Jurnal Ilmiah
Teknologi Informasi dan Robotika

ISSN (Online): 2686-4339
Volume 7 Nomor 1, Juni 2025
Halaman: 11-22

Evaluasi Keamanan Aplikasi Mobile Banking: Ancaman, Perlindungan dan Studi Kasus Pada Sistem Perbankan Digital

*Nur Aziza, Dyah Febria Wardhani

Universitas Islam Negeri Antasari Banjarmasin, Indonesia

Artikel Histori:
Disubmit: Maret 2025
Diterima: Mei 2025
Diterbitkan: Juni 2025

DOI
10.33005/jifti.v7i1.184

ABSTRAK

Keamanan aplikasi mobile banking merupakan isu krusial di era digital, seiring dengan meningkatnya jumlah pengguna dan kompleksitas ancaman siber yang dapat membahayakan integritas serta kerahasiaan data nasabah. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan aplikasi mobile banking dengan mengidentifikasi potensi ancaman serta menelaah strategi mitigasi yang diterapkan. Kebaruan dari penelitian ini terletak pada pendekatan komprehensif terhadap celah keamanan yang belum banyak dibahas secara mendalam dalam studi sebelumnya, terutama yang berkaitan dengan manajemen sesi pengguna dan eksploitasi perangkat lunak berbahaya. Metode yang digunakan adalah library research, dengan menganalisis berbagai literatur akademik, laporan industri keamanan, dan hasil penelitian terdahulu terkait sistem perbankan digital. Hasil menunjukkan bahwa sebagian besar aplikasi telah menerapkan enkripsi data dan autentikasi berlapis, namun masih rentan terhadap serangan man-in-the-middle, injeksi kode berbahaya, serta serangan berbasis malware. Kesimpulan dari penelitian ini menekankan pentingnya penguatan sistem keamanan melalui penerapan autentikasi multifaktor, algoritma enkripsi yang lebih kuat, serta peningkatan literasi dan kesadaran pengguna terhadap praktik keamanan digital yang baik.

Kata Kunci: Keamanan Mobile Banking; Ancaman Siber; Enkripsi Data; Autentikasi; Malware

How to Cite:
Aziza, N., Wardhani, D. F. (2025). Evaluasi Keamanan Aplikasi Mobile Banking: Ancaman, Perlindungan dan Studi Kasus Pada Sistem Perbankan Digital. *Jurnal Ilmiah Teknologi Informasi dan Robotika, 7*(1), 11-22. https://doi.org/10.33005/jifti.v7i1.184.

***Corresponding Author:**
Email : azizaalhusain966@gmail.com
Alamat : Jenderal Ahmad Yani KM. 4,5 Banjarmasin, Kalimantan Selatan, Indonesia 70235

PENDAHULUAN

Perkembangan teknologi digital telah mendorong transformasi signifikan dalam sektor perbankan, terutama melalui adopsi mobile banking yang memberikan kemudahan akses terhadap layanan keuangan bagi nasabah. Digitalisasi ini telah mengubah sistem operasional perbankan dari metode manual menuju platform digital yang lebih efisien dan fleksibel. Generasi milenial, yang memiliki tingkat literasi teknologi tinggi, menjadi pendorong utama dalam peningkatan penggunaan layanan mobile banking. Namun demikian, di balik kemudahan tersebut, aspek keamanan tetap menjadi tantangan utama yang berpotensi memengaruhi tingkat kepercayaan dan kepuasan nasabah (Kitsios dkk., 2021; Zakiah, 2023).

Isu keamanan dalam layanan mobile banking menjadi semakin krusial seiring meningkatnya ancaman siber yang menargetkan data pribadi dan informasi keuangan pengguna. Berbagai jenis serangan siber seperti malware, phishing, dan social engineering masih menjadi ancaman serius yang dapat membahayakan integritas sistem perbankan. Rendahnya kesadaran pengguna terhadap praktik keamanan informasi turut memperbesar risiko kebocoran data. Oleh karena itu, edukasi mengenai keamanan siber menjadi langkah penting dalam meningkatkan kesadaran dan perlindungan pengguna (Anastasiah & Pandia, 2024; Faizal dkk., 2023).

Dalam konteks mitigasi risiko, pemanfaatan kecerdasan buatan telah diidentifikasi sebagai strategi yang efektif dalam mendeteksi dan menganalisis potensi serangan siber secara real-time. Selain itu, komunikasi risiko yang efektif serta pelatihan bagi karyawan turut berperan penting dalam memperkuat sistem keamanan internal perbankan. Kolaborasi antarlembaga keuangan melalui platform seperti information sharing and analysis center (isac) juga menjadi mekanisme strategis dalam meningkatkan efektivitas deteksi dan respons terhadap ancaman siber (Fitria & Mutijarsa, 2023; Putra & Aferudin, 2022).

