Penerapan Zero Trust Architecture untuk Mitigasi Ancaman Pembajakan Akun WhatsApp

Ikhsan Zuhriyanto [a,1*], Sri Rahayu Astari [b,2]

[a] Sekolah Tinggi Teknologi Bontang, Kota Bontang, 75313, Indonesia
[b] Sekolah Tinggi Teknologi Bontang, Kota Bontang, 75313, Indonesia
[1] Ikhsan@stitek.ac.id *; [2] tarisrtari@gmail.com;
* Korespondensi penulis

Submission:29/04/2025, Revision: 29/04/2025, Accepted: 04/05/2025

Abstract

Account hijacking on WhatsApp has become an increasingly prevalent cybersecurity threat, particularly through social engineering and the misuse of One-Time Passwords (OTPs). This study investigates the implementation of Zero Trust Architecture (ZTA) as a mitigation approach for such threats. Based on the principle of "never trust, always verify," ZTA is applied through multi-factor authentication (MFA), device validation, access segmentation, and continuous monitoring. The findings indicate that the application of ZTA significantly reduces the risk of account hijacking. The use of MFA and contextual identity verification proves effective in preventing unauthorized access, even when OTP information has been compromised. Additionally, real-time monitoring of user behavior enables swift responses to suspicious activities. The study also notes increased user awareness of digital security practices as a positive impact of ZTA implementation. In conclusion, integrating Zero Trust Architecture into the security system of messaging applications like WhatsApp can be an effective strategy for minimizing account hijacking threats. This research aims to explore the application of Zero Trust Architecture in mitigating WhatsApp account hijacking, and how this concept can enhance the authentication and communication security of WhatsApp users.

Keywords: Zero Trust Architecture, Account Hijacking, WhatsApp, Cybersecurity, Authentication

Abstrak

Pembajakan akun WhatsApp merupakan salah satu ancaman keamanan siber yang semakin marak terjadi, terutama melalui rekayasa sosial dan penyalahgunaan kode *One-Time Password* (OTP). Studi ini meneliti penerapan Zero Trust Architecture (ZTA) sebagai pendekatan mitigasi untuk ancaman tersebut. Dengan prinsip "*never trust, always verify*," ZTA diterapkan melalui *autentikasi multifaktor* (MFA), validasi perangkat, segmentasi akses, dan monitoring berkelanjutan. Hasil penelitian menunjukkan bahwa penerapan ZTA mampu menurunkan risiko pembajakan akun secara signifikan. Penggunaan MFA dan verifikasi identitas kontekstual terbukti efektif dalam mencegah akses tidak sah, bahkan ketika informasi OTP telah bocor. Selain itu, pemantauan perilaku pengguna secara real-time memberikan respons cepat terhadap aktivitas mencurigakan. Studi ini juga mencatat peningkatan kesadaran pengguna terhadap praktik keamanan digital sebagai dampak positif penerapan ZTA. Kesimpulannya, integrasi Zero Trust Architecture dalam sistem keamanan aplikasi perpesanan seperti WhatsApp dapat menjadi strategi yang efektif dalam meminimalkan ancaman pembajakan akun. Penelitian ini bertujuan untuk mengeksplorasi penerapan Zero Trust Architecture dalam mitigasi pembajakan akun WhatsApp, serta bagaimana konsep tersebut dapat meningkatkan keamanan autentikasi dan komunikasi pengguna WhatsApp.

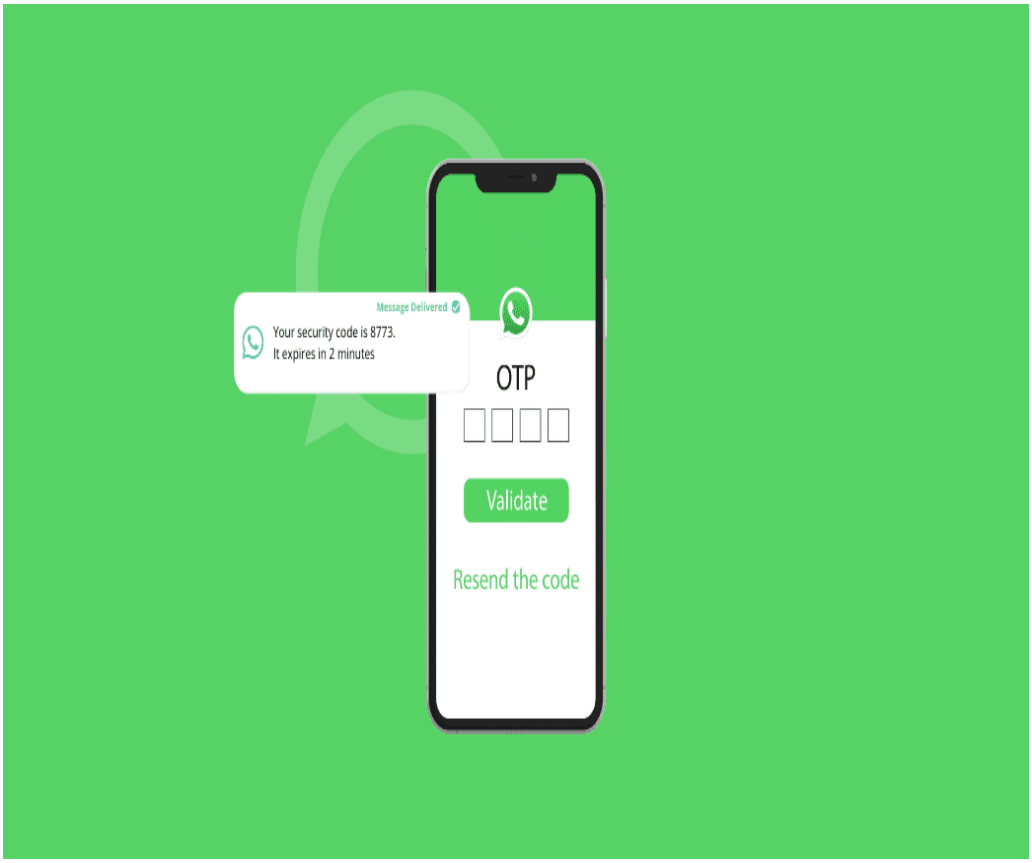
Kata kunci: Zero Trust Architecture, Pembajakan Akun, WhatsApp, Keamanan Siber, Autentikasi

