

**Meta-Analisis Dampak Pencurian Data terhadap Tingkat
Kepercayaan Nasabah pada Layanan Perbankan**

***Meta-Analysis of the Impact of Data Theft on Customer
Trust Levels in Banking Services***

Risky Mezi Muria¹, Imam Wahyudi², Ika Oktaviana Dewi³

¹Universitas Negeri Jakarta, Indonesia

^{2,3}Universitas Islam Madura, Indonesia

*¹Corresponding email: riamura97@gmail.com

ABSTRAK - Penelitian ini bertujuan untuk menganalisis dampak pencurian data terhadap tingkat kepercayaan nasabah pada layanan perbankan melalui pendekatan meta-analisis. Pencurian data telah menjadi ancaman signifikan bagi industri perbankan, yang tidak hanya menyebabkan kerugian finansial tetapi juga mempengaruhi kepercayaan nasabah terhadap institusi perbankan. Dengan mengumpulkan dan menganalisis data dari berbagai studi sebelumnya, penelitian ini mengeksplorasi faktor-faktor yang mempengaruhi persepsi keamanan, risiko yang dirasakan, dan tingkat kepercayaan nasabah setelah insiden pencurian data. Hasil meta-analisis menunjukkan bahwa pencurian data secara signifikan menurunkan tingkat kepercayaan nasabah, yang pada gilirannya mempengaruhi keputusan mereka untuk menggunakan layanan perbankan online. Temuan ini juga mengidentifikasi bahwa penerapan langkah-langkah keamanan yang kuat dan transparansi dalam penanganan insiden dapat membantu memulihkan kepercayaan nasabah. Penelitian ini memberikan wawasan penting bagi bank dan regulator dalam mengembangkan strategi untuk meningkatkan keamanan data dan membangun kembali kepercayaan nasabah di era digital.

Kata Kunci: Pencurian Data, Kepercayaan Nasabah, Layanan Perbankan, Meta-Analisis, Keamanan Data

ABSTRACT - This study aims to analyze the impact of data theft on the level of customer trust in banking services through a meta-analysis approach. Data theft has become a significant threat to the banking industry, which not only causes financial losses but also affects customer trust in banking institutions. By collecting and analyzing data from various previous studies, this study explores the factors that influence customer security perceptions, perceived risks, and levels of trust after a data theft incident. The results of the meta-analysis indicate that data theft significantly decreases customer trust levels, which in turn affects their decision to use online banking services. The findings also identify that implementing strong security measures and transparency in incident handling can help restore customer trust. This study provides important insights for banks and regulators in developing strategies to improve data security and rebuild customer trust in the digital era.

Keywords: Data Theft, Customer Trust, Banking Services, Meta-Analysis, Data Security

PENDAHULUAN

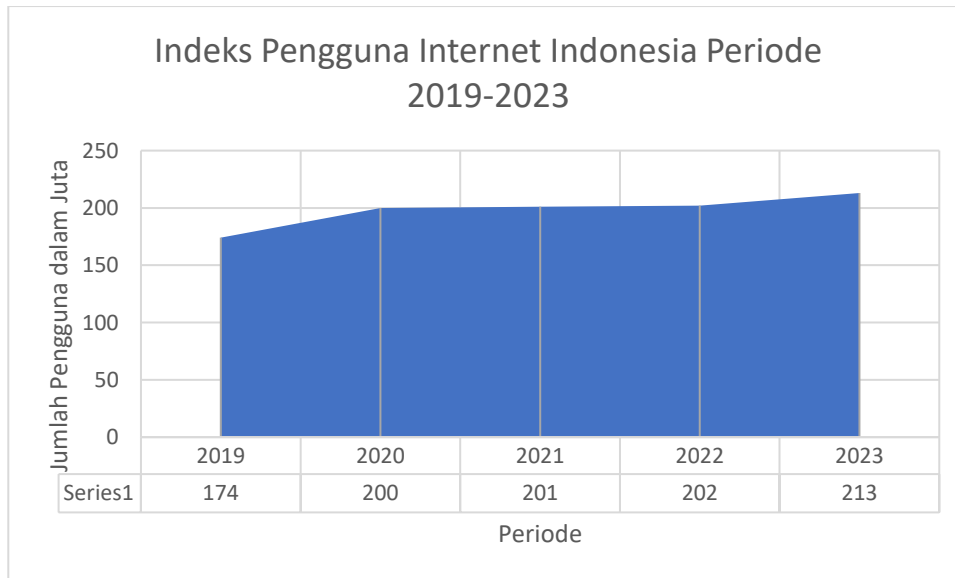
Perkembangan teknologi dan informasi saat ini sudah semakin pesat, begitu juga di dunia perbankan. Untuk selalu meningkatkan pelayanan sekarang dunia perbankan sudah mengembangkan pelayanan jasa-jasa perbankan yang diselaraskan dengan kemajuan teknologi dan informasi. Sebagai contoh dunia perbankan sudah mengeluarkan suatu layanan digital yang bernama *Electronic Banking (E-Banking)*. Kemudahan layanan perbankan yang dilakukan secara elektronik ini bertujuan untuk mempermudah nasabah dalam memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah, dan sesuai dengan kebutuhan (*customer experience*), serta dapat dilakukan secara mandiri sepenuhnya oleh nasabah dengan memperhatikan aspek pengamanan (Otoritas Jasa Keuangan, 2018). Namun dalam beberapa kasus, serangan *hacker* dapat menyebabkan gangguan pada layanan digital di bank. Gangguan tersebut dapat mencakup pencurian informasi nasabah, gangguan pada sistem perbankan atau pencurian dana yang tidak sah.

Serangan *hacker* terhadap bank tidak hanya menimbulkan ketidaknyamanan bagi nasabah, tetapi juga menimbulkan kerugian finansial dan reputasi bagi bank. Setiap perangkat apa pun yang terhubung ke Internet tidak tertutup kemungkinan mendapat serangan keamanan, karena selalu ada pihak-pihak yang ingin mengambil keuntungan dari serangan tersebut. Masalah dalam layanan digital yang terganggu oleh serangan *hacker* di perbankan melibatkan aspek yang sangat penting dalam dunia keuangan, yaitu keamanan dan kepercayaan. Perlu disadari bahwa risiko dari pencurian data dan serangan keamanan ini dapat sangat mengancam industri perbankan seperti merusak citra atau reputasi perusahaan.

