

Eksplorasi Keamanan Ganda melalui Verifikasi Dua Langkah dalam Menjaga Kerahasiaan Komunikasi Digital pada Aplikasi WhatsApp

Maulidan^{1*}, Safarul Akbar², Amanda Mauliyani³, Ristia Alma⁴, Muhammad Fadhil Hasibuan⁵

^{1,2,3,4,5} Universitas Malikussaleh, Indonesia

¹ maulidan.240170027@mhs.unimal.ac.id, ² safarul.240170078@mhs.unimal.ac.id,

³ amanda.240170065@mhs.unimal.ac.id, ⁴ ristia.240170066@mhs.unimal.ac.id,

⁵ muhammad.240170215@mhs.unimal.ac.id

ABSTRACT

Tingginya ketergantungan global pada platform komunikasi digital, khususnya melalui aplikasi terkemuka seperti WhatsApp, telah menjadikan perlindungan dan kerahasiaan data pengguna sebagai isu krusial dalam keamanan siber. Meskipun WhatsApp telah mengadopsi enkripsi *end-to-end* secara *default* untuk menjamin privasi isi pesan—sejalan dengan konsep dasar Kerahasiaan (Confidentiality) dalam kriptografi—kerentanan serius masih terdeteksi pada lapisan Autentikasi akun. Ancaman modern seperti upaya pengambilalihan akun secara paksa, serangan *phishing*, hingga eksploitasi *SIM Swap* memungkinkan pihak yang tidak berwenang untuk mendaftarkan ulang nomor telepon pengguna, yang berpotensi menyebabkan penyalahgunaan sistem dan pencurian data. Penelitian ini bertujuan untuk melakukan eksplorasi komprehensif terhadap mekanisme Verifikasi Dua Langkah (Two-Step Verification/2FA) yang diimplementasikan pada aplikasi WhatsApp sebagai lapisan keamanan ganda. Mekanisme 2FA ini berfungsi sebagai benteng pertahanan kritis kedua, mewajibkan pengguna memasukkan Kode Identifikasi Pribadi (PIN) rahasia yang bersifat independen dari kode verifikasi SMS. Dalam konteks ilmu kriptografi, penerapan 2FA merupakan solusi kriptografi modern yang mengalihkan penekanan keamanan dari kerahasiaan algoritma ke kerahasiaan kunci (PIN) yang digunakan, memungkinkan sistem yang terbuka namun tetap andal terhadap serangan. Metode yang digunakan dalam studi ini melibatkan dua pendekatan: (1) Analisis sistematis terhadap arsitektur 2FA WhatsApp dan dampaknya terhadap proses verifikasi ulang akun, serta (2) Studi kualitatif/kuantitatif (misalnya: survei pengguna) untuk mengevaluasi tingkat adopsi dan kemudahan penggunaan (usabilitas) fitur ini di kalangan pengguna awam. Hasil penelitian ini diharapkan dapat menunjukkan sejauh mana penerapan 2FA efektif dalam melindungi akun dari upaya pengambilalihan yang tidak sah. Studi ini menyimpulkan bahwa 2FA tidak hanya secara signifikan memperkuat aspek Autentikasi sebagai pilar keamanan informasi, tetapi juga berhasil mencapai keseimbangan antara keamanan yang kuat dan antarmuka yang sederhana, menjadikannya kunci untuk menjaga keamanan data dengan kuat dan andal bagi masyarakat luas.

Kata Kunci: Keamanan Data, Whatsapp, Verifikasi Dua Langkah, Keamanan Ganda

PENDAHULUAN

Ketergantungan masyarakat modern terhadap teknologi jaringan komputer untuk komunikasi dan pengiriman data telah meningkat secara eksponensial. Dalam konteks ini, pemasangan sistem keamanan untuk komunikasi data yang aman adalah suatu keharusan untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang dikirim melalui jaringan. Dalam praktiknya, pencurian data seringkali terwujud sebagai pembacaan oleh pihak yang tidak berwenang, biasanya dengan menyadap saluran publik.

WhatsApp, sebagai salah satu platform komunikasi utama, telah mengadopsi teknologi enkripsi mutakhir, yaitu enkripsi *end-to-end*, untuk melindungi kerahasiaan isi pesan. Meskipun teknologi ini efektif mengurangi bahkan menghilangkan kemungkinan kerusakan data akibat konektivitas fisik, gangguan keamanan yang mengarah pada penyalahgunaan sistem tetap bisa terjadi karena adanya unsur kesengajaan dari pihak tertentu. Risiko tersebut terutama timbul pada tingkat Autentikasi atau verifikasi kepemilikan akun.