1. Pendahuluan

Dalam era digital modern, aplikasi pesan instan seperti WhatsApp telah menjadi komponen esensial dalam komunikasi harian, baik secara personal maupun professional. Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada tahun 2022 jumlah pengguna internet di Indonesia mencapai lebih dari 215 juta orang, menjadikan WhatsApp sebagai salah satu platform komunikasi paling dominan [1]. Seiring

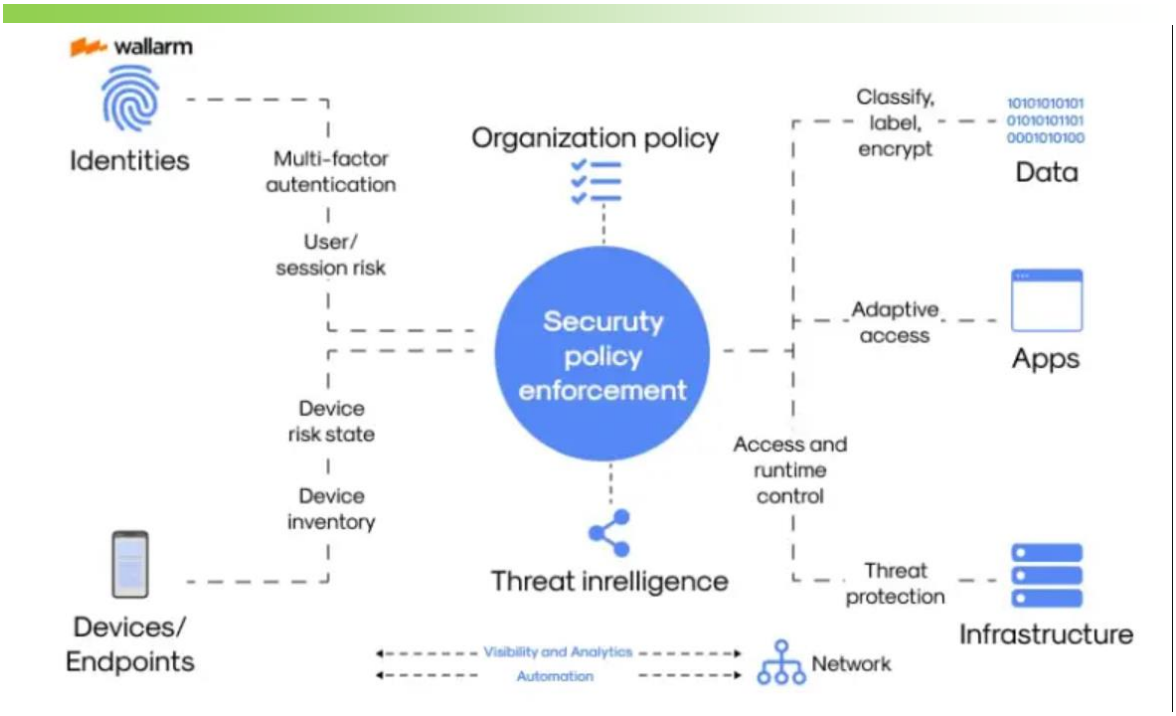
dengan meningkatnya penggunaan, risiko keamanan siber juga berkembang, terutama dalam bentuk pembajakan akun *(account hijacking*).

Salah satu metode umum yang digunakan oleh pelaku kejahatan siber adalah memperoleh kode OTP (*One-Time Password*) dari korban melalui teknik rekayasa sosial, kemudian menggunakannya untuk mengakses akun dari perangkat baru tanpa sepengetahuan pemilik asli [2]. Setelah mendapatkan akses, pelaku dapat membaca pesan, menyamar sebagai korban, dan menyalahgunakan identitas korban. Hal ini menunjukkan adanya kelemahan signifikan dalam sistem autentikasi WhatsApp, yang saat ini hanya mengandalkan OTP sebagai metode verifikasi utama seperti yang dapat dilihat pada Gambar 1.