Pencurian data dinilai mampu mempengaruhi kepercayaan nasabah, dan yang paling utama dampak dari kepercayaan nasabah dapat meningkatkan atau mengurangi pendapatan perbankan (Sari & Aprianti, 2020; Strzelecki & Rizun, 2022; Temkar & Vardhini, 2023) Pencurian data menjadi trending kembali pada saat pandemic covid-19 berlangsung (Alwi et al., 2023), pandemic covid-19 secara tidak sengaja mengubah

perilaku konsumen yang sebelumnya *physical economy* menjadi kearah *virtual economy* (Belitski et al., 2022).

Perilaku tersebut ditunjukkan dengan indeks pertumbuhan pengguna internet di Indonesia dari tahun 2019-2023 terus mengalami peningkatan hal tersebut ditunjukkan oleh gambar 1 sebagai berikut:



Gambar 1. Indeks Pengguna Internet Indonesia Periode 2019-2023

Berdasarkan gambar 1 diatas perlu diketahui bahwa jumlah pengguna internet Indonesia pada tahun 2013 berjumlah 85% dari jumlah penduduk Indonesia. Tinggi jumlah pengguna internet tersebut dapat memicu kejahatan digital atau cybercrime seperti pencurian data (Bhuller et al., 2012; Kim et al., 2011; Patel et al., 2017; Sharma et al., 2019; Stevani & Sudirman, 2021). Pencurian data merupakan tindakan yang merampas informasi sensitif tanpa izin, seperti data pribadi, keuangan, atau perusahaan. Hal ini dapat mengakibatkan berbagai masalah, termasuk pembobolan rekening, pencurian akun media sosial, penipuan, dan pencatutan identitas. Ancaman ini memicu kekhawatiran akan privasi dan keamanan data individu ataupun organisasi (Al-Harrasi et al., 2023; Angelis & Miller, 2021; Clough, 2011)

Mencuatnya pencurian data di Indonesia terjadi pada tahun 2022 dan menjadi masalah serius yang harus segera ditangani baik oleh organisasi maupun pemerintah. Beberapa kasus yang mencuat diantaranya bocornya data pelanggan Indihome, PLN, Jasa Marga, SIM card, KPU, Polri, Data Pejabat, My Pertamina, Pedulilindungi, dan Nasabah

Perbankan (CNN Indonesia, 2022; Hukuma, 2023). Kasus pencurian data nasabah perbankan menjadi sorotan publik mengingat perbankan sebagai lembaga yang sangat riskan (ACFE, 2017; Setiawan, 2024; Setiawan & Wahyudi, 2023).

Atas beberapa kasus tersebut atensi terhadap pencurian data terutama dalam perbankan harus segera disikapi dengan baik oleh pemerintah, organisasi bahkan individu (Solove, 2003). (Al-Harrasi et al., 2023; Barati & Yankson, 2022; Cassim, 2015) menyatakan bahwa dampak dari pencurian data yang ditimbulkan sangatlah signifikan seperti kerugian finansial, ancaman keamanan, penyalahgunaan data dan gangguan operasional. (Belitski et al., 2022; Corbitt et al., 2003; M. Zidny Nafi' Hasbi, 2019; Nguyen-Thi et al., 2021) menggambarkan kerugian finansial sebagai penurunan pendapatan yang diakibatkan berkurangnya kepercayaan antara entitas keuangan (perbankan) dengan nasabah. (Hakim, 2018; Mukherjee & Nath, 2003) dalam kajiannya menerangkan bahwa Kepercayaan nasabah adalah aspek yang sangat penting dan harus dijaga, karena nasabah merupakan tulang punggung utama dalam industri perbankan. (Achmad Rasyid Jauhari & Shiroth Rasyid Jauhari, 2022; Megawati et al., 2018; Rivaldo et al., 2022) menambahkan bahwa kepercayaan nasabah merupakan elemen kunci dalam hubungan antara bank dan nasabah. Ini tercermin dalam beberapa penelitian yang menyoroti peran penting kepercayaan dalam berbagai konteks terkait layanan perbankan.

Pengaruh terhadap Tingkat Kepuasan: Penelitian menunjukkan bahwa kepercayaan nasabah berpengaruh signifikan terhadap tingkat kepuasan nasabah terhadap layanan perbankan, terutama dalam situasi yang melibatkan pandemi COVID-19. Kepercayaan yang tinggi dapat meningkatkan kepuasan nasabah terhadap penggunaan layanan perbankan, yang pada gilirannya memperkuat hubungan antara bank dan nasabah (Sitorus & Yustisia, 2018; Syarifuddin, 2021). Mediator Pengaruh terhadap Loyalitas: Kepercayaan nasabah juga berperan sebagai mediator pengaruh terhadap loyalitas nasabah. Hal ini menunjukkan bahwa kepercayaan yang kuat dapat meningkatkan loyalitas nasabah terhadap bank, yang merupakan indikator penting bagi keberhasilan jangka panjang bank dalam mempertahankan basis nasabahnya (Batuhan GEÇİT & Taşkin, 2020; Murti, 2021; Osman & Sentosa, 2013).

Pengaruh terhadap Loyalitas Nasabah: penelitian lain menegaskan bahwa kepercayaan nasabah secara langsung memengaruhi loyalitas nasabah terhadap bank. Kepercayaan yang tinggi pada bank dapat meningkatkan loyalitas nasabah dan memperkuat hubungan jangka panjang antara bank dan nasabahnya (Leninkumar, 2017; Lubis et al., 2022). Pengaruh terhadap Kualitas Layanan: Penelitian juga menunjukkan bahwa kepercayaan nasabah berpengaruh terhadap persepsi kualitas layanan bank. Kepercayaan yang tinggi dapat meningkatkan persepsi nasabah terhadap kualitas layanan yang diberikan oleh bank, yang pada gilirannya dapat meningkatkan loyalitas nasabah (Kundu, 2018; Lien et al., 2014; Mohamad Aras et al., 2023).

