ISSN 2621- 458X

IMPLEMENTASI MULTI FACTOR AUTHENTICATION (MFA) DALAM SISTEM PELAYANAN PEMERINTAHAN DIGITAL INDONESIA: Analisis Permasalahan, Keamanan, dan Solusi Berbasis Identitas Digital

ILHAM
Program Studi Magister Administrasi Publik, ITBA Al Gazali Barru
ilham.amid86@gmail.com

ABSTRAK

Penelitian ini bertujuan menganalisis kondisi implementasi *Multi-Factor Authentication* (MFA) pada portal layanan publik digital di Indonesia, mengidentifikasi faktor-faktor yang memengaruhi adopsinya, serta merumuskan rekomendasi kebijakan untuk memperkuat keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE). Penelitian menggunakan pendekatan *mixed methods* melalui audit teknis terhadap 50 portal layanan publik pemerintah, survei kuantitatif yang dianalisis menggunakan regresi logistik ordinal dan *Structural Equation Modeling-Partial Least Squares* (SEM-PLS), serta triangulasi hasil untuk penyusunan rekomendasi kebijakan. Hasil penelitian menunjukkan bahwa hanya 24% portal telah mengimplementasikan MFA secara penuh, 30% secara parsial, dan 46% masih menggunakan autentikasi berbasis kata sandi tunggal, yang mengindikasikan rendahnya tingkat adopsi MFA pada layanan publik digital. Model empiris memiliki kemampuan prediksi yang baik (Nagelkerke R^2 = 0,623), dengan literasi digital sebagai faktor paling dominan memengaruhi adopsi MFA (OR = 3,424), diikuti pengalaman menggunakan layanan perbankan digital (OR = 2,867), kepercayaan terhadap pemerintah (OR = 2,438), persepsi keamanan (OR = 2,102), persepsi kemudahan penggunaan (OR = 1,844), dan kesiapan infrastruktur internet (OR = 1,721), sedangkan usia di atas 50 tahun menjadi faktor penghambat (OR = 0,434). Berdasarkan triangulasi temuan, penelitian merekomendasikan penerapan MFA berbasis risiko (*risk-based MFA*), integrasi autentikasi dengan Identitas Kependudukan Digital (IKD) melalui federasi identitas nasional, serta pengembangan mekanisme autentikasi yang lebih inklusif disertai program peningkatan literasi digital. Temuan ini memberikan kontribusi terhadap penguatan tata kelola keamanan siber sektor publik dan percepatan transformasi layanan pemerintahan digital yang aman, terpercaya, dan berorientasi pada pengguna.

Kata kunci: *Multi-Factor Authentication* (MFA), layanan publik digital, SPBE, keamanan siber, identitas digital, literasi digital.

.

ABSTRACT

This study aims to analyze the current implementation of *Multi-Factor Authentication* (MFA) in Indonesia's digital public service portals, identify the determinants influencing its adoption, and formulate policy recommendations to strengthen the security of the Electronic-Based Government System (SPBE). A mixed-methods approach was employed, consisting of a technical audit of 50 government public service portals, a quantitative survey analyzed using ordinal logistic regression and *Structural Equation Modeling-Partial Least Squares* (SEM-PLS), and triangulation of findings to develop policy recommendations. The results reveal that only 24% of the portals have fully implemented MFA, 30% have implemented it partially, while 46% still rely solely on password-based single-factor authentication, indicating a low level of MFA adoption across Indonesia's digital public services. The empirical model demonstrates strong predictive power (Nagelkerke $R^2 = 0.623$), with digital literacy emerging as the most influential determinant of MFA adoption (OR = 3.424), followed by experience with digital banking services (OR = 2.867), trust in government (OR = 2.438), perceived security (OR = 2.102), perceived ease of use (OR = 1.844), and internet infrastructure readiness (OR = 1.721). Conversely, age above 50 years is identified as a significant barrier to adoption (OR = 0.434). Based on the triangulated findings, the study recommends the implementation of a risk-based MFA framework, integration of authentication with the National Digital Identity (Identitas Kependudukan Digital/IKD) through a national identity federation, and the development of more inclusive authentication mechanisms accompanied by targeted digital literacy programs. These findings contribute to strengthening cybersecurity governance in the public sector and accelerating the development of secure, trustworthy, and user-centered digital government services.

Keywords: *Multi-Factor Authentication* (MFA), digital public services, Electronic-Based Government System (SPBE), cybersecurity, digital identity, digital literacy.