Gambar 1. Vrifikasi OTP WhatsApp

Penggunaan autentikasi tunggal berbasis OTP sangat rentan apabila tidak dilengkapi dengan mekanisme verifikasi tambahan seperti deteksi perangkat, geolokasi, atau pola perilaku pengguna. Dalam konteks ini, pendekatan keamanan berbasis Zero Trust Architecture (ZTA) menjadi sangat relevan dengan menerapkan prinsip "n*ever trust, always verify*," di mana setiap permintaan akses, bahkan dari perangkat yang sebelumnya dikenal, harus melalui proses verifikasi yang ketat [3]. Arsitektur ZTA dapat dilihat pada Gambar 2.



Gambar 2. Arsitektur ZTA

Badan Siber dan Sandi Negara (BSSN) menekankan pentingnya implementasi ZTA di berbagai infrastruktur digital nasional, termasuk dalam konteks aplikasi komunikasi [4]. Penerapan ZTA dalam sistem informasi dapat diintegrasikan dengan autentikasi adaptif dan notifikasi ke perangkat terpercaya guna meningkatkan ketahanan terhadap pembajakan akun [5]. Penelitian lain juga menunjukkan bahwa penguatan kebijakan akses berbasis konteks dapat mengurangi vektor serangan siber secara signifikan .Penelitian ini bertujuan untuk menganalisis dan merancang penerapan prinsip ZTA dalam proses login WhatsApp di perangkat baru sebagai bentuk mitigasi terhadap risiko pembajakan akun.

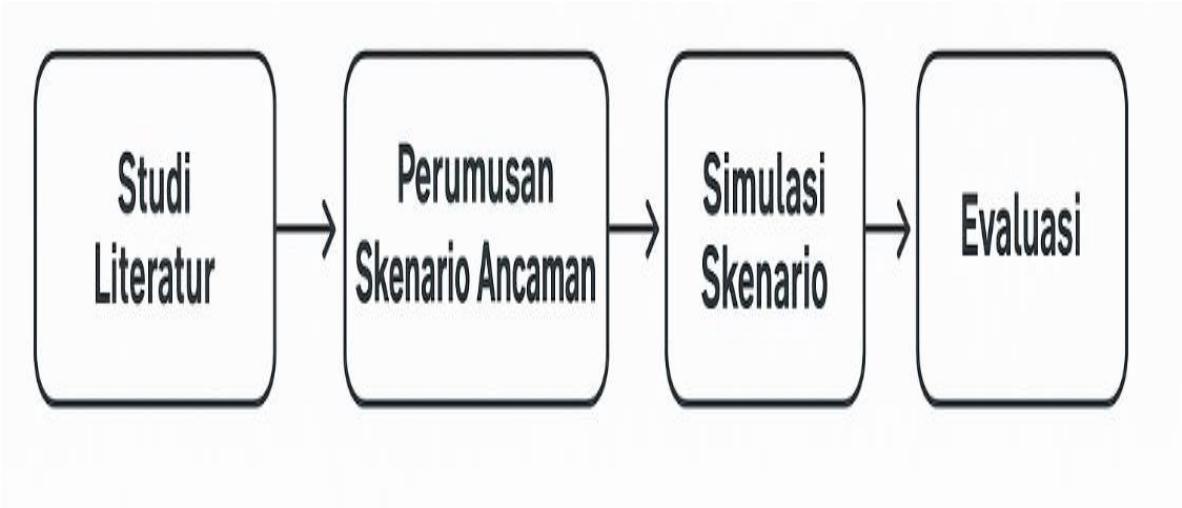
Keamanan informasi merupakan aspek krusial dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Salah satu ancaman paling umum dalam aplikasi pesan instan adalah pembajakan akun akibat kebocoran atau penyalahgunaan data autentikasi. Maulana mencatat bahwa sistem autentikasi satu lapis mudah dieksploitasi melalui teknik manipulasi sosial [6]. Proses autentikasi tanpa analisis kontekstual, seperti lokasi akses atau perangkat yang digunakan, memberikan celah bagi pihak tidak berwenang untuk menyamar sebagai pengguna sah [7].

ZTA merupakan paradigma keamanan yang menolak kepercayaan implisit terhadap pengguna, perangkat, maupun jaringan internal. Semua permintaan akses divalidasi secara menyeluruh berdasarkan identitas, perangkat, lokasi, dan atribut lainnya. BSSN menyatakan bahwa ZTA terdiri dari kebijakan akses berbasis identitas, verifikasi perangkat, segmentasi jaringan, serta pemantauan berkelanjutan [8]. Pendekatan ini dapat digabungkan dengan autentikasi adaptif dan otorisasi dari perangkat terpercaya sebagai upaya tambahan mitigasi [9]. Studi terbaru juga menggarisbawahi pentingnya orkestrasi keamanan dan integrasi sistem analitik untuk memantau akses real-time secara berkelanjutan [10], [11].

