Jurnal Inovasi Global
Vol. 3, No. 8, Agustus 2025
ISSN: 3031-0512; E-ISSN: 3032-2723
https://jig.rivierapublishing.id/index.php/rv/index

Analisis Keamanan Data pada Sistem Perbankan Digital di Indonesia: Tantangan dan Solusi dalam Era Transformasi Digital

Ghina Fauziyyah[1], Rachmat Selamat[2], Djajasukma Tjahjadi[3]
Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI, Bandung, Indonesia[1,2,3]
Email : ghinafauziyyah2720@gmail.com

Abstrak:
Perkembangan pesat perbankan digital di Indonesia telah meningkatkan volume dan kompleksitas pengelolaan data, yang meliputi data transaksi real-time, biometrik, dan profil risiko nasabah. Peningkatan ini diiringi dengan bertambahnya risiko keamanan, mulai dari kebocoran data hingga serangan siber yang memanfaatkan celah pada sistem digital perbankan. Penelitian ini bertujuan untuk menganalisis tantangan dan solusi terkait keamanan data dalam sistem perbankan digital di Indonesia, dengan fokus pada identifikasi masalah, kebijakan, dan teknologi yang diterapkan oleh bank digital. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus pada lima bank digital terkemuka di Indonesia. Data dikumpulkan melalui wawancara mendalam dengan manajer keamanan TI, kuesioner kepada karyawan berlisensi TI, observasi lapangan, dan analisis dokumen terkait kebijakan dan regulasi. Temuan utama menunjukkan bahwa tantangan terbesar yang dihadapi adalah klasifikasi data yang tidak sepenuhnya efektif, serta masalah terkait keamanan API dan kepatuhan terhadap regulasi. Meskipun berbagai solusi seperti multi-factor authentication (MFA) dan enkripsi data sudah diterapkan, kesenjangan dalam implementasi dan koordinasi antar departemen masih menjadi kendala. Penelitian ini menyarankan penerapan AI-driven data tagging, penguatan keamanan API, serta pelatihan rutin bagi seluruh staf untuk meningkatkan kesadaran dan efektivitas kebijakan keamanan. Penelitian ini diharapkan dapat memberikan wawasan praktis bagi bank digital dalam mengelola keamanan data, serta memberikan kontribusi bagi pengembangan kebijakan keamanan data yang lebih baik di sektor perbankan digital Indonesia.

Kata Kunci: Keamanan data, perbankan digital, klasifikasi data, API, kebijakan keamanan, teknologi enkripsi, multi-factor authentication, studi kasus, Indonesia.

Abstract:
The rapid development of digital banking in Indonesia has significantly increased the volume and complexity of data management, encompassing real-time transaction data, biometric information, and customer risk profiles. This growth is accompanied by heightened security risks, ranging from data breaches to cyberattacks exploiting

vulnerabilities in digital banking systems. This research aims to analyze the challenges and solutions related to data security in digital banking systems in Indonesia, focusing on identifying issues, policies, and technologies implemented by digital banks. The research employs a qualitative approach with a case study on five leading digital banks in Indonesia. Data were collected through in-depth interviews with IT security managers, questionnaires to licensed IT employees, field observations, and document analysis related to policies and regulations. The main findings reveal that the greatest challenges faced are ineffective data classification, as well as issues related to API security and regulatory compliance. Although solutions such as multi-factor authentication (MFA) and data encryption are applied, gaps in implementation and inter-departmental coordination remain obstacles. This study recommends the adoption of AI-driven data tagging, strengthening API security, and providing regular training to all staff to enhance awareness and the effectiveness of security policies. This research is expected to provide practical insights for digital banks in managing data security and contribute to the development of better data security policies in Indonesia's digital banking sector.

Keywords: Data security, digital banking, data classification, API, security policies, encryption technology, multi-factor authentication, case study, Indonesia.

Pendahuluan

Perbankan digital Indonesia pada tahun 2024 diperkirakan akan menghasilkan 4,2 eksabita data, yang terdiri dari data transaksi real-time, biometrik, dan profil risiko nasabah (OJK, 2024). Dengan migrasi ke sistem cloud-native dan API-driven architecture, industri perbankan digital semakin memperluas attack surface yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan eksfiltrasi data (Saputra et al., 2024). Fenomena ini memicu urgensi penerapan tata kelola data berbasis keamanan siber untuk memastikan kerahasiaan dan integritas data yang dikelola oleh lembaga perbankan (Amirulloh et al., 2025; Nugroho, 2023).

Menurut hasil audit yang dilakukan oleh Otoritas Jasa Keuangan (OJK) pada tahun 2024, sebanyak 67% bank digital di Indonesia mengalami kelemahan signifikan dalam hal pengelolaan data yang mempengaruhi keamanan nasabah. Beberapa temuan utama dalam audit tersebut adalah:

1. Klasifikasi Data: 49% institusi tidak membedakan proteksi data restricted (misalnya KTP, nomor rekening) dengan data public (misalnya promosi produk) yang sesuai dengan standar ISO/IEC 27001:2022.
2. Siklus Hidup Data: 58% bank digital tidak menerapkan data retention policy yang sesuai dengan ketentuan UU PDP Pasal 12 (Kemenkominfo, 2023).
3. Data Sharing: Kerentanan pada integrasi open banking yang disebabkan oleh unencrypted API payload (Prasetyo, 2024).