Setelah bagian ini, penulis akan membahas tinjauan literatur terkait pencurian data dan layanan perbankan. Bagian berikutnya akan menjelaskan metodologi penelitian yang mencakup metode yang digunakan. Setelah itu, penulis akan menyajikan hasil penelitian serta analisisnya dalam bagian hasil dan pembahasan. Terakhir, tulisan akan diakhiri dengan kesimpulan.

KERANGKA TEORITIS

Perbankan

Perbankan merupakan wali masyarakat yang dipercaya untuk mengelola dan mengatur keuangan milik masyarakat, oleh sebab itu perbankan harus melindungi uang nasabah terhadap resiko penipuan keuangan seperti yang tercantum dalam Undang-Undang No. 10 tahun 1998 tentang Undang-Undang Perbankan, antara lain mulai dari pidana yang berkaitan dengan perizinan industri perbankan, tindak pidana yang berkaitan dengan rahasia bank, tindak pidana yang berkaitan dengan pengawasan dan pembinaan bank, yang berkaitan dengan usaha bank serta tindak pidana kejahatan perbankan yang paling ekstrem adalah perampokan bank hingga pengalihan rekening secara tidak sah. Kegagalan perbankan dalam menjaga kepercayaan perbankan dapat berdampak sistemik dan mengganggu stabilitas keuangan Nasional (Meliana & Hartono, 2019).

Cybercrime

Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet (Setiawan, 2024). *Cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai

objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain (Abidin, 2015; Setiawan & Wahyudi, 2023). Cybercrime adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (cyber space), baik yang menyerang fasilitas umum didalam cyber space ataupun kepemilikan pribadi (Hakim, 2018). (Wibowo et al., 2021) *cybercrime* sering identic sebagai kejahatan yang menggunakan computer atau perangkat keras. *Cybercrime* dianggap sebagai risiko kejahatan digital yang dilakukan oleh orang yang tidak bertanggung jawab dengan pengrusakan system (Julianti & Sugiantari, 2021)

Jenis-jenis *cybercrime* yang dapat terjadi pada keamanan data nasabah:

1. *Unauthorized Access* merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya dengan tujuan untuk mensabotase atau melakukan pencurian data. Misalnya Probing atau port scanning merupakan contoh dari kejahatan ini (Gema, 2000).
2. *Email Phising* adalah tindakan memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank, nomor kartu kredit seseorang secara tidak sah. Penyebaran virus dilakukan secara sengaja dan dilakukan dengan menggunakan email (Julianti & Sugiantari, 2021).
3. *Scamming* adalah penipuan yang sangat mirip dengan phishing, namun bukannya mengelabui pengguna agar berbagi informasi pribadi, penipu mencoba memeras uang secara langsung dari pengguna (Szurdi et al., 2020).
4. *Data Forgery* (Pemalsuan data) kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Pemalsuan data ini bisa menjadi sangat berbahaya, terutama jika sudah menyangkut dengan kartu kredit, serta pinjaman online. Salah satu contoh data forgery adalah pemalsuan alamat pada situs bank, dan pemalsuan identitas.
5. *Infringements of Privacy* adalah kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara *computerized*. Yang apabila diketahui orang lain maka dapat merugikan korban secara materiil atau immaterial, seperti nomor PIN ATM, nomor kartu kredit dan sebagainya (Gema, 2000).

6. *Cyber Espionage, Sabotage, and Extortion:*

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet (Abidin, 2015). Penipu dapat memblokir akses ke sebuah sistem atau data, sehingga korban tidak dapat mengakses atau mengendalikan data di dalamnya.

7. *Carding* merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet. Jenis carding yaitu *Wiretapping* (transaksi kartu kredit disadap melalui jaringan komunikasi), *Counterfeiting* (kartu kredit dipalsukan sehingga terlihat sangat mirip dengan aslinya), *Phishing* (mencuri informasi kartu kredit melalui situs web), dan *Misuse of Card Data* (penyalahgunaan kartu kredit yang tidak diketahui oleh pemilik aslinya) (Zulkarnain & Sutabri, 2023).

8. *Hacking dan Cracker* mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran (Abidin, 2015).

9. *Cybersquatting and Typosquatting*

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal (Bhusari & Rampure, 2022). Sedangkan *typosquatting* adalah kejahatan dengan membuat domain mirip (sengaja membuat kesalahan ketik pada nama domain yang akan didaftarkan) dengan nama domain perusahaan lain. Kejahatan ini dapat mengambil informasi pribadi, kredensial, dan detail kartu kredit dari para korban serta dapat memasang malware di komputer pengunjung (Szurdi et al., 2020).

10. *Hijacking* (pembajakan) merupakan jenis malware yang mengambil alih browser untuk mendapatkan akses browser tanpa izin dan melakukan sesuatu hal yang tidak pengguna inginkan biasanya kejahatan ini menyerang situs jejaring sosial dan situs perbankan (Kumar Baitha & Vinod, 2018) selain itu pembajakan browser juga dapat berisi spyware (perangkat pengintai) yang bertujuan untuk mendapatkan informasi dan data sensitif.

Berdasarkan motif kegiatan yang dilakukannya, *cybercrime* dapat digolongkan menjadi dua jenis sebagai berikut (Abidin, 2015):

1. *Cybercrime* sebagai tindakan murni kriminal. Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (spamming) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.
2. *Cybercrime* sebagai kejahatan "abu-abu". Pada jenis kejahatan di internet yang masuk dalam wilayah "abu-abu", cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

Berdasarkan sasaran kejahatan, *cybercrime* dapat dikelompokkan menjadi beberapa kategori seperti berikut ini (Abidin, 2015):

1. *Cybercrime* yang menyerang individu (Against Person). Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain: Pornografi. Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas. Cyberstalking. Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya. Cyber-Tresspass. Kegiatan yang

- dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.
2. *Cybercrime* menyerang hak milik (Against Property) *Cybercrime* yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquatting, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain
 3. *Cybercrime* menyerang pemerintah (Against Government) *Cybercrime* Against Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya cyber terorism sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

