ANALISA KEAMANAN PADA APLIKASI WHATSAPP MENGGUNAKAN ENKRIPSI END TO END

Ananda Aufa R[1], Januar Putra W[2], Muhammad Aditya[3]

[1]*Teknik Informtika/Universitas Duta Bangsa Surakarta*
[1]*220103046@mhs.udb.ac.id*

[2] *Teknik Informatika/Universitas Duta Bangsa Surakarta*
[2]*220103061@mhs.udb.ac.id*

[3] *Teknik Informatika/Universitas Duta Bangsa Surakarta*
[3]*220103065@mhs.udb.ac.id*

***Abstrak*— Penggunaan aplikasi chatting seperti WhatsApp di Indonesia telah meningkat pesat dan telah menjadi fenomena besar di era modern. Aplikasi ini digunakan untuk komunikasi pribadi, kerja tim, dan bisnis. Penelitian ini bertujuan untuk menganalisis keamanan aplikasi WhatsApp menggunakan teknik enkripsi end-to-end, yang merupakan keunggulan utamanya, yang memastikan bahwa haya orang yang mengirim dan menerima pesan yang dapat membacanya. Metodologi penelitian ini menegaskan pentingnya teknik enkripsi end-to-end dalam melindungi privasi dan keamanan data pengguna saat berkomunikasi melalui aplikasi digital. Penemuan ini juga menunjukkan bahwa lapisan keamanan tambahan ini melindungi privasi pengguna dari serangan peretas dan penyalahgunaan data oleh pihak ketiga.**
Kata kunci— WhatsApp, enkripsi end-to-end, keamanan data, privasi, aplikasi chatting.

***Abstract*— The use of chat applications such as WhatsApp in Indonesia has increased rapidly and has become a major phenomenon in the modern era. This application is used for personal communication, team collaboration, and business. This research aims to analyze the security of the WhatsApp application using end-to-end encryption techniques, which is its main advantage, ensuring that only the people who send and receive messages can read them. The research methodology involves a literature study to gather relevant data and materials. This research emphasizes the importance of end-to-end encryption techniques in protecting user privacy and data security when communicating through digital applications. The findings also show that this additional layer of security protects user privacy from hacker attacks and data misuse by third parties..**
Keywords—WhatsApp, end-to-end encryption, data security, privacy, chat application..

I. PENDAHULUAN

Peningkatan penggunaan aplikasi chatting seperti WhatsApp, Telegram, dan Signal di Indonesia telah menjadi fenomena signifikan dalam era digital. Aplikasi ini tidak hanya digunakan untuk komunikasi pribadi tetapi juga untuk kolaborasi tim dan bisnis, didorong oleh kemudahan akses, kecepatan komunikasi, serta fitur tambahan seperti panggilan suara, video call, dan berbagi file. Peningkatan mobilitas dan konektivitas internet semakin memperkuat posisi aplikasi chatting sebagai sarana utama komunikasi real-time. [1]

Salah satu aplikasi Android yang paling populer adalah WhatsApp Messenger, yang tetap menjadi favorit banyak orang di seluruh dunia sebagai aplikasi pesan instan. Beberapa alasan mengapa WhatsApp Messenger disukai adalah karena aplikasi ini ringan, mudah terhubung ke jaringan, dan tidak memerlukan ID pengguna, yang merupakan keunggulan tersendiri bagi WhatsApp Messenger.[2]

Namun, dengan meningkatnya penggunaan aplikasi WhatsApp, keamanan data menjadi sangat penting. Banyak informasi pribadi dan sensitif yang ditransmisikan melalui platform ini, termasuk informasi pribadi, lokasi, nomor telepon, dan data keuangan. Ancaman yang dihadapi mencakup serangan peretas, penggunaan data tanpa izin, dan penyalahgunaan data. [3]

WhatsApp Messenger, sebagai aplikasi pesan yang sangat populer, membutuhkan peningkatan keamanan untuk mencegah kejahatan siber yang tidak diinginkan. Seiring dengan meningkatnya penggunaan aplikasi ini, tingkat kejahatan yang memanfaatkan aplikasi pesan juga meningkat. Aplikasi pesan sering digunakan untuk bertukar informasi ilegal atau melakukan pemerasan, sehingga diperlukan penanganan khusus. Dengan menerapkan teknik enkripsi end-to-end pada WhatsApp Messenger.

