Jurnal Bersama Ilmu Ekonomi
https://jurnal.literasisains.id/index.php/EKONOM
e-ISSN 3090-6393 | p-ISSN 3090-6407
Vol. 1 No. 2 (Mei 2025) 154-165
DOI: 10.55123/ekonom.v1i2.197

Keamanan Perbankan di Era Digital: Tantangan dan Solusinya

Alfina Ali[1], Anggun Okta Fitri[2]
[1,2]Program Studi Perbankan Syariah, Fakultas Ekonomi dan Bisnis Islam, UIN Raden Intan Lampung, Bandar Lampung, Indonesia
Email: [1]alfinaa189@gmail.com, [2]anggunoktafitri@radenintan.ac.id

Informasi Artikel
Submitted : 16-04-2025
Accepted : 10-05-2025
Published : 20-05-2025

Keywords:
Banking Security
Digital Era
Challenges
Solutions

Abstrak

This study aims to determine banking security in the digital era along with its challenges and solutions. This study combines quantitative and qualitative approaches to dig deeper into the challenges and solutions faced by the digital banking sector in maintaining transaction security. The results of the study indicate that most customers have a good awareness of the importance of security in digital transactions, although there are several obstacles and challenges that need to be overcome. The main challenges faced by banks in implementing an effective cybersecurity system: The development of digital technology has brought significant changes in the banking industry, enabling increased operational efficiency and convenience for customers. Solutions to the level of cyber threats faced by the banking sector in the digital era: Cyber threats to the banking sector in the digital era are a very serious issue because they involve sensitive customer data, public trust, and the stability of the financial system. Solutions to the main challenges faced by banks in implementing an effective cybersecurity system: There are 17 solutions to overcome the main challenges faced by banks in implementing an effective cybersecurity system.

Abstrak

Penelitian ini bertujuan untuk mengetahui keamanan perbankan di era digital beserta tantangan dan solusinya. Penelitian ini menggabungkan pendekatan kuantitatif dan kualitatif untuk menggali lebih dalam mengenai tantangan dan solusi yang dihadapi oleh sektor perbankan digital dalam menjaga keamanan transaksi. Hasil penelitian menunjukkan bahwa sebagian besar nasabah memiliki kesadaran yang baik terhadap pentingnya keamanan dalam transaksi digital, meskipun ada beberapa hambatan dan tantangan yang perlu diatasi. Tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif: Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, memungkinkan peningkatan efisiensi operasional dan kemudahan bagi nasabah. Solusi tingkat ancaman siber yang dihadapi sektor perbankan di era digital: Ancaman siber terhadap sektor perbankan di era digital merupakan isu yang sangat serius karena melibatkan data sensitif nasabah, kepercayaan publik, dan stabilitas sistem keuangan. Solusi tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif: solusi untuk mengatasi tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif ada 17 solusi.

Kata Kunci: Keamanan Perbankan, Era Digital, Tantangan, Solusi.

1. PENDAHULUAN

Keamanan perbankan di era digital menjadi tantangan utama bagi lembaga-lembaga keuangan di seluruh dunia. Dalam beberapa dekade terakhir, sektor perbankan telah mengalami transformasi digital yang luar biasa, memungkinkan berbagai layanan finansial menjadi lebih mudah diakses oleh masyarakat. Mobile banking, internet banking, serta aplikasi pembayaran digital telah mengubah cara kita berinteraksi dengan uang dan melakukan transaksi. Namun, dengan semua kemudahan yang ditawarkan, sektor perbankan juga dihadapkan pada berbagai ancaman baru yang muncul akibat perkembangan teknologi digital (Mufid, 2018).

Kemajuan teknologi informasi, terutama dalam bidang interkoneksi jaringan, telah memberikan pengaruh yang sangat signifikan terhadap berbagai aspek kehidupan manusia. Perkembangan ini tidak hanya mempermudah komunikasi dan akses informasi, tetapi juga mengubah cara kita bekerja, belajar, dan berinteraksi. Sejak revolusi industri pada abad ke 18-20 , perkembangan teknologi telah mengalami percepatan yang luar biasa, membawa dampak signifikan pada ekonomi, sosial, dan budaya. Memasuki abad ke-21, perkembangan teknologi informasi dan komunikasi (TIK) telah menjadi pilar utama kemajuan teknologi. Internet, yang awalnya dikembangkan sebagai proyek militer pada tahun 1960-an, kini telah menjadi infrastruktur global yang menghubungkan miliaran orang di seluruh dunia. Teknologi informasi telah memungkinkan kita untuk terhubung dengan orangorang di seluruh dunia dalam hitungan detik, mengakses informasi dari berbagai sumber dengan mudah, dan melakukan pekerjaan secara lebih efisien melalui berbagai alat dan platform digital (Maharani & Prakoso, 2024).

Seiring dengan semakin meluasnya penggunaan internet, kebutuhan akan perlindungan data pribadi menjadi semakin mendesak. Data pribadi kini menjadi aset yang sangat berharga dan rentan terhadap berbagai ancaman, seperti peretasan, pencurian identitas, dan penyalahgunaan informasi. Setiap hari, jutaan data pribadi dikumpulkan, disimpan, dan diproses oleh berbagai entitas, mulai dari perusahaan teknologi besar hingga layanan online kecil. Hal ini menimbulkan risiko yang signifikan terhadap privasi dan keamanan data pribadi. Di era digital, data kini menjadi aset paling berharga bagi organisasi dan individu. Data berfungsi sebagai sumber informasi yang sangat penting untuk pengambilan keputusan strategis, menciptakan nilai tambah bagi perusahaan, dan mendorong inovasi (Satria et al., 2024).