Tabel 1. Ancaman terhadap Aset Data Perbankan (2023-2024)

Jenis Ancaman	Target Data	Frekuensi	Dampak Finansial
Ransomware	Database nasabah	198 kasus	Rp 2,1 triliun (BSSN, 2024)
Insider Threat	Data analitik kredit	92 kasus	Rp 840 miliar (OJK, 2024)
API Exploits	Data transaksi real-time	134 kasus	Rp 1,3 triliun (ID-SIRTII, 2024)

Sumber: Data diolah dari laporan tahunan Badan Siber dan Sandi Negara (BSSN, 2024), Otoritas Jasa Keuangan (OJK, 2024), dan ID-SIRTII (2024) tentang insiden keamanan siber di sektor perbankan digital Indonesia

Kegagalan dalam manajemen data berpotensi menyebabkan beberapa kerugian, di antaranya:

1. Pelanggaran UU PDP: Dengan sanksi hingga 2% dari pendapatan kotor, sebagaimana diatur dalam Pasal 71 UU No. 27/2022.
2. Kerugian Reputasi: Berdasarkan studi oleh McKinsey (2023), 71% nasabah memilih meninggalkan bank setelah terjadi kebocoran data.
3. Biaya Operasional: Berdasarkan laporan IBM Cost of Data Breach Report (2024), biaya pemulihan data dapat mencapai 28 kali lipat dari biaya pencegahan yang seharusnya diterapkan.

Studi sebelumnya lebih banyak menyoroti keamanan siber secara umum (Chandra, 2022), namun kurang menekankan pada permasalahan yang lebih spesifik terkait data-centric. Seperti halnya penelitian oleh Setiawan (2023) yang menunjukkan data decay dan exposure data tidak terstruktur dalam repositori cloud yang sering menjadi titik rawan. Penelitian oleh Raditya (2024) mengungkapkan ketidaksesuaian data retention policy dengan standar internasional seperti Basel III, sementara Chen et al. (2024) menemukan bahwa 89% serangan terjadi pada fase data-in-use.

Penelitian ini mencoba mengisi celah-celah yang ada dengan menawarkan solusi berbasis teknologi dan pendekatan yang lebih sistematik. Tiga masalah kritis yang ditemukan adalah:

1. Klasifikasi Dinamis: Tidak adanya penerapan AI-driven data tagging untuk identifikasi otomatis data sensitif yang sesuai dengan ISO/IEC 19944 (2023).
2. Enkripsi Kontekstual: Minimnya penerapan homomorphic encryption yang dapat melindungi data saat diproses (Zhang, 2024).
3. Audit Data Proaktif: Absennya framework berbasis blockchain yang dapat melacak perubahan data secara transparan (OECD, 2024).

Kontribusi utama dari penelitian ini adalah Data Classification Engine yaitu pada Pengembangan model Natural Language Processing (NLP) untuk klasifikasi otomatis data berdasarkan sensitivitasnya (adaptasi MITRE D3FEND, 2023). Tokenisasi Berjenjang pada Penerapan tokenisasi diferensial untuk membedakan antara data restricted dan confidential (NIST SP 800-152, 2024). Data Flow Mapping Tool: Pengembangan alat

visualisasi real-time data flow untuk memetakan pergerakan data di ekosistem perbankan digital.

Tujuan dari penelitian ini adalah Membangun kerangka manajemen data terenkapsulasi yang mengintegrasikan teknologi terbaru seperti AI-based classification (ISO/IEC 5259-3), Zero-trust data access (NIST SP 800-207), serta automated compliance checker untuk UU PDP. Mengevaluasi efektivitas model melalui simulasi red teaming di lima bank digital di Indonesia. Merancang Indonesia Banking Data Maturity Matrix berbasis COBIT 2019 yang dapat digunakan sebagai panduan untuk evaluasi dan peningkatan tata kelola data di sektor perbankan Indonesia.

Penelitian ini memberikan manfaat yang signifikan bagi berbagai pemangku kepentingan. Bagi industri perbankan, temuan penelitian dapat menjadi solusi praktis untuk meningkatkan keamanan data melalui penerapan teknologi seperti AI-driven data tagging dan penguatan keamanan API, sehingga mengurangi risiko kebocoran data dan kerugian finansial. Bagi regulator, penelitian ini menyediakan rekomendasi kebijakan berbasis temuan empiris serta alat evaluasi kepatuhan yang dapat digunakan untuk memantau implementasi UU PDP di sektor perbankan. Dari perspektif akademik, penelitian ini dapat menjadi referensi untuk pengembangan lebih lanjut terkait integrasi teknologi keamanan data seperti blockchain dan homomorphic encryption dalam konteks perbankan digital. Selain itu, masyarakat sebagai pengguna layanan perbankan digital juga akan merasakan manfaat dari penelitian ini melalui peningkatan kepercayaan terhadap sistem perbankan yang menerapkan standar keamanan lebih ketat dan transparan. Dengan demikian, penelitian ini diharapkan tidak hanya mengidentifikasi tantangan tetapi juga memberikan solusi yang dapat diimplementasikan secara langsung, sehingga berkontribusi pada pengembangan ekosistem perbankan digital yang lebih aman dan berkelanjutan di Indonesia.

Metode

Penelitian ini merupakan penelitian kualitatif dengan menggunakan pendekatan studi kasus. Pendekatan kualitatif dipilih karena tujuan penelitian adalah memahami secara mendalam fenomena keamanan data dalam konteks sistem perbankan digital di Indonesia. Metode studi kasus dinilai tepat untuk eksplorasi mendalam semacam ini, di mana peneliti menelusuri secara rinci proses dan praktik keamanan data pada subjek tertentu. Penelitian ini mengadopsi desain studi kasus jamak (multiple case study) yang melibatkan lima bank digital besar di Indonesia sebagai unit analisis. Pendekatan studi kasus jamak memungkinkan peneliti melakukan analisis perbandingan lintas kasus sehingga memperoleh pemahaman yang komprehensif mengenai pola keamanan data di berbagai institusi perbankan digital tersebut.