Autentikasi kontekstual pada aplikasi *mobile* memungkinkan sistem mendeteksi anomali berdasarkan lingkungan akses, seperti lokasi geografis, waktu, dan jenis perangkat. Proses ZTA menunjukkan bahwa pendekatan ini mampu meningkatkan keamanan tanpa mengorbankan kenyamanan pengguna [12]. Studi serupa menegaskan bahwa penggunaan pembelajaran mesin dalam mendeteksi anomali perilaku dapat meningkatkan akurasi deteksi hingga 92% [13], [14]Dengan demikian, kombinasi antara ZTA dan autentikasi berbasis konteks dianggap ideal untuk mengatasi tantangan pembajakan akun pada WhatsApp.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan deskriptif-kualitatif dan menerapkan metode skenario (*scenario-based method*) untuk mengevaluasi penerapan Zero Trust Architecture dalam mitigasi pembajakan akun WhatsApp. Pendekatan ini dinilai efektif dalam memodelkan ancaman dan respons sistem keamanan berbasis studi kasus [15]. Alur penelitian ditunjukan pada Gambar 3.



Gambar 3. Metode Penelitian

a. Tahap *Studi Literatur*.

Pada tahap awal penelitian ini merupakan langkah yang sangat penting dalam penelitian untuk membangun fondasi teoritis yang kuat dan memastikan relevansi serta validitas pendekatan yang digunakan. Pada tahap ini, peneliti melakukan telaah sistematis terhadap berbagai sumber pustaka baik primer maupun sekunder Literatur dikumpulkan dari jurnal ilmiah, buku referensi, dan dokumen kebijakan resmi BSSN terkait ZTA sebagai landasan perancangan model keamanan.Tahap ini memberikan landasan konseptual dan praktis untuk merancang pendekatan berbasis *Zero Trust* dalam konteks aplikasi *mobile*. Hasil studi menjadi acuan dalam merancang arsitektur sistem, menentukan parameter verifikasi, serta menyusun simulasi autentikasi pada skenario login dari perangkat baru.

b. Tahap Perumusan Skenario Ancaman.

Tahap ini bertujuan untuk menggambarkan secara sistematis potensi ancaman keamanan yang realistis dan sering terjadi, guna dijadikan dasar dalam pengembangan serta evaluasi sistem keamanan berbasis Zero Trust Architecture (ZTA*).* Pada tahap ini pembuatan skenario dilakukan yaitu Seorang pelaku mencoba login ke akun WhatsApp korban dari perangkat baru. Setelah kode OTP dikirim ke nomor korban, pelaku memperoleh OTP melalui manipulasi sosial. Tanpa validasi tambahan, pelaku berhasil masuk dan mengambil alih akun.

c. Tahap Perancangan *Model Zero Trust.*

Tahap ini bertujuan untuk merancang sistem keamanan guna memitigasi skenario ancaman pembajakan akun WhatsApp melalui login dari perangkat baru. Prinsip utama yang diterapkan adalah "*never trust, always verify*", yang mengharuskan setiap permintaan akses untuk divalidasi secara menyeluruh berdasarkan berbagai parameter. Selanjunya mengusulkan untuk model keamanan yang mencakup: Validasi perangkat dan lokasi akses. Otorisasi eksplisit dari perangkat terpercaya. Deteksi perilaku anomali seperti login di luar jam normal dan Autentikasi adaptif berbasis risiko.

d. Tahap Simulasi Skenario.

Tahap ini bertujuan untuk menguji efektivitas model yang telah dirancang sebelumnya melalui simulasi berbasis skenario autentikasi WhatsApp pada perangkat baru. Simulasi dilakukan secara konseptual dan berbasis skema sistem yang telah dirancang, guna mengevaluasi bagaimana sistem merespons permintaan akses yang mencurigaka Pada tahapan selanjutnya model disimulasikan dalam bentuk alur proses sebagai berikut :

1. Permintaan login dari perangkat baru
2. Verifikasi OTP
3. Validasi perangkat dan lokasi
4. Permintaan otorisasi dari perangkat lama
5. Penolakan akses jika otorisasi tidak diberikan