Serangan siber, pencurian data, dan penipuan online menjadi masalah besar yang harus dihadapi oleh perbankan digital. Sebagai contoh, peretasan sistem, seperti yang terjadi pada sejumlah bank besar di dunia, telah menyebabkan kerugian finansial yang signifikan dan merusak reputasi lembaga keuangan tersebut. Selain itu, kebocoran data nasabah dan meningkatnya kejahatan dunia maya seperti phishing dan malware turut memperburuk keadaan. Dalam konteks ini, penting bagi lembaga perbankan untuk memahami berbagai tantangan yang ada dan mengembangkan solusi yang efektif untuk mengatasi ancaman tersebut. Teknologi enkripsi, otentikasi ganda, serta pembaruan kebijakan dan prosedur keamanan menjadi langkah-langkah yang sangat dibutuhkan. Di samping itu, penting juga untuk meningkatkan literasi digital bagi masyarakat agar mereka lebih waspada terhadap potensi ancaman yang ada (Sutedi, 2023).

Seiring dengan perkembangan teknologi informasi yang pesat, sektor perbankan kini berada pada persimpangan antara inovasi dan tantangan besar dalam hal keamanan. Teknologi digital telah memungkinkan adanya kemudahan dalam akses layanan perbankan, seperti pembukaan rekening online, transaksi instan melalui mobile banking, dan layanan pembayaran elektronik. Namun, setiap kemajuan teknologi juga membawa potensi risiko yang tidak bisa dianggap remeh, terutama dalam hal keamanan data dan transaksi finansial. Keamanan perbankan di era digital bukan hanya menjadi isu teknis semata, tetapi juga mencakup aspek sosial dan hukum. Ancaman yang paling sering muncul adalah serangan siber yang menargetkan sistem informasi perbankan, seperti ransomware, phishing, dan DDoS (*Distributed Denial of Service*). Di sisi lain, kebocoran data nasabah atau transaksi palsu yang dilakukan oleh pihak ketiga semakin sering terjadi, menyebabkan kerugian material maupun non-material bagi pihak bank dan nasabah (Ali, 2008).

Berkembangnya teknologi *blockchain* dan kecerdasan buatan (AI) memberikan solusi potensial dalam meningkatkan keamanan, namun adopsi teknologi ini juga memunculkan tantangan baru terkait regulasi, biaya, dan kesiapan sumber daya manusia. Oleh karena itu, sektor perbankan perlu bekerja sama dengan berbagai pihak, baik pemerintah, regulator, maupun penyedia teknologi, untuk menciptakan ekosistem keamanan yang lebih baik. Oleh karena itu, menjaga keamanan data menjadi

hal yang sangat krusial dan penting dalam proses transformasi digital. Transformasi digital berkembang pesat di Indonesia, dengan pemerintah meluncurkan berbagai inisiatif untuk mempercepat proses ini. Inisiatif-inisiatif tersebut mencakup pengembangan infrastruktur digital, peningkatan literasi digital, dan penerapan teknologi baru di berbagai sektor. Namun, seiring dengan pesatnya perkembangan transformasi digital, masalah keamanan data telah menjadi isu yang sangat serius di seluruh dunia. Data pribadi dan informasi sensitif lainnya rentan terhadap berbagai ancaman, seperti peretasan, pencurian identitas, dan penyalahgunaan informasi. Data yang tidak terlindungi dengan baik dapat dilihat oleh pihak yang tidak berwenang dan digunakan untuk tujuan jahat, seperti penipuan, pemerasan, atau bahkan sabotase. Untuk mengatasi masalah ini, penting bagi organisasi dan individu untuk menerapkan langkah-langkah keamanan data yang komprehensif. Ini termasuk penggunaan teknologi enkripsi, kebijakan privasi yang ketat, dan pelatihan keamanan siber bagi karyawan. Selain itu, regulasi dan standar keamanan data yang ketat juga perlu diterapkan untuk memastikan bahwa data pribadi dilindungi dengan baik (Rustam, 2013). Penelitian ini bertujuan untuk mengetahui keamanan perbankan di era digital beserta tantangan dan solusinya.

1.1 Keamanan Perbankan

Keamanan adalah kondisi atau keadaan yang bebas dari ancaman, bahaya, atau kerusakan yang dapat merusak integritas, kerahasiaan, dan ketersediaan suatu sistem atau informasi. Keamanan mencakup langkah-langkah perlindungan terhadap informasi, sistem, serta aset lainnya dari berbagai ancaman yang bisa merugikan individu, organisasi, atau bahkan negara. Dalam sektor perbankan, keamanan berfokus pada perlindungan terhadap data nasabah, transaksi finansial, dan sistem perbankan secara keseluruhan, untuk menghindari ancaman seperti peretasan, pencurian data, atau penipuan online (Widiana et al., 2023).

1.2 Era Digital

Era digital merujuk pada periode di mana teknologi digital mendominasi berbagai aspek kehidupan manusia, mulai dari cara berkomunikasi, bekerja, berbelanja, hingga berinteraksi sosial. Era ini ditandai dengan penggunaan luas perangkat elektronik, internet, serta teknologi informasi dan komunikasi (TIK), yang memungkinkan digitalisasi dalam berbagai sektor kehidupan. Peningkatan ancaman terhadap keamanan transaksi menjadi perhatian utama dalam era digital. Oleh karena itu, bank telah mengadopsi teknologi keamanan seperti otentikasi dua faktor (2FA), enkripsi data, serta penggunaan biometrik (seperti sidik jari dan pengenalan wajah) untuk meningkatkan perlindungan data dan transaksi nasabah (Widiana et al., 2023). Digital mengacu pada representasi atau penyimpanan data dalam bentuk angka atau kode biner, yang mewakili informasi dengan menggunakan karakteristik diskrit, terutama dalam bentuk nol dan satu. Dalam konteks yang lebih luas, istilah digital juga merujuk pada teknologi dan solusi yang menggunakan data atau informasi dalam bentuk digital (Renaldo et al., 2022). Konsep digital juga mencakup berbagai aspek, termasuk: (1) Teknologi Digital: Penggunaan teknologi yang berbasis kode biner, seperti komputer, perangkat mobile, sensor, dan perangkat lainnya yang mengolah dan menyimpan data dalam bentuk digital. (2) Transformasi Digital: Proses di mana organisasi atau industri mengadopsi teknologi digital untuk meningkatkan efisiensi, inovasi, dan pengalaman pelanggan. (3) Isi Digital: Konten atau informasi yang disajikan dalam format digital, seperti teks, gambar, video, atau audio yang dapat diakses melalui perangkat digital. (4) Ekonomi Digital: Model bisnis yang berfokus pada pemanfaatan teknologi digital, seperti *e-commerce* (perdagangan elektronik), layanan streaming, dan layanan berbasis aplikasi. (5) Sosial Media dan Jaringan Digital: Platform online yang memungkinkan orang berinteraksi, berbagi informasi, dan berkomunikasi melalui media digital. Penggunaan konsep digital terus berkembang seiring dengan kemajuan teknologi, dan penerapan teknologi digital telah mengubah banyak aspek kehidupan, termasuk cara bertransaksi, berkomunikasi, dan berinteraksi dengan dunia di sekitar masyarakat (Junaedi et al., 2023).

