Seminar Nasional Manajemen, Ekonomi dan Akuntansi
Fakultas Ekonomi dan Bisnis UNP Kediri
ISSN: 2776-8171
URL: https://proceeding.unpkediri.ac.id/index.php/senmea

ANALISIS RISIKO DAN KEAMANAN DALAM LAYANAN PERBANKAN *ONLINE*: STUDI LITERATUR

Urika[1], Mustafidah Mahardhika[2]*
[1),2)] Universitas Sultan Ageng Tirtayasa, Jl.Raya Palka KM. 3 Sindangsari, Kec. Pabuaran, Kab. Serang, Prov. Banten
urika@untirta.ac.id
mustafidah.mahardhika@untirta.ac.id*

Informasi artikel :
Tanggal Masuk : 31-10-2025 Tanggal Revisi : 10-11-2025 Tanggal diterima: 20-11-2025

Abstract

The development of digital technology has driven a major transformation in the banking system, particularly through online banking services that provide easy access for customers. However, this progress has also been accompanied by an increase in cybercrime risks that threaten the security of financial institutions. This study aims to analyze the forms of risk and security threats in digital banking services, evaluate the mitigation strategies that have been implemented, and provide recommendations for strengthening the digital banking security system in Indonesia. The method used is a literature study by reviewing national journals and publications from the Financial Services Authority (OJK). The results of the study show that the main risks faced by banks include phishing attacks, malware, and personal data leaks that impact both financial institutions and customers. The mitigation strategies implemented have not been fully effective due to weak supervision and uneven implementation. Therefore, a comprehensive approach is needed through strengthening security technology, improving cyber governance, increasing digital literacy, and collaborating on research and innovation to build a sustainable digital banking ecosystem.

Keywords: Digital Banking Services, Data Security, Cyber Threats, Mitigation Strategies, Policy Recommendations

Abstrak

Perkembangan teknologi digital telah mendorong transformasi besar dalam sistem perbankan, khususnya melalui layanan perbankan daring yang memberikan kemudahan akses bagi nasabah. Namun, kemajuan ini juga disertai dengan meningkatnya risiko kejahatan siber yang mengancam keamanan lembaga keuangan. Penelitian ini bertujuan untuk menganalisis bentuk risiko dan ancaman keamanan dalam layanan perbankan digital, mengevaluasi strategi mitigasi yang telah diterapkan, serta memberikan rekomendasi penguatan sistem keamanan perbankan digital di Indonesia. Metode yang digunakan adalah studi literatur dengan menelaah jurnal nasional dan publikasi dari Otoritas Jasa Keuangan (OJK). Hasil penelitian menunjukkan bahwa risiko utama yang dihadapi perbankan meliputi serangan *phishing, malware*, dan kebocoran data pribadi yang berdampak pada lembaga keuangan maupun nasabah. Strategi mitigasi yang diterapkan belum sepenuhnya efektif akibat lemahnya pengawasan serta implementasi yang belum merata. Dengan demikian, diperlukan pendekatan komprehensif melalui penguatan teknologi keamanan, perbaikan tata kelola siber, peningkatan literasi digital, serta kolaborasi riset dan inovasi untuk membangun ekosistem perbankan digital yang berkelanjutan.

Kata Kunci: Layanan Perbankan Digital, Keamanan Data, Ancaman Siber, Strategi Mitigasi, Rekomendasi Kebijakan

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan mendasar dalam sistem keuangan global. Hal ini ditandai dengan kemunculan berbagai inovasi seperti financial technology (fintech), mobile banking, dan e-wallet yang memungkinkan transaksi berlangsung secara cepat, efisien, dan lintas batas (1). Transformasi digital ini tidak hanya meningkatkan aksesibilitas layanan keuangan, tetapi juga mendorong inklusi finansial di berbagai negara berkembang (1). Menurut laporan World Bank (2025), persentase pengguna perbankan digital (*mobile money*) adalah 15% secara global dan sekitar 40% di wilayah Sub-Saharan Africa serta Amerika Latin & Karibia. Perubahan ini menunjukkan bahwa digitalisasi mulai memainkan peran strategis dalam transformasi sistem keuangan.

Di Negara Indonesia, digitalisasi perbankan berkembang pesat seiring meningkatnya penetrasi internet dan adopsi teknologi keuangan oleh masyarakat. Laporan Celios (2025) mencatat bahwa nilai transaksi SMS/mobile

banking mengalami pertumbuhan pesat hingga 2022, namun menurun tajam sejak 2023 akibat perubahan perilaku konsumen dan pergeseran menuju teknologi perbankan yang lebih modern. Digitalisasi ini membawa manfaat besar berupa efisiensi transaksi, kemudahan akses layanan, dan percepatan proses keuangan bagi pelaku ekonomi, termasuk Usaha Mikro, Kecil, dan Menengah (UMKM) (4). Selain itu, perbankan digital juga mendorong inklusi keuangan nasional dengan memperluas jangkauan layanan hingga ke daerah terpencil (4). Akan tetapi, peningkatan aktivitas digital di sektor perbankan juga memperbesar eksposur terhadap risiko keamanan dan potensi kejahatan siber yang semakin kompleks (5).

Kemajuan teknologi digital dalam sektor keuangan juga diiringi dengan meningkatnya ancaman siber yang berpotensi merugikan lembaga perbankan dan nasabah. Risiko yang sering terjadi mencakup pencurian data pribadi, serangan *phishing, malware, ransomware*, hingga praktik *social engineering* yang mengeksploitasi kelemahan pengguna (6). Menurut data Badan Siber dan Sandi Negara (BSSN), sektor keuangan merupakan sektor dengan tingkat serangan siber tertinggi, yaitu mencapai 361 juta kasus pada tahun 2023 (7). Salah satu contoh nyata adalah kasus kebocoran di BSI akibat serangan siber oleh LockBit 3.0 pada Mei 2023 yang menyebabkan layanan terhenti dan data nasabah bocor (8). Kondisi tersebut memperlihatkan bahwa sistem keamanan digital perbankan masih menghadapi tantangan serius dalam menjaga integritas data dan kepercayaan publik.

