KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi, Manajemen, Bisnis dan Akuntansi (JEMBA)
Vol.3, No.4 Juli 2026
e-ISSN: 3047-6240, p-ISSN : 3047-6232, Hal 606-617
DOI : https://doi.org/10.61722/jemba.v3i4.2740

PERLINDUNGAN DATA DAN SALDO NASABAH *MOBILE BANKING* DARI ANCAMAN KEJAHATAN SIBER DAN PENIPUAN KOMPUTER DALAM SISTEM TRANSAKSI KEUANGAN DIGITAL

Dini Marwati [1], Wina Agustina [2], Rahma Mughmi Cahyani [3], Ria Susilawati [4]

[1]Departem, Prodi Akuntansi, Universitas Teknologi Digital, Jl Cibogo Indah No. III , Bandung, Jawa Barat, Indonesia 40151
[2]Departem, Prodi Akuntansi, Universitas Teknologi Digital, Jl Cibogo Indah No. III , Bandung, Jawa Barat, Indonesia 40151
dini10424012@digitechuniversity.ac.id, wina10424008@digitechuniversity.ac.id, rahma10424002@digitechuniversity.ac.id, ria10424005@digitechuniversity.ac.id

Abstrak Perkembangan teknologi digital membuat layanan perbankan menjadi lebih mudah, cepat, dan efisien melalui Mobile Banking, namun juga meningkatkan risiko kejahatan siber seperti phishing, malware, ransomware, pencurian identitas, dan berbagai penipuan digital yang mengancam data pribadi serta saldo nasabah. Penelitian ini bertujuan mempelajari peran keamanan siber dalam melindungi uang nasabah pengguna Mobile Banking, mengidentifikasi jenis ancaman yang terjadi, serta menganalisis langkah pencegahan yang dapat dilakukan bank maupun pengguna, menggunakan metode studi literatur dengan pendekatan kualitatif melalui buku, jurnal ilmiah, peraturan perundang-undangan, artikel, dan penelitian terdahulu. Hasil penelitian menunjukkan bahwa teknologi keamanan seperti enkripsi data, autentikasi multifaktor, Cyber Threat Intelligence, sistem deteksi penipuan, dan autentikasi biometrik dapat meningkatkan keamanan transaksi digital dan mengurangi kemungkinan serangan siber. Namun, keamanan siber belum dapat melindungi secara penuh karena metode serangan yang semakin canggih dan kesalahan manusia yang masih banyak terjadi akibat rendahnya literasi digital masyarakat. Oleh karena itu, perlindungan yang optimal hanya dapat tercapai melalui kerja sama antara pemerintah, lembaga perbankan, dan masyarakat dalam memperkuat sistem keamanan, regulasi, serta pemahaman digital, karena tingkat keberhasilan keamanan siber tetap bergantung pada kesadaran dan kewaspadaan pengguna dalam menjaga data pribadi serta akun Mobile Banking mereka.

Kata kunci; Keamanan Siber, Mobile Banking, Cybercrime, Cyber Threat Intelligence (CTI), Perlindungan Data, Literasi Digital.

Naskah Masuk: 05 Juli 2026; Revisi: 05 Juli 2026; Diterima: 05 Juli 2026; ; Terbit: 06 Juli 2026.

1. LATAR BELAKANG

Kemajuan teknologi digital di era globalisasi telah membawa transformasi signifikan dalam sektor ekonomi dan transaksi keuangan, salah satunya melalui layanan *Mobile Banking* yang memungkinkan nasabah melakukan transfer dana, pembayaran tagihan, pembelian produk digital, hingga pengecekan saldo hanya melalui *smartphone* yang terhubung internet (Nurdin et al., 2021)Kemudahan akses, kecepatan transaksi, serta efisiensi waktu dan tenaga membuat layanan ini semakin banyak digunakan oleh berbagai kalangan masyarakat (*Ekonomi-Dan-Keuangan-Digital-Konsep-Dan-Implementasi-Di-Indonesia.Pdf*, n.d.)