1.3 Tantangan

Tantangan adalah suatu keadaan atau situasi yang mengandung kesulitan atau hambatan yang perlu dihadapi dan diatasi untuk mencapai suatu tujuan atau keberhasilan. Tantangan sering kali melibatkan kondisi yang memerlukan keterampilan, usaha, dan pemecahan masalah untuk mengatasinya. Dalam sektor perbankan digital, tantangan yang dihadapi bisa meliputi masalah keamanan data, perlindungan privasi nasabah, kesulitan dalam mengadopsi teknologi baru, serta risiko serangan siber yang semakin canggih (Raharja, 2024).

1.4 Solusi

Solusi adalah jawaban atau cara untuk menyelesaikan suatu masalah atau tantangan. Solusi berfokus pada pemecahan masalah yang ada, dengan mengidentifikasi langkah-langkah yang dapat diambil untuk mengatasi hambatan atau kesulitan tertentu.Dalam sektor perbankan digital, solusi yang digunakan untuk mengatasi tantangan keamanan dan privasi nasabah bisa melibatkan teknologi seperti enkripsi data, otentikasi dua faktor (2FA), dan sistem keamanan berbasis kecerdasan buatan (AI) (Sudjana, 2004).

2. METODOLOGI PENELITIAN

Penelitian ini menggabungkan pendekatan kuantitatif dan kualitatif untuk menggali lebih dalam mengenai tantangan dan solusi yang dihadapi oleh sektor perbankan digital dalam menjaga keamanan transaksi. Penelitian ini dilakukan melalui kajian pustaka yang melibatkan berbagai sumber ilmiah, seperti buku, jurnal penelitian, artikel kebijakan, serta regulasi yang relevan, termasuk Undang-Undang Perlindungan Data Pribadi di Indonesia dan pedoman internasional terkait perlindungan data (Sugiyono, 2016).

Dalam memilih literatur yang relevan, kriteria tertentu digunakan untuk memastikan kualitas dan keakuratan informasi yang diperoleh. Pertama, literatur yang dipilih harus terkait dengan risiko teknologi informasi pada bank syariah. Fokus utama adalah pada identifikasi ancaman dan tantangan terkini dalam teknologi informasi yang dihadapi oleh bank syariah. Kedua, literatur yang digunakan harus bersifat ilmiah dan telah melalui proses peer review, sehingga dapat diandalkan dalam memberikan informasi yang akurat dan berbasis bukti. Ketiga, literatur yang diperoleh harus merupakan sumber yang mutakhir, termasuk publikasi dalam kurun waktu yang relevan dengan penelitian ini. Validitas studi literatur dalam penelitian ini sangat penting untuk memastikan kualitas dan keandalan data yang digunakan. Untuk menjamin validitas studi literatur, langkah-langkah berikut diambil. Pertama, penggunaan sumber literatur yang terpercaya dan berkualitas, seperti jurnal ilmiah yang diindeks dan buku dari penerbit terkemuka. Kedua, kritikalitas dan analisis yang hati-hati dilakukan dalam memilih literatur yang relevan dan sesuai dengan tujuan penelitian. Ketiga, proses seleksi literatur yang transparan dan dapat direplikasi, dengan mempertimbangkan kriteria yang telah ditetapkan sebelumnya. Dengan pendekatan yang didasarkan pada studi literatur dan memperhatikan validitas penelitian, artikel ini bertujuan untuk menyajikan informasi yang terpercaya dan berbasis bukti tentang risiko teknologi informasi pada bank syariah, dengan fokus pada identifikasi ancaman dan tantangan terkini. Metode ini dirancang untuk memberikan gambaran yang komprehensif mengenai tantangan utama yang dihadapi oleh sektor perbankan dalam menjaga keamanan data pribadi nasabah, seperti risiko peretasan, pencurian identitas, dan pelanggaran privasi yang dapat merusak kepercayaan nasabah (Suharsaputra, 2012).

Proses penelitian dilakukan dengan cara yang teliti dan sistematis, memastikan bahwa hanya sumber yang dapat diandalkan yang digunakan. Hal ini termasuk buku fisik yang memiliki kredibilitas tinggi, literatur daring yang diakui, dan jurnal akademik yang membahas topik disrupsi digital marketing. Dengan pendekatan ini, peneliti dapat memperoleh informasi yang komprehensif

dan mendalam mengenai fenomena disrupsi dalam pemasaran digital tanpa perlu melibatkan interaksi langsung dengan subjek penelitian. Sebaliknya, fokus penelitian adalah pada pencarian dan analisis referensi yang ada, yang memberikan dasar kuat untuk memahami dan menjelaskan dinamika yang terjadi dalam konteks pemasaran digital saat ini. Pendekatan ini memberikan keuntungan dalam menyusun argumen dan temuan yang berbasis pada sumber yang sudah ada, memastikan bahwa analisis dilakukan secara menyeluruh dan berbasis bukti. Kajian ini diharapkan dapat memberikan kontribusi dalam pengembangan kebijakan yang lebih efektif untuk menjaga keamanan data nasabah di tengah perkembangan teknologi yang pesat. Selain itu, kajian ini bertujuan untuk menganalisis solusi teknis dan kebijakan yang diterapkan, termasuk enkripsi data, penggunaan sistem deteksi intrusi, serta edukasi literasi digital untuk nasabah (Sutopo, 2002).

