ANALISIS PENGGUNAAN ENKRIPSI END-TO-END PADA APLIKASI INSTAGRAM MESSENGGER

Andreas Avelino Lama[1], Mario Gonsaga Reymon Efi[2]
andreasavelinolama@gmail.com[1], mariogonsagaraymonefi@gmail.com[2]
Universitas Timor

ABSTRAK

Peningkatan penggunaan aplikasi media sosial seperti Instagram di Indonesia telah menjadi fenomena yang signifikan di era digital saat ini. Aplikasi ini tidak hanya digunakan untuk berbagi konten pribadi, tetapi juga untuk komunikasi antar individu dan kolaborasi dalam berbagai proyek. Penelitian ini bertujuan untuk menganalisis keamanan aplikasi Instagram dengan menerapkan teknik enkripsi end-to-end, yang menjadi salah satu fitur unggulannya, memastikan bahwa hanya pengirim dan penerima pesan yang memiliki akses untuk membacanya. Metodologi yang digunakan dalam penelitian ini mencakup studi literatur untuk mengumpulkan informasi dan materi yang relevan. Penelitian ini menyoroti pentingnya enkripsi end-to-end dalam menjaga privasi pengguna serta keamanan data saat berinteraksi melalui platform digital. Hasil penelitian menunjukkan bahwa lapisan keamanan tambahan ini efektif dalam melindungi privasi pengguna dari serangan siber dan penyalahgunaan data oleh pihak ketiga.
Kata Kunci: Instagram, Keamanan Data Dan Privacy Chat, Enkripsi End To End.

ABSTRACT

The increasing use of social media applications such as Instagram in Indonesia has become a significant phenomenon in today's digital era. This application is not only used to share personal content, but also for communication between individuals and collaboration on various projects. This study aims to analyze the security of the Instagram application by implementing end-to-end encryption techniques, which are one of its superior features, ensuring that only the sender and recipient of the message have access to read it. The methodology used in this study includes a literature study to collect relevant information and materials. This study highlights the importance of end-to-end encryption in maintaining user privacy and data security when interacting through digital platforms. The results of the study indicate that this additional layer of security is effective in protecting user privacy from cyber attacks and data misuse by third parties.
Keywords: *Instagram, Data Security And Chat Privacy, End To End Encryption.*

PENDAHULUAN

Peningkatan penggunaan aplikasi media sosial seperti Instagram, Facebook, dan TikTok di Indonesia telah menjadi fenomena yang sangat mencolok dalam era digital saat ini. Aplikasi-aplikasi ini tidak hanya berfungsi untuk berbagi konten pribadi, tetapi juga untuk kolaborasi tim dan kegiatan bisnis. Hal ini didorong oleh kemudahan akses, kecepatan interaksi, serta fitur tambahan seperti siaran langsung, pengiriman pesan, dan berbagi cerita. Dengan meningkatnya mobilitas dan konektivitas internet, Posisi aplikasi media sosial semakin meningkat sebagai platform utama untuk komunikasi secara langsung, memungkinkan pengguna untuk terus menerima pesan dari rekan dan keluarga kapan saja[1]

Instagram merupakan salah satu aplikasi yang sangat populer dan terus menjadi pilihan utama bagi banyak pengguna di seluruh dunia sebagai platform untuk berbagi gambar dan video. Beberapa faktor yang membuat Instagram disukai adalah antarmukanya yang intuitif, kemudahan dalam terhubung dengan pengguna lain, serta beragam fitur menarik yang ditawarkan, termasuk alat pengeditan foto dan filter yang mudah digunakan.

Namun, dengan meningkatnya jumlah pengguna Instagram, masalah keamanan data menjadi bagian yang sangat penting dalam kehidupan sehari-hari[2]. Banyak informasi

pribadi dan sensitif yang dibagikan di platform ini, seperti foto, lokasi, dan data kontak. Ancaman yang ada meliputi serangan siber, penggunaan informasi tanpa izin, dan penyalahgunaan data oleh pihak ketiga.

Sebagai salah satu aplikasi yang sangat populer, Instagram perlu meningkatkan aspek keamanannya guna mencegah tindakan kejahatan siber yang tidak diinginkan. Dengan semakin banyaknya pengguna, risiko kebocoran data pun meningkat[3]. Platform ini juga sering digunakan untuk menyebarkan informasi palsu atau melakukan penipuan, sehingga penanganan khusus menjadi semakin mendesak. Penerapan teknik enkripsi end-to-end pada fitur pesan langsung di Instagram merupakan langkah penting untuk melindungi privasi penggunanya.

