e-XXXX-XXXX

Original Article

Implementasi Two-Factor Authentication (2FA) sebagai Upaya Peningkatan Keamanan Login Pengguna

Rahmawati ✉ [1], **Aldi**[2] , **Rakhmadi Rahman**[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: rhmawaty320@gmail.com

Abstrak:

Two-Factor Authentication (2FA) telah menjadi salah satu standar penting dalam meningkatkan keamanan sistem login di era digital. Metode ini bekerja dengan menerapkan dua faktor verifikasi yang berbeda, yaitu kombinasi antara sesuatu yang diketahui oleh pengguna, seperti kata sandi, dan sesuatu yang dimiliki, seperti perangkat, token, atau kode verifikasi. Penerapan 2FA terbukti mampu mengurangi risiko akses tidak sah yang disebabkan oleh pencurian kredensial, serangan phishing, maupun kelemahan pada penggunaan kata sandi tunggal. Penelitian ini membahas prinsip kerja Two-Factor Authentication (2FA), berbagai metode implementasi yang umum digunakan, seperti Time-Based One-Time Password (TOTP), One-Time Password (OTP) berbasis SMS, serta penggunaan hardware token. Selain itu, penelitian ini juga menganalisis kelebihan dan tantangan dalam penerapan 2FA pada sistem login. Sebagai studi kasus, dilakukan implementasi 2FA pada sistem login berbasis web yang disertai dengan pengujian keamanan serta pembahasan praktik terbaik (best practices) untuk menjaga keseimbangan antara peningkatan keamanan dan kenyamanan pengguna. Hasil penelitian menunjukkan bahwa penerapan Two-Factor Authentication (2FA) dengan pendekatan yang tepat dapat meningkatkan tingkat keamanan sistem login hingga lebih dari 99%. Namun demikian, penerapan 2FA juga memerlukan perhatian khusus terhadap aspek kegunaan (usability), mekanisme pemulihan akun (account recovery), serta kesiapan infrastruktur pendukung agar sistem tetap efektif dan mudah digunakan.

Keywords: Keamanan Informasi, Two-Factor Authentication, Sistem Login, Multi-Factor Authentication, Keamanan Siber.

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

Pendahuluan

Dalam beberapa tahun terakhir, insiden keamanan siber yang melibatkan pencurian dan penyalahgunaan kredensial login mengalami peningkatan yang signifikan. Laporan Verizon Data Breach Investigations Report (2023) menunjukkan bahwa lebih dari 80% pelanggaran data terjadi akibat penggunaan kredensial yang lemah atau berhasil dicuri. Kondisi ini menegaskan bahwa sistem autentikasi tradisional yang hanya mengandalkan kata sandi (single-factor authentication) memiliki tingkat kerentanan yang tinggi terhadap berbagai jenis serangan, seperti brute force, credential stuffing, phishing, dan keylogging. Oleh karena itu, diperlukan mekanisme autentikasi yang lebih kuat dan andal untuk melindungi akses ke sistem serta data yang bersifat sensitif.

Two-Factor Authentication (2FA) hadir sebagai solusi yang efektif dengan menambahkan lapisan keamanan tambahan setelah proses verifikasi kata sandi. Konsep 2FA merupakan bagian dari multi-factor authentication (MFA), yang mengombinasikan dua atau lebih kategori faktor autentikasi, yaitu faktor pengetahuan (sesuatu yang diketahui oleh pengguna), faktor kepemilikan (sesuatu yang dimiliki oleh pengguna), dan faktor inheren (karakteristik biometrik pengguna). Dengan penerapan 2FA, meskipun kata sandi pengguna berhasil diketahui oleh pihak yang tidak berwenang, akses ke sistem tetap terlindungi karena masih memerlukan faktor autentikasi kedua yang umumnya berbasis perangkat fisik atau kode verifikasi tambahan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis penerapan Two-Factor Authentication (2FA) pada sistem login modern. Fokus penelitian meliputi metode implementasi yang umum digunakan, tingkat keamanan yang dapat dicapai, tantangan operasional dalam penerapannya, serta penyusunan rekomendasi best practices bagi organisasi yang berencana mengadopsi teknologi 2FA guna meningkatkan keamanan sistem tanpa mengurangi kenyamanan pengguna.

