open access
Published online on: https://journal.uii.ac.id/jurnalsnati/
Check for updates
DOI: 10.20885/snati.v4.i2.40362
JURNAL SNATI Sains, Nalar, dan Aplikasi Teknologi Informasi
Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi
Vol. 4 No. 2 (2025) 149 - 156 ISSN Media Electronic: 2807-5935

Analisis Risiko Keamanan Data Pribadi Pada Penggunaan Media Sosial Instagram Dengan Menggunakan Metode DREAD

Analysis of Personal Data Security Risks on the Use of Instagram Social Media Using the DREAD Method

Rapina[1*], Ikhwan Fitrah Albuchori[2]
[1,2]Jurusan Sains Alam dan Ilmu Formal, Fakultas Sains dan Teknik, Universitas Bangka Belitung, Merawang, Indonesia
[1*]rafinapkp@gmail.com, [2]pitotbuntot999@gmail.com

Abstract

The rapid development of information technology, especially through social media such as Instagram, has facilitated digital interactions but also increased potential risks to personal data security. Lack of user awareness in maintaining privacy and weak security settings are often exploited by irresponsible parties to commit data breaches. This study was conducted to analyze the level of risk of personal data security in Instagram users, given the high user activity on the platform without adequate protection. The study used DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) method to measure and classify the risk of various threats that may occur. The sample was selected from 15 active Instagram users, with data collection through a questionnaire based on a Likert scale of 1 to 3. The results of the analysis show that threats such as identity theft and data leakage fall into the high-risk category with an average value above 2.6. To reduce these risks, the implementation of two-factor authentication (2FA), stricter privacy settings, and increased digital security literacy among users are recommended. This study emphasizes the importance of individual awareness and platform policy support in maintaining personal data security in the digital era.

Keywords: Instagram; Data Security; DREAD Method; Privacy Risk; Mitigation

Abstrak

Perkembangan teknologi informasi yang pesat, khususnya melalui media sosial seperti Instagram, telah mempermudah interaksi digital namun juga meningkatkan potensi risiko terhadap keamanan data pribadi. Kurangnya kesadaran pengguna dalam menjaga privasi serta lemahnya pengaturan keamanan sering kali dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan pelanggaran data. Penelitian ini dilakukan untuk menganalisis tingkat risiko keamanan data pribadi pada pengguna Instagram, mengingat tingginya aktivitas pengguna di platform tersebut tanpa perlindungan yang memadai. Penelitian menggunakan metode DREAD (Damage, Reproducibility, Exploitability, Affected Users, dan Discoverability) untuk mengukur dan mengklasifikasikan risiko dari berbagai ancaman yang mungkin terjadi. Sampel dipilih secara purposive terhadap 15 responden aktif pengguna Instagram, dengan pengumpulan data melalui kuesioner berbasis skala Likert 1 hingga 3. Hasil analisis menunjukkan bahwa ancaman seperti pencurian identitas dan kebocoran data termasuk dalam kategori risiko tinggi dengan nilai rata-rata di atas 2,6. Untuk mengurangi risiko tersebut, disarankan penerapan two-factor authentication (2FA), pengaturan privasi yang lebih ketat, dan peningkatan literasi keamanan digital di kalangan pengguna. Penelitian ini menegaskan pentingnya kesadaran individu dan dukungan kebijakan platform dalam menjaga keamanan data pribadi di era digital.

Kata kunci: Instagram; Keamanan Data; Metode DREAD; Risiko Privasi; Mitigasi

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi sekarang ini semakin berkembang dengan sangat cepat dan maju. Teknologi ini telah mengubah pola hidup manusia, seperti cara mereka bekerja, bertindak, ataupun dalam kegiatan sehari-hari. Teknologi ini ada berbagai macam, salah satu contohnya adalah internet. Internet merupakan sebuah sistem komunikasi digital yang bisa menghubungkan komputer beserta jaringannya ke seluruh dunia. Dengan adanya kemajuan seperti ini dapat menyediakan atau memfasilitasi terciptanya digital yang semakin luas, yang dimana hal ini hampir semua aspek kehidupan bisa dilakukan secara online [1].

Teknologi digital membawa banyak manfaat signifikan dalam kehidupan sekarang. Di bidang

Received: 18-05-2025 | Revised: 02-07-2025 | Accepted: 03-07-2025 | Published: 10-07-2025

komunikasi, seperti membuat orang dapat berinteraksi secara *real-time* tanpa hambatan waktu maupun jarak. Di kehidupan sehari-hari, teknologi juga membantu mempermudah pekerjaan dan kegiatan seperti belanja, transaksi, pemesanan transportasi, dan mencari hiburan. Manfaat-manfaat ini menjadi bukti bahwa teknologi menjadi acuan untuk membangun masyarakat di masa sekarang agar lebih terhubung dan efisien [2].

Namun, dibalik manfaatnya yang luar biasa, perkembangan teknologi juga membawa dampak yang signifikan, baik dalam aspek sosial, psikologis, maupun keamanan informasi. Meskipun teknologi memberikan banyak kemudahan, teknologi juga menimbulkan dampak negatif. Salah satu dampak yang paling krusial yaitu ancaman terhadap privasi dan keamanan data pribadi. Banyak kasus penyalahgunaan informasi sensitif seseorang karena kurangnya kesadaran dan pemahaman terhadap pentingnya perlindungan data di dunia digital [3].