Di balik kemudahan tersebut, penggunaan *Mobile Banking* juga menghadirkan tantangan keamanan data dan saldo nasabah, seiring meningkatnya kejahatan siber (*cybercrime*) yang menyasar pengguna layanan keuangan digital (Kementerian Komunikasi dan Informatika Republik Indonesia 2023, 2023). Beberapa modus yang paling umum adalah *phishing* (penipuan untuk memperoleh data pribadi melalui manipulasi atau penyamaran), *malware* (pencurian data atau pengambilalihan akses perangkat), pencurian identitas, dan *social engineering* yang memanfaatkan kelengahan pengguna. Modus tersebut umumnya dilakukan melalui pesan, email, atau situs palsu yang mengatasnamakan institusi terpercaya, sehingga banyak korban tidak menyadari telah menjadi target penipuan hingga mengalami kerugian ((Rifka Alkhilyatul Ma'rifat, I Made Suraharta, 2024)

Meningkatnya kasus pembobolan rekening dan penyalahgunaan data pribadi menjadi bukti bahwa keamanan transaksi digital masih memiliki kelemahan, salah satunya karena banyak nasabah yang mudah membagikan kode OTP, mengakses tautan tidak jelas, atau mengunduh aplikasi dari sumber tidak resmi (BSSN, 2024)Pihak perbankan telah berupaya meningkatkan keamanan melalui autentikasi dua faktor, enkripsi data, dan notifikasi transaksi *real-time* (*Pertemuan Tahunan Bank Indonesia 2022*, 2022) namun keamanan *Mobile Banking* tidak hanya bergantung pada sistem bank, melainkan juga pada tingkat literasi digital pengguna yang hingga kini masih tergolong rendah (Otoritas Jasa Keuangan (OJK), 2023)

Kondisi ini menunjukkan bahwa keamanan layanan *Mobile Banking* tidak hanya ditentukan oleh sistem perlindungan bank, tetapi juga oleh kesadaran dan kewaspadaan pengguna dalam menjaga kerahasiaan data pribadinya. Rendahnya literasi digital masyarakat menjadi salah satu penyebab utama masih terjadinya penipuan, penyalahgunaan data, dan kebocoran informasi dalam penggunaan layanan keuangan digital.

2. KAJIAN TEORITIS

Pengertian Keamanan Siber (*Cyber Security*)

Keamanan siber merujuk pada upaya melindungi perangkat komputer, jaringan, aplikasi, dan informasi dari berbagai risiko dunia maya seperti peretasan, perangkat lunak jahat, dan penipuan digital. Dalam layanan perbankan melalui ponsel, keamanan siber sangat krusial karena proses keuangan dilakukan secara daring dan melibatkan data

pribadi serta saldo rekening pengguna, sehingga sistem perlindungan yang memadai menjadi syarat utama untuk menjaga kerahasiaan informasi dan membangun kepercayaan masyarakat terhadap layanan perbankan digital (Nurhania et al., 2025 p. 4)

Tujuan Keamanan Siber

Tujuan utama keamanan siber adalah melindungi informasi pribadi, saldo akun, dan sistem transaksi *online* dari berbagai risiko kejahatan siber, termasuk peretasan, pencurian informasi, dan penipuan digital dalam layanan *mobile banking*. Selain menciptakan sistem transaksi yang aman dan terpercaya, keamanan siber juga berperan mengidentifikasi serta mencegah serangan sebelum menimbulkan kerugian yang lebih besar (Nurhania et al., 2025 p. 6)

Ciri-Ciri Keamanan Siber

Keamanan siber memiliki beberapa ciri utama, yaitu menjaga kerahasiaan informasi agar tidak diakses pihak yang tidak berhak, melindungi keutuhan data agar tidak diubah pihak lain, serta memastikan sistem digital tetap berfungsi baik. Dalam praktiknya, keamanan siber memanfaatkan berbagai teknologi seperti kata sandi, PIN, OTP, autentikasi dua faktor, *firewall*, dan enkripsi data, disertai pemantauan berkelanjutan untuk mendeteksi aktivitas mencurigakan (Nurhania et al., 2025 p. 7)

Fungsi Keamanan Siber dalam *Mobile Banking* dan Transaksi Keuangan Digital

Dalam konteks *mobile banking*, keamanan siber berfungsi menjaga kerahasiaan data pribadi nasabah agar tidak diakses atau disalahgunakan pihak tak berwenang, serta menjaga keaslian data agar tidak diubah atau dimanipulasi sehingga transaksi dan saldo nasabah tetap akurat dan aman (Pertamina, 2020)Fungsi lainnya adalah mengidentifikasi dan menghentikan ancaman melalui pengawasan dan intelijen ancaman siber atau *Cyber Threat Intelligence* (CTI), yang mendukung organisasi menemukan, menganalisis, dan merespons ancaman sebelum menimbulkan kerugian signifikan (Pertamina, 2020 p. 21)

Peranan Keamanan Siber dalam *Mobile Banking* dan Transaksi Keuangan Digital

Keamanan siber juga berperan menjaga keamanan data, sistem, dan jaringan dari ancaman yang terus berevolusi (Pertamina, 2020 p. 19-20)sekaligus mendukung deteksi dan respons ancaman yang lebih cepat melalui CTI (Pertamina, 2020 p. 21)serta menjaga kestabilan layanan digital agar gangguan sistem dan kerugian finansial dapat diminimalkan.