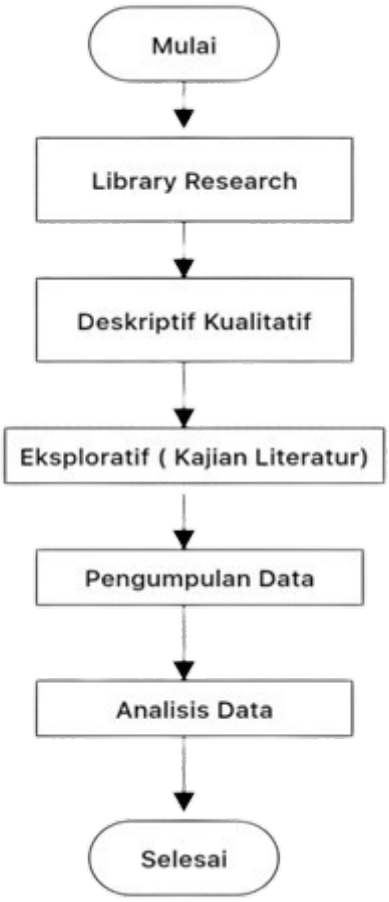
Serangan seperti man-in-the-middle, injeksi kode berbahaya, dan penyebaran malware menjadi tantangan teknis yang signifikan bagi keamanan mobile banking. Serangan-serangan ini memungkinkan pihak tidak bertanggung jawab untuk mengintersepsi komunikasi, mengeksploitasi kerentanan aplikasi, serta mencuri data sensitif milik pengguna. Untuk mengantisipasi hal tersebut, evaluasi keamanan secara berkala menggunakan metode owasp menjadi langkah penting dalam mendeteksi dan menutup celah keamanan yang ada. Penerapan algoritma enkripsi yang lebih kuat dan penggunaan autentikasi multi-faktor (mfa) juga dinilai efektif dalam meningkatkan perlindungan data serta mengurangi risiko akses tidak sah (Maharani & Suciati, 2024; Sam dkk., 2024).

Lebih lanjut, pengembangan sistem berbasis blockchain dapat menjadi alternatif inovatif dalam peningkatan keamanan mobile banking, karena menawarkan transparansi serta integritas data yang lebih tinggi. Di samping itu, regulasi yang ketat dan kerja sama antarpemangku kepentingan menjadi elemen penting dalam menjaga kepercayaan nasabah dan menjamin keamanan transaksi digital. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi tingkat keamanan aplikasi mobile banking melalui pendekatan library research dengan menganalisis berbagai literatur akademik, laporan keamanan, serta studi terkait sistem keamanan mobile banking. Melalui analisis ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai potensi ancaman

serta strategi mitigasi yang dapat diterapkan untuk meningkatkan perlindungan data dan transaksi pengguna (Abubakar & Handayani, 2022; Maulani dkk., 2023).

METODE PENELITIAN

Penelitian ini menggunakan metode library research karena sesuai denghan tujuan kajian yang bersifat teoritis dan konseptual. Metode ini dilakukan dengan mengumpulkan dan menganalisis berbagai literatur ilmiah seperti jurnal, laporan keamanan, dan studi relevan yang membahas isu-isu keamanan pada aplikasi mobile banking. Library research dipilih karena memungkinkan penyusunan pemahaman yang mendalam dan sistematis mengenai dinamika ancaman siber serta strategi mitigasi yang diterapkan. Melalui pendekatan ini, penelitian mengkaji aspek teknis seperti enkripsi dan autentikasi, serta aspek kebijakan seperti regulasi dan kesadaran pengguna. Struktur pendekatan ini bertujuan untuk mendukung proses penelitian agar berjalan lebih terarah, sistematis, dan berbasis pada sumber-sumber terpercaya. Tahapan penelitian tersebut disusun secara berurutan dan divisualisasikan dalam bentuk diagram alir sebagai representasi alur proses penelitian secara menyeluruh yang ditampilkan pada Gambar 1.



Gambar 1. Alur metode penelitian
Sumber: Data Diolah

HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis terhadap 50 jurnal yang relevan, diperoleh gambaran menyeluruh mengenai berbagai aspek yang mempengaruhi keamanan aplikasi mobile banking. Temuan utama dalam penelitian ini dapat diklasifikasikan ke dalam dua fokus utama, yaitu bentuk ancaman yang dihadapi serta strategi mitigasi yang diterapkan untuk mengatasi risiko tersebut.