Salah satu platform utama terjadinya penyebaran informasi pribadi adalah media sosial, terutama Instagram, yang menjadi fokus utama pada penelitian ini. Instagram merupakan salah satu media sosial berbasis visual yang paling disukai di seluruh dunia, termasuk di Indonesia. Dengan fitur-fitur seperti *story, reel, direct message*, dan tag lokasi, Instagram menyediakan tempat untuk pengguna membagikan momen dengan mudah dan menarik. Namun, Instagram menyimpan banyak celah yang dapat membahayakan data pribadi penggunanya. Banyak pengguna membagikan informasi yang sensitif secara terbuka tanpa mengetahui bahayanya. Selain itu, penggunaan aplikasi pihak ketiga yang terhubung ke akun instagram juga dapat meningkatkan risiko kebocoran data. Sehingga, pentingnya melakukan analisis terhadap potensi risiko keamanan data pribadi pada penggunaan instagram, agar dapat lebih bijak dalam menjaga privasi digital [4]. Berbagai faktor dapat memicu risiko keamanan data di Instagram, misalnya kelemahan sistem (ancaman siber), serangan dari peretas (*hacking* atau *phishing*), atau kebocoran data karena kecerobohan pengguna. Selain itu, penyalahgunaan data oleh pihak dalam, kebijakan privasi yang tidak jelas, ketidakpatuhan Instagram terhadap aturan perlindungan data (seperti GDPR atau UU PDP), serta kurangnya pengawasan dari pihak berwenang juga bisa menjadi pemicu [5].

Selain itu, pengguna Instagram rentan menghadapi berbagai masalah, seperti pencurian identitas, penyebaran informasi pribadi tanpa izin (*doxing*), atau manipulasi data untuk penipuan. Tidak hanya itu, ketidakpuasan pengguna terhadap kebijakan keamanan Instagram seperti enkripsi yang lemah, pelacakan aktivitas berlebihan, atau kegagalan platform dalam menangani perundungan siber dapat memperburuk risiko privasi. Oleh sebab itu, semua pihak, termasuk pengguna, penyedia layanan, dan pemerintah, harus aktif dalam mengenali, mengevaluasi, dan mengendalikan risiko keamanan data agar kerugian yang mungkin timbul dapat diminimalkan [6].

Selain doxing, Instagram juga menghadapi risiko kebocoran data melalui eksploitasi API (*Application Programming Interface*). Aplikasi pihak ketiga yang berintegrasi dengan Instagram tanpa diawasi oleh platform dapat mengakses data pengguna yang berlebihan, seperti riwayat aktivitas, daftar pengikut (*followers*), dan bahkan pesan pribadi (*Direct Messages* atau DMs). Misalnya, aplikasi filter atau alat analitik sering meminta izin untuk mengakses profil pengguna. Hal ini dapat menyebabkan data disalahgunakan untuk iklan atau dijual ke data broker. Hal ini lebih buruk karena pengguna tidak memahami persyaratan dan ketentuan privasi yang rumit, yang membuat mereka tidak tahu seberapa banyak data mereka digunakan [7].

Sebagai platform yang mengutamakan konten visual, Instagram memiliki keunikan dalam risiko privasi dibandingkan media sosial lainnya. Fitur seperti Instagram *Stories* yang menghilang setelah 24 jam sering dianggap aman, padahal konten tersebut dapat disimpan atau di-*screenshot* oleh pihak lain. Selain itu, *Reels* dan IG *Live* memicu budaya *oversharing*, di mana pengguna tanpa sadar membagikan detail kehidupan pribadi seperti rutinitas, lingkungan rumah, atau bahkan dokumen penting yang terlihat di latar belakang [8].

Di sisi lain, keragaman penggunaan alat link-in-bio seperti *Linktree* menambah masalah. Tautan *phising* atau malware sering menyembunyikan alamat URL yang dipendekkan atau diarahkan ke situs eksternal. Pengguna yang tidak berhati-hati dapat mengklik tautan palsu yang mengatasnamakan survei berhadiah, giveaway, atau iklan produk, yang dapat mengakibatkan pencurian data atau infeksi perangkat. Akun bisnis atau influencer yang sering mempromosikan link eksternal tanpa verifikasi memiliki risiko yang lebih besar. Selain itu, ketika Anda menggunakan Instagram, Anda tidak hanya menghadapi masalah teknis, tetapi juga dapat menyebabkan masalah psikologis seperti *comparison fatigue* dan kelelahan mental karena membandingkan diri dengan kehidupan yang "sempurna" di media sosial. Kondisi ini dapat membuat pengguna kurang waspada terhadap keamanan data mereka, seperti dengan mudah mengklik tautan atau berbagi data pribadi untuk mengikuti tren tertentu. Studi menunjukkan bahwa orang yang mengalami stres digital lebih cenderung mengabaikan peringatan *phising* atau permintaan akses data yang tidak wajar [9].

