IMPLEMENTASI TWO FAKTOR AUTHENTICATION (2FA) PADA SISTEM KEAMANAN DATA DI PT. ARIDZKA



Disusun Oleh :

Ahmad Atha Fadhiilah (2111510422)

Fribyan Yusuf (2111510406)

Abstrak  
  
Keamanan data merupakan isu penting di era digital, terutama dengan maraknya ancaman siber seperti phishing, brute force attacks, dan credential stuffing. Meskipun banyak perusahaan mengandalkan username dan password sebagai langkah pengamanan, metode ini sering kali tidak cukup kuat untuk mencegah akses tidak sah. Two-Factor Authentication (2FA) hadir sebagai solusi untuk meningkatkan keamanan dengan menambahkan lapisan verifikasi kedua, seperti kode OTP ataupun autentikasi biometrik.

Penelitian ini dilakukan pada PT Aridzka, yang meskipun tidak memiliki sistem internal untuk menyimpan data sensitif, tetap membutuhkan langkah-langkah keamanan saat mengakses layanan eksternal, seperti email, sistem manajemen vendor, atau aplikasi keuangan. Fokus penelitian adalah menganalisis implementasi 2FA dalam mengamankan akses ke sistem-sistem eksternal tersebut, mengevaluasi tantangan yang muncul, serta memahami dampak terhadap pengalaman pengguna dan operasional perusahaan.

Dengan demikian, penerapan 2FA di PT Aridzka menjadi langkah preventif yang penting untuk menjaga integritas akses ke sistem eksternal dan meningkatkan kepercayaan internal serta mitra bisnis. Studi ini diharapkan dapat memberikan panduan bagi PT Aridzka dan organisasi serupa dalam mengoptimalkan penerapan 2FA untuk mencapai keamanan yang lebih baik tanpa mengganggu efisiensi operasional.

Latar Belakang.

Seiring dengan pesatnya perkembangan teknologi digital, ancaman terhadap keamanan data semakin meningkat. Berbagai serangan siber, seperti phishing, brute force attack, dan credential stuffing, sering kali berhasil menembus sistem yang hanya mengandalkan kombinasi username dan password. Kelemahan metode otentikasi satu faktor ini membuat banyak organisasi mencari solusi keamanan tambahan untuk mencegah akses tidak sah dan menjaga data sensitif tetap aman.

Two-Factor Authentication (2FA) hadir sebagai solusi efektif untuk meningkatkan keamanan dengan menambahkan lapisan otentikasi kedua. Sistem 2FA meminta pengguna untuk membuktikan identitas mereka dengan menggunakan password atau PIN, kode OTP, dan sidik jari atau pemindai wajah. Kehadiran lapisan kedua ini menjadikan akses data lebih sulit diretas meskipun kredensial utama pengguna telah bocor.

Penerapan 2FA semakin relevan karena berbagai organisasi dan layanan digital mulai mengalami peningkatan risiko keamanan. Layanan seperti perbankan online, aplikasi e-commerce, dan media sosial membutuhkan metode otentikasi yang kuat untuk melindungi akun penggunanya dari potensi pencurian data atau penyalahgunaan akses. Dengan menggunakan 2FA, risiko serangan siber dapat diminimalkan karena pengguna harus melewati lebih dari satu mekanisme verifikasi.

Meskipun menawarkan keamanan lebih tinggi, implementasi 2FA tidak luput dari tantangan. Kompleksitas tambahan seperti penggunaan token, pengiriman kode OTP melalui SMS atau E-mail, atau pemindai biometrik dapat mempengaruhi pengalaman pengguna. Beberapa pengguna mungkin merasa proses ini terlalu merepotkan, terutama jika akses cepat dibutuhkan. Oleh karena itu, desain sistem 2FA harus memperhatikan keseimbangan antara keamanan dan kenyamanan pengguna agar dapat diadopsi secara luas.

Secara keseluruhan, implementasi 2FA merupakan langkah strategis dalam memperkuat keamanan data dan menjaga kepercayaan pengguna. Dengan meningkatkan ketahanan sistem terhadap serangan siber, 2FA membantu melindungi data sensitif dan mengurangi risiko penyalahgunaan akses. Di tengah meningkatnya ancaman dan tuntutan regulasi, adopsi 2FA bukan lagi sekadar opsi melainkan kebutuhan penting bagi organisasi modern untuk menjaga keamanan informasi dan keberlanjutan operasional.

Tujuan dan Manfaat

Tujuan :

1. Meningkatkan Keamanan Data

Memperkuat sistem otentikasi agar lebih tahan terhadap serangan siber dengan menambahkan lapisan verifikasi kedua.

2. Mencegah Akses Tidak Sah

Mengurangi risiko pencurian identitas atau penggunaan kredensial curian dengan mempersulit akses bagi penyerang.

3. Mengidentifikasi Tantangan Implementasi

Meneliti kendala teknis dan operasional yang mungkin muncul saat menerapkan 2FA pada sistem yang ada.

4. Menciptakan Keseimbangan antara Keamanan dan Kenyamanan

Merancang solusi 2FA yang tidak hanya aman tetapi juga mudah digunakan, sehingga pengguna merasa nyaman.

Manfaat

1. Peningkatan Keamanan Informasi

Dengan adanya 2FA, sistem lebih tahan terhadap berbagai jenis serangan siber, sehingga data sensitif terlindungi dengan lebih baik.

2. Pengurangan Risiko Kebocoran Data

2FA membantu mencegah akses ilegal bahkan ketika kredensial utama pengguna telah dicuri atau dibobol.

3. Kepatuhan terhadap Standar Keamanan

Organisasi dapat lebih mudah mematuhi regulasi terkait keamanan data, menghindari denda, dan mempertahankan reputasi.

4. Kepercayaan Pengguna Meningkat

Dengan keamanan yang lebih baik, pengguna merasa lebih aman dalam mengakses layanan, meningkatkan loyalitas dan kepercayaan mereka.

5. Peningkatan Kesadaran Keamanan

Penggunaan 2FA turut mendorong pengguna dan organisasi lebih sadar akan pentingnya praktik keamanan digital dalam kehidupan sehari-hari.

Dengan tujuan dan manfaat tersebut, penerapan 2FA tidak hanya berperan dalam menjaga keamanan data, tetapi juga memberikan dampak positif bagi keberlanjutan operasional dan kepuasan pengguna.