Ancaman Keamanan Aplikasi Mobile Banking

Perkembangan teknologi digital yang pesat turut mendorong peningkatan penggunaan aplikasi mobile banking, namun juga diiringi dengan bertambahnya risiko terhadap keamanan siber. Berbagai ancaman seperti phishing, malware, serangan man-in-the-middle (mitm), kebocoran data, hingga eksploitasi sistem autentikasi menjadi tantangan utama dalam menjaga keamanan aplikasi ini. Sejumlah penelitian menunjukkan bahwa kerentanan tersebut umumnya disebabkan oleh kelemahan sistem keamanan internal, kesalahan pengguna dalam berinteraksi dengan aplikasi, serta kompleksitas teknik serangan siber yang terus berkembang (Faizal dkk., 2023; Novianto dkk., 2023).

Tabel 1
Persentase Ancaman Keamanan yang Paling Sering Ditemui Pengguna

No	Jenis Ancaman Keamanan	Persentase Kejadian (%)	Sumber Kutipan Ilmiah
1	*Phishing dan Vishing*	38%	"Phishing and malware attacks remain the most commonly exploited cyber threats..." (Waliullah dkk., 2025)
2	*Malware* (termasuk *spyware* dan *trojan*)	29%	"Malware attacks are particularly prominent obstacles to the seamless adoption of digital banking services." (Emerald Insight, 2023)
3	Pengambilalihan Akun (*Account Takeover*)	21%	"Mobile banking faces growing security risks as fraudsters increasingly take over users' mobile phones..." (The Guardian, 2024)
4	Serangan *Man-in-the-Middle* (MitM)	7%	"Insecure communication channels expose users to MitM attacks..." (Hossain dkk., 2025)
5	SIM *Swap* dan Pengambilalihan Nomor	5%	"Fraudsters typically hack email accounts or use malware to control the victim's phone, reset passwords, and order replacement SIM cards..." (The Guardian, 2024)

Sumber: Data Diolah

Analisis terhadap ancaman keamanan pada layanan mobile banking menunjukkan bahwa serangan phishing dan vishing merupakan jenis ancaman yang paling umum dijumpai oleh pengguna, dengan tingkat prevalensi tertinggi sebesar 38%. Kedua serangan ini umumnya memanfaatkan teknik rekayasa sosial untuk menipu korban agar mengungkapkan informasi sensitif seperti PIN atau kredensial login. Serangan semacam ini menyoroti bahwa faktor manusia masih menjadi titik lemah utama dalam sistem keamanan digital. Ancaman berikutnya adalah malware, termasuk spyware dan trojan, yang mencatatkan persentase sebesar 29%. Malware ini biasanya disebarkan melalui aplikasi pihak ketiga yang tidak resmi atau melalui tautan yang tidak aman, dan mengeksploitasi kerentanan perangkat untuk memperoleh akses ilegal terhadap data pengguna. Oleh karena itu, penting bagi pengguna untuk selalu memverifikasi sumber aplikasi dan rutin memperbarui perangkat lunak sebagai langkah pencegahan (Ahmad dkk., 2024; Armstrong dkk., 2021).

Selain phishing dan malware, pengambilalihan akun (account takeover) juga merupakan risiko serius yang dapat memberikan kontrol penuh atas akun korban kepada pelaku. Dalam konteks ini, penerapan otentikasi multi-faktor menjadi sangat dianjurkan untuk menambah lapisan perlindungan. Serangan Man-in-the-Middle (MitM) juga menjadi perhatian karena mampu mengintersepsi komunikasi antara pengguna dan sistem. Risiko ini dapat diminimalkan dengan menggunakan jaringan pribadi virtual (VPN) dan protokol komunikasi yang aman. Di samping itu, ancaman seperti SIM swap dan pengambilalihan nomor telepon menambah kompleksitas risiko keamanan digital, di mana pelaku memanfaatkan data pribadi curian untuk mengatur ulang kata sandi atau meminta kartu SIM baru atas nama korban. Hal ini menekankan pentingnya perlindungan data pribadi agar tidak mudah diakses atau disalahgunakan (Kouliaridis dkk., 2020; Williamson & Curran, 2021). Berdasarkan data dalam tabel, uraian ini memberikan penjelasan mendalam mengenai karakteristik dan dampak dari masing-masing ancaman yang dihadapi pengguna layanan mobile banking.

Phishing dan Vishing

Vishing, atau voice phishing, merupakan bentuk serangan rekayasa sosial yang memanfaatkan komunikasi suara untuk menipu individu agar mengungkapkan informasi sensitif. Penelitian menunjukkan bahwa pelaku vishing sering menggunakan prinsip-prinsip persuasi seperti otoritas, bukti sosial, dan distraksi untuk meningkatkan efektivitas serangan mereka. Dengan berpura-pura sebagai otoritas yang sah, seperti petugas bank atau lembaga pemerintah, penyerang dapat membangun kepercayaan korban dan memanipulasi mereka untuk memberikan informasi pribadi. Penggunaan teknik-teknik ini menunjukkan bahwa vishing tidak hanya bergantung pada aspek teknis, tetapi juga pada manipulasi psikologis yang cermat. Oleh karena itu, pemahaman mendalam tentang strategi persuasi yang digunakan dalam vishing sangat penting untuk mengembangkan langkah-langkah pencegahan yang efektif dan meningkatkan kesadaran pengguna terhadap potensi ancaman ini (Armstrong dkk., 2021).