Beberapa penelitian terdahulu telah mengkaji penerapan metode threat modeling seperti STRIDE dan DREAD dalam berbagai konteks sistem informasi. Penelitian oleh Alang dkk. (2025) mengungkapkan bahwa sistem layanan pendidikan menghadapi risiko

tinggi akibat konfigurasi CORS yang permisif, yang memungkinkan akses tidak sah dan kebocoran data. Melalui mitigasi seperti validasi CORS, enkripsi, dan otentikasi berbasis peran, risiko tersebut berhasil ditekan secara signifikan. Hal ini menunjukkan bahwa kombinasi STRIDE dan DREAD efektif dalam merancang pengamanan sistem pendidikan [10].

Penelitian lain oleh Gina dkk. (2023) menilai risiko keamanan pada *website* menggunakan kombinasi DREAD dan ISO 27005:2018. Mereka menemukan bahwa risiko tertinggi terdapat pada aspek *availability*, terutama pada proses unggah berkas, dengan skor risiko sedang (11,5). Mereka menyarankan penggunaan pendekatan berbasis aset dan *tools* penilaian untuk perbaikan lanjutan [11]. Sementara itu, Azis dkk. (2021) menerapkan STRIDE dan DREAD untuk mengidentifikasi ancaman pada sistem informasi akademik, dan menemukan bahwa *spoofing*, *tampering*, dan *repudiation* memiliki risiko tinggi. Mereka merekomendasikan penguatan kontrol keamanan untuk menekan potensi ancaman tersebut [12]. Dalam konteks media sosial, Mesra dkk. (2022) menekankan pentingnya keamanan data pribadi dengan menyoroti enam prinsip utama: keamanan data, kesadaran pengguna, kontrol privasi, manajemen risiko, transparansi, dan etika. Mereka mendorong pendekatan yang memprioritaskan kontrol pengguna atas data pribadinya [2]. Penelitian oleh Hena dkk. (2023) juga menunjukkan bahwa evaluasi risiko menggunakan *framework* NIST SP 800-30 dapat membantu merancang langkah-langkah pengamanan yang sesuai dengan tingkat risiko dan kontrol yang dibutuhkan [13]. Terakhir, Mokhamad dkk. (2021) melakukan penilaian kerentanan pada sistem *e-learning* menggunakan STRIDE dan DREAD, menghasilkan laporan keamanan yang mencakup deskripsi ancaman, tingkat dan jenis serangan, serta langkah pencegahan [14].

Penelitian ini dilakukan karena meningkatnya kekhawatiran terhadap keamanan data pribadi di *platform* media sosial, khususnya Instagram. Banyak pengguna Instagram tidak menyadari dampak berbagi data pribadi secara terbuka dan bahaya yang timbul dari aplikasi pihak ketiga yang menghubungkan akun mereka. Oleh karena itu, analisis risiko yang lebih mendalam diperlukan untuk memberikan pemahaman dan upaya pencegahan kebocoran data.

Berdasarkan latar belakang dan tinjauan literatur, penelitian ini bertujuan untuk menjawab beberapa pertanyaan kritis terkait risiko keamanan data pribadi di Instagram. Pertama, bagaimana tingkat risiko keamanan data pribadi pengguna Instagram jika dinilai menggunakan metode DREAD? Kedua, ancaman apa saja yang termasuk dalam kategori risiko tinggi, sedang, dan rendah berdasarkan analisis tersebut? Ketiga, langkah mitigasi seperti apa yang dapat direkomendasikan untuk mengurangi risiko tersebut, baik bagi pengguna maupun platform Instagram? Dengan menjawab pertanyaan-pertanyaan ini, penelitian diharapkan dapat memberikan panduan praktis dalam meningkatkan kesadaran dan keamanan data pribadi di media sosial.

Tujuan utama dari penelitian ini adalah untuk menganalisis risiko keamanan data pribadi pada penggunaan media sosial instagram dengan menggunakan metode DREAD. Metode DREAD adalah model penghitungan risiko *Microsoft* yang dapat memberikan informasi penilaian risiko untuk ancaman yang teridentifikasi [11]. Selain itu, metode ini digunakan untuk menilai dan mengklasifikasikan ancaman berdasarkan risiko eksploitasi kerentanannya. Meskipun demikian, kelemahan dari model ini terletak pada kurangnya konkretisasi dalam deskripsi atribut dan tingkat risikonya, yang dapat menyebabkan penilaian risiko menjadi lebih subjektivitas. Ini berarti bahwa hasil analisis sangat bergantung pada pendapat individu atau kelompok yang melakukan evaluasi. Oleh sebab itu, penelitian ini diharapkan dapat membantu pengguna dan pihak terkait dalam menemukan ancaman dan merancang solusi yang efektif untuk melindungi data pribadi mereka [10].

