Keamanan siber sebagai fondasi pengembangan aplikasi keuangan *mobile*: Studi literatur mengenai *cybercrime* dan mitigasinya

Shofie Azizah[1*], Zava Nurruzzuhrotil Ula[2], Dwi Mutiara[3], Michelle Prajna Prameswari[4]

[1,2,3,4]Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri K.H. Abdurrahman Wahid Pekalongan, Indonesia

DOI: https://doi.org/10.24123/jati.v17i2.6409

Abstract

This study examines the importance of cybersecurity in mobile financial applications, particularly in the face of rising cybercrime threats. The aim of this research is to provide deeper insights into the significance of cybersecurity in mobile financial apps and to develop approaches that financial companies can adopt to protect their users' data and information. The research employs a qualitative descriptive method using a systematic literature review (SLR) approach. Meta-synthesis analysis is applied to synthesize data from 26 journal articles published between 2019 and 2024. The findings reveal that cybercrime in the financial and FinTech industries is driven by internal factors such as weak security systems, lack of system updates, limited human resource competencies, and careless user behavior. External factors include malware attacks, unclear regulations, and the use of advanced technology. To counter these, it is necessary to implement technologies such as firewalls and blockchain, strong risk management, enhanced network infrastructure, the establishment of cybersecurity teams, the development of clear regulations, and user education to raise awareness and improve cybersecurity. Therefore, the implementation of a comprehensive cybersecurity strategy is crucial in maintaining the integrity and trust of users in mobile financial applications.

Keywords: Cybercrime; Cybersecurity; FinTech; Mitigation; Mobile Banking

Abstrak

Penelitian ini mengkaji pentingnya keamanan siber dalam aplikasi keuangan mobile, khususnya dalam menghadapi ancaman cybercrime yang semakin meningkat. Tujuan dari penelitian ini adalah untuk memberikan wawasan yang lebih dalam tentang pentingnya keamanan siber dalam aplikasi keuangan mobile, serta untuk mengembangkan pendekatan yang dapat diadopsi oleh perusahaan keuangan dalam melindungi data dan informasi pengguna mereka. Metode penelitian yang digunakan adalah deskriptif kualitatif melalui pendekatan systematic literature review (SLR). Teknik analisis meta-sintesis diterapkan dalam penelitian ini guna mensintesis data penelitian yang bersumber dari 26 sumber artikel jurnal dalam kurun waktu 2019 sampai dengan 2024. Hasil penelitian menunjukkan bahwa serangan cybercrime di industri keuangan dan FinTech dipicu oleh faktor internal seperti lemahnya sistem keamanan, kurangnya pembaruan sistem, keterbatasan kompetensi SDM, dan perilaku pengguna yang ceroboh. Faktor eksternalnya mencakup serangan malware, ketidakjelasan regulasi, dan penggunaan teknologi canggih. Untuk mengatasi ini, diperlukan penerapan teknologi seperti firewall dan blockchain, manajemen risiko yang kuat, peningkatan infrastruktur jaringan, pembentukan tim keamanan siber, pengembangan regulasi yang jelas, serta edukasi pengguna untuk meningkatkan kesadaran dan keamanan siber. Sehingga penerapan strategi keamanan siber yang komprehensif sangat penting dalam menjaga integritas dan kepercayaan pengguna terhadap aplikasi keuangan mobile.

Kata kunci: Cybercrime; Cybersecurity; Mitigasi; Perbankan Seluler; Teknologi Keuangan

Riwayat artikel
Artikel masuk : 23 April 2024
Artikel direvisi : 1 September 2024
Artikel diterima : 18 September 2024

*Email korespondensi : shofie.azizah@mhs.uingusdur.ac.id

Azizah, S., Ula, Z.N., Mutiara, D., & Prameswari, M.P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan *mobile*: Studi literatur mengenai *cybercrime* dan mitigasinya. *Akuntansi dan Teknologi Informasi*, *17*(2), 221-237. https://doi.org/10.24123/jati.v17i2.6409

PENDAHULUAN

Pada era di mana teknologi informasi semakin mendominasi hampir setiap aspek kehidupan, aplikasi keuangan *mobile* telah menjadi salah satu inovasi terkemuka yang mempermudah akses dan pengelolaan keuangan bagi individu maupun bisnis. Saat ini, manusia memiliki akses yang luas dan tak terbatas terhadap teknologi informasi. Aplikasi keuangan *mobile* telah berkembang pesat dan menjadi salah satu solusi utama bagi individu maupun bisnis dalam mengakses dan mengelola keuangan secara lebih efisien. Dengan hanya menggunakan perangkat *mobile*, seseorang dapat melakukan transaksi perbankan, membayar tagihan, mengirim uang, dan mengelola investasi tanpa harus mengunjungi kantor bank atau bertatap muka dengan petugas bank.

Meskipun memberikan banyak manfaat dalam memenuhi kebutuhan informasi untuk berbagai aktivitas kehidupan, ketersediaan teknologi ini juga membawa dampak negatif (Raodia, 2019). Di era di mana akses terhadap teknologi informasi semakin luas dan tak terbatas, muncul pula risiko yang signifikan terhadap keamanan siber. Ancaman seperti serangan siber atau *cybercrime*, pencurian identitas, dan peretasan data menjadi isu yang tidak bisa diabaikan. Hal ini menimbulkan kekhawatiran yang mendalam bagi banyak organisasi, terutama dalam sektor keuangan, yang bertanggung jawab untuk melindungi data sensitif milik nasabah mereka.