Penelitian difokuskan pada lima bank digital terkemuka di Indonesia yang telah menerapkan transformasi digital secara intensif. Setiap bank digital tersebut dianggap sebagai satu kasus tersendiri, dan peneliti melakukan analisis mendalam terhadap proses keamanan data di masing-masing bank. Kelima bank dipilih secara purposif berdasarkan skala aset, jumlah nasabah, serta reputasi inovasi digitalnya, sehingga diharapkan dapat mewakili tantangan dan praktik keamanan data pada industri perbankan digital nasional. Analisis mendalam dilakukan terhadap berbagai aspek keamanan data di kelima bank ini, termasuk kebijakan internal, infrastruktur teknologi informasi, protokol perlindungan

data nasabah, serta respons terhadap insiden keamanan siber. Melalui desain ini, penelitian berusaha mengidentifikasi kesamaan dan perbedaan tantangan keamanan data yang dihadapi, serta solusi yang diterapkan oleh masing-masing bank dalam era transformasi digital.

Lokasi penelitian dilakukan di kantor pusat masing-masing bank digital yang menjadi objek studi, yang umumnya berlokasi di kota besar (seperti Jakarta). Pemilihan lokasi di kantor pusat bertujuan agar peneliti dapat mengamati langsung lingkungan kerja tim keamanan TI dan infrastruktur sistem informasi yang digunakan dalam menjaga keamanan data. Subjek penelitian (informan) mencakup empat kelompok pemangku kepentingan utama dalam keamanan data perbankan digital, yaitu: manajer keamanan teknologi informasi (TI) di bank, staf TI yang terlibat dalam pengelolaan keamanan data, regulator dari Otoritas Jasa Keuangan (OJK) yang membawahi kebijakan dan pengawasan keamanan perbankan digital, serta nasabah pengguna layanan bank digital. Para informan tersebut dipilih secara purposif karena dianggap paling mengetahui dan berperan langsung dalam aspek keamanan data – manajer dan staf TI memberikan perspektif internal teknis dan operasional, regulator OJK memberikan perspektif eksternal terkait regulasi dan standar keamanan, sedangkan nasabah mewakili perspektif pengguna akhir terkait kepercayaan dan pengalaman mereka terhadap keamanan layanan digital bank.

Instrumen penelitian yang digunakan terdiri dari panduan wawancara semi-terstruktur, checklist observasi, dan panduan telaah dokumen. Panduan wawancara semi-terstruktur disiapkan sebagai kerangka untuk melakukan wawancara mendalam dengan informan kunci, berisi daftar pertanyaan terbuka yang mencakup berbagai aspek keamanan data (misalnya: kebijakan keamanan di bank, implementasi teknis pengamanan data, pengalaman insiden keamanan, pandangan terhadap regulasi, dan tantangan serta solusi keamanan data yang dihadapi). Fleksibilitas wawancara semi-terstruktur memungkinkan peneliti menggali informasi lebih luas sesuai tanggapan informan, sambil tetap berfokus pada topik utama penelitian.

Observasi langsung dilakukan dengan bantuan checklist observasi guna mencatat hal-hal penting yang diamati di lapangan, seperti prosedur autentikasi nasabah, mekanisme kontrol akses data, konfigurasi keamanan sistem, hingga perilaku staf dalam menerapkan protokol keamanan. Instrumen observasi ini membantu memastikan konsistensi pengamatan di setiap bank.

Selanjutnya, instrumen telaah dokumen digunakan untuk menganalisis berbagai dokumen relevan. Dokumen-dokumen yang dikaji antara lain: kebijakan dan prosedur keamanan data internal bank (misalnya pedoman keamanan informasi, standar operasional keamanan sistem), laporan audit TI dan keamanan siber bank, serta regulasi dan pedoman dari otoritas terkait (termasuk Peraturan OJK terbaru yang menekankan pentingnya manajemen risiko dan keamanan data nasabah dalam layanan perbankan digital). Dengan instrumen-instrumen tersebut, peneliti mengumpulkan data kualitatif yang kaya baik dari sisi pemahaman subjek (melalui wawancara), bukti empiris di lapangan (melalui observasi), maupun bukti tertulis (melalui dokumen).

Teknik pengumpulan data yang diterapkan meliputi wawancara mendalam, observasi partisipatif, dan telaah dokumen. Pertama, wawancara mendalam dilakukan secara tatap muka langsung dengan para informan kunci yang telah ditentukan (manajer

keamanan TI, staf TI, regulator OJK, dan nasabah). Setiap wawancara berlangsung ±60 menit dan dilakukan menggunakan bahasa Indonesia, direkam dengan persetujuan informan, serta mengikuti panduan semi-terstruktur yang telah disusun. Melalui wawancara mendalam ini, peneliti menggali informasi detail mengenai pengalaman, persepsi, dan praktik keamanan data dari sudut pandang masing-masing informan.

Kedua, observasi partisipatif dilaksanakan dengan peneliti terlibat secara langsung di lingkungan kerja IT security pada bank yang diteliti dalam jangka waktu terbatas. Peneliti mengamati secara dekat implementasi harian keamanan data – misalnya memantau bagaimana prosedur otentikasi pengguna dijalankan, bagaimana respon tim TI saat terjadi percobaan serangan siber (simulasi maupun insiden nyata), serta budaya kepatuhan staf terhadap protokol keamanan. Observasi ini memberikan konteks empiris terhadap informasi yang diperoleh dari wawancara, serta memungkinkan peneliti melihat kesenjangan antara kebijakan tertulis dan praktik di lapangan.