Serangan siber terhadap sistem perbankan tidak hanya menimbulkan kerugian finansial secara langsung, tetapi juga berdampak luas terhadap reputasi lembaga keuangan dan stabilitas ekonomi. Kerugian finansial akibat kejahatan siber di sektor perbankan Indonesia dapat mencapai skala besar (9). Selain itu, kejahatan ini juga menurunkan kepercayaan nasabah terhadap keamanan sistem digital sehingga berpotensi mengurangi loyalitas dan penggunaan layanan perbankan digital (9). Jika kondisi tersebut tidak diatasi maka kredibilitas sektor perbankan nasional dapat terancam dan menghambat agenda transformasi ekonomi digital Indonesia.

Untuk menghadapi tantangan tersebut, lembaga perbankan di Indonesia telah melakukan berbagai upaya penguatan sistem keamanan digital. Beberapa langkah strategis yang diterapkan mencakup penggunaan teknologi enkripsi tingkat lanjut, sistem *multi-factor authentication*, serta pemantauan transaksi berbasis kecerdasan buatan untuk mendeteksi aktivitas mencurigakan (5). Pemerintah juga telah mengeluarkan berbagai regulasi, seperti Peraturan OJK Nomor 38/POJK.03/2016 tentang Manajemen Risiko Teknologi Informasi, yang menjadi pedoman dalam menjaga keamanan sistem digital perbankan (5). Namun, efektivitas implementasi kebijakan ini masih menghadapi berbagai kendala, termasuk keterbatasan sumber daya manusia, perbedaan tingkat kesiapan teknologi antarbank, dan rendahnya kesadaran keamanan digital di kalangan pengguna (5). Hal ini menandakan bahwa upaya mitigasi yang ada belum sepenuhnya mampu menekan laju kejahatan siber di sektor keuangan.

Kasus dan penelitian terdahulu telah banyak menyoroti isu keamanan perbankan digital, seiring meningkatnya intensitas serangan siber dalam sektor keuangan global maupun nasional. Penelitian Khan et al. (2023) menekankan pentingnya penguatan sistem autentikasi berlapis, sementara Jayana, Rafael, & Rahman (2022) berfokus pada optimalisasi algoritma enkripsi untuk perlindungan data nasabah. Namun, kedua studi tersebut masih terbatas pada aspek teknis dan belum mengaitkannya secara menyeluruh dengan strategi mitigasi maupun efektivitas kebijakan. Oleh karena itu, penelitian ini hadir untuk mengisi kesenjangan tersebut dengan melakukan kajian literatur yang mengintegrasikan dimensi risiko, ancaman, dan strategi keamanan dalam sistem perbankan digital.

Berdasarkan uraian permasalahan di atas, penelitian ini diarahkan untuk mengkaji secara komprehensif berbagai risiko dan ancaman keamanan yang dihadapi oleh layanan perbankan daring di era digital. Fokus kajian ini tidak hanya mencakup identifikasi bentuk-bentuk serangan siber yang umum terjadi, tetapi juga menelaah faktor-faktor penyebab yang memperbesar kerentanan sistem perbankan terhadap ancaman tersebut. Selain itu, penelitian ini berupaya menganalisis berbagai strategi mitigasi yang telah diterapkan oleh lembaga keuangan dalam mencegah dan menanggulangi kebocoran data nasabah. Melalui pendekatan studi literatur, penelitian ini juga berusaha mengintegrasikan temuan-temuan terdahulu untuk menilai efektivitas kebijakan keamanan digital yang berlaku di Indonesia. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi landasan bagi pihak perbankan dan regulator dalam memperkuat sistem keamanan siber serta meningkatkan kepercayaan publik terhadap layanan perbankan online.

ISSN: 2776-8171
URL: https://proceeding.unpkediri.ac.id/index.php/senmea

METODE

Penelitian ini menggunakan metode studi literatur (literature review) dengan menelaah berbagai sumber ilmiah yang relevan, berupa jurnal nasional, serta publikasi resmi dari Otoritas Jasa Keuangan (OJK). Fokus utama penelitian ini adalah menganalisis berbagai kajian terdahulu yang membahas risiko, ancaman keamanan, dan strategi mitigasi pada layanan perbankan digital. Data yang diperoleh kemudian dianalisis secara kualitatif dengan mengelompokkan hasil temuan berdasarkan kategori risiko, jenis ancaman, serta bentuk upaya perlindungan yang telah diterapkan oleh lembaga keuangan.

Selanjutnya, dilakukan analisis komparatif untuk mengidentifikasi pola serangan siber dan penipuan keuangan, serta menilai efektivitas strategi keamanan yang telah dijalankan di berbagai konteks perbankan digital. Melalui pendekatan ini, penelitian diharapkan dapat memberikan gambaran menyeluruh mengenai tingkat kerentanan dan kesiapan sistem keamanan digital perbankan, sekaligus merumuskan rekomendasi strategis bagi peningkatan perlindungan data dan kepercayaan nasabah di masa mendatang.

Dengan demikian, penelitian ini diharapkan mampu memberikan kontribusi teoretis dan praktis dalam pengembangan kebijakan serta penerapan strategi keamanan perbankan digital di Indonesia. Hasil kajian ini juga dapat menjadi acuan bagi lembaga keuangan dan regulator dalam memperkuat sistem pengawasan, meningkatkan efektivitas mitigasi risiko siber, serta membangun ekosistem perbankan digital yang aman, adaptif, dan berkelanjutan di tengah pesatnya perkembangan teknologi informasi.

HASIL PENELITIAN DAN PEMBAHASAN

Keamanan Layanan Perbankan Online

Digitalisasi perbankan tidak hanya bergantung pada sistem teknologi informasi yang digunakan, tetapi juga pada kesiapan sumber daya manusia, kebijakan internal, dan kesadaran pengguna. Keamanan layanan perbankan daring merupakan hasil dari interaksi berbagai faktor yang saling berkaitan. Jika salah satu faktor tidak berjalan optimal, maka celah keamanan dapat muncul dan mengancam keberlangsungan sistem secara keseluruhan. Oleh karena itu, memahami faktor-faktor yang memengaruhi keamanan menjadi langkah penting dalam merumuskan strategi perlindungan yang efektif.

Berdasarkan hasil kajian pustaka dan analisis terhadap berbagai laporan keamanan siber di sektor keuangan, terdapat beberapa faktor utama yang berpengaruh terhadap tingkat keamanan layanan perbankan daring di Indonesia. Faktor-faktor tersebut tidak hanya mencakup aspek teknis, tetapi juga sosial dan regulatif, yang secara kolektif menentukan sejauh mana sistem perbankan dapat menghadapi risiko dan ancaman digital.