Kemajuan teknologi komputasi menciptakan peluang untuk meningkatkan efisiensi, namun juga menghadirkan tantangan dalam cara menjalankan bisnis perbankan dan jasa keuangan (Kumari et al., 2017). *Financial Technology* (*Fintech*) atau teknologi untuk keuangan, menciptakan suatu model yang baru dengan lebih efisien untuk konsumen di dalam pengaksesan suatu produk serta untuk layanan dari keuangan. Menurut Professor Douglas W. Arner dalam Mawarni, 2017 dari Hongkok *University* memberikan penjelasan terkait perkembangan *financial technology* ke dalam empat masa. Empat masa tersebut yaitu *financial technology* 1.0 berlangsung dari tahun 1866-1997, *financial technology* 2.0 dari tahun 1987-2008, serta *financial technology* 3.0 dan *financial technology* 3.5 yang berlangsung dari tahun 2008 sampai dengan sekarang. *Financial technology* 3.0 merupakan masa pengunaan telepon atau *smartphone* di sektor keuangan. Sedangkan *financial technology* 3.5 merupakan masa kemunculan wujud bisnis tekologi keuangan sebagai pendatang baru yang sangat memanfaatkan peluang dari inovasi proses teknologi, produk, model bisnis serta perubahan gaya atau perilaku masyarakat dalam berinteraksi dengan layanan keuangan. (Widiyati & Erliana, 2024).

Seiring dengan pesatnya adopsi teknologi dalam sektor keuangan, seperti *internet banking*, *mobile banking*, dan layanan keuangan berbasis digital lainnya, keamanan aplikasi keuangan *mobile* menjadi semakin krusial. Keamanan dalam aplikasi keuangan *mobile* bukan hanya tentang data pribadi pengguna, tetapi juga karena aplikasi tersebut seringkali terhubung dengan informasi keuangan yang sensitif, seperti rekening bank, kartu kredit, dan transaksi finansial lainnya. Kerentanan terhadap serangan *cyber* dapat mengakibatkan kerugian finansial yang besar, kehilangan kepercayaan pengguna, serta berdampak negatif terhadap reputasi penyedia layanan keuangan (Rawindaran et al., 2023). Hadirnya *internet banking*, *mobile banking*, *financial technology*, serta transaksi lainnya yang berbasis digital menunjukkan bahwa saat ini lembaga jasa keuangan syariah sebagai penyedia jasa layanan transaksi keuangan untuk masyarakat terus melakukan inovasi berbasis digital untuk memenuhi kebutuhan masyarakat dan memenangkan persaingan global (Kurniawan & Solihin, 2022).

Salah satu bukti yang relevan dengan rentannya keamanan *cyber* pada aplikasi keuangan *mobile* yakni adanya kasus serangan *ransomware* yang menimpa Bank Syariah Indonesia (BSI) pada 8 Mei 2023. Serangan ini tidak hanya mengakibatkan gangguan layanan yang signifikan namun juga melumpuhkan operasional perbankan selama empat hari serta pencurian data pribadi dari 15 juta nasabah dan pegawai BSI. Data yang dicuri termasuk informasi sensitif seperti nama, nomor telepon, alamat, dokumen identitas, isi rekening, nomor kartu, dan detail transaksi. Kasus kejahatan *cyber* ini menunjukkan arti penting *cybersecurity* dalam menjaga kepercayaan dan keamanan nasabah di tengah kemajuan teknologi keuangan.

Cybercrime adalah bentuk kejahatan baru yang terfokus pada komputer, jaringan komputer, dan penggunaannya, serta melibatkan kejahatan tradisional yang kini dilakukan dengan menggunakan atau dibantu oleh peralatan komputer (Suhaemin & Muslih, 2023). Keamanan data dan informasi semakin penting. Keamanan siber menjadi hal utama yang tidak boleh diabaikan dalam pengembangan dan penggunaan aplikasi keuangan. *Cybersecurity* merupakan organisasi dan gugusan sumber daya, proses, dan struktur yang ditujukan agar dapat melindungi ruang maya dan sistem yang mendukung ruang maya dari insiden yang tidak selaras secara *de jure* dari hak milik *de facto*. Bidang *cybersecurity* memiliki sedikit perbedaan terutama mengenai metodologi yang dipakai, pendekatan terhadap subjek, dan area konsentrasi yang mana masih saling berhubungan dan mempunyai tujuan yang sama untuk memberikan perlindungan kerahasiaan, integritas, dan ketersediaan informasi (Sumadi et al., 2022).

Kejahatan siber lain seperti *keylogger*, *spyware*, virus, *trojan*, atau serangan *malware* lainnya juga menjadi sebuah ancaman untuk *financial technology* (*fintech*). Dalam upaya

memahami dan memecahkan masalah tersebut, penelitian ini berfokus pada penerapan *cyber security* sebagai langkah strategis dalam mengembangkan aplikasi keuangan *mobile* yang aman dan dapat diandalkan. *Cybersecurity*, yang mencakup organisasi, sumber daya, proses, dan struktur yang ditujukan untuk melindungi sistem dan informasi dari ancaman siber, menjadi kunci dalam mitigasi risiko yang muncul akibat inovasi teknologi.

Tujuan dari penelitian ini adalah untuk memberikan wawasan yang lebih dalam tentang pentingnya keamanan *cyber* dalam aplikasi keuangan *mobile*, serta untuk mengembangkan pendekatan yang dapat diadopsi oleh perusahaan keuangan dalam melindungi data dan informasi pengguna mereka. Kajian teoritik yang mendasari penelitian ini mencakup analisis risiko keamanan siber, dampak serangan *ransomware* terhadap operasional perbankan, serta strategi mitigasi risiko yang dapat diterapkan dalam konteks aplikasi keuangan *mobile*. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya meningkatkan keamanan siber pada aplikasi keuangan *mobile*, khususnya di sektor perbankan.

TELAAH TEORETIS

Cybersecurity

Cybersecurity merujuk pada berbagai alat, kebijakan, konsep keamanan, pedoman, dan teknologi yang bertujuan untuk melindungi lingkungan *cyber*, organisasi, dan aset pengguna dari serangan dan ancaman *cyber*. *Cyber-security* lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi dari adanya *cybercrime* ataupun masalah *cyber* lainnya (Ardiyanti, 2019).

Keamanan siber merupakan upaya untuk melindungi infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan informasi yang tersimpan dalam lingkungan *cyber* atau *cloud*. Tujuannya adalah untuk memastikan bahwa organisasi atau pengguna dilindungi dari serangan dan ancaman digital. Ini melibatkan perlindungan terhadap perangkat komputer, *mobile server*, dan jaringan sistem elektronik dari berbagai jenis serangan digital (Septasari, 2023).