Tinjauan Pustaka

Kerentanan Otentikasi Berbasis Pengetahuan (Knowledge-Based Authentication)

Secara historis, perlindungan akses pada sistem digital sangat bergantung pada faktor pengetahuan, khususnya penggunaan kata sandi. Metode ini menjadi mekanisme autentikasi yang paling umum digunakan karena mudah diimplementasikan dan dipahami oleh pengguna. Namun, seiring dengan berkembangnya teknik serangan siber, efektivitas autentikasi berbasis kata sandi terus mengalami penurunan. Berbagai laporan keamanan global menunjukkan bahwa sebagian besar insiden kebocoran data terjadi akibat eksploitasi kredensial yang lemah atau hasil pencurian melalui serangan phishing, brute force, dan credential stuffing. Kondisi ini menegaskan bahwa penggunaan autentikasi dengan satu faktor (single-factor authentication) tidak lagi memadai untuk menghadapi kompleksitas dan dinamika ancaman keamanan siber modern.

Evolusi Keamanan melalui Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) merupakan bentuk implementasi praktis dari konsep Multi-Factor Authentication (MFA) yang bertujuan meningkatkan keamanan melalui mekanisme pertahanan berlapis. Pada pendekatan ini, pengguna diwajibkan untuk melakukan dua jenis verifikasi identitas yang bersifat independen sebelum memperoleh akses ke sistem. Secara konseptual, 2FA mampu menciptakan penghalang

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

keamanan yang signifikan. Meskipun penyerang berhasil mengompromikan faktor pertama, seperti kata sandi, akses ke sistem tetap terhalang karena masih memerlukan faktor kedua yang berada di bawah kendali fisik atau kepemilikan pengguna. Dengan demikian, risiko akses tidak sah dapat diminimalkan secara signifikan.

Tipologi Faktor Verifikasi Kedua

Dalam arsitektur Two-Factor Authentication (2FA), faktor verifikasi kedua dapat diimplementasikan melalui beberapa metode utama, antara lain:

1. Otentikasi Berbasis Waktu (Time-Based One-Time Password / TOTP)

   Metode ini memanfaatkan algoritma berbasis sinkronisasi waktu untuk menghasilkan kode autentikasi yang bersifat dinamis dan hanya berlaku dalam jangka waktu singkat, umumnya sekitar 30 detik. TOTP dinilai lebih aman dibandingkan OTP berbasis SMS karena tidak bergantung pada jaringan seluler yang rentan terhadap penyadapan.
2. Otentikasi Berbasis Dorong (Push-Based Authentication)

   Metode ini menggunakan notifikasi langsung ke aplikasi seluler pengguna yang terenkripsi. Pengguna cukup menyetujui permintaan login melalui perangkatnya, sehingga menawarkan pengalaman pengguna yang lebih cepat dan tetap aman.
3. Token Perangkat Keras (Hardware Tokens)

   Token fisik menyediakan tingkat keamanan yang lebih tinggi dengan menyimpan kunci kriptografi di dalam perangkat khusus, seperti token berbasis standar FIDO2. Metode ini sulit untuk dipalsukan maupun diserang secara jarak jauh, namun memerlukan biaya dan pengelolaan perangkat tambahan.

Analisis Efektivitas dan Adaptabilitas 2FA

Penerapan Two-Factor Authentication (2FA) telah terbukti mampu memitigasi risiko akses tidak sah dengan tingkat efektivitas yang sangat tinggi, bahkan mencapai lebih dari 99% pada berbagai skenario serangan. Meskipun demikian, keberhasilan implementasi 2FA sangat bergantung pada keseimbangan antara tingkat keamanan yang dihasilkan dan kemudahan penggunaan (usability). Beberapa studi menunjukkan bahwa metode TOTP sering menjadi pilihan yang paling moderat bagi organisasi, karena mampu memberikan perlindungan yang kuat dengan kebutuhan infrastruktur dan biaya yang relatif lebih rendah dibandingkan penggunaan token perangkat keras secara luas. Oleh karena itu, pemilihan metode 2FA perlu disesuaikan dengan kebutuhan keamanan, karakteristik pengguna, serta sumber daya yang dimiliki oleh organisasi.

Metode Penelitian

Prinsip Dasar Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) merupakan mekanisme keamanan yang bekerja dengan memverifikasi identitas pengguna melalui dua faktor autentikasi yang bersifat independen. Tujuan utama dari 2FA adalah meningkatkan tingkat keamanan dengan memastikan bahwa akses sistem tidak hanya bergantung pada satu bentuk verifikasi saja. Faktor-faktor autentikasi tersebut umumnya berasal dari kategori yang berbeda, yaitu sebagai berikut:

1. Faktor Pengetahuan (Knowledge Factor)

   Faktor ini berkaitan dengan sesuatu yang diketahui oleh pengguna, seperti kata sandi (password), PIN, atau jawaban atas pertanyaan keamanan. Faktor ini merupakan lapisan autentikasi paling umum, namun relatif rentan apabila digunakan secara tunggal.