1. Faktor Teknologi

Perkembangan infrastruktur teknologi informasi menjadi fondasi utama bagi keamanan sistem perbankan digital. Ketergantungan terhadap jaringan internet dan penggunaan sistem cloud menjadikan bank rentan terhadap serangan siber, terutama apabila sistem tidak diperbarui secara berkala. Ketidakterpaduan sistem keamanan antarplatform seperti mobile banking dan internet banking juga dapat menciptakan celah yang mudah dieksploitasi.

Faktor ini dapat diperkuat melalui implementasi sistem keamanan berlapis seperti enkripsi data, autentikasi multifaktor, dan deteksi intrusi otomatis. Dengan penerapan teknologi yang lebih mutakhir, bank dapat memperkecil potensi gangguan operasional akibat serangan eksternal dan menjaga stabilitas transaksi secara real-time.

2. Faktor Sumber Daya Manusia (SDM)

Kemampuan dan kesadaran pegawai bank terhadap praktik keamanan siber sangat berpengaruh terhadap perlindungan data nasabah. Banyak kasus kebocoran data yang justru bermula dari kelalaian internal, seperti penggunaan kata sandi yang lemah atau tidak mengikuti protokol keamanan. Kurangnya pelatihan keamanan siber membuat sebagian pegawai belum mampu mendeteksi aktivitas mencurigakan dalam sistem. Untuk mengatasi hal tersebut, lembaga keuangan perlu menerapkan program peningkatan kapasitas SDM secara berkelanjutan. Pelatihan keamanan digital, simulasi serangan siber, dan audit internal berkala dapat meningkatkan kewaspadaan pegawai terhadap potensi ancaman. Dengan SDM yang kompeten, bank dapat memperkuat garis pertahanan pertama dalam sistem keamanannya.

ISSN: 2776-8171
URL: https://proceeding.unpkediri.ac.id/index.php/senmea

3. Faktor Regulasi dan Kepatuhan

Kebijakan pemerintah dan peraturan otoritas keuangan seperti Otoritas Jasa Keuangan (OJK) serta Bank Indonesia (BI) memiliki peran signifikan dalam menjaga keamanan sistem perbankan. Regulasi mengenai perlindungan data pribadi, keamanan transaksi, serta tata kelola risiko menjadi dasar bagi setiap lembaga keuangan dalam menjalankan operasional digital. Kelemahan dalam implementasi atau ketidakpatuhan terhadap regulasi dapat membuka peluang bagi terjadinya pelanggaran keamanan. Penerapan kepatuhan terhadap regulasi perlu dilakukan secara konsisten dan diintegrasikan dengan standar internasional, seperti ISO 27001 tentang keamanan informasi. Dengan pengawasan yang kuat dari otoritas, bank dapat memastikan bahwa sistemnya berjalan sesuai prinsip keamanan, transparansi, dan akuntabilitas.

4. Faktor Kesadaran Pengguna (*User Awareness*)

Nasabah memegang peranan penting dalam menjaga keamanan akun dan data pribadi mereka. Rendahnya kesadaran terhadap modus kejahatan digital seperti phishing, tautan palsu, dan aplikasi tidak resmi menjadi salah satu penyebab utama kebocoran data nasabah. Banyak pengguna masih mudah tergoda oleh pesan berhadiah atau tautan dari sumber tidak dikenal tanpa memverifikasi keasliannya.

Peningkatan literasi digital masyarakat menjadi langkah kunci dalam memperkuat sistem keamanan perbankan daring. Melalui edukasi publik, kampanye keamanan digital, dan pemberitahuan resmi dari pihak bank, pengguna dapat lebih waspada terhadap potensi kejahatan siber. Dengan pengguna yang lebih cerdas secara digital, risiko kebocoran data akibat kelalaian pribadi dapat diminimalkan secara signifikan.

Keseluruhan faktor di atas saling berinteraksi dan membentuk ekosistem keamanan digital yang kompleks dalam layanan perbankan daring. Ketidakseimbangan di salah satu aspek, seperti lemahnya kesadaran pengguna atau kurangnya pembaruan sistem, dapat membuka celah bagi risiko dan ancaman siber. Oleh karena itu, keamanan tidak dapat hanya dipandang sebagai tanggung jawab bagian teknologi informasi semata, melainkan sebagai komitmen kolektif antara lembaga keuangan, regulator, penyedia layanan jaringan, dan nasabah.

Pemahaman terhadap faktor-faktor tersebut memberikan landasan bagi identifikasi risiko yang lebih mendalam. Dengan mengenali sumber potensial kelemahan dari setiap aspek, bank dapat merancang strategi mitigasi yang lebih terarah dan efektif. Dalam konteks inilah, penting untuk menelaah berbagai bentuk risiko yang secara nyata dihadapi oleh layanan perbankan daring. Berikut adalah bentuk risiko yang dihadapi oleh layanan perbankan daring (12):

1. Risiko Operasional

Risiko operasional muncul ketika terjadi gangguan dalam sistem perbankan akibat kesalahan manusia (*human error*), ketidaksempurnaan prosedur kerja, maupun kerusakan perangkat teknologi. Cara kerja risiko ini biasanya diawali dari ketidaksesuaian prosedur standar operasional dengan praktik di lapangan. Misalnya, kesalahan input data oleh petugas *back office* atau keterlambatan dalam memperbarui server dapat menimbulkan ketidaksesuaian saldo nasabah. Misalnya, kasus hilangnya dana nasabah akibat SIM *swap fraud* pada transaksi *mobile banking* (13). Insiden seperti ini menunjukkan bahwa gangguan operasional kecil dapat memicu efek domino yang besar, terutama karena sistem transaksi perbankan saling terhubung secara real-time. Risiko ini semakin besar bila sistem pemantauan tidak berjalan otomatis dan masih bergantung pada intervensi manual.

2. Risiko Teknologi

Risiko teknologi terjadi ketika sistem digital bank memiliki celah keamanan (*vulnerability*) yang dapat dimanfaatkan oleh peretas. Secara teknis, serangan dapat dilakukan dengan cara mengeksploitasi bug dalam aplikasi, injeksi kode berbahaya (*malicious code*), atau pemindaian port jaringan untuk menemukan titik masuk ke server bank. Serangan semacam ini bisa berlangsung tanpa terdeteksi selama berbulan-bulan sebelum menimbulkan kerusakan nyata. Contohnya, peristiwa ransomware yang terjadi pada tahun 2023 di PT Bank Syariah Indonesia merupakan bentuk serangan malware yang menyebabkan layanan peribankan tidak dapat diakses selama empat hari (14). Proses ini umumnya diawali dengan pengiriman file berbahaya ke sistem bank, kemudian file tersebut menanamkan script untuk mengakses data sensitif atau mengambil kendali sistem dari jarak jauh. Karena itu, patch management dan enkripsi data menjadi aspek krusial dalam mitigasi risiko teknologi.