Cybercrime

Menurut Gregory (2005), *Cybercrime* adalah bentuk kejahatan yang terjadi secara *virtual* melalui penggunaan media komputer yang terhubung ke internet, dimana komputer lain yang terhubung ke internet juga dieksploitasi. C*ybercrime* mencakup segala penggunaan jaringan komputer untuk melakukan tindakan kriminal atau kejahatan yang menggunakan teknologi digital dengan tidak benar. Oleh karena itu, secara khusus, *cybercrime* merujuk pada

kejahatan komputer yang ditargetkan terhadap sistem atau jaringan komputer. Namun, secara umum, definisi *cybercrime* mencakup segala bentuk kejahatan baru yang terfokus pada komputer, jaringan komputer, dan penggunaannya, serta melibatkan kejahatan tradisional yang kini dilakukan dengan menggunakan atau dibantu oleh peralatan komputer (Suhaemin & Muslih, 2023).

Cybercrime merupakan tindakan yang bertujuan untuk merusak jaringan sebuah organisasi dengan mencuri informasi berharga, dokumen, meretas rekening bank, dan mengalihkan dana ke rekening pihak yang melakukan kejahatan. Berbagai macam bentuk *cybercrime*, diantaranya *spoofing email*, peretasan sistem (*hacking*), penyebaran virus atau *malware*, *phishing*, kegiatan pemantauan (*stalking*), dan lainnya. Untuk memahami secara mendalam tentang fenomena kejahatan ini, dibutuhkan disiplin ilmu *cybercriminology* yang menggabungkan pengetahuan dari berbagai bidang seperti kriminologi, psikologi, sosiologi, ilmu komputer, dan *cyber security* (Riskiyadi et al., 2021).

Malware

Malware adalah perangkat lunak yang dibuat dengan maksud untuk masuk ke dalam sebuah sistem dan melakukan aktivitas yang merugikan bagi pemiliknya. Dampak negatif dari *malware* bisa bermacam-macam, mulai dari mengganggu kinerja sistem hingga merusak atau bahkan menghapus data penting yang tersimpan dalam sistem. Tujuan utama pembuatan *malware* adalah untuk merusak, mencuri, atau mengubah data milik orang lain demi keuntungan tertentu, dengan maksud untuk melakukan tindakan kriminal (Ilhamdi & Kunang, 2021).

Beberapa jenis *malware* dapat membahayakan sistem *Fintech*. Berikut ini adalah berbagai jenis serangan *malware* yang berpotensi menyerang *Fintech*. Pertama, *spyware*, adalah sebuah program yang melacak informasi penting dari sebuah sistem. Data yang dicuri dapat digunakan dengan tidak semestinya, seperti menjual alamat email kepada pengirim spam. Selanjutnya virus, adalah program menular yang terhubung ke perangkat lunak atau program lain dan kemudian mereplikasi setelah perangkat lunak tersebut mulai berjalan. Lalu *worm*, adalah perangkat lunak komputer yang menyebarkan dirinya sendiri ke seluruh sistem dan menghapus *file* dan data. *Worm* dapat menyebar ke seluruh jaringan komputer dengan memanfaatkan kelemahan dalam sistem operasi. Kemudian *Trojan*, program *trojan* ditulis untuk mendapatkan data keuangan pengguna dan mendapatkan kendali atas sumber daya sistem. Ponsel cerdas yang terhubung dapat melakukan serangan lebih lanjut terhadap router menggunakan virus *trojan* yang terinfeksi android. *Hacker*, perangkat lunak berbahaya yang

terutama berdampak pada peramban adalah pembajak atau pembajak peramban. Perangkat lunak ini mengalihkan aktivitas pencarian yang biasa dilakukan dan menampilkan hasil yang diinginkan oleh pembuatnya untuk dilihat oleh pengguna. *Ransomware*, *malware* ini mengunci data pengguna atau mengunci layar sistem sampai atau kecuali jumlah tertentu (disebut "tebusan") dibayarkan. Perangkat lunak ini melarang pengguna untuk menggunakan perangkat yang mereka rancang (Fitria, 2023).

Ransomware

Ransomware merupakan ancaman serius dalam ranah keamanan siber yang sering menimpa organisasi, dengan tujuan utama menghentikan operasi server atau mengunci data dan *file* hingga tebusan dibayarkan. Dalam hal ini, *malware* tersebut mengunci sistem operasi dan *file* pengguna, dan meminta pembayaran sebelum melepaskan kendali. Melalui pembatasan hak akses dan *enkripsi file*, *ransomware* memaksa pengguna untuk membayar tebusan agar data mereka dilepaskan (Fitria, 2023)

Ransomware sering kali memasuki sistem melalui tautan atau lampiran yang mencurigakan dalam surel, situs web yang terinfeksi, atau dengan memanfaatkan celah keamanan dalam perangkat lunak atau sistem operasi. Ancaman ini dianggap signifikan karena bisa menimbulkan kerugian finansial besar dan mengganggu jalannya bisnis atau aktivitas individu. Secara umum, cara kerja *ransomware* melibatkan beberapa tahapan. Pertama, *ransomware* akan masuk ke dalam sistem target melalui berbagai cara seperti *e-mail* dengan lampiran atau tautan yang mencurigakan, situs web yang terinfeksi, atau menggunakan kerentanan dalam perangkat lunak atau sistem operasi. Setelah berhasil masuk, *ransomware* akan mulai mengenkripsi data dengan menggunakan algoritma enkripsi yang kuat, membuat data tersebut tidak bisa diakses oleh pemiliknya. Selanjutnya, *ransomware* akan menampilkan pesan tebusan kepada korban yang berisi instruksi untuk membayar sejumlah uang tebusan, biasanya dalam bentuk mata uang *crypto* seperti *bitcoin*, sebagai syarat untuk mendapatkan kunci dekripsi yang diperlukan untuk mengembalikan akses ke data tersebut (Hartono, 2023).