Ancaman seperti upaya pengambilalihan akun secara tidak sah (*account takeover*), yang sering terjadi melalui skema *phishing* atau eksploitasi *SIM Swap*, menunjukkan bahwa meskipun pesan terlindungi, akses ke akun dan riwayat komunikasi dapat dikompromikan. Untuk memperkuat pertahanan pada lapisan autentikasi, fitur Verifikasi Dua Langkah (2FA) hadir sebagai solusi keamanan ganda.

Fitur Verifikasi Dua Langkah mewajibkan pengguna untuk membuat dan memasukkan Kode Identifikasi Pribadi (PIN) rahasia setiap kali ada upaya pendaftaran ulang nomor telepon pada perangkat baru. Konsep ini selaras dengan perkembangan dalam ilmu kriptografi, yaitu algoritma kriptografi modern. Algoritma kriptografi modern tidak didasarkan atas kerahasiaan algoritmanya (*restricted algorithm*), melainkan lebih menekankan pada keamanan atau kerahasiaan kunci yang digunakan. Dalam kasus 2FA, PIN rahasia bertindak sebagai kunci sekunder yang harus dijaga kerahasiaannya. Hal ini mengatasi masalah pada algoritma lama; jika ada kebocoran kunci, algoritma yang dipakai tidak perlu diganti, namun cukup mengganti kuncinya saja (PIN 2FA).

Tujuan utama dari penelitian ini adalah untuk melihat dan mempelajari berbagai konsep dan prinsip dalam merancang dan mengimplementasikan sistem keamanan data—dalam hal ini, melalui mekanisme Verifikasi Dua Langkah pada WhatsApp.

Secara spesifik, penelitian ini bertujuan untuk:

- Menganalisis secara mendalam bagaimana Verifikasi Dua Langkah bekerja sebagai lapisan keamanan ganda untuk melindungi akun WhatsApp dari pengambilalihan yang tidak sah.
- Mengevaluasi efektivitas 2FA dalam memperkuat aspek Autentikasi dan Integritas Data akun pengguna.
- Menilai kemudahan penggunaan fitur 2FA, sejalan dengan kebutuhan akan algoritma kriptografi modern yang dapat digunakan dan gampang dimengerti oleh semua orang.

Diharapkan hasil penelitian ini dapat memberikan pemahaman yang komprehensif mengenai pentingnya adopsi Verifikasi Dua Langkah sebagai strategi esensial untuk menjaga kerahasiaan komunikasi digital.

KAJIAN LITERATUR

Keamanan Komunikasi Digital

Perkembangan teknologi komunikasi digital telah membawa perubahan signifikan dalam cara manusia bertukar informasi. Aplikasi pesan instan seperti WhatsApp memungkinkan pengiriman pesan secara cepat, real-time, dan lintas wilayah. Namun, kemudahan ini juga diiringi dengan meningkatnya ancaman keamanan, seperti penyadapan, peretasan akun, pencurian identitas, serta kebocoran data pribadi. Oleh karena itu, aspek keamanan komunikasi digital menjadi perhatian penting, terutama dalam menjaga kerahasiaan pesan yang dikirimkan melalui jaringan publik.

Keamanan komunikasi digital secara umum bertujuan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Beberapa prinsip utama dalam keamanan informasi meliputi kerahasiaan (confidentiality), integritas data (integrity), dan autentikasi (authentication). Ketiga prinsip tersebut saling berkaitan dan menjadi dasar dalam perancangan sistem keamanan pada aplikasi komunikasi modern.

Konsep Autentikasi dalam Sistem Informasi

Autentikasi merupakan proses verifikasi identitas pengguna sebelum sistem memberikan akses ke layanan atau data tertentu. Pada sistem informasi digital, autentikasi berfungsi untuk memastikan bahwa pengguna yang mengakses sistem adalah pihak yang sah. Metode autentikasi yang umum digunakan antara lain autentikasi berbasis kata sandi (password), biometrik, serta autentikasi berbasis token atau kode verifikasi.