3. Risiko Privasi Data

Risiko privasi data muncul karena lemahnya sistem perlindungan informasi pribadi nasabah, baik di sisi server maupun pengguna. Cara kerja ancaman ini biasanya melalui teknik *phishing, keylogging*, atau kebocoran data akibat sistem yang tidak terenkripsi dengan baik. Misalnya, pelaku kejahatan mengirim tautan palsu melalui email atau pesan singkat yang meniru tampilan bank resmi. Setelah nasabah mengklik tautan tersebut dan memasukkan data pribadinya, informasi seperti *username, password*, dan nomor OTP otomatis tersimpan di server pelaku. Data yang dicuri kemudian dapat dijual di pasar gelap (*dark web*) atau digunakan untuk transaksi ilegal. Misalnya, pada Mei 2022 dan Mei 2023 terjadi kasus phishing di Bank BRI yang menyebabkan dua nasabah mengalami kerugian besar hingga miliaran rupiah akibat tautan penipuan melalui pesan WhatsApp yang digunakan pelaku untuk mengakses dan menguras rekening korban (15). Risiko ini memperlihatkan pentingnya keamanan berlapis (*multi-factor authentication*) dan edukasi keamanan digital bagi nasabah.

4. Risiko Reputasi

Risiko reputasi merupakan konsekuensi tidak langsung dari insiden keamanan yang berdampak pada persepsi publik terhadap suatu lembaga keuangan. Secara mekanis, risiko ini bekerja melalui penyebaran informasi negatif yang cepat di media sosial dan pemberitaan daring. Misalnya, kasus peretasan yang menimpa Bank Syariah Indonesia merupakan bentuk risiko reputasi, karena para peretas memberikan tenggat waktu 72 jam dan mengancam akan merusak citra serta kepercayaan publik terhadap bank apabila tuntutan mereka tidak dipenuhi (16). Dalam dunia perbankan digital, kepercayaan merupakan aset utama ketika reputasi terganggu, nasabah cenderung memindahkan dananya ke lembaga lain yang dianggap lebih aman. Maka dari itu, pengelolaan komunikasi krisis dan transparansi informasi menjadi strategi penting untuk memulihkan reputasi pasca-insiden.

Selain risiko internal, terdapat pula ancaman eksternal dari kejahatan siber yang secara langsung menargetkan pengguna maupun infrastruktur bank. Berikut penjelasan tentang bagaimana ancaman tersebut bekerja:

1. Phishing

Phishing bekerja dengan cara menipu korban agar memberikan informasi sensitif melalui situs palsu atau pesan tiruan yang seolah-olah berasal dari bank resmi. Pelaku biasanya mengirim tautan dengan domain mirip situs bank, seperti “bca-id.co” atau “loginbri.net”. Saat korban mengisi data login, sistem palsu itu otomatis menyimpan data kredensial yang kemudian digunakan untuk mengakses rekening korban. Kasus phishing terhadap pengguna Bank BRI pada 2022 dan 2023 menjadi contoh nyata metode ini (15).

2. *Malware* dan *Ransomware*

Malware masuk ke perangkat korban melalui file atau aplikasi berbahaya. Begitu terpasang, malware dapat mencuri data login atau mengenkripsi seluruh file sistem perbankan (*ransomware*), lalu meminta tebusan agar data dikembalikan. Studi oleh Sulubara (2024) menunjukkan bahwa dalam lima tahun terakhir terjadi peningkatan frekuensi serangan ransomware hingga mencapai 300% karena banyak aktivitas perbankan beralih ke sistem daring tanpa persiapan keamanan memadai.

3. Social Engineering

Ancaman ini tidak bergantung pada celah teknologi, tetapi pada manipulasi psikologis. Pelaku berpura-pura menjadi petugas bank, meminta data OTP dengan alasan verifikasi transaksi atau peningkatan limit. Cara kerja *social engineering* menargetkan emosi korban, seperti rasa panik, takut, atau keinginan cepat menyelesaikan masalah (18).

4. *Data Breach* (Pelanggaran Data)

Terjadi ketika pihak tidak berwenang berhasil menembus sistem penyimpanan data bank dan mengakses informasi ribuan akun nasabah. Biasanya hal ini dilakukan melalui eksploitasi celah keamanan di server atau penggunaan akun internal yang disusupi. Menurut Fadhlina et al. (2024), kejahatan siber dapat dilakukan lintas batas negara karena pelaku dapat mengakses sistem dan data dari jarak jauh melalui jaringan internet, sehingga penanganannya memerlukan kerja sama internasional dan regulasi yang terpadu.

ISSN: 2776-8171
URL: https://proceeding.unpkediri.ac.id/index.php/senmea

Berdasarkan hasil telaah berbagai literatur dan laporan keamanan digital, risiko serta ancaman keamanan pada layanan perbankan daring menimbulkan sejumlah dampak signifikan bagi lembaga keuangan maupun nasabah. Dampak tersebut tidak hanya bersifat finansial, tetapi juga mencakup aspek psikologis, hukum, dan sistemik sebagai berikut:

1. Kerugian Finansial

   Dampak paling nyata dari serangan siber adalah hilangnya dana secara langsung akibat penipuan atau pencurian digital. Contohnya, kasus phishing yang menimpa nasabah BRI pada 2022 dan 2023 menyebabkan kerugian individu hingga puluhan juta rupiah. Selain itu, bank juga menanggung biaya pemulihan sistem dan kompensasi kepada korban.

2. Penurunan Kepercayaan Publik

   Keamanan menjadi faktor utama dalam mempertahankan loyalitas nasabah. Ketika terjadi insiden kebocoran data atau penipuan digital, kepercayaan masyarakat terhadap keamanan layanan bank digital menurun drastis.

3. Risiko Hukum dan Kepatuhan Regulasi

   Lembaga keuangan memiliki kewajiban untuk menjaga kerahasiaan data nasabah sesuai dengan Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) dan peraturan OJK. Pelanggaran terhadap regulasi tersebut dapat berakibat pada sanksi hukum dan administratif.