Perlindungan data menjadi perhatian utama, terutama karena data merupakan aset berharga yang mencakup informasi pribadi, finansial, medis, dan rahasia bisnis. Perlindungan ini tidak hanya

melibatkan pencegahan serangan peretas tetapi juga memastikan data hanya diakses oleh pihak berwenang sesuai ketentuan yang berlaku. Enkripsi end-to-end telah menjadi solusi efektif dalam menjaga keamanan data, dengan mengenkripsi informasi pada perangkat pengirim dan hanya dapat didekripsi oleh penerima yang sah, sehingga pesan terlindungi dari serangan peretas dan mata-mata digital. [4]

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode analisis, yang bertujuan untuk menganalisis keamanan pesan WhatsApp menggunakan enkripsi end-to-end serta mengembangkan teknologi tersebut guna mencegah pencurian data melalui WhatsApp. Untuk mengumpulkan data dan bahan penelitian, penulis melakukan Studi Literatur. Studi literatur ini melibatkan pencarian referensi teori yang relevan dengan kasus atau permasalahan yang ditemukan. Referensi tersebut dapat diperoleh dari buku, jurnal, artikel, laporan penelitian, dan situs internet. Hasil dari studi literatur ini adalah terkumpulnya referensi yang relevan dengan perumusan masalah. Tujuan dari langkah ini adalah untuk memperkuat permasalahan yang ada serta menyediakan dasar teori dalam pelaksanaan studi dan desain solusi terhadap masalah yang diteliti.

III. HASIL DAN PEMBAHASAN

1. Skema Enkripsi End To end

Skema Pengamanan Pesan Dengan Teknik Enkripsi End-to-end. Teknik enkripsi end-to-end adalah suatu sistem yang menjamin bahwa pesan yang dikirim melalui aplikasi atau platform tertentu dienkripsi selama proses pengiriman, sehingga hanya dapat dibaca oleh pengirim dan penerima. Dengan demikian, pihak yang mengelola aplikasi atau platform tersebut tidak dapat mengakses pesan tersebut.

Bahkan WhatsApp sendiri tidak dapat memberikan rekaman data penggunanya kepada pihak berwenang karena sistem ini dirancang agar tidak dapat dibobol, bahkan oleh pembuatnya. Dengan sistem enkripsi end-to-end, pengguna WhatsApp tidak perlu khawatir tentang privasi mereka. Pemerintah dan kepolisian juga akan kesulitan memata-matai percakapan pengguna karena semua pesan dan data yang dikirimkan adalah kode yang telah terenkripsi dan tidak dapat dimengerti. Kode tersebut hanya dapat dibaca pada perangkat penerima, sehingga pihak ketiga tidak dapat menyadap percakapan di WhatsApp.

Sebagai contoh, jika pengirim pesan di WhatsApp mengirimkan pesan "Bagaimana Kabarmu?", pesan tersebut akan secara otomatis terenkripsi menjadi "CQGHJK980" saat dikirim. Kode ini tidak dapat dimengerti oleh pihak ketiga yang menyadapnya. Namun, sesampainya di penerima, kode tersebut akan secara otomatis didekripsi menjadi pesan aslinya "Bagaimana Kabarmu?". Dengan menggunakan teknik enkripsi end-to-end, privasi pengguna WhatsApp lebih terjamin.

Menurut pakar teknologi Onno W. Purbo, penggunaan fitur enkripsi end-to-end di WhatsApp akan menyulitkan penyidik dalam melakukan penyadapan, sehingga teknik ini penting untuk melindungi privasi seseorang. Namun, di sisi lain, fitur keamanan tingkat tinggi ini juga dapat dimanfaatkan oleh pelaku kejahatan seperti teroris dan koruptor. Seorang praktisi keamanan internet di Indonesia menyatakan bahwa fitur enkripsi end-to-end di WhatsApp sangat menguntungkan bagi penjahat dalam merencanakan dan melaksanakan kejahatan mereka.

