KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Manajemen Bisnis dan Akuntansi
Vol.2, No.4 Juli 2025
e-ISSN: 3047-6240; p-ISSN: 3047-6232, Hal 276-289
DOI : https://doi.org/10.61722/jemba.v2i4.1157

IMPLEMENTASI *CYBER SECURITY* DALAM SISTEM TRANSAKSI KEUANGAN DIGITAL

Aiva Tyanka Farahdiva
Universitas Teknologi Digital
Siti Linda Mulyana
Universitas Teknologi Digital
Tika Permata Asri
Universitas Teknologi Digital
Alamat: Jl. Cibogo No.Indah 3, Mekarjaya, Kec. Rancasari, Kota Bandung, Jawa Barat
Korespondensi penulis: aiva10423004@digitechuniversity.ac.id, siti10423007@digitechuniversity.ac.id, tika10423008@digitechuniversity.ac.id

Abstrak. *The advancement of digital technology has significantly transformed financial transaction systems, with the emergence of services such as mobile banking, e-wallets, and QRIS. Behind the convenience and speed of these transactions lies a serious threat from increasingly sophisticated cyberattacks. This article discusses the implementation of cyber security as a crucial element in securing digital financial transaction systems. Strategies applied include data encryption, multi-factor authentication, real-time transaction monitoring, firewalls, and the use of technologies such as blockchain and tokenization. Case studies on mobile banking, e-wallets, and QRIS show that security relies not only on technology but also on internal policies, regulations, and users' digital literacy. This research employs a literature review method and a qualitative analysis approach based on various recent scientific journals and publications. The findings indicate that cyber security implementation must be comprehensive and continuous, involving active roles from governments, service providers, financial institutions, and end users to establish a safe and trustworthy digital ecosystem.*
Keywords: *Cyber Security; Digital Financial Transactions; E-Wallet; Mobile Banking; QRIS; Data Security*

Abstrak. Perkembangan teknologi digital telah membawa perubahan signifikan dalam sistem transaksi keuangan, dengan munculnya layanan seperti mobile banking, e-wallet, dan QRIS. Di balik kemudahan dan kecepatan transaksi, terdapat ancaman serius berupa serangan siber yang terus berkembang. Artikel ini membahas implementasi cyber security sebagai elemen kunci dalam menjaga keamanan sistem transaksi keuangan digital. Strategi yang diterapkan meliputi enkripsi data, autentikasi multi-faktor, pemantauan transaksi secara real-time, penggunaan firewall, serta pemanfaatan teknologi seperti blockchain dan tokenisasi. Studi kasus pada layanan mobile banking, e-wallet, dan QRIS menunjukkan bahwa keamanan tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan internal, regulasi, dan literasi digital pengguna. Penelitian ini menggunakan metode studi pustaka dan pendekatan analisis kualitatif terhadap berbagai jurnal ilmiah dan publikasi terkini. Hasil penelitian mengindikasikan bahwa implementasi cyber security harus dilakukan secara menyeluruh dan berkelanjutan, melibatkan peran aktif dari pemerintah, penyedia layanan, institusi keuangan, hingga pengguna akhir untuk menciptakan ekosistem digital yang aman dan terpercaya.
Kata Kunci: *Cyber Security, Transaksi Keuangan Digital, Mobile Banking, E-Wallet, QRIS, Keamanan Data*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk sektor keuangan. Inovasi berbasis digital seperti *internet banking, e-wallet, mobile banking*, dan layanan *fintech* kini telah mengubah cara masyarakat bertransaksi secara signifikan. Proses keuangan yang sebelumnya memerlukan interaksi fisik kini dapat dilakukan dengan cepat dan praktis hanya melalui perangkat digital. Namun, di balik kemudahan

Received April 29, 2025; Revised Mei 30, 2025;Juni 25, 2025
* Aiva Tyanka Farahdiva, aiva10423004@digitechuniversity.ac.id

yang ditawarkan, muncul tantangan besar dalam bentuk ancaman terhadap keamanan sistem digital tersebut.

Sektor keuangan menjadi salah satu target utama dalam serangan siber global. Menurut Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 terdapat 47.729 anomali trafik di sektor keuangan, di mana lebih dari 56% di antaranya melibatkan aktivitas *malware*. Hal ini menunjukkan bahwa sistem keuangan digital merupakan sasaran empuk bagi pelaku kejahatan siber karena menyimpan data sensitif dan memiliki nilai ekonomi tinggi. Serangan tersebut tidak hanya menimbulkan kerugian materi tapi juga berpotensi merusak kepercayaan masyarakat terhadap sistem keuangan digital.

Salah satu elemen utama dari transformasi tersebut adalah sistem transaksi keuangan digital, yaitu sistem yang memungkinkan perpindahan nilai secara elektronik menggunakan teknologi jaringan. Menurut Laudon dan Traver (2021), sistem transaksi digital adalah proses pertukaran informasi dan nilai yang dilakukan melalui perangkat berbasis internet, yang mencakup pembayaran elektronik, transfer dana, hingga aktivitas investasi daring. Sistem ini mengedepankan kecepatan, efisiensi, dan kemudahan namun rentan terhadap gangguan.

Kasus pembobolan rekening melalui *mobile banking* telah menjadi ancaman serius dalam sistem perbankan digital di Indonesia. Contohnya adalah kasus yang dialami oleh wartawan senior bernama Ilham Bintang pada Januari 2020. Ia merupakan korban pembobolan *mobile banking* melalui modus *social engineering* dan SIM *swap*, yang mengakibatkan kerugian senilai ratusan juta rupiah. SIM swap merupakan teknik kejahatan dimana pelaku mengambil alih nomor telepon korban dengan membuat kartu SIM baru menggunakan identitas palsu hasil pencurian, sehingga pelaku dapat menerima semua OTP transaksi. Fenomena ini menunjukkan bahwa sistem keamanan siber Indonesia masih memiliki celah yang dapat dimanfaatkan pelaku kejahatan sehingga perlu diperkuat secara signifikan. (Azizah, Ula, Mutiara, & Prameswari, 2024)

Untuk melindungi sistem digital tersebut, dibutuhkan penerapan *cyber security* yang andal. Menurut Stallings dan Brown (2018), *cyber security* adalah praktik dan pendekatan teknis untuk menjaga sistem informasi dari ancaman seperti akses ilegal, sabotase digital, dan pencurian data. Tiga prinsip utama yang dijaga dalam keamanan siber adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Dalam konteks keuangan, *cyber security* tidak hanya melindungi sistem, tetapi juga menjadi dasar kepercayaan antara penyedia layanan dan nasabah. (Sachlos & Auguste, 2022)

Penerapan cyber security di sektor keuangan harus mencakup pengamanan jaringan, perlindungan data pribadi, sistem otentikasi ganda, serta pemantauan aktivitas yang mencurigakan secara *real-time*. Namun, banyak lembaga keuangan terutama yang berbasis digital masih mengalami keterbatasan dalam sumber daya, baik dari sisi teknologi maupun personel. Ini membuat sistem mereka rentan terhadap serangan, khususnya yang bersifat *zeroday* atau serangan yang mengeksploitasi celah keamanan yang belum dikenali.