Pencurian Data

Salah satu bentuk cyber related crime yang terus mengalami perkembangan dan sedikitnya korban yang sadar akan viktimisasi kejahatan tersebut adalah pencurian identitas atau identity theft. Privasi akan data personal kemudian menjadi isu yang cukup penting dalam era big data (Sun et al., 2020). Pencurian data menjadi permasalahan yang cukup disoroti dalam masyarakat modern yang terhubung dengan internet. Berbeda dengan pencurian data konvensional, pencurian data pribadi digital melalui medium internet dapat mengakibatkan kerugian yang sangat besar kepada korbannya (Chawki & Abdel Wahab, 2006). Pencurian data didalamnya terdapat banyak komponen kegiatan ilegal seperti pencurian dan penyalahgunaan penggunaan data pribadi, yang bisa digunakan untuk pelanggaran lain seperti penipuan akun, pemalsuan dengan dokumen palsu, perdagangan manusia, hingga terorisme (Veiraitis, Copes, & Birch, 2014). Sementara itu, pencurian data juga dapat dijelaskan sebagai langkah awal pengumpulan, pemilikan, dan perdagangan identitas untuk tujuan kejahatan seperti penipuan atau pun penyalahgunaan kartu debit dan kredit (Justice, 2010). Menurut CIPPIC, terdapat setidaknya 12 tipe informasi pribadi yang sering di curi, yaitu: (1) nomor kartu kredit, (2) nomor CW (di belakang kartu kredit), (3) laporan kredit, (4) Social Security Number, (5) nomor surat izin mengemudi, (6) nomor ATM, (7) nomor telepon, (8) nomor gadai, (9) tanggal lahir, (10) kata sandi dan PIN, (11) alamat rumah, (12) nomor handphone (Policy & Clinic, 2007).

METODE PENELITIAN

Penelitian ini menggunakan metode meta analisis. Meta-analisis adalah metode statistik yang menggabungkan dan menganalisis hasil dari beberapa studi independen tentang topik yang sama untuk mencapai kesimpulan yang lebih kuat secara statistik. Ini melibatkan sintesis data kuantitatif dari penelitian-penelitian yang ada untuk menghasilkan estimasi efek yang lebih akurat (Carlin, 2000). Prosesnya melibatkan identifikasi penelitian yang relevan, ekstraksi data yang relevan dari setiap studi, penggabungan data untuk analisis statistik, dan interpretasi hasilnya. Meta-analisis digunakan untuk mengukur ukuran efek suatu intervensi atau fenomena tertentu dengan cara mengumpulkan dan menganalisis data dari penelitian-penelitian sebelumnya yang telah dilakukan tentang topik tersebut (Lee, 2018). Hal ini membantu dalam menyederhanakan informasi dan menyediakan gambaran yang lebih komprehensif tentang topik yang diteliti (Khaer et al., 2023; Lee, 2019).

Sumber data dalam penelitian ini meliputi artikel ilmiah dari berbagai jurnal internasional dan nasional yang diakses melalui aggregator seperti Emerald, ScienceDirect, Scopus, dan Google Scholar (Dewi et al., 2023, 2024a, 2024b; Muria et al., 2022; Risky Mezi Muria, 2023; Wahyudi, Alim, et al., 2021; Wahyudi, Muntasa, et al., 2021). Penulis melakukan proses pengumpulan, pengolahan, dan penyajian data secara sistematis untuk mengidentifikasi hubungan antar-paper terkait penelitian pencurian data terhadap tingkat kepercayaan nasabah pada layanan perbankan dengan bantuan software publish or perish. Metode analisis meta digunakan untuk mengurai unsur-unsur dari setiap paper hasil penelitian dan menemukan hubungan antara mereka, sehingga dapat mencapai kesimpulan dan pemahaman yang komprehensif terhadap objek penelitian yang diteliti (Novie et al., 2023).

HASIL DAN PEMBAHASAN

Proses reduksi data dimulai dengan menjadikan Emerald, ScienceDirect, Scopus dan Google Scholar sebagai pengumpul data. Kata kunci yang digunakan adalah "theft of data; bank; impact of theft". Setelah melewati serangkaian filter maka kami menemukan 26 studi terbitan jurnal internasional dan nasional terkait dampak pencurian data terhadap layanan perbankan yang secara dominan membahas tema sesuai dengan keyword yang sudah ditetapkan yakni "the impact of banking data theft".

Berikut ini merupakan tabel lengkap berisi nama penerbit disertai jumlah paper terbitan the impact of banking data theft dalam riset.

Tabel 1. Publikasi Riset Bertema *The Impact of Banking Data Theft*

<i>Publication</i>	<i>Total of publication</i>	<i>Type of publication</i>
International Symposium on Big Data and Cloud Computing	1	Proceedings
Fiabilitate Si Durabilitate	1	Journal
Indonesian Journal of Multidisciplinary	1	Journal
Jurnal Peneliti Ekonomi	1	Journal
Jurnal Cahaya Mandalika	1	Journal
Jurnal Mantik	1	Journal
Conference On Islamic Management, Accounting, And Economics (CIMAЕ) Proceeding	1	Proceedings
Jemper (Jurnal Ekonomi Manajemen Perbankan)	1	Journal
International Journal of Bank Marketing	1	Journal
Potchefstroom Electronic Law Journal	1	Journal
Journal IMAGE	1	Journal
Jurnal Ilmu Multidisiplin	1	Journal
Criminal Law Forum	1	Journal
Journal Of Public Administration	1	Journal
Wacana Journal of Social and Humanity Studies	1	Journal
Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi	1	Journal
Information Systems	1	Journal
Gordon Institute of Business Science University of Pretoria	1	Journal
Forum Ekonomi	1	Journal
Journal Of Emerging Technologies and Innovative Research (JETIR)	1	Journal
Journal Of Judicial Review	1	Journal
Applied Sciences	1	Journal
Banks And Bank Systems	1	Journal
Proceedings of The ACM Symposium on Women in	1	Proceedings

Research		
International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)	1	Proceedings
Procedia Computer Science	1	Journal
Total	26	

Berdasarkan Tabel 1 diatas, sumber publikasi yang paling dominan berasal dari jurnal sebanyak 22 paper dan prosiding sebanyak 5 paper. Setiap publikasi baik di jurnal ataupun di prosiding masing masing menerbitkan 1 paper. Selanjutnya penelitian ini dilakukan dalam rentang waktu 2003 sampai 2023 atau dalam kurun waktu dua decade kebelakang. Selama kurun waktu tersebut penelitian terkait the impact of banking data theft banyak dilakukan pada interval waktu 4 tahun terakhir yaitu tahun 2020 sampai dengan 2023. Jumlah paper yang paling terbit paling banyak adalah 5 paper pada tahun 2022 dan 2023