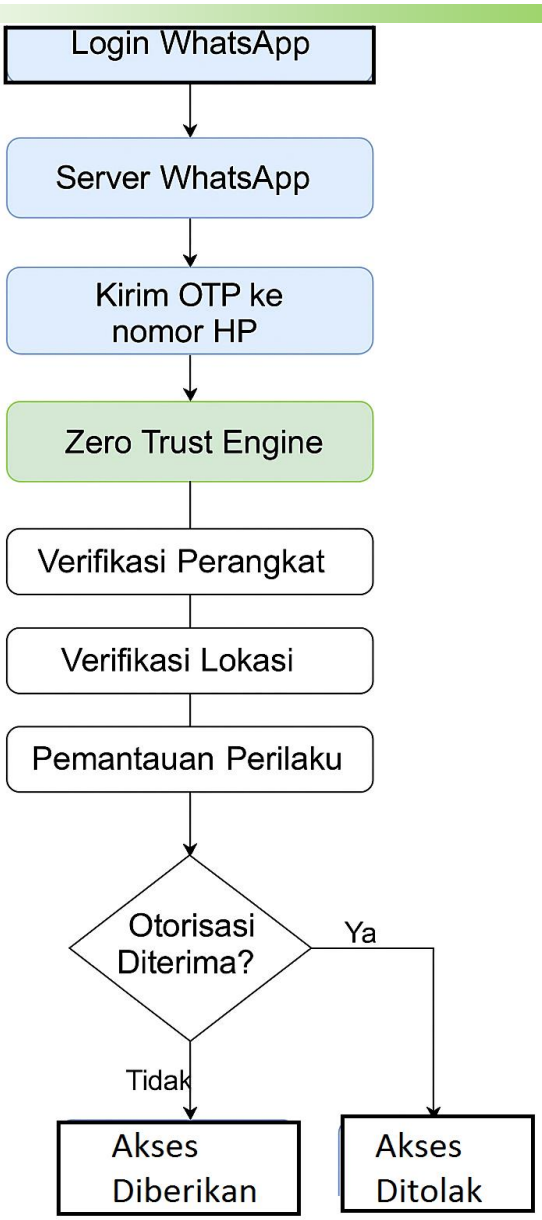
e. Tahap Evaluasi.

Tahap evaluasi dilakukan untuk menilai efektivitas model yang telah dirancang dan disimulasikan sebelumnya dalam menghadapi ancaman pembajakan akun WhatsApp. Evaluasi ini bersifat kualitatif dan berbasis skenario, mengingat penelitian belum sampai pada tahap implementasi sistem riil. Pada tahap terakhir Evaluasi dilakukan secara naratif dengan menilai: Efektivitas mitigasi pembajakan akun. Dampak terhadap kenyamanan pengguna dan Potensi implementasi pada aplikasi WhatsApp.

3. Hasil dan Pembahasan

Perancangan penerapan Zero Trust Architecture menggunakan proses login WhatsApp yang saat ini konvensional hanya mengandalkan pengiriman OTP ke nomor telepon yang terdaftar, tanpa adanya validasi tambahan terhadap perangkat atau lokasi akses. Hal ini memudahkan pelaku kejahatan siber untuk melakukan pembajakan apabila berhasil memperoleh OTP melalui teknik manipulasi sosial. Berdasarkan banyak kasus yang terjadi sistem gagal membedakan antara akses sah dan tidak sah, sehingga risiko pengambilalihan akun sangat tinggi.

Model Zero Trust yang dirancang mampu mengidentifikasi aktivitas login yang mencurigakan berdasarkan lokasi geografis, perangkat yang tidak dikenal, serta perilaku akses yang menyimpang dari pola biasa. Ketika permintaan login terjadi dari perangkat baru, sistem segera memicu permintaan otorisasi dari perangkat terpercaya. Jika otorisasi tidak diberikan, akses ditolak. Deteksi perilaku anomali juga berperan signifikan dalam mengidentifikasi upaya pembajakan. Dengan memanfaatkan autentikasi adaptif berbasis konteks, sistem dapat menyesuaikan tingkat verifikasi berdasarkan tingkat risiko. Penelitian ini menghasilkan sebuah model arsitektur keamanan berbasis Zero Trust Architecture (ZTA) yang diterapkan dalam konteks login akun WhatsApp dari perangkat baru yang dapat ditunjukan pada Gambar 4 yaitu flowchart scenario pembajakan akun WhatsApp.



Gambar 4. Flowchart Skenario

Pada gambar 2 merepresentasikan alur proses autentikasi pengguna pada aplikasi WhatsApp yang telah diperkuat melalui pendekatan Zero Trust Architecture (ZTA) sebagai upaya mitigasi terhadap ancaman pembajakan akun. Proses diawali dari aktivitas login oleh pengguna, yang kemudian memicu sistem untuk mengirimkan kode *One-Time Password* (OTP) ke nomor telepon yang telah terdaftar. OTP berfungsi sebagai autentikasi awal berbasis kepemilikan. Namun, mengingat kerentanannya terhadap teknik rekayasa sosial, tahapan ini dilanjutkan dengan mekanisme verifikasi berlapis berbasis ZTA.

Pada tahap selanjutnya, seluruh permintaan akses akan dianalisis oleh modul Zero Trust Engine, yang menjalankan serangkaian prosedur verifikasi lanjutan. Verifikasi pertama adalah identifikasi perangkat melalui teknik device fingerprinting, yang mencocokkan karakteristik perangkat dengan data historis guna mendeteksi perangkat baru atau mencurigakan. Dilanjutkan dengan verifikasi lokasi geografis berbasis alamat IP dan koordinat GPS untuk mengevaluasi apakah lokasi login sesuai dengan kebiasaan pengguna sebelumnya. Selain itu, dilakukan pula pemantauan perilaku pengguna secara *real-time*, seperti pola waktu login dan interaksi dalam aplikasi, guna mengidentifikasi anomali yang berpotensi mengindikasikan akses tidak sah.

Hasil dari seluruh proses verifikasi ini menentukan langkah akhir, yakni tahap otorisasi eksplisit. Jika sistem mendeteksi risiko atau ketidaksesuaian, maka notifikasi otorisasi dikirimkan ke perangkat yang telah terdaftar sebelumnya (*trusted device*). Hanya setelah otorisasi ini dikonfirmasi oleh pengguna, akses diberikan.