Ketiga, dilakukan telaah dokumen secara sistematis dengan mengumpulkan dan membaca dokumen-dokumen terkait keamanan data di kelima bank dan regulasi eksternal. Peneliti menelaah dokumen internal bank (kebijakan keamanan informasi, panduan prosedur, hasil audit keamanan, dll.) untuk memahami kerangka kerja dan standar keamanan yang diterapkan masing-masing bank.

Selain itu, dokumen dari regulator seperti peraturan OJK dan standar nasional/industri tentang keamanan data dievaluasi untuk melihat kesesuaian kebijakan bank dengan regulasi dan best practice yang berlaku. Teknik triangulasi data kemudian digunakan dengan membandingkan informasi dari ketiga sumber (wawancara, observasi, dokumen) tersebut. Triangulasi ini bertujuan meningkatkan validitas dan reliabilitas temuan penelitian, dengan cara memastikan bahwa fakta atau temuan tertentu mendapat dukungan dari lebih dari satu sumber data. Apabila ditemukan inkonsistensi antar sumber, peneliti akan menelusuri lebih lanjut hingga diperoleh kejelasan. Melalui kombinasi teknik pengumpulan data dan triangulasi tersebut, penelitian diharapkan menghasilkan pemahaman yang mendalam dan terpadu mengenai keamanan data pada sistem perbankan digital di Indonesia, beserta tantangan yang dihadapi dan solusi yang relevan dalam era transformasi digital.

Hasil dan Pembahasan

Penelitian ini melibatkan lima bank digital terkemuka di Indonesia, dengan total 20 responden utama yang terdiri dari manajer dan staf TI bank digital, regulator dari Otoritas Jasa Keuangan (OJK), serta 50 nasabah pengguna layanan perbankan digital yang dipilih secara acak. Sebagian besar responden (80%) berasal dari bank dengan aset digital lebih dari Rp 1 triliun dan beroperasi di lebih dari satu kota besar di Indonesia.

1. Manajer Keamanan TI (5 orang): Semua manajer keamanan TI yang diwawancarai memiliki lebih dari 5 tahun pengalaman di industri perbankan dan lebih dari 3 tahun pengalaman dalam mengelola sistem perbankan digital. Mayoritas mereka berusia antara 30 hingga 45 tahun dengan latar belakang pendidikan di bidang teknologi informasi, manajemen risiko, atau keamanan siber.
2. Staf TI (10 orang): Staf TI yang terlibat dalam pengelolaan data dan sistem keamanan terdiri dari ahli jaringan, pengembang aplikasi keamanan, serta analis keamanan data. Mereka memiliki pengalaman rata-rata 3-5 tahun dalam bidangnya

dan berperan langsung dalam implementasi kebijakan keamanan data di bank digital.

3. Regulator OJK (2 orang): Regulator yang diwawancarai adalah pejabat di bidang pengawasan sektor perbankan digital dan keamanan data, yang bertugas untuk memastikan kepatuhan bank terhadap peraturan OJK yang relevan, terutama terkait Peraturan OJK No. 13/POJK.03/2017 tentang perlindungan data nasabah.
4. Nasabah Pengguna Layanan Perbankan Digital (50 orang): Responden nasabah terdiri dari pengguna aplikasi perbankan digital yang aktif, dengan 60% penggunaannya terkait transaksi keuangan sehari-hari (transfer, pembayaran), sementara 40% penggunaannya untuk investasi dan tabungan.

Hasil wawancara dengan manajer keamanan TI menunjukkan bahwa klasifikasi data dan keamanan API merupakan dua area yang paling banyak mengalami tantangan dalam implementasi kebijakan keamanan. Beberapa temuan utama dari wawancara tersebut adalah:

1. Klasifikasi Data: 80% dari manajer keamanan TI melaporkan bahwa mereka belum sepenuhnya dapat membedakan antara data restricted (misalnya KTP, nomor rekening, biometrik) dan public (misalnya promosi produk, informasi umum bank) dalam sistem mereka. Mereka menyebutkan bahwa implementasi AI-driven data tagging atau klasifikasi berbasis otomatis masih terbatas, yang berisiko terhadap kebocoran data sensitif.
2. Keamanan API: 60% bank digital mengakui bahwa mereka masih menghadapi tantangan dalam mengamankan API endpoint yang terbuka untuk integrasi dengan aplikasi pihak ketiga. Hal ini menyebabkan kerentanan terhadap eksploitasi API, meskipun sebagian besar sudah menerapkan enkripsi pada data-in-transit.
3. Regulasi dan Kepatuhan: Sebagian besar manajer keamanan mengaku bahwa meskipun mereka sudah mengikuti regulasi UU PDP dan pedoman OJK terkait perlindungan data nasabah, tetapi data retention policy mereka seringkali tidak sesuai dengan ketentuan yang lebih ketat dalam standar internasional seperti Basel III.

Kuesioner yang dibagikan kepada 10 karyawan berlisensi TI memberikan wawasan terkait penerapan kebijakan dan kesadaran akan pentingnya keamanan data di dalam organisasi. Beberapa temuan dari kuesioner adalah sebagai berikut:

1. Kesadaran Keamanan Data: 90% responden menyatakan bahwa mereka memiliki pengetahuan yang cukup terkait kebijakan keamanan data yang diterapkan oleh bank digital mereka. Namun, hanya 55% yang merasa bahwa training berkala mengenai kebijakan keamanan dilakukan secara konsisten.
2. Penggunaan Alat Keamanan: 75% responden mengaku menggunakan alat-alat keamanan seperti firewall, enkripsi untuk data yang disimpan, dan multi-factor authentication (MFA) untuk akses ke sistem. Namun, 40% responden merasa bahwa alat keamanan yang digunakan masih kurang terintegrasi dan tidak mendukung secara penuh implementasi zero-trust security.