4. Kerusakan Reputasi dan Citra Lembaga Keuangan

   Serangan siber yang viral di media sosial dapat menimbulkan krisis kepercayaan publik yang sulit dipulihkan. Misalnya, kasus peretasan yang menimpa Bank Syariah Indonesia menimbulkan gelombang kritik di media digital dan menurunkan persepsi keamanan bank terkait.

5. Gangguan Operasional dan Stabilitas Sistem

   Serangan *ransomware,* kesalahan manusia (*human error*), ketidaksempurnaan prosedur kerja, maupun kerusakan perangkat teknologi dapat menghambat operasional bank secara menyeluruh. Gangguan semacam ini tidak hanya memperlambat transaksi, tetapi juga dapat memengaruhi stabilitas sistem pembayaran nasional jika terjadi dalam skala besar.

Strategi Keamanan Siber dalam Layanan Perbankan Daring dan Efektivitasnya

Seiring meningkatnya risiko dan ancaman siber di sektor perbankan, berbagai strategi telah diterapkan oleh lembaga keuangan dan otoritas pengawas di Indonesia untuk memperkuat sistem keamanan digital. Strategi-strategi ini mencakup pendekatan teknis, manajerial, maupun edukatif. Masing-masing memiliki keunggulan dan keterbatasan tersendiri dalam memastikan keamanan transaksi perbankan daring.

1. Implementasi Sistem Keamanan Berlapis (*Multi-Factor Authentication*)

   Salah satu strategi utama yang telah diterapkan adalah penggunaan sistem keamanan berlapis atau *multi-factor authentication (MFA*). Sistem ini bekerja dengan menggabungkan dua atau lebih faktor otentikasi, seperti kombinasi *password,* kode OTP (*One-Time Password*), biometrik wajah atau sidik jari, dan perangkat yang terdaftar. Dengan demikian, walaupun data login pengguna diketahui pihak lain, transaksi tetap tidak dapat dilakukan tanpa otorisasi tambahan.

   Bank-bank besar di Indonesia seperti BCA, BNI, dan Mandiri telah mengadopsi sistem ini dalam aplikasi mobile banking dan internet banking-nya. Secara teknis, MFA memecah proses login menjadi dua tahap: verifikasi kredensial dan validasi perangkat. Data otorisasi juga dikirim dalam format terenkripsi agar tidak bisa disadap. Menurut Firdaus & Ilham (2025), penerapan MFA berhasil mencegah kasus pencurian identitas. Namun, efektivitas sistem ini masih terbatas bila pengguna kurang berhati-hati, misalnya tetap memberikan kode OTP kepada pihak lain akibat rekayasa sosial (*social engineering*).

2. Penguatan Enkripsi dan Pembaruan Sistem Keamanan Jaringan

   Langkah berikutnya adalah penerapan teknologi enkripsi data dan pembaruan sistem keamanan (patch management) secara berkala. Enkripsi berfungsi mengubah data sensitif menjadi format acak sehingga tidak dapat dibaca pihak luar. Protokol keamanan seperti *Transport Layer Security* (TLS) dan *Secure Socket Layer* (SSL) kini

menjadi standar wajib untuk seluruh transaksi perbankan daring di Indonesia. Selain itu, bank diwajibkan melakukan pembaruan sistem (*security patching*) setiap kali vendor mengeluarkan versi terbaru untuk menutup celah kerentanan.

Menurut Azizah et al. (2024), penerapan pembaruan sistem otomatis dapat menurunkan serangan *cybercrime* pada perbankan digital dan FinTech. Namun, kendala utama terletak pada kecepatan pembaruan: beberapa lembaga keuangan masih tertinggal dalam melakukan update karena keterbatasan sumber daya TI dan kompleksitas sistem lama (*legacy system*). Hal ini menyebabkan beberapa celah keamanan tetap terbuka lebih lama dari yang seharusnya.

3. Penerapan Sistem Deteksi Dini dan *Monitoring Real-Time*

Bank-bank kini juga menggunakan sistem *Security Operation Center* (SOC) yang beroperasi 24 jam untuk memantau aktivitas jaringan secara real-time. SOC bekerja dengan menganalisis pola lalu lintas data dan mendeteksi anomali yang berpotensi menjadi ancaman siber. Misalnya, jika ada login dari lokasi tidak wajar atau upaya akses berulang dari perangkat yang berbeda, sistem otomatis memblokir aktivitas tersebut.

Efektivitas strategi ini cukup tinggi. Menurut Laksana & Mulyani (2024), lembaga keuangan yang memiliki sistem deteksi dini mampu mengurangi waktu respons terhadap insiden siber dari rata-rata 280 hari menjadi hanya 75 hari. Di Indonesia, Bank BRI telah menerapkan teknologi berlapis dan protokol keamanan mutakhir yang untuk meneka *data breach* (23). Meskipun demikian, sistem ini SDM dengan keahlian khusus di bidang analitik keamanan digital untuk menciptakan system keamana yang efektif.

4. Penguatan Regulasi dan Pengawasan oleh Otoritas Keuangan

Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) berperan besar dalam menetapkan regulasi keamanan perbankan digital. Melalui POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, lembaga perbankan diwajibkan melakukan risk assessment terhadap teknologi yang digunakan dan menyampaikan laporan keamanan siber secara berkala. Regulasi ini juga mewajibkan audit independen untuk memastikan kepatuhan terhadap standar keamanan.

Efektivitas kebijakan ini cukup signifikan karena memaksa lembaga perbankan memperkuat tata kelola keamanan digital. Tingkat kepatuhan perbankan terhadap standar keamanan informasi meningkat setelah regulasi tersebut diberlakukan. Namun, implementasinya masih belum merata antar lembaga keuangan digital pada peraturan yang berlaku (24).

5. Edukasi dan Literasi Keamanan Digital bagi Nasabah

Selain upaya teknis, aspek edukasi juga menjadi strategi penting dalam mencegah kejahatan siber. Bank Indonesia dan OJK secara rutin menyelenggarakan kampanye "Waspada Modus Penipuan Digital" melalui media sosial, iklan televisi, dan kerja sama dengan influencer. Tujuannya meningkatkan kesadaran masyarakat agar tidak mudah membagikan data pribadi, OTP, atau PIN kepada pihak lain.

