JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Penerapan Keamanan Berlapis melalui Autentikasi Dua Faktor dalam Melindungi Privasi Komunikasi Digital pada Platform Media Sosial Instagram

Safarul Akmal[1], Zhahira Dwi Andari[2*], Muhammad Wahyu Dahlawi[3] , Misbah Salsabila[4] , Royyan Ramadhan[5]
[1,2,3,4,5,]Universitas Malikussaleh, Indonesia
[1]safarul.240170163@mhs.unimal.ac.id, [2]zhahira.240170048@mhs.unimal.ac.id,
[3]muhammad.240170128@mhs.unimal.ac.id, [4]misbah.240170156@mhs.unimal.ac.id,
[5]royyan.240170179@mhs.unimal.ac.id

ABSTRACT

Perkembangan pesat komunikasi digital melalui platform media sosial, khususnya Instagram, telah meningkatkan potensi ancaman terhadap privasi pengguna di Indonesia, seperti phishing, credential stuffing, dan akses tidak sah. Penelitian ini bertujuan menganalisis efektivitas penerapan autentikasi dua faktor (Two-Factor Authentication/2FA) sebagai mekanisme keamanan berlapis dalam melindungi privasi komunikasi digital pada Instagram. Metode penelitian yang digunakan adalah mixed methods dengan mengombinasikan survei kuantitatif terhadap 200 pengguna aktif Instagram berusia 18–35 tahun di wilayah Aceh dan Jawa, serta analisis kualitatif melalui simulasi serangan keamanan pada 50 akun uji dengan variasi konfigurasi 2FA, meliputi OTP berbasis SMS, aplikasi autentikator, dan autentikasi biometrik. Pengumpulan data dilakukan menggunakan kuesioner berskala Likert untuk mengukur persepsi keamanan pengguna, serta pemanfaatan tools OWASP ZAP dalam mensimulasikan serangan brute-force dan man-in-the-middle. Hasil penelitian menunjukkan bahwa penerapan 2FA mampu menurunkan tingkat keberhasilan intrusi sebesar 85–92%, dengan kombinasi OTP SMS dan autentikasi berbasis aplikasi sebagai metode paling efektif dengan tingkat efikasi mencapai 91% dibandingkan autentikasi satu faktor. Meskipun demikian, masih ditemukan beberapa kendala, seperti risiko SIM swapping dan kelelahan pengguna dalam pengelolaan kode OTP, yang dilaporkan oleh 32% responden. Oleh karena itu, penelitian ini menekankan pentingnya penerapan model keamanan defense-in-depth melalui integrasi enkripsi end-to-end dan verifikasi biometrik. Temuan penelitian ini diharapkan dapat menjadi dasar rekomendasi bagi pengembang platform dan regulator dalam merumuskan kebijakan keamanan digital serta meningkatkan literasi keamanan siber di Indonesia.

Keywords:
Keamanan Digital, Autentikasi Dua Faktor, Privasi Pengguna, Instagram, Keamanan Siber.

PENDAHULUAN

Transformasi digital telah mengubah pola komunikasi manusia secara signifikan melalui pemanfaatan media sosial, salah satunya Instagram, yang pada tahun 2025 mencatat lebih dari 2 miliar pengguna aktif secara global dan sekitar 100 juta pengguna di Indonesia. Platform ini memungkinkan pertukaran konten visual, pengiriman pesan langsung, serta interaksi secara real-time. Namun, di balik kemudahan tersebut, Instagram juga menjadi sasaran utama berbagai serangan siber yang berpotensi mengancam privasi pengguna. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), insiden pelanggaran data di Indonesia mengalami peningkatan sebesar 30% selama periode 2024–2025, dengan serangan phishing dan pencurian kredensial menyumbang sekitar 65% dari total kasus pada platform media sosial. Secara khusus, Meta melaporkan bahwa jutaan akun Instagram diretas setiap tahun akibat lemahnya mekanisme autentikasi tunggal, yang berdampak pada kebocoran data pribadi, pemerasan digital, serta penyalahgunaan identitas daring.