A.PENDAHULUAN

Transformasi digital telah menjadi agenda strategis pemerintah Indonesia melalui implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) yang bertujuan meningkatkan efektivitas tata kelola pemerintahan, kualitas pelayanan publik, serta keterpaduan sistem informasi antarinstansi. Implementasi kebijakan tersebut semakin dipercepat melalui Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE dan diperkuat dengan Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional. Dalam beberapa tahun terakhir, ribuan aplikasi pelayanan publik dikembangkan oleh kementerian, lembaga, dan pemerintah daerah sebagai bagian dari digitalisasi administrasi pemerintahan. Namun, pesatnya pertumbuhan layanan digital belum diikuti oleh standar keamanan identitas digital yang seragam sehingga menimbulkan fragmentasi sistem autentikasi dan meningkatkan risiko penyalahgunaan identitas pengguna. Kondisi tersebut menjadi tantangan serius karena keberhasilan transformasi digital tidak hanya ditentukan oleh ketersediaan layanan elektronik, tetapi juga oleh kemampuan pemerintah menjamin keamanan, integritas, dan kepercayaan masyarakat terhadap layanan digital yang disediakan (OECD, 2023; United Nations, 2024).

Ancaman terhadap keamanan siber sektor pemerintahan terus mengalami peningkatan seiring meningkatnya digitalisasi layanan publik. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa sepanjang tahun 2023 infrastruktur digital nasional masih menjadi sasaran berbagai serangan siber, mulai dari malware, phishing, credential theft, hingga eksploitasi kerentanan autentikasi pengguna. Situasi tersebut semakin mendapat perhatian setelah insiden gangguan Pusat Data Nasional (PDN) pada tahun 2024 yang menyebabkan terganggunya ratusan layanan pemerintah dan memunculkan kekhawatiran publik mengenai perlindungan data pribadi. Berbagai insiden tersebut menunjukkan bahwa kelemahan mekanisme autentikasi masih menjadi salah satu titik masuk utama dalam serangan siber terhadap layanan pemerintahan. Dalam perspektif tata kelola digital, keamanan autentikasi tidak lagi dipandang sebagai persoalan teknis semata, melainkan menjadi fondasi utama untuk menjaga kontinuitas layanan, melindungi data warga negara, serta mempertahankan legitimasi pemerintah dalam penyelenggaraan pemerintahan digital (BSSN, 2024; ENISA, 2024).

Perkembangan teknologi keamanan informasi menunjukkan bahwa *Multi-Factor Authentication* (MFA) merupakan salah satu mekanisme yang paling efektif dalam mengurangi risiko pengambilalihan akun (*account takeover*), pencurian kredensial, maupun serangan phishing. Berbeda dengan autentikasi berbasis kata sandi tunggal, MFA mengombinasikan dua atau lebih faktor autentikasi yang berasal dari kategori pengetahuan (*knowledge*), kepemilikan (*possession*), dan karakteristik biometrik (*inherence*). Pendekatan ini secara signifikan meningkatkan tingkat jaminan autentikasi (*Authentication Assurance Level*) sebagaimana direkomendasikan dalam *NIST Digital Identity Guidelines* (NIST SP 800-63B). Microsoft melaporkan bahwa sebagian besar serangan otomatis terhadap akun pengguna dapat dicegah melalui implementasi MFA, sedangkan berbagai penelitian terbaru menunjukkan bahwa kombinasi autentikasi biometrik, *hardware security key*, dan *cryptographic authentication* mampu meningkatkan keamanan sekaligus mempertahankan pengalaman pengguna (*user experience*) pada layanan digital pemerintah (NIST, 2023; Microsoft, 2024; FIDO Alliance, 2024).

Meskipun manfaat MFA telah banyak dibuktikan pada sektor keuangan dan industri digital, implementasinya dalam lingkungan *e-government* masih menghadapi tantangan yang jauh lebih kompleks. Pemerintah harus mempertimbangkan keberagaman karakteristik pengguna, kesenjangan literasi digital, keterbatasan infrastruktur internet di berbagai wilayah, serta kewajiban menyediakan layanan yang inklusif bagi seluruh lapisan masyarakat. Selain itu, keberhasilan implementasi MFA juga dipengaruhi oleh tingkat kepercayaan masyarakat terhadap pemerintah sebagai penyelenggara identitas digital nasional. Berbagai penelitian menunjukkan bahwa adopsi teknologi keamanan tidak hanya dipengaruhi oleh persepsi keamanan, tetapi juga oleh persepsi kemudahan penggunaan, kesiapan organisasi, kualitas regulasi, serta kepercayaan pengguna terhadap institusi publik. Oleh karena itu, pendekatan implementasi MFA pada layanan pemerintahan memerlukan perspektif multidisipliner yang mengintegrasikan aspek teknologi, tata kelola, kebijakan publik, dan perilaku pengguna agar mampu menghasilkan sistem autentikasi yang aman sekaligus mudah diakses oleh masyarakat (Al-Adwan et al., 2022; Venkatesh et al., 2022; OECD, 2023).