2. Metode Penelitian

Pada penelitian ini tahapan untuk menganalisis risiko keamanan data pribadi pada penggunaan media sosial Instagram sebagai berikut:

Gambar 1. Tahapan Penelitian

2.1. Identifikasi Masalah

Dalam tahap penelitian, identifikasi masalah merupakan langkah yang sangat krusial karena menjadi fondasi bagi tujuan dan konsentrasi studi. Penelitian ini menunjukkan bahwa pengguna platform media sosial, terutama Instagram, banyak yang tidak menyadari potensi risiko terkait privasi dan keamanan ketika mereka membagikan informasi pribadi seperti lokasi, foto keluarga, atau kegiatan sehari-hari. Penggunaan fungsi-fungsi seperti penandaan lokasi, Instagram *stories*, dan penghubungan dengan aplikasi lain semakin memperbesar kemungkinan

penyalahgunaan data oleh individu yang tidak bertanggung jawab. Sebagai contoh, penandaan lokasi dapat menunjukkan kebiasaan pergerakan pengguna, Kisah yang sementara dapat tetap tersimpan atau dibagikan, sementara sambungan ke aplikasi lain berisiko mengambil data tanpa izin yang cukup. Selain itu, masalah ini diperparah oleh rendahnya pemahaman pengguna mengenai pengaturan privasi dan keamanan akun, seperti kurangnya penggunaan fitur *two-factor authentication* (2FA), ketidaktahuan tentang opsi privasi akun, serta minimnya pemantauan terhadap aplikasi pihak ketiga yang terhubung. Dampaknya tidak hanya berupa pelanggaran privasi, tetapi juga berpotensi memicu kejahatan siber, penipuan, *doxxing*, hingga ancaman fisik [15].

2.2. Pengumpulan Data

Pada tahapan ini, peneliti menyebarkan kuesioner melalui link google form kepada responden yaitu para pengguna aktif instagram dengan berfokus pada risiko keamanan data mereka di media sosial instagram dan dengan menggunakan skala penilaian dari 1 hingga 3 untuk setiap elemen model DREAD [12]. Tujuan dari pertanyaan ini adalah untuk mengukur seberapa besar kerugian, seberapa mudah digunakan, dan seberapa banyak data pribadi yang ditemukan di akun Instagram mereka. Jawaban responden diberi label antara "Sangat Kecil", "Sedang", dan "Sangat Besar", masing-masing Selanjutnya, data direkap untuk menilai risiko secara kuantitatif [11].

2.3. Penilaian Tingkat Risiko

Tabel 1. Penilaian Risiko DREAD [16]

	Tinggi (3)	Sedang (2)	Rendah (1)
D	Sistem lumpuh; Dapat mengakses administrator; Sistem diambil alih; Dapat menambah konten.	Bocornya informasi sensitif.	Bocornya informasi biasa.
R	Serangan dapat terjadi setiap saat dan berulang-ulang.	Serangan dapat terjadi pada saat tertentu.	Serangan sulit dilakukan walaupun memiliki kerentanan.
E	Serangan dengan mudah dilakukan.	Serangan berhasil namun membutuhkan beberapa kali percobaan.	Membutuhkan orang yang sangat ahli dalam melakukan serangan.
A	Semua pengguna, konfigurasi default, pelanggan.	Beberapa pengguna, konfigurasi non default.	Persentase yang sangat kecil dari pengguna, fitur tidak jelas.
D	Informasi kesalahan sistem dapat terlihat dengan jelas. Kerentanan ditemukan dengan mudah.	*Bug* sistem jarang terlihat.	Kesalahan sulit di identifikasi.

Pada Tabel 1 penilaian risiko di atas dengan metode DREAD digunakan untuk menilai tingkat risiko, di mana peringkat 1 dianggap rendah, peringkat 2 berada pada tingkat sedang, dan peringkat 3 dikategorikan sebagai tinggi. Setelah dilakukan analisis potensi risiko, kemudian dilanjutkan dengan penilaian ancaman dengan rumus sebagai berikut [16].

DREAD RISK = (Damage + Reproducibility + Exploitability + Affected User + Discoverability) / 5

Tabel 2. Deskripsi DREAD [16]

No	Kategori	Deskripsi
1	*Damage*	Seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan.
2	*Reproducibility*	Seberapa sering serangan diulang dan seberapa mudah untuk mereproduksi serangan.
3	*Exploitability*	Berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman.
4	*Affected*	Seberapa banyak pengguna yang terpengaruh jika ancaman dieksploitasi.
5	*Discoverability*	Seberapa mudah bagi penyerang untuk menemukan ancaman pada sistem.

Berdasarkan tabel 2 di atas, terdapat lima kategori DREAD digunakan untuk menilai risiko: *Damage Potential* (tingkat kerusakan yang ditimbulkan), *Reproducibility* (kemudahan serangan diulang), *Exploitability* (kemudahan dan sumber daya untuk menyerang), *Affected Users* (jumlah pengguna yang terdampak), dan *Discoverability* (kemudahan menemukan celah ancaman) [20]. Seperti yang disebutkan sebelumnya, model DREAD memerlukan nilai antara satu hingga tiga untuk setiap lima elemen utama. Oleh karena itu, setiap ancaman akan memiliki nilai total antara satu hingga tiga. Menurut model DREAD, ancaman dengan nilai atau rata-rata antara 1,0 dan 1,5 menunjukkan risiko rendah, nilai antara 1,6 dan 2,5 menunjukkan risiko sedang, dan nilai antara 2,6 dan 3,0 menunjukkan risiko tinggi [10].