Menurut Suwiknyo (2021), nasabah yang pernah menjadi korban *fraud internet banking* tidak tahu ada serangan karena pelaku mengaku sebagai pergawai bank. Oleh karena itu, kampanye edukasi digencarkan, untuk menurun korban *fraud internet banking* di kemudia hari. Namun, upaya ini harus dilakukan secara berkelanjutan karena pola kejahatan siber terus berubah dan semakin kompleks.

6. Kolaborasi dan Pertukaran Informasi Antar Lembaga

Upaya penguatan keamanan digital juga dilakukan melalui kolaborasi antarbank, lembaga keamanan nasional, dan penyedia jasa teknologi. Program seperti *Financial Services Information Sharing and Analysis Center* (FS-ISAC) memungkinkan bank-bank berbagi data terkait ancaman terbaru dan teknik pertahanan yang efektif. Di Indonesia, BSSN bersama OJK dan BI membentuk forum "Komite Keamanan Siber Sektor Keuangan" yang bertujuan mempercepat respons terhadap insiden siber lintas lembaga. Secara efektivitas, kolaborasi ini terbukti memperpendek waktu mitigasi serangan. Namun, tantangan terbesar terletak pada koordinasi antarinstansi dan kesediaan lembaga berbagi informasi sensitif, karena isu reputasi dan kerahasiaan data masih menjadi hambatan utama (26).

ISSN: 2776-8171
URL: https://proceeding.unpkediri.ac.id/index.php/senmea

Dari berbagai strategi tersebut, dapat disimpulkan bahwa efektivitasnya sangat bergantung pada sinkronisasi antara sistem keamanan teknologi dan kesiapan manusia. Upaya teknis seperti enkripsi dan MFA terbukti menurunkan frekuensi serangan langsung, sementara pendekatan edukatif dan regulatif meningkatkan kesadaran dan kepatuhan. Namun, ancaman siber terus berevolusi, artinya, tidak ada sistem yang benar-benar kebal terhadap risiko. Oleh karena itu, pendekatan keamanan harus bersifat adaptif dan berkelanjutan, dengan penekanan pada peningkatan kapasitas SDM, respons cepat terhadap insiden, serta kolaborasi lintas sektor.

Rekomendasi untuk Meningkatkan Keamanan Layanan Perbankan *Online*

Meskipun berbagai strategi pengamanan digital telah diterapkan oleh lembaga keuangan, seperti penerapan multi-factor authentication, enkripsi data, serta peningkatan literasi digital bagi nasabah, namun efektivitasnya masih terbatas akibat lemahnya pengawasan dan inkonsistensi pelaksanaan di lapangan. Kondisi ini menunjukkan perlunya pendekatan yang lebih menyeluruh dan berkelanjutan untuk memastikan keamanan sistem perbankan digital tidak hanya bergantung pada teknologi semata, tetapi juga pada tata kelola, regulasi, dan partisipasi aktif seluruh pemangku kepentingan. Oleh karena itu, dibutuhkan strategi penguatan yang terintegrasi mencakup pengawasan sistem teknologi keamanan digital yang lebih adaptif terhadap ancaman baru, pembenahan kebijakan serta tata kelola keamanan siber agar lebih konsisten dan transparan, peningkatan literasi serta kesadaran keamanan digital bagi karyawan dan nasabah, serta dorongan terhadap riset dan inovasi di bidang keamanan siber. Sinergi antara lembaga keuangan, regulator, pemerintah, dan masyarakat menjadi kunci untuk membangun sistem pertahanan digital yang tangguh dan responsif terhadap perkembangan kejahatan siber yang semakin kompleks. Dengan demikian, rekomendasi berikut disusun untuk memberikan arah strategis dalam memperkuat keamanan dan kepercayaan publik terhadap layanan perbankan digital di Indonesia.

1. Penguatan Sistem Teknologi Keamanan Digital

Lembaga keuangan perlu secara aktif memperkuat infrastruktur digital melalui penerapan teknologi keamanan mutakhir seperti enkripsi end-to-end, autentikasi biometrik, serta sistem pemantauan transaksi berbasis kecerdasan buatan (AI). Penggunaan machine learning memungkinkan bank mendeteksi aktivitas mencurigakan secara real-time, sehingga potensi penipuan dapat diidentifikasi sebelum menimbulkan kerugian besar. Selain itu, sistem keamanan wajib diperbarui secara berkala melalui mekanisme patch management untuk menutup celah yang mungkin dimanfaatkan oleh peretas. Langkah ini harus diintegrasikan dengan network monitoring system yang mampu mengidentifikasi pola anomali sejak dini. Dengan demikian, teknologi berperan sebagai lapisan pertahanan pertama dalam menjaga keamanan transaksi perbankan daring.

Bank juga perlu mengimplementasikan sistem keamanan adaptif yang mampu merespons perubahan pola ancaman secara dinamis. Integrasi teknologi blockchain dapat meningkatkan transparansi dan keandalan pencatatan transaksi, sehingga mengurangi potensi data tampering. Selain itu, pengujian penetrasi (penetration testing) harus dilakukan secara berkala untuk menilai ketahanan sistem terhadap serangan siber terkini. Tim keamanan siber internal harus bekerja sama dengan lembaga eksternal bersertifikat untuk memastikan standar keamanan selalu sesuai dengan pedoman nasional maupun internasional. Dengan menerapkan langkah-langkah aktif tersebut, lembaga perbankan dapat menciptakan sistem digital yang tangguh, aman, dan berorientasi pada perlindungan data nasabah.

2. Penguatan Kebijakan dan Tata Kelola Keamanan Siber

Regulator seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) perlu secara aktif memperkuat implementasi kebijakan risk-based supervision terhadap layanan digital perbankan. Pengawasan berbasis risiko ini harus disertai dengan kewajiban audit keamanan siber secara periodik untuk setiap lembaga keuangan yang mengoperasikan layanan daring. Bank juga wajib mengembangkan kerangka manajemen risiko TI yang mencakup prosedur incident response, sistem pelaporan insiden yang transparan, serta protokol mitigasi darurat untuk mencegah eskalasi serangan. Dengan pendekatan ini, tata kelola keamanan tidak hanya menjadi tanggung jawab teknis, tetapi juga bagian integral dari manajemen strategis bank. Hal tersebut akan meningkatkan akuntabilitas dan kesiapsiagaan lembaga keuangan dalam menghadapi ancaman siber.