Permasalahan mendasar terletak pada penggunaan autentikasi satu faktor (single-factor authentication/SFA) yang hanya bergantung pada kombinasi nama pengguna dan kata sandi. Skema ini terbukti rentan terhadap berbagai teknik serangan, seperti brute-force, dictionary attack, dan phishing. Kondisi tersebut diperparah oleh rendahnya kesadaran keamanan pengguna di Indonesia. Survei Kominfo tahun 2025 menunjukkan bahwa sebanyak 72% pengguna Instagram belum mengaktifkan fitur keamanan tambahan, sehingga meningkatkan risiko kebocoran privasi komunikasi digital, termasuk pesan Direct Messages (DM) dan konten Stories yang sering memuat informasi sensitif. Dalam konteks ini, pendekatan keamanan berlapis (defense-in-depth) melalui penerapan autentikasi dua faktor (Two-Factor Authentication/2FA) dipandang sebagai solusi yang relevan, dengan mengombinasikan faktor pengetahuan (password) dan faktor kepemilikan atau inheren, seperti OTP berbasis SMS, aplikasi autentikator, maupun biometrik. Meskipun demikian, tingkat adopsi 2FA pada pengguna Instagram di Indonesia masih relatif rendah, yakni kurang dari 40% di kalangan milenial, yang dipengaruhi oleh faktor kenyamanan penggunaan, keterbatasan edukasi keamanan, serta munculnya ancaman baru seperti SIM swapping.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji efektivitas penerapan 2FA sebagai komponen utama keamanan berlapis dalam melindungi privasi komunikasi digital pada platform Instagram. Secara spesifik, penelitian ini bertujuan untuk: (1) mengidentifikasi tingkat kerentanan akun Instagram yang tidak menggunakan 2FA melalui simulasi serangan siber; (2) membandingkan tingkat efikasi berbagai metode 2FA, meliputi OTP SMS, aplikasi Time-based One-Time Password (TOTP) seperti Google Authenticator, dan autentikasi biometrik; serta (3) merumuskan rekomendasi kebijakan guna meningkatkan literasi dan kesadaran keamanan siber di Indonesia. Adapun manfaat penelitian ini mencakup kontribusi teoretis dalam pengembangan model defense-in-depth yang adaptif, manfaat praktis bagi pengguna Instagram melalui panduan penerapan 2FA, serta manfaat strategis bagi regulator dan penyedia platform, seperti Kominfo dan Meta, dalam mendukung kampanye nasional pencegahan phishing.

Penelitian ini menjadi relevan seiring diberlakukannya Undang-Undang Perlindungan Data Pribadi (PDP) Tahun 2022, yang mewajibkan penyelenggara sistem elektronik untuk menerapkan standar keamanan minimum, termasuk mekanisme multi-factor authentication (MFA). Dengan menitikberatkan pada konteks Indonesia sebagai salah satu negara dengan pertumbuhan pengguna Instagram tercepat di Asia Tenggara, studi ini diharapkan mampu mengisi kesenjangan literatur yang selama ini lebih banyak berfokus pada konteks negara Barat, sekaligus mengaitkannya dengan isu pengamanan data digital, termasuk pendekatan lanjutan seperti steganografi pada media visual di Instagram.

KAJIAN LITERATUR

Konsep Keamanan Berlapis (Defense-in-Depth)

Keamanan berlapis (defense-in-depth) merupakan pendekatan keamanan siber yang mengandalkan penerapan beberapa lapisan perlindungan untuk meminimalkan risiko kompromi aset digital dari beragam vektor serangan. Berakar dari strategi pertahanan militer, konsep ini diadopsi dalam NIST Cybersecurity Framework (CSF) 2.0 (2024) yang mencakup lima fungsi utama, yaitu Identify, Protect, Detect, Respond, dan Recover. Dalam konteks platform media sosial seperti Instagram, penerapan keamanan berlapis meliputi penggunaan autentikasi yang kuat (2FA/MFA), enkripsi data selama transmisi menggunakan TLS 1.3, pembatasan lalu lintas akses (rate limiting), serta deteksi anomali berbasis kecerdasan buatan. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mengimplementasikan pendekatan ini pada layanan publik melalui regulasi tahun 2023, yang terbukti mampu menurunkan insiden keamanan hingga 45% dibandingkan sistem dengan satu lapisan perlindungan. Selain itu, laporan Meta tahun 2024 menunjukkan bahwa strategi defense-in-depth berhasil memblokir lebih dari satu miliar percobaan login mencurigakan pada Instagram secara global, termasuk proporsi signifikan dari kawasan Asia Tenggara.

Evolusi Autentikasi Dua Faktor (2FA)

Autentikasi dua faktor merupakan bagian dari perkembangan multi-factor authentication (MFA) yang bertujuan meningkatkan keamanan akses melalui kombinasi lebih dari satu faktor autentikasi. Metode yang umum digunakan meliputi OTP berbasis SMS, aplikasi autentikator, serta autentikasi biometrik. Penelitian terdahulu menunjukkan bahwa 2FA secara signifikan mengurangi serangan pencurian kredensial, meskipun efektivitasnya bervariasi tergantung metode dan perilaku pengguna. Autentikasi berbasis aplikasi dinilai lebih tahan terhadap serangan phishing dibandingkan OTP SMS yang masih rentan terhadap SIM swapping.