Manfaat Keamanan Siber

Keamanan siber memberikan banyak keuntungan dalam sistem transaksi keuangan digital, seperti melindungi informasi pribadi dan data nasabah dari pencurian, menjaga keamanan saldo dan transaksi *Mobile Banking*, serta meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital karena menurunkan risiko *phishing*, *malware*, dan pencurian identitas. Bagi bank, keamanan siber juga membantu

mempertahankan reputasi, mendorong pengembangan sistem yang lebih mutakhir dan saling terhubung sehingga nasabah dapat bertransaksi kapan saja dan di mana saja, serta mendukung kepatuhan terhadap regulasi perlindungan data dan privasi.

Kelemahan Keamanan Siber

Di samping manfaatnya, keamanan siber juga memiliki kelemahan, terutama kebutuhan dana yang tinggi untuk pengembangan, pemeliharaan, dan pembaruan sistem seiring ancaman yang terus berubah. Kelalaian pengguna, seperti membagikan OTP atau kata sandi kepada pihak ketiga, tetap menjadi faktor utama penipuan digital, sementara sistem keamanan yang kompleks juga membutuhkan tenaga profesional untuk pengawasan berkala. Dengan demikian, keberhasilan keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran pengguna dalam melindungi data serta akun mereka.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur (*library research*) dengan pendekatan kualitatif, yaitu mengumpulkan, membaca, dan menganalisis berbagai sumber tertulis yang relevan dengan topik penelitian (Mestika Zed, 2014, p. 21). guna memahami dan menjelaskan fenomena berdasarkan landasan teori, pandangan ahli, serta hasil penelitian terdahulu (Moleong, n.d., p. 6). Sumber referensi yang digunakan meliputi buku, jurnal ilmiah, artikel, peraturan perundang-undangan, serta dokumen pendukung lain yang relevan (Sugiyono, 2022, p. 3), yang terdiri atas data primer dari jurnal dan buku referensi utama, serta data sekunder dari artikel dan laporan penelitian sebagai pelengkap pembahasan (Arikunto, 2019, p. 22).

Pengumpulan data dilakukan melalui dokumentasi dan studi kepustakaan dari sumber akademik seperti Google Scholar, repositori jurnal, dan buku elektronik yang diseleksi agar relevan dan dapat dipertanggungjawabkan secara ilmiah (Hardani, n.d., p. 70).Data dianalisis secara deskriptif kualitatif dengan menelaah, membandingkan, dan menyusunnya secara sistematis sebelum ditarik kesimpulan berdasarkan teori dan temuan terdahulu yang relevan (Miles, n.d., p. 10) guna memberikan pemahaman komprehensif mengenai peran keamanan siber dalam melindungi data dan saldo nasabah *Mobile Banking*.

4. HASIL DAN PEMBAHASAN

Perkembangan teknologi digital telah membawa dampak signifikan terhadap sistem transaksi keuangan, salah satunya melalui layanan *Mobile Banking* yang memungkinkan nasabah melakukan transfer dana, pembayaran, dan pengecekan saldo secara cepat dan efisien melalui *smartphone* tanpa harus mengunjungi kantor bank (Ningtias, 2025). Transformasi digital ini mendorong perubahan layanan perbankan dari yang bersifat konvensional menjadi berbasis digital yang dapat diakses kapan pun, sekaligus meningkatkan efisiensi operasional dan memperluas jangkauan layanan, seiring berkembangnya *financial technology* (fintech) di Indonesia. Namun, kemudahan tersebut

juga diikuti oleh meningkatnya ancaman kejahatan siber (*cybercrime*) yang menyasar pengguna layanan keuangan digital.

Sektor perbankan digital menjadi salah satu target utama kejahatan siber karena mengelola data sensitif dan bernilai ekonomi tinggi, seperti data pribadi nasabah, informasi rekening, dan transaksi dalam jumlah besar (Maheswari, 2024). *Cybercrime* sendiri didefinisikan sebagai segala perbuatan melawan hukum yang memanfaatkan jaringan komputer atau internet, baik dengan komputer sebagai sarana maupun sebagai target kejahatan (Birlin, 2025).. Berbeda dari kejahatan konvensional, pelaku *cybercrime* kini dapat beraksi dari jarak jauh melalui jaringan atau kelompok yang terorganisasi, dengan teknik yang semakin maju dan sulit dideteksi.

