau Cyber Crime merupakan bentuk kejahatan yang dilakukan dengan memanfaatkan tekonologi internet. Dalam hal perbankan ada berbagai macam bentuk cybercrime berupa pencurian data, mulai dari pencurian gawai nasabah, kartu ATM atau kredit nasabah, hingga pencurian pin ATM dan kode *internet banking*. Tidak peduli seberapa maju perkembangan perbankan dalam melindungi data pribadi nasabah, pelaku kejahatan juga mengembangkan teknik pencuriannya.

Bentuk kejahatan tersebut seperti Pishing, yaitu tindakan yang berpura-pura menjadi seseorang yang terpecaya di bidangnya untuk memancing nasabah memberikan informasi sensitif, seperti username, password, dan rincian kartu kredit. Selain itu terdapat kejahatan ransomware perangkat lunak yang dirancang untuk mengenkripsi data pada komputer atau sistem korban, sehingga akses ke data tersebut dibatasi hingga tebusan dibayarkan kepada penyerang[9]. Jenis-jenis kejahatan ini dapat terjadi dikarenakan adanya kelalaian nasabah yang tidak berhati-hati dalam memberikan data pribadinya ke orang lain ataupun dengan mudahnya mengakses link atau website mencurigakan yang dapat memberikan

[8] Galih Pratama, "Bank Mandiri Ungkap Tantangan dalam Melindungi Data Nasabah," Infobanknews.com, https://infobanknews.com/bank-mandiri-ungkap-tantangan-dalam-melindungi-data-nasabah/, 2024
[9] Sri Retno Rahayu, "White Paper Pishing," Universitas Brawijaya, 2019

akses kepada pelaku kejahatan untuk mengakses gawai mereka khususnya aplikasi banking[10].

Sehingga diperlukan kesadaran oleh nasabah agar tidak mempercayai orang lain dengan mudah dan memberikan data pribadinya serta tidak sembarangan mengakses link dari orang tidak dikenal serta segera melapor ke pihak jika menghadapi hal-hal tersebut.

3. Rendahnya Literasi Digital

   Berkaitan dengan tantangan sebelumnya, masih banyaknya masayarakat yang rendahliterasi digital. Nasabah-nasabah perbankan tersebut tidak memiliki pengetahuan cukup mengenai risiko siber dan pentingnya menjaga keamanan data pribadi. Hal ini menjadikan mereka lebih rentan terhadap serangan siber, di mana pelaku kejahatan memanipulasi nasabah untuk memberikan informasi sensitif. Tanpa literasi digital yang memadai, nasabah cenderung menjadi target bagi penipuan dan pencurian data[11]. Oleh karena itu, bank perlu melaksanakan program edukasi bagi nasabah mengenai praktik keamanan data yang baik, seperti tidak membagikan informasi login atau kata sandi dengan pihak ketiga.

   Tidak hanya edukasi dari bank, nasabah sendiri harus memiliki kesadaran diri akan pentingnya mengetahui informasi digital khususnya yang berkaitan dengan perbankan sehingga saat menghadapi pelaku kejahatan ataupun kegiatan yang mencurigakan, mereka dapat menganalisa dengan baik apakah hal tersebut dapat dipercayai atau harus dicurigai.

Dalam menghadapi tantangan menjaga privasi data nasabah, perbankan tidak dapat bekerja sendiri, diperlukan bantuan dari nasabah juga untuk lebih sadar akan keamanan digital dan menambah pengetahuan akan bentuk-bentuk kejahatan siber yang sudah banyak dibahas melalui internet maupun himbauan yang diberikan oleh pihak bank sendiri. Selain itu, diperlukan dukungan dari pemerintah dengan mengadakan regulasi yang akurat dan memberikan kepastian akan perlindungan data nasabah.