Perlindungan data harus menjadi perhatian utama, terutama karena data pribadi adalah aset berharga yang mencakup informasi sensitif, finansial, dan rahasia bisnis. Upaya perlindungan ini tidak hanya mencakup pencegahan serangan siber, tetapi juga memastikan bahwa akses data hanya diberikan kepada pihak yang berwenang sesuai dengan peraturan yang berlaku. Enkripsi end-to-end terbukti efektif dalam menjaga keamanan data, dengan mengenkripsi informasi pada perangkat pengirim dan hanya dapat dibaca oleh penerima yang sah, sehingga pesan tetap aman dari pengintaian dan serangan digital[4].

METODE PENELITIAN

Penelitian ini menggunakan metode analisis dengan pendekatan studi literatur yang bertujuan untuk mengevaluasi keamanan pesan di Instagram melalui penerapan enkripsi end-to-end, serta mengembangkan teknologi tersebut untuk mencegah pencurian data di aplikasi ini. Dalam pengumpulan data dan bahan penelitian, penulis melakukan pencarian referensi teori yang relevan dengan isu yang dihadapi. Referensi ini diperoleh dari buku, jurnal, artikel, laporan penelitian, dan sumber daring. Hasil dari studi literatur ini adalah terkumpulnya referensi yang mendukung perumusan masalah. Tujuan dari langkah ini adalah untuk memperkuat permasalahan yang ada serta menyediakan dasar teori dalam pelaksanaan studi, serta merancang solusi untuk mengatasi masalah yang diteliti.

HASIL DAN PEMBAHASAN

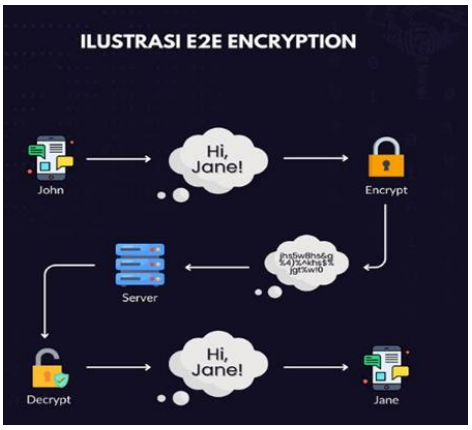
Skema Pengamanan Pesan dengan Teknik Enkripsi End-to-end pada Instagram

Instagram telah secara resmi memperkenalkan fitur keamanan menggunakan teknik enkripsi end-to-end. Fitur ini menjamin bahwa setiap pesan yang dikirim melalui Direct Message (DM) akan dienkripsi secara aman dan hanya dapat diakses oleh pengirim dan penerima. Dengan metode ini, semua pesan, termasuk gambar, video, dan pesan suara, tidak dapat disadap oleh pihak ketiga[5].

Enkripsi end-to-end merupakan sistem di mana enkripsi terjadi saat pesan dikirim dan hanya dapat didekripsi ketika pesan tiba di penerima. Bahkan Instagram pun akan kesulitan untuk menyerahkan data pengguna kepada pihak berwenang, karena sistem enkripsi dirancang agar tidak bisa dibongkar, bahkan oleh pembuatnya.

Dengan adanya sistem ini, pengguna Instagram tidak perlu khawatir tentang privasi mereka. Pihak pemerintah atau kepolisian akan menghadapi kesulitan dalam memantau percakapan pengguna, karena semua pesan dan data yang dikirimkan adalah kumpulan kode terenkripsi yang tidak dapat dipahami. Kode ini hanya bisa dibaca pada perangkat penerima, sehingga pihak ketiga tidak dapat menyadap percakapan di Instagram.

Sebagai contoh, jika seorang pengguna mengirim pesan "Apa Kabar?", pesan itu akan secara otomatis dienkripsi menjadi format seperti "9XB80FFAH", dan kemudian dapat dideskripsikan kembali menjadi "Apa Kabar?". Dengan menerapkan teknik enkripsi end-to-end, privasi pengguna Instagram semakin terjamin.



Gambar 1: Ilustrasi Pengiriman Pesan

Namun, perlu dicatat bahwa fitur enkripsi end-to-end ini juga bisa disalahgunakan oleh individu tertentu untuk melakukan kejahatan, seperti teroris atau penjahat lainnya. Seorang praktisi keamanan internet di Indonesia menyatakan bahwa fitur ini sangat menguntungkan bagi penjahat dalam merencanakan dan melaksanakan tindakan mereka.

Enkripsi end-to-end selalu aktif di Instagram, dan tidak ada cara untuk menonaktifkannya. Semua pengguna yang terlibat dalam percakapan harus menggunakan versi terbaru dari aplikasi untuk memanfaatkan fitur ini.

Cara Kerja Enkripsi End to End pada Instagram Massengger

Enkripsi end-to-end pada Instagram memastikan bahwa hanya pengguna dan lawan bicara yang dapat mengakses isi pesan yang dikirim, tanpa pihak lain, termasuk Instagram sendiri, yang dapat membaca pesan tersebut. Setiap pesan dilindungi oleh kunci khusus yang hanya dimiliki oleh pengirim dan penerima, memungkinkan mereka untuk membuka dan membaca pesan dengan aman.