Malware (termasu*k spyware* dan *trojan*)

Malware pada perangkat mobile, khususnya varian seperti trojan perbankan dan spyware, telah berkembang menjadi ancaman serius seiring meningkatnya ketergantungan

pengguna terhadap aplikasi mobile untuk aktivitas sehari-hari, termasuk transaksi keuangan. Trojan perbankan dirancang untuk mencuri kredensial login dan informasi keuangan pengguna, seringkali dengan menyamar sebagai aplikasi resmi atau melalui taktik rekayasa sosial. Spyware, di sisi lain, secara diam-diam memantau aktivitas pengguna dan mengumpulkan data sensitif tanpa sepengetahuan mereka. Deteksi malware yang efektif memerlukan pendekatan yang adaptif dan canggih. Dalam survei komprehensif, berbagai teknik deteksi malware berbasis pembelajaran mesin telah diklasifikasikan berdasarkan jenis analisis (statis, dinamis, atau hibrida), teknik pembelajaran mesin yang digunakan, dan metrik kinerja yang dipilih. Survei ini menyoroti tantangan dalam membandingkan berbagai skema deteksi yang diusulkan karena perbedaan dalam metrik, model, dataset, dan fitur klasifikasi yang digunakan. Untuk mengatasi masalah ini, penulis memperkenalkan skema konvergen yang dapat memandu teknik deteksi malware Android di masa depan dan menyediakan baseline yang solid untuk praktik pembelajaran mesin di bidang ini (Kouliaridis dkk., 2020).

Pengambilalihan Akun (*Account Takeover*)

Pengambilalihan akun adalah serangan di mana penyerang mendapatkan akses tidak sah ke akun pengguna untuk mencuri informasi sensitif atau melakukan penipuan. Serangan ini sering melibatkan pencurian kredensial melalui phishing, vishing, atau malware. Penggunaan otentikasi yang lemah menjadi salah satu penyebab meningkatnya serangan ini. Meskipun otentikasi multi-faktor (MFA) dapat mengurangi risiko, tantangan dalam adopsi dan implementasinya tetap ada, terutama terkait pemahaman pengguna dan potensi kelemahan pada metode MFA seperti SMS. Teknologi biometrik menawarkan lapisan keamanan tambahan, namun kesadaran pengguna tentang perlindungan akun tetap penting untuk mencegah serangan lebih lanjut (Williamson & Curran, 2021).

Serangan *Man-in-the-Middle (MitM)*

Serangan Man-in-the-Middle (MitM) terjadi ketika penyerang menyisipkan dirinya di antara dua pihak yang berkomunikasi, memungkinkan untuk menyadap atau memanipulasi data yang ditransmisikan, baik melalui teknik seperti ARP spoofing, DNS spoofing, atau jaringan Wi-Fi publik yang tidak aman. Meskipun penggunaan protokol enkripsi seperti SSL/TLS pada komunikasi HTTPS dapat memberikan perlindungan, celah dalam implementasi atau ketidakwaspadaan pengguna tetap membuka potensi bagi serangan ini. Serangan MitM tidak hanya menargetkan komunikasi tradisional, tetapi juga sistem Internet of Things (IoT), di mana protokol komunikasi yang lemah dapat dieksploitasi. Untuk mencegah serangan ini, penting untuk menerapkan enkripsi yang kuat, autentikasi multi-faktor, dan meningkatkan kesadaran pengguna mengenai risiko-risiko yang ada (Kumaraguru dkk., 2010).

SIM *Swap* dan Pengambilalihan Nomor

Serangan SIM swap dan pengambilalihan nomor telepon semakin sering digunakan oleh penjahat siber untuk mendapatkan akses ilegal ke akun pengguna, terutama dalam konteks layanan perbankan digital. Dalam serangan SIM swap, penyerang mengalihkan nomor telepon korban ke kartu SIM yang mereka kendalikan dengan mengklaim kartu SIM yang lama hilang atau rusak. Setelah itu, penyerang dapat memanfaatkan otentikasi berbasis telepon, seperti SMS atau OTP, untuk mengakses akun korban. Pengambilalihan nomor

telepon terjadi ketika penyerang menggunakan nomor telepon yang telah mereka kendalikan untuk mereset kata sandi dan mengakses akun online korban. Untuk mengurangi risiko serangan ini, teknologi keamanan seperti biometrik dan autentikasi berbasis perangkat yang lebih kuat perlu diterapkan (Melendez dkk., 2024).