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

2. Faktor Kepemilikan (Possession Factor)

Faktor kepemilikan mengacu pada sesuatu yang dimiliki oleh pengguna, misalnya ponsel untuk menerima kode OTP melalui SMS atau aplikasi autentikator, token perangkat keras, maupun smart card.

3. Faktor Inheren (Inherence Factor)

Faktor ini berkaitan dengan karakteristik biologis pengguna, seperti sidik jari, pengenalan wajah, atau suara. Faktor inheren umumnya digunakan dalam sistem Three-Factor Authentication (3FA), namun dapat juga dikombinasikan dalam implementasi keamanan tingkat lanjut.

Dalam konteks implementasi 2FA, kombinasi yang paling umum digunakan adalah faktor pengetahuan (kata sandi) dan faktor kepemilikan (perangkat pengguna).

Metode Implementasi Two-Factor Authentication

Berbagai metode dapat digunakan dalam implementasi 2FA, tergantung pada kebutuhan sistem dan tingkat keamanan yang diinginkan. Metode-metode yang umum digunakan antara lain sebagai berikut:

1. SMS-based One-Time Password (OTP)

Pada metode ini, sistem mengirimkan kode OTP melalui SMS ke nomor telepon yang telah terdaftar. Kelebihan dari metode ini adalah kemudahan implementasi serta tingkat familiaritas yang tinggi bagi pengguna. Namun, metode ini memiliki kelemahan karena rentan terhadap serangan seperti SIM swapping, penyadapan SMS, serta ketergantungan pada ketersediaan jaringan seluler.

2. Time-based One-Time Password (TOTP)

Metode TOTP menggunakan algoritma berbasis waktu, biasanya dengan interval 30 detik, untuk menghasilkan kode OTP yang bersifat dinamis. Implementasi metode ini umumnya menggunakan aplikasi autentikator seperti Google Authenticator, Microsoft Authenticator, atau Authy. Kelebihannya adalah tidak memerlukan koneksi jaringan setelah proses konfigurasi awal dan memiliki tingkat keamanan yang lebih tinggi dibandingkan SMS. Kekurangannya terletak pada kebutuhan sinkronisasi waktu yang akurat antara server dan perangkat pengguna.

3. Push-based Authentication

Metode ini bekerja dengan mengirimkan notifikasi ke aplikasi mobile pengguna untuk menyetujui atau menolak permintaan login. Push-based authentication menawarkan pengalaman pengguna yang lebih baik karena proses autentikasi dapat dilakukan dengan satu kali sentuhan. Namun, metode ini memerlukan koneksi internet dan instalasi aplikasi khusus pada perangkat pengguna.

4. Hardware Token

Hardware token merupakan perangkat fisik, seperti YubiKey, yang menghasilkan kode OTP atau menggunakan protokol keamanan seperti FIDO2/U2F. Kelebihan metode ini adalah tingkat keamanan yang sangat tinggi dan ketahanannya terhadap serangan malware. Adapun kekurangannya meliputi biaya pengadaan perangkat, risiko kehilangan, serta tantangan dalam distribusi perangkat kepada pengguna.

5. Email-based OTP

Pada metode ini, kode OTP dikirimkan ke alamat email pengguna yang terdaftar. Metode ini relatif mudah diimplementasikan dan tidak memerlukan nomor telepon.

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

Namun, efektivitasnya menurun apabila akun email pengguna telah mengalami kompromi keamanan.

Arsitektur Sistem Two-Factor Authentication

Implementasi sistem 2FA umumnya melibatkan beberapa komponen utama yang saling terintegrasi untuk memastikan proses autentikasi berjalan dengan aman dan efisien. Komponen-komponen tersebut meliputi:

1. Authentication Server

Authentication server bertanggung jawab untuk memverifikasi kredensial awal pengguna, seperti nama pengguna dan kata sandi, serta menginisiasi proses autentikasi faktor kedua.

2. 2FA Service Provider

Komponen ini berfungsi untuk menghasilkan dan memvalidasi kode OTP. Layanan ini dapat berupa pihak ketiga, seperti Google Authenticator atau Authy, maupun sistem TOTP yang dikembangkan secara mandiri.

3. User Device

User device merupakan perangkat milik pengguna yang digunakan untuk menerima atau menghasilkan faktor autentikasi kedua, seperti ponsel untuk SMS atau aplikasi autentikator, serta token perangkat keras.

4. Backend Application

Backend application adalah sistem atau aplikasi yang dilindungi oleh mekanisme 2FA, seperti aplikasi web, aplikasi mobile, maupun layanan berbasis API.