Teknik enkripsi end-to-end adalah suatu sistem yang menjamin bahwa pesan yang dikirim melalui aplikasi atau platform tertentu dienkripsi selama proses pengiriman, sehingga hanya dapat dibaca oleh pengirim dan penerima. Dengan demikian, pihak yang mengelola aplikasi atau platform tersebut tidak dapat mengakses pesan tersebut.

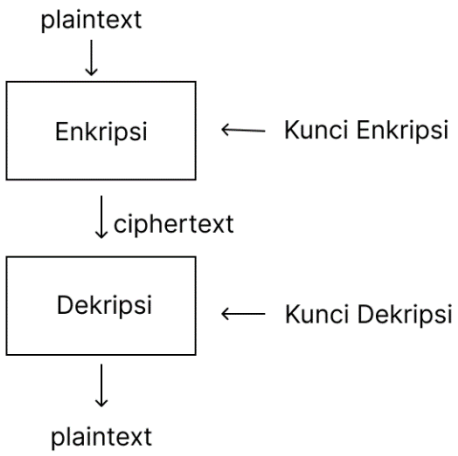
Ini karena teknik enkripsi End-to-end memiliki tingkat keamanan yang tinggi, yang membuatnya sulit untuk dibobol melalui metode kriptanalisis, bahkan oleh pihak yang mengembangkannya sendiri. Dengan demikian, teknik enkripsi End-to-end memberikan lapisan keamanan tambahan yang sangat kuat yang melindungi privasi dan keamanan data pengguna saat mereka berkomunikasi melalui aplikasi atau platform digital.

Teknik enkripsi end-to-end ini mempertahankan privasi pengguna saat

berkomunikasi melalui aplikasi pesan. Karena fitur enkripsi end-to-end dalam aplikasi pesan akan membuat penyidik lebih sulit untuk menyadapnya, penggunaan teknologi enkripsi end-to-end ini sangat penting untuk menjaga privasi individu. Namun demikian, kekuatan keamanan yang tinggi ini juga dapat dimanfaatkan oleh individu yang melakukan kejahatan, seperti teroris, koruptor, dan lainnya. Seorang ahli keamanan internet di Indonesia mengatakan bahwa fitur enkripsi end-to-end pada aplikasi chat sangat membantu para penjahat dalam merencanakan dan menjalankan berbagai macam tindakan kriminal.

2. Cara Kerja Enkripsi End To end

Dalam kriptografi, ada dua konsep utama: enkripsi dan dekripsi. Enkripsi adalah suatu proses dimana informasi atau data yang dikirim diubah menjadi bentuk yang tidak dapat dikenali dari informasi aslinya dengan menggunakan algoritma tertentu. Sebaliknya, dekripsi adalah proses mengubah kembali bentuk tersamar tersebut menjadi informasi asli. Teknik ini memungkinkan pesan rahasia diubah menjadi pesan acak sehingga tidak sesuai dengan pesan aslinya.

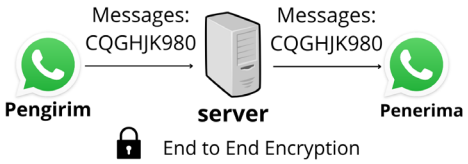


Gambar 1. Proses Enkripsi dan Dekripsi pada kriptografi

Pada Gambar 1 Menunjukan Bahwa untuk menjaga keamanan data, kriptografi mengubah informasi asli, yang disebut plaintext, menjadi bentuk informasi yang diacak atau terenkripsi yang disebut ciphertext, yang tidak dapat dikenali. Ciphertext ini kemudian akan dikirimkan oleh pengirim kepada penerima. Ketika ciphertext sampai ke penerima, proses dekripsi dilakukan untuk mengubahnya kembali menjadi plaintext sehingga dapat dikenali.

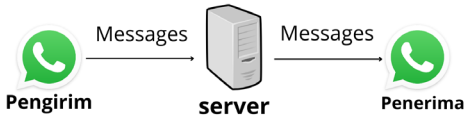
Pesan yang tidak terenkripsi disebut plaintext atau cleartext. Proses mengubah plaintext menjadi ciphertext disebut enkripsi. Kedua proses tersebut dilakukan dengan menggunakan algoritma tertentu yang disebut kunci.