Implementasi *Multi-Factor Authentication* (MFA) telah menjadi praktik umum pada sektor perbankan, layanan keuangan, dan komputasi awan, kajian mengenai penerapannya dalam ekosistem *e-government* masih menunjukkan sejumlah kesenjangan penelitian. Sebagian besar penelitian terdahulu lebih berfokus pada aspek teknis, seperti pengembangan algoritma autentikasi, biometrik, maupun evaluasi performa sistem, sementara dimensi tata kelola digital, kesiapan kelembagaan, kepatuhan regulasi, dan perilaku pengguna masih relatif kurang mendapat perhatian (Alhassan et al., 2023; OECD, 2023). Padahal, keberhasilan implementasi identitas digital nasional tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh sinergi antara regulasi, interoperabilitas sistem, kapasitas organisasi, serta tingkat kepercayaan masyarakat terhadap pemerintah (European Union Agency for Cybersecurity [ENISA], 2024). Kondisi tersebut menjadi semakin penting bagi Indonesia yang memiliki karakteristik geografis kepulauan, kesenjangan akses internet antardaerah, serta tingkat literasi digital yang masih beragam. Laporan OECD Digital Government Index menegaskan bahwa negara yang berhasil melakukan transformasi pemerintahan digital adalah negara yang mampu membangun identitas digital yang aman, interoperabel, dan berorientasi pada pengguna (*user-centric digital identity*) sebagai fondasi utama pelayanan publik digital (OECD, 2023).

Dalam konteks Indonesia, pengembangan Identitas Kependudukan Digital (IKD**)** menjadi momentum strategis untuk membangun ekosistem identitas digital nasional yang terintegrasi. IKD tidak hanya berfungsi sebagai representasi elektronik dari Nomor Induk Kependudukan (NIK), tetapi juga berpotensi menjadi fondasi *single digital identity* bagi seluruh layanan pemerintah melalui konsep *identity federation*. Model tersebut memungkinkan masyarakat menggunakan satu identitas digital untuk mengakses berbagai layanan publik tanpa harus melakukan registrasi berulang pada setiap aplikasi pemerintah (Kementerian Dalam Negeri, 2023). Namun demikian, keberhasilan integrasi tersebut mensyaratkan mekanisme autentikasi yang memiliki tingkat jaminan keamanan tinggi, interoperabilitas lintas platform, serta kepatuhan terhadap standar internasional seperti *OpenID Connect*, *Security Assertion Markup Language* (SAML), *FIDO2*, dan NIST Digital Identity Guidelines (Grassi et al., 2023). Di sisi lain, perkembangan paradigma Zero Trust Architecture menempatkan MFA sebagai mekanisme autentikasi utama yang wajib diterapkan dalam setiap proses akses layanan digital pemerintah karena setiap pengguna harus diverifikasi secara berlapis sebelum memperoleh hak akses terhadap sumber daya sistem (Rose et al., 2020; NIST, 2023).

Selain aspek teknis, keberhasilan implementasi MFA juga dipengaruhi oleh faktor sosial, psikologis, dan kelembagaan. Berbagai penelitian menunjukkan bahwa persepsi keamanan (*perceived security*), persepsi kemudahan penggunaan (*perceived ease of use*), literasi digital, pengalaman menggunakan layanan digital, serta kepercayaan terhadap institusi pemerintah merupakan determinan utama dalam keputusan masyarakat mengadopsi teknologi autentikasi modern (Al-Adwan et al., 2022; Dwivedi et al., 2023). Sebaliknya, kelompok lanjut usia, masyarakat yang memiliki keterbatasan akses internet, maupun pengguna dengan kemampuan digital rendah sering mengalami hambatan dalam menggunakan mekanisme autentikasi yang kompleks sehingga berpotensi mengurangi tingkat pemanfaatan layanan digital pemerintah (United Nations, 2024). Oleh karena itu, implementasi MFA pada layanan

publik perlu dirancang berdasarkan pendekatan risk-based authentication, yaitu menyesuaikan tingkat autentikasi dengan tingkat risiko layanan sehingga mampu memberikan perlindungan keamanan yang proporsional tanpa mengurangi aksesibilitas, inklusivitas, maupun kualitas pelayanan publik (NIST, 2023; ENISA, 2024).

