Statistik Kejahatan Siber di Indonesia Tahun 2024: Tren, Tantangan, dan Upaya Pencegahan di Era Digital

Cybercrime Statistics in Indonesia 2024: Trends, Challenges, and Preventive Measures in the Digital Era

Robby Rohman Sukarya [1], Novita Anggraini, [2] ,Hegar Krisna Cambara[3], Ismaya Dewi Priyani [4], Alwi Al Hadad[5]

[1,2]Hukum, [3]DKV, [4,5]Informatika, Universitas Teknologi Digital, Bandung, Indonesia,
Email correspondensi: ismayapriyani@digitechuniversity.ac.id

Info Artikel

Riwayat Artikel:
Diajukan: 11/05/2025
Diterima: 23/05/2025
Diterbitkan: 27/08/2025

Kata Kunci:
Kejahatan siber, Penipuan online, Keamanan siber, Informasi, Statistik

Keyword:
Cybercrime, Online fraud, Cybersecurity, Information, Statistics

https://doi.org/

A B S T R A K

Artikel ini membahas fenomena kejahatan siber di Indonesia dengan menekankan tren statistik pada periode 2024. Penelitian ini menggunakan metode statistik deskriptif dengan pendekatan yuridis-empiris, di mana data diperoleh dari laporan resmi Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). Analisis dilakukan dengan menghitung jumlah kasus, tren kenaikan atau penurunan, serta distribusi jenis kejahatan digital yang kemudian dipresentasikan melalui tabel dan grafik. Hasil penelitian menunjukkan peningkatan signifikan pada penipuan online, phishing, dan ransomware. Aduan penipuan online mencapai lebih dari 572.000 kasus sejak 2017, sementara pada 2024 tercatat 26,7 juta aktivitas phishing dan 514 ribu serangan ransomware. Tingkat kekhawatiran publik terhadap penipuan online juga melonjak dari 10,3% (2023) menjadi 32,5% (2024). Temuan ini menegaskan bahwa ruang digital kini menjadi arena kriminalitas baru yang lebih kompleks dibanding kejahatan konvensional. Upaya pencegahan perlu diarahkan pada peningkatan literasi digital, penguatan keamanan siber, serta kolaborasi antara pemerintah, aparat hukum, penyedia layanan digital, dan masyarakat.

A B S T R A C T

This article examines the phenomenon of cybercrime in Indonesia, focusing on statistical trends during the 2024 period. The study employs a descriptive statistical method with a juridical-empirical approach, using data obtained from official reports by the Ministry of Communication and Information Technology (Kominfo), the National Cyber and Crypto Agency (BSSN), and the Indonesian Internet Service Providers Association (APJII). The analysis involves calculating the number of cases, trends of increase or decrease, and the distribution of types of digital crimes, which are then presented through tables and graphs. The results indicate a significant increase in online fraud, phishing, and ransomware attacks. Complaints regarding online fraud have exceeded 572,000 cases since 2017, while in 2024, there were 26.7 million phishing activities and 514,000 ransomware attacks. Public concern over online fraud also rose sharply from 10.3% in 2023 to 32.5% in 2024. These findings highlight that the digital space has become a new, more complex arena for criminal activity compared to conventional crimes. Preventive efforts should focus on enhancing digital literacy, strengthening cybersecurity, and fostering collaboration among the government, law enforcement, digital service providers, and the public.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah banyak aspek kehidupan manusia, termasuk cara interaksi, transaksi ekonomi, hingga sistem pemerintahan. Di satu sisi, kemajuan ini membawa kemudahan dan efisiensi, namun di sisi lain menciptakan celah bagi tindakan kriminal baru yang dikenal sebagai kejahatan siber (cybercrime). Kejahatan siber tidak hanya menimbulkan kerugian finansial bagi individu dan perusahaan, tetapi juga mengancam keamanan data, reputasi, dan stabilitas sosial. Fenomena ini menjadi semakin relevan di Indonesia mengingat penetrasi internet yang tinggi dan peningkatan penggunaan layanan digital di berbagai sektor. Dalam perspektif kriminologi, kejahatan siber dapat dianalisis menggunakan beberapa teori klasik dan modern. Teori Strain (Robert Merton) menekankan bahwa ketidaksesuaian antara tujuan sosial dan sarana yang tersedia dapat mendorong individu melakukan kejahatan, termasuk di dunia digital. Selain itu, teori Opportunity (Clarke & Cornish) menjelaskan bahwa kemudahan akses dan kelemahan sistem keamanan digital menciptakan peluang bagi pelaku untuk melakukan tindakan kriminal. Teori-teori ini membantu memahami motif dan kondisi yang memfasilitasi munculnya kejahatan siber di masyarakat modern. Penelitian ini didasarkan pada hubungan antara tren statistik kejahatan siber, faktor-faktor yang memengaruhi terjadinya cybercrime, dan upaya pencegahan yang dapat dilakukan. Dengan menganalisis data resmi dari Kominfo, BSSN, dan APJII, penelitian ini mencoba memetakan jenis kejahatan siber yang paling sering terjadi, pertumbuhan kasus dari tahun ke tahun, serta persepsi masyarakat terhadap risiko keamanan digital. Analisis ini diharapkan memberikan gambaran empiris untuk merumuskan strategi pencegahan yang efektif. Penelitian ini bertujuan untuk menyoroti peningkatan signifikan kejahatan siber di Indonesia pada periode 2023–2024, serta memberikan rekomendasi berbasis data untuk penguatan literasi digital, keamanan siber, dan kolaborasi antar pemangku kepentingan. Dengan memahami tren dan pola kejahatan siber, pemerintah, aparat hukum, penyedia layanan digital, dan masyarakat dapat bersama-sama membangun ekosistem digital yang lebih aman dan terpercaya. Temuan ini juga menekankan pentingnya pendekatan yuridis-empiris dalam memformulasikan kebijakan pencegahan cybercrime secara terukur dan berkelanjutan. Selain itu pentingnya privasi menyadarkan kita perlunya menyoroti pentingnya pemahaman yang lebih mendalam tentang harapan dan kebutuhan pengguna dalam pengelolaan privasi di media sosial serta kebutuhan akan langkah-langkah lebih lanjut untuk meningkatkan kesadaran, keamanan, dan perlindungan privasi bagi pengguna di platform-platform media sosial tersebut [1].