Dengan menggunakan metode ini, pesan hanya dapat diketahui oleh pengirim pesan dan penerima pesan saja. Berikut adalah ilustrasi implementasi enkripsi end-to-end



Gambar 2. Ilustrasi penggunaan end-to-end encrypted

Pada Gambar 2 menunjukkan bahwa pesan klien telah terenkripsi sebelum sampai ke server. Ini berarti server tidak dapat mengetahui isi asli pesan dan tidak dapat mendekripsinya karena penerima memiliki kunci dekripsi. Sehingga pesan tetap aman selama proses pengiriman.



Gambar 3. Ilustrasi pengiriman pesan tanpa end to end encription

\

Pada gambar 3 menunjukkan bahwa pesan yang dikirim oleh klien ke server adalah pesan asli yang belum terenkripsi, server dapat memeriksa isi

pesan sebelum menyimpan versi terenkripsinya. Jika seseorang dapat mengakses jalur komunikasi antara klien dan server, metode ini dapat diserang. Pihak yang tidak berwenang dapat dengan mudah mengubah atau menghapus pesan.

Gambar 2 dan gambar 3 menunjukkan perbedaan dalam pengiriman pesan dari klien ke server. Pada implementasi enkripsi end-to-end, pesan yang dikirim sudah dalam keadaan terenkripsi. Server tidak mengetahui isi asli pesan tersebut dan tidak dapat mendekripsinya karena tidak memiliki kunci dekripsi. Sebaliknya, pada pengiriman pesan tanpa enkripsi end-to-end, pesan yang dikirim ke server adalah pesan asli yang belum terenkripsi. Server dapat membaca isi pesan sebelum menyimpannya dalam versi terenkripsi. Metode ini rentan terhadap serangan jika penyerang dapat mengakses jalur komunikasi antara klien dan server. Pesan dapat dengan mudah dimodifikasi atau dihapus.

Untuk mengimplementasikan enkripsi end-to-end, pertama-tama kedua klien harus melakukan pertukaran kunci. Beberapa algoritma dapat digunakan untuk pertukaran kunci ini, namun yang paling umum adalah algoritma Diffie-Hellman dan Elliptic Curve Diffie-Hellman seperti yang telah dijelaskan sebelumnya. Setelah kedua klien menerima kunci simetris yang sama, mereka akan mengenkripsi pesan sebelum mengirimkannya dan mendekripsi pesan yang diterima. Pihak ketiga tidak dapat membaca pesan tersebut karena tidak memiliki kunci simetris yang digunakan untuk enkripsi. Algoritma enkripsi yang biasanya digunakan adalah algoritma kriptografi kunci simetris, yang dipilih karena kedua klien memiliki kunci yang sama dan karena kompleksitas komputasinya yang rendah.

3. Metode Enkripsi End To end

Proses pembuatan shared secret key, juga dikenal sebagai "kunci rahasia bersama", adalah langkah penting dalam menerapkan enkripsi end-to-end. Shared secret key digunakan untuk mendekripsi dan mengenkripsi pesan yang dikirimkan antara pengirim dan penerima. Untuk menjamin keamanan dan kerahasiaan kunci tersebut, proses ini melibatkan beberapa langkah penting.

Pertama, ada tahap pembangkitan kunci acak. Untuk menghasilkan shared secret key, algoritma kriptografi yang kuat dan generator angka acak yang dapat menghasilkan nilai-nilai acak yang sulit ditebak biasanya digunakan. Hal ini penting untuk menghindari serangan kekerasan atau mencoba menebak kunci dengan berbagai pilihan.

Kedua, pengirim dan penerima harus menyetujui dan membagikan kunci yang telah dibangkitkan secara aman. Protokol pertukaran kunci seperti Diffie-Hellman adalah salah satu pendekatan yang paling umum digunakan. Ini memungkinkan kedua belah pihak untuk berbagi data tanpa mengungkapkan kunci sebenarnya kepada pihak lain atau pihak yang dapat mencurinya. Melindungi kunci selama pertukaran dan penggunaan juga penting. Teknik hashing dapat digunakan untuk menyimpan kunci yang telah disepakati dengan aman. Penggunaan kunci yang bersifat sementara atau berganti secara berkala juga dapat meningkatkan keamanan sistem enkripsi.