Sebaliknya, jika otorisasi tidak diterima atau ditolak, akses ke akun akan diblokir secara otomatis. Pendekatan ini mencerminkan prinsip dasar ZTA, yakni "*never trust, always verify*," dan menunjukkan efektivitas strategi berbasis konteks dalam meningkatkan ketahanan sistem terhadap serangan pembajakan akun berbasis rekayasa sosial dan pencurian kredensial.

Simulasi terhadap skenario login yang dilakukan oleh pihak tidak sah menunjukkan bahwa proses autentikasi berbasis ZTA dapat menghambat akses tidak sah bahkan jika OTP berhasil diperoleh. Akses hanya diberikan jika pengguna memberikan otorisasi eksplisit melalui perangkat yang sebelumnya telah dikenali. Pada Tabel 1 menunjukan lebih jelas mengenai perbandingan dari penggunaan ZTA dan tanpa menggunakan ZTA.

Tabel 1. Diagram Perbandingan

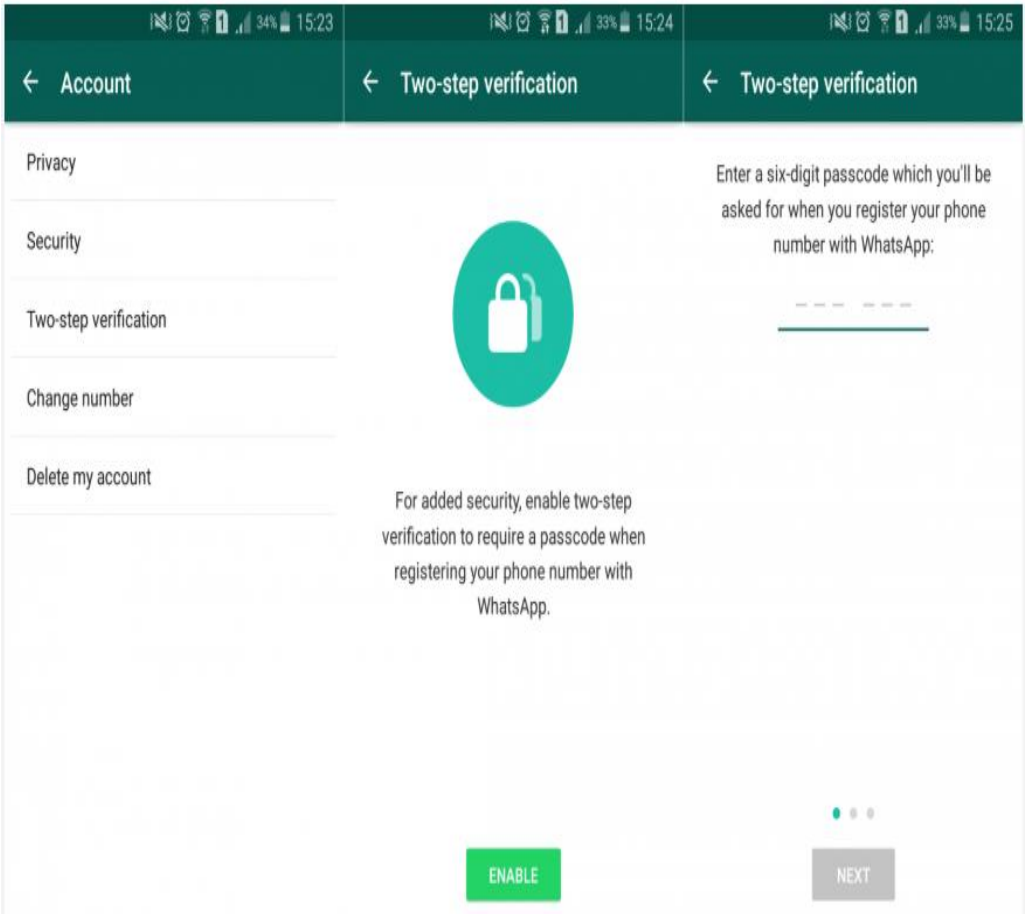
Aspek	Tanpa ZTA (OTP SMS)	Dengan ZTA (Zero Trust)
Otentikasi	OTP via SMS	OTP + Multi-Factor Authentication (MFA)
Deteksi Perangkat Asing	Tidak ada verifikasi perangkat	Verifikasi Device ID, deteksi perangkat baru
Verifikasi Lokasi	Tidak ada verifikasi lokasi	Verifikasi lokasi melalui IP/GPS, deteksi lokasi yang tidak biasa
Verifikasi Perilaku	Tidak ada verifikasi perilaku	Analisis perilaku pengguna (kecepatan mengetik, pola penggunaan perangkat)
Blokir Login	Tidak ada pembatasan jika OTP benar	Login diblokir jika perilaku atau perangkat mencurigakan
Deteksi Perangkat Asing	Tidak ada verifikasi perangkat	Verifikasi Device ID, deteksi perangkat baru
Verifikasi Lokasi	Tidak ada verifikasi lokasi	Verifikasi lokasi melalui IP/GPS, deteksi lokasi yang tidak biasa
Verifikasi Perilaku	Tidak ada verifikasi perilaku	Analisis perilaku pengguna (kecepatan mengetik, pola penggunaan perangkat)