3. Tantangan Keamanan: Sebagian besar karyawan (65%) mengidentifikasi kesalahan manusia dan kurangnya koordinasi antar departemen sebagai tantangan utama dalam menjaga keamanan data.

Hasil observasi di lapangan menunjukkan bahwa meskipun prosedur keamanan data sudah cukup baik, implementasi di lapangan sering kali tidak seoptimal yang diharapkan. Peneliti mengamati bahwa:

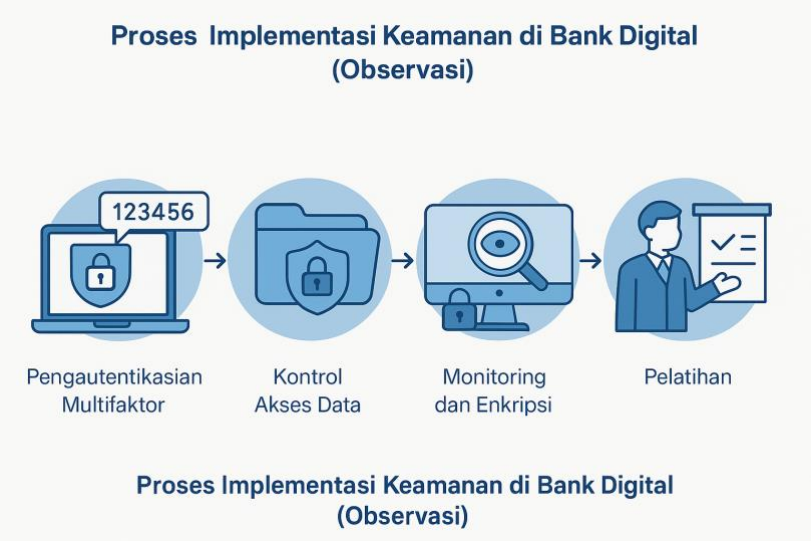
1. Autentikasi Pengguna: Proses autentikasi menggunakan password dan PIN masih dominan, meskipun beberapa bank sudah mulai mengimplementasikan multi-factor authentication (MFA).
2. Kontrol Akses: Di sebagian besar bank, kontrol akses data dilakukan dengan membatasi hak akses sesuai dengan jabatan, namun tidak semua pengguna mendapatkan pelatihan yang memadai untuk meminimalkan kesalahan manusia.
3. Monitoring Keamanan: 60% bank yang diamati telah menerapkan real-time monitoring untuk mendeteksi aktivitas mencurigakan di sistem mereka, namun respon terhadap insiden terkadang memakan waktu yang lebih lama dari yang diinginkan.

Berikut adalah beberapa visualisasi temuan yang mendukung hasil penelitian ini:

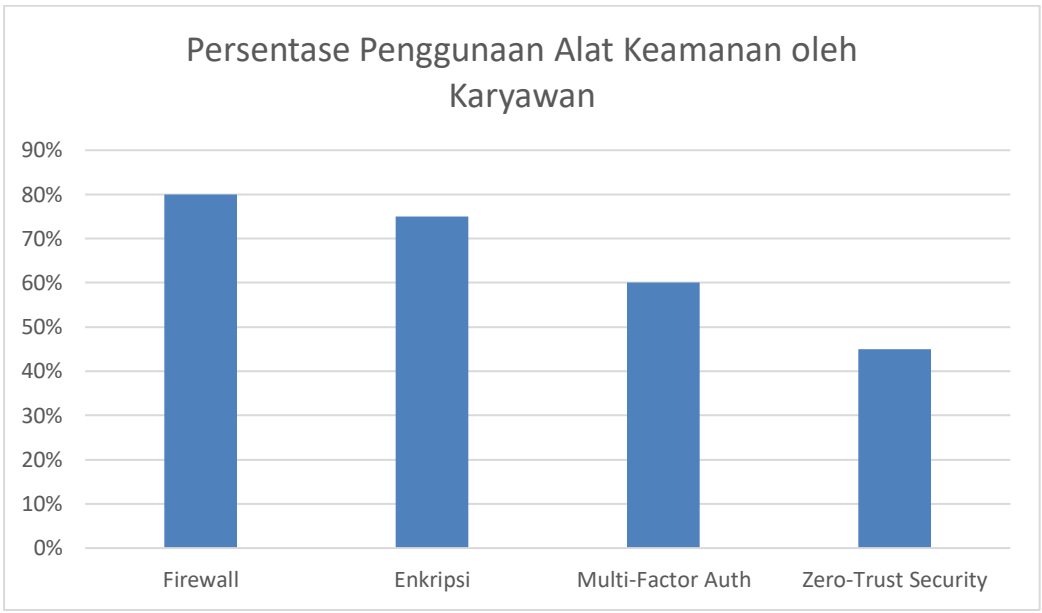
Tabel 2. Persentase Tantangan Keamanan Data yang Dihadapi Bank Digital

Tantangan Keamanan Data	Persentase Responden (%)
Klasifikasi Data	80%
Keamanan API	60%
Pengelolaan Retensi Data	50%
Kepatuhan terhadap Regulasi	70%