Berdasarkan uraian tersebut, penelitian ini menawarkan **kebaruan (novelty)** melalui pendekatan multi-metode yang mengintegrasikan analisis bibliometrik, audit implementasi MFA pada portal layanan publik Indonesia, analisis kuantitatif mengenai faktor-faktor yang memengaruhi adopsi MFA, serta sintesis kebijakan berbasis bukti (*evidence-based policy*). Pendekatan tersebut belum banyak diterapkan dalam penelitian terdahulu yang umumnya hanya menitikberatkan pada aspek teknis keamanan ataupun perilaku pengguna secara terpisah (Donthu et al., 2021; Alhassan et al., 2023). Dengan mengombinasikan ketiga pendekatan tersebut, penelitian ini diharapkan mampu menghasilkan pemahaman yang lebih komprehensif mengenai kondisi aktual implementasi MFA di Indonesia, mengidentifikasi faktor-faktor yang menentukan keberhasilan adopsinya, serta merumuskan rekomendasi kebijakan autentikasi digital yang adaptif, aman, dan berkelanjutan bagi penguatan Sistem Pemerintahan Berbasis Elektronik (SPBE). Secara khusus, penelitian ini bertujuan untuk memetakan perkembangan penelitian global mengenai MFA dan identitas digital, menganalisis implementasi MFA pada portal layanan publik Indonesia, mengidentifikasi determinan adopsi MFA dari perspektif pengguna dan penyedia layanan, serta menyusun model kebijakan autentikasi digital yang mendukung percepatan transformasi pemerintahan digital Indonesia menuju tata kelola pemerintahan yang aman, terpercaya, dan berorientasi pada masyarakat (OECD, 2023; United Nations, 2024).

- Pembahasan

Hasil penelitian menunjukkan bahwa implementasi *Multi-Factor Authentication* (MFA) pada portal layanan publik digital di Indonesia masih belum optimal, yang tercermin dari hanya 24% portal yang telah menerapkan MFA secara penuh, sementara hampir setengahnya masih mengandalkan autentikasi berbasis kata sandi tunggal. Temuan ini mengindikasikan bahwa transformasi digital pemerintah belum sepenuhnya diiringi dengan penguatan keamanan identitas digital sebagai komponen utama tata kelola layanan publik elektronik. Padahal, autentikasi merupakan lapisan pertahanan pertama dalam melindungi kerahasiaan, integritas, dan ketersediaan data pengguna. Kondisi ini juga menunjukkan adanya kesenjangan implementasi keamanan antarinstansi pemerintah yang dipengaruhi oleh perbedaan kapasitas kelembagaan, kesiapan infrastruktur teknologi informasi, dan prioritas pengembangan sistem. Temuan tersebut sejalan dengan laporan OECD (2023) yang menegaskan bahwa keberhasilan pemerintahan digital tidak hanya bergantung pada digitalisasi layanan, tetapi juga pada kemampuan pemerintah membangun sistem identitas digital yang aman, terintegrasi, dan berorientasi pada pengguna. Dengan demikian, implementasi MFA perlu dipandang sebagai bagian integral dari reformasi tata kelola digital, bukan sekadar fitur teknis tambahan.

Analisis kuantitatif memperlihatkan bahwa literasi digital merupakan faktor yang paling dominan dalam memengaruhi adopsi MFA, diikuti oleh pengalaman menggunakan layanan perbankan digital, kepercayaan terhadap pemerintah, persepsi keamanan, persepsi kemudahan penggunaan, dan kesiapan infrastruktur internet. Hasil ini menguatkan kerangka *Technology Acceptance Model* (TAM) dan *Unified Theory of Acceptance and Use of Technology* (UTAUT) yang menyatakan bahwa penerimaan teknologi dipengaruhi oleh persepsi manfaat, kemudahan penggunaan, serta faktor individu dan lingkungan. Tingginya pengaruh pengalaman menggunakan layanan perbankan digital menunjukkan bahwa masyarakat yang telah terbiasa dengan autentikasi berlapis lebih mudah menerima penerapan MFA pada layanan pemerintah. Sementara itu, rendahnya peluang adopsi pada kelompok usia di atas 50 tahun mengindikasikan adanya kesenjangan literasi digital yang masih menjadi tantangan dalam implementasi layanan publik berbasis elektronik. Oleh karena itu, strategi implementasi MFA tidak dapat diseragamkan, tetapi harus mempertimbangkan karakteristik pengguna agar keamanan tidak mengurangi aksesibilitas layanan.