Dengan demikian, artikel ini berupaya untuk menyusun rekomendasi yang konkret bagi pihak perbankan, baik dari sisi teknologi maupun kebijakan, agar mampu meningkatkan kepercayaan masyarakat melalui perlindungan data yang lebih kuat. Hasil penelitian menunjukkan bahwa sebagian besar nasabah memiliki kesadaran yang baik terhadap pentingnya keamanan dalam transaksi digital, meskipun ada beberapa hambatan dan tantangan yang perlu diatasi.

3. HASIL DAN PEMBAHASAN

3.1 Tingkat Ancaman Siber yang dihadapi Sektor Perbankan di Era Digital

Di era digital yang semakin maju, inovasi teknologi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor perbankan. Di Indonesia, sistem perbankan telah mengadopsi berbagai aplikasi dengan fitur-fitur terkini yang dirancang untuk memudahkan dan meningkatkan efisiensi dalam melakukan transaksi keuangan. Melalui electronic banking, nasabah kini dapat melakukan berbagai aktivitas perbankan hanya dengan beberapa klik di perangkat mereka. Fitur-fitur seperti pengecekan saldo, transfer dana antar rekening bank, dan pembayaran tagihan dapat dilakukan secara praktis dan cepat, tanpa harus mengunjungi bank secara fisik. Selain itu, aplikasi ini seringkali dilengkapi dengan fitur keamanan yang canggih, seperti autentikasi biometrik dan notifikasi transaksi, yang memberikan perlindungan tambahan bagi nasabah. Dengan kemudahan akses dan kecepatan layanan yang ditawarkan oleh teknologi ini, kehidupan sehari-hari masyarakat menjadi lebih efisien, memungkinkan mereka untuk mengelola keuangan dengan lebih baik dan menghemat waktu (Abubakar & Handayani, 2022).

Di era digital, teknologi informasi telah menjadi bagian tak terpisahkan dalam kehidupan manusia, mengubah berbagai sektor, termasuk sektor perbankan. Kemajuan teknologi, seperti internet, cloud computing, dan big data, telah memungkinkan bank untuk memberikan layanan yang lebih cepat, efisien, dan mudah diakses oleh nasabah. Namun, dengan kemajuan tersebut muncul tantangan besar dalam hal keamanan data pribadi. Data nasabah perbankan, yang meliputi informasi finansial, riwayat transaksi, dan data identitas, kini menjadi aset berharga yang rentan terhadap berbagai ancaman keamanan. Meningkatnya penggunaan teknologi digital di sektor perbankan juga diiringi dengan lonjakan ancaman siber yang semakin canggih. Risiko pencurian identitas, peretasan data, dan penyalahgunaan informasi pribadi semakin tinggi, terutama karena data yang disimpan oleh bank mengandung nilai ekonomi yang sangat tinggi. Oleh karena itu, keamanan data pribadi telah menjadi perhatian utama bagi sektor perbankan, yang diharapkan dapat melindungi data nasabah secara efektif untuk menjaga kepercayaan publik. Ancaman keamanan siber yang terus berkembang menjadi tantangan utama bagi perlindungan data di sektor perbankan. Bank menjadi target utama bagi para peretas karena data yang disimpan mengandung informasi keuangan bernilai tinggi. Serangan siber seperti phishing, ransomware, dan serangan malware semakin sering terjadi, yang dapat merusak sistem perbankan dan mengekspos data pribadi nasabah (Krippendorff, 2019).

Tantangan berikutnya datang dari rendahnya literasi digital di kalangan nasabah. Banyak nasabah perbankan yang tidak memiliki pengetahuan cukup mengenai risiko siber dan pentingnya menjaga keamanan data pribadi. Hal ini menjadikan mereka lebih rentan terhadap serangan social engineering, di mana pelaku kejahatan memanipulasi nasabah untuk memberikan informasi sensitif. Tanpa literasi digital yang memadai, nasabah cenderung menjadi target empuk bagi penipuan dan pencurian data (Smith, 2020).

Transformasi digital dalam perbankan tidak hanya meningkatkan kenyamanan bagi nasabah, tetapi juga mendorong inklusi keuangan dengan memberikan akses yang lebih luas kepada masyarakat untuk menggunakan layanan perbankan. Hal ini membuat adanya tuntutan secara tidak langsung kepada pihak perbankan untuk memberikan inovasi terbaru dalam sistem keuangan dalam bentuk mobile banking. Namun, pihak Bank juga harus memikirkan bagaimana cara memastikan keamanan data para nasabah agar aman sehingga tidak terjadi hal hal yang tidak diinginkan seperti tersebarnya data pribadi dan merusak kepercayaan nasabah. Di sektor perbankan pada tahun 2023, aspek keamanan siber yang menjadi perhatian utama meliputi peningkatan serangan siber yang mencapai 43% menurut BSSN. Serangan ini mencakup berbagai bentuk, seperti malware dan phishing, yang mengancam integritas data dan operasional bank. Bank Indonesia telah menetapkan standar keamanan siber melalui PBI No. 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran, namun pelaksanaannya masih terhambat oleh berbagai kendala teknis dan operasional. Insiden-insiden ini menyoroti kerentanan dalam sistem transfer keuangan global dan pentingnya keamanan siber yang lebih ketat. Pola penyerangan yang umum terjadi saat ini sering kali menargetkan pengguna atau nasabah yang melakukan transaksi melalui internet. Salah satu teknik yang banyak digunakan oleh para penyerang adalah phishing. Teknik phishing ini berfungsi untuk menyusup ke dalam jaringan dengan cara memanipulasi jalur data, sehingga penyerang dapat mengganti informasi yang seharusnya dengan data palsu. Melalui metode ini, penyerang dapat menciptakan situasi di mana korban menerima informasi yang tampak sah, tetapi sebenarnya telah dimanipulasi. Selain itu, teknik phishing juga dapat dimanfaatkan untuk menyebarkan malware. Para penyerang sering mengirimkan email yang berisi informasi terinfeksi kepada korban, yang dapat mengakibatkan sistem korban terinfeksi dan data sensitif mereka jatuh ke tangan yang salah (Abil et al., 2024).