Regulasi pemerintah seperti Undang-undang Perlindungan Data Pribadi (UU PDP) dan Peraturan OJK tentang Manajemen Risiko Teknologi Informasi telah disusun untuk mendorong peningkatan keamanan siber. Namun, dalam praktiknya, implementasi regulasi ini masih perlu dikaji ulang efektivitasnya. Lemahnya pengawasan serta minimnya hukuman terhadap pelanggaran membuat lembaga keuangan belum sepenuhnya terdorong untuk menerapkan sistem keamanan yang optimal.

Sistem keuangan digital seharusnya tidak hanya berorientasi pada inovasi teknologi, tetapi juga menempatkan aspek keamanan sebagai prioritas utama. Sistem yang inovatif namun rentan terhadap serangan justru akan merugikan pengguna dan menurunkan nilai tambah dari layanan digital itu sendiri. Maka*, cyber security* bukan lagi pilihan, melainkan sebuah kebutuhan mutlak dalam sistem keuangan modern. (Samudra, Hidayat, & Wahyu, 2023)

Penelitian mengenai implementasi *cyber security* dalam sistem transaksi keuangan digital sangat relevan dengan kondisi saat ini. Kajian ilmiah dibutuhkan untuk mengidentifikasi faktor-faktor penghambat dalam penerapan sistem keamanan digital serta memberikan rekomendasi strategis yang dapat diterapkan oleh lembaga keuangan. Studi ini juga diharapkan dapat menyoroti sejauh mana organisasi keuangan telah memahami dan menerapkan kebijakan *cyber security* untuk menjaga keberlangsungan dan kepercayaan publik terhadap ekosistem keuangan digital Indonesia yang sedang berkembang pesat.

KAJIAN TEORI

Menurut Thompson & William dalam jurnal (Angsito, 2018) *Cyber security* adalah Kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan dan organisasi dan asset pengguna. *Cyber Security* adalah sistem yang dirancang khusus untuk melindungi jaringan dan perangkat dari serangan siber yang beragam, seperti *malware, phishing*, dan *denial of service*. Hal ini sering kali mengarah pada tindakan kejahatan siber yang dapat merugikan individu, organisasi, perusahaan, bahkan pemerintahan. Oleh karena itu, *Cyber Security* menjadi sangat penting untuk dipahami. Selain memperkuat sistem keamanan komputer, *Cyber Security* juga membutuhkan tenaga kerja yang terampil dalam membangun infrastruktur keamanan, mencegah serangan, dan menangani retas informasi yang disebut dengan *Cyber Security Officer*. (Sari R. P., 2024)

Keamanan siber adalah upaya melindungi infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan informasi yang tersimpan dalam cloud. Adapun tujuan dari kemanan siber menurut Septasari dalam jurnal (Azizah, Ula, Mutiara, & Prameswari, 2024) adalah untuk memastikan organisasi atau pengguna dilindungi dari berbagai jenis serangan digital terhadap perangkat komputer, mobile server dan jaringan sistem elektronik.

Cyber security memiliki beberapa fungsi dasar yang menjadi pilar utama dalam sistem keamanan digital yang disebut sebagai bagian dari kerangka kerja keamanan informasi yang dikenal dengan istilah CIA Triad (*Confidentiality*. *Integrity, availability*). Menurut (Andhika, 2023) fungsi-fungsi tersebut yaitu: a. *Confidentiality* yaitu menjaga kerahasiaan data agar tidak diakses oleh pihak yang tidak berwenang. b. *Integrity* yaitu menjamin bahwa data yang disimpan atau dikirim tidak dimodifikasi oleh pihak yang tidak sah. c. *Availability* yaitu memastikan bahwa data dan sistem selalu tersedia dan dapat diakses oleh pengguna yang sah saat dibutuhkan. d. *Authentication* yaitu memverifikasi identitas pengguna atau sistem. e. *Non-repudiation* yaitu mencegah adanya penyangkalan oleh pengirim atau penerima data.

Dengan segala fungsinya, *cyber security* memiliki berbagai manfaat penting bagi organisasi maupun individu, diantaranya (Sugiarti, 2024): a. Melindungi Data Sensitif, dengan keamanan data yang kuat mencegah kebocoran informasi penting, seperti data pribadi dan finansial, yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. b. Menjaga Reputasi Organisasi, kebocoran data dapat merusak reputasi perusahaan atau organisasi, yang

berpotensi mengurangi kepercayaan pelanggan dan mitra bisnis. c. Meningkatkan Kepercayaan Pelanggan, sehingga pelanggan lebih cenderung bertransaksi dengan perusahaan yang memiliki reputasi dalam menjaga data pribadi mereka dengan aman. d. Menjamin Kelangsungan Operasional, *cyber security* bisa membantu melindungi bisnis dari gangguan yang dapat menghambat operasional, termasuk serangan yang dapat menyebabkan *down-time* atau kehilangan data. e. Mendukung Kepatuhan Hukum, dengan meningkatnya regulasi perlindungan data, seperti UU PDP di Indonesia, sistem keamanan yang baik membantu organisasi mematuhi kewajiban hukum.

Adapun Kelebihan dari *cyber security* menurut (Rizki, 2024) sangat beragam, seperti meningkatkan keamanan data, mencegah ancaman siber, hingga menjaga kelangsungan operasional organisasi. Berikut merupakan beberapa kelebihannya. a. Mendeteksi dan Mencegah Serangan Secara *Real-Time*, *Cyber security* mampu mendeteksi dan mencegah serangan dengan cepat menggunakan teknologi seperti IDS/IPS, yang memungkinkan respon langsung terhadap ancaman yang muncul. b. Skalabilitas dan Fleksibilitas, Salah satu kelebihan utama *cyber security* adalah kemampuannya untuk diterapkan di berbagai sektor dan ukuran organisasi. Dari perusahaan kecil hingga besar, sistem keamanan dapat disesuaikan dengan kebutuhan spesifik, memberikan perlindungan yang optimal sesuai dengan skala operasional yang ada. c. Integrasi dengan Teknologi Canggih, *Cyber security* dapat diintegrasikan dengan teknologi lain seperti *Artificial Intelligence* (AI) dan *Machine Learning* (ML) untuk meningkatkan deteksi ancaman secara otomatis. Penggunaan teknologi canggih ini memungkinkan sistem untuk belajar dari pola serangan sebelumnya dan memberikan respons yang lebih cepat serta lebih tepat. d. Meningkatkan Kepercayaan Pengguna dan Pelanggan , Keamanan yang terjamin dalam transaksi dan pengelolaan data pribadi meningkatkan kepercayaan pelanggan terhadap perusahaan atau layanan yang menggunakan sistem digital. Kepercayaan ini menjadi faktor penting dalam membangun hubungan jangka panjang dengan konsumen.