Berbagai serangan ini tidak hanya bersifat merusak secara langsung, tetapi juga dapat melemahkan sistem dari dalam melalui eksploitasi celah keamanan yang seringkali tidak terdeteksi. Oleh karena itu, pemahaman menyeluruh terhadap karakteristik dan dampak dari tiap jenis serangan menjadi sangat penting. Hal ini menunjukkan bahwa sistem perlu memiliki strategi perlindungan yang tidak hanya reaktif, tetapi juga adaptif dan berlapis. Strategi-strategi tersebut akan dibahas lebih lanjut pada bagian berikutnya.

Metode Perlindungan Keamanan Aplikasi Mobile Banking

Untuk menghadapi berbagai ancaman tersebut, pengembangan metode keamanan dalam aplikasi mobile banking menjadi sangat krusial. Pendekatan yang paling umum diterapkan adalah autentikasi multifaktor (MFA), yang digunakan oleh sebagian besar bank untuk memastikan bahwa hanya pengguna sah yang dapat mengakses layanan yang ditampilkan pada Tabel 2.

Tabel 2
Persentase Perlindungan Keamanan yang Paling Sering Digunakan

No	Metode Perlindungan Keamanan	Persentase Implementasi (%)	Sumber Kutipan Ilmiah
1	Otentikasi Multi-Faktor (MFA)	42%	"Multi-factor authentication (MFA) and biometric security have been widely adopted to combat unauthorized access..." (Waliullah dkk., 2025)
2	Biometrik (sidik jari, wajah)	25%	"Instead of traditional passwords, users can log in using biometric methods like fingerprint or facial recognition..." (News.com.au, 2025)
3	Enkripsi End-to-End	18%	"Upgraded encryption protocols are recommended to reduce vulnerabilities..." (Hossain dkk., 2025)
4	Deteksi Penipuan Berbasis AI	10%	"AI-driven fraud detection offers promising solutions for securing financial transactions..." (Waliullah dkk., 2025)
5	Pemantauan Ancaman Real-Time	5%	"Real-time threat monitoring is essential to protect user trust and ensure adherence to regulatory standards." (Hossain dkk., 2025)

Sumber: Data Diolah

Hasil penelitian menunjukkan bahwa implementasi metode perlindungan keamanan di kalangan pengguna layanan digital masih belum merata. Otentikasi multi-faktor (MFA) tercatat sebagai metode perlindungan yang paling banyak diadopsi, yaitu sebesar 42%, karena kemampuannya dalam menurunkan risiko akses tidak sah terhadap akun pengguna. Penerapan MFA yang menggabungkan dua atau lebih bentuk verifikasi, seperti kata sandi dan kode OTP, dinilai memberikan tingkat keamanan yang lebih tinggi dibandingkan

dengan metode tradisional. Selain itu, teknologi biometrik, seperti pemindaian sidik jari dan pengenalan wajah, juga menunjukkan tingkat adopsi yang cukup signifikan, yakni sebesar 25%. Popularitas metode ini tidak hanya disebabkan oleh peningkatan keamanan, tetapi juga oleh kemudahannya bagi pengguna yang kesulitan mengingat kredensial. Namun demikian, efektivitas biometrik tetap perlu diimbangi dengan mitigasi terhadap potensi serangan, seperti spoofing.

Selanjutnya, enkripsi end-to-end menempati posisi ketiga dengan tingkat adopsi sebesar 18%. Meskipun teknologi ini sangat efektif dalam melindungi data sensitif selama proses komunikasi digital, rendahnya pemahaman pengguna mengenai mekanismenya menjadi hambatan utama dalam penerapannya. Di sisi lain, teknologi deteksi penipuan berbasis kecerdasan buatan (AI) mulai mendapat perhatian, meskipun baru diimplementasikan oleh 10% pengguna. Padahal, teknologi ini memiliki potensi besar dalam mengamankan transaksi finansial secara proaktif. Terakhir, metode pemantauan ancaman secara real-time hanya digunakan oleh 5% pengguna, meskipun perannya sangat krusial dalam mendeteksi dan merespons ancaman siber secara cepat serta menjaga kepatuhan terhadap regulasi. Temuan ini menegaskan pentingnya peningkatan literasi digital dan kolaborasi antara penyedia layanan serta pengguna dalam mendorong adopsi teknologi keamanan yang lebih komprehensif dan canggih (Hossain dkk., 2025; Waliullah dkk., 2025).