Tabel 2. Klasifikasi Publikasi Berdasarkan Tahun Penerbitan

<i>Year of Publication</i>	Total
2003	1
2011	1
2014	1
2015	3
2016	1
2018	2
2019	1
2020	4
2021	2
2022	5
2023	5
Total	26

Penelitian ini mereview 26 paper yang ada berdasarkan negara yang menjadi studi kasus terkait penelitian data theft in banking. Negara Indonesia merupakan negara terbanyak yang menjadi studi kasus dalam penelitian terkait tema tersebut sebanyak 14 paper. Selain itu, negara yang sering menjadi studi kasus dalam penelitian ini adalah india 3 paper, afrika selatan 2 paper, Indian 2 paper serta beberapa negara lainnya sebanyak 1 paper (Tabel 3)

Tabel 3. Klasifikasi Publikasi Berdasarkan Negara

<i>Case Study</i>	Total
Indonesia	14
Afrika Selatan	2
Australia	1
Arab Saudi	1
India	3
Ekuador	1
Korea	1
Indian	2
Romania	1
Total	26

Selanjutnya, klasifikasi paper berdasarkan metodologi yang digunakan oleh penulis dapat dilihat dalam tabel 4. Sesuai hasil review pada 26 paper, terdapat dalam 3 kelompok kategori, yaitu pendekatan kuantitatif 11 paper atau 42% dari jumlah paper yang digunakan, pendekatan kualitatif 13 paper atau 50% dari jumlah paper yang digunakan, mix method 1 paper atau 4% dari jumlah paper yang digunakan, dan Cyber Security Financial Sector Management (CS-FSM) sebanyak 1 paper atau 4% dari jumlah paper yang digunakan.

Tabel 5. klasifikasi Berdasarkan Metode

<i>Research Method</i>	Total
Kuantitatif	11

Kualitatif	13
Mix Method	1
CS-FSM	1

PEMBAHASAN

Berdasarkan hasil analisis dan olah data, tema yang menjadi focus pembahasan para peneliti adalah sebagaimana terncatum pada table 6 berikut ini.

Tabel 6. Tema Utama “*The Impact of Banking Data Theft*”

Temuan utama	Ranking
<i>Big Data Analytics and Banking</i>	1
<i>Cybercrime and Data Protection</i>	2
<i>Cybersecurity and Power Industry</i>	3
<i>Sharia Banking in Indonesia</i>	4
<i>Digital Banking Challenges</i>	5
<i>Customer Service and Loyalty</i>	6
<i>Customer Loyalty in Banking</i>	7
<i>Online Relationship Banking</i>	8
<i>Identity Theft</i>	9
<i>Consumer Loyalty and Mobile Banking</i>	10

Berdasarkan data yang terdapat dalam dokumen, terlihat bahwa berbagai studi kasus dan penelitian mengenai perbankan digital, keamanan siber, dan loyalitas nasabah telah dilakukan di berbagai negara, dengan fokus pada berbagai aspek penting dalam industri keuangan. Berikut adalah analisis dan pembahasan merujuk pada data yang telah disebutkan:

Big Data dalam Perbankan: Studi berjudul "Impact of Big Data Analytics on Banking Sector" (2015) dari India menunjukkan bagaimana analitik big data digunakan untuk mengoptimalkan operasional dan meningkatkan pengambilan keputusan di sektor perbankan. Dengan meningkatnya kompleksitas data di era digital, big data menjadi alat yang sangat penting untuk meningkatkan efisiensi dan daya saing bank. **Penerapan big data** memungkinkan perbankan untuk memahami perilaku konsumen lebih baik dan memberikan layanan yang dipersonalisasi, meningkatkan loyalitas nasabah (Krismiaji & Grediani, 2019; Srivastava & Gopalkrishnan, 2015).

Keamanan Data dan Perbankan Digital: Beberapa penelitian seperti "Impact Of The Loss And Theft Of Electronic Data On Companies" (2014) dan "Pertanggungjawaban Lembaga Perbankan terhadap Pencurian Data Nasabah" (2018) membahas tantangan keamanan siber yang terus meningkat seiring dengan digitalisasi perbankan. Studi ini menyoroti bagaimana **serangan siber** dan pencurian data dapat menyebabkan kerugian signifikan, baik secara finansial maupun reputasi, terutama jika perbankan gagal mengamankan informasi pribadi nasabah (Hakim, 2018; Iovan & Dinu, 2014).

Loyalitas Nasabah: Banyak studi meneliti faktor-faktor yang memengaruhi loyalitas nasabah, seperti "Pengaruh kualitas layanan dan kepercayaan nasabah terhadap loyalitas nasabah" (2019) dan "Pengaruh keamanan, keandalan, dan kepuasan terhadap loyalitas konsumen dalam menggunakan mobile banking" (2020). Hasil dari penelitian-penelitian ini menggarisbawahi pentingnya **kualitas layanan** dan **kepercayaan** dalam mempertahankan loyalitas nasabah, terutama di tengah persaingan yang semakin ketat di era perbankan digital (Handoko & Ronny, 2021; Sari & Aprianti, 2020).

Peluang dan Tantangan Perbankan Digital: Studi "Tantangan Dan Peluang Perbankan Digital" (2023) menyoroti bagaimana inovasi teknologi dan digitalisasi menawarkan peluang besar bagi bank untuk memperluas layanannya, namun juga menghadirkan tantangan signifikan terkait **adopsi teknologi** dan **keamanan data**. Perbankan harus mampu berinovasi dalam menawarkan layanan yang lebih cepat dan aman untuk tetap kompetitif (Alwi et al., 2023).

Pengaruh Pencurian Data Terhadap Kepercayaan Nasabah: Insiden pencurian data yang terjadi pada layanan perbankan memengaruhi secara langsung tingkat kepercayaan nasabah. Sebuah studi di Afrika Selatan, Amerika Serikat, dan India menunjukkan bahwa kepercayaan nasabah menurun drastis setelah terjadi pencurian data atau serangan siber yang berhasil.