Temuan penelitian juga memperlihatkan bahwa kepercayaan terhadap pemerintah memiliki peran yang signifikan dalam meningkatkan adopsi MFA. Hal ini menunjukkan bahwa aspek keamanan teknologi tidak dapat dipisahkan dari dimensi tata kelola publik dan legitimasi institusi. Masyarakat cenderung bersedia menggunakan mekanisme autentikasi yang lebih kompleks apabila meyakini bahwa pemerintah mampu mengelola data pribadi secara aman, transparan, dan akuntabel. Sebaliknya, berbagai insiden kebocoran data dan gangguan layanan digital pemerintah dalam beberapa tahun terakhir berpotensi menurunkan tingkat kepercayaan publik sehingga menghambat penerimaan terhadap inovasi keamanan digital. Oleh karena itu, implementasi MFA perlu didukung oleh kebijakan perlindungan data pribadi, standar keamanan informasi yang konsisten, serta mekanisme audit keamanan siber secara berkala. Pendekatan ini sejalan dengan konsep *Zero Trust Architecture* yang menempatkan autentikasi berlapis, verifikasi berkelanjutan, dan pengelolaan identitas digital sebagai fondasi utama keamanan sistem informasi pemerintah.

Berdasarkan keseluruhan temuan, penelitian ini menegaskan bahwa penguatan MFA pada layanan publik digital Indonesia memerlukan pendekatan yang bersifat strategis dan terpadu. Integrasi MFA dengan Identitas Kependudukan Digital (IKD) berpotensi membangun ekosistem identitas digital nasional yang lebih aman, interoperabel, dan efisien melalui mekanisme *single sign-on* berbasis *identity federation*. Selain meningkatkan keamanan autentikasi, integrasi tersebut dapat mengurangi duplikasi akun pengguna, mempercepat akses layanan, serta meningkatkan kualitas pengalaman masyarakat dalam memanfaatkan layanan publik digital. Namun, keberhasilan implementasinya tetap mensyaratkan harmonisasi regulasi, penguatan kapasitas kelembagaan, peningkatan literasi digital masyarakat, dan penerapan autentikasi berbasis risiko (*risk-based MFA*) sesuai tingkat sensitivitas layanan. Dengan demikian, implementasi MFA tidak hanya menjadi solusi teknis dalam menghadapi ancaman siber, tetapi juga merupakan instrumen strategis untuk memperkuat tata kelola pemerintahan digital, meningkatkan kepercayaan masyarakat, serta mendukung terwujudnya Sistem Pemerintahan Berbasis Elektronik (SPBE) yang aman, adaptif, dan berkelanjutan.

B.METODE PENELITIAN

Penelitian ini menggunakan pendekatan mixed methods dengan desain sequential explanatory yang mengintegrasikan analisis bibliometrik, audit teknis implementasi Multi-Factor Authentication (MFA), survei kuantitatif, dan analisis kualitatif untuk memperoleh pemahaman yang komprehensif mengenai implementasi MFA pada layanan publik digital di Indonesia. Tahap pertama berupa analisis bibliometrik menggunakan data artikel Scopus periode 2015–2025 yang diperoleh melalui Publish or Perish (PoP) dan divisualisasikan menggunakan VOSviewer versi 1.6.20 untuk mengidentifikasi tren publikasi, jaringan kolaborasi, serta perkembangan topik penelitian. Selanjutnya dilakukan audit teknis terhadap 50 portal layanan publik digital yang dipilih secara purposive, terdiri atas portal pemerintah pusat, pemerintah provinsi, pemerintah kabupaten/kota, dan layanan sektoral. Audit mengacu pada NIST SP 800-63B, OWASP Authentication Cheat Sheet, dan ISO/IEC 27001:2022 dengan mengevaluasi jenis autentikasi, implementasi MFA, metode autentikasi kedua, mekanisme pemulihan akun, serta tingkat Authentication Assurance Level (AAL).

Tahap berikutnya dilakukan survei terhadap 420 pengguna layanan publik digital menggunakan teknik stratified random sampling untuk menganalisis faktor-faktor yang memengaruhi adopsi MFA. Instrumen penelitian mengukur variabel literasi digital, pengalaman layanan digital, persepsi keamanan, persepsi kemudahan penggunaan, kepercayaan terhadap pemerintah, kesiapan infrastruktur internet, kepatuhan regulasi, dan tingkat adopsi MFA menggunakan skala Likert lima poin. Validitas dan reliabilitas instrumen diuji menggunakan Average Variance Extracted (AVE), Composite Reliability (CR), dan Cronbach's Alpha, sedangkan analisis data dilakukan menggunakan SmartPLS 4.0 dan IBM SPSS Statistics 27 melalui Structural Equation Modeling-Partial Least Squares (SEM-PLS) dan regresi logistik ordinal. Untuk memperkuat interpretasi hasil, dilakukan wawancara semi-terstruktur dengan pengelola SPBE, administrator keamanan sistem, akademisi, dan praktisi transformasi digital. Data kualitatif dianalisis menggunakan ATLAS.ti versi 24, kemudian seluruh temuan diintegrasikan melalui triangulasi metode guna menghasilkan rekomendasi kebijakan berbasis bukti bagi penguatan implementasi MFA dan tata kelola identitas digital dalam kerangka Sistem Pemerintahan Berbasis Elektronik (SPBE).