Namun demikian, *cyber security* juga tentunya memiliki beberapa kelemahan dan tantangan. Adapun kelebihan dan kelemahan menurut (Muslim, 2024): a. Perkembangan Teknologi, Perkembangan teknologi yang pesat menciptakan tantangan baru bagi keamanan siber. Semakin banyak perangkat yang terhubung ke Internet, semakin besar potensi kerentanan yang dapat dieksploitasi oleh penyerang. Selain itu, penyerang dapat memanfaatkan teknologi seperti kecerdasan buatan dan komputasi awan untuk melancarkan serangan yang lebih canggih dan kompleks. b. Serangan Berasal dari Berbagai Pihak : Serangan siber dilakukan tidak hanya oleh individu atau kelompok tertentu, namun juga oleh negara atau kelompok terorganisir. Serangan-serangan ini dapat berupa pencurian data, sabotase, dan bahkan serangan siber yang dapat menghancurkan infrastruktur penting suatu negara. Meningkatnya intensitas dan variasi serangan meningkatkan kompleksitas perlindungan sistem dan data. c. Kekurangan Pakar Keamanan *Cyber*, Kekurangan pakar keamanan siber merupakan masalah serius. Permintaan akan tenaga profesional keamanan siber yang berkualifikasi jauh melebihi pasokan yang tersedia. Hal ini menciptakan kesenjangan dalam perlindungan dan membatasi kemampuan perusahaan untuk merespons dan mencegah serangan siber: a. Penyerang sering menggunakan teknik media sosial dalam serangannya. Mereka mengeksploitasi ketidaktahuan, kelalaian, atau kecerdasan emosional korban untuk mendapatkan akses tidak sah atau informasi sensitif. Metode paling populer yang digunakan oleh penyerang adalah serangan *phishing*, serangan *spear phishing*, atau serangan rekayasa sosial. b. Kerentanan pada sistem operasi, perangkat lunak, atau aplikasi merupakan kerentanan yang sering dieksploitasi oleh penyerang. Kerentanan yang tidak

terdeteksi atau perangkat lunak yang tidak diperbarui secara rutin dapat menjadi pintu gerbang serangan siber.

Cyber security telah menjadi elemen krusial dalam menjaga keamanan informasi di era digital. Beragam bentuk implementasi *cyber security* digunakan secara luas untuk melindungi data pribadi, sistem informasi, serta infrastruktur digital dari potensi ancaman yang terus berkembang. Berikut beberapa contoh implementasi *cyber security* yang umum diterapkan (Fa'izi, 2024): a. *Firewall dan Antivirus,* Digunakan sebagai perlindungan dasar pada perangkat untuk mendeteksi dan memblokir aktivitas berbahaya yang berasal dari malware, virus, dan ancaman siber lainnya. b. *Two-Factor Authentication* (2FA), Merupakan sistem verifikasi berlapis yang menambahkan keamanan tambahan saat proses autentikasi, dengan menggabungkan kata sandi dan kode verifikasi yang dikirim melalui SMS, email, atau aplikasi autentikasi. c. Sistem Keamanan Jaringan (VPN dan IDS), *Virtual Private Network* (VPN) berfungsi mengenkripsi lalu lintas jaringan untuk menjaga kerahasiaan data, sementara Intrusion Detection System (IDS) digunakan untuk memantau serta mendeteksi aktivitas mencurigakan dalam jaringan internal. d. *Enkripsi End-to-End,* Teknologi ini memastikan bahwa informasi yang dikirim hanya dapat diakses oleh pengirim dan penerima, sehingga dapat mencegah intersepsi atau penyadapan oleh pihak yang tidak berwenang. e. Keamanan *Cloud,* Digunakan untuk melindungi data yang disimpan dan dikelola melalui layanan berbasis *cloud*, dengan penerapan kontrol akses, autentikasi pengguna, serta enkripsi data guna menjaga integritas dan kerahasiaan informasi. f. Penerapan Tokenisasi dan Enkripsi pada Transaksi Digital, Dalam sistem transaksi keuangan digital seperti *e-wallet* dan *mobile banking*, data sensitif seperti nomor kartu kredit ditransformasikan menjadi token yang tidak memiliki arti di luar sistem, sehingga mengurangi risiko pencurian data selama transaksi berlangsung. g. Sertifikasi Digital dan *Secure Socket Layer* (SSL), Digunakan untuk memastikan keamanan dalam komunikasi antara pengguna dan server layanan keuangan digital, menjaga agar data yang dikirim tetap terlindungi dari modifikasi atau pencurian. h. Pemantauan Transaksi *Real-Time*, Lembaga keuangan menggunakan sistem berbasis AI untuk mendeteksi aktivitas mencurigakan seperti anomali transaksi yang dapat menunjukkan potensi fraud, dan segera melakukan mitigasi sebelum kerugian terjadi. i. Manajemen Akses dan Otentikasi Berbasis Risiko, Sistem keuangan digital menerapkan pengendalian akses berdasarkan tingkat risiko pengguna, lokasi, dan perangkat yang digunakan, guna membatasi akses terhadap data sensitif jika terdeteksi potensi ancaman.

Seiring dengan meningkatnya digitalisasi di berbagai sektor, jenis-jenis ancaman siber juga semakin beragam dan kompleks. Adapun beberapa jenis ancaman siber yang umum dijumpai meliputi : a. *Malware* , Merupakan perangkat lunak berbahaya yang dirancang untuk merusak atau mengakses sistem secara ilegal, seperti virus, worm, trojan horse, dan ransomware. b. *Phishing*, Teknik penipuan yang dilakukan dengan menyamar sebagai entitas tepercaya untuk mencuri data sensitif seperti username, password, atau data kartu kredit. c. *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), Serangan yang membanjiri server atau jaringan dengan lalu lintas palsu sehingga layanan menjadi tidak tersedia. d. *Man-in-the-Middle* (MitM) *Attack*, Serangan di mana pelaku menyusup di antara dua pihak yang berkomunikasi untuk mencuri atau memanipulasi data. e. SQL *Injection*, Teknik serangan yang mengeksploitasi celah keamanan pada database melalui perintah SQL berbahaya untuk mencuri atau mengubah informasi.

Sistem transaksi keuangan digital merupakan bagian dari sistem informasi akuntansi yang bertujuan untuk mencatat, mengelola, dan melaporkan transaksi keuangan secara elektronik

menggunakan teknologi informasi. Menurut (Susanto, 2015) dalam bukunya Sistem Informasi Akuntansi, sistem transaksi keuangan digital adalah "Sistem yang memproses transaksi keuangan dengan menggunakan teknologi informasi berbasis komputerisasi yang dirancang untuk memberikan informasi keuangan yang akurat dan tepat waktu."

Adapun pengertian pembayaran digital menurut (Azhari dkk., 2024) adalah sebuah alat yang menggunakan teknologi via ponsel untuk melakukan pembayaran, transfer, atau transaksi lainnya yang kini telah menggeser peran uang tunai. (Susanto, 2015) menyebutkan bahwa tujuan sistem informasi akuntansi berbasis digital adalah "Menyediakan informasi yang dibutuhkan manajemen dalam pengambilan keputusan, meningkatkan efisiensi operasional, serta menjaga keamanan dan integritas data keuangan."