Tabel 3. Pernyataan Responden

No	Kategori	Pernyataan
1	*Damage*	Seberapa besar kerugian yang Anda rasakan jika informasi pribadi (seperti alamat, nomor HP, atau lokasi) yang Anda bagikan di Instagram disalahgunakan oleh orang lain?
2	*Reproducibility*	Menurut Anda, seberapa mudah seseorang dapat melihat kembali atau menyebarkan informasi pribadi Anda yang pernah Anda bagikan di Instagram (misalnya story atau postingan lama)?
3	*Exploitability*	Seberapa mudah menurut Anda pihak tidak bertanggung jawab bisa menyalahgunakan akun Instagram Anda (misalnya lewat tautan phising, login dari aplikasi pihak ketiga, atau lupa log out)?.
4	*Affected*	Jika akun Instagram Anda dibobol atau datanya bocor, seberapa besar kemungkinan bahwa teman, keluarga, atau follower Anda juga akan terkena

		dampaknya (seperti penipuan lewat DM)?
5	*Discoverability*	Seberapa mudah menurut Anda orang lain bisa menemukan data pribadi Anda di Instagram (misalnya lewat bio, postingan, tag lokasi, atau story highlight)?

Tabel 3 di atas merupakan pernyataan yang diajukan kepada responden. Setiap pernyataan merupakan elemen dari setiap DREAD, yaitu (*Damage Potential, Reproducibility, Exploitability, Affected Users,* dan *Discoverability).*

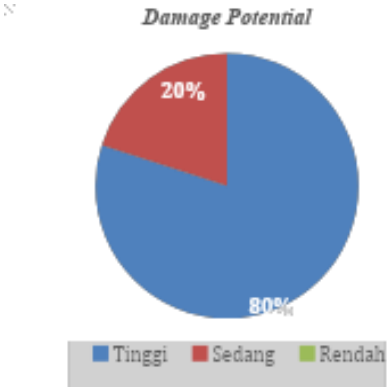
2.4. Mitigasi

Berdasarkan tingkat risiko yang telah diidentifikasi, disusun rencana mitigasi untuk setiap ancaman dengan memprioritaskan ancaman yang memiliki risiko lebih tinggi. Maka dari itu, pengguna dan platform harus mengambil tindakan pencegahan. Untuk mengurangi bahaya tersebut pengguna dapat Pengguna disarankan untuk mengaktifkan *two-factor authentication* (2FA), menghindari mengakses aplikasi pihak ketiga, dan selalu keluar dari perangkat umum saat mereka keluar. Gunakan pengaturan privasi untuk membatasi akses ke konten, menghentikan highlight sensitif, dan menghindari tag lokasi real-time. Beritahu teman tentang penipuan DM dan beri tahu kontak jika ada sesuatu yang mencurigakan. Metode ini membantu mengelola ancaman keamanan dan privasi di Instagram [17].

3. Hasil dan Pembahasan

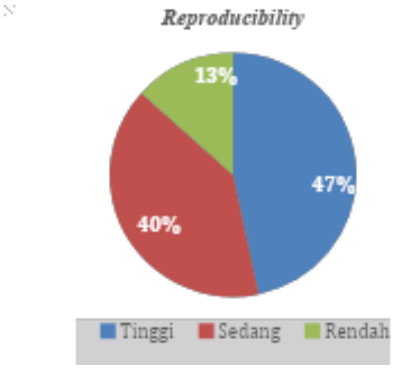
3.1. Hasil

Dibawah ini merupakan diagram dari setiap elemen model DREAD yang dihasilkan dari beberapa pernyataan yang telah diajukan kepada responden.

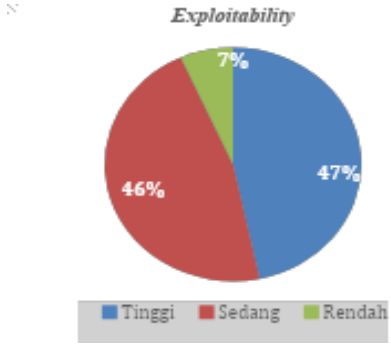


Gambar 2. Pernyataan *Damage Potential*

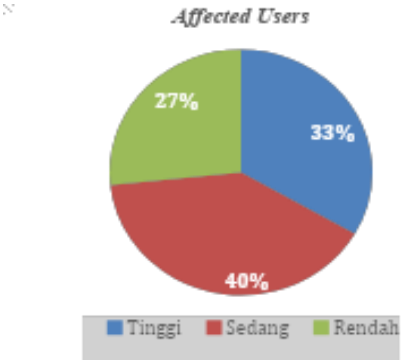
Pada gambar 2 di atas, menunjukkan sebagian besar responden, yaitu 80%, menganggap risiko kerusakan akibat penyalahgunaan informasi pribadi di Instagram sebagai sangat tinggi. Sementara itu, 20% responden lainnya menilai risikonya sebagai sedang, dan tidak ada yang memilih opsi rendah. Hasil ini memperkuat argumen bahwa kebocoran data pribadi di Instagram merupakan ancaman serius yang perlu diwaspadai.