Dalam hal enkripsi end-to-end pada aplikasi chat, pembangkitan dan pengelolaan shared secret key harus dilakukan dengan hati-hati dan dijamin keamanannya. Kunci yang kuat dan terlindungi secara aman dapat menjadi fondasi utama dalam menjaga kerahasiaan pesan dan menghindari serangan terhadap sistem enkripsi. Dengan memperhatikan proses pembangkitan dan pengelolaan shared secret key secara teliti, maka keamanan data dalam komunikasi digital dapat terjaga dengan baik.

Proses enkripsi end-to-end melibatkan beberapa tahapan yang penting untuk memastikan keamanan dan kerahasiaan data yang dikirimkan antara pengirim dan penerima. Berikut adalah tahapan-tahapan utama dalam proses enkripsi end-to-end:

a. Pembangkitan Kunci: Pembangkitan Kunci: Tahap pertama adalah pembuatan kunci enkripsi dan dekripsi yang kuat. Kunci ini digunakan oleh pengirim untuk mengenkripsi pesan dan oleh penerima untuk mendekripsi pesan. Pembangkitan kunci harus dilakukan dengan menggunakan algoritma kriptografi yang aman

dan generator angka acak yang menghasilkan nilai-nilai acak yang sulit ditebak.

b. Pertukaran Kunci: Setelah kunci dibuat, pengirim dan penerima bertukar kunci secara aman. Ini dapat dicapai dengan menggunakan protokol seperti Diffie-Hellman, yang memungkinkan kedua belah pihak untuk berbagi data tanpa mengungkapkan kunci sebenarnya kepada orang lain atau orang yang mungkin mencurinya.

c. Enkripsi Pesan: Setelah kunci dibuat dan disetujui, pengirim menggunakan kunci tersebut untuk mengenkripsi pesan sebelum dikirim melalui jaringan atau media komunikasi. Proses ini mengubah bentuk pesan menjadi format yang tidak dapat dipahami oleh orang lain yang tidak memiliki kunci dekripsi yang tepat.

d. Pengiriman Pesan: Pesan yang telah dienkripsi kemudian dikirim ke penerima melalui jaringan atau media komunikasi lainnya.

e. Dekripsi Pesan: Setelah pesan sampai ke penerima, penerima menggunakan kunci yang telah disepakati untuk mendekripsi pesan yang telah dienkripsi oleh pengirim. Proses ini mengembalikan pesan ke format aslinya sehingga penerima dapat membacanya.

f. Verifikasi dan Autentikasi: Selain proses enkripsi dan dekripsi, ada juga proses verifikasi dan autentikasi untuk memastikan bahwa pesan yang diterima benar-benar berasal dari pengirim yang sah dan tidak diubah selama proses pengiriman.

g. Manajemen Kunci: Selama seluruh proses enkripsi end-to-end, penting untuk melakukan manajemen kunci yang baik. Ini termasuk menjaga sistem enkripsi aman dengan menyimpan kunci dengan aman, menggunakan kunci yang bersifat sementara atau berganti secara berkala, dan melakukan pembaruan kunci secara teratur.

IV. KESIMPULAN

Enkripsi end-to-end yang diterapkan pada WhatsApp sangat efektif dalam menjaga keamanan dan kerahasiaan data pengguna. Teknologi ini memastikan bahwa hanya pengirim dan penerima pesan yang dapat membaca isi pesan, melindungi pesan dari peretasan dan penyadapan selama transmisi. Meskipun ada beberapa masalah kinerja yang perlu diperbaiki, enkripsi end-to-end memberikan perlindungan yang kuat terhadap berbagai serangan siber. Selain itu, kesadaran pengguna tentang pentingnya keamanan data meningkat dengan penggunaan enkripsi end-to-end. Namun, meskipun memberikan keamanan tinggi, teknologi ini juga memiliki potensi disalahgunakan oleh pihak yang melakukan pelanggaran hukum, sehingga diperlukan keseimbangan antara melindungi privasi pengguna dan mencegah penyalahgunaan teknologi.