Proses enkripsi dilakukan sebelum pesan dikirim ke server, yang berfungsi sebagai infrastruktur komunikasi untuk menghubungkan pengguna. Untuk meningkatkan keamanan, setiap pesan dilengkapi dengan kunci unik. Misalnya, pesan dapat dilindungi menggunakan algoritma enkripsi tertentu yang memastikan bahwa setiap pesan memiliki kunci yang berbeda, sehingga kunci yang digunakan untuk mengenkripsi pesan tidak dapat diprediksi.

Sistem enkripsi end-to-end ini berfungsi secara otomatis tanpa memerlukan pengaturan tambahan dari pengguna atau penyesuaian untuk mengamankan percakapan tertentu. Setiap obrolan dilengkapi dengan kode keamanan yang memastikan bahwa pesan dan panggilan yang dikirimkan telah terenkripsi secara end-to-end. Dengan demikian, fitur ini membungkus data pengguna saat dikirim dan membukanya saat diterima.

Gambar 2: Konsep Dasar Enkripsi End to end Pada Intagram

Gambar yang menyertai analisis ini menggambarkan bahwa fitur enkripsi end-to-end menciptakan jalur komunikasi yang aman, meskipun jalur tersebut hanyalah representasi yang menggambarkan pembungkus data dalam komunikasi antar pengguna. Instagram mengadopsi protokol yang dirancang untuk mencegah serangan dari pihak ketiga yang ingin mencuri informasi, baik berupa data pesan maupun informasi panggilan. Bahkan jika kunci enkripsi suatu pengguna dicuri oleh penyerang, mereka tetap tidak dapat mendekripsi pesan yang telah dikirim[6].

Metode Enkripsi End to End

1. Tipe Kunci Publik

a. Identity Key Pair

Pasangan kunci jangka panjang yang digunakan untuk mengidentifikasi pengguna. Kunci ini bersifat permanen dan digunakan dalam proses pertukaran kunci.

b. Signed Pre Key

Pasangan kunci jangka menengah yang dihasilkan saat instalasi aplikasi. Kunci ini dapat diperbarui secara berkala untuk meningkatkan keamanan.

c. One-Time Pre Keys

Barisan pasangan kunci yang digunakan hanya sekali. Kunci ini dihasilkan saat instalasi dan akan digunakan saat dibutuhkan untuk meningkatkan keamanan komunikasi.

Instagram menggunakan algoritma Curve25519 untuk menghasilkan kunci publik dan privat. Curve25519 adalah kurva eliptik yang menawarkan keamanan yang baik dan kecepatan komputasi yang tinggi, menjadikannya pilihan yang baik untuk aplikasi yang memerlukan enkripsi.

2. Tipe Kunci Sesi

a. Root Key

Kunci ini digunakan untuk menghasilkan Chain Keys dan memiliki panjang 32 Byte.

b. Chain Key

Kunci ini juga memiliki panjang 32 Byte dan digunakan untuk menghasilkan Message Keys.

c. Message Key

Kunci ini memiliki panjang 80 Byte, di mana 32 Byte digunakan sebagai kunci untuk algoritma AES-256 yang digunakan untuk mengenkripsi isi pesan.

3. Registrasi Pengguna (Client Registration)

Saat pengguna baru mendaftar, mereka mengirimkan Public Identity Key, Signed Pre Key (beserta tanda tangannya), dan sejumlah public One-Time Pre Key ke server Instagram. Server menyimpan kunci publik ini bersama dengan identitas pengguna.

4. Inisialisasi Pembentukan Sesi

Untuk memulai komunikasi yang aman, pengguna harus membentuk sesi. Proses ini dilakukan sebagai berikut:

a. Inisiator: Pengguna yang ingin memulai komunikasi meminta public Identity Key, public Signed Pre Key, dan satu public One-Time Pre Key dari penerima.
b. Server: Mengembalikan permintaan dengan nilai public key. One-Time Pre Key yang digunakan akan dihapus dari penyimpanan server setelah dikirim.
c. Kunci Ephemeral: Inisiator membangkitkan pasangan kunci ephemeral menggunakan Curve25519.
d. Master Secret: Inisiator menghitung master secret menggunakan kunci yang diterima dan kunci yang dihasilkan.
e. Root Key dan Chain Keys: Inisiator menggunakan HKDF untuk menghasilkan Root Key dan Chain Keys dari master secret.