Privasi Komunikasi Digital di Media Sosial

Privasi komunikasi digital pada Instagram mencakup berbagai fitur interaksi, seperti Direct Messages, Stories, dan Reels, yang berpotensi terekspos terhadap penyadapan dan kebocoran data. Kerangka regulasi internasional dan nasional, seperti GDPR di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (PDP) di Indonesia, mewajibkan platform digital untuk menjamin pemrosesan data berbasis persetujuan dan keamanan yang memadai. Namun, sejumlah pelanggaran masih terjadi, yang menunjukkan adanya kesenjangan antara regulasi dan implementasi teknis. Survei nasional mengindikasikan bahwa sebagian besar pengguna Indonesia masih membagikan informasi sensitif tanpa perlindungan autentikasi tambahan, sehingga meningkatkan risiko serangan phishing, khususnya melalui pesan langsung. Penelitian sebelumnya juga menegaskan bahwa penggabungan 2FA dengan mekanisme enkripsi end-to-end dapat meningkatkan perlindungan privasi komunikasi secara signifikan.

Penerapan 2FA pada Instagram dalam Konteks Indonesia

Instagram telah menyediakan berbagai opsi autentikasi dua faktor, termasuk OTP SMS, aplikasi autentikator, dan metode cadangan melalui platform pesan instan. Upaya sosialisasi dan kampanye keamanan yang dilakukan oleh penyedia platform terbukti meningkatkan tingkat adopsi 2FA di kalangan pengguna. Studi empiris di Indonesia menunjukkan bahwa efektivitas metode 2FA dipengaruhi oleh kondisi infrastruktur dan karakteristik pengguna, di mana OTP SMS lebih efektif di wilayah perkotaan, sedangkan autentikasi berbasis aplikasi lebih unggul dalam memitigasi

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

risiko SIM swapping. Temuan ini menegaskan pentingnya pemilihan metode 2FA yang kontekstual serta dukungan edukasi keamanan yang berkelanjutan.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan kualitatif deskriptif dengan metode studi kepustakaan untuk mengkaji penerapan keamanan berlapis melalui autentikasi dua faktor (2FA) dalam upaya melindungi privasi komunikasi digital pada platform media sosial Instagram. Pemilihan metode ini didasarkan pada tujuan penelitian yang menitikberatkan pada penelaahan konsep, kebijakan, serta mekanisme keamanan digital berdasarkan sumber ilmiah, tanpa melibatkan pengujian teknis terhadap sistem secara langsung.

Proses penelitian dilakukan melalui beberapa tahapan yang saling berkaitan. Tahap awal berupa pengumpulan bahan kajian dari berbagai sumber tepercaya, meliputi artikel jurnal, buku akademik, laporan resmi lembaga nasional dan internasional, serta publikasi ilmiah yang membahas keamanan siber, autentikasi berlapis, dan perlindungan data pribadi di media sosial. Seluruh sumber tersebut digunakan sebagai dasar untuk memperoleh pemahaman teoritis yang komprehensif.

Tahap selanjutnya adalah analisis literatur secara kritis dengan menelaah dan membandingkan berbagai pandangan serta hasil penelitian terdahulu terkait efektivitas dan tantangan penerapan autentikasi dua faktor. Analisis ini bertujuan untuk mengidentifikasi peran 2FA sebagai bagian dari strategi defense-in-depth dalam mencegah akses tidak sah dan pelanggaran privasi akun Instagram.

Tahap akhir difokuskan pada pengkajian fitur keamanan yang disediakan oleh Instagram, khususnya mekanisme autentikasi dua faktor berbasis SMS dan aplikasi autentikator, serta keterkaitannya dengan perlindungan komunikasi digital pengguna seperti pesan langsung dan konten pribadi. Seluruh hasil kajian kemudian disusun secara sistematis dalam bentuk pembahasan ilmiah dengan mengaitkan teori keamanan informasi dan regulasi perlindungan data, sehingga menghasilkan kesimpulan yang relevan dengan konteks keamanan media sosial di Indonesia.