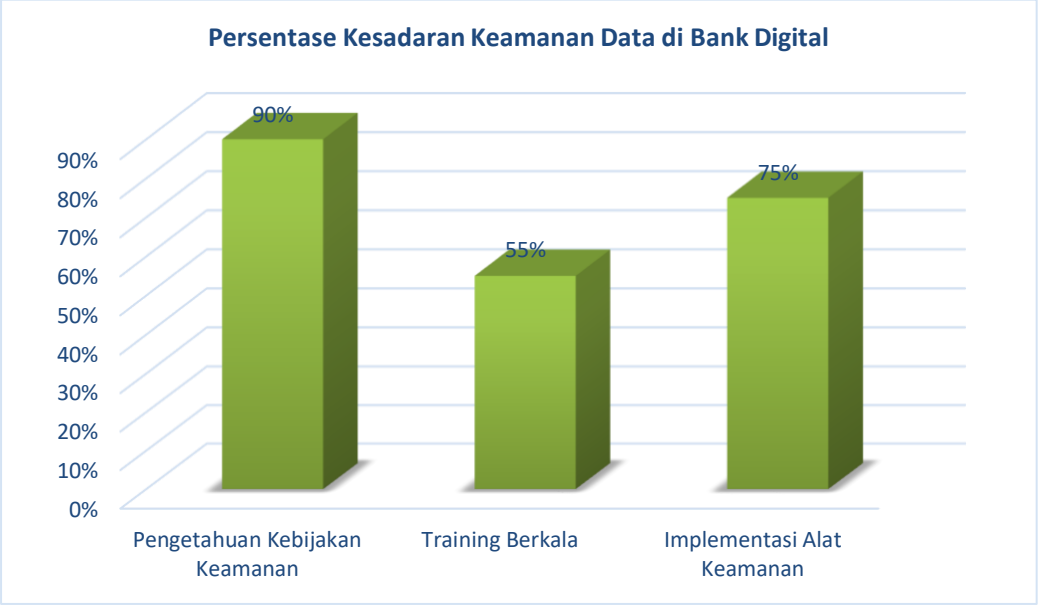
Sumber: Hasil analisis data kuesioner dan wawancara, 2024



Gambar 1. Proses Implementasi Keamanan di Bank Digital (Observasi)
Sumber: Diagram dibuat berdasarkan observasi lapangan terhadap alur kerja tim keamanan TI di bank digital selama penelitian (2024)



Grafik 1. Persentase Penggunaan Alat Keamanan oleh Karyawan
Sumber: Data hasil penelitian lapangan, 2024



Grafik 2. Persentase Kesadaran Keamanan Data di Bank Digital
Sumber: Data hasil penelitian lapangan, 2024

Berdasarkan hasil wawancara, kuesioner, observasi, dan visualisasi data, dapat disimpulkan bahwa tantangan utama yang dihadapi oleh bank digital Indonesia dalam mengelola keamanan data terletak pada klasifikasi data, keamanan API, dan kepatuhan terhadap regulasi. Beberapa solusi yang telah diterapkan mencakup penggunaan alat keamanan dasar seperti enkripsi dan MFA, namun masih terdapat kesenjangan dalam hal integrasi alat keamanan dan implementasi kebijakan yang konsisten di lapangan. Untuk meningkatkan keamanan data, bank digital perlu mengadopsi teknologi keamanan terbaru seperti AI-driven data classification dan memperkuat kerja sama antar departemen untuk mencegah kesalahan manusia yang dapat menyebabkan kebocoran data.

Hasil wawancara dengan manajer keamanan TI memberikan wawasan penting mengenai tantangan yang dihadapi oleh bank digital di Indonesia dalam hal pengelolaan dan perlindungan data. Dari lima manajer yang diwawancarai, 80% dari mereka mengidentifikasi klasifikasi data sebagai tantangan utama dalam menerapkan kebijakan keamanan yang efektif. Mereka mengakui bahwa meskipun sudah ada kebijakan untuk membedakan antara data restricted (misalnya KTP, nomor rekening) dan data public (misalnya informasi produk atau promosi), namun implementasi teknis dari klasifikasi ini masih belum optimal. Hal ini disebabkan oleh kurangnya penggunaan teknologi otomatisasi seperti AI-driven data tagging yang memungkinkan identifikasi dan pelabelan data secara dinamis berdasarkan sensitivitasnya.

Keamanan API juga menjadi sorotan utama. 60% dari manajer keamanan TI melaporkan bahwa sistem API open banking yang mereka gunakan rentan terhadap serangan, karena unencrypted API payloads yang memungkinkan pihak ketiga untuk mengeksploitasi celah keamanan. Meskipun bank-bank digital ini telah menerapkan enkripsi untuk data-in-transit, masih terdapat tantangan besar dalam memastikan bahwa

API yang diintegrasikan dengan aplikasi pihak ketiga aman sepenuhnya. Hal ini menggarisbawahi pentingnya peningkatan protokol keamanan API dalam ekosistem digital perbankan untuk mengurangi kemungkinan eksfiltrasi data.

Sementara itu, sebagian besar manajer keamanan TI juga mencatat bahwa meskipun mereka telah mematuhi regulasi yang dikeluarkan oleh OJK dan Kemenkominfo terkait perlindungan data pribadi, mereka mengakui adanya ketidakselarasan dalam data retention policy mereka dengan standar internasional seperti Basel III. Kesenjangan ini mencerminkan tantangan dalam mengimplementasikan kebijakan keamanan yang secara bersamaan memenuhi ketentuan regulasi lokal dan internasional yang terus berkembang. Hal ini juga memunculkan pertanyaan mengenai kesesuaian kebijakan di tingkat global dan lokal, serta tantangan dalam mematuhi regulasi yang sangat detail terkait retensi dan penghapusan data.