Dengan semakin canggihnya teknik-teknik ini, penting bagi pengguna untuk selalu waspada dan menerapkan langkah-langkah keamanan yang tepat saat bertransaksi secara online, agar terhindar dari ancaman yang merugikan. Untuk mengurangi risiko serangan siber, lembaga perbankan dapat menerapkan sistem otentikasi dua faktor, yang berfungsi untuk memvalidasi data atau informasi yang akan diterima oleh nasabah. Sistem ini biasanya mencakup dua elemen otentikasi, yaitu penggunaan password yang diketahui oleh nasabah dan token, seperti smartcard atau aplikasi autentikasi yang menghasilkan kode unik. Dengan mengharuskan nasabah untuk memenuhi kedua persyaratan ini, perbankan dapat meningkatkan tingkat keamanan dalam proses transaksi. Tetapi untuk mencapai tingkat keamanan yang lebih tinggi, sangat disarankan agar bank juga menambahkan proses validasi biometrik. Metode biometrik, seperti pemindaian sidik jari, pengenalan wajah, atau pemindaian iris, dapat memberikan lapisan perlindungan tambahan yang sulit untuk dipalsukan atau dibobol. Dengan menggabungkan otentikasi dua faktor dengan teknologi biometrik, bank tidak hanya dapat melindungi data nasabah dengan lebih efektif, tetapi juga memberikan rasa aman yang lebih besar bagi nasabah saat melakukan transaksi. Hal ini sangat penting di era digital saat ini, di mana ancaman terhadap keamanan informasi semakin meningkat dan nasabah perlu merasa yakin bahwa data mereka terlindungi dengan baik. Tingkatan serangan siber yang terjadi khususnya di Indonesia bukan hanya menjadi permasalahan nasional. Namun, permasalahan ini cukup mendunia dan seringkali terjadi tanpa adanya penanganan yang cepat dan tepat sehingga sulit untuk mempertahankan data tanpa adanya kebocoran yang masif (Simatangkir et al., 2025).

3.2 Tantangan Utama yang Dihadapi Oleh Perbankan dalam Menerapkan Sistem Keamanan Siber yang Efektif

Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, memungkinkan peningkatan efisiensi operasional dan kemudahan bagi nasabah. Namun, transformasi ini juga menghadirkan tantangan baru, terutama dalam hal keamanan siber. Ancaman siber yang semakin kompleks dan canggih, seperti pencurian data, ransomware, dan serangan *Distributed Denial of Service* (DDoS), menjadi perhatian utama dalam menjaga integritas sistem perbankan. Perbankan tidak hanya harus melindungi data nasabah yang sensitif, tetapi juga memastikan kelancaran layanan operasional untuk mencegah kerugian finansial dan reputasi (Khairunnisa et al., 2024).

1. *Serangan Phishing* dan *Social Engineering* adalah tantangan signifikan dalam keamanan siber industri perbankan karena memanfaatkan faktor kelemahan manusia. Phishing dilakukan dengan mengelabui korban agar memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya melalui email, pesan teks, atau situs web palsu. Dalam konteks perbankan, serangan ini sering menyasar nasabah untuk mendapatkan akses ke rekening bank mereka. Tingginya tingkat kepercayaan nasabah terhadap komunikasi resmi bank menjadi celah bagi pelaku untuk membuat serangan mereka tampak meyakinkan. Phishing juga sering dikombinasikan dengan teknik lain, seperti *malware*, untuk meningkatkan efektivitas serangan. Teknik *Social Engineering* memanfaatkan psikologi manusia, seperti rasa takut atau kepanikan, untuk memanipulasi individu agar mengambil tindakan tertentu yang menguntungkan pelaku serangan. Contohnya adalah telepon palsu yang mengaku dari bank dan meminta informasi rahasia atas nama "keamanan akun". Serangan ini sangat sulit dideteksi karena tidak hanya bergantung pada kerentanan teknis tetapi juga pada kelemahan emosional manusia. Dalam industri perbankan, serangan phishing dan social engineering menjadi ancaman utama karena dampaknya dapat mencakup pencurian identitas, pengurasan dana, dan kerugian reputasi yang serius bagi bank.

2. *Malware* dan *Ransomware.* Dalam industri perbankan, *malware* dan ransomware merupakan tantangan signifikan bagi keamanan siber karena dampaknya yang luas terhadap operasional dan reputasi. Malware sering digunakan untuk mencuri data sensitif seperti informasi pelanggan atau kredensial login. Dalam konteks perbankan, serangan semacam ini menjadi lebih kompleks karena pelaku kejahatan siber mengadopsi teknik seperti trojan perbankan yang dapat menargetkan transaksi keuangan secara langsung. Ancaman ini semakin parah dengan peningkatan adopsi teknologi keuangan (*FinTech*) yang sering kali memperluas permukaan serangan dengan banyaknya interkoneksi antar sistem. Implementasi langkah-langkah pencegahan seperti autentikasi multifaktor (MFA) dan pengawasan ketat akses data menjadi solusi yang sering diterapkan untuk mengurangi risiko ini. Ransomware, di sisi lain, menonjol sebagai ancaman yang mengunci akses ke sistem penting dan sering kali diiringi dengan tuntutan tebusan besar. Dalam industri keuangan, serangan ransomware tidak hanya mengganggu operasional tetapi juga dapat membahayakan data pelanggan yang disandera atau diekspos. Strategi mitigasi yang direkomendasikan termasuk pengelolaan backup data yang solid, implementasi kontrol akses berbasis prinsip *least-privileged*, dan pelaporan insiden kepada otoritas seperti FBI, yang dapat membantu mengurangi dampak serangan. Selain itu, bank juga didorong untuk meningkatkan kebijakan tata kelola data dan pengawasan siber guna memenuhi persyaratan regulasi yang terus berkembang.