Bentuk dan Modus Kejahatan Siber Pada *Mobile Banking*

Salah satu bentuk *cybercrime* yang paling banyak ditemukan pada layanan *Mobile Banking* adalah *phishing*, yaitu penipuan digital berbasis rekayasa sosial (*social engineering*) untuk memperoleh informasi rahasia korban seperti *username*, *password*, PIN, atau kode OTP. Modusnya umumnya berupa pesan palsu melalui SMS, email, WhatsApp, atau media sosial yang mengatasnamakan bank dan berisi informasi mendesak, seperti pemblokiran rekening atau tawaran hadiah, yang mengarahkan korban ke tautan atau situs palsu. Apabila korban memasukkan data pribadinya, informasi tersebut akan dicuri dan disalahgunakan untuk mengakses rekening korban secara tidak sah. (Nuzula, 2024).

Selain *phishing*, ancaman lain yang berpotensi membahayakan transaksi digital antara lain *malware* (perangkat lunak berbahaya untuk mencuri data atau mengambil alih akses perangkat), *hacking*, *ransomware* (yang mengenkripsi data korban dan meminta tebusan untuk memulihkannya), *carding* (penyalahgunaan data kartu kredit/debit curian), pencurian identitas, serta *skimming* (perekaman data kartu melalui alat khusus yang dipasang pada mesin ATM). Beragamnya bentuk kejahatan ini menunjukkan bahwa ancaman terhadap keamanan transaksi digital semakin kompleks dan terus berkembang seiring kemajuan teknologi.

***Fraud* Digital dan Penyebab Kejahatan Siber**

Perkembangan teknologi digital juga memunculkan berbagai bentuk *fraud* berbasis komputer (*computer fraud*), yaitu tindakan kecurangan yang memanfaatkan sistem komputer untuk memperoleh keuntungan ilegal, mulai dari pencurian data, manipulasi transaksi elektronik, penyalahgunaan akses sistem, hingga pemalsuan laporan keuangan (Revalina, 2025). *Fraud* digital dapat berbentuk *input fraud* (memasukkan data palsu ke sistem), *process fraud* (menyalahgunakan sistem untuk kepentingan pribadi), *computer instruction fraud* (memanipulasi perangkat lunak agar bekerja sesuai keinginan pelaku), dan *data fraud* (mengubah atau merusak data penting). Bentuk-bentuk tersebut

menunjukkan bahwa kejahatan digital dapat mengancam baik pengguna individu maupun sistem perusahaan dan lembaga keuangan.

Dampak Kejahatan Siber Terhadap Pengguna *Mobile Banking*

Meningkatnya kasus pembobolan rekening dan pencurian data pribadi menunjukkan bahwa keamanan transaksi digital masih menghadapi banyak tantangan, terutama karena rendahnya pemahaman nasabah dalam menjaga keamanan akun, seperti mengklik tautan mencurigakan, menggunakan *password* lemah, atau membagikan kode OTP. Hal ini sejalan dengan teori *Fraud Triangle*, yang menjelaskan bahwa *fraud* terjadi karena adanya tekanan (*pressure*), kesempatan (*opportunity*), dan rasionalisasi (*rationalization*), di mana lemahnya pengawasan dan literasi digital membuka peluang besar bagi pelaku (Revalina Annisa Antoine, ddk ,2025). Data Indonesia Anti-Phishing Data Exchange (IDADX) mencatat lonjakan serangan *phishing* dari 6.106 kasus pada kuartal IV 2022 menjadi 26.675 kasus pada kuartal I 2023, menandakan masih adanya kelemahan sistem keamanan dan literasi digital masyarakat yang membuat banyak pengguna belum mampu membedakan situs resmi dari situs palsu . (Maheswari, 2024).

Selain kerugian finansial, kejahatan siber juga menimbulkan dampak psikologis bagi korban, seperti rasa takut, cemas, trauma, dan hilangnya rasa aman maupun kepercayaan terhadap layanan digital. (Ramayani, Early Ridho Kismawadi, 2020) menunjukkan bahwa persepsi keamanan data pribadi berpengaruh signifikan terhadap tingkat kepercayaan pengguna *mobile banking* semakin tinggi persepsi keamanan yang diberikan, semakin tinggi pula kepercayaan nasabah, yang sangat penting bagi bank sebagai lembaga penyimpan dana masyarakat.