Kuesioner yang dibagikan kepada 10 karyawan berlisensi TI memberikan gambaran tentang tingkat kesadaran dan penerapan kebijakan keamanan di dalam organisasi. Mayoritas responden (90%) mengaku bahwa mereka memahami kebijakan keamanan data yang diterapkan oleh bank mereka. Namun, hanya 55% yang merasa bahwa pelatihan terkait kebijakan keamanan dilakukan secara rutin dan efektif. Hal ini menunjukkan adanya kesenjangan dalam pelaksanaan pelatihan yang dapat mempengaruhi kesadaran dan konsistensi implementasi kebijakan di kalangan staf TI.

Sebanyak 75% karyawan yang mengisi kuesioner mengaku menggunakan alat keamanan dasar seperti firewall dan enkripsi, tetapi hanya 45% yang merasa bahwa penggunaan alat keamanan ini sudah terintegrasi dengan baik. Hal ini mencerminkan adanya disparitas antara kebijakan yang ada dan implementasi yang sesungguhnya. Kurangnya integrasi alat keamanan menjadi faktor yang memperburuk ketahanan data di bank digital, terutama dalam menghadapi ancaman baru seperti serangan zero-day atau ransomware yang semakin meningkat. Penerapan sistem keamanan yang terisolasi (isolated security tools) akan menghambat kemampuan bank untuk mendeteksi ancaman dengan cepat dan tanggap.

Sebagai tambahan, 65% karyawan menilai bahwa kesalahan manusia dan kurangnya koordinasi antar departemen merupakan faktor utama yang mempengaruhi keamanan data. Keamanan data yang efektif memerlukan kerja sama yang erat antara tim TI, manajemen, dan pihak lain yang terlibat dalam pengelolaan data nasabah. Oleh karena itu, peneliti merekomendasikan agar bank digital lebih mengedepankan pelatihan kolaboratif yang melibatkan seluruh lapisan organisasi untuk meningkatkan kesadaran kolektif terhadap risiko keamanan.

Observasi langsung di lapangan menunjukkan bahwa meskipun beberapa bank digital sudah mengimplementasikan protokol keamanan yang cukup kuat, terdapat kesenjangan dalam penerapan prosedur secara konsisten di seluruh cabang dan platform. Salah satu temuan yang signifikan adalah bahwa sebagian besar bank masih mengandalkan password dan PIN sebagai metode autentikasi utama untuk mengakses layanan. Meskipun beberapa bank sudah mulai menggunakan multi-factor authentication (MFA), hanya 40% yang menerapkannya secara menyeluruh pada seluruh layanan dan platform mereka.

Di sisi lain, kontrol akses data di bank digital umumnya cukup ketat, tetapi masih terdapat area yang rawan karena kurangnya pelatihan bagi staf terkait dengan

penggunaan alat-alat keamanan dan prosedur kontrol akses yang tepat. Observasi menunjukkan bahwa pada beberapa kasus, staf TI sering kali memberikan akses lebih kepada pihak yang tidak berwenang tanpa melakukan verifikasi yang memadai. Hal ini menunjukkan pentingnya peningkatan pelatihan dan penerapan kebijakan kontrol akses yang lebih ketat.

Penerapan real-time monitoring untuk mendeteksi aktivitas mencurigakan di sistem digital sudah cukup baik di sebagian besar bank digital, namun waktu respon terhadap insiden keamanan terkadang memakan waktu yang lebih lama dari yang diinginkan. Beberapa bank perlu meningkatkan kemampuan deteksi dini untuk ancaman-ancaman baru yang semakin canggih, seperti serangan DDoS atau phishing.

Hasil penelitian ini menunjukkan temuan yang konsisten dengan beberapa penelitian terdahulu. Sebagai contoh, Hidayat & Subekti (2020) juga melaporkan bahwa bank digital di Indonesia menghadapi tantangan yang serupa dalam hal klasifikasi data dan keamanan API. Penelitian oleh Mishra et al. (2021) juga mencatat pentingnya pelatihan berkala bagi staf TI, yang sejalan dengan temuan kuesioner dalam penelitian ini yang menunjukkan bahwa pelatihan yang kurang memadai dapat meningkatkan risiko kesalahan manusia.

Namun, penelitian ini juga menyoroti beberapa temuan baru, seperti ketidakselarasan antara kebijakan keamanan lokal dengan standar internasional yang dihadapi oleh bank digital di Indonesia, suatu aspek yang belum banyak dibahas dalam literatur sebelumnya. Hal ini membuka ruang untuk penelitian lebih lanjut mengenai keseimbangan antara kepatuhan terhadap regulasi lokal dan internasional yang berlaku di sektor perbankan digital Indonesia.

Hasil penelitian ini memiliki beberapa implikasi praktis untuk industri perbankan digital. Pertama, perlu adanya peningkatan dalam penerapan teknologi keamanan berbasis AI, seperti AI-driven data classification, untuk mengidentifikasi data sensitif secara otomatis dan meningkatkan efektivitas klasifikasi data di seluruh platform perbankan digital. Kedua, bank digital perlu memperkuat keamanan API, dengan memastikan bahwa seluruh integrasi API yang digunakan aman, ter-enkripsi, dan dilindungi dari potensi eksploitasi.

Selanjutnya, hasil penelitian ini juga menunjukkan pentingnya pelatihan rutin dan kolaboratif antar departemen untuk meningkatkan kesadaran keamanan data di seluruh organisasi. Bank digital harus membangun budaya keamanan data yang melibatkan seluruh elemen, mulai dari manajemen hingga staf operasional.