Munculnya transaksi berbasis digital seperti internet banking, *mobile banking*, *e-wallet* dan transaksi digital lainnya menunjukkan bahwa lembaga jasa keuangan terus melakukan inovasi berbasis digital untuk memenuhi kebutuhan Masyarakat dan memenangkan persaingan global (Azizah, Ula, Mutiara, & Prameswari, 2024). Transformasi digital dalam dunia perbankan tidak hanya meningkatkan kenyamanan para nasabah namun juga mendorong inklusi keuangan dengan memberikan akses lebih luas pada masyarakat (Nur afifah, Faliha, & Simatangkir, 2025).

METODE PENELITIAN

Metode yang digunakan dalam penulisan artikel ini menggunakan pencarian Pustaka, yaitu mencari referensi melalui jurnal ilmiah, buku-buku, dan bahan publikasi yang relevan dengan keamanan siber (cyber security) dalam transaksi keuangan digital. Menurut (Sugiyono, 2016: 22) menyatakan bahwa literatur merupakan catatan peristiwa yang sudah berlalu yang berbentuk tulisan, gambar, atau karya-karya monumental dari seseorang. Dalam penelitian ini studi literatur dilakukan terhadap 28 sumber artikel jurnal yang terbit dalam kurun tahun 2018 hingga 2024 dan 1 buku.

Pada proses analisis data, penelitian ini menggunakan Teknik analisis kualitatif yang melibatkan proses mendalam untuk memahami, menginterpretasi, dan mengevaluasi konten dari berbagai sumber literatur. Metode kualitatif menurut (Sugiyono, 2011) adalah metode yang digunakan untuk meneliti objek alamiah yang dimana peneliti sebagai instrumen kunci dan analisis data bersifat induktif. Penelitian kualitatif lebih menekan pada makna daripada generalisasi. Teknik ini dilakukan untuk menarik sebuah kesimpulan dengan sumber acuan pada berbagai jurnal ilmiah yang telah dikaji untuk mendapatkan pemahaman yang komprehensif.

HASIL PENELITIAN DAN PEMBAHASAN

Implementasi *cyber security* dalam sistem transaksi keuangan digital menjadi kebutuhan fundamental seiring meningkatnya adopsi layanan keuangan berbasis teknologi seperti *internet banking*, *e-wallet*, *mobile banking*, dan *fintech*. Layanan-layanan ini sangat memudahkan masyarakat dalam melakukan transaksi, tetapi juga membuka potensi celah keamanan yang bisa dimanfaatkan pelaku kejahatan siber. Oleh karena itu, penerapan sistem keamanan digital yang efektif menjadi aspek penting yang tidak bisa diabaikan oleh lembaga keuangan digital.

Salah satu implementasi utama *cyber security* dalam sistem transaksi keuangan digital adalah penggunaan autentikasi berlapis, terutama *Two-Factor Authentication* (2FA). Teknologi ini memperkuat keamanan akun pengguna dengan memverifikasi identitas melalui dua tahapan—biasanya berupa *password* dan kode verifikasi yang dikirim ke perangkat pengguna. Menurut

studi oleh (Fa'izi, 2024), 2FA terbukti menurunkan risiko pembobolan akun hingga 80% karena memperkecil kemungkinan akun diakses hanya dengan satu kredensial.

Selain itu, lembaga keuangan digital juga menggunakan sistem pemantauan transaksi secara real-time yang berbasis *Artificial Intelligence* (AI). Sistem ini mampu mendeteksi pola anomali atau perilaku yang mencurigakan dalam aktivitas nasabah, seperti *login* dari lokasi tidak biasa atau jumlah transaksi yang melebihi batas wajar. Deteksi dini ini memungkinkan lembaga keuangan untuk melakukan *freeze* akun secara otomatis dan mencegah transaksi penipuan. (Samudra, Hidayat, & Wahyu, 2023) menyebut bahwa AI dalam monitoring transaksi digital telah meningkatkan efektivitas mitigasi kejahatan finansial di sektor perbankan.

Teknologi enkripsi *end-to-end* juga menjadi implementasi wajib dalam pengamanan data sensitif selama transaksi berlangsung. Dalam praktiknya, data seperti informasi kartu kredit atau PIN pengguna dienkripsi sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga meskipun berhasil disadap. Menurut studi oleh (Sugiarti, 2024) teknologi enkripsi telah menurunkan risiko pencurian data keuangan pada platform digital hingga 70%. Di sisi lain, penerapan *firewall, antivirus*, serta *intrusion detection system* (IDS) menjadi lapisan perlindungan dasar terhadap ancaman malware dan serangan siber lainnya. *Firewall* memblokir akses tidak sah ke jaringan, sementara IDS memantau aktivitas mencurigakan. Seperti diuraikan oleh (Azhari dkk., 2024) kombinasi sistem keamanan dasar ini penting untuk menjaga infrastruktur TI dari serangan yang bersifat *brute-force* atau DDoS.

Implementasi keamanan siber juga mencakup pengamanan data di cloud. Banyak lembaga keuangan saat ini menyimpan data di layanan cloud karena skalabilitasnya. Namun, tanpa kontrol akses yang tepat, data ini rentan dicuri. Oleh karena itu, digunakan teknologi seperti tokenisasi, yaitu proses menggantikan informasi sensitif dengan kode unik (token) yang tidak bisa dimanfaatkan di luar sistem. Penggunaan token ini secara signifikan meningkatkan keamanan transaksi *e-wallet* dan *mobile banking* sebagaimana ditunjukkan oleh penelitian (Muslim, 2024).

Sertifikasi digital dan penerapan protokol SSL (*Secure Socket Layer*) juga menjadi kunci dalam menjamin keamanan komunikasi antara pengguna dan server lembaga keuangan. SSL mencegah serangan seperti *man-in-the-middle* yang berusaha mencuri informasi saat proses pertukaran data berlangsung. (Sari R. P., 2024) mencatat bahwa hampir seluruh transaksi digital modern kini berjalan di atas protokol HTTPS yang menggunakan SSL sebagai standar pengamanan komunikasi. Namun, keberhasilan implementasi *cyber security* juga bergantung pada regulasi dan kepatuhan lembaga terhadap kebijakan yang berlaku. Di Indonesia, Undang-undang Perlindungan Data Pribadi (UU PDP) dan Peraturan OJK menjadi dasar hukum yang mewajibkan penerapan keamanan data.

Maka dari itu di era digitalisasi sistem keuangan yang semakin masif, keamanan siber menjadi elemen fundamental yang tidak dapat diabaikan. Artikel ini secara khusus membahas bagaimana implementasi *cyber security* diterapkan dalam sistem transaksi keuangan digital, dengan menyoroti dua contoh utama yang paling banyak digunakan masyarakat, yaitu *mobile banking* dan *e-wallet*. Kedua layanan ini menjadi representasi nyata dari transformasi digital di sektor keuangan, sekaligus menghadirkan tantangan serius terkait perlindungan data dan pencegahan tindak kejahatan siber. Oleh karena itu, pembahasan berikut akan menguraikan secara rinci strategi dan praktik keamanan digital yang diterapkan pada masing-masing layanan, untuk melihat sejauh mana keamanan pengguna dapat dijamin di tengah meningkatnya ancaman cybercrime.