Pemerintah juga perlu mendorong kolaborasi lintas lembaga untuk membentuk pusat koordinasi keamanan siber antarbank. Melalui mekanisme ini, setiap bank dapat saling bertukar informasi tentang pola serangan, tren kejahatan siber, dan langkah mitigasi yang telah terbukti efektif. Regulator juga dapat berperan sebagai fasilitator dalam menyediakan pedoman teknis dan sistem peringatan dini (early warning system) terhadap ancaman yang

bersifat lintas sektor. Implementasi kebijakan yang responsif dan adaptif akan mendorong terciptanya ekosistem perbankan digital yang aman dan terpercaya. Dengan demikian, sinergi antara regulasi yang kuat dan tata kelola yang transparan menjadi kunci untuk memperkuat pertahanan keamanan digital nasional.

3. Peningkatan Literasi dan Kesadaran Keamanan Digital

Peningkatan literasi digital dan kesadaran keamanan (*security awareness*) merupakan langkah strategis untuk memperkuat perlindungan dari sisi manusia. Bank harus secara aktif mengadakan pelatihan berkala bagi karyawan tentang tata cara mengenali potensi ancaman seperti phishing, social engineering, dan malware injection. Edukasi internal ini membantu pegawai mengenali tanda-tanda anomali dalam sistem dan menindaklanjutinya dengan cepat. Di sisi lain, kampanye edukatif kepada nasabah perlu diperluas melalui kanal resmi seperti aplikasi perbankan, media sosial, dan layanan pelanggan. Langkah ini penting untuk memastikan nasabah memahami cara menjaga kerahasiaan data pribadi serta tidak mudah tertipu oleh pesan atau situs palsu.

Bank juga dapat mengembangkan program literasi siber nasional bekerja sama dengan universitas, komunitas digital, dan lembaga pemerintah. Program ini berfungsi meningkatkan kesadaran publik terhadap pentingnya keamanan informasi dalam transaksi keuangan daring. Bank juga dapat menggunakan pendekatan berbasis perilaku, seperti gamifikasi atau simulasi phishing, untuk melatih pengguna dalam menghadapi ancaman digital nyata. Dengan menumbuhkan budaya keamanan yang kuat di antara pengguna dan pegawai, risiko kesalahan manusia dapat diminimalkan. Upaya proaktif ini menjadikan literasi digital bukan sekadar edukasi formal, tetapi bagian dari perilaku finansial modern yang berkesinambungan.

4. Penguatan Riset, Inovasi, dan Kolaborasi Keamanan Siber

Lembaga keuangan perlu berinvestasi dalam riset dan inovasi keamanan siber untuk menghadapi ancaman yang terus berevolusi. Kolaborasi dengan universitas, pusat riset teknologi, dan perusahaan keamanan digital dapat mempercepat pengembangan solusi yang lebih efektif. Penelitian mengenai *cyber threat intelligence* dan *behavioral analytics* perlu diperluas guna memahami pola serangan yang kompleks dan dinamis di sektor perbankan. Selain itu, hasil riset tersebut dapat dijadikan dasar pengembangan algoritma deteksi ancaman yang lebih akurat dan adaptif terhadap perubahan teknologi. Pendekatan berbasis riset ini memastikan bahwa sistem keamanan bank selalu berada selangkah lebih maju dari potensi pelaku kejahatan siber.

Bank juga harus secara aktif mendukung ekosistem inovasi dengan membuka ruang kolaborasi antara sektor publik dan swasta. Pembentukan *Cybersecurity Innovation Hub* misalnya, dapat menjadi wadah untuk berbagi data, hasil penelitian, serta solusi teknologi yang dapat diimplementasikan lintas lembaga. Selain itu, kolaborasi internasional dengan lembaga keuangan global dapat memperkaya strategi pertahanan digital melalui pertukaran keahlian dan teknologi keamanan terbaru. Dengan menjadikan riset dan inovasi sebagai bagian inti dari strategi keamanan, lembaga keuangan tidak hanya bereaksi terhadap ancaman, tetapi mampu beradaptasi dan berinovasi untuk mengantisipasinya. Pendekatan ini akan memperkuat daya saing sekaligus ketahanan sistem keuangan nasional di era digital.

KESIMPULAN

Keamanan digital tidak dapat bergantung pada satu elemen tunggal, melainkan merupakan hasil interaksi kompleks antara lembaga keuangan, regulator, penyedia layanan teknologi, dan pengguna. Penelitian ini menunjukkan bahwa ancaman seperti phishing, malware, ransomware, serta kebocoran data pribadi berdampak signifikan terhadap stabilitas sistem perbankan, kepercayaan publik, dan reputasi lembaga keuangan. Upaya mitigasi melalui penerapan multi-factor authentication, penguatan enkripsi, serta peningkatan literasi digital masih belum efektif sepenuhnya karena lemahnya pengawasan, inkonsistensi kebijakan, dan kesenjangan kemampuan teknologi di lapangan. Oleh karena itu, dibutuhkan strategi komprehensif yang mencakup penguatan regulasi dan tata kelola siber, peningkatan pengawasan terhadap sistem keamanan digital, serta kolaborasi riset dan inovasi antar lembaga untuk memperkuat ketahanan perbankan digital. Selain itu, peningkatan literasi dan kesadaran keamanan di tingkat individu perlu terus dilakukan guna membangun budaya keamanan yang berkelanjutan dan adaptif terhadap perkembangan ancaman siber di masa depan.

Kontribusi penelitian ini terletak pada penyajian pendekatan komprehensif terhadap keamanan perbankan daring yang tidak hanya menyoroti aspek teknis, tetapi juga memperhatikan dimensi manusia, regulatif, dan kelembagaan yang saling berkaitan dalam menjaga integritas sistem keuangan digital. Penelitian ini memberikan

pandangan holistik bahwa keberhasilan perlindungan data finansial tidak dapat dicapai hanya melalui peningkatan teknologi keamanan, melainkan juga harus diimbangi dengan kesiapan sumber daya manusia, tata kelola organisasi, serta kepatuhan terhadap regulasi yang berlaku. Kebaruan penelitian ini terletak pada penegasan pentingnya sinkronisasi antara sistem keamanan digital dan kompetensi SDM sebagai fondasi utama dalam membangun ekosistem perbankan yang tangguh dan adaptif terhadap dinamika ancaman siber yang terus berkembang. Temuan penelitian ini diharapkan dapat menjadi dasar bagi pengembangan kebijakan keamanan siber yang lebih adaptif, terukur, dan berorientasi pada kolaborasi lintas lembaga, baik antara pemerintah, industri perbankan, maupun penyedia teknologi. Selain itu, hasil penelitian ini juga dapat dijadikan acuan bagi lembaga keuangan dalam memperkuat tata kelola risiko digital yang terintegrasi, meningkatkan kapasitas SDM melalui pelatihan berkelanjutan, serta memperluas kolaborasi strategis dalam menciptakan sistem keamanan digital yang berkelanjutan dan terpercaya di era transformasi digital perbankan.