Penggunaan kata sandi saja dinilai belum cukup aman karena rentan terhadap serangan brute force, phishing, maupun kebocoran data. Oleh sebab itu, sistem keamanan modern mulai mengadopsi autentikasi berlapis untuk meningkatkan perlindungan akun pengguna.

Verifikasi Dua Langkah (Two-Step Verification)

Verifikasi dua langkah atau Two-Step Verification (2SV) merupakan metode keamanan yang menggabungkan dua tahap autentikasi untuk memverifikasi identitas pengguna. Tahap pertama umumnya berupa kata sandi atau nomor identitas, sedangkan tahap kedua berupa kode tambahan yang dikirimkan melalui SMS, email, atau aplikasi autentikator.

Konsep dasar verifikasi dua langkah bertujuan untuk menambah lapisan keamanan sehingga meskipun kata sandi diketahui oleh pihak tidak berwenang, akses ke akun tetap dapat dicegah tanpa kode verifikasi tambahan. Dengan demikian, risiko pembajakan akun dapat diminimalkan secara signifikan. Beberapa penelitian menyatakan bahwa penerapan verifikasi dua langkah mampu meningkatkan tingkat keamanan akun pengguna, terutama pada aplikasi yang menangani data sensitif dan komunikasi pribadi. Metode ini dinilai efektif karena menggabungkan sesuatu yang diketahui pengguna (password) dan sesuatu yang dimiliki pengguna (kode verifikasi).

Keamanan WhatsApp dan End-to-End Encryption

WhatsApp merupakan salah satu aplikasi pesan instan yang paling banyak digunakan di dunia. Untuk menjaga keamanan komunikasi penggunanya, WhatsApp menerapkan teknologi end-to-end encryption, yaitu metode enkripsi yang memastikan pesan hanya dapat dibaca oleh pengirim dan penerima. Pihak ketiga, termasuk penyedia layanan, tidak dapat mengakses isi pesan yang dikirimkan.

Selain enkripsi, WhatsApp juga menyediakan fitur verifikasi dua langkah sebagai mekanisme tambahan untuk melindungi akun pengguna. Fitur ini mengharuskan pengguna memasukkan PIN enam digit saat melakukan pendaftaran ulang nomor telepon atau saat akun diakses pada perangkat baru. Dengan adanya fitur ini, keamanan akun menjadi lebih kuat karena tidak hanya bergantung pada kode OTP yang dikirim melalui SMS.

Peran Verifikasi Dua Langkah dalam Menjaga Kerahasiaan Komunikasi



Penerapan verifikasi dua langkah pada aplikasi WhatsApp berperan penting dalam menjaga kerahasiaan komunikasi digital. Fitur ini membantu mencegah pengambilalihan akun oleh pihak yang tidak berwenang, terutama dalam kasus pencurian SIM card atau penyalahgunaan kode OTP.

Dengan adanya verifikasi dua langkah, pengguna memiliki kontrol tambahan terhadap keamanan akunnya. Kombinasi antara enkripsi end-to-end dan autentikasi berlapis menjadikan WhatsApp sebagai salah satu aplikasi pesan instan yang memiliki sistem keamanan cukup kuat. Oleh karena itu, eksplorasi terhadap efektivitas verifikasi dua langkah menjadi penting untuk memahami sejauh mana fitur ini mampu melindungi kerahasiaan komunikasi digital pengguna.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur (library research) dengan pendekatan deskriptif kualitatif. Metode ini dipilih karena penelitian berfokus pada pengkajian konsep, mekanisme, serta peran verifikasi dua langkah dalam menjaga kerahasiaan komunikasi digital, khususnya pada aplikasi WhatsApp, tanpa melakukan pengujian sistem secara langsung.

Tahapan Penelitian

Tahapan penelitian dilakukan secara sistematis agar pembahasan yang dihasilkan memiliki dasar teoritis yang kuat dan relevan dengan topik yang dikaji. Adapun tahapan penelitian yang dilakukan adalah sebagai berikut:

Pengumpulan Data

Data dikumpulkan melalui studi literatur yang bersumber dari jurnal ilmiah, buku referensi, artikel penelitian, serta dokumentasi resmi terkait keamanan komunikasi digital, autentikasi, verifikasi dua langkah, dan sistem keamanan WhatsApp. Sumber-sumber tersebut digunakan untuk memperoleh pemahaman yang komprehensif mengenai konsep dan penerapan keamanan ganda dalam aplikasi pesan instan.