1. Implementasi *Cyber Security* pada *Mobile Banking*

Kemajuan teknologi digital telah mengubah cara masyarakat dalam mengakses layanan keuangan. Aplikasi keuangan *mobile* seperti *mobile banking*, dompet digital, hingga layanan *fintech* memberikan kemudahan dalam bertransaksi. Namun, di balik kenyamanan tersebut, muncul tantangan serius dalam bentuk ancaman keamanan digital. Penelitian oleh (Azizah, Ula, Mutiara, & Prameswari, 2024) menggaris bawahi pentingnya *cyber security* sebagai fondasi utama dalam pengembangan aplikasi keuangan *mobile*.

Kasus nyata seperti serangan *ransomware* terhadap Bank Syariah Indonesia (BSI) tahun 2023 menjadi contoh betapa seriusnya risiko keamanan yang dihadapi. Data 15 juta nasabah bocor dan operasional lumpuh selama beberapa hari. Hal ini menunjukkan bahwa tanpa sistem keamanan berlapis, aplikasi keuangan *mobile* sangat rentan terhadap eksploitasi oleh peretas.

Untuk menanggulangi ancaman ini, implementasi *cyber security* dalam aplikasi *mobile* dilakukan melalui berbagai strategi teknis dan manajerial. Strategi pertama adalah penerapan *firewall*, yang bertindak sebagai sistem penyaring lalu lintas jaringan agar hanya aktivitas legal yang diizinkan. *Firewall* juga mencegah akses ilegal ke server aplikasi, sehingga memperkecil kemungkinan *malware* masuk ke dalam sistem.

Strategi kedua adalah integrasi *blockchain* sebagai sistem pencatatan transaksi yang transparan dan tidak dapat dimanipulasi. Dalam konteks keamanan *mobile, blockchain* membantu memastikan bahwa data tidak dapat diubah tanpa izin seluruh jaringan, yang penting dalam memverifikasi transaksi dan melindungi informasi pengguna dari manipulasi. Ketiga, pentingnya penerapan manajemen risiko yang kuat. Hal ini meliputi kebijakan keamanan internal, prosedur operasional standar (SOP), dan pengendalian internal yang konsisten. Sistem pencadangan data berlapis dan penyimpanan terdistribusi juga direkomendasikan agar data tetap aman jika terjadi gangguan di satu titik. Selanjutnya, penguatan mekanisme autentikasi, seperti *Three-Factor Authentication* (3FA), menjadi krusial. Selain *password* dan perangkat, aplikasi perlu menambahkan elemen biometrik seperti sidik jari atau pemindai wajah untuk memperkuat identifikasi pengguna. Autentikasi berlapis ini sangat efektif dalam mencegah akses ilegal, bahkan jika satu lapisan keamanan berhasil ditembus. Investasi dalam infrastruktur jaringan yang aman dan andal juga sangat dianjurkan. Jaringan yang menggunakan single secure gateway lebih mudah dimonitor dibanding *open gateway*. Hal ini memungkinkan deteksi dini terhadap aktivitas mencurigakan dan respon yang cepat. Implementasi *cyber security* yang baik juga memerlukan keberadaan tim keamanan siber internal. Tim ini bertanggung jawab atas monitoring aktivitas jaringan, audit berkala, serta penyusunan dan pengembangan kebijakan keamanan yang relevan. (Azizah, Ula, Mutiara, & Prameswari, 2024)

Adapun berdasarkan penelitian oleh (Priyadi, 2023), implementasi cyber security dalam mobile banking diukur melalui enam dimensi PIECES: *Performance, Information, Economy, Control, Efficiency,* dan *Service*, dengan responden pengguna *BCA Mobile, BRImo, dan Livin' by Mandiri*. Dari aspek *Performance* (Kinerja), seluruh aplikasi *mobile banking* menunjukkan hasil sangat baik dalam hal kemudahan navigasi dan kecepatan akses. Pengguna merasa fitur-fitur seperti monitoring transaksi mencurigakan dan transaksi multifungsi (transfer, pembayaran, top-up) berjalan dengan efisien. Ini menunjukkan bahwa keamanan sistem juga mendukung kinerja aplikasi tanpa menurunkan pengalaman pengguna.

Pada dimensi *Information* (Informasi), fitur notifikasi real-time menjadi salah satu indikator penting. *Mobile banking* seperti *BRImo* dan *Livin' by Mandiri* secara aktif memberikan peringatan melalui SMS dan email saat login mencurigakan atau transaksi dilakukan. Ini merupakan bagian dari implementasi *real-time alert system* yang menjadi standar keamanan siber

global (Priyadi, 2023). Aspek *Economy* (Ekonomi) dinilai dari keterbukaan biaya transaksi dan efisiensi waktu. Seluruh aplikasi dinilai baik karena tidak membebani pengguna dengan biaya tambahan tersembunyi dan memungkinkan transaksi dilakukan dengan cepat. Ini secara tidak langsung mendukung keamanan melalui transparansi proses.

Dimensi *Control* (Pengendalian dan Keamanan) menjadi fokus utama dalam implementasi cyber security. Hasil penelitian menunjukkan bahwa seluruh aplikasi *mobile banking* telah menerapkan sistem otentikasi yang ketat, seperti penggunaan password pada setiap transaksi dan pembatasan akses hanya pada perangkat terdaftar. Ini merupakan bentuk kontrol akses berbasis perangkat yang terbukti mengurangi risiko pembobolan, termasuk teknik serangan SIM *Swap* atau *phishing*. Untuk *Efficiency* (Efisiensi), BRImo mendapatkan skor tertinggi. Pengguna menilai bahwa sistem autentikasi dan pengelolaan data perbankan dilakukan dengan cepat dan tidak berulang. Fitur seperti *session timeout* otomatis juga menunjukkan bahwa aplikasi telah didesain untuk mencegah akses tidak sah jika pengguna lalai menutup sesi.

Namun, pada dimensi *Service* (Layanan), seluruh aplikasi mencatat skor yang relatif lebih rendah. Masalah jaringan, kesulitan akses ke pusat bantuan, dan terbatasnya fitur *live chat* atau pengaduan langsung menunjukkan bahwa aspek pelayanan pelanggan belum sejalan dengan sistem keamanan yang telah diterapkan. Ini penting diperhatikan karena *cyber security* juga mencakup manajemen insiden yang cepat dan responsif. Secara keseluruhan, nilai rata-rata tingkat kepuasan pengguna terhadap *cyber security* pada *mobile banking* mencapai kategori "baik": BCA Mobile (3,86), BRImo (3,93), dan Livin' by Mandiri (3,84) dari skala 5. Ini menunjukkan bahwa pengguna merasa cukup yakin terhadap keamanan data dan sistem yang digunakan pada *mobile banking* di Indonesia. (Priyadi, 2023)

Kesimpulannya, implementasi *cyber security* pada layanan *mobile banking* telah mencakup berbagai komponen penting seperti autentikasi ganda, enkripsi, dan pemantauan aktivitas mencurigakan. Namun, perlu ada perbaikan pada aspek layanan pelanggan dan peningkatan *awareness* pengguna agar tidak hanya sistemnya yang kuat, tetapi juga penggunanya semakin sadar akan pentingnya keamanan digital.