Tindakan Pemulihan Kepercayaan: Penelitian dari tahun 2020 mengenai dampak pencurian data pada loyalitas nasabah bank di Afrika Selatan menunjukkan bahwa pemulihan kepercayaan tidak hanya bergantung pada tindakan keamanan setelah insiden, tetapi juga pada transparansi dan komunikasi yang dilakukan oleh bank untuk mengatasi masalah tersebut.

Faktor yang Memengaruhi Tingkat Pemulihan Kepercayaan: Selain tindakan keamanan, komunikasi yang efektif dengan nasabah dan penyediaan solusi kompensasi juga memainkan peran penting dalam memulihkan kepercayaan. Studi yang dilakukan pada nasabah bank di Indonesia juga menegaskan bahwa kualitas layanan dan kepercayaan nasabah menjadi indikator penting dalam menjaga loyalitas nasabah setelah insiden pencurian data.

Loyalitas Nasabah dan Keamanan Data: Studi lain menunjukkan bahwa bank yang telah memperkuat keamanan data dan memiliki mekanisme perlindungan yang kuat dapat menjaga loyalitas nasabah lebih baik dibandingkan dengan bank yang kurang berinvestasi pada sistem keamanan siber.

KESIMPULAN

Berdasarkan data yang tersedia, terlihat bahwa adopsi teknologi, keamanan data, dan peningkatan kualitas layanan adalah tiga tema utama yang sangat penting untuk meningkatkan daya saing bank di era digital. Big data analytics, loyalitas nasabah, dan pengelolaan risiko siber menjadi fokus utama untuk mengatasi tantangan yang dihadapi dalam transformasi perbankan digital di Indonesia dan global.

Referensi

- Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor*, 10(2), 1–8.
- ACFE. (2017). *Fraud Examiners Manual*. ACFE, 1913.
- Achmad Rasyid Jauhari, H., & Shiroth Rasyid Jauhari, M. (2022). Customer Service Strategy in Increasing the Number of Customers At Bank Bjb Syariah Braga Branch Office. *Journal of Public Administration*, 1(1), 1–8. <https://doi.org/10.61317/jc.v1i1.7>
- Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, 31(3), 875–888. <https://doi.org/10.1108/IJOA-01-2021-2598>
- Alwi, M. N., Bahari, F., Ramadhan, A., Andriani, M., & Semmawi, R. (2023). Tantangan Dan Peluang Perbankan Digital: Studi Kasus Inovasi Keuangan Dan Transformasi Perbankan. *Jurnal Cahaya Mandalika (JCM)*, Vol 3(No 2), 2160–2177.
- Angelis, J. N., & Miller, J. C. (2021). An empirical investigation of the

- effects of individuality on responses to data theft crimes. *IEEE Transactions on Engineering Management*, 68(6), 1663–1676. <https://doi.org/10.1109/TEM.2020.2974742>
- Barati, M., & Yankson, B. (2022). Predicting the Occurrence of a Data Breach. *International Journal of Information Management Data Insights*, 2(2), 100128. <https://doi.org/https://doi.org/10.1016/j.jjime.2022.100128>
- Batuhan GEÇİT, B., & Taşkin, E. (2020). The Effect of Value and Service Perceptions on Customer Loyalty for Electronic Commerce Sites; Mediator Role of Satisfaction and Trust. *Business Management Dynamics*, 10(03), 1–12.
- Belitski, M., Guenther, C., Kritikos, A. S., & Thurik, R. (2022). Economic effects of the COVID-19 pandemic on entrepreneurship and small businesses. *Small Business Economics*, 58(2), 593–609. <https://doi.org/10.1007/s11187-021-00544-y>
- Bhuller, M., Havnes, T., Leuven, E., & Mogstad, M. (2012). Broadband Internet: An Information Superhighway to Sex Crime? *SSRN Electronic Journal*, 3871. <https://doi.org/10.2139/ssrn.1881507>
- Bhusari, R. V., & Rampure, K. R. (2022). Cybersquatting: A Threat To The Globalising World. *Indian Journal of Law and Legal Research*, III(Ii), 1–22.
- Carlin, J. B. (2000). Tutorial in biostatistics. Meta-analysis: Formulating, evaluating, combining, and reporting (multiple letters). *Statistics in Medicine*, 19(5), 753–759. [https://doi.org/10.1002/\(SICI\)1097-0258\(20000315\)19:5<753::AID-SIM427>3.0.CO;2-F](https://doi.org/10.1002/(SICI)1097-0258(20000315)19:5<753::AID-SIM427>3.0.CO;2-F)
- Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal*, 18(2), 69–110. <https://doi.org/10.4314/pelj.v18i2.02>
- Chawki, M., & Abdel Wahab, M. (2006). Identity Theft in Cyberspace: Issues and Solutions. *Lex Electronica*, 11, 1–41.
- Clough, J. (2011). Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 22(1–2), 145–170. <https://doi.org/10.1007/s10609-011-9133-5>
- CNN Indonesia. (2022). *10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah*. Cnnindonesia.Com.
- Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, 2(3), 203–215. [https://doi.org/10.1016/S1567-4223\(03\)00024-3](https://doi.org/10.1016/S1567-4223(03)00024-3)
- Dewi, I. O., Wahyudi, I., & Setiawan, N. (2024a). Identity Theft In Peer-To-Peer Lending Platform. *Proceedings of the 2nd International & 5th*