2. METODE PELAKSANAAN

Penelitian ini menggunakan metode statistik deskriptif yang merupakan deskripsi yang berkenaan dengan deskripsi data [2], dengan pendekatan yuridis-empiris. Metode ini dipilih untuk menganalisis secara sistematis jumlah kasus, tren kenaikan atau penurunan, serta distribusi jenis kejahatan siber di Indonesia. Pendekatan yuridis-empiris memungkinkan penelitian untuk mengaitkan fenomena kriminal digital dengan kerangka hukum yang berlaku serta kondisi nyata di masyarakat. Analisis dilakukan melalui perhitungan kuantitatif dan visualisasi data dalam bentuk tabel dan grafik. Lokasi Penelitian mencakup wilayah nasional Indonesia, dengan data yang diperoleh dari sumber resmi yaitu Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) [3]. Pemilihan lokasi berskala nasional bertujuan untuk mendapatkan gambaran menyeluruh mengenai kejahatan siber yang terjadi di seluruh Indonesia. Sasaran Penelitian adalah seluruh kasus kejahatan siber yang tercatat pada periode 2023–2024, termasuk penipuan online, phishing, dan ransomware. Selain itu, penelitian juga menyoroti tingkat kekhawatiran publik terhadap kejahatan digital, sehingga dapat mengukur dampak sosial dan persepsi masyarakat terhadap risiko keamanan digital.

3. HASIL DAN PEMBAHASAN

Fenomena kejahatan siber di Indonesia menunjukkan tren yang semakin kompleks dan meningkat signifikan pada periode 2024. Berdasarkan data resmi dari Kominfo, BSSN, dan APJII, tercatat bahwa aduan mengenai penipuan online melalui cekrekening.id mencapai 572.000 kasus kumulatif sejak 2017 hingga 2024. Dari jumlah tersebut, mayoritas berupa penipuan jual-beli online sebanyak 528.415 aduan, sementara investasi fiktif tercatat sebanyak 43.770 aduan. Angka ini