2. Implementasi *Cyber Security* pada *E-Wallet*

Secara global, *e-wallet* menjadi pendorong utama dalam perubahan yang membawa kemudahan dalam transaksi antara penjual dan pembeli. Pertumbuhan *e-wallet* dipengaruhi oleh berbagai faktor diantaranya kemajuan teknologi, perubahan perilaku konsumen, serta inisiatif penyedia *e-wallet* dan pemerintah untuk mendorong teknologi keuangan yang canggih (Putra, Rahma, & Wahyuni, 2024). Adapun beberapa penyedia e-wallet yang sering digunakan di Indonesia antara lain: *Gopay, Dana, OVO, LinkAja, dan Shopeepay*.

Perkembangan *e-wallet* sebagai alat transaksi digital modern telah membawa perubahan signifikan dalam perilaku keuangan masyarakat. Kemudahan dalam melakukan pembayaran, pembelian, dan transfer dana menjadi keunggulan utama. Namun, kemudahan ini juga menimbulkan tantangan serius terkait keamanan data dan perlindungan terhadap ancaman siber. Dan untuk mengatasi tantangan-tantangan ini, perusahaan memerlukan pendekatan keamanan siber yang seimbang dan aktif (Dr. Joseph, 2023: 147).

Adapun kasus yang menimpa warga Medan bernama Rolas Naibaho menjadi korban *phishing* setelah melihat postingan bersponsor melalui platform media sosial yang menawarkan pembuatan kartu *e-money*. Ia diarahkan ke halaman login palsu Dana melalui browser, memasukkan nomor ponsel, password, dan kode OTP, hingga tanpa sadar mengizinkan akses ke akunnya hingga berakibat kehilangan Rp 1,8 juta tanpa persetujuannya. Kasus ini menunjukkan

betapa rentannya pengguna terhadap postingan bersponsor palsu yang menyamar sebagai layanan resmi, dan menegaskan pentingnya kewaspadaan dan perlindungan oleh penyedia e-wallet.

Menurut (Azhari dkk., 2024), manajemen sekuriti menjadi faktor krusial dalam menjaga kepercayaan dan keselamatan pengguna *e-wallet*. Implementasi manajemen sekuriti dalam transaksi e-wallet bertujuan untuk memastikan keamanan informasi sensitif, seperti data pribadi, nomor kartu kredit, dan riwayat transaksi pengguna. Strategi pertama yang digunakan adalah enkripsi data, yakni proses mengubah data menjadi bentuk tidak terbaca oleh pihak ketiga. Enkripsi ini diterapkan baik saat data disimpan maupun saat dikirimkan melalui jaringan, sehingga mengurangi risiko pencurian data oleh peretas. Selanjutnya, otentikasi multifaktor (MFA) merupakan lapisan keamanan tambahan yang telah banyak diadopsi oleh penyedia layanan *e-wallet*. Sistem ini memverifikasi identitas pengguna dengan menggabungkan dua atau lebih metode: seperti *password*, OTP (*One-Time Password*), dan *biometrik* (sidik jari atau pemindai wajah). MFA terbukti sangat efektif dalam mencegah akses ilegal bahkan ketika kredensial utama pengguna dicuri.

Langkah berikutnya adalah pemantauan transaksi secara *real-time*. Sistem ini dirancang untuk mendeteksi perilaku mencurigakan, seperti jumlah transaksi yang tidak biasa, lokasi akses yang berbeda dari biasanya, atau aktivitas *login* berturut-turut. Ketika sistem mendeteksi anomali, tindakan otomatis seperti pembatasan akses atau notifikasi ke pengguna segera dilakukan. Pembaruan sistem secara berkala juga menjadi elemen penting dalam strategi keamanan. Kerentanan sering muncul akibat penggunaan perangkat lunak yang usang atau tidak ditambal. Dengan melakukan *patching* dan *update* sistem secara rutin, penyedia layanan dapat menutup celah keamanan yang mungkin dimanfaatkan oleh peretas.

Untuk mengatasi ancaman eksternal seperti *phishing* dan *malware, e-wallet* dilengkapi dengan proteksi tambahan, seperti filter domain palsu, pemblokir situs berbahaya, dan sistem deteksi *malware*. Serangan seperti ini biasa digunakan untuk mencuri kredensial pengguna melalui email atau situs palsu, dan menjadi ancaman serius di era digital. Di luar aspek teknis, pendidikan dan kesadaran pengguna menjadi bagian penting dari manajemen sekuriti. Banyak serangan terjadi karena kelalaian pengguna, seperti membagikan OTP atau menggunakan kata sandi lemah. Oleh karena itu, edukasi tentang praktik keamanan digital seperti penggunaan aplikasi resmi, tidak mengklik tautan mencurigakan, dan menjaga kerahasiaan informasi *login* menjadi sangat penting.

Dari sisi organisasi, tim keamanan siber internal bertanggung jawab dalam menilai dan mengelola risiko, merespons insiden keamanan, dan memastikan kepatuhan terhadap standar keamanan. Audit sistem, simulasi serangan (*penetration testing*), dan pelatihan rutin kepada staf dilakukan untuk memastikan sistem keamanan selalu dalam kondisi optimal. Dalam Penelitian (Azhari dkk., 2024) juga menekankan pentingnya penggunaan teknologi tokenisasi, yag menggantikan data sensitif seperti nomor kartu dengan kode unik (token) yang tidak memiliki nilai di luar sistem. Ini menambah lapisan proteksi saat transaksi berlangsung. Penerapan seluruh praktik ini menunjukkan bahwa manajemen sekuriti bukan sekadar proteksi teknis, tetapi pendekatan holistik yang mencakup kebijakan, teknologi, infrastruktur, dan literasi pengguna. Hasilnya*, e-wallet* menjadi lebih aman, kredibel, dan dapat dipercaya sebagai alat pembayaran digital utama di era modern.

Kesimpulannya, Perkembangan *e-wallet* sebagai alat transaksi digital menerapkan beberapa strategi yang meliputi enkripsi data, penggunaan otentikasi multi-faktor, serta pemantauan transaksi secara *real-time*. Selain itu, pembaruan sistem secara berkala dan teknologi tokenisasi turut memperkuat perlindungan menyeluruh. Dengan pendekatan yang meliputi aspek

teknis, kebijakan, serta literasi digital, *e-wallet* dapat menjadi platform pembayaran yang aman dan terpercaya di era digital saat ini.