Tabel 1 menunjukan diagram perbandingan dari berbagai aspek skenario pembajakan akun WhatsApp dengan menggunakan ZTA dan tanpa menggunakan ZTA. Perbandingan antara sistem autentikasi tradisional berbasis OTP melalui SMS dan pendekatan keamanan dengan Zero Trust Architecture (ZTA) menunjukkan perbedaan signifikan dalam hal kedalaman proteksi dan efektivitas mitigasi terhadap ancaman pembajakan akun. Pada sistem tanpa ZTA, autentikasi hanya mengandalkan pengiriman OTP melalui SMS, yang meskipun umum digunakan, rentan terhadap penyadapan, SIM *swap*, atau rekayasa sosial. Sebaliknya, ZTA menerapkan multi-factor authentication (MFA) sebagai tambahan lapisan keamanan, yang memastikan bahwa autentikasi tidak hanya berdasarkan sesuatu yang diketahui (OTP), tetapi juga sesuatu yang dimiliki (perangkat tepercaya) atau sesuatu yang melekat (biometrik).

Dilihat dari aspek deteksi perangkat, sistem konvensional tidak melakukan verifikasi terhadap perangkat pengguna, sehingga siapa pun yang memiliki OTP dapat mengakses akun, terlepas dari perangkat yang digunakan. Sementara itu, ZTA melakukan verifikasi Device ID dan menerapkan deteksi terhadap perangkat baru yang belum terdaftar, guna mengidentifikasi potensi akses tidak sah sejak awal. Di samping itu, ZTA juga memperkuat keamanan melalui verifikasi lokasi, dengan membandingkan alamat IP dan data GPS terhadap lokasi-lokasi login sebelumnya, sehingga login dari lokasi geografis yang tidak biasa dapat dikenali dan dicegah secara otomatis.

Selain itu, pendekatan ZTA mencakup verifikasi perilaku pengguna, yang melibatkan analisis parameter seperti kecepatan mengetik, pola interaksi dengan perangkat, dan waktu penggunaan. Verifikasi ini memungkinkan sistem untuk mendeteksi anomali perilaku yang mungkin tidak teridentifikasi melalui metode autentikasi konvensional. Dalam hal kontrol akses, sistem tanpa ZTA akan memberikan akses selama OTP yang dimasukkan benar, tanpa mempertimbangkan konteks perangkat atau perilaku pengguna. Sebaliknya, pada sistem ZTA, login dapat diblokir secara otomatis jika ditemukan indikasi mencurigakan pada perilaku pengguna atau perangkat yang digunakan. Dengan demikian, ZTA memberikan pendekatan keamanan yang

lebih adaptif, berbasis konteks, dan mampu merespons ancaman siber secara proaktif. Pendekatan dalam studi ini menawarkan peningkatan signifikan dalam konteks keamanan berbasis konteks dan adaptif. Misalnya, pada penguatan autentikasi dua faktor (2FA) sebagai solusi terhadap serangan berbasis OTP, tanpa mempertimbangkan aspek verifikasi perangkat atau perilaku pengguna, 2FA dapat diluhat pada Gambar 5.



Gambar 5. 2FA pada WhatsApp

Demikian pula, penggunaan enkripsi end-to-end dan pengamanan SIM sebagai upaya mitigasi, tetapi belum mengintegrasikan verifikasi lokasi dan pemantauan perilaku sebagai bagian dari sistem deteksi anomali. Sementara itu, penelitian ini menunjukkan bahwa ZTA mampu menjawab celah keamanan yang belum disentuh oleh pendekatan konvensional, yakni dengan menggabungkan device fingerprinting, analisis lokasi, dan verifikasi perilaku untuk menghasilkan respons adaptif terhadap potensi pembajakan akun.

Pendekatan ini juga melengkapi dan melampaui model keamanan berbasis *rule-based* yang sebelumnya dikembangkan dalam konteks aplikasi perpesanan, dengan memberikan respons yang lebih dinamis terhadap ancaman yang tidak dikenali sebelumnya. Penerapan Zero Trust dalam studi ini dapat dianggap sebagai pengembangan lanjutan dari pendekatan tradisional, yang mampu memberikan mitigasi lebih holistik terhadap risiko kompromi identitas digital di platform seperti WhatsApp.

4. Kesimpulan

Penerapan Zero Trust Architecture (ZTA) dalam sistem autentikasi akun WhatsApp terbukti memberikan peningkatan signifikan terhadap keamanan pengguna, khususnya dalam menghadapi skenario pembajakan akun yang melibatkan login dari perangkat baru atau akses oleh pihak tidak sah. Dengan mengedepankan prinsip dasar "*never trust, always verify*," pendekatan ini mengubah paradigma tradisional yang hanya bergantung pada autentikasi satu faktor seperti OTP melalui SMS, menjadi sistem yang lebih holistik dan berbasis kontekstual.