Regulasi dan Perlindungan Hukum Dalam Perbankan Digital

Sebagai lembaga yang menghimpun dana masyarakat, bank memiliki tanggung jawab hukum menjaga kerahasiaan data nasabah berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, sejalan dengan hak setiap individu atas perlindungan data pribadinya , (Pratikno, 2022) dan kewajiban penuh bank memproteksi data nasabah dari ancaman internal maupun eksternal (Iqbal Asnawi et al., 2024). Perlindungan ini juga didasarkan pada Undang-Undang Perlindungan Konsumen dan Undang-Undang ITE (Lange, 2015), meski pengaturan yang spesifik untuk *internet banking* masih belum optimal sehingga kerap menimbulkan ketidakpastian hukum.

Dalam praktiknya, bank menerapkan berbagai teknologi keamanan seperti autentikasi dua langkah, OTP, *firewall*, enkripsi data, *Fraud Detection System* (FDS), verifikasi biometrik, serta pemantauan aktivitas mencurigakan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi (Cinar, 2023), Selain itu, sektor perbankan juga mulai menerapkan *Cyber Threat Intelligence* (CTI), yakni sistem intelijen keamanan siber untuk mengidentifikasi, menganalisis, dan mendeteksi ancaman digital sebelum serangan terjadi, sehingga lembaga dapat mengambil tindakan pencegahan secara lebih cepat dan tepat (Cinar, 2023),.

Teknologi Keamanan dan *Cyber Threat Intelligence (*CTI)

Penerapan CTI menjadi penting dalam layanan *Mobile Banking* karena ancaman *cybercrime* terus berkembang dan semakin kompleks. Sistem ini membantu bank memantau aktivitas mencurigakan, mendeteksi transaksi tidak normal, serta mengidentifikasi potensi *phishing*, *malware*, *ransomware*, dan pencurian data, sekaligus mendukung proses respons dan pemulihan pascaserangan. Beberapa bank telah menerapkan teknologi pendukung CTI seperti *Fraud Detection System* (FDS), autentikasi dua langkah, pemantauan transaksi *real time*, *firewall*, dan enkripsi data guna menjaga kerahasiaan dan integritas data nasabah (Cinar, 2023),

Pengawasan Internal dan Peran Nasabah

Selain penguatan sistem keamanan, pengawasan internal juga penting dalam mencegah *cyber fraud* di sektor perbankan. Audit internal berperan mendeteksi, memonitor, dan mengevaluasi aktivitas transaksi digital dengan memanfaatkan teknologi seperti *software* audit, *Electronic Data Interchange* (EDI), dan *whistleblowing system* (Egidius Egia Aginta Ginting et al., 2025). Namun, perlindungan data dan saldo nasabah bukan hanya tanggung jawab bank—nasabah juga perlu berperan aktif dengan tidak membagikan kode OTP, tidak mudah percaya pesan yang mengatasnamakan bank, menggunakan *password* kuat, mengaktifkan verifikasi ganda, dan rutin memperbarui sistem keamanan perangkat. Rendahnya literasi digital—kemampuan memahami, menggunakan, dan mengelola teknologi secara aman—menjadi salah satu penyebab utama masyarakat rentan menjadi korban *phishing* karena sulit membedakan tautan palsu dari situs resmi. (Iqbal Asnawi et al., 2024). Pencegahan kejahatan siber karenanya memerlukan kerja sama lintas sektor melalui protokol keamanan yang kuat, edukasi masyarakat, dan koordinasi efektif antara penyedia layanan dan pengguna (Lufti Nasution, 2023), didukung sinergi antara pemerintah, perbankan, dan masyarakat untuk menciptakan sistem transaksi digital yang aman dan berkelanjutan.

Secara hukum, perlindungan nasabah dari kejahatan siber telah diatur melalui Undang-Undang ITE, Undang-Undang Perbankan, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi, termasuk POJK No. 12 Tahun 2018 yang mewajibkan bank memastikan keamanan sistem, menjaga kerahasiaan data, dan menyediakan mekanisme pengaduan (Iqbal Asnawi et al., 2024) Meski demikian, pengaturan tanggung jawab bank atas kerugian akibat *phishing* masih belum terintegrasi secara utuh, sehingga penyelesaian kasus kejahatan siber kerap menghadapi ketidakpastian hukum.