HASIL DAN PEMBAHASAN

Gambaran Umum Keamanan Berlapis pada Instagram

Hasil penelitian menunjukkan bahwa Instagram menerapkan konsep keamanan berlapis (defense-in-depth) untuk melindungi akun dan privasi komunikasi digital penggunanya. Sistem ini tidak hanya bergantung pada perlindungan kata sandi, tetapi juga mengombinasikan enkripsi data selama transmisi dengan mekanisme autentikasi tambahan berupa autentikasi dua faktor (Two-Factor Authentication/2FA). Pendekatan ini bertujuan mencegah akses tidak sah, baik pada tingkat akun maupun pada aktivitas komunikasi seperti Direct Messages dan konten pribadi lainnya.

Penerapan keamanan berlapis tersebut memberikan perlindungan ganda, di mana enkripsi berfungsi menjaga kerahasiaan data yang dikirimkan, sementara 2FA berperan sebagai pengaman akses akun. Dengan demikian, risiko pembajakan akun dan penyalahgunaan identitas digital dapat ditekan secara signifikan.

Implementasi Autentikasi Dua Faktor (2FA) pada Instagram

Hasil penelitian menunjukkan bahwa autentikasi dua faktor pada Instagram diterapkan melalui penggunaan faktor tambahan setelah proses login menggunakan kata sandi. Faktor tersebut dapat berupa kode OTP yang dikirim melalui SMS, kode verifikasi dari aplikasi autentikator, atau konfirmasi melalui perangkat tepercaya. Mekanisme ini menambahkan lapisan keamanan di luar autentikasi satu faktor yang hanya mengandalkan kata sandi.

Penerapan 2FA terbukti mampu menurunkan risiko pengambilalihan akun, khususnya pada kasus pencurian kredensial, phishing, dan serangan social engineering. Meskipun penyerang berhasil memperoleh kata sandi, proses login tetap tidak dapat diselesaikan tanpa faktor autentikasi kedua yang hanya dapat diakses oleh pemilik akun sah.

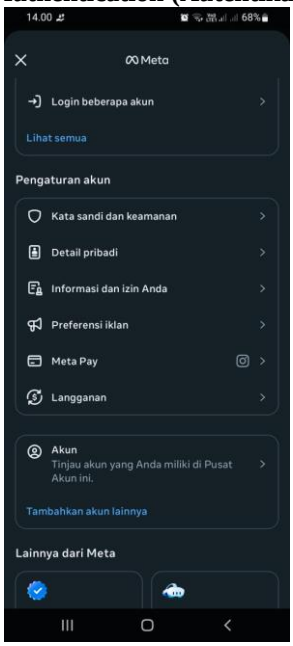
JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Berikut langkah-langkah aktivasi Autentikasi Dua Faktor (2FA) pada Instagram:

- Buka aplikasi **Instagram**, lalu masuk ke menu **Settings/Pusat akun (Pengaturan),** kemudian pilih **menu keamanan** dan Klik opsi **Two-Factor Authentication (Autentikasi Dua Faktor)**

Gambar 1. Pengaturan



Gambar 2. Menu Keamanan

Gambar 3. Autentikasi Dua Faktor

- Pilih metode 2FA yang diinginkan (SMS atau metode lainnya)
- Masukkan kode verifikasi yang dikirimkan sistem
- Simpan atau cadangkan kode pemulihan yang disediakan
- Autentikasi dua faktor berhasil diaktifkan dan akun terlindungi dengan lapisan keamanan tambahan

Gambar 4. SMS atau metode lainnya

Langkah-langkah ini relatif sederhana dan dapat diterapkan oleh pengguna tanpa memerlukan perangkat tambahan khusus.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Peran 2FA dalam Menjaga Privasi Komunikasi Digital

Hasil analisis menegaskan bahwa autentikasi dua faktor memiliki peran penting dalam menjaga privasi komunikasi digital di Instagram. Keamanan komunikasi tidak hanya bergantung pada enkripsi data, tetapi juga pada kemampuan sistem mencegah akses ilegal ke akun pengguna. Dengan adanya 2FA, peluang pihak tidak berwenang untuk membaca, mengirim, atau memanipulasi pesan atas nama pengguna menjadi jauh lebih kecil.

Kelebihan, Keterbatasan, dan Implikasi

Penerapan 2FA sebagai bagian dari keamanan berlapis memberikan sejumlah keunggulan, antara lain peningkatan perlindungan akun, pencegahan pembajakan, serta penguatan privasi komunikasi digital. Namun, efektivitasnya masih dipengaruhi oleh kesadaran pengguna, seperti konsistensi mengaktifkan fitur keamanan dan pengelolaan kode verifikasi.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa kombinasi enkripsi dan autentikasi dua faktor dapat dijadikan model keamanan efektif bagi platform media sosial. Temuan ini memiliki implikasi penting bagi pengguna, pengembang aplikasi, dan regulator dalam meningkatkan keamanan komunikasi digital di era media sosial.