menegaskan bahwa penipuan daring tetap menjadi bentuk kejahatan siber yang paling dominan dan merugikan masyarakat. Selain penipuan online, insiden siber lainnya juga menunjukkan tren yang menarik. BSSN mencatat sebanyak 279 juta serangan siber pada tahun 2023, sedikit menurun dibandingkan tahun sebelumnya yang mencapai 370 juta insiden. Namun, meskipun total anomali trafik menurun dari sekitar 404 juta pada 2023 menjadi 330 juta pada 2024, jenis serangan yang lebih canggih justru meningkat [4]. Aktivitas phishing melonjak hingga 26,7 juta kasus, ransomware tercatat sebanyak 514.508 aktivitas, dan Advanced Persistent Threat (APT) mencapai 2,49 juta aktivitas. Fenomena ini menunjukkan bahwa meskipun volume keseluruhan trafik anomali menurun, kompleksitas dan intensitas serangan meningkat, sehingga tetap menjadi ancaman serius bagi keamanan digital. Tren ini juga tercermin dari persepsi publik. Survei APJII 2024 menunjukkan bahwa 32,5% pengguna internet menganggap penipuan online sebagai bentuk kejahatan siber yang paling mengkhawatirkan, meningkat drastis dari 10,3% pada 2023. Lonjakan sebesar 22,2 poin persentase ini menandakan kesadaran masyarakat terhadap risiko cybercrime yang meningkat, seiring dengan semakin banyaknya kasus yang terungkap dan diberitakan. Berdasarkan temuan tersebut, kejahatan siber di Indonesia saat ini menunjukkan pola yang semakin beragam dan kompleks, mulai dari penipuan daring hingga serangan digital canggih seperti phishing, ransomware, dan APT. Penurunan jumlah total anomali trafik bukan berarti risiko menurun, melainkan menandakan pergeseran jenis serangan ke bentuk yang lebih sulit dideteksi. Oleh karena itu, upaya pencegahan perlu difokuskan pada peningkatan literasi digital, penguatan keamanan siber, serta kolaborasi aktif antara pemerintah, aparat hukum, penyedia layanan digital, dan masyarakat agar ekosistem digital di Indonesia menjadi lebih aman dan terpercaya.

3.1 Data Statistik Resmi Mengenai Jumlah, Jenis, dan Tren Kejahatan Siber

Berdasarkan laporan resmi dari Kominfo (cekrekening.id), BSSN, dan APJII, berikut ringkasan data kejahatan siber di Indonesia pada periode 2024:

Tabel 1: Data *Cybercrime* (2024) [5]

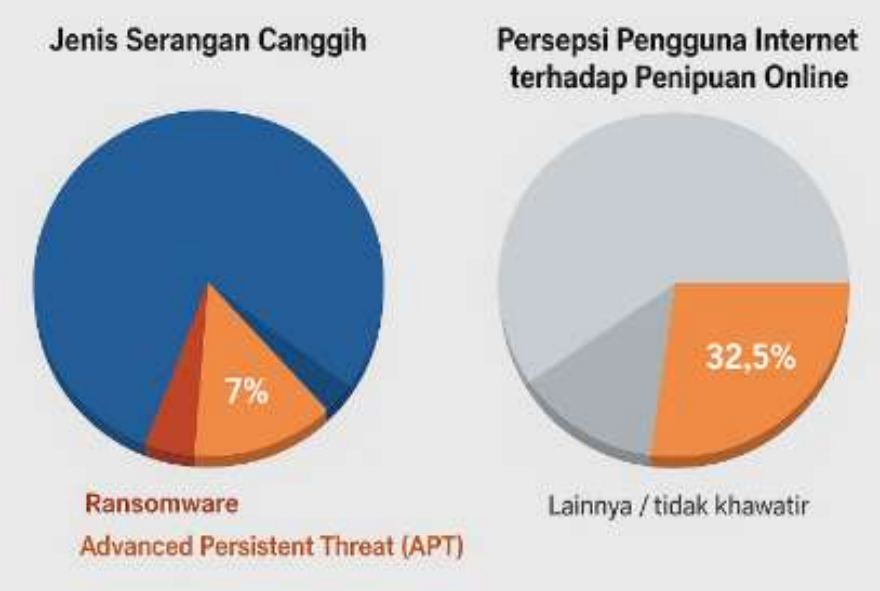
Kategori	Jenis / Keterangan	2024	Keterangan / Perubahan
Penipuan Online	Aduan rekening (cekrekening.id)	572.000 kumulatif (2017–2024)	Total kumulatif
	Jual-beli online	528.415 aduan	-
	Investasi fiktif	43.770 aduan	-
Serangan Siber (BSSN)	Total Kejahatan	-	Turun dibanding 2022 (370 juta)
Trafik Anomali	Jumlah	330.527.636	Turun 73.463.177
Jenis Serangan Canggih	*Phishing*	26.771.610 aktivitas	-
	Ransomware	514.508 aktivitas	-
	Advanced Persistent Threat (APT)	2.487.041 aktivitas	-
Persepsi Pengguna Internet terhadap Penipuan Online	Persentase merasa penipuan paling mengkhawatirkan	32,5%	Meningkat 22,2 poin persentase

Jika dilihat dari jenis serangan siber yang lebih canggih, *phishing* masih menjadi ancaman terbesar dengan 26.771.610 aktivitas, diikuti *ransomware* sebanyak 514.508 aktivitas, serta serangan *Advanced Persistent Threat* (APT) mencapai 2.487.041 aktivitas.