Kasus Nyata Kejahatan Siber Pada Perbankan

Kasus nyata terlihat dalam peristiwa yang melibatkan PT Varash Saddan Nusantara (PT VSN) dan Bank Rakyat Indonesia (BRI) pada 2025, ketika dana perusahaan senilai Rp1,8

miliar lenyap akibat peretasan pada server internal. Penyelidikan mengungkap bahwa transaksi menggunakan *username* dan kata sandi resmi nasabah dari alamat IP perusahaan sendiri, sehingga bank menyimpulkan kerugian disebabkan oleh kelalaian nasabah, bukan kesalahan sistem bank—menunjukkan bahwa ancaman siber di sektor perbankan nyata dan dapat menimbulkan kerugian besar bagi kedua pihak (*Dana Rp 1,8 Miliar PT VSN Raib, BRI Tegaskan Bukan Salah Sistem Bank, Melainkan Server Nasabah Disusupi Hacker*, n.d.).
Dalam penanganan kasus semacam ini, teknologi komputer forensik berperan penting untuk menemukan dan menganalisis bukti digital seperti *email phishing* dan log transaksi guna mendukung proses hukum.

Penerapan enkripsi, verifikasi identitas, dan sistem perlindungan pada *mobile banking* dapat menurunkan risiko pencurian data dan akses ilegal terhadap saldo nasabah (Ramayani, Early Ridho Kismawadi, 2020), karena kualitas sistem keamanan bank secara langsung memengaruhi sejauh mana saldo nasabah terlindungi (Oping & Gunadi, 2025).

Kami tidak sependapat dengan pandangan bahwa keamanan siber dapat sepenuhnya melindungi saldo nasabah dari serangan siber. Meski lembaga keuangan telah menerapkan enkripsi data, autentikasi berlapis (*Multi-Factor Authentication*/MFA), biometrik, dan sistem deteksi kecurangan di mana MFA mensyaratkan dua atau lebih bentuk verifikasi seperti kata sandi, OTP, atau sidik jari sebelum mengakses akun (Nist & Publication, 2025) metode kejahatan siber terus berkembang semakin kompleks. Banyak kasus pencurian dana justru terjadi akibat faktor manusia, misalnya pengguna yang tanpa sadar membagikan kode OTP, mengklik tautan penipuan, atau memakai kata sandi yang mudah ditebak, sehingga sistem keamanan bank sering tidak dapat mencegah kerugian ketika informasi penting telah diserahkan sendiri oleh korban kepada pelaku. Dengan demikian, keamanan siber lebih berfungsi mengurangi potensi risiko daripada menghapusnya secara total.

Keamanan siber tetap krusial sebagai salah satu bentuk proteksi utama layanan perbankan melalui ponsel, namun belum memadai untuk memastikan keselamatan dana nasabah secara penuh. Proteksi yang diberikan bank memang mendapat respons positif karena dianggap mampu menjaga keamanan dan kerahasiaan informasi, tetapi belum sepenuhnya mampu mencegah *phishing*, *malware*, pencurian informasi, dan pembobolan akun (taufik hidayatullah pratama, 2023, p. 1) Perlindungan yang optimal hanya dapat tercapai apabila sistem keamanan yang andal didukung oleh kesadaran dan kewaspadaan pengguna.

Pratama dan Nurhayati (2023) mengungkapkan bahwa tantangan implementasi keamanan siber meliputi keterbatasan alat, evolusi taktik kejahatan, serta kesalahan manusia seperti memberikan PIN atau OTP kepada pihak tak bertanggung jawab (taufik hidayatullah pratama, 2023, p. 4)yang diperkuat oleh hasil kuesioner penelitian tersebut yang menunjukkan sebagian nasabah masih pernah mengalami *cybercrime* (taufik hidayatullah pratama, 2023, p. 7).

Kami sependapat bahwa *cyber security* berperan penting mengurangi risiko dan meminimalkan kerugian nasabah, namun belum dapat menjamin perlindungan penuh

karena pelaku kejahatan siber selalu mencari celah baik pada sistem maupun pengguna, sehingga keamanan optimal hanya dapat tercapai melalui kombinasi sistem keamanan yang kuat, pengawasan berkelanjutan, dan partisipasi aktif nasabah dalam menjaga data pribadinya.

Langkah Pencegahan dan Solusi

Pencegahan kejahatan siber perlu dimulai dari level individu, lembaga, hingga pemerintah, antara lain melalui kebijakan keamanan yang ketat seperti *firewall* dan enkripsi data. (Parulian et al., 2021, p. 6) pelatihan berkala bagi pengguna untuk mengenali serangan siber (Hukum, 2025) sinergi tanggung jawab antara penyedia jasa dan pengguna (Parulian et al., 2021) serta kebijakan antipenipuan yang komprehensif dan tegas (Collins et al., 2021).