3. Implementasi Cyber Security pada QRIS

Menurut Susanti dalam jurnal (Azhari dkk., 2024) dompet digital atau *e-wallet* merupakan jenis teknologi keuangan yang membuat pembayaran lebih mudah dan nyaman bagi konsumen. Saat ini, layanan dompet digital sudah tidak asing lagi bagi Masyarakat karena sudah menjadi bagian dari kehidupan sehari-hari. berdasarkan hasil laporan *E-wallet Industry Outlook* 2023 melalui *website Jubelio*, 74% masyarakat telah menggunakan dompet digital. Gopay sebagai salah satu dompet digital berhasil meraih posisi tertinggi apabila dibandingkan dengan OVO, Dana, serta *Shopeepay*. Bukan hanya sebagai alat bantu pengguna, dompet digital juga berhasil mengambil alih sebagian sistem pembayaran dalam beberapa sektor. Bahkan, tidak sedikit pelaku usaha yang hanya menerima pembayaran melalui metode ini.

Dengan adanya *e-wallet*, Masyarakat dapat bertransaksi melalui fitur *scan* kode QR atau *Quick Response* yang penggunaanya sangat mudah dan praktis. Dalam jurnal (Bodhi & Tan, 2022) pada tanggal 1 Januari 2020 Bank Indonesia bersama Asosiasi Sistem Pembayaran meresmikan sistem kode QR yang dinamai QRIS (*Quick Response Code Indonesia*) sebagai salah satu metode pembayaran di Indonesia. Adapun latar belakang pembuatan QRIS ini disebabkan banyaknya pihak pedagang yang memberikan kode QR dari berbagai jasa pembayaran saat pelanggan melakukan transaksi *cashless* atau tanpa tunai. Kemudian dari situlah muncul tujuan untuk mendorong efisiensi transaksi, melajukan inklusi keuangan, mendorong pertumbuhan ekonomi untuk Indonesia maju. Adapun pengaturan mengenai QRIS diatur dalam "Peraturan Anggota Dewan Gubernur Nomor 23/8/PADG/2021" tentang perubahan atas Peraturan Anggota Dewan Gubernur Nomor 21/18/PADG/2019 tentang Implementasi Standar Nasional *Quick Response Code Indonesia* untuk pembayaran.

Meningkatnya jumlah pengguna QRIS tentunya menunjukkan bahwa pembayaran lebih nyaman dan cepat karena metodenya sangat mudah untuk dipelajari, dengan sekali tekan dan mengarahkan kamera pada *barcode*, transaksi sudah berhasil dilakukan. Namun tentunya dibalik kemudahan, keuntungan, serta manfaat pada metode ini, terdapat akibat yang muncul salah satunya yaitu *scam* atau penipuan seperti *phising* dimana pelaku mengganti kode QR asli dengan versi yang telah dimodifikasi untuk mencuri informasi pengguna. Manipulasi kode QR telah berkembang yang dimana tidak hanya mengganti kode QR fisik, tetapi juga menggunakan teknik *social engineering* untuk meyakinkan korban melakukan transaksi ke rekening yang salah.

Salah satu kasus *phishing* dalam sistem pembayaran QRIS yaitu salah satunya melibatkan penyalahgunaan kode QR yang dimana QR tersebut hanya bisa dipindai menggunakan *Google Lens*. Kode tersebut kemudian mengarahkan pengguna ke situs *phishing* yang domainnya dapat dipalsukan menjadi mobile banking yang meminta informasi sensitif seperti username, password, dan PIN. Jika kode itu dipindai melalui aplikasi resmi seperti *mobile banking* atau *e-wallet*, sistem tidak mengenalinya dan menampilkan pesan kesalahan. Pakar keamanan siber, Alfons Tanujaya menegaskan kejadian tersebut memanfaatkan kode QR palsu untuk memanipulasi pengguna.

Adapun pengimplementasian dalam sistem keamanan QRIS harus menggunakan keamanan berlapis yaitu *Multi-Factor Authentication* (MFA) yang tidak hanya mengandalkan *password* atau PIN, tetapi juga memanfaatkan biometrik, token fisik, atau verifikasi melalui perangkat sekunder. MFA juga banyak digunakan oleh banyak penyedia layanan *e-wallet* karena terbukti sangat efektif dalam mencegah akses *illegal*.

Enkripsi *end-to-end* juga menjadi fondasi penting dalam melindungi integritas data transaksi. Enkripsi yang diterapkan tidak hanya pada level transmisi data, tetapi juga dalam

penyimpanan serta memproses informasi. Selain itu, implementasi teknologi *blockchain* juga menunjukkan potensi besar sebagai solusi jangka panjang yang dimana setiap transaksi dapat dicatat secara transparan, sehingga meminimalkan risiko *fraud*.

Kemudian yang terakhir, standar keamanan harus disertai dengan mekanisme audit dan *monitoring* yang efektif untuk memastikan sistem keamanan terkendali dan optimal. Edukasi mengenai praktik keamanan digital pun sangat penting dan tidak bisa dilewatkan karena program ini menjadi komponen kritis dalam implementasi *cyber security*. Adapun edukasi harus mencakup penggunaan aplikasi resmi, menjaga kerahasiaan informasi *login*, identifikasi tanda-tanda penipuan, praktik keamanan digital yang baik, dan pemahaman mengenai hak-hak privasi. Edukasi ini tidak hanya ditujukan untuk pengguna individu, tetapi juga untuk pelaku usaha yang menjadi bagian dari ekosistem QRIS.

Kesimpulannya, ancaman seperti phishing, manipulasi kode QR, dan teknik *social engineering* menunjukkan bahwa risiko penyalahgunaan tetap tinggi jika tidak ditangani secara tepat. Oleh karena itu, implementasi keamanan siber dalam QRIS harus menjadi prioritas utama. Pendekatan pengamanan berlapis, seperti penggunaan *Multi-Factor Authentication* (MFA) dan enkripsi *end-to-end*, terbukti mampu memperkuat sistem dari potensi akses ilegal. Selain itu, pemanfaatan teknologi *blockchain* menjadi solusi strategis untuk memastikan transparansi dan akurasi dalam pencatatan transaksi. Langkah-langkah ini perlu dilengkapi dengan audit rutin, *monitoring* berkala, serta edukasi menyeluruh kepada pengguna dan pelaku usaha mengenai praktik keamanan digital yang baik.