Selain itu, persepsi pengguna internet terhadap penipuan online menunjukkan peningkatan kekhawatiran. Persentase pengguna yang merasa penipuan online sebagai ancaman paling mengkhawatirkan mencapai 32,5%, meningkat 22,2 poin persentase dibandingkan tahun sebelumnya. Hal ini menunjukkan bahwa meskipun beberapa insiden menurun, dampak psikologis dan kekhawatiran masyarakat terhadap kejahatan siber justru meningkat secara signifikan.

Perkembangan teknologi informasi yang pesat tidak hanya membawa manfaat positif bagi masyarakat, tetapi juga membuka peluang baru bagi para pelaku kejahatan siber. Ancaman-ancaman digital semakin beragam dan kompleks, mulai dari serangan *ransomware* yang dapat melumpuhkan sistem dengan cara mengenkripsi data penting hingga ancaman jangka panjang berupa *Advanced Persistent Threat* (APT) yang dilakukan secara tersembunyi dan berkesinambungan. Di sisi lain, tingkat kewaspadaan pengguna internet terhadap ancaman penipuan online juga bervariasi. Sebagian besar masyarakat mungkin masih menganggap risiko tersebut tidak terlalu mengkhawatirkan, padahal kenyataannya, modus kejahatan siber terus berkembang dan semakin sulit dideteksi.

Oleh karena itu, memahami gambaran umum tentang jenis serangan canggih dan persepsi pengguna internet terhadap ancaman online, sebagaimana ditunjukkan dalam diagram, menjadi langkah awal yang krusial untuk meningkatkan kesadaran serta mendorong tindakan pencegahan yang lebih efektif.



Gambar 1. Jenis Serangan Canggih dan Persepsi Pengguna Internet Terhadap Penipuan Online

Berdasarkan diagram pertama mengenai jenis serangan canggih, terlihat bahwa *ransomware* dan *Advanced Persistent Threat* (APT) hanya menempati porsi kecil yaitu sebesar 7%. Hal ini menunjukkan bahwa meskipun jumlahnya relatif kecil dibandingkan bentuk serangan siber lainnya, kedua jenis serangan ini tetap memiliki tingkat bahaya yang sangat tinggi karena dapat menyebabkan kerugian besar bagi individu maupun organisasi. Sementara itu, pada diagram kedua yang menggambarkan persepsi pengguna internet terhadap penipuan online, tercatat sebanyak 32,5% pengguna merasa tidak khawatir atau menganggap ancaman ini bukan hal yang serius. Data tersebut mengindikasikan adanya kesenjangan antara tingkat ancaman nyata yang semakin kompleks dengan kewaspadaan masyarakat yang masih rendah. Dengan demikian, hasil ini menegaskan pentingnya peningkatan literasi digital dan kesadaran keamanan siber agar masyarakat lebih siap menghadapi berbagai modus kejahatan online yang terus berkembang.

Berdasarkan data-data tersebut, jelas bahwa ruang digital telah berkembang menjadi arena kriminalitas baru yang lebih kompleks daripada kejahatan konvensional. Kompleksitas tersebut tidak hanya terletak pada variasi modus operandi, tetapi juga pada sifat kejahatan siber yang lintas batas negara dan sulit dilacak.

3.2. Dampak Sosial-Ekonomi, Kesenjangan Literasi Digital, Implikasi Kebijakan, Proyeksi Ke Depan

Selain gambaran statistik, penting untuk melihat dampak sosial-ekonomi yang ditimbulkan oleh meningkatnya kejahatan siber di Indonesia. Dari sisi ekonomi, penipuan online yang mencapai 572.000 aduan sejak 2017 telah menimbulkan kerugian finansial yang sangat besar, baik bagi individu maupun sektor bisnis. Mayoritas kasus berupa penipuan jual-beli

online (528.415 aduan) menunjukkan bahwa kejahatan ini langsung menyasar masyarakat umum yang aktif bertransaksi digital. Hal ini dapat menurunkan tingkat kepercayaan publik terhadap ekosistem e-commerce dan fintech yang sedang berkembang pesat di Indonesia. Sementara itu, investasi fiktif yang tercatat sebanyak 43.770 aduan juga berimplikasi pada menurunnya kepercayaan terhadap instrumen keuangan digital, padahal sektor ini berperan penting dalam mendukung pertumbuhan ekonomi nasional.