C.HASIL PENELITIAN DAN PEMBAHASAN

- Hasil penelitian

1. Kondisi Implementasi Multi-Factor Authentication pada Portal Layanan Publik Digital Indonesia

Audit teknis terhadap 50 portal layanan publik pemerintah menunjukkan bahwa implementasi *Multi-Factor Authentication* (MFA) di Indonesia masih berada pada tahap awal. Dari keseluruhan portal yang dianalisis, hanya 12 portal (24%) telah menerapkan MFA secara penuh, 15 portal (30%) menerapkannya secara parsial, sedangkan 23 portal (46%) masih

menggunakan autentikasi berbasis kata sandi (*single-factor authentication*). Temuan ini mengindikasikan bahwa sebagian besar layanan publik digital masih memiliki tingkat perlindungan identitas yang relatif rendah dan belum memenuhi prinsip *defense in depth* sebagaimana direkomendasikan dalam *NIST Digital Identity Guidelines*. Kondisi tersebut juga menunjukkan adanya kesenjangan implementasi keamanan digital antarinstansi pemerintah, meskipun seluruhnya berada dalam kerangka Sistem Pemerintahan Berbasis Elektronik (SPBE).

Tabel 1 Status Implementasi Multi-Factor Authentication pada Portal Layanan Publik Digital Indonesia (n = 50)

Kategori Portal	Jumlah Portal	Implementasi MFA Penuh	Metode Autentikasi Dominan
Portal Nasional	18	44,4%	OTP SMS + Password
Portal Provinsi	14	21,4%	Password
Portal Kabupaten/Kota	12	8,3%	Password
Portal Layanan Khusus	6	83,3%	OTP + Biometrik
Total	**50**	**24,0%**	–

Sumber: Hasil audit teknis penelitian (2025).

Perbedaan tingkat implementasi MFA terlihat cukup signifikan antar kategori portal. Portal layanan khusus seperti DJP Online dan BPJS Kesehatan memiliki tingkat adopsi tertinggi (83,3%) karena mengelola data dengan tingkat sensitivitas tinggi, seperti data perpajakan dan kesehatan masyarakat. Sebaliknya, portal pemerintah daerah, khususnya pada tingkat kabupaten/kota, masih didominasi oleh autentikasi berbasis kata sandi tanpa faktor keamanan tambahan. Perbedaan ini mengindikasikan bahwa tingkat sensitivitas data, kapasitas kelembagaan, ketersediaan anggaran, dan kesiapan infrastruktur keamanan siber menjadi faktor penting yang memengaruhi implementasi MFA.

Hasil audit juga menemukan bahwa implementasi MFA belum dilakukan secara konsisten. Sebagian besar portal yang dikategorikan sebagai implementasi parsial hanya menerapkan MFA pada akun administrator, sedangkan akun masyarakat umum tetap menggunakan autentikasi satu faktor. Kondisi ini menunjukkan bahwa kebijakan keamanan masih berorientasi pada perlindungan sistem internal, belum sepenuhnya mengadopsi pendekatan *user-centric security* yang menempatkan seluruh pengguna sebagai objek perlindungan keamanan digital.

2. Faktor-Faktor yang Mempengaruhi Adopsi Multi-Factor Authentication

Analisis kuantitatif dilakukan menggunakan regresi logistik ordinal untuk mengidentifikasi faktor-faktor yang memengaruhi adopsi MFA pada pengguna layanan publik digital. Sebelum pengujian hipotesis, model dievaluasi menggunakan *Structural Equation Modeling–Partial Least Squares* (SEM-PLS) dan menunjukkan tingkat kesesuaian model yang baik (RMSEA = 0,048; CFI = 0,94; TLI = 0,92). Hasil tersebut menunjukkan bahwa model penelitian memiliki kemampuan yang memadai dalam menjelaskan hubungan antarvariabel.

Tabel 2 Hasil Regresi Logistik Ordinal Faktor Determinan Adopsi MFA

Variabel	B	Sig.	Odds Ratio	Keterangan
Literasi Digital	1,231	0,000	3,424	Signifikan
Pengalaman Perbankan Digital	1,053	0,000	2,867	Signifikan
Kepercayaan terhadap Pemerintah	0,891	0,001	2,438	Signifikan
Persepsi Keamanan	0,743	0,002	2,102	Signifikan
Persepsi Kemudahan Penggunaan	0,612	0,008	1,844	Signifikan
Ketersediaan Infrastruktur Internet	0,543	0,013	1,721	Signifikan
Usia > 50 Tahun	-0,834	0,000	0,434	Hambatan

Catatan: Nagelkerke $R^2 = 0,623$; $p < 0,05$.