3. Serangan DDoS (*Distributed Denial of Service*) adalah salah satu ancaman terbesar dalam keamanan siber, terutama bagi sektor perbankan. Serangan ini melibatkan membanjiri server atau jaringan dengan lalu lintas palsu, sehingga mengganggu layanan yang sah. Dalam konteks

perbankan, serangan DDoS sering kali bertujuan untuk melumpuhkan situs web atau aplikasi layanan pelanggan, menghalangi transaksi penting, atau bahkan mengalihkan perhatian dari serangan lain yang lebih merusak, seperti pencurian data atau ransomware. Kompleksitas serangan ini meningkat seiring dengan pemanfaatan perangkat botnet yang tersebar secara global, menjadikannya sulit untuk dibedakan dari lalu lintas sah. Akibatnya, institusi perbankan sering menghadapi risiko kerugian finansial yang signifikan, termasuk biaya mitigasi dan kerusakan reputasi. Selain dampaknya terhadap layanan pelanggan, serangan DDoS memengaruhi kepercayaan publik terhadap keamanan sistem perbankan. Teknologi berbasis cloud yang semakin banyak diadopsi sektor perbankan juga menjadi target utama karena kerentanannya terhadap kelebihan kapasitas jaringan. Sementara solusi seperti deteksi berbasis machine learning atau blockchain mulai diterapkan untuk mitigasi, upaya ini masih menghadapi tantangan teknis dan kebutuhan sumber daya yang besar. Strategi keamanan proaktif, termasuk pemantauan jaringan secara real-time dan pengujian ketahanan, menjadi kunci untuk mengurangi ancaman DDoS di masa depan.

4. Keterbatasan Sumber Daya dan Keterampilan Dalam sektor perbankan, keterbatasan sumber daya dan kekurangan tenaga ahli menjadi tantangan utama dalam memastikan keamanan siber yang memadai. Institusi keuangan harus melindungi data sensitif dalam jumlah besar, tetapi sering kali menghadapi keterbatasan anggaran dan sumber daya manusia. Hal ini menjadi masalah yang signifikan mengingat ancaman siber terus berkembang. Institusi kecil, khususnya, kesulitan untuk mengikuti langkah-langkah keamanan yang diperlukan karena kurangnya dana untuk menginvestasikan teknologi terbaru serta kekurangan keahlian untuk menerapkannya secara efektif. Selain itu, mereka juga dihadapkan pada tekanan besar untuk mematuhi regulasi yang kompleks terkait perlindungan data dan privasi. Salah satu aspek penting dari masalah ini adalah kesenjangan keterampilan dalam keamanan siber, yang sangat dirasakan di industri perbankan. Seiring dengan semakin canggihnya ancaman siber, permintaan terhadap profesional keamanan siber yang berkualitas terus melebihi pasokan. Banyak institusi keuangan, terutama yang lebih kecil, kesulitan merekrut dan mempertahankan talenta dengan keahlian yang diperlukan untuk menangani ancaman ini. Meski kebutuhan terus meningkat, sistem pendidikan belum sepenuhnya menyesuaikan dengan tuntutan yang berubah di bidang keamanan siber, sehingga terjadi ketidaksesuaian antara keterampilan yang tersedia dan kebutuhan industri. Program seperti Cybersecurity Workforce Alliance berupaya menjembatani kesenjangan ini dengan menciptakan jalur yang lebih efektif antara dunia akademik dan sektor perbankan, tetapi tantangan besar masih ada.

5. Regulasi dan Kepatuhan Kepatuhan terhadap regulasi menjadi tantangan besar dalam keamanan siber di industri perbankan, khususnya dalam menghadapi perubahan undang-undang dan standar yang terus berkembang. Regulator di seluruh dunia kini menyesuaikan kerangka kerja mereka untuk menangani ancaman siber yang semakin kompleks, dengan fokus pada perlindungan kerahasiaan, integritas, dan ketersediaan sistem keuangan. Namun, sering kali terdapat kesenjangan antara kepatuhan teoretis dengan hasil keamanan yang nyata. Hal ini terjadi ketika lembaga keuangan hanya memenuhi persyaratan minimum regulasi tanpa memastikan bahwa langkah-langkah keamanan mereka benar-benar tangguh, sehingga menciptakan celah dalam sistem. Misalnya, meskipun regulasi seperti GDPR dan ISO 27001 mewajibkan penilaian risiko dan kontrol keamanan, penelitian menunjukkan bahwa kepatuhan saja tidak selalu meningkatkan performa keamanan secara signifikan. Selain itu, keragaman regulasi di berbagai wilayah menambah kompleksitas kepatuhan bagi bank internasional. Penerapan undang-undang seperti regulasi keamanan siber oleh New York Department of Financial Services atau PSD2 di Uni Eropa menciptakan lanskap regulasi yang terfragmentasi. Bank harus menavigasi persyaratan yang berbeda ini sambil menyeimbangkan biaya kepatuhan dengan kebutuhan untuk menerapkan strategi keamanan siber yang efektif. Ketidaksesuaian antara praktik kepatuhan dan keamanan

yang sebenarnya dapat merusak efektivitas keduanya, karena organisasi mungkin terlalu berfokus pada pemenuhan kewajiban hukum tanpa benar-benar mengatasi risiko keamanan mendasar. Seiring meningkatnya ancaman keamanan siber, regulator semakin menekankan integrasi kerangka kerja keamanan siber dan manajemen risiko untuk memberikan perlindungan yang lebih komprehensif di sektor keuangan (Khairunnisa et al., 2024).

Industri perbankan menghadapi tantangan besar dalam melawan ancaman siber, seperti phishing, ransomware, hingga pelanggaran data. Untuk mengatasi hal ini, bank harus menerapkan pendekatan multi-lapis yang mencakup pemanfaatan teknologi canggih dan kebijakan keamanan yang ketat. Salah satu solusi utama adalah adopsi teknologi seperti kecerdasan buatan (AI) untuk mendeteksi dan merespons ancaman secara *real-time*. Selain itu, penggunaan autentikasi multifaktor (MFA) dan pendekatan "*zero-trust network architecture*" (ZTNA) dapat memperkuat kontrol akses dan melindungi data pelanggan. Program pelatihan kesadaran siber juga menjadi langkah penting untuk mengurangi risiko dari ancaman yang melibatkan kesalahan manusia. Dari sisi regulasi, bank perlu mematuhi standar keamanan global seperti *Payment Card Industry Data Security Standard* (PCI DSS) dan membangun kerangka kerja kolaboratif dengan institusi keuangan lainnya. Selain itu, pengawasan ketat terhadap vendor pihak ketiga menjadi penting karena banyak pelanggaran data terjadi melalui kelemahan dalam rantai pasokan. Untuk mitigasi risiko sistemik, lembaga seperti *Financial Systemic Analysis and Resilience Center* (FSARC) membantu mengidentifikasi titik lemah pada sistem keuangan yang dapat memperbesar dampak serangan. Pendekatan ini, jika dilakukan secara konsisten, dapat meningkatkan ketahanan sektor perbankan terhadap ancaman siber yang terus berkembang (Edilius & Sudarsono, 2004).