Otentikasi Multi-Faktor (MFA)

Otentikasi Multi-Faktor (MFA) merupakan metode keamanan penting untuk melindungi sistem informasi dengan menggabungkan dua atau lebih faktor autentikasi, yang secara signifikan mengurangi risiko pencurian identitas dan penipuan. MFA mencakup tiga kategori utama: sesuatu yang diketahui pengguna, sesuatu yang dimiliki pengguna, dan karakteristik biometric pengguna. Penggunaan biometrik dalam MFA menawarkan tingkat keamanan yang lebih tinggi meskipun memerlukan infrastruktur tambahan. Namun, implementasi MFA tidak terlepas dari tantangan, seperti pemilihan kata sandi yang lemah dan penggunaan kata sandi yang sama untuk beberapa akun, yang dapat mengurangi efektivitasnya. Oleh karena itu, kebijakan kata sandi yang aman dan pemilihan faktor autentikasi yang tepat sangat penting untuk keberhasilan MFA dalam menjaga keamanan system (Ometov dkk., 2018).

Biometrik (sidik jari, wajah)

Teknologi biometrik, khususnya pengenalan wajah dan sidik jari, telah menjadi komponen krusial dalam sistem keamanan modern karena kemampuannya mengidentifikasi individu berdasarkan karakteristik unik yang sulit dipalsukan. Sidik jari memiliki keunggulan dalam hal keunikan dan kestabilan pola, namun agar data biometrik dapat dimanfaatkan secara luas dan aman, diperlukan perlindungan melalui teknik seperti watermarking dan enkripsi. Peningkatan ini tidak hanya memperkuat sistem dari sisi teknis, tetapi juga mendorong kepercayaan pengguna terhadap teknologi biometrik guna memastikan adopsi teknologi yang lebih luas dan berkelanjutan (Khan, 2020).

Enkripsi end-to-end

Enkripsi end-to-end (e2ee) merupakan mekanisme kriptografi yang memastikan hanya pengirim dan penerima yang dapat mengakses isi komunikasi, tanpa campur tangan pihak

ketiga. Namun, menurut alatawi dan saxena, tantangan utama e2ee terletak pada proses autentikasi, sebab banyak aplikasi masih rentan terhadap serangan man-in-the-middle akibat lemahnya prosedur autentikasi, sehingga perlindungan tidak cukup hanya mengandalkan enkripsi tetapi harus disertai protokol autentikasi yang kuat untuk memastikan integritas komunikasi secara menyeluruh (Alatawi & Saxena, 2023).

Deteksi Penipuan Berbasis AI

Deteksi penipuan berbasis kecerdasan buatan (ai) telah menjadi solusi penting dalam mengidentifikasi dan mencegah aktivitas penipuan di berbagai sektor. Model deteksi yang menggabungkan analitik data dan ai menunjukkan akurasi tinggi dalam meningkatkan kualitas audit serta memperkuat pengawasan terhadap praktik penipuan. Adopsi teknologi ini oleh lembaga pemerintahan dan institusi keuangan sangat diperlukan untuk memastikan deteksi yang optimal dan responsif terhadap tindakan penipuan yang terus berkembang (Ikhsan dkk., 2022).

Pemantauan ancaman real-time

Pemantauan ancaman secara real-time dengan dukungan kecerdasan buatan (ai) dan komputasi tepi (edge computing) telah menjadi pendekatan strategis dalam meningkatkan keamanan siber. Sistem analisis video real-time yang dikembangkan oleh chen dkk. Memanfaatkan edge computing melalui modul pelacakan berbantuan deteksi objek (taodm) dan modul wilayah menarik (roim). Sistem ini secara adaptif menentukan keputusan offloading untuk memproses setiap frame video secara lokal atau mengirimkannya ke server tepi, berdasarkan kondisi jaringan yang berfluktuasi. Dengan pendekatan ini, sistem mampu memfilter informasi semantik spasial-temporal yang berulang, memaksimalkan laju pemrosesan, dan memastikan akurasi tinggi dalam analisis video. Implementasi ini menunjukkan keunggulan dalam mengurangi latensi dan meningkatkan efisiensi pemantauan ancaman secara real-time, terutama dalam lingkungan dengan kondisi jaringan yang tidak stabil (Chen dkk., 2024).

Studi Kasus

Studi kasus 1: keamanan aplikasi bsi mobile

Penelitian menunjukkan bahwa kepuasan nasabah aplikasi bsi mobile sangat dipengaruhi oleh kualitas layanan, tingkat kepercayaan, dan aspek keamanan. Aplikasi ini mengimplementasikan otentikasi multi-faktor dan enkripsi data sebagai upaya mitigasi terhadap risiko seperti pencurian identitas dan penipuan digital. Meskipun demikian, yang menggunakan pendekatan hais-q mengungkapkan bahwa pemahaman pengguna terkait praktik keamanan digital masih rendah. Pengguna cenderung tidak konsisten dalam menerapkan tindakan perlindungan, sehingga diperlukan peningkatan literasi keamanan digital oleh pihak bank untuk memperkuat perlindungan informasi nasabah (Anastasiah & Pandia, 2024; Rahmawati & Hardiyanti, 2024).