- National Conference Accounting & Fraud*, 2(February), 1–12.
- Dewi, I. O., Wahyudi, I., & Setiawan, N. (2024b). PROBLEMATIKA TERKINI IMPLEMENTASI SAK EMKM SEBUAH STUDI LITERATUR. *Jafis*, 5(1), 1–29.
- Dewi, I. O., Wahyudi, I., Setiawan, N., & Uyun, J. (2023). Fraud Ditinjau dari Etika Profesi dan Etika Bisnis Kasus PT Garuda Indonesia. *Media Komunikasi Ilmu Ekonomi*, 40(1), 41–53. <https://doi.org/https://doi.org/10.58906/melati.v40i1.101>
- Gema, A. J. (2000). *Cybercrime, Sebuah Fenomena Di Dunia Maya*.
- Hakim, L. (2018). Pertanggungjawaban Lembaga Perbankan Terhadap Pencurian Data Nasabah. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*, 10(1), 01–15. <https://doi.org/10.28932/di.v10i1.918>
- Handoko, A. D., & Ronny, R. (2021). Pengaruh Faktor Keamanan, Keandalan Dan Kepuasan Terhadap Loyalitas Nasabah Bri Dalam Menggunakan Mobile Banking. *Image : Jurnal Riset Manajemen*, 9(2), 79–91. <https://doi.org/10.17509/image.v9i2.28598>
- Hukuma, S. Y. (2023). Selidiki Kasus Pencurian 15 Juta Data Nasabah BSI, Polri: Kami Tunggu Aduan. *Mediaindonesia.Com*.
- Iovan, S., & Dinu, M. B. (2014). Impact of the Loss and Theft of Electronic Data on Companies. *Fiability & Durability / Fiabilitate Si Durabilitate*, 1, 39–45.
- Julianti, L., & Sugiantari, A. A. P. W. (2021). Tanggung Jawab Hukum Perbankan dalam Pencurian Data Pribadi Nasabah dengan Teknik “Phising” Pada Transaksi Perbankan. *Prosiding Seminar Nasional Fh Unmas Denpasar*, 1, 96–105.
- Khaer, R., Firmansyah, A., & Saepul Rohman, P. (2023). Meta-Analysis Of Wakaf Based Sharia Microfinance Institutions. *Perisai: Islamic Banking and Finance Journal*, 7(2), 237–254. <https://doi.org/10.21070/perisai.v7i2.1661>
- Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 36(3), 675–705. <https://doi.org/10.1016/j.is.2010.11.003>
- Krismiaji, & Grediani, E. (2019). Effects of Company Size, Company Age, Audit Committee, and Auditor Quality on Sharia Information Disclosure Compliance -An Indonesian Sharia 'Financial Industry Evidence. *KnE Social Sciences*, 2019, 200–216. <https://doi.org/10.18502/kss.v3i26.5374>
- Kumar Baitha, A., & Vinod, S. (2018). Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology*, 7(2.6), 193. <https://doi.org/10.14419/ijet.v7i2.6.10566>
- Kundu, S. (2018). Impact of trust on the relationship of e-service quality

- and customer satisfaction. *EuroMed Journal of Business*, 34(1), 1–5.
- Lee, Y. H. (2018). An overview of meta-analysis for clinicians. *The Korean Journal of Internal Medicine*, 33(2), 277–283. <https://doi.org/10.3904/kjim.2016.195>
- Lee, Y. H. (2019). Strengths and Limitations of Meta-Analysis. *Korean J Med*, 94(5), 391–395. <https://doi.org/10.3904/kjm.2019.94.5.391>
- Leninkumar, V. (2017). The Relationship between Customer Satisfaction and Customer Trust on Customer Loyalty. *International Journal of Academic Research in Business and Social Sciences*, 7(4), 450–465. <https://doi.org/10.6007/ijarbss/v7-i4/2821>
- Lien, C. H., Wu, J. J., Chen, Y. H., & Wang, C. J. (2014). Trust transfer and the effect of service quality on trust in the healthcare industry. *Managing Service Quality*, 24(4), 399–416. <https://doi.org/10.1108/MSQ-11-2013-0255>
- Lubis, A., Effendi, I., & Rosalina, D. (2022). Pengaruh Kepercayaan dan Komitmen Terhadap Loyalitas Nasabah Bank Syariah Indonesia di Kota Medan. *Ekonomi, Keuangan, Investasi Dan Syariah (EKUITAS)*, 3(4), 896–902. <https://doi.org/10.47065/ekuitas.v3i4.1600>
- M. Zidny Nafi' Hasbi. (2019). Dampak Krisis Keuangan Global Terhadap Perbankan Di Indonesia. *LISAN AL-HAL: Jurnal Pengembangan Pemikiran Dan Kebudayaan*, 13(2), 385–400. <https://doi.org/10.35316/lisanalhal.v13i2.602>
- Megawati, T., Rofianty, & Hadiwidjojo, D. (2018). Role of Trust and Customer Satisfaction as a Mediation Effect of Human Resource Competence on Customer Loyalty (Study on Commercial Customer BCA Kanwil VII Malang). *Wacana*, 21(1), 34–41.
- Meliana, M., & Hartono, T. R. (2019). Fraud Perbankan Indonesia: Studi Eksplorasi. *Prosiding Seminar Nasional Pakar*, 1–7. <https://doi.org/10.25105/pakar.v0i0.4335>
- Mohamad Aras, Indra Nara Persada, & Septa Diana Nabella. (2023). the Influence of Service Quality, Trust, and Facilities on the Decision To Choose Sp Hotel Batam. *International Journal of Accounting, Management, Economics and Social Sciences (IJAMESC)*, 1(4), 417–431. <https://doi.org/10.61990/ijamesc.v1i4.39>
- Morgan, R. M., & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, 58(3), 20–38. [https://doi.org/10.1016/0022-0531\(82\)90041-2](https://doi.org/10.1016/0022-0531(82)90041-2)
- Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, 21(1), 5–15. <https://doi.org/10.1108/02652320310457767>
- Muria, R. M., Muntasa, A., Yusuf, M., & Hamzah, A. (2022). Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan Cyber Crime.