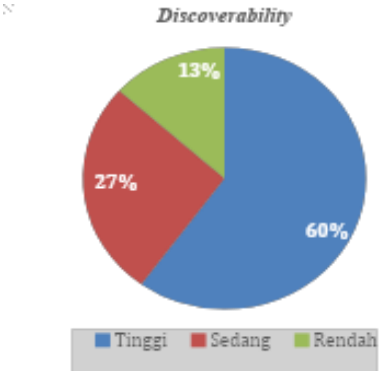
Gambar 3. Pernyataan *Reproducibility*



Gambar 4. Pernyataan *Exploitability*



Gambar 5. Pernyataan *Affected Users*



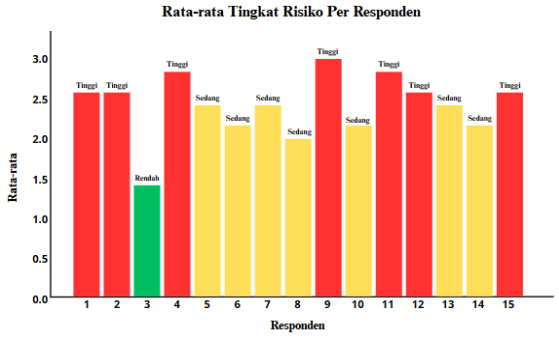
Gambar 6. Pernyataan *Discoverability*

Gambar 3 menunjukkan bahwa sebanyak 47% dari responden menanggapi serangan atau penyalahgunaan data pribadi Instagram memiliki risiko yang tinggi. Sebaliknya, 40% responden menganggap risikonya sedang, dan hanya 13% yang memilih tingkat risiko rendah.

Gambar 4 menunjukkan bahwa sebanyak 47% responden yang memiliki risiko tinggi, dan 46% yang memiliki risiko sedang. Sementara itu, 7% lainnya rendah.

Pada gambar 5 menunjukkan bahwa sebanyak 40% responden menilai jumlah pengguna yang terdampak jika terjadi kebocoran data sebagai tinggi, 33% menganggapnya sedang, dan 27% menganggapnya rendah.

Pada gambar 6 di atas menunjukkan bahwa 60% dari responden yang menjawab menilai kemudahan menemukan data pribadi di Instagram sebagai tinggi, yang berarti informasi seperti lokasi dan detail profil dapat ditemukan dengan sangat mudah, 27% menganggapnya sedang, dan 13% menganggapnya rendah.



Gambar 7. Rata-rata Tingkat Risiko Responden

Dari penyebaran kuesioner kepada responden yang aktif menggunakan instagram, diperoleh hasil data terkait risiko keamanan berdasarkan model DREAD. Setiap elemen (*Damage Potential, Reproducibility, Exploitability, Affected Users,* dan *Discoverability)* dinilai dengan skala 1 hingga 3. Hasil penilaian tingkat risiko selengkapnya disajikan pada Tabel 5.

Tabel 4. Tingkat Risiko

Responden	D	R	E	A	D	Rata-rata	Risiko
1	3	2	3	2	3	2,6	Tinggi
2	3	2	3	3	2	2,6	Tinggi
3	3	1	1	1	1	1,4	Rendah
4	3	3	2	3	3	2,8	Tinggi
5	2	3	2	2	3	2,4	Sedang
6	3	2	2	1	3	2,2	Sedang
7	3	3	2	1	3	2,4	Sedang
8	3	1	2	2	2	2	Sedang
9	3	3	3	3	3	3	Tinggi
10	3	2	3	2	1	2,2	Sedang
11	3	2	3	3	3	2,8	Tinggi
12	3	3	2	3	2	2,6	Tinggi
13	2	3	3	2	2	2,4	Sedang
14	2	2	2	2	3	2,2	Sedang
15	3	3	3	1	3	2,6	Tinggi

Hasil perhitungan kelompok di atas merupakan hasil keseluruhan dari perhitungan seluruh responden, yang ditunjukkan dalam tabel 4. Hasil ini memudahkan analisis dengan mengklasifikasikan ancaman secara keseluruhan, dimana responden dengan tingkat ancaman risiko tinggi, yaitu R1, R2, R4, R9, R11, R12 dan R15. Ancaman dengan risiko sedang, seperti R5, R6, R7, R8, R10, R13 dan R14, serta Ancaman dengan risiko rendah, yaitu R3.

Dari hasil nilai ancaman tersebut dapat dibuatkan grafik keseluruhan ancaman dengan metode DREAD, grafik dapat dilihat pada Gambar 2.

3.2. Pembahasan

Berdasarkan hasil tabel 5 dan gambar 7 di atas yang dilakukan dengan metode DREAD, penelitian ini menunjukkan bahwa sebagian besar pengguna Instagram mengalami risiko besar terhadap keamanan informasi pribadi mereka. Di antara 15 peserta yang disurvei, 7 orang termasuk dalam kategori risiko tinggi dengan skor lebih dari 2,6, terutama yang berkaitan dengan ancaman pencurian identitas dan kebocoran informasi. Hasil ini mengindikasikan bahwa faktor-faktor seperti penggunaan aplikasi dari pihak ketiga, berbagi informasi sensitif, dan minimnya penggunaan fitur keamanan seperti otentikasi dua langkah (2FA) adalah penyebab utama peningkatan kerentanan. Temuan penelitian ini sejalan dengan hasil yang diperoleh oleh Agustin (2020), yang juga menyoroti rendahnya kesadaran pengguna sebagai elemen penting dalam isu keamanan data. Untuk menyelesaikan permasalahan ini, dibutuhkan kerja sama dari berbagai pihak. Pengguna disarankan untuk lebih aktif dalam melakukan langkah-langkah keamanan seperti mengaktifkan autentikasi dua faktor, membatasi akses aplikasi dari pihak ketiga, serta lebih berhati-hati saat membagikan informasi pribadi. Di sisi lain, platform Instagram harus meningkatkan pendidikan mengenai keamanan digital dan mengetatkan regulasi yang berkaitan dengan integrasi dengan aplikasi pihak ketiga. Sementara itu, pemerintah dapat berkontribusi melalui peningkatan sosialisasi mengenai perlindungan data pribadi dan penetapan regulasi yang lebih ketat. Walaupun penelitian ini memberikan pemahaman yang berarti mengenai risiko keamanan data di Instagram, terdapat batasan dalam jumlah responden dan adanya subjektivitas dalam evaluasi yang menggunakan metode DREAD. Oleh sebab itu, penelitian lanjutan dengan jumlah sampel yang lebih besar dan metode yang lebih menyeluruh diperlukan untuk memperoleh hasil yang lebih representatif.