Implementasi *Cyber Threat Intelligence* (CTI) pada *Mobile Banking* menjadi semakin krusial karena metode keamanan konvensional tidak lagi memadai menghadapi kompleksitas kejahatan siber yang terus berkembang. Keberhasilan CTI juga tidak hanya ditentukan oleh teknologi yang dimiliki bank, tetapi juga kompetensi sumber daya manusia yang mengelolanya—sistem secanggih apa pun tidak akan optimal tanpa didukung individu yang responsif dan tepat dalam menangani ancaman.

Pertumbuhan *Mobile Banking* memberikan manfaat besar bagi masyarakat karena transaksi menjadi lebih cepat dan efisien, didukung sistem keamanan seperti CTI, *firewall*, dan enkripsi. Namun, kemajuan ini juga membuka peluang bagi pelaku kejahatan siber, terutama karena masih banyak pengguna yang kurang memahami keamanan digital—menunjukkan bahwa akar masalah tidak hanya pada sistem, tetapi juga pada pengguna, sehingga kolaborasi lembaga keuangan, pemerintah, dan masyarakat menjadi krusial untuk keamanan layanan digital.

Bank perlu terus memperkuat sistem keamanannya dengan memperbarui teknologi enkripsi, meningkatkan autentikasi multifaktor (MFA), menerapkan sistem deteksi dan pencegahan penipuan, serta secara rutin mengedukasi nasabah mengenai ancaman seperti *phishing*, *malware*, dan pencurian data. Di sisi lain, nasabah perlu meningkatkan kewaspadaan dengan tidak membagikan PIN, kata sandi, atau OTP kepada siapa pun, serta memastikan aplikasi yang digunakan berasal dari sumber resmi dan selalu diperbarui. Melalui kolaborasi antara bank dan nasabah dalam program edukasi digital yang berkelanjutan, potensi kejahatan siber dapat diminimalkan sehingga keamanan saldo dan data pribadi nasabah lebih terjaga.

5. KESIMPULAN DAN SARAN

Kesimpulan Setuju

a. Pentingnya keamanan siber sangat besar dalam menjaga informasi dan saldo pelanggan *Mobile Banking* dari ancaman berbagai kejahatan siber.

b. Penerapan teknologi seperti pengkodean, verifikasi dua langkah (MFA), dan Intelijen Ancaman Siber (CTI) terbukti efisien dalam menurunkan kemungkinan pencurian data dan pembobolan akun.
c. Keamanan transaksi secara digital akan lebih optimal bila didukung oleh kolaborasi antara lembaga perbankan, pemerintah, dan masyarakat melalui peningkatan pengetahuan digital.

Kesimpulan Tidak Setuju

a. Keamanan siber tidak bisa memastikan bahwa saldo pelanggan terlindungi sepenuhnya, sebab cara kejahatan siber terus mengalami perkembangan.
b. Perlindungan tidak semata-mata ditentukan oleh teknologi perbankan, tetapi juga dipengaruhi oleh tindakan pengguna yang sering melakukan kesalahan seperti membagikan kode OTP atau mengunjungi tautan *phishing*.
c. Walaupun sistem perlindungan semakin maju, ancaman kebocoran data dan penipuan online masih ada, sehingga kewaspadaan pengguna tetap sangat penting.

Saran

a. Untuk pihak bank, penting untuk terus memperbaiki sistem perlindungan *Mobile Banking* dan memberikan pendidikan rutin kepada pelanggan mengenai potensi ancaman dari kejahatan siber.
b. Untuk pemerintah dan OJK, penting untuk memperkuat peraturan serta pengawasan terkait keamanan transaksi digital untuk menjamin perlindungan data dan saldo nasabah.
c. Untuk pelanggan, penting untuk meningkatkan kewaspadaan dengan tidak memberikan PIN, kata sandi, atau kode OTP kepada siapa pun serta memastikan perangkat yang digunakan selalu aman.
d. Untuk masyarakat umum, penting untuk meningkatkan pengetahuan digital agar dapat mengenali dan menghindari berbagai jenis penipuan online seperti phishing dan malware.