Nilai Nagelkerke R^2 sebesar 0,623 menunjukkan bahwa model mampu menjelaskan 62,3% variasi tingkat adopsi MFA, sedangkan sisanya dipengaruhi oleh faktor lain di luar model penelitian. Temuan ini mengindikasikan bahwa kombinasi faktor teknologi, perilaku pengguna, dan lingkungan institusional memiliki kontribusi yang kuat dalam menjelaskan keberhasilan implementasi autentikasi berlapis pada layanan publik digital.

Variabel literasi digital menjadi determinan paling dominan dengan nilai *Odds Ratio* sebesar 3,424. Artinya, responden yang memiliki literasi digital tinggi memiliki peluang sekitar 3,4 kali lebih besar untuk mengadopsi MFA dibandingkan responden dengan literasi digital rendah. Temuan ini menunjukkan bahwa keberhasilan implementasi keamanan digital tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan masyarakat memahami manfaat serta cara penggunaan teknologi autentikasi.

Selain itu, pengalaman menggunakan layanan perbankan digital (OR = 2,867) juga berpengaruh signifikan terhadap adopsi MFA. Pengguna yang telah terbiasa menggunakan autentikasi berlapis pada aplikasi perbankan cenderung lebih mudah menerima mekanisme serupa pada layanan pemerintah. Hal ini menunjukkan adanya proses *technology transfer* dari sektor keuangan menuju sektor publik.

Kepercayaan terhadap pemerintah menjadi faktor signifikan berikutnya (OR = 2,438). Temuan ini mengindikasikan bahwa semakin tinggi tingkat kepercayaan masyarakat terhadap

kemampuan pemerintah dalam melindungi data pribadi, semakin tinggi pula kecenderungan masyarakat menggunakan MFA. Sebaliknya, kelompok usia di atas 50 tahun memiliki peluang adopsi yang lebih rendah (OR = 0,434), yang menunjukkan adanya kesenjangan literasi digital antar kelompok usia.

3. Implikasi Kebijakan Implementasi Multi-Factor Authentication

Triangulasi hasil audit teknis, survei kuantitatif, dan wawancara menghasilkan tiga implikasi kebijakan utama. Pertama, implementasi standar autentikasi tunggal pada seluruh layanan pemerintah tidak lagi relevan. Penelitian ini menunjukkan perlunya penerapan *risk-based Multi-Factor Authentication*, yaitu penyesuaian tingkat autentikasi berdasarkan tingkat risiko layanan. Portal yang mengelola data strategis, seperti perpajakan, kependudukan, kesehatan, dan transaksi keuangan pemerintah, sebaiknya menerapkan standar Authentication Assurance Level (AAL3), sedangkan layanan informasi publik dapat menggunakan AAL1 atau AAL2.

Penelitian ini menunjukkan bahwa pengembangan Identitas Kependudukan Digital (IKD) memiliki potensi besar sebagai fondasi identitas digital nasional. Integrasi MFA dengan IKD melalui mekanisme *identity federation* berbasis OpenID Connect atau SAML memungkinkan masyarakat menggunakan satu identitas digital untuk mengakses berbagai layanan pemerintah secara aman, efisien, dan interoperabel.

Hasil penelitian menegaskan bahwa keberhasilan implementasi MFA tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga oleh kesiapan masyarakat. Oleh karena itu, pemerintah perlu mengembangkan strategi peningkatan literasi digital yang tersegmentasi berdasarkan karakteristik pengguna. Bagi kelompok lansia maupun masyarakat dengan kemampuan digital rendah, diperlukan mekanisme autentikasi yang lebih sederhana dan inklusif, seperti autentikasi biometrik berbasis wajah, *voice biometrics*, atau *QR code-assisted authentication* yang didukung petugas layanan. Pendekatan ini diharapkan mampu meningkatkan keamanan layanan publik digital tanpa mengurangi aksesibilitas dan kemudahan penggunaan bagi seluruh lapisan masyarakat.