Analisis Literatur

Literatur yang telah dikumpulkan kemudian dianalisis untuk mengidentifikasi konsep utama yang berkaitan dengan autentikasi berlapis dan mekanisme verifikasi dua langkah. Analisis dilakukan dengan membandingkan berbagai pendapat dan temuan penelitian sebelumnya guna memahami kelebihan, keterbatasan, serta efektivitas penerapan verifikasi dua langkah dalam menjaga keamanan akun dan kerahasiaan pesan.

Pengkajian Mekanisme Keamanan WhatsApp

Pada tahap ini, dilakukan pengkajian terhadap fitur keamanan yang diterapkan pada aplikasi WhatsApp, khususnya verifikasi dua langkah dan keterkaitannya dengan sistem end-to-end encryption. Pengkajian ini bertujuan untuk memahami bagaimana kombinasi kedua mekanisme tersebut mampu meningkatkan perlindungan terhadap komunikasi digital pengguna.

Penyusunan Hasil Kajian

Hasil analisis literatur dan pengkajian mekanisme keamanan kemudian disusun secara sistematis dalam bentuk pembahasan ilmiah. Penyusunan ini dilakukan dengan mengaitkan teori-teori yang relevan dengan penerapan nyata verifikasi dua langkah pada WhatsApp, sehingga diperoleh gambaran yang jelas mengenai peran keamanan ganda dalam menjaga kerahasiaan komunikasi digital.

HASIL DAN PEMBAHASAN

Gambaran Umum Keamanan Ganda pada WhatsApp

Berdasarkan hasil kajian literatur yang telah dilakukan, WhatsApp menerapkan sistem keamanan berlapis dalam menjaga kerahasiaan komunikasi digital penggunanya. Sistem keamanan tersebut tidak hanya mengandalkan teknologi enkripsi end-to-end, tetapi juga dilengkapi dengan mekanisme autentikasi tambahan berupa verifikasi dua langkah. Kombinasi kedua mekanisme ini membentuk konsep keamanan ganda yang bertujuan untuk melindungi pesan dan akun pengguna dari akses tidak sah.

Enkripsi end-to-end berfungsi untuk menjaga isi pesan agar tidak dapat dibaca oleh pihak ketiga selama proses pengiriman. Sementara itu, verifikasi dua langkah berperan dalam mengamankan akses ke akun pengguna, terutama saat terjadi pendaftaran ulang nomor atau perpindahan perangkat. Dengan demikian, perlindungan tidak hanya diberikan pada data yang dikirimkan, tetapi juga pada identitas dan akun pengguna itu sendiri.

Implementasi Verifikasi Dua Langkah pada WhatsApp

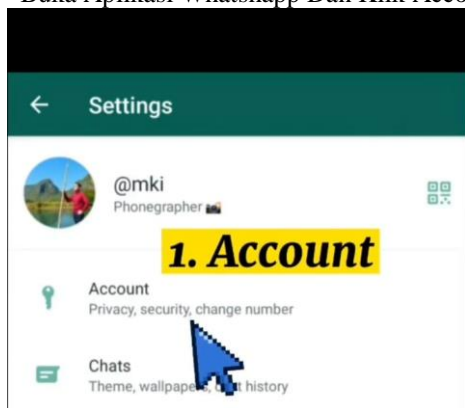


Hasil kajian menunjukkan bahwa verifikasi dua langkah pada WhatsApp diterapkan melalui penggunaan PIN enam digit yang ditentukan oleh pengguna. PIN ini akan diminta ketika pengguna melakukan verifikasi nomor telepon pada perangkat baru atau saat proses pemulihan akun. Mekanisme ini menambah lapisan keamanan di luar kode OTP yang dikirimkan melalui SMS.

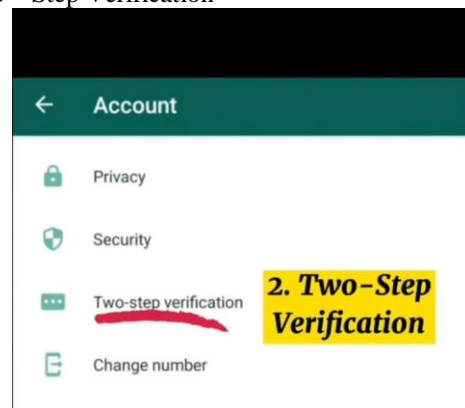
Penerapan verifikasi dua langkah terbukti mampu mengurangi risiko pengambilalihan akun, khususnya pada kasus penyalahgunaan kode OTP akibat pencurian kartu SIM atau serangan social engineering. Tanpa mengetahui PIN yang telah ditetapkan pengguna, pihak yang tidak berwenang tidak dapat menyelesaikan proses aktivasi akun, meskipun telah memperoleh kode verifikasi awal.