3.3 Solusi Tingkat Ancaman Siber yang dihadapi Sektor Perbankan di Era Digital

Ancaman siber terhadap sektor perbankan di era digital merupakan isu yang sangat serius karena melibatkan data sensitif nasabah, kepercayaan publik, dan stabilitas sistem keuangan. Untuk mengatasi ancaman tersebut, dibutuhkan solusi komprehensif yang mencakup aspek teknis, kebijakan, dan kesadaran manusia. Berikut adalah solusi untuk mengatasi tingkat ancaman siber di sektor perbankan di era digital (Ichsan, 2014):

1. Peningkatan infrastruktur keamanan siber. Implementasi teknologi enkripsi untuk seluruh data nasabah, baik dalam penyimpanan (*data at rest*) maupun saat transmisi (*data in transit*), *firewall* generasi terbaru (*Next-Generation Firewalls*), *Intrusion Detection/Prevention Systems* (IDS/IPS), dan *Security Information and Event Management* (SIEM) untuk mendeteksi aktivitas mencurigakan secara real time dan segmentasi jaringan untuk membatasi akses internal dan mengisolasi potensi serangan.
2. Penerapan *multi-factor authentication* (MFA). Meningkatkan keamanan login dengan penggunaan MFA, seperti OTP, biometrik, dan token keamanan, terutama untuk transaksi keuangan penting.
3. Audit dan Penilaian Keamanan Berkala. Melakukan *penetration testing*, audit keamanan sistem TI, evaluasi risiko siber secara berkala untuk menilai kesiapan, kerentanan sistem dan mengadopsi standar keamanan internasional seperti ISO/IEC 27001.
4. Pelatihan dan kesadaran keamanan siber. Melakukan edukasi rutin kepada karyawan dan nasabah tentang *phishing*, rekayasa sosial, dan bentuk-bentuk ancaman siber lainnya dan membangun budaya *cyber hygiene*, seperti penggunaan password kuat, tidak membuka tautan mencurigakan.
5. Penerapan teknologi AI dan *machine learning*. Menggunakan AI/ML untuk deteksi anomali secara *real time* dalam aktivitas transaksi dan mendeteksi *fraud pattern* yang tidak bisa dilihat secara manual.
6. Kolaborasi dengan regulator dan pihak ketiga. Bekerja sama dengan otoritas keuangan (OJK, BI) untuk memenuhi regulasi keamanan, mengikuti kerangka kerja perlindungan data pribadi, seperti UU PDP (perlindungan data pribadi) dan berkolaborasi dengan penyedia layanan keamanan siber terpercaya.

7. Perencanaan dan respons insiden (*incident response plan*). Menyusun rencana tanggap insiden untuk mengurangi dampak serangan siber dan mempercepat pemulihan dan simulasi berkala melalui *cyber drill* untuk menguji kesiapan tanggap darurat.
8. *Zero trust architecture* (ZTA). Menerapkan prinsip "*never trust, always verify*" di seluruh sistem dan membatasi akses hanya pada pengguna atau sistem yang telah diverifikasi secara ketat.
9. Penggunaan *blockchain* untuk keamanan transaksi. Teknologi *blockchain* dapat memberikan transparansi dan integritas yang tinggi dalam pencatatan transaksi, mengurangi risiko manipulasi data.
10. Redundansi dan *backup* sistem. Menyediakan *backup* data berkala dan *disaster recovery site* untuk menjamin kontinuitas operasional jika terjadi serangan seperti *ransomware* (Ichsan, 2014).

3.4 Solusi Tantangan Utama yang Dihadapi Oleh Perbankan dalam Menerapkan Sistem Keamanan Siber yang Efektif

Berikut adalah solusi untuk mengatasi tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif (Mukhlis, 2015):

1. Menerapkan arsitektur *zero trust*, di mana setiap akses harus diverifikasi tanpa asumsi kepercayaan.
2. Melakukan integrasi sistem keamanan berbasis SIEM dan SOAR untuk visibilitas menyeluruh dan respon otomatis.
3. Investasi pada pelatihan internal dan sertifikasi keamanan siber (seperti CEH, CISSP).
4. Bermitra dengan vendor keamanan siber eksternal untuk mendapatkan keahlian tambahan.
5. Mengadopsi *security-as-a-service* (SECaaS).
6. Gunakan *user behavior analytics* (UBA) untuk mendeteksi perilaku mencurigakan.
7. Terapkan akses berbasis prinsip *least privilege* dan audit aktivitas internal secara berkala.
8. Membentuk divisi khusus *compliance* dan keamanan TI untuk memantau dan menyesuaikan kebijakan secara proaktif.
9. Gunakan *platform governance, risk* dan *compliance* (GRC) untuk pemantauan terpadu.
10. Gunakan AI/ML untuk mendeteksi pola anomali dalam aktivitas sistem secara *real-time*.
11. Terapkan sistem *threat intelligence sharing* untuk berbagi data ancaman dengan lembaga lain.
12. Jalankan program *cybersecurity awareness training* secara berkala.
13. Gunakan simulasi *phishing* untuk mengukur kesiapan karyawan dan memberikan *feedback* langsung.
14. Terapkan kebijakan *third-party risk management* (TPRM).
15. Lakukan audit keamanan pada vendor secara berkala sebelum integrasi.
16. Pendekatan berbasis risiko (*risk-based investment*) agar anggaran difokuskan pada aset paling kritis.
17. ROI keamanan dapat ditunjukkan dengan simulasi potensi kerugian jika terjadi pelanggaran (Mukhlis, 2015).