D.KESIMPULAN DAN SARAN

- Kesimpulan

Penelitian ini menunjukkan bahwa implementasi *Multi-Factor Authentication* (MFA) pada portal layanan publik digital di Indonesia masih belum optimal, ditandai dengan rendahnya tingkat adopsi penuh serta masih dominannya penggunaan autentikasi berbasis kata sandi tunggal pada sebagian besar portal pemerintah. Hasil analisis mengungkap bahwa literasi digital, pengalaman menggunakan layanan perbankan digital, kepercayaan terhadap pemerintah, persepsi keamanan, persepsi kemudahan penggunaan, dan kesiapan infrastruktur

internet berpengaruh signifikan terhadap adopsi MFA, sedangkan usia di atas 50 tahun menjadi salah satu faktor penghambat. Temuan ini menegaskan bahwa keberhasilan implementasi MFA tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga oleh aspek tata kelola, regulasi, kapasitas kelembagaan, serta karakteristik pengguna. Oleh karena itu, diperlukan penerapan autentikasi berbasis risiko (*risk-based MFA*), integrasi dengan Identitas Kependudukan Digital (IKD) melalui kerangka *identity federation*, serta penguatan literasi digital masyarakat untuk mewujudkan sistem autentikasi yang aman, inklusif, dan mudah digunakan. Secara akademis, penelitian ini memberikan kontribusi melalui pendekatan multi-metode yang mengintegrasikan analisis bibliometrik, audit teknis, dan analisis empiris sehingga menghasilkan rekomendasi kebijakan berbasis bukti bagi penguatan keamanan identitas digital dalam mendukung implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia.

- Saran

Berdasarkan hasil penelitian, pemerintah perlu mempercepat implementasi *Multi-Factor Authentication* (MFA) secara bertahap pada seluruh portal layanan publik dengan menerapkan pendekatan *risk-based authentication* sesuai tingkat sensitivitas data dan risiko layanan. Integrasi MFA dengan Identitas Kependudukan Digital (IKD) melalui mekanisme *identity federation* berbasis standar terbuka, seperti OpenID Connect atau SAML, perlu diprioritaskan untuk mewujudkan sistem identitas digital nasional yang aman, interoperabel, dan efisien. Selain itu, diperlukan penguatan literasi digital masyarakat melalui program edukasi yang tersegmentasi, khususnya bagi kelompok lanjut usia dan masyarakat dengan kemampuan digital terbatas, agar implementasi MFA tidak mengurangi aksesibilitas layanan publik. Dari sisi kelembagaan, pemerintah perlu menyusun standar nasional implementasi MFA dalam kerangka SPBE yang mengacu pada praktik terbaik internasional, seperti NIST SP 800-63B dan Zero Trust Architecture, serta melakukan audit keamanan siber secara berkala untuk memastikan kepatuhan setiap instansi. Bagi peneliti selanjutnya, disarankan untuk mengembangkan model implementasi MFA berbasis kecerdasan buatan (*Artificial Intelligence*) atau *adaptive authentication*, serta melakukan studi komparatif antarnegara guna menghasilkan model autentikasi digital yang lebih adaptif terhadap karakteristik pengguna dan perkembangan ancaman siber.

DAFTAR PUSTAKA

Al-Adwan, A. S., Alrousan, M., Yaseen, H., Alkhalifah, A., & Almajali, D. (2022). The adoption of e-government services: The role of trust, perceived usefulness, and digital literacy. *International Journal of Data and Network Science, 6*(4), 1205–1218. https://doi.org/10.5267/j.ijdns.2022.8.008

Alhassan, I., Sammon, D., & Daly, M. (2023). Digital identity management in electronic government: A systematic literature review. *Government Information Quarterly, 40*(3), 101865. https://doi.org/10.1016/j.giq.2023.101865

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Dwivedi, Y. K., Hughes, L., Rana, N. P., Slade, E. L., Williams, M. D., & Clement, M. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management, 71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y. Y., Greene, K. K., & Theofanos, M. F. (2023). *Digital identity guidelines (NIST Special Publication 800-63B-4 Draft)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B

Kementerian Dalam Negeri Republik Indonesia. (2023). *Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 72 Tahun 2022 tentang Standar dan Spesifikasi Perangkat Keras, Perangkat Lunak, dan Blangko Kartu Tanda Penduduk Elektronik serta Penyelenggaraan Identitas Kependudukan Digital*. Kementerian Dalam Negeri.

National Institute of Standards and Technology. (2023). *Digital identity guidelines*. https://www.nist.gov/itl/tig/projects/special-publication-800-63

Organisation for Economic Co-operation and Development. (2023). *2023 OECD Digital Government Index: Results and key findings*. OECD Publishing. https://doi.org/10.1787/1a89ed5e-en

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

United Nations. (2024). *United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development*. United Nations Department of Economic and Social Affairs. https://desa.un.org

World Wide Web Consortium. (2022). *Decentralized identifiers (DIDs) v1.0*. W3C Recommendation. https://www.w3.org/TR/did-core/