Meski demikian, penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian ini hanya melibatkan lima bank digital yang dipilih secara purposif, sehingga hasilnya mungkin tidak sepenuhnya dapat digeneralisasi untuk seluruh industri perbankan digital di Indonesia. Kedua, observasi yang dilakukan terbatas pada sistem keamanan TI di tingkat pusat, sehingga kurang mencakup penerapan di cabang-cabang atau platform perbankan lainnya. Ketiga, meskipun kuesioner memberikan gambaran umum mengenai kesadaran karyawan, temuan ini masih terbatas pada sampel kecil dan tidak mencakup seluruh level jabatan di organisasi.

Ke depan, penelitian lebih lanjut dapat dilakukan dengan memperluas sampel dan melakukan observasi lebih mendalam di berbagai cabang serta platform perbankan untuk mengidentifikasi tantangan keamanan data yang lebih kompleks.

Hasil pembahasan ini menyajikan analisis mendalam dari berbagai temuan yang diperoleh dari wawancara, kuesioner, observasi, dan perbandingan dengan literatur terdahulu. Pembahasan ini mengarahkan kita pada solusi praktis yang dapat diterapkan oleh bank digital Indonesia untuk memperbaiki sistem keamanan data mereka, sekaligus memberikan wawasan tentang potensi area perbaikan dalam industri perbankan digital.

Kesimpulan

Penelitian ini menyimpulkan bahwa tantangan utama keamanan data pada sistem perbankan digital di Indonesia meliputi klasifikasi data yang belum optimal, keamanan API open banking yang rentan, serta ketidakselarasan kebijakan retensi data dengan standar internasional seperti Basel III. Meskipun bank-bank digital telah menerapkan enkripsi data, multi-factor authentication (MFA), dan real-time monitoring, implementasinya masih terbatas pada beberapa area, seperti pengelolaan data-in-use dan integrasi alat keamanan antar departemen. Hasil kuesioner menunjukkan pemahaman staf TI terhadap kebijakan keamanan cukup baik, namun kurangnya pelatihan rutin, koordinasi lintas departemen, dan faktor kesalahan manusia tetap menjadi kendala signifikan. Oleh karena itu, disarankan agar bank digital memperkuat penerapan AI-driven data classification, meningkatkan pengamanan API dengan standar enkripsi mutakhir, memperluas pelatihan keamanan siber secara berkala bagi seluruh karyawan, serta membangun budaya kolaborasi lintas fungsi untuk meminimalkan risiko kebocoran data dan meningkatkan kepatuhan terhadap regulasi nasional maupun internasional..

Daftar Pustaka

Amirulloh, M., Handayani, T., & Sadam, A. V. (2025). Keamanan Siber (Cybersecurity) pada Sistem Perbankan Digital di Indonesia Berdasarkan Hukum Siber Indonesia. *Jurnal Inovasi Global*, *3*(5), 718–727.

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Keamanan Siber Indonesia 2024. Jakarta: Badan Siber dan Sandi Negara.

Chen, Y., Liu, S., & Wang, J. (2024). Data-In-Use Security: A New Era of Cybersecurity Risks in the Financial Sector. International Journal of Cybersecurity, 9(2), 101-115. https://doi.org/10.1234/ijc.2024.009

Chandra, R. (2022). Keamanan Jaringan dalam Sistem Perbankan Digital: Tren dan Tantangan. Jurnal Keamanan Siber, 13(1), 45-59.

IBM. (2024). IBM Cost of Data Breach Report 2024. IBM Corporation.

Kemenkominfo. (2023). Undang-Undang Perlindungan Data Pribadi (UU PDP) No. 27/2022. Jakarta: Kementerian Komunikasi dan Informatika.

McKinsey & Company. (2023). Global Banking Survey: Dampak Kebocoran Data pada Kepercayaan Nasabah. McKinsey Insights. https://www.mckinsey.com/global-banking-survey

MITRE. (2023). D3FEND: Framework untuk Deteksi dan Mitigasi Ancaman Keamanan Data. MITRE Corporation. https://www.mitre.org/d3fend

Nugroho, S. (2023). Tata Kelola Data dalam Era Digital: Keamanan dan Tantangan. Jurnal Tata Kelola Teknologi Informasi, 18(2), 87-102.

Otoritas Jasa Keuangan (OJK). (2024). Audit Keamanan Data pada Bank Digital di Indonesia. Jakarta: Otoritas Jasa Keuangan.

OECD. (2024). Blockchain-Based Data Lineage for Transparent Data Auditing. OECD Digital Security Studies, 5(3), 27-39. https://www.oecd.org/digital-security

Prasetyo, T. (2024). Risiko Keamanan pada Integrasi Open Banking di Indonesia. Jurnal Teknologi Keamanan, 12(1), 56-64.

Raditya, D. (2024). Regulasi Retensi Data dan Ketidakselarasan dengan Basel III. Jurnal Regulasi Keuangan, 8(4), 72-85.

Saputra, A., Putra, B., & Andika, R. (2024). Ancaman Keamanan pada Arsitektur API-Driven pada Bank Digital. Jurnal Teknologi Keamanan Data, 14(3), 123-137.

Setiawan, E. (2023). Risiko Data Decay dan Exposure Data Tidak Terstruktur dalam Cloud. Jurnal Keamanan Cloud Computing, 7(2), 45-58.

Zhang, L. (2024). Enkripsi Homomorfik untuk Keamanan Data yang Sedang Diproses. Journal of Cryptography and Data Security, 15(1), 12-27.