- Jurnal Aplikasi Teknologi Informasi Dan Manajemen (JATIM)*, 3(1), 12–20. <https://doi.org/10.31102/jatim.v3i1.1422>
- Murti, A. P. U. & Tri R. (2021). Kepuasan Nasabah Sebagai Mediator Pengaruh Kepercayaan Terhadap Loyalitas Nasabah. *Jurnal IKRA-ITH Ekonomika*, 4(2), 79–86.
- Nguyen-Thi, T., Pham-Thi-Ngoc, L., Nguyen-Ngoc, Q., Dang-Xuan, S., Lee, H. S., Nguyen-Viet, H., Padungtod, P., Nguyen-Thu, T., Nguyen-Thi, T., Tran-Cong, T., & Rich, K. M. (2021). An Assessment of the Economic Impacts of the 2019 African Swine Fever Outbreaks in Vietnam. *Frontiers in Veterinary Science*, 8(October), 1–14. <https://doi.org/10.3389/fvets.2021.686038>
- Novie, D., Arta, C., Leuhery, F., Abubakar, H., Yusuf, M., Cakranegara, P. A., Jayapura, P. P., Pattimura, U., Bosowa, U., Bandung, S., & Presiden, U. (2023). Literature Review: Analysis of the Relationship Between Training and Employee Performance in a Company Literature Review: Analisis Hubungan Antara Pelatihan dan Kinerja Karyawan di Sebuah Perusahaan. *Management Studies and Entrepreneurship Journal*, 4(1), 162–168.
- Osman, Z., & Sentosa, I. (2013). A study of mediating effect of trust on customer satisfaction and customer loyalty relationship in Malaysian rural tourism. *European Journal of Tourism Research*, 6(2), 192–206. <https://doi.org/10.54055/ejtr.v6i2.132>
- Otoritas Jasa Keuangan. (2018). Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum. *Ojk RI*, 1, 1–55.
- Patel, P., Kannoorpatti, K., Shanmugam, B., Azam, S., & Yeo, K. C. (2017). A theoretical review of social media usage by cyber-criminals. *2017 International Conference on Computer Communication and Informatics, ICCCI 2017*. <https://doi.org/10.1109/ICCCI.2017.8117694>
- Policy, C. I., & Clinic, P. I. (2007). *Techniques of identity theft*. 2(2).
- Risky Mezi Muria. (2023). Fraud Detection Credit Card: A Bibliometric Analysis Approach. *International Journal of Economics ...*, 5(October 2023), 391–398.
- Rivaldo, Y., Kamanda, S. V., & Yusman, E. (2022). The Effect Of Products, Services And Promotions On Decision On Customer Requests On Service Products At Bank BSI Tiban Batam Branch. *Jurnal Mantik*, 6(36), 2377–2384.
- Sari, R. J., & Aprianti, I. (2020). Pengaruh Kualitas Layanan Dan Kepercayaan Terhadap Loyalitas Nasabah (Studi Kasus Pada Nasabah Bank BNI Cabang JPK Bandung. *Jurnal Ekonomi Manajemen Perbankan*, 2(2), 77–84.

- Setiawan, N. (2024). Internet Banking Anti-Cybercrime. *Journal of Business Improvement*, 1(1), 1–12. <https://journal.iaialfatimah.ac.id/index.php/job/article/view/2>
- Setiawan, N., & Wahyudi, I. (2023). Pencegahan fraud pada kejahatan siber perbankan. *Kabillah: Journal of Social Community*, 8(1), 508–518. <https://doi.org/10.35127/kabillah.v8i1.280>
- Sharma, P., Gupta, D., & Khanna, A. (2019). e-Commerce Security: Threats, Issues, and Methods. In *Cyber Security in Parallel and Distributed Computing*. <https://doi.org/10.1002/9781119488330.ch4>
- Sitorus, T., & Yustisia, M. (2018). The influence of Service Quality and Customer Trust toward Customer Loyalty: The role of customer satisfaction. *International Journal for Quality Research*, 12(3), 639–654. <https://doi.org/10.18421/IJQR12.03-06>
- Solove, D. J. (2003). Identity theft, privacy, and the architecture of vulnerability. *Hastings Law Journal*, 54(4), 1227–1276. <https://doi.org/10.2139/ssrn.416740>
- Srivastava, U., & Gopalkrishnan, S. (2015). Impact of big data analytics on banking sector: Learning for Indian Banks. *Procedia Computer Science*, 50, 643–652. <https://doi.org/10.1016/j.procs.2015.04.098>
- Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. *Journal of Judicial Review*, 23(2), 197. <https://doi.org/10.37253/jjr.v23i2.5028>
- Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability (Switzerland)*, 14(10). <https://doi.org/10.3390/su14105866>
- Sun, Z., Strang, K. D., & Pambel, F. (2020). Privacy and security in the big data paradigm. *Journal of Computer Information Systems*, 60(2), 146–155. <https://doi.org/10.1080/08874417.2017.1418631>
- Syarifuddin, A. D. I. (2021). Pengaruh Kepercayaan Terhadap Tingkat Kepuasan Nasabah Pada Mobile Banking Di Era Pandemi Covid-19 (Studi Bank BNI Cabang Makassar). *YUME: Journal of Management*, 4(1), 2021–2208. <https://doi.org/10.37531/yume.vxiv.76>
- Szurdi, J., Christin, N., Antonakakis, M., Bauer, L., & Sekar, V. (2020). *Measuring and Analyzing Typosquatting Toward Fighting Abusive Domain Registrations Thesis Committee*. July.
- Temkar, S., & Vardhini, V. (2023). Examining the Consequences of Security Breaches on Customer Satisfaction and Loyalty in Banking: Insights from Case Studies. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 10(4), 368–377.

- Utami, M., Handayani, T., & Pusporini. (2020). Pengaruh Kualitas Layanan dan Kepercayaan Terhadap Keputusan Loyalitas Nasabah. *JEMPER (Jurnal Ekonomi Manajemen Perbankan)*, 2(2), 77. <https://doi.org/10.32897/jemper.v2i2.377>
- Wahyudi, I., Alim, M. N., Malia, E., & Dewi, I. O. (2021). Budaya organisasi dan sistem pengendalian manajemen pada perguruan tinggi. *Jabilah : Journal of Social Community*, 6(2), 126–140.
- Wahyudi, I., Haryadi, B., & Hayati, N. (2022). Uncovering the Dark Side of Ponzi Schemes Through Money Game. *Jurnal Ilmiah Akuntansi Dan Bisnis*, 17(2), 201. <https://doi.org/10.24843/jiab.2022.v17.i02.p02>
- Wahyudi, I., Muntasa, A., Yusuf, M., & Hamzah, A. (2021). Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop. *Jurnal Aplikasi Teknologi Informasi Dan Manajemen (JATIM)*, 2(2), 120–127. <https://doi.org/10.31102/jatim.v2i2.1068>
- Wibowo, S. A., Syahrin, A., Mulyadi, M., & Sunarmi. (2021). Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Skimming Di Tinjau Menurut Undang-Undang. *Jurnal Kajian Hukum*, 2(2), 138–143.
- Zulkarnain, & Sutabri, T. (2023). Analisis Kejahatan Carding Pada Bni 46. *Blantika : Multidisciplinary Journal*, 2(1), 33–43. <https://doi.org/10.57096/blantika.v2i1.10>