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif melalui pendekatan *systematic literature review (SLR)*, yakni metode penelitian yang dilakukan secara sistematis untuk mengidentifikasi literatur dari berbagai jurnal penelitian terindeks yang dilaksanakan melalui tiga tahapan utama yaitu perencanaan, pelaksanaan, dan pelaporan tinjauan literatur (Suwarno et al., 2022). Metode ini mengedepankan pernyataan

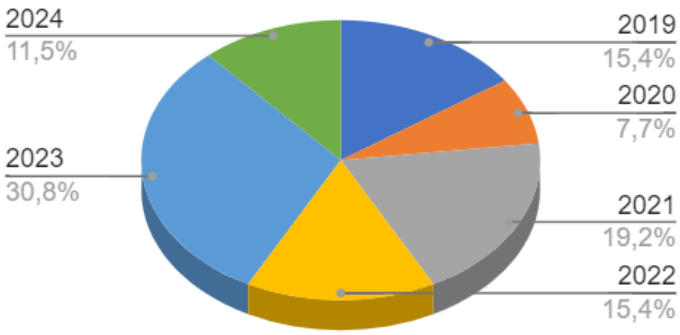
yang jelas mengenai tujuan, bahan, dan metode penelitian, serta memberikan kesimpulan berdasarkan pengembangan metodologi yang tepat. *Systematic literature review* dilakukan terhadap 26 sumber artikel jurnal tentang *cybersecurity* yang terbit dalam kurun tahun 2019 sampai dengan 2024 yang terdiri dari 15 jurnal internasional, 9 jurnal nasional serta 2 thesis. Kualifikasi jurnal yang digunakan yaitu jurnal-jurnal yang relevan mengenai ancaman *cybercrime* serta tindakan antisipatif keamanan siber (*cyber security*).

Teknik analisis meta-sintesis diterapkan dalam penelitian ini guna mensintesis atau merangkum temuan-temuan penelitian yang bersifat deskriptif kualitatif. Tujuan dari meta-sintesis adalah untuk menyimpulkan informasi dari berbagai temuan dengan analisis yang lebih tajam dan tepat (Kitchenham & Brereton, 2013). Langkah awal dalam meta-sintesis adalah merumuskan pertanyaan penelitian, kemudian mencari jurnal yang relevan. Jurnal-jurnal yang telah dikumpulkan kemudian diseleksi yang relevan dengan topik penelitian. Selanjutnya, data yang diperoleh dari jurnal-jurnal tersebut dianalisis dan dilakukan kontrol kualitas terhadap hasil temuan. Meta-sintesis diakhiri dengan menyusun laporan akhir.

HASIL DAN PEMBAHASAN

Hasil Pengelompokan Jurnal berdasarkan Tahun Terbit

Berikut hasil pemetaan berdasarkan tahun penerbitan jurnal yang membehas mengenai isu *cybercrime* dan *cybercrime*, yang ditunjukkan pada gambar dibawah. Dapat dilihat bahwa jumlah artikel yang membahas topik ini mencapai puncaknya pada tahun 2023 dengan total delapan artikel. Sebaliknya, pada tahun-tahun lainnya, jumlah artikel yang diterbitkan rata-rata berkisar antara dua hingga lima artikel per tahun. Hal ini menunjukkan peningkatan minat penelitian pada tahun 2023, yang kemungkinan disebabkan oleh perkembangan *fintech* yang sangat pesat pada tahun 2019, sebagaimana yang diberitakan oleh OJK.go.id. Minat penelitian masyarakat terhadap *cybersecurity* mengalami puncak kenaikan pada tahun 2023. Dalam kurun waktu 2019-2023, masyarakat masih melakukan penyesuaian dan pemahaman dalam memanfaatkan perkembangan *fintech*. Ternyata, perkembangan *fintech* ini memiliki pola yang kompleks serta mengandung berbagai ancaman. Oleh karena itu, pada tahun 2023 banyak peneliti tertarik untuk mendalami isu-isu terkait *cybercrime* dan *cybersecurity*, guna menjawab tantangan yang muncul dari kemajuan teknologi keuangan tersebut.

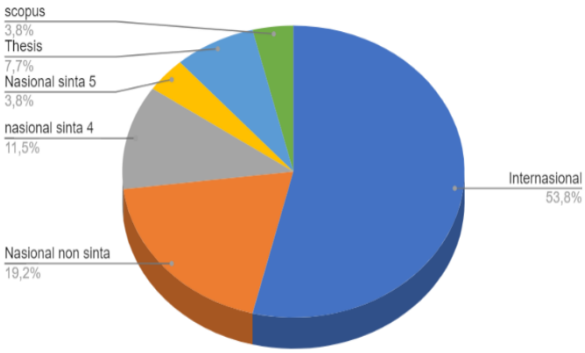


Gambar 1. Hasil Pengelompokan Jurnal Berdasarkan Tahun Terbit

Hasil Pengelompokan Jurnal berdasarkan Jenis Jurnal

Hasil mapping berdasarkan *Publisher Accreditation Level* yang membahas topik *cybercrime* dan *cyber security* dapat dilihat pada diagram dibawah. Ilmuwan Indonesia saat ini sedang giat berusaha mendongkrak hasil penelitian dalam bentuk artikel ilmiah untuk dipublikasikan baik secara nasional dan internasional. Artikel ilmiah yang dapat diakses oleh pengguna internet sangat penting, karena tingkat keamanan siber dan kesadaran akan kejahatan siber mampu dipengaruhi oleh kualitas publikasi.

Untuk saat ini, level akreditasi jurnal di Indonesia dibedakan menjadi Sinta 1, 2, 3, 4, 5, dan 6. Berdasarkan hasil *mapping*, jumlah artikel yang membahas *cybercrime* dan *cybersecurity* paling banyak dipublikasikan di jurnal internasional sebesar 53,8%, diikuti dengan jurnal nasional non-akreditasi sebesar 19,2%, dan jurnal sinta 4 sebesar 11,5%. Adapun publikasi di jurnal Sinta 5 sebesar 3,8%, sedangkan thesis sebesar 7,7% dan jurnal internasional terindeks scopus 3,8%. Penjelasan mengenai persentase ini menggambarkan bahwa perhatian dan penelitian di bidang keamanan siber dan kejahatan siber semakin meningkat, dengan dukungan kuat dari pemerintah untuk publikasi di tingkat global.