Berikut Adalah Langkah – Langkah Verification di WA:

- Buka Aplikasi Whatsapp Dan Klik Account dan Klik Two – Step Verification

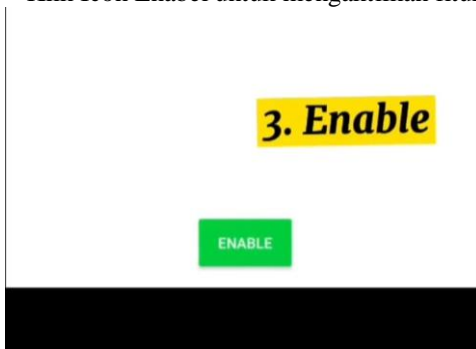


Gambar 1. Aplikasi Whatsapp Dan Klik Account

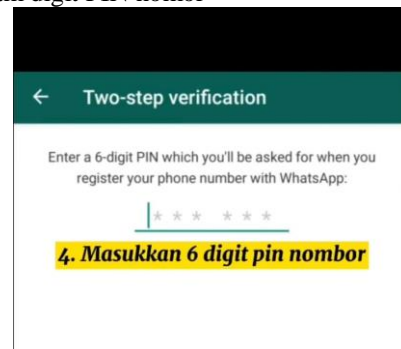


Gambar 2. Step Verification

- Klik Icon Enabel untuk mengaktifkan fitur dan Masukkan Enam digit PIN nomor



Gambar 3. Icon Enabel untuk mengaktifkan fitur

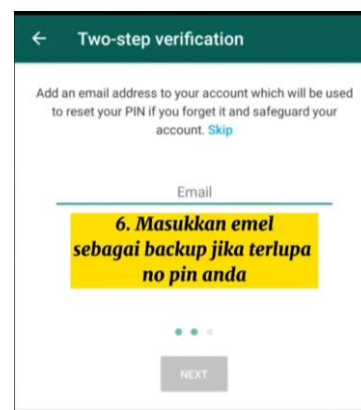


Gambar 4. Enam digit PIN nomor

- Masukkan Konfigurasi PIN nomor Yang telah diisi dan Masukkan gmail Anda untuk memperkuat keamanan dan mempermudah anda jika lupa PIN