Dari sisi sosial, meningkatnya kasus phishing dan ransomware juga menimbulkan dampak psikologis yang serius. Korban tidak hanya kehilangan data atau uang, tetapi juga mengalami trauma digital berupa rasa tidak aman saat menggunakan internet. Hal ini dapat mengurangi produktivitas digital masyarakat, menghambat adopsi teknologi baru, serta memperburuk kesenjangan literasi digital antar kelompok pengguna. Fakta bahwa 67,5% pengguna internet masih belum menganggap penipuan online sebagai ancaman serius menunjukkan bahwa mayoritas masyarakat berada dalam kondisi rawan menjadi korban berikutnya.

Implikasi kebijakan dari temuan ini sangat penting. Pertama, regulasi keamanan siber perlu diperbarui secara adaptif untuk merespons pola serangan baru seperti ransomware dan *Advanced Persistent Threat* (APT). Kedua, kapasitas aparat penegak hukum di bidang *cybercrime investigation* dan *digital forensic* harus diperkuat agar penanganan kasus tidak tertinggal dari modus kejahatan yang semakin kompleks. Ketiga, kolaborasi lintas sektor menjadi krusial, di mana pemerintah, penyedia layanan digital (e-commerce, perbankan, fintech), serta masyarakat harus bersinergi dalam mencegah kejahatan siber. Mekanisme *public-private partnership* dapat diwujudkan dalam bentuk sistem deteksi dini (*early warning system*), berbagi data insiden siber, hingga kampanye literasi digital yang masif.

Ke depan, tren kejahatan siber di Indonesia diperkirakan akan terus mengalami pergeseran dari sekadar serangan kuantitatif menuju serangan yang lebih berkualitas dan canggih. Jika tidak diantisipasi dengan baik, potensi kebocoran data masif maupun kerugian ekonomi bernilai miliaran rupiah bisa semakin meningkat. Oleh karena itu, strategi nasional keamanan siber harus menempatkan aspek literasi digital, penguatan teknologi pertahanan, dan kerja sama internasional sebagai prioritas utama agar Indonesia mampu menghadapi tantangan kriminalitas digital yang semakin kompleks.

3.3. Upaya Pencegahan Kejahatan Siber di Indonesia

Upaya pencegahan kejahatan siber di Indonesia harus dilakukan secara komprehensif dengan melibatkan seluruh pemangku kepentingan. Dari sisi masyarakat, peningkatan literasi digital menjadi langkah paling mendasar untuk mengurangi potensi korban. Edukasi yang berkelanjutan perlu diberikan agar pengguna internet mampu mengenali modus penipuan online, phishing, maupun investasi fiktif, serta memahami pentingnya praktik keamanan digital seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, dan verifikasi situs sebelum melakukan transaksi. Di tingkat infrastruktur, pemerintah dan sektor swasta perlu memperkuat sistem keamanan siber melalui penerapan teknologi deteksi dini, termasuk pemanfaatan kecerdasan buatan (*Artificial Intelligence/AI)* dan pembelajaran mesin (*Machine Learning*) untuk mengidentifikasi pola serangan secara real-time. Pusat operasi keamanan siber (*Security Operation Center/SOC*) di berbagai lembaga vital juga harus dioptimalkan agar mampu merespons insiden dengan cepat [7],[8],9],[10].

Selain itu, aspek regulasi memainkan peran penting dalam menciptakan perlindungan hukum yang tegas. Regulasi keamanan siber harus disesuaikan dengan perkembangan modus serangan, harmonis dengan standar internasional, dan dilengkapi sanksi yang mampu memberikan efek jera. Perlindungan data pribadi juga harus diperketat guna meminimalisasi risiko kebocoran informasi yang kerap menjadi pintu masuk kejahatan digital. Dalam konteks kolaborasi, diperlukan sinergi aktif antara pemerintah, aparat penegak hukum, penyedia layanan digital, perbankan, *fintech*, hingga masyarakat luas. Kolaborasi ini dapat diwujudkan dalam bentuk forum koordinasi nasional, berbagi data insiden siber secara cepat, serta protokol bersama dalam penanganan darurat serangan ransomware maupun kebocoran data.