Berdasarkan evaluasi model DREAD terhadap keamanan informasi pribadi di Instagram, terungkap bahwa kemungkinan penyalahgunaan data pribadi cukup tinggi, terutama pada aspek *Damage Potential*, 80% responden berpendapat bahwa penyalahgunaan data pribadi seperti alamat, nomor telepon, atau lokasi bisa mengakibatkan kerugian yang sangat besar. Dalam konteks *Reproducibility*, penelitian menunjukkan bahwa 47% responden menganggap informasi pribadi yang pernah dibagikan di Instagram memiliki risiko tinggi untuk disalahgunakan kembali. Aspek *Exploitability* memperlihatkan bahwa 47% responden menilai akun Instagram mereka rentan terhadap berbagai teknik eksploitasi. Pada aspek

Affected Users, 40% responden menyadari bahwa pembobolan akun mereka dapat berdampak sistemik terhadap jaringan pertemanan mereka. Dan pada aspek *Discoverability*, 60% menganggap bahwa data pribadi mudah dicari melalui bio, tag lokasi, atau sorotan cerita.

3.3. Mitigasi

Setelah mengetahui berapa besar nilai dari setiap risiko, kontrol mitigasi dapat dibuat untuk mengurangi risiko setiap ancaman. Berdasarkan data penilaian ancaman yang disajikan pada Tabel 3, langkah-langkah mitigasi dapat disusun sesuai dengan tingkat risiko yang telah teridentifikasi. Ancaman dengan tingkat risiko tinggi, yaitu R1, R2, R4, R9, R11, R12 dan R15, memerlukan langkah-langkah pencegahan yang lebih ketat, dimana pengguna harus fokus pada proteksi ketat informasi sensitif melalui kombinasi *technical control* (seperti enkripsi data dan sistem autentikasi kuat) dan *administrative control* (kebijakan privasi yang ketat). Ancaman dengan risiko sedang, seperti R5, R6, R7, R8, R10, R13 dan R14, membutuhkan langkah mitigasi yang signifikan tetapi dapat disesuaikan dengan tingkat urgensi yang lebih rendah dibandingkan dengan ancaman berisiko tinggi. Metode pencegahan, seperti melakukan audit konten lama secara teratur dan membatasi akses melalui pengaturan privasi, harus diprioritaskan. Ancaman R3 dengan risiko rendah mungkin tidak memerlukan tindakan segera. Namun, untuk memastikan bahwa risiko tidak meningkat di masa mendatang, tetap perlu dipantau secara berkala. Meskipun efeknya kecil, pengguna harus dididik tentang dasar-dasar keselamatan *cyber*.

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa penggunaan Instagram memiliki berbagai risiko keamanan data pribadi, seperti pencurian identitas, kebocoran data, dan penyalahgunaan informasi pribadi. Metode DREAD digunakan untuk mengklasifikasikan risiko-risiko tersebut ke dalam kategori tinggi, sedang, dan rendah. Berdasarkan metode DREAD, dari 15 responden, 7 responden memiliki risiko tinggi, 7 lainnya berisiko sedang, dan 1 responden berisiko rendah. Selain itu, Analisis model DREAD menunjukkan bahwa keamanan data pribadi di Instagram sangat rentan, terutama dalam hal kemungkinan kerusakan (80%) dan kemudahan penemuan data (60%). Hampir separuh responden mengakui bahwa akun mereka rentan terhadap peretasan (47%) dan penyalahgunaan data lama (47%), sementara 40% mengakui dampak sistemik pada jaringan pertemanan. Oleh karena itu, ancaman dengan tingkat risiko yang tinggi perlu langkah mitigasi yang ketat, seperti penerapan enkripsi data dan penyusunan kebijakan privasi yang jelas. Sedangkan, ancaman dengan risiko yang sedang dan rendah dapat dikelola melalui edukasi pengguna dan pemantauan secara berkala. Hasil penelitian ini menekankan betapa pentingnya kolaborasi antara pengguna, platform, dan pemerintah untuk menjaga keamanan data pribadi. Secara keseluruhan, artikel ini menegaskan pentingnya kesadaran dan tindakan proaktif dari semua pihak untuk melindungi data pribadi di era digital yang semakin kompleks.