5. Pengaturan Sesi Penerimaan (Receiving Session Setup)

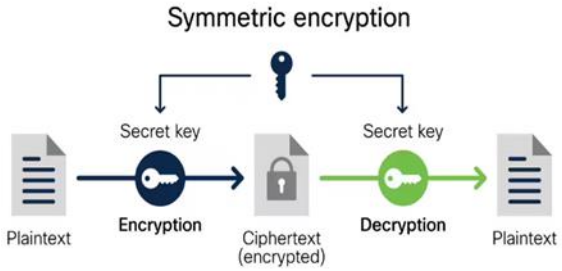
Setelah sesi dibentuk, inisiator dapat mengirim pesan ke penerima, bahkan jika penerima offline. Penerima akan menghitung master secret menggunakan kunci publik yang diterima dan kunci privat mereka.

6. Pertukaran Pesan (Exchanging Messages)

Setelah sesi terbentuk, pesan dapat dipertukarkan. Proses ini melibatkan:

a. Message Key: Dihasilkan dari Chain Key dan digunakan untuk mengenkripsi pesan dengan AES-256 dalam mode CBC.

Message Key akan selalu berbeda pada tiap paket yang kirim karena bersifat ephemeral (penggunaan secara singkat). Seperti halnya Message Key yang telah mengenkripsi pesan tidak dapat mengenkripsi ulang. Message Key diadapatkan dari Chain key pengirim/inisiator dimana akan bangkit secara berkesinambungan dan akan kembali ke suatu titik tertentu "ratchets method". Berikut adalah blok diagram proses enkripsi pesan, ditunjukkan pada gambar 3:



Gambar 3: Enkripsi end to end pada Instagram Messenger

b. Integritas Data: HMAC-SHA256 digunakan untuk memastikan integritas data pesan.

7. Konsep Grup (Grouping Message)

Instagram juga mendukung fitur grup, di mana pesan dapat dikirim ke beberapa pengguna sekaligus. Proses ini dapat dilakukan dengan metode server-side fan-out, di mana pesan dikirim ke server terlebih dahulu sebelum diteruskan ke anggota grup.

8. Call Setup

Untuk panggilan suara atau video, Instagram menggunakan protokol yang aman untuk mengenkripsi komunikasi secara real-time. Proses ini mirip dengan yang digunakan dalam pengaturan sesi dan melibatkan pembangkitan kunci acak untuk menjaga kerahasiaan data.

KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan enkripsi end-to-end pada aplikasi Instagram sangat penting untuk melindungi privasi pengguna dan keamanan data. Dengan memastikan bahwa hanya pengirim dan penerima yang dapat mengakses pesan, enkripsi ini efektif dalam mencegah intersepsi dari pihak ketiga. Meskipun fitur ini memberikan lapisan keamanan tambahan, ada potensi penyalahgunaan oleh individu tertentu, seperti penjahat. Oleh karena itu, penting bagi pengguna untuk memahami cara kerja enkripsi ini dan tetap waspada terhadap potensi risiko yang mungkin muncul.

Secara keseluruhan, penelitian ini menegaskan perlunya peningkatan keamanan data dalam aplikasi komunikasi dan mendorong pengembangan teknologi enkripsi yang lebih baik di masa mendatang. Saran untuk penelitian selanjutnya adalah mengeksplorasi solusi untuk mengatasi tantangan yang dihadapi dalam implementasi enkripsi, serta mengevaluasi dampaknya terhadap pengalaman pengguna.

DAFTAR PUSTAKA

A. Pemanfaatan, I. Dan, W. Dalam, U. Terbuka, and U. I. Kadiri, “strategi pemasaran bisnis produk dan jasa . Adanya kemajuan ilmu pengetahuan dan teknologi,” vol. 6, no. 2, pp. 210–223, 2025.

G. Urva, “Analisis Penggunaan Enkripsi End To End Pada Aplikasi Whatsapp Messengger,” J. Unitek, vol. 10, no. 1, pp. 34–45, 2017, doi: 10.52072/unitek.v10i1.69.

P. T. Hastuti, B. Fitriandra, and S. Lestari, “Kesadaran dan Perlindungan Privasi dalam Penggunaan Media Sosial,” pp. 518–523, 2024.

S. P. Lestari, H. N. Fadlan, R. Angelia Purba, and I. Gunawan, “Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp,” J. Media Inform., vol. 4, no. 1, pp. 1–8, 2022, doi: 10.55338/jumin.v4i1.423.

T. Agustin, “Analisis Keamanan Sistem Informasi Terhadap Data Pribadi di Media Sosial,” 2020, [Online]. Available: https://www.academia.edu/44882254/Analisis_Keamanan_Sistem_Informasi_Terhadap_Data_Pribadi_di_Media_sosial

T. Keamanan and D. Aplikasi, “Peran Cybersecurity Terhadap Keamanan Data Aplikasi Media,” vol. 4, no. 1, pp. 28–32, 2025.