Keterbatasan penelitian ini terletak pada sifatnya yang masih bersandar pada kajian literatur dan laporan sekunder, sehingga belum menggambarkan kondisi empiris di setiap lembaga keuangan secara menyeluruh. Penelitian lanjutan disarankan untuk dilakukan dengan pendekatan studi kasus atau survei lapangan terhadap bank-bank di Indonesia guna memperoleh data primer mengenai efektivitas implementasi strategi keamanan siber. Dengan demikian, hasil penelitian selanjutnya diharapkan mampu memberikan rekomendasi yang lebih aplikatif bagi peningkatan ketahanan digital sektor perbankan nasional.

DAFTAR PUSTAKA

[1] Rihani S, Shodiq J, Ghalib N, Astuti RP. Inovasi Digital dan Kebijakan Bank Sentral dalam Era Teknologi. J Penelit Nusant. 2025;1(5):276–80.
[2] World Bank. The Global Findex Database 2025. 2025.
[3] Huda N, Ayu D, Septyarini R. Outlook Ekonomi Digital Outlook Ekonomi Digital 2025. 2025.
[4] Karim A, Sirait E, Dwihandoko TH, Mustajirin J, Patty JP. Peran Financial Technology Terhadap Pembiayaan UMKM Di Indonesia. Edunomika. 2024;08(02):1–15.
[5] Muhtadien AZ, Aziz A, Hermawan H. Analisis Penguatan Digitalisasi Perbankan Melalui Peningkatan Perlindungan Dana Bank Konsumen Oleh OJK. J Ekon Akuntansi, dan Perpajak. 2024;1(3):213–23.
[6] Ali A, Fitri AO. Keamanan Perbankan di Era Digital : Tantangan dan Solusinya. J Bersama Ilmu Ekon. 2025;1(2):154–65.
[7] Otoritas Jasa Keuangan. Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK). 2025.
[8] Sugiarto AJ, Lie G, Putra MRS. Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia). JALAKOTEK J Account Law Commun Technol. 2025;2(1):107–14.
[9] Isnugraheny RF, Megawati ZE, Susilawati S. Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. Media Huk Indones. 2024;2(4):258–64.
[10] Khan HU, Sohail M, Nazir S, Hussain T, Shah B, Ali F. Role of authentication factors in Fin - tech mobile transaction security. J Big Data [Internet]. 2023; Available from: https://doi.org/10.1186/s40537-023-00807-3
[11] Jayana MA, Rafael D, Rahman AA. Implementasi Pengamanan Data Pengarsipan Studi Kasus Pada Bank BJB KCP Pasteur Bandung. In: Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik (SoBAT) ke-4. 2022. p. 184–95.
[12] Indrawati A. Analisis Yuridis terhadap Hak Milik Atas Tanah di Kawasan Perkotaan: Antara Regulasi dan Realitas Sosial. Arus J Sos dan Hum. 2024;4(3):2392–8.
[13] Assyifa A, Firmansyah A, Supriatna R. Tanggung Jawab Bank terhadap Dana Nasabah yang Mengalami SIM Swap Fraud Atas Transaksi Mobile Banking Ditinjau dari POJK Nomor 12 / POJK . 03 / 2018 Tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum. In: Bandung Conference Series: Law Studies. 2022. p. 829–34.
[14] Larasati NM, Firdaus R. Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan. Merkurius J Ris Sist Inf dan Tek Inform. 2024;2(4):102–9.
[15] Putri RAT, Sugiyono H. Tanggung Jawab Bank Terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk). J Interpret Huk.

2023;4(3):682–90.
[16] Ghozali M, Liana N, Afra C, Siregar Z. Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI). CENDEKIA J Hukum, Sos Hum. 2024;2(4):797–809.
[17] Sulubara SM. Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? Eksekusi J Ilmu Huk dan Adm Negara. 2024;2(4):426–34.
[18] Efendi NA, Harahap MI, Syahbudi M. Pengaruh Social Engineering Dan Cyber Crime Terhadap Persepsi Keamanan Pada Aplikasi BSI Mobile. J Manaj Terap dan Keuang Vol. 2025;14(03):1237–50.
[19] Fadhlina A, Resentia R, Rukhsal SF, Hadiwibowo H, Azzahra AS. Perlindungan Data Pribadi Nasabah dalam Transaksi Central Bank Digital Currency (CBDC) dalam Rupiah Digital. UNES LAW RREVIEW. 2024;7(1):307–17.
[20] Firdaus MA, Ilham M. Volume 1 Nomor 3 (2025) Pages 333 – 342 JHN : Jurnal Hukum Nusantara Strategi Pencegahan Kebocoran Rahasia Dagang dalam Industri Teknologi. JHN J Huk Nusant. 2025;1(3):333–42.
[21] Azizah S, Ula ZN, Mutiara D, Prameswari MP, Ekonomi F, Islam U, et al. 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. J Akunt dan Teknol Inf. 2024;17(2):221–37.
[22] Laksana TG, Mulyani S. Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. J Ilm Multidisiplin. 2024;3(1):109–22.
[23] Handayani AA, Izzati BN, Nur D, Farida I, Prawira A. Strategi Mengatasi Data Breaches di Era Industri 4 . 0 : Kasus Data Breaches Bank Rakyat Indonesia 2021 lalu . Bank Rakyat Indonesia atau BRI adalah badan usaha milik Indonesia yang. J Manaj dan Bisnis Ekon. 2025;3(2).
[24] Hapsari PP, Khairunnisa SS, Baidhowi. Evaluasi Efektivitas Pengaturan Dan Pengawasan Bank Indonesia. J Cendekia Ilm. 2025;4(4):1427–47.
[25] Suwiknyo FB, Rompi T, Muaja HS. Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. Lex Priv. 2021;IX(4):183–92.
[26] Setiawan R. Digitalisasi Perbankan dan Ancaman Keamanan Siber : Tantangan dan Strategi Mitigasi Risiko Operasional. Adv Stud Econ Financ Bank. 2025;1(1).