Reference

[1] A. P. Kehista *dkk.*, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)," Nusantara Journal of Multidisciplinary Science, vol. 2, no. 1, hlm. 201–207, 2024, doi: 10.31933/jimt.v4i5.

[2] M. B. Yel dan M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," Jurnal Informatika Kaputama (JIK), vol. 6, no. 1, hlm. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

[3] A. D. Naomira, E. Soesanto, dan L. Vilani, "Implementasi Nilai-Nilai Kebangsaan Bersumber UUD 45 dan NKRI Pada Peran Manajemen Sekuriti Guna Meningkatkan Kesadaran, Keamanan Data Pribadi Media Sosial Instagram," Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane, vol. Vol.2, No., no. 2, hlm. 114–121, 2024, [Daring]. Tersedia pada: https://ojs.daarulhuda.or.id/index.php/MHI/index

[4] D. Y. Ratnadewati dan R. V. Oktarina, "Pengaruh Kesadaran Keamanan Informasi terhadap Pengguna Media Sosial Instagram," Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB) 2024, hlm. 442–448, 2024.

[5] F. Ardyansyah, "Analisis Risiko Operasional Pada Kawasan Pantai Jumiang Pamekasan," Jurnal Ekonomi, Manajemen Pariwisata dan Perhotelan, vol. 1, no. Vol 1 No 1 (2022): Januari : Jurnal Ekonomi, Manajemen Pariwisata Dan Perhotelan, hlm. 56–62, 2022, [Daring]. Tersedia pada: https://ejurnal.stie-trianandra.ac.id/index.php/jempper/article/view/197/151

[6] D. Alfiansyah, "Analisa Kepekaan Masyarakat Terhadap Risiko Cybercrime Pada Penggunaan Dan Media Sosial," no. 5.

[7] Y. Septian dan P. Febriana, "Manajemen Kesan Dalam Pembentukan Identitas Daring : Studi Kasus Pada Dea Anugrah di Media Sosial Instagram," vol. 0672, no. OIIF, hlm. 11–16, 2025.

[8] N. I. Salmiati, "Evaluasi Dan Peningkatan Keamanan Instagram Melalui Audit Sistem Informasi," Jurnal Sistem Informasi (TEKNOFILE), vol. 55, no. 4, hlm. 524–530, 2019, doi: 10.1134/s0514749219040037.

[9] F. Novita, P. Nugroho, M. F. Listanto, dan N. Amelia, "Analisis Kebocoran Data Pribadi Dalam Media Sosial," Jurnal Ilmu Ekonomi, Manajemen dan Keuangan, vol. 1, no. 2, hlm. 58–65, 2024.

[10] A. A. Iwana, R. B. Huwae, dan A. H. Jatmika, "Threat Modeling Menggunakan Pendekatan Stride Dan Dread Untuk Mengetahui Risiko Dan Mitigasi Keamanan Pada Sistem Layanan Pendidikan," JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), vol. 6, no. 1, hlm. 9–20, 2021, doi: 10.32528/justindo.v6i1.3944.

[11] Gina Cahya Utami, Aden Bahtiar Supramaji, dan Khairunnisak Nur Isnaini, "Penilaian Risiko Keamanan Informasi pada Website dengan Metode DREAD dan ISO 27005:2018," JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), vol. 8, no. 1, hlm. 47–56, 2023, doi: 10.32528/justindo.v8i1.219.

[12] A. C. Laksono dan Y. Prayudi, "Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik," JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), vol. 6, no. 1, hlm. 9–20, 2021, doi: 10.32528/justindo.v6i1.3944.

[13] H. Sulaeman, H. P. Utomo, dan A. I. Suryana, "Penilaian Risiko Keamanan Informasi Pada Sistem Informasi

Akademik (Siakad) Dengan Menggunakan Framework Nist-Sp 800 30," Naratif : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika, vol. 5, no. 2, hlm. 171–185, 2023, doi: 10.53580/naratif.v5i2.254.

[14] M. Hendayun, H. P. Utomo, dan D. P. Nababan, "Pengujian dan Penilaian Kerentanan E-Learning Universitas Langlangbuana Menggunakan Metode STRIDE dan DREAD," Jurnal Info Secure, vol. 2, no. 2, hlm. 2–6, 2021, [Daring]. Tersedia pada: https://journal.if-unla.web.id/index.php/infosecure/article/view/4

[15] T. Agustin, "Analisis Keamanan Sistem Informasi Terhadap Data Pribadi di Media Sosial," 2020, [Daring]. Tersedia pada: https://www.academia.edu/44882254/Analisis_Keamanan_Sistem_Informasi_Terhadap_Data_Pribadi_di_Media_sosial

[16] M. K. Faridi, "Pemodelan Ancaman pada Sistem E-Health Menggunakan Metode OWASP dan Metode DREAD," 2021, [Daring]. Tersedia pada: https://dspace.uii.ac.id/bitstream/handle/123456789/33162/17917115 Muhammad Khairul Faridi.pdf?sequence=1&isAllowed=y

[17] W. Prihatiningsih, "Motif Penggunaan Media Sosial Instagram Di Kalangan Remaja," Communication, vol. 8, no. 1, hlm. 51, 2017, doi: 10.36080/comm.v8i1.651.