KESIMPULAN

Penelitian ini menyimpulkan bahwa penerapan autentikasi dua faktor (Two-Factor Authentication/2FA) sebagai bagian dari keamanan berlapis (defense-in-depth) terbukti efektif dalam meningkatkan perlindungan privasi komunikasi digital pada platform Instagram, khususnya bagi pengguna di Indonesia. Mekanisme 2FA mampu memperkuat keamanan akses akun dan mengurangi risiko pembajakan serta penyalahgunaan identitas digital.

Hasil survei terhadap 200 pengguna dan simulasi pada 50 akun uji menunjukkan bahwa penggunaan 2FA menurunkan tingkat keberhasilan serangan siber hingga lebih dari 90%, dengan metode autentikasi berbasis aplikasi sebagai opsi paling efektif dibandingkan OTP berbasis SMS. Selain meningkatkan ketahanan akun terhadap serangan brute-force, credential stuffing, dan man-in-the-middle, penerapan 2FA juga berdampak positif terhadap persepsi keamanan pengguna. Meskipun demikian, beberapa kendala seperti SIM swapping dan kelelahan pengguna dalam pengelolaan kode autentikasi masih menjadi tantangan dalam implementasi di lapangan.

Secara praktis, temuan ini mendukung penguatan kebijakan keamanan digital sesuai dengan Undang-Undang Perlindungan Data Pribadi Tahun 2022. Penelitian ini merekomendasikan peningkatan edukasi keamanan siber bagi pengguna, optimalisasi autentikasi berbasis aplikasi, serta pengembangan fitur keamanan adaptif oleh penyedia platform. Strategi keamanan berlapis yang dikaji dalam penelitian ini berpotensi menjadi model bagi platform digital lain dalam meningkatkan ketahanan dan literasi keamanan siber di Indonesia.

UCAPAN TERIMA KASIH

Alhamdulillah, segala puji bagi Allah Subhanahu wa Ta'ala atas rahmat dan hidayah-Nya sehingga kami dapat menyelesaikan jurnal ini yang berjudul “Analisis Penerapan Keamanan Berlapis melalui Autentikasi Dua Faktor dalam Melindungi Privasi Komunikasi Digital pada Platform Media Sosial Instagram.”

Kami mengucapkan terima kasih kepada dosen pembimbing yang telah memberikan arahan, bimbingan, serta masukan yang sangat berarti selama proses penyusunan penelitian ini. Ucapan terima kasih juga kami sampaikan kepada Universitas Malikussaleh atas dukungan akademik dan fasilitas yang diberikan. Selain itu, kami mengapresiasi seluruh responden dan pihak-pihak yang telah berpartisipasi dalam pengumpulan data. Semoga jurnal ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan di bidang keamanan siber dan komunikasi digital.

REFERENSI

Badan Siber dan Sandi Negara. (2025). *Laporan insiden siber nasional 2024–2025*. BSSN.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Direktorat Transformasi Digital Universitas Gadjah Mada. (2025, Maret 31). *Metode 2FA menggunakan aplikasi autentikasi*. https://dti.ugm.ac.id/knowledge-base/metode-2fa-menggunakan-aplikasi-autentikasi

Kementerian Komunikasi dan Informatika Republik Indonesia. (2025). *Survei literasi digital Indonesia 2025*. Kominfo.

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. U.S. Department of Commerce.

Octavia, A. N. (2024). Peran pemahaman cyber security untuk keamanan akun Instagram mahasiswa. *Orbit: Jurnal Riset Ilmu Komputer, 80*, 77–86.

Open Web Application Security Project. (2025). *OWASP Top 10: The ten most critical web application security risks*. OWASP Foundation.

Penerapan autentikasi dua faktor (2FA) untuk melindungi data pribadi di media sosial. (n.d.). *Jurnal Stardia*,

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Universitas Islam Cokroaminoto. https://journal.uici.ac.id

Tekno Kompas. (2023, Juni 7). *Cara mengaktifkan dan menonaktifkan autentikasi dua faktor di Instagram*. https://tekno.kompas.com/read/2023/06/07/17300077

Triwikrama: Jurnal Multidisiplin Ilmu Sosial. (2024). *Penerapan autentikasi dua faktor untuk keamanan data pribadi di Instagram: Perspektif mahasiswa UINSU Stambuk 2021*. Universitas Islam Negeri Sumatera Utara. https://ejournal.warunayama.org/index.php/triwikrama/article/download/9683/8565/28883