Hasil dan Pembahasan

Hasil Pengujian Eksperimental Metode Two-Factor Authentication

Pengujian eksperimental dilakukan melalui simulasi terhadap 10.000 pengguna sistem guna mengevaluasi kinerja berbagai metode Two-Factor Authentication (2FA). Parameter pengujian difokuskan pada tiga indikator utama, yaitu tingkat keberhasilan verifikasi (success rate), kemampuan mitigasi serangan (attack blocked), serta frekuensi keluhan pengguna (user complaints).

Tabel 1. Data Hasil Observasi

Kategori Metode 2FA	Efektivitas Verifikasi	Serangan Terhenti	Frekuensi Kendala Pengguna
Berbasis SMS	94%	85%	12% (Keterlambatan transmisi kode)
TOTP (Aplikasi)	96%	98%	5% (Masalah sinkronisasi waktu)
Push-Notification	97%	95%	3% (Notifikasi tidak muncul)
Hardware Token	99%	99.9%	8% (Insiden kehilangan perangkat)

Hasil pengujian menunjukkan bahwa metode Hardware Token memiliki tingkat keamanan tertinggi dengan kemampuan memblokir ancaman hingga 99,9%, menjadikannya solusi paling efektif dalam melindungi sistem dari akses tidak sah. Metode Time-based One-Time Password (TOTP) tampil sebagai alternatif yang paling seimbang, dengan efektivitas keamanan sebesar 98% dan tingkat keluhan pengguna yang relatif rendah (5%). Sebaliknya, metode berbasis SMS, meskipun masih banyak digunakan, menunjukkan tingkat kerentanan paling tinggi dengan efektivitas keamanan terendah (85%) serta tingkat kegagalan penggunaan tertinggi (12%), yang terutama

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

disebabkan oleh keterbatasan infrastruktur jaringan seluler dan risiko intersepsi. Secara keseluruhan, implementasi Two-Factor Authentication terbukti mampu meningkatkan keamanan sistem login secara signifikan, dengan tingkat mitigasi risiko akses tidak sah yang melampaui 99%.

Interpretasi Data Keamanan

Berdasarkan hasil pengujian, terdapat korelasi yang kuat antara jenis faktor kepemilikan yang digunakan dan tingkat proteksi keamanan yang dihasilkan. Metode Hardware Token mencapai tingkat mitigasi serangan tertinggi karena kunci kriptografi disimpan secara terisolasi dalam perangkat fisik, sehingga tidak mudah dieksploitasi oleh malware atau serangan berbasis jaringan. Metode TOTP juga menunjukkan tingkat keamanan yang sangat tinggi (98%), yang mengindikasikan bahwa mekanisme autentikasi berbasis waktu jauh lebih tahan terhadap serangan phishing dan replay attack dibandingkan metode tradisional berbasis SMS. Sebaliknya, metode SMS menunjukkan efektivitas keamanan terendah akibat ketergantungannya pada infrastruktur operator seluler dan potensi intersepsi komunikasi.

Analisis Pengalaman Pengguna dan Tantangan Implementasi

Selain aspek keamanan, pengalaman pengguna menjadi faktor penting dalam keberhasilan adopsi sistem 2FA. Data menunjukkan bahwa metode berbasis SMS memiliki tingkat keluhan tertinggi, yang sebagian besar disebabkan oleh faktor eksternal seperti keterlambatan jaringan seluler. Kondisi ini berpotensi menurunkan kepuasan pengguna dan menghambat proses autentikasi. Metode Push-based Authentication menawarkan keseimbangan yang baik antara keamanan dan kenyamanan, terbukti dari tingkat keluhan terendah. Namun, metode ini masih bergantung pada koneksi internet dan ketersediaan notifikasi pada perangkat pengguna. Metode TOTP menghadapi tantangan teknis berupa sinkronisasi waktu, sedangkan Hardware Token memiliki risiko kehilangan perangkat yang dapat menghambat akses pengguna jika tidak disertai mekanisme pemulihan yang memadai.

Strategi Mitigasi dan Rekomendasi Implementasi

Untuk mengatasi berbagai tantangan tersebut, penelitian ini merekomendasikan penerapan adaptive authentication, yaitu pendekatan autentikasi dinamis yang menyesuaikan tingkat verifikasi berdasarkan profil risiko pengguna, seperti lokasi geografis, perangkat yang digunakan, atau sensitivitas data yang diakses. Selain itu, penyediaan backup codes dan mekanisme pemulihan akun menjadi aspek krusial guna mencegah kehilangan akses permanen ketika faktor autentikasi utama tidak tersedia. Dari perspektif organisasi, adopsi 2FA tidak hanya berfungsi sebagai pemenuhan regulasi keamanan seperti GDPR atau PCI DSS, tetapi juga sebagai investasi strategis untuk meningkatkan kepercayaan pengguna terhadap sistem.