Gambar 2. Hasil Pengelompokan Jurnal Berdasarkan Jenis Jurnal

Hasil Pengelompokan Jurnal Berdasarkan Isu Penelitian

Berdasarkan hasil pengelompokan dari 26 jurnal dalam kurun waktu penelitian lima tahun (2019-2024), peneliti mengangkat dua isu untuk dibahas dalam penelitian ini. Terdapat beberapa jurnal yang mengangkat lebih dari satu isu yang telah ditentukan oleh peneliti. Hal tersebut dijabarkan pada tabel di bawah ini. Sehingga total terdapat 33 jurnal berdasarkan isu penelitian, sedangkan jumlah jurnal yang di*mapping* adalah 26. Isu-isu yang diangkat dalam artikel adalah:

Tabel 1. Hasil Pengelompokan Jurnal Berdasarkan Isu Penelitian

No	*Isu Research*	Jumlah
1	Faktor Penyebab *Cybercrime*	19
2	*Cyber security* untuk Memitigasi Risiko *Cybercrime*	14
	Total	33

Faktor Internal Penyebab Serangan Cybercrime

Pertama, lemahnya sistem keamanan**.** Masih lemahnya sistem keamanan pada lembaga keuangan, meskipun telah diterapkan tindakan keamanan, tetap rentan terhadap serangan *ransomware* (Assifa, 2023). Serangan *ransomware* merusak sistem IT, mengenkripsi data sensitif, dan mengganggu layanan perbankan secara keseluruhan. Tindakan keamanan yang lebih kuat memerlukan biaya besar yang mungkin belum dapat dipenuhi oleh lembaga keuangan (Kunnas, 2022).

Kedua, kurangnya penerapan keamanan dan pembaruan sistem**.** Kurangnya penerapan tindakan keamanan yang memadai, serta kurangnya pembaruan sistem dan perangkat lunak yang rentan terhadap serangan. Kekurangan dalam penanganan keamanan internal membuat *Mobile Banking* rentan terhadap serangan siber, yang dapat mengancam operasional dan reputasi perusahaan (Kunnas, 2022).

Ketiga, keterbatasan kompetensi SDM dan kebijakan**.** Pesatnya perkembangan teknologi dan inovasi di *Fintech*, staf dan sistem yang terlibat dalam pengendalian internal tradisional atau audit internal mungkin tidak dilengkapi dengan keterampilan yang memadai atau mereka kurang berkompeten untuk mencegah dan mendeteksi penipuan di *Fintech* (Una & Prabowo, 2022). Tingkat pergantian staf yang tinggi dan kurangnya pemahaman manajemen terhadap teknologi informasi membuat *Fintech* lebih rentan terhadap penipuan (Ng & Kwok, 2019). Keempat, perilaku pengguna. Perilaku pengguna yang kurang waspada, seperti mengklik tautan mencurigakan dalam *e-mail phishing* dan menggunakan kata sandi yang lemah, meningkatkan risiko terkena *cybercrime* (Fitria, 2023; Ouytsel, 2021). Pembagian kata

sandi terjadi ketika kepercayaan antara dua individu, yang dapat meningkatkan risiko terkena serangan (Ouytsel, 2021).

Kelima, kurangnya kebijakan dan prosedur internal. Lembaga keuangan atau *Fintech* yang sedang berkembang mungkin tidak memiliki kebijakan dan prosedur yang diperlukan untuk mencegah dan menghalangi penipuan. Karyawan senior yang menyalah gunakan wewenang dapat terlibat dalam pencurian, sabotase, atau pengungkapan yang tidak disengaja (Rawindaran et al., 2023). Keenam, kerja sama dengan pihak ketiga. Kerja sama dengan pihak ketiga, pelibatan pihak ketiga, seperti penyedia layanan teknologi keuangan, dapat membuka celah baru untuk serangan *cyber*. Saat Lembaga keuangan bermitra dengan penyedia layanan pihak ketiga, khususnya dalam sektor teknologi keuangan, risiko tambahan bisa timbul. Mitra pihak ketiga tersebut mungkin memiliki standar keamanan yang berbeda atau kurang ketat dibandingkan dengan organisasi utama, sehingga membuka peluang bagi peretas untuk mengeksploitasi celah keamanan yang ada (Yohanes & Perajaka, 2021). Terakhir, kurangnya evaluasi dan komunikasi. Kurangnya sistem penilaian untuk memahami reaksi nasabah terhadap kebijakan dan tindakan penanggulangan, serta komunikasi yang kurang dengan nasabah, menyulitkan evaluasi efektivitas strategi dan mengurangi kepercayaan nasabah (Maulana & Nasrulloh, 2024).

Faktor Eksternal Penyebab Serangan Cybercrime

Pertama, Serangan *Malware*. *Malware* dirancang khusus untuk menyasar aplikasi *mobile banking* dan dapat mencuri informasi pribadi pengguna, seperti kata sandi dan detail akun, serta melakukan transaksi ilegal tanpa sepengetahuan pengguna (Fitria, 2023). Contoh *malware* adalah virus *ransomware*, yang mengunci sistem komputer atau mengenkripsi data, memaksa perusahaan untuk mempertimbangkan pembayaran uang tebusan untuk mengakses kembali data yang terkunci seperti yang terjadi pada kasus Bank BSI tanggal 8 Mei tahun 2023. *Ransomware* menimbulkan masalah utama yang mengancam keberlanjutan operasional, risiko pengungkapan data yang dapat merusak kepercayaan nasabah, dan kompleksitas keamanan dalam produk dan layanan syariah (Restika & Sonita, 2023). *Malware* lintas *platform* menambah tantangan dengan infeksi yang bisa menyebar antar perangkat dan sistem operasi, menciptakan lingkungan yang berisiko bagi pengguna *mobile banking*. Penggunaan URL palsu dalam SMS atau panggilan VOIP untuk mengarahkan korban ke situs web palsu atau layanan suara palsu menjadi ancaman signifikan. Teknik ini digunakan untuk mengelabui pengguna agar memberikan informasi login atau data pribadi mereka, yang kemudian digunakan untuk mengakses akun keuangan (Islam, 2019).