4. KESIMPULAN

Tingkat ancaman siber yang dihadapi sektor perbankan di era digital: Di era digital yang semakin maju, inovasi teknologi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor perbankan. Tantangan berikutnya datang dari rendahnya literasi digital di kalangan nasabah. Transformasi digital dalam perbankan tidak hanya meningkatkan kenyamanan bagi nasabah, tetapi juga mendorong inklusi keuangan dengan memberikan akses yang lebih luas kepada masyarakat untuk menggunakan layanan perbankan. Dengan semakin canggihnya teknik-teknik, penting bagi pengguna untuk selalu waspada dan menerapkan langkah-langkah keamanan yang tepat saat bertransaksi secara online, agar terhindar dari ancaman yang merugikan.

Tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif: Perkembangan teknologi digital telah membawa perubahan signifikan dalam industri perbankan, memungkinkan peningkatan efisiensi operasional dan kemudahan bagi nasabah. Namun, transformasi ini juga menghadirkan tantangan baru, terutama dalam hal keamanan siber. Ancaman siber yang semakin kompleks dan canggih, seperti pencurian data, ransomware, dan serangan *Distributed Denial of Service* (DDoS), menjadi perhatian utama dalam menjaga integritas sistem perbankan. Perbankan tidak hanya harus melindungi data nasabah yang sensitif, tetapi juga memastikan kelancaran layanan operasional untuk mencegah kerugian finansial dan reputasi. Solusi tingkat ancaman siber yang dihadapi sektor perbankan di era digital: Ancaman siber terhadap sektor perbankan di era digital merupakan isu yang sangat serius karena melibatkan data sensitif nasabah, kepercayaan publik, dan stabilitas sistem keuangan. Untuk mengatasi ancaman tersebut, dibutuhkan solusi komprehensif yang mencakup aspek teknis, kebijakan, dan kesadaran manusia. Solusi tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif: solusi untuk mengatasi tantangan utama yang dihadapi oleh perbankan dalam menerapkan sistem keamanan siber yang efektif ada 17 solusi.

DAFTAR PUSTAKA

Abil, Y. I. M., Rizky, D. S. M., & Rachma, I. (2024). Pengaruh Perlindungan Data Dan Cyber SecurityTerhadap Tingkat Kepercayaan MenggunakanFintech Masyarakat Di Surabaya. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(11), 618–628.

Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. *Masalah-Masalah Hukum*, *51*(3), 259–270.

Ali, Z. (2008). *Hukum Perbankan Syariah*. Sinar Grafika.

Edilius, & Sudarsono. (2004). *Kamus Ekonomi Uang dan Bank*. Rineka Cipta.

Ichsan, H. N. (2014). *Pengantar Perbankan*. Gaung Persada Press Group.

Junaedi, A. T., Renaldo, N., Yovita, I., Veronica, K., & Sudarno. (2023). Opportunities And Challenges Of Islamic Banks In The Digital Banking Era In The Perspective Of Generation Z. *Kurs: Jurnal Akuntansi, Kewirausahaan Dan Bisnis*, *8*(2), 116–125.

Khairunnisa, Komariah, N., Akbar, K., Mucriadin, & Suriati. (2024). Inovasi Dan Tantangan Perbankan Syariah Di Era Digital. *Jurnal El Rayyan : Jurnal Perbankan Syariah*, *3*(2), 113–122. https://www.kompasiana.com/rismacamelia7530/66425533c57afb14b3580f43/inovasi-dan-tantangan-perbankan-syariah-di-era-digital

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

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan substansial dalam penggunaan platform e-commerce di Indonesia telah. *Jurnal USM Law Review*, *7*(1), 333–347.

Mufid, M. (2018). *Ushul Fiqh Ekonomi dan Keuangan Kontemporer dari Teori ke Aplikasi*. Prenadamedia Group.

Mukhlis, I. (2015). *Ekonomi Keuangan, Perbankan Teori Dan Aplikasi*. Salemba Empat.

Raharja. (2024). *Keamanan Jaringan*. KBM Indonesia.

Renaldo, N., Hafni, L., Hocky, A., Suhardjo, & Junaedi, A. T. (2022). The Influence Of Digital Technology And Efficiency Strategy On Business Sustainability With Quality Management As Moderating Variables. *International Conference on Business & Social Sciences (ICOBUSS)*, *1*(1), 1–10.

Rustam, B. R. (2013). *Manajemen Risiko Perbankan Syariah di Indonesia*. Salemba Empat.

Satria, A., Ulina, N. P. H., Safira, P., & Pangestu, B. (2024). Perspektif Hukum Terhadap Keamanan Data: Tantangan Dan Solusi Di Era Teknologi Informasi. *Warta Dharmawangsa*, *18*(1), 177–192.

Simatangkir, D. W. E., Afifah, E. F. N., & Faliha, N. S. (2025). Keamanan Siber Dalam Perbankan Serta Tantangan Dan Solusi Di Era Digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42.

Smith, A. (2020). Digital Literacy and Cybersecurity in the Financial Sector. *Journal of Information Technology*, *17*(3), 85–98.

Sudjana. (2004). *Manajemen Program Pendidikan*. Falah Production.

Sugiyono. (2016). *Metode Penelitian Kualitatif, Kuantitatif, dan R&D.* Alfabeta.

Suharsaputra, U. (2012). *Metode Penelitian Kuantitatif, Kualitatif, dan Tindakan*. Refika Aditama.

Sutedi, A. (2023). *Hukum Perbankan: Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, dan Kepailitan*. Sinar Grafika.

Sutopo, H. (2002). *Metode Penelitian Kualitatif*. Remaja Rosdakarya.

Widiana, W., Anggara, F. S. A., Purnamasari, S., Nugraha, J. P., Ardianto, R., Harto, B., Nuraeni, Sulistiyo, H., Elsa, Suartini, S., B, S., & Dasman, S. (2023). *Keuangan Bisnis Digital*. PT Global Eksekutif Teknologi.