Karena sifat kejahatan siber yang lintas batas negara, kerja sama internasional juga menjadi bagian yang tidak terpisahkan. Indonesia perlu berperan aktif dalam jaringan internasional seperti INTERPOL *Cybercrime* Program maupun ASEAN *Cybersecurity Cooperation* untuk memperkuat kapasitas nasional dalam menghadapi ancaman global. Pertukaran intelijen siber, perjanjian bilateral atau multilateral, serta peningkatan kemampuan aparat hukum melalui pelatihan digital forensic internasional akan memperkuat daya tangkal Indonesia terhadap serangan lintas negara. Dengan kombinasi literasi digital, penguatan infrastruktur teknologi, regulasi yang adaptif, kolaborasi lintas sektor, serta kerja sama internasional,

ekosistem digital di Indonesia diharapkan dapat berkembang lebih aman, terpercaya, dan mendukung pertumbuhan ekonomi digital nasional secara berkelanjutan.

4. KESIMPULAN

Kejahatan siber di Indonesia pada 2024 menunjukkan pola yang semakin kompleks. Meski total anomali trafik menurun, serangan canggih seperti phishing (26,7 juta aktivitas), ransomware (514 ribu), dan Advanced Persistent Threat (APT) (2,4 juta) justru meningkat. Aduan penipuan online melalui cekrekening.id juga mencapai 572 ribu kasus kumulatif sejak 2017, didominasi penipuan jual-beli daring dan investasi fiktif. Kesadaran publik terhadap ancaman ini mulai tumbuh, ditunjukkan oleh kenaikan persepsi risiko penipuan online dari 10,3% (2023) menjadi 32,5% (2024), meski sebagian besar masyarakat masih kurang waspada. Situasi ini menegaskan bahwa ruang digital telah menjadi arena kriminalitas baru dengan dampak ekonomi dan sosial yang serius, termasuk kerugian finansial, hilangnya kepercayaan terhadap layanan digital, serta rasa tidak aman dalam bertransaksi daring. Untuk mengatasinya, Indonesia memerlukan strategi pencegahan komprehensif melalui literasi digital, penguatan infrastruktur keamanan, regulasi adaptif, kolaborasi multipihak, dan kerja sama internasional. Dengan langkah tersebut, ekosistem digital nasional dapat terbangun lebih aman, terpercaya, dan mendukung pertumbuhan ekonomi digital berkelanjutan.

5. SARAN

Dalam penerapannya, tentu data musti di perkuat dengan analisis yang lebih baik, dengan begitu hasil juga akan lebih baik.

6. DAFTAR PUSTAKA

[1] A. Sriyani, F. Faturahman, Z. Isnan, dan Darsiti, "Survei Kesejahteraan Digital Dalam Pengelolaan Privasi Di Media Sosial," *ITech J. Inf. Syst. Inform.*, vol. 1, no. 1, hlm. 14–18, 2024.
[2] I. D. Priyani dan N. Anggraini, "Survei Jenis Tindak Kejahatan Cyber dalam Lingkungan Universitas di Indonesia," *ITech J. Inf. Syst. Inform.*, vol. 1, no. 1, hlm. 28–35, 2024.
[3] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2024). Survei penetrasi internet dan keamanan siber. Jakarta: APJII.
[4] Badan Siber dan Sandi Negara (BSSN). (2024). Data insiden siber nasional 2023–2024. Jakarta: BSSN.
[5] Cekrekening.id. (2024). Rekap aduan penipuan online 2017–2024. Diakses dari https://www.cekrekening.id
[6] Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). Laporan statistik kejahatan siber Indonesia 2023–2024. Jakarta: Kominfo.
[7] Marzuki, P. M. (2021). Penegakan hukum dan teknologi informasi. Jakarta: Kencana.
[8] Nugroho, A. (2022). Kriminalitas siber dan hukum di Indonesia. Jakarta: Rajawali Pers.
[9] Simanjuntak, H. (2019). Perlindungan hukum terhadap korban penipuan online. Bandung: Refika Aditama.
[10] Subekti, R., & Tjitrosoedibio, S. (2020). Hukum pidana Indonesia (12th ed.). Jakarta: Pradnya Paramita.