Kedua, ketidakjelasan regulasi dan kepatuhan. *Cybercrime* dalam industrif *Fintech* disebabkan oleh tekanan untuk memenuhi target keuangan yang memicu perilaku curang, serta penggunaan model bisnis baru yang menciptakan kerentanan dalam proses dan kontrol internal yang dapat dieksploitasi (Ng & Kwok, 2019). Ketidak jelasan mengenai peraturan yang berlaku membuka peluang serangan *cybercrime*, dan regulasi perlindungan data dan informasi *fintech* merupakan tantangan global yang memerlukan regulasi internasional (Laidlaw, 2021). Transaksi digital yang sering kali tidak meninggalkan jejak audit yang terlihat membuat deteksi dan pencegahan penipuan lebih sulit (Ng & Kwok, 2019).

Ketiga, penggunaan teknologi canggih. Penerapan teknologi canggih seperti kecerdasan buatan dan analisis *big data* dalam perbankan syariah membawa tantangan dan peluang dalam keamanan *cyber* (S. Wang et al., 2024). Kesulitan memproses volume data besar dapat menyebabkan serangan *phishing* yang merusak reputasi bank dan menyebabkan kehilangan dana nasabah (Restika & Sonita, 2023). Ancaman *malware* dan *ransomware* dapat mengakibatkan kebocoran data, pencurian informasi keuangan, atau penguncian sistem yang mengganggu operasional bank (Y. Wang, 2023; Yang, 2020). Berkembangnya teknologi inovatif juga membawa peningkatan pencurian hak kekayaan intelektual seperti hak paten, hak cipta, dan rahasia dagang yang berawal dari serangan *cybercrime* pada *fintech* (Al-Harrasi et al., 2021).

Keempat, akses internet dan penggunaan aplikasi pihak ketiga. Penggunaan aplikasi pihak ketiga yang tidak terpercaya dapat membuka celah bagi penjahat *cyber* untuk menyusupkan kode berbahaya. Ketergantungan pada jaringan *Wi-Fi* publik yang tidak aman dapat memudahkan serangan *man-in-the-middle* (Fitria, 2023). Akses internet yang tidak terbatas memungkinkan kejahatan siber berkembang pesat dengan potensi keuntungan besar dan risiko tertangkap yang lebih rendah (Raodia, 2019).

Kelima, tantangan transportasi dan jaringan. Sistem transportasi seluler dan jaringan seperti HTTP, WAP, GSM, dan CDMA memiliki kelemahan yang dapat dieksploitasi oleh penyerang, termasuk *intercept data, bluejacking, bluesnarfing*, serta penyadapan dan peretasan jaringan yang membahayakan komunikasi dan data pribadi pengguna (Islam, 2019).

Cyber security untuk Memitigasi Risiko Cybercrime

Perlindungan dari ancaman internal dan eksternal yang telah dijabarkan bergantung pada faktor internal yang baik. Oleh karena itu, penelitian ini memberikan solusi yang dapat dilakukan oleh suatu entitas yang menjalankan *fintech* untuk meningkatkan *cybersecurity* yang

dimilikinya. Berikut ini merupakan beberapa hal yang dapat dilakukan untuk meningkatkan *cybersecurity* dari ancaman internal maupun eksternal:

Pertama, penerapan *firewall*. Pemanfaatan teknologi digital berbasis internet membuka celah bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan pembobolan yang sangat merugikan. Perusahaan harus mampu memanfaatkan teknologi yang semakin canggih sebagai upaya untuk mencegah maupun menyelesaikan permasalahan *cybercrime*. Salah satu upaya yang dapat dilakukan adalah penggunaan *firewall*. *Firewall* merupakan salah satu elemen kunci dalam pertahanan siber yang berperan dalam menjaga sistem dan data dari serangan yang timbul dari internet. Keamanan *firewall* berupa tembok penghalang untuk menghalau pengguna ilegal yang berusaha menerobos server, di mana pengguna dari luar tidak akan dapat menembus ke dalam server jika tidak memiliki izin akses.

Penggunaan *firewall* untuk meningkatkan keamanan *cyber* sangatlah penting bagi perusahaan atau institusi keuangan mana pun. Prosedur yang dapat dilakukan untuk peningkatan *cybersecurity* yaitu dengan identifikasi kebutuhan yang relevan, pemilihan jenis *firewall* yang tepat, pemisahan kelompok jaringan untuk mencegah penyebaran *malware*, konfigurasi *firewall* secara ketat, *controlling* dan pelaporan, *update* secara berkala, pengujian keamanan, pelatihan karyawan, serta kerja sama dengan penyedia keamanan untuk terus *update* informasi terbaru (Meidiandra et al., 2023).

Kedua, *blockchain*. Pada sektor keuangan, peningkatan *cyber security* juga dapat dilakukan dengan penerapan teknologi *blockchain*. *Blockchain* adalah buku besar terdistribusi di mana salinan buku besar disimpan di setiap komputer yang terhubung. Jaringan ini disebut *Blockchain* karena terdiri dari blok-blok yang saling berhubungan yang melayani catatan transaksi (Javaid et al., 2022). Teknologi *blockchain* menyediakan infrastruktur yang aman, transparan, dan sulit dimanipulasi. Dalam jaringan yang terdistribusi dan terdesentralisasi, banyak komputer digunakan untuk mencatat transaksi dalam buku besar yang tersebar luas. Dengan struktur dan sifatnya, *blockchain* menjamin keamanan dan keakuratan transaksi, serta menghambat upaya perubahan, penghapusan, atau penambahan data yang belum diverifikasi karena setiap anggota jaringan memiliki salinan sendiri.

Teknologi *blockchain* telah menunjukkan bahwa *fintech* dapat dilakukan secara digital dengan cepat, mudah, dan aman dibandingkan dengan metode konvensional (Mohamed, 2023). Hal tersebut dapat dilakukan dengan memperhatikan tiga komponen utama *cybersecurity* yaitu kerahasiaan, integritas, dan ketersediaan (Demirkan et al., 2020). Selain itu, seluruh sistem dan *software* baru yang dirancang dengan mempertimbangkan teknologi *blockchain* perlu diuji

berdasarkan tiga aspek penting, yaitu verifikasi identitas, pengesahan akses, dan pencatatan transaksi secara ketat.