[10] Krippendorff, K, "The Cybersecurity Dilemma: Policy and Strategy in the Internet Era". Oxford University Press, 2019

[11] Bellovin, S. M., & Schneier, B, "Emerging Security Threats in Digital Banking". Financial Security Today, 6(2), hlm. 15-23, 2017

C. Efektivitas Sistem Keamanan Oleh Bank Dalam Melindungi Data Pribadi Nasabah

Pentingnya sistem keamanan yang ketat dalam melindungi data pribadi nasabah semakin meningkat di era digital. [12]Layanan perbankan digital, yang mencakup akses melalui perangkat elektronik seperti komputer, smartphone, atau tablet, kini menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Era ekonomi digital sendiri ditandai oleh penggunaan teknologi informasi dan komunikasi yang mendalam di berbagai aspek aktivitas ekonomi. Popularitas perbankan digital semakin terus meningkat karena adanya kemudahan akses dan efisiensi waktu dalam pelaksanaannya. Peraturan Bank Indonesia Nomor 22 Tahun 2020 tentang Sistem Pembayaran menegaskan bahwa penyelenggaraan sistem pembayaran memiliki tujuan utama untuk menciptakan layanan pembayaran yang mudah diakses, berbiaya rendah, aman, cepat, dan andal. Dalam mencapai tujuan ini, aspek perlindungan nasabah menjadi salah satu elemen yang sangat penting.

[13]Perlindungan nasabah tidak hanya berfungsi untuk memberikan rasa aman kepada pengguna, tetapi juga menjadi bagian integral dari operasional perbankan digital. Hal ini didukung oleh kebutuhan untuk menjaga integritas sistem perbankan dan memastikan stabilitas sektor keuangan, khususnya dalam bidang layanan digital. Perlindungan yang dimaksud mencakup berbagai langkah untuk melindungi data pribadi nasabah, mencegah potensi penyalahgunaan informasi, dan memastikan bahwa layanan digital berjalan dengan standar keamanan tinggi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mewajibkan bank untuk menjaga kerahasiaan informasi pribadi nasabah sebagai bagian dari upaya melindungi privasi dan hak mereka. Meski aturan ini sudah ditetapkan, pelaksanaannya di lapangan masih sering menghadapi berbagai kendala sehingga belum sepenuhnya memenuhi standar yang diharapkan.

Oleh karena itu, bank memiliki tanggung jawab besar untuk terus memperkuat sistem keamanan mereka guna melindungi data nasabah dari berbagai ancaman yang semakin kompleks di era digital. [14]Upaya ini tidak hanya mencakup peningkatan teknologi dan protokol keamanan, tetapi juga melibatkan pendekatan yang proaktif dalam

[12] 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.
[13] Sitorus, H. A. M. (2023). Perlindungan Hukum Terhadap Nasabah Atas Fraud Pada Transaksi Bank Digital. *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)*, 7(1), 554-569.
[14] 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.

memberikan edukasi kepada nasabah. Bank perlu mengedukasi nasabah mengenai pentingnya langkah-langkah perlindungan data, seperti menggunakan kata sandi yang kuat, mengenali potensi penipuan, dan memahami prosedur keamanan yang diterapkan oleh bank. Dengan cara ini, nasabah tidak hanya merasa lebih terlindungi, tetapi juga memiliki pemahaman yang lebih baik tentang peran mereka dalam menjaga keamanan data pribadi.

KESIMPULAN

Kesimpulan dari artikel ini menegaskan bahwa dalam era globalisasi dan modernisasi yang ditandai dengan kemajuan teknologi, sektor perbankan di Indonesia harus mampu beradaptasi dengan cepat untuk melindungi data pribadi nasabah. Meskipun teknologi seperti internet banking dan mobile banking memberikan kemudahan akses bagi nasabah, tantangan keamanan siber tetap menjadi ancaman serius, termasuk pencurian data dan kejahatan digital lainnya. Oleh karena itu, penting bagi bank untuk menerapkan berbagai teknologi keamanan, seperti enkripsi data dan autentikasi multi-faktor, serta meningkatkan literasi digital di kalangan nasabah. Perlindungan data bukan hanya tanggung jawab bank, tetapi juga memerlukan kesadaran dan partisipasi aktif dari nasabah serta dukungan regulasi yang kuat dari pemerintah. Dengan langkah-langkah ini, diharapkan kepercayaan masyarakat terhadap sistem perbankan dapat terjaga, sekaligus menciptakan lingkungan perbankan yang lebih aman dan efisien.