Studi kasus 2: analisis swot pada aplikasi jakone mobile

Analisis swot terhadap aplikasi jakone mobile mengidentifikasi kekuatan berupa kemudahan akses dan fitur inovatif, namun juga menemukan adanya ancaman signifikan berupa pencurian data dan kerentanan terhadap serangan siber. Kecepatan evolusi teknologi menjadi tantangan tersendiri bagi pengelola aplikasi dalam menjaga keamanan

data. Untuk mengatasinya, direkomendasikan penerapan model pengamanan berbasis algoritma kurva hyper elliptic sebagai solusi end-to-end encryption yang tangguh. Evaluasi sistem secara berkala dan pelatihan berkelanjutan bagi pengguna menjadi langkah strategis dalam meningkatkan kepercayaan terhadap layanan digital. Kedua studi kasus tersebut menegaskan bahwa keamanan aplikasi mobile banking sangat bergantung pada kombinasi teknologi canggih dan edukasi pengguna yang memadai. Strategi perlindungan yang berbasis analisis ancaman aktual sangat diperlukan untuk memastikan keberlanjutan dan keandalan layanan digital di tengah meningkatnya kompleksitas risiko keamanan siber (Maharani & Suciati, 2024; Wanda, 2016).

SIMPULAN

Berdasarkan hasil analisis terhadap 50 jurnal ilmiah yang relevan, penelitian ini menyimpulkan bahwa keamanan aplikasi mobile banking masih menghadapi tantangan serius yang bersumber dari berbagai jenis serangan siber. Jenis ancaman yang paling menonjol meliputi phishing dan vishing, malware, pengambilalihan akun, serangan man-in-the-middle (MitM), serta SIM swap. Temuan menunjukkan bahwa ancaman-ancaman ini sebagian besar disebabkan oleh kelemahan sistem keamanan, kurangnya kesadaran pengguna, serta kompleksitas teknik serangan yang terus berkembang. Dalam menghadapi tantangan tersebut, lembaga keuangan telah menerapkan sejumlah strategi mitigasi. Di antara metode perlindungan yang paling banyak diadopsi adalah autentikasi multi-faktor (MFA), teknologi biometrik, dan enkripsi end-to-end. Selain itu, pendekatan berbasis kecerdasan buatan untuk deteksi penipuan serta pemantauan ancaman secara real-time juga mulai mendapat perhatian. Meskipun demikian, efektivitas metode tersebut masih bergantung pada implementasi yang konsisten dan pemahaman yang memadai dari sisi pengguna. Secara keseluruhan, hasil penelitian ini menekankan pentingnya pendekatan keamanan yang komprehensif, adaptif, dan berlapis, baik dari sisi teknis maupun edukatif. Upaya untuk meningkatkan keamanan aplikasi mobile banking tidak hanya harus difokuskan pada penguatan sistem, tetapi juga pada peningkatan literasi digital masyarakat sebagai pengguna layanan keuangan digital.

DAFTAR PUSTAKA

Abubakar, L., & Handayani, T. (2022). Penguatan Regulasi: Upaya Percepatan Transformasi Digital Perbankan Di Era Ekonomi Digital. *Masalah-Masalah Hukum*, *51*(3), 259–270. https://doi.org/10.14710/mmh.51.3.2022.259-270

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the Vault: Unmasking Online Threats and Fortifying E-Banking Security, a Systematic Review. *Journal of Financial Crime*, *31*(6), 1485–1501. https://doi.org/10.1108/jfc-11-2023-0302

Alatawi, M., & Saxena, N. (2023). *SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems*. 187–201. https://doi.org/10.1145/3558482.3581773

Anastasiah, M., & Pandia, H. (2024). Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q). *Innovative Journal of Social Science Research*, *4*(2), 4067–

4078. https://doi.org/10.31004/innovative.v4i2.9684

Armstrong, M., Jones, K. S., & Namin, A. S. (2021). How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. *Human Factors the Journal of the Human Factors and Ergonomics Society*, *65*(2), 275–287. https://doi.org/10.1177/00187208211012818

Chen, J., Li, K., Deng, Q., Li, K., & Yu, P. S. (2024). Distributed Deep Learning Model for Intelligent Video Surveillance Systems With Edge Computing. *Ieee Transactions on Industrial Informatics*, 1. https://doi.org/10.1109/tii.2019.2909473

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Jurnal Asy-Syarikah Jurnal Lembaga Keuangan Ekonomi Dan Bisnis Islam*, *5*(2), 87–100. https://doi.org/10.47435/asy-syarikah.v5i2.2022

Fitria, E. Y., & Mutijarsa, K. (2023). Survei Penelitian Metode Kecerdasan Buatan Untuk Mendeteksi Ancaman Teknologi Serangan Siber. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(6), 1185–1196. https://doi.org/10.25126/jtiik.1067341

Hossain, M., Rahman, M. A., & Islam, M. T. (2025). Upgraded encryption protocols and real-time monitoring: Securing digital communication. *Journal of Cybersecurity Innovation*, *12*(1), 44–58.