Ketiga, manajemen risiko, pemanfaatan teknologi digital untuk meningkatkan pelayanan kepada anggota dan untuk mencapai efektivitas serta efisiensi dalam bisnis perlu didampingi oleh manajemen risiko yang kuat guna memitigasi ancaman *cybersecuriity*. Manajemen risiko dilakukan dengan pengawasan dan pengendalian oleh pimpinan, kebijakan dan prosedur SOP yang jelas, menjalankan sistem pengendalian internal, serta membangun sistem keamanan berlapis (Kurniawan & Solihin, 2022). Perlindungan data juga dapat dilakukan dengan membangun penyimpanan server mandiri yang berlapis. Jika data dicadangkan pada banyak *database*, maka akan meminimalisir kehilangan data jika terjadi kejahatan. Sehingga apabila salah satu *database* terkena serangan, maka masih ada cadangan pada *database* yang lain.

Autentikasi tiga faktor (3FA) juga dapat dterapkan dalam *fintech* sebagai langkah keamanan yang memperkuat perlindungan akses akun pengguna dengan menggabungkan tiga elemen verifikasi berbeda (Fitria, 2023). Pertama, ada faktor pengetahuan, yaitu sesuatu yang diketahui oleh pengguna seperti kata sandi atau PIN. Ini adalah bentuk autentikasi dasar yang paling umum. Berikutnya adalah faktor kepemilikan, yang melibatkan sesuatu yang dimiliki oleh pengguna seperti perangkat seluler, token keamanan, atau kartu pintar. Terakhir yaitu faktor inheren, yaitu karakteristik unik dari pengguna seperti biometrik, yang dapat berupa sidik jari, pengenalan wajah, atau pemindaian iris untuk menyelesaikan autentikasi. Hal ini secara signifikan meningkatkan keamanan dan mengurangi risiko terhadap serangan siber. Keempat, perbaikan infrastruktur jaringan dan karyawan. Infrastruktur jaringan maupun karyawan yang menjalankannya memiliki peran penting dalam *cybersecurity*. Karyawan berperan dalam pembuatan, pengoperasian, maupun pengontrolan aplikasi *fintech*. Oleh karena itu, perkembangan teknologi harus diiringi dengan sumber daya yang dapat mengimbanginya. Peningkatan keahlian karyawan dengan memberikan pelatihan untuk meningkatkan *skill* karyawannya yang sesuai dengan tugasnya juga dibutuhkan untuk meningkatkan keamanan siber (Rawindaran et al., 2023).

Berdasarkan hasil uji pada Widiyati & Erliana (2024) dijelaskan bahwa perlindungan data dam *cybersecurity* memiliki pengaruh positif terhadap penggunaan *fintech*, sehingga diperlukan peningkatan keamanan data pengguna. Pembaruan infrastruktur jaringan untuk meningkatkan keamanan data dapat dilakukan dengan menggantikan *open gateway* dengan gateway tunggal yang memungkinkan pengawasan lebih efisien dan terpusat terhadap lalu

lintas data (Maulana & Nasrulloh, 2024). Pendekatan ini meningkatkan kemampuan untuk mendeteksi dan merespons ancaman keamanan secara lebih cepat.

Kelima, membuat tim keamanan *cyber* serta regulasi yang jelas. Tim keamanan *cyber* menjadi salah satu elemen kunci dalam menjaga integritas dan keamanan infrastruktur digital suatu organisasi. Tugas utama dari tim ini adalah memantau dan mengelola infrastruktur keamanan, serta bertanggung jawab atas pengawasan terhadap serangan siber potensial serta merespons secara cepat dan efektif terhadap insiden keamanan yang terjadi (Meidiandra et al., 2023).

Selain itu, tim keamanan juga bertanggung jawab untuk mengembangkan kebijakan keamanan yang relevan dan diperlukan, baik itu dalam hal teknologi, prosedur, atau kepatuhan terhadap regulasi guna memastikan perlindungan yang optimal terhadap aset dan data organisasi dari ancaman siber yang terus berkembang. Regulasi menyediakan kepastian hukum terhadap tindakan kejahatan siber yang dapat membahayakan sektor *fintech*, sehingga pelaku usaha, pelanggan, dan regulator memiliki pedoman yang jelas mengenai langkah-langkah yang harus diambil dan tindakan yang sesuai dengan peraturan yang berlaku (Riskiyadi et al., 2021).

Keenam, edukasi pengguna. Manusia dalam hal ini adalah pengguna juga berpengaruh dalam menentukan keamanan penggunan *fintech*. Upaya peningkatan keamanan siber dapat dilakukan dengan meningkatkan kesadaran pengguna internet, karena pengguna memegang peranan penting dalam kesadaran keamanan siber, yang sering kali menjadi pertahanan awal terhadap ancaman terhadap aset informasi. Penting untuk memiliki anggota yang cerdas dalam mengamankan akun mereka, termasuk *user*, *password*, nomor OTP, dan identitas lainnya guna menghindari kerugian akibat kelalaian dalam penggunaan sistem (Kurniawan & Solihin, 2022).

Menurut Abdulrahaman et al. (2019) ancaman yang berasal dari sisi pengguna dapat ditangani melalui peningkatan kesadaran dan penerapan kebijakan serta prosedur keamanan yang memastikan pelanggan senantiasa mematuhi pedoman keamanan minimum, seperti pemasangan perangkat lunak antivirus dan deteksi *malware* pada perangkat mereka; keterampilan dalam pengelolaan kata sandi; serta selalu meng*instal*, memperbarui, dan meningkatkan aplikasi *fintech* asli yang terbaru. Selain itu, diperlukan pula peningkatan kesadaran (*awareness*) pengguna untuk berhati-hati dalam mengklik, men*download*, maupun membuka *file* yang diterima dalam lampiran *e-mail* karena dapat mengandung *malware* (Fitria, 2023).