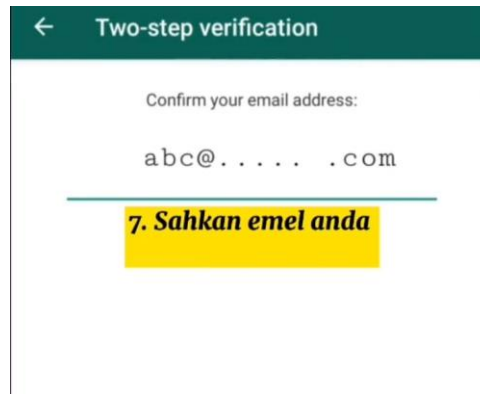


Gambar 5. Konfigurasi PIN



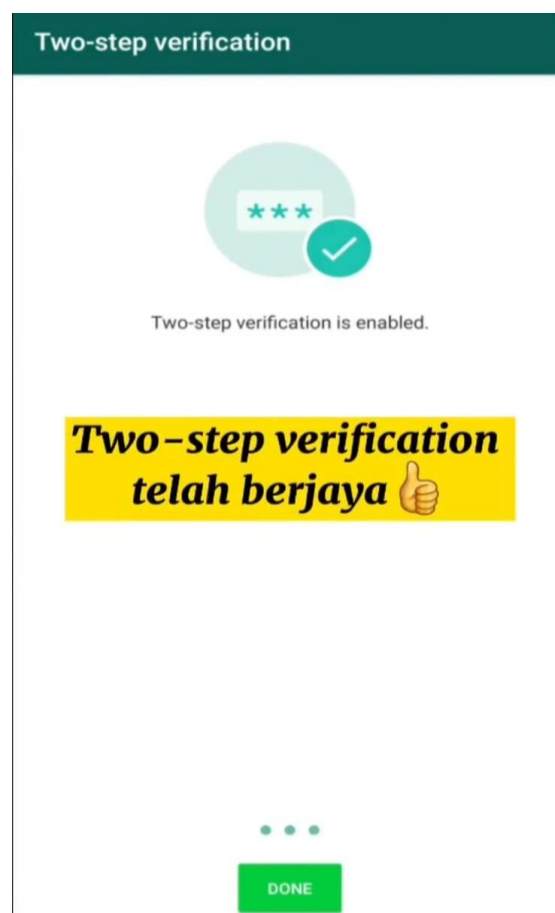
Gambar 6. lupa PIN

- Sahkan atau setuju gmail yang anda masukkan



Gambar 7. Sahkan atau setuju gmail

- Klik Icon Done dan anda telah berhasil dan selesai melakukan verifikasi dua Langkah



Gambar 8. selesai melakukan verifikasi dua Langkah

Peran Verifikasi Dua Langkah dalam Menjaga Kerahasiaan Komunikasi

Dari hasil analisis, verifikasi dua langkah memiliki peran penting dalam menjaga kerahasiaan komunikasi digital. Keamanan komunikasi tidak hanya ditentukan oleh kuatnya algoritma enkripsi, tetapi juga oleh sejauh mana sistem mampu mencegah akses ilegal ke akun pengguna. Dalam hal ini, verifikasi dua langkah berfungsi sebagai pengaman tambahan yang melindungi akun dari pembajakan.

Dengan adanya verifikasi dua langkah, kemungkinan pihak tidak berwenang untuk membaca, mengirim, atau

memanipulasi pesan atas nama pengguna dapat diminimalkan. Hal ini menunjukkan bahwa autentikasi berlapis memberikan kontribusi nyata dalam meningkatkan tingkat kepercayaan dan keamanan pengguna terhadap aplikasi komunikasi digital.

Kelebihan dan Keterbatasan Keamanan Ganda

Keamanan ganda yang diterapkan WhatsApp memiliki beberapa kelebihan, di antaranya adalah peningkatan perlindungan akun, pencegahan akses tidak sah, serta perlindungan kerahasiaan pesan secara menyeluruh. Sistem ini relatif mudah diterapkan oleh pengguna dan tidak memerlukan perangkat tambahan, sehingga tetap ramah digunakan oleh berbagai kalangan.

Namun demikian, hasil kajian juga menunjukkan adanya keterbatasan. Keamanan verifikasi dua langkah sangat bergantung pada kesadaran pengguna dalam mengaktifkan dan menjaga kerahasiaan PIN. Apabila pengguna lupa PIN atau tidak mengaktifkan fitur tersebut, maka tingkat perlindungan akun menjadi berkurang. Oleh karena itu, peran pengguna tetap menjadi faktor penting dalam efektivitas sistem keamanan ganda.

Implikasi terhadap Keamanan Komunikasi Digital

Penerapan verifikasi dua langkah pada WhatsApp memberikan implikasi positif terhadap keamanan komunikasi digital secara umum. Sistem ini dapat dijadikan contoh penerapan autentikasi berlapis pada aplikasi pesan instan lainnya. Dengan mengombinasikan enkripsi dan verifikasi dua langkah, aplikasi komunikasi digital dapat memberikan perlindungan yang lebih komprehensif terhadap ancaman keamanan yang semakin kompleks.

KESIMPULAN

Berdasarkan kajian literatur yang telah dilakukan, dapat disimpulkan bahwa keamanan komunikasi digital pada aplikasi WhatsApp tidak hanya ditentukan oleh penggunaan teknologi enkripsi, tetapi juga oleh penerapan mekanisme autentikasi yang memadai. WhatsApp menerapkan konsep keamanan ganda melalui kombinasi end-to-end encryption dan verifikasi dua langkah sebagai upaya untuk melindungi pesan serta akun pengguna dari berbagai bentuk ancaman keamanan.

Hasil pembahasan menunjukkan bahwa verifikasi dua langkah memiliki peran strategis dalam memperkuat perlindungan akun pengguna. Mekanisme ini menambahkan lapisan keamanan tambahan di luar kode verifikasi yang dikirimkan melalui SMS, sehingga mampu mengurangi risiko pengambilalihan akun akibat pencurian identitas, penyalahgunaan kartu SIM, maupun serangan rekayasa sosial. Dengan adanya PIN yang hanya diketahui oleh pengguna, akses tidak sah terhadap akun dapat diminimalkan meskipun pihak lain berhasil memperoleh kode verifikasi awal.