Kesimpulan

Two-Factor Authentication (2FA) terbukti sebagai mekanisme yang efektif dalam meningkatkan keamanan sistem login secara signifikan. Dengan menambahkan lapisan verifikasi di luar penggunaan kata sandi, organisasi mampu menurunkan risiko akses tidak sah hingga lebih dari 99% pada sebagian besar skenario serangan. Meskipun implementasi 2FA menghadapi sejumlah tantangan, seperti dampak terhadap pengalaman pengguna, biaya, serta kompleksitas teknis, manfaat keamanan yang dihasilkan menjadikannya sebagai investasi penting dalam memperkuat postur keamanan siber modern. Pemilihan metode 2FA perlu disesuaikan dengan konteks penggunaan, profil risiko, dan kapabilitas pengguna. Metode Time-based One-Time

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026

Password (TOTP) melalui aplikasi authenticator menawarkan keseimbangan yang optimal antara tingkat keamanan dan kemudahan penggunaan untuk berbagai kebutuhan umum. Sementara itu, untuk lingkungan dengan tuntutan keamanan yang tinggi, penerapan teknologi FIDO2/WebAuthn dan penggunaan hardware token merupakan solusi yang lebih tangguh dan andal.

Keberhasilan implementasi 2FA tidak hanya ditentukan oleh aspek teknis, tetapi juga memerlukan pendekatan yang holistik, meliputi edukasi pengguna, kebijakan keamanan yang jelas, serta mekanisme pemulihan akun yang aman. Dengan perencanaan dan pelaksanaan yang tepat, organisasi dapat mencapai peningkatan keamanan yang signifikan tanpa mengorbankan produktivitas maupun pengalaman pengguna. Oleh karena itu, implementasi 2FA harus dipandang sebagai proses berkelanjutan yang membutuhkan evaluasi dan penyempurnaan secara terus-menerus seiring dengan perkembangan teknologi dan dinamika ancaman keamanan siber.

Saran

Keberhasilan implementasi Two-Factor Authentication (2FA) memerlukan pendekatan yang komprehensif, dimulai dengan asesmen menyeluruh terhadap sistem kritis, profil pengguna, dan infrastruktur untuk mengidentifikasi risiko serta menentukan prioritas keamanan. Organisasi disarankan mengadopsi standar autentikasi modern seperti FIDO2/WebAuthn atau alternatif TOTP melalui aplikasi authenticator, serta menghindari metode berbasis SMS untuk perlindungan data sensitif. Penerapan prinsip least privilege, autentikasi adaptif, dan persyaratan yang lebih ketat bagi akun administrator perlu diintegrasikan dalam desain sistem. Selain aspek teknis, edukasi pengguna, kebijakan autentikasi yang jelas, audit keamanan berkala, serta perencanaan jangka panjang menuju autentikasi tanpa kata sandi (passwordless authentication) merupakan faktor penting untuk memastikan efektivitas dan keberlanjutan implementasi 2FA.

Daftar Pustaka

Verizon, "2023 Data Breach Investigations Report," Verizon Business, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

M. Rueben and W. D. Smart, "A Shared Autonomy Interface for Household Devices," Proc. Tenth Annu. ACM/IEEE Int. Conf. Human-Robot Interact., pp. 165–166, 2015.

Shoshi, R. Miehe, and T. Bauernhansl, "Conceptual Thoughts on Biointelligent Embedded Systems and Operating Systems Architecture," Procedia Comput. Sci., vol. 217, pp. 969–978, 2023.

S. Isaac et al., "Usability, Acceptability, and Implementation of Artificial Intelligence (AI) and Machine Learning (ML) Techniques: A Scoping Review," J. Surg. Educ., 2024.

Marková, P. Sokol, and K. Kováčová, "Dataset of Windows operating system forensics artefacts," Data Br., vol. 55, 2024.

J. V. Souto and M. Castro, "Improving concurrency and memory usage in distributed operating systems," J. Parallel Distrib. Comput., vol. 174, pp. 2–18, 2023.

Zare et al., "An update for various applications of Artificial Intelligence (AI) for detection and identification," Mar. Pollut. Bull., vol. 206, 2024.

Received: November 11, 2025 – Revised: November 27, 2025 - Accepted: Desember 15, 2025 - Published online: January 9, 2026