Lapisan-lapisan verifikasi yang diterapkan, seperti validasi perangkat melalui device fingerprinting, verifikasi lokasi geografis berdasarkan IP dan GPS, pemantauan perilaku pengguna melalui analisis pola interaksi, serta autentikasi adaptif berbasis tingkat risiko, membentuk sistem pertahanan berlapis yang jauh lebih tangguh. Salah satu keunggulan utama dari pendekatan ini adalah kemampuannya dalam mencegah akses

tidak sah meskipun informasi OTP telah berhasil dikompromikan oleh pihak ketiga. Melalui simulasi skenario yang dilakukan dalam penelitian ini, terlihat bahwa sistem dapat mendeteksi anomali secara efektif dan memblokir upaya login mencurigakan sebelum akses diberikan.

Selain aspek keamanan, penerapan ZTA juga mempertimbangkan faktor pengalaman pengguna. Sistem ini dirancang agar tetap efisien dan tidak mengganggu aktivitas pengguna sehari-hari, dengan cara mengaktifkan lapisan verifikasi tambahan hanya ketika terdeteksi anomali atau percobaan login dari perangkat yang belum dikenali. Pendekatan ini memastikan bahwa keamanan tidak mengorbankan kenyamanan, sehingga menciptakan keseimbangan optimal antara proteksi akun dan kemudahan penggunaan aplikasi.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa integrasi Zero Trust Architecture merupakan langkah strategis dan relevan dalam menghadapi dinamika ancaman siber masa kini, khususnya dalam konteks aplikasi komunikasi seperti WhatsApp. Diperlukan dukungan lebih lanjut dari penyedia layanan untuk mengadopsi model keamanan ini secara menyeluruh, serta edukasi berkelanjutan kepada pengguna agar dapat memahami pentingnya autentikasi kontekstual dan menjaga integritas identitas digital mereka.

5. Daftar Pustaka

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, “Laporan Survei Internet APJII 2022,” Tersedia : https://apjii.or.id. [Diakses : 24 April 2025].
[2] M. R. Hidayat, “Analisis keamanan akun WhatsApp pada proses registrasi perangkat baru,” *Jurnal Keamanan Siber Indonesia*, vol. 3, no. 1, pp. 12–20, doi: 10.25077/jksi.3.1.2022.12-20.
[3] A. Kurniawan, *Pengantar Keamanan Siber: Teori dan Praktik*. Bandung: Informatika.
[4] *Badan Siber dan Sandi Negara, Strategi Keamanan Siber Nasional dan Arsitektur Zero Trust dalam Infrastruktur Digital Indonesia*. Jakarta: BSSN.
[5] R. Surya and S. Andriani, “Implementasi arsitektur Zero Trust pada infrastruktur TI modern,” *Jurnal Teknik Informatika dan Keamanan Siber*, vol. 9, no. 3, pp. 110–118.
[6] R. Maulana, “Penerapan kontrol akses berbasis konteks pada sistem keamanan informasi,” *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 2, pp. 91–98, doi: 10.14710/jtsiskom.8.2.2020.91-98.
[7] A. Nugroho and D. Kurniawan, “Evaluasi metode autentikasi pengguna pada aplikasi mobile berbasis risiko,” *Jurnal Sistem Informasi dan Keamanan*, vol. 6, no. 2, pp. 44–53.
[8] M. F. Ramadhan and M. Aziz, “Autentikasi adaptif berbasis konteks untuk aplikasi mobile banking,” *Jurnal Teknologi Informasi dan Komputer*, vol. 7, no. 1, pp. 25–32.
[9] S. T. Prasetyo and H. Adi, “Implementasi kontrol akses berbasis konteks pada sistem mobile,” *Jurnal Sistem Informasi*, vol. 10, no. 1, pp. 20–29.
[10] F. G. Hikmatyar, “Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases,” vol. 7, no. 2, pp. 19–22, 2018.
[11] I. W. Kurniawan and L. Santosa, “Orkestrasi keamanan berbasis Zero Trust dalam lingkungan enterprise,” *Jurnal Ilmiah Teknologi Informasi Terapan*, vol. 4, no. 1, pp. 45–52.
[12] D. Setiawan, “Integrasi sistem monitoring keamanan berbasis konteks,” *Jurnal Riset Teknologi Informasi*, vol. 3, no. 2, pp. 70–78.
[13] P. A. Wijaya, “Penerapan machine learning untuk deteksi perilaku anomali pengguna pada aplikasi mobile,” *Jurnal Teknologi dan Informatika*, vol. 6, no. 3, pp. 90–98.
[14] Y. H. Gunawan and S. Pradipta, “Peningkatan akurasi deteksi anomali pada autentikasi adaptif menggunakan Random Forest,” *Jurnal Sistem Cerdas*, vol. 2, no. 1, pp. 33–41.
[15] S. Dewi and T. R. Nugraha, “Evaluasi kebijakan keamanan berbasis user behavior analytics,” *Jurnal Ilmiah Keamanan Siber*, vol. 5, no. 1, pp. 10–18.