DAFTAR REFERENSI

BSSN. (2024). Laporan Tahunan 2023: Monitoring Keamanan Siber Nasional. *Badan Siber Dan Sandi Negara*, *70*. https://bssn.go.id

Cinar, B. (2023). Cyber Threat Intelligence: Current Trends and Future Perspectives. *Journal of Engineering Research and Reports*, *25*(4), 91–105. https://doi.org/10.9734/jerr/2023/v25i4905

Dana Rp 1,8 Miliar PT VSN Raib, BRI Tegaskan Bukan Salah Sistem Bank, Melainkan Server Nasabah Disusupi Hacker. (n.d.). Radar Bali. https://radarbali.jawapos.com/ekonomi/2506210018/dana-rp-18-miliar-pt-vsn-raib-bri-tegaskan-bukan-salah-sistem-bank-melainkan-server-nasabah-disusupi-hacker

Egidius Egia Aginta Ginting, Fadillah Janadiyah, Vina Julianti, Nia Syahfitri,

Muhammad Roy Prayudha, Aprilia Ananda Putri, & Jufri Darma. (2025). Audit Sistem Informasi Berbasis Komputer Terhadap Pencegahan Kecurangan (Fraud) : Kajian Teoritis. *Jurnal Publikasi Ekonomi Dan Akuntansi*, *5*(2), 16–26. https://doi.org/10.51903/jupea.v5i2.3838

Ekonomi-dan-Keuangan-Digital-Konsep-dan-Implementasi-di-Indonesia.pdf. (n.d.).

Iqbal Asnawi, M., Fitriani, R., Syafrina Tala, W., Aikel Primsa Tarigan, J., Maulana Daffa, T., & Habibi, W. (2024). *Locus: Jurnal Konsep Ilmu Hukum*. *5*(July). https://doi.org/10.56128/jkih.v4i3.402

Kementerian Komunikasi dan Informatika Republik Indonesia 2023. (2023). *Laporan Kinerja Kementerian Komunikasi dan Informatika Republik Indonesia 2023*.

Lange, T. A. (1998). Internet Banking. *Internet Banking*, *1*, 149–160. https://doi.org/10.1007/978-3-322-84622-8

Lufti Nasution, M. (2023). *Recht Studiosum Law Review*. *02*(02), 2985–9867. https://talenta.usu.ac.id/rslr

Nurdin, Rukma Ningrum, Sofyan Bacmid, & Abdul Jalil. (2021). Pengaruh Manfaat, Kepercayaan Dan Kemudahan Penggunaan Terhadap Minat Nasabah Menggunakan Mobile Banking Di Bank Mega Syariah Cabang Palu. In *Jurnal Ilmu Perbankan dan Keuangan Syariah* (Vol. 3, Issue 1, pp. 30–45). https://doi.org/10.24239/jipsya.v3i1.37.30-45

Nurhania, N., Reza Aulia Putri, Indah Purnamasari, Fehlirrah Bunga Apriana, Alfino Gibran Elfathar, & M. Ilham Marli. (2025). Analisis Keefektifan Sistem Keamanan dalam Transaksi Online Perbankan Syariah. *Journal of Economics and Business*, *3*(1), 41–50. https://doi.org/10.61994/econis.v3i1.548

Otoritas Jasa Keuangan (OJK). (2023). Penguatan Sektor Jasa Keuangan Dalam Menjaga Pertumbuhan Ekonomi. *Laporan Tahunan Annual Report 2023*.

Pertamina. (2020). *Keamanan Siber Perusahaan*. https://www.pertamina.com/id/keamanan-siber-perusahaan%0Ahttps://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/458

Pertemuan Tahunan Bank Indonesia 2022. (2022). Bank Indonesia. https://www.bi.go.id/id/ptbi-2022/default.aspx

Pratikno. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Hukum Online*, 1–38. https://learning.hukumonline.com/wp-content/uploads/2023/07/Undang-Undang-No.27-Tahun-2022-Hukumonline.pdf

Ramayani, Early Ridho Kismawadi, R. D. C. (2020). *Pengaruh Kepercayaan, Keamanan, Manfaat dan Kemudahan Terhadap Penggunaan Mobile Banking. Jurnal Ilmiah Mahasiswa,1-16,2020.* 1–16.

Rifka Alkhilyatul Ma'rifat, I Made Suraharta, I. I. J. (2024). *No Title 済無No Title No Title No Title*. *2*(1), 306–312.

Semarang), R. A. A. (Universitas N., Semarang), N. S. F. (Universitas N., Semarang), A. H. H. (Universitas N., & Semarang), M. P. (Universitas N. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 1.

taufik hidayatullah pratama. (2023). Perlindungan Nasabah Pengguna Layanan E-Banking Dalam Perspektif Cybercrime. *AT-TAWASSUTH: Jurnal Ekonomi Islam*, *VIII*(I), 1–19.