SIMPULAN

Serangan *cybercrime* di industri keuangan dan *fintech* dipicu oleh faktor internal seperti lemahnya sistem keamanan, kurangnya pembaruan sistem, keterbatasan kompetensi SDM, dan perilaku pengguna yang ceroboh. Faktor eksternalnya mencakup serangan *malware*, ketidakjelasan regulasi, dan penggunaan teknologi canggih. Untuk mengatasi ini, diperlukan penerapan teknologi seperti *firewall* dan *blockchain*, manajemen risiko yang kuat, peningkatan infrastruktur jaringan, pembentukan tim keamanan siber, pengembangan regulasi yang jelas, serta edukasi pengguna untuk meningkatkan kesadaran dan keamanan siber. Penelitian ini mencakup fokus yang terbatas pada data sekunder dari literatur yang ada dan tidak adanya data primer seperti wawancara atau laporan investigasi sehingga belum mencakup semua aspek penting terkait keamanan siber dalam aplikasi keuangan mobile. Penelitian selanjutnya diharapkan mampu menggunakan sumber data tambahan, seperti wawancara dengan saksi kunci dan berfokus pada evaluasi efektivitas strategi keamanan siber di sektor teknologi keuangan.

DAFTAR PUSTAKA

Abdulrahaman, M. D., Alhassan, J. K., Ojeniyi, J. A., & Abdulhamid, S. M. (2019). Security Risk Analysis and Management in mobile wallet transaction: A Case study of Pagatech Nigeria Limited. *International Journal of Computer Network and Information Security*, *10*(12), 21–33. https://doi.org/10.5815/ijcnis.2018.12.03

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875–888.

Ardiyanti, H. (2019). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica*, *5*(1), 95–110.

Assifa, B. A. (2023). *Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia dari serangan Cybercrime*. Universitas Islam Negeri Syarif Hidayatullah Jakarta.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. *Jurnal Informatika Dan Teknik Elektro Terapan*, *11*(3). https://doi.org/10.23960/jitet.v11i3.3312

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Ilhamdi, Y., & Kunang, Y. N. (2021). Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik. *Bina Darma Conference on Computer Science*, *3*, 256–264.

Islam, M. S. (2019). Systematic Literature Review: Security Challenges of Mobile Banking and Payments System. *International Journal of U- and e-Service, Science and Technology*, *7*(6), 107–116. https://doi.org/10.14257/ijunesst.2014.7.6.10

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. In *Information and Software Technology* (Vol. 55, Issue 12).

https://doi.org/10.1016/j.infsof.2013.07.010
Kumari, R., Jasojit, T., Kumari, R., Jasojit, T., Keuangan, K., & Penulis, U. (2017). *Jurnal Regulasi dan Kepatuhan Keuangan*.
Kunnas, J. (2022). *EMPLOYEE ATTITUDES TOWARDS INFORMATION Identifying archetypes using machine learning Bachelor ' s Thesis Juho Kunnas Aalto University School of Business Information and Service Management*. Aalto University School of Business Information and Service Management.
Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, *1*(1), 1–20. https://doi.org/10.35878/jiose.v1i1.360
Laidlaw. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. *SSRN Electronic*, *10*(1), 1–81.
Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. *Ekonomi Syariah Dan Bisnis Perbankan*, *8*(1), 76–91.
Meidiandra, M. K., Sari, Y. P., & Sutabri, T. (2023). Mendesain Cyber Security Core Banking System untuk Keamanan Menggunakan Firewall Pada PT. Bank Syariah Indonesia Tbk. *Syntax Idea*, *5*(7), 843–848.
Mohamed, A. O. Y. (2023). Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System. *International Journal of Interactive Mobile Technologies*, *17*(4), 37–46. https://doi.org/10.3991/ijim.v17i04.37671
Ng, A., & Kwok, B. K. B. (2019). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance*, *25*(4), 422–434. https://doi.org/10.1108/jfrc-01-2017-0013
Ouytsel, J. Van. (2021). The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships – A mixed-methods study. *Telematics and Informatics*, *63*(101668).
Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2), 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399
Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191
Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929
Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen Dan Organisasi*, *12*(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528
Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)*, *5*(2), 227–233. https://doi.org/10.30604/jti.v5i2.231
Suhaemin, A., & Muslih. (2023). Karakteristik Cybercrime di Indonesia. *EduLaw : Journal of Islamic Law and Yurisprudance*, *5*(2), 15–26.
Sumadi, M. I. T. B. N., Putra, R., & Firmansyah, A. (2022). Peran Perkembangan Teknologi Pada Profesi Akuntan Dalam Menghadapi Industri 4.0 Dan Society 5.0. *Journal of Law, Administration, and Social Science*, *2*(1), 56–68. https://doi.org/10.54957/jolas.v2i1.162
Suwarno, R., Cahyono, D., & Maharani, A. (2022). Systematic Literature Review: Faktor Keunggulan Bank Syariah Di Indonesia. *Jurnal Peneliti Ekonomi*, *1*(6), 40–54.
Una, B. K., & Prabowo, H. Y. (2022). Fintech lending fraud prevention strategy: A case study. *Journal of Contemporary Accounting*, *4*(1), 37–52.
Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Journal Computers & Security*, *147*(104051).
Wang, Y. (2023). Application of Big Data Technology in Mobile Payment Security. *Journal of*

Research in Social Science and Humanities, *2*(12), 18–23. https://doi.org/10.56397/jrssh.2023.12.04

Widiyati, D., & Erliana. (2024). Pengaruh Literasi Keuangan, Perlindungan Data, dan Cybersecurity terhadap Penggunaan Financial Technology. *JURNAL AKUNTANSI DAN EKONOMI AKREDITASI NOMOR*, *9*(1), 130–141. https://doi.org/10.29407/jae.v9i1.21945

Yang, T. (2020). Mobile Payment Security in the Context of Big Data: Certificateless Public Key Cryptography. *International Journal of Network Security*, *22*(4), 621–626.

Yohanes, N., & Perajaka, M. A. (2021). Penerapan Model Manajemen Risiko Teknologi Digital di Lembaga Perbankan Berkaca pada Cetak Biru Transformasi Digital Perbankan Indonesia. *Jurnal Manajemen Risiko*, *2*(2), 59–74.