Studi ini juga menekankan pentingnya pengelolaan kunci enkripsi yang baik, termasuk pembangkitan, pertukaran, dan penyimpanan kunci yang aman, serta penggunaan generator angka acak yang handal dan algoritma kriptografi yang kuat. Secara keseluruhan, enkripsi end-to-end pada WhatsApp terbukti efektif dalam melindungi data pengguna dan privasi mereka, membantu mengatasi masalah keamanan siber di era digital.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan bantuan dalam penelitian ini. Penulis secara khusus ingin menyampaikan terima kasih kepada Bapak Bondan atas masukan dan saran yang sangat berharga. Dukungan dan bimbingan dari Bapak Bondan telah membantu meningkatkan kualitas penelitian ini dan mengarahkannya ke arah yang tepat. Terima kasih atas waktu dan usaha yang telah Anda berikan untuk membantu kami.

REFERENSI

[1] Santria, U., Arsoetar, N., Pascasarjana, P., Matematika, P., & Yogyakarta, U. N. (n.d.). Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp.

[2] Khasanah, S., & Sutabri, T. (2023). ANALISIS PENCEGAHAN PENCURIAN DATA MELALUI APLIKASI WHATSAPP MENGGUNAKAN METODE KRIPTOGRAFI. In Jurnal Sain dan Teknik (Vol. 5, Issue 2).

[3] Sri Maharani, Y., Trisdiatin, S., Rafli Ihsanuddin, M., & Rahma, F. (2023). SEMIOTIKA Seminar Nasional Teknologi Informasi dan Matematika Kekuatan Enkripsi End-to-End: Kajian Literatur Mengenai Kerahasiaan Komunikasi Digital dalam Aplikasi Pesan Instan (Vol. 2, Issue 1).

[4] Diandra, D. (n.d.). Peran Aplikasi WhatsApp Dalam Pemasaran: State of The Art. In Bisnis Madani (Vol. 2022, Issue 2). https://journal.paramadina.ac.id/

[5] Juniarmi, I. (2024). Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Enkripsi End-to-End. Technologia Journal: Jurnal Informatika, 1(2), 3046–9163. https://doi.org/10.62872/ppr42775

[6] KEAMANAN SIBER (Cyber Security). (n.d.).

[7] Liander, G. V. (n.d.). Penggunaan Algoritma Elliptic Curve Diffie Hellman dan AES 256 pada Implementasi End-to-End Encryption WhatsApp. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-danKoding/T

[8] *Adhiwibowo, W., Hirzan, A. M., & Suprayogi, M. S. (2022). PENINGKATAN KEAMANAN DATA END-TO-END SMART DOOR MENGGUNAKAN ADVANCED ENCRYPTION STANDARD. Jurnal ELTIKOM, 6(2), 186–194. https://doi.org/10.31961/eltikom.v6i2.574*

[9] Junikhah, A. (n.d.). IMPLEMENTASI VIGENERE CIPHER PADA APLIKASI MYPRICHAT END-TO-END ENCRYPTED SMS BERBASIS ANDROID.

[10] Lestari, S. P., Fadlan, H. N., Purba, R. A., Gunawan, I., Studi, P., Informatika, T., Tunas, S., & Pematangsiantar, B. (n.d.). *JURNAL MEDIA INFORMATIKA [JUMIN] Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp*. http://ejournal.sisfokomtek.org/index.php/jumin

[11] Urva.G, "AnalisisPenggunaan EnkripsiEnd ToEndPadaAplikasiWhatsappMessengger,"e-Proceeding of Engineering : Vol.7, No.2 Agustus 2020, [Online].

[12] Maharani, Y. S., Trisdiatin, S., Ihsanuddin, M. R., & Rahma, F. (2023). Kekuatan Enkripsi End-to-End: Kajian Literatur Mengenai Kerahasian Komunikasi Digital dalam Aplikasi Pesan Instan. In Seminar Nasional Teknologi Informasi dan Matematika (SEMIOTIKA) (Vol. 2, No. 1, pp. 1-7)

[13] E. Wehner and E. Moran, "End to end encryption: an answer to security concerns in the private sector," unpublished.