Selain itu, penerapan verifikasi dua langkah turut berkontribusi dalam menjaga kerahasiaan komunikasi digital secara tidak langsung. Ketika akun pengguna terlindungi dengan baik, maka potensi pihak tidak berwenang untuk membaca, mengirim, atau memanipulasi pesan menjadi semakin kecil. Hal ini menunjukkan bahwa keamanan komunikasi merupakan hasil dari integrasi antara perlindungan data dan pengamanan akses pengguna.

Meskipun demikian, efektivitas sistem keamanan ganda ini masih sangat bergantung pada kesadaran pengguna. Pengguna yang tidak mengaktifkan verifikasi dua langkah atau kurang menjaga kerahasiaan PIN berisiko mengalami penurunan tingkat keamanan akun. Oleh karena itu, edukasi kepada pengguna mengenai pentingnya fitur keamanan tambahan menjadi faktor pendukung yang tidak dapat diabaikan. Secara keseluruhan, verifikasi dua langkah dapat dipandang sebagai solusi yang relevan dan efektif dalam meningkatkan keamanan dan kerahasiaan komunikasi digital pada aplikasi WhatsApp.

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulisan jurnal yang berjudul "*Eksplorasi Keamanan Ganda melalui Verifikasi Dua Langkah dalam Menjaga Kerahasiaan Komunikasi Digital pada Aplikasi WhatsApp*" dapat diselesaikan dengan baik.

Penulis menyampaikan apresiasi dan terima kasih yang sebesar-besarnya kepada dosen pembimbing dan seluruh dosen yang telah memberikan arahan, masukan, serta ilmu pengetahuan selama proses penyusunan jurnal ini. Ucapan terima kasih juga penulis sampaikan kepada pihak-pihak yang telah memberikan referensi dan dukungan akademik yang sangat membantu dalam penyelesaian penelitian ini.

Tidak lupa, penulis mengucapkan terima kasih kepada keluarga dan rekan-rekan yang telah memberikan dukungan moral, motivasi, serta semangat selama proses penulisan berlangsung. Semoga jurnal ini dapat memberikan manfaat dan kontribusi bagi pengembangan pengetahuan di bidang keamanan komunikasi digital serta menjadi referensi bagi penelitian selanjutnya.

REFERENSI

- Abrar, M. F., & Nasution, M. I. P. (2025). *Analisis peningkatan keamanan data two step verification pada aplikasi WhatsApp Messenger. Surplus: Jurnal Ekonomi dan Bisnis Islam*. [YPTB](#)
- Flora, H. S. F. (2025). *Faktor penyebab dan penanggulangan terjadinya peretasan WhatsApp. Jurnal Profil Hukum. Ejournal UST*
- Harnovik, T., Alfarisy, T. A., Hutapea, W., & Batubara, S. (2024). *Implementation of end-to-end security and privacy of the WhatsApp social media application. Journal of Information Technology, Computer Science and Electrical Engineering*, *1*(2), 97–99. <https://doi.org/10.61306/jitcse.v1i2.55> [YSMK](#)
- Hariyadi, D., et al. (2025). *Peningkatan kewaspadaan terhadap kejahatan siber pada aplikasi WhatsApp di Kalurahan Bangunjiwo. Jurnal Pengabdian Masyarakat – Teknologi Digital Indonesia. UTDI eJournal*
- Juniarmi, I. (2025). *Data security analysis of chatting applications using end-to-end encryption. Technologia Journal. Naw*
- Rusmala & Prasti, D., 2019. Implementasi Metode Rail Fence Cipher dan Row Transposition Cipher Pada Mata Kuliah Kriptografi. *Jurnal Ilmiah d'Computare* , Volume Vol.9
- Syahputri, N. I., et al. (2025). *Penyuluhan pentingnya two factor authentication dan aplikasinya di era keamanan digital. Jurnal Pengabdian Masyarakat Bangsa. Jurnal Pengabdian Masyarakat Bangsa*
- Zuhriyanto, I., & Astari, S. R. (2025). *Penerapan Zero Trust Architecture untuk mitigasi ancaman pembajakan akun WhatsApp. JITU: Journal Informatic Technology And Communication. E-journal UBY*