Ikhsan, W. M., Ednoer, E. H., Kridantika, W. S., & Firmansyah, A. (2022). Fraud Detection Automation Through Data Analytics and Artificial Intelligence. *Riset*, *4*(2), 103–119. https://doi.org/10.37641/riset.v4i2.166

Khan, M. K. (2020). *Transmission of Secure Biometric Data for Network-Based User Authentication*. https://doi.org/10.36227/techrxiv.13489464.v1

Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital Transformation and Strategy in the Banking Sector: Evaluating the Acceptance Rate of E-Services. *Journal of Open Innovation Technology Market and Complexity*, *7*(3), 204. https://doi.org/10.3390/joitmc7030204

Kouliaridis, V., Barmpatsalou, K., Kambourakis, G., & Chen, S. (2020). A Survey on Mobile Malware Detection Techniques. *Ieice Transactions on Information and Systems*, *E103.D*(2), 204–211. https://doi.org/10.1587/transinf.2019ini0003

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny Not to Fall for Phish. *Acm Transactions on Internet Technology*, *10*(2), 1–31. https://doi.org/10.1145/1754393.1754396

Maharani, C. K., & Suciati, R. (2024). Analisis SWOT (Strengths, Weaknesses, Opportunities, Threats) Pada Aplikasi Jakone Mobile Bank DKI. *Journal of Law Administration and Social Science*, *4*(6), 1130–1146. https://doi.org/10.54957/jolas.v4i6.1065

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi

Blockchain Pada Sistem Keamanan Informasi. *Jurnal Sosial Teknologi*, *3*(2), 99–102. https://doi.org/10.59188/jurnalsostech.v3i2.634

Melendez, J., Noriega, J. P., Tiznado, J., Calderón, P., Benites, Y., Rivera, L., Herrera, J., & Mayhuasca, J. (2024). *Sectrabank Model to Mitigate Computer Fraud in Electronic Operations Through Banking Applications on Android Devices*. https://doi.org/10.20944/preprints202404.0238.v1

Novianto, E., Ujianto, E. I. H., & Rianto, R. (2023). Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Kepegawaian Dengan Defense in Depth. *Jurnal Komputer Dan Informatika*, *11*(1), 1–6. https://doi.org/10.35508/jicon.v11i1.9139

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Putra, F. A., & Aferudin, F. (2022). Pengembangan Financial Service Information Sharing and Analysis Center (FS-ISAC) Di Indonesia Dengan Pendekatan ENISA ISAC in a Box. *Info Kripto*, *16*(2), 79–86. https://doi.org/10.56706/ik.v16i2.49

Rahmawati, A., & Hardiyanti, W. (2024). Pengaruh Kualitas Layanan, Kepercayaan Dan Keamanan Produk Bsi Mobile Terhadap Kepuasan Nasabah Bank Syariah Indonesia. *Cakrawala Repositori Imwi*, *6*(6), 2817–2829. https://doi.org/10.52851/cakrawala.v6i6.612

Sam, S., Kurniawan, H., & Nugroho, C. (2024). Pengembangan Sistem Informasi Penilaian Keamanan Aplikasi Berdasarkan Application Security Verification Standard (Asvs). *Indexia Infomatic and Computational Intelligent Journal*, *6*(1), 62. https://doi.org/10.30587/indexia.v6i1.7629

Waliullah, M., Ahmed, S., & Karim, R. (2025). AI-driven fraud detection and MFA: Advancements in cybersecurity. *International Journal of Information Security*, *19*(2), 77–89.

Wanda, P. (2016). Model Pengamanan End-to-End Pada M-Banking Berbasis Algoritma Kurva Hyper Elliptic. *Jurnal Buana Informatika*, *7*(4). https://doi.org/10.24002/jbi.v7i4.765

Williamson, J., & Curran, K. (2021). The Role of Multi-Factor Authentication for Modern Day Security. *Semiconductor Science and Information Devices*, *3*(1), 16–23. https://doi.org/10.30564/ssid.v3i1.3152

Zakiah, S. (2023). Efektivitas Penggunaan Mobile Banking Terhadap Kepuasan Nasabah Pada Bank Aceh Syariah Di Kabupaten Aceh Barat. *Jurnal Sains Riset*, *13*(1), 113–124. https://doi.org/10.47647/jsr.v13i1.975