SARAN

Saran yang dapat diberikan dalam artikel ini adalah agar sektor perbankan di Indonesia meningkatkan kolaborasi dengan berbagai pihak, termasuk pemerintah, penyedia teknologi, dan masyarakat, untuk memperkuat perlindungan data pribadi nasabah. Bank sebaiknya menerapkan program edukasi yang komprehensif untuk meningkatkan literasi digital nasabah, sehingga mereka lebih sadar akan risiko kejahatan siber dan cara melindungi informasi pribadi mereka. Selain itu, penting bagi bank untuk terus berinvestasi dalam teknologi keamanan terbaru, seperti enkripsi data yang lebih kuat dan sistem autentikasi multi-faktor, guna menghadapi ancaman yang terus berkembang. Dengan mengedepankan transparansi dan komunikasi yang baik kepada nasabah mengenai langkah-langkah keamanan yang diambil, bank dapat membangun kepercayaan

dan memastikan bahwa data nasabah terlindungi dengan baik. Terakhir, dukungan regulasi dari pemerintah juga sangat diperlukan untuk menciptakan kerangka hukum yang jelas dan efektif dalam melindungi data pribadi di sektor perbankan.

DAFTAR PUSTAKA

Alim, Z. (2016). Meningkatkan Keamanan Data Cloud Computing menggunakan Algoritma Vigenere Cipher Modifikasi. *Jurnal TIMES*, *5*(1), 23-27.

Arum, S., Kaltsum, D., & Muslichah, I. (2022). Artikel Hasil Penelitian Mobile Banking. 01(02), 31– 46. https://journal.uii.ac.id/selma/index

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, *2*(01), 163-171.

Bellovin, S. M., & Schneier, B. (2017). "Emerging Security Threats in Digital Banking". Financial Security Today. 6(2). hlm. 15-23.

Direktorat Penelitan dan Pengaturan Perbankan Bank Indonesia, "Internet Banking di Indonesia," Bank Indonesia.

Fahri, A. A. R., & Melda, M. (2023). Perbandingan Regulasi Teknologi Finansial (Fintech) Terhadap Perlindungan Data Nasabah Di Indonesia Dengan Filipina dan Uni Eropa. *Indonesian Journal of Management Studies*, *1*(3), 7-13.

Fasa, M. I., & Susanto, I. (2024). ANALISIS PERAN KEAMANAN DATA DALAM MENINGKATKAN KEPUASAN NASABAH PADA PENGGUNAAN MOBILE BANKING. *Jurnal Media Akademik (JMA)*, *2*(11).

Galih Pratama. (2024). "Bank Mandiri Ungkap Tantangan dalam Melindungi Data Nasabah". Infobanknews.com. https://infobanknews.com/bank-mandiri-ungkap-tantangan-dalam-melindungi-data-nasabah

Krippendorff, K. (2019). "The Cybersecurity Dilemma: Policy and Strategy in the Internet Era". Oxford University Press

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.

Muhammad Akbar Suharbi dan Hendro Margono. (2022). "Kebutuhan transformasi bank digital Indonesia di era revolusi industri 4.0". Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan Volume 4, Number 10. hlm. 4750.

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.

Sri Retno Rahayu. 2019. "White Paper Pishing". Universitas Brawijaya.

Sitorus, H. A. M. (2023). Perlindungan Hukum Terhadap Nasabah Atas Fraud Pada Transaksi Bank Digital. *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)*, *7*(1), 554-569.