KESIMPULAN

Implementasi *cyber security* dalam sistem transaksi keuangan digital merupakan suatu keharusan mutlak di era transformasi digital yang semakin pesat. Ancaman terhadap keamanan siber semakin kompleks dan bervariasi, seiring meningkatnya penggunaan layanan seperti *mobile banking, e-wallet*, dan *fintech*. Oleh karena itu, lembaga keuangan harus mampu menerapkan sistem perlindungan digital yang tidak hanya bersifat teknis, tetapi juga strategis dan berkelanjutan, dengan tetap memperhatikan aspek regulasi dan edukasi kepada pengguna. Dari pembahasan diatas ada berbagai strategi yang digunakan untuk memperkuat sistem keamanan digital, seperti penggunaan enkripsi *end-to-end, two-factor authentication, intrusion detection system*, hingga penerapan teknologi seperti *blockchain* dan *tokenisasi*. Selain teknologi, peran kebijakan internal, tim keamanan siber, dan audit berkala juga menjadi bagian integral dari sistem pertahanan siber yang efektif. Penggunaan sistem *monitoring* berbasis AI turut memperkuat deteksi dan respons terhadap aktivitas mencurigakan secara *real-time*. Studi kasus pada layanan *mobile banking, e-wallet*, dan QRIS menunjukkan bagaimana penerapan keamanan siber bisa dilakukan secara nyata tanpa mengorbankan kenyamanan pengguna. Aspek seperti kontrol, efisiensi, dan performa tetap terjaga jika sistem dirancang dengan cermat dan responsif. Meski demikian, tantangan masih ada, seperti kurangnya pelayanan pelanggan yang sigap, rendahnya literasi digital di sebagian masyarakat, serta keterbatasan tenaga ahli di bidang keamanan siber. Dengan demikian, keberhasilan sistem transaksi keuangan digital tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kemampuan lembaga keuangan dalam membangun ekosistem yang aman, andal, dan dipercaya oleh pengguna. *Cyber security* bukan sekadar pelindung teknis, tetapi merupakan fondasi utama dalam menjaga kepercayaan publik, mendorong inklusi keuangan, dan memastikan keberlangsungan sistem keuangan digital yang berintegritas di Indonesia. Akhirnya, keberhasilan implementasi *cyber security* dalam QRIS tidak

bisa berdiri sendiri, tetapi memerlukan kolaborasi erat antara pemerintah, penyedia layanan, institusi keuangan, dan masyarakat.

DAFTAR PUSTAKA

Andhika. (2023, April 11). *Pilar Utama dalam Cyber Security: Mengenal Confidentiality, Integrity, dan Availability*. Retrieved from Fourtrezz: https://fourtrezz.co.id/tiga pilarutama-dalam-cyber-security-mengenal-confidentiality-integrity-dan-availability/

Angsito, F. K. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, 99-110.

Azhari dkk. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-Wallet. *Jurnal Kewirausahaan dan Multi Talenta (JKMT)*, 138-147.

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan Siber sebagai Fondasi Pengembangan Aplikasi Keuangan Mobile : Studi literatur mengenai cybercrime dan mitigasinya. *Jurnal Akuntansi dan Teknologi Informasi*, 221-237.

Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cybercrime). *Unes Law Review*, 297-308.

Dr. Joseph Teguh Santoso, S. M. (2023). *Teknologi Keamanan Siber (Cyber Security)*. Semarang: Yayasan Prima Agus Teknik .

Fa'izi, M. B. (2024, Desember 02). *Pentingnya Cybersecurity Awareness*. Retrieved from Cloud Computing Indonesia: https://www.cloudcomputing.id/pengetahuandasar/cybersecurity-awareness

Farmita, A. R. (2024, November 21). *Menyesatkan, Video Modus Pencurian Data dengan QRIS*. Retrieved from Tempo: https://www.tempo.co/cekfakta/menyesatkan-video modus-pencurian-data-dengan-qris--1171497

Feriyanto, O., Qur'anisa, Z., Herawati, M., Lisvi, & Putri, M. H. (2024). Peran Fintech Dalam Meningkatkan Akses Keuangan di Era Digital. *GEMILANG : Jurnal Manajemen dan Akuntansi*, 99-114.

Muslim, A. S. (2024). Analisis Keamanan Siber (Cyber Security) Dalam Era Digital "Tantangan Dan Strategi Pengamanan". *Jurnal Ilmu 13 Komputer, XIII*, Februari. Retrieved from https://com.ojs.co.id/index.php/jikr/article/view/116

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

Permatasari, D. (2021, Agustus 31). *Tantangan Cyber Security di Era Revolusi Industri 4.0*. Retrieved from Kementrian Keuangan: https://www.djkn.kemenkeu.go.id/kanwilsulseltrabar/baca-artikel/14190/tantangan cyber-security-di-era-reavolusi-industri- 40.html

Priyadi, W. (2023). Analisis Cyber Security Pada Pengguna Mobile Banking Di Indonesia . *Bina Insani ICT Journal*.

Putra, A. N., Rahma, F., & Wahyuni, E. G. (2024). Kajian Literatur: Kesadaran Keamanan Siber

pada Pengguna E-Wallet. *SNESTIK*, 404-411.

Rania, D. (2024, April 5). *Survei Dompet Digital Paling Favorit di Indonesia [2024]*. Retrieved from Jubelio Blog: https://jubelio.com/hasil-survei-dompet-digital-palingfavorit-di indonesia/

Rizki. (2024, Agustus 23). *Pentingnya Cybersecurity Dalam Era Digital*. Retrieved from PT Rizki Tujuhbelas Kelola: https://r17.co.id/en/blog/apa-itu-cybersecurity-pengertiandan pentingnya-dalam-era-digital

Samudra, Y., Hidayat, A., & Wahyu, M. F. (2023). Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital. *AMMA : Jurnal Pengabdian Masyarakat*, 1594-1601.

Sari, R. N. (2020, November 3). *Kilas Balik Pembobolan Rekening Ilham Bintang, Gunakan Nomor Ponsel hingga Rugi Ratusan Juta Rupiah*. Retrieved from Kompas.com: https://megapolitan.kompas.com/read/2020/07/08/18275931/kronologi-ilham-bintangkehilangan-ratusan-juta-rupiah-akibat-pembobolan

Sari, R. P. (2024, April 30). *Apa itu Cyber Security? Pengertian, Jenis, dan Ancamannya*. Retrieved from Cloud Computing Indonesia: https://www.cloudcomputing.id/pengetahuan-dasar/apa-itu-cyber-security

Sugiarti, U. (2024, September 11). *Cyber Security: Definisi, Jenis, Ancaman, dan Solusi Pencegahannya*. Retrieved from Lowencon: https://www.lawencon.com/cybersecurity/#:~:text=Fungsi%20dari%20cyber%20secur ity%20akan,dan%20berinteraksi %20dengan%20sistem%20digital.

Sugiyono, P. D. (2016). M*etodologi Penelitian Kuantitatif, Kualitatif, dan R & D*. Bandung: Alfabeta.

Sugiyono. (2011). *Metode penelitian kualitatif*. Bandung: R&D.

Sukarna, M. (2022). Analisis Keamanan dan Privasi dalam Transaksi Menggunkan QRIS : Tantangan dan Solusi. *Jurnal Manajemen Riset Bisnis Indonesia*, 37-46.

Susanto, A. (2015). *Sistem Informasi Akuntansi*. Bandung: Lingga Jaya.

Syahputra, A. (2023, Juni 14). *Tertipu Postingan IG, Warga Medan Kehilangan Rp 1,8 Juta dari e-Money*. Retrieved from Detik: https://www.detik.com/sumut/hukum-dan kriminal/d-6771674/tertipu-postingan-ig-warga-medan-kehilangan-rp-1-8-juta-dari-e money