Impression: Jurnal Teknologi dan Informas, Vol. 4 (2) (2025)
Published by: Lembaga Riset Ilmiah – YMMA Sumut
Impression: Jurnal Teknologi dan Informasi
Journal homepage: https://jurnal.risetilmiah.ac.id/index.php/jti

Analisis Persepsi Pengguna terhadap MFA pada Aplikasi SAKTI Berdasarkan TAM

Grace Anne Sheila Herman[1], Theodorus Sendjaja[2]
Program Studi Manajemen, Perbanas Institute, Indonesia

ARTICLEINFO

Article history:
Received: 27 September 2025
Revised: 10 Oktober 2025
Accepted: 20 November 2025

Keywords:
Multi-Factor Authentication (MFA),
Technology Acceptance Model (TAM),
Perceived Security,
PLS-SEM,
SAKTI.

Published by
Impression : Jurnal Teknologi dan Informasi
Copyright © 2025 by the Author(s) |This is an open-access article distributed under the Creative Commons Attribution which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
https://creativecommons.org/licenses/by/4.0/

ABSTRACT

Penelitian ini menganalisis penerimaan Multi-Factor Authentication (MFA) pada aplikasi SAKTI dengan kerangka Technology Acceptance Model (TAM) yang diperluas oleh Perceived Security (PS). Analisis menggunakan PLS-SEM untuk mengevaluasi model pengukuran dan model struktural. Survei potong lintang terhadap 69 pengguna dilakukan sebagai dasar analisis. Hasil menunjukkan PS berpengaruh kuat terhadap Perceived Usefulness (PU) dan Perceived Ease of Use (PEOU), dengan signifikansi tinggi ($p < 0{,}001$), sementara PU dan PEOU membentuk sikap terhadap MFA (ATT) secara positif, keduanya signifikan (PU: $p = 0{,}010$; PEOU: $p = 0{,}011$), sedangkan hubungan langsung PEOU ke PU tidak terbukti ($p = 0{,}870$). Temuan ini menegaskan PS sebagai variabel eksternal kunci yang memperkaya penerapan TAM pada konteks penggunaan wajib di sektor publik. Persepsi pengguna menegaskan bahwa MFA dipandang meningkatkan perlindungan akun dan data, namun sebagian masih merasakan kendala penggunaan berupa waktu tambahan, ketergantungan perangkat, serta proses pemulihan yang belum mulus. Untuk meningkatkan penerimaan, kebijakan penguatan keamanan perlu disertai pengurangan kendala penggunaan dan perbaikan pengalaman pemulihan, agar keseimbangan antara keamanan dan kemudahan tercapai sehingga kemanfaatan dan kemudahan yang dirasakan mendorong terbentuknya sikap positif terhadap MFA yang wajib di aplikasi SAKTI.

This study analyzes user acceptance of Multi-Factor Authentication (MFA) in the SAKTI application using the Technology Acceptance Model (TAM) extended with Perceived Security (PS). PLS-SEM was employed to evaluate the measurement and structural models. A cross-sectional survey of 69 users provided the empirical basis. The results show that PS strongly influences Perceived Usefulness (PU) and Perceived Ease of Use (PEOU), with high significance ($p < 0.001$), while PU and PEOU positively shape attitudes toward MFA (ATT), both significant (PU: $p = 0.010$; PEOU: $p = 0.011$). In contrast, the direct relationship from PEOU to PU is not supported ($p = 0.870$). These findings position PS as a key external variable that enriches the application of TAM in mandatory-use settings within the public sector. User perceptions indicate that MFA is seen as enhancing account and data protection, although some still experience usage constraints such as additional time at login, device dependence, and recovery processes that are not yet seamless. To improve acceptance, security-strengthening policies should be accompanied by reductions in usage constraints and improvements in recovery experience, so that a balance between security and ease is achieved and perceived usefulness and ease foster more positive attitudes toward mandatory MFA in SAKTI.

Corresponding Author:
Theodorus Sendjaja
Program Studi Manajemen, Perbanas Institute, Indonesia
Jl. Perbanas, Karet Kuningan, Setiabudi, Jakarta, 12940, Indonesia
Email: theodorus.sendjaja@perbanas.id

PENDAHULUAN

Perkembangan sistem informasi telah mengubah tata kelola organisasi dari mulai cara organisasi melakukan pengolahan data, menjalankan operasional, hingga pengambilan keputusan strategis untuk mencapai tujuan organisasi. Laudon dan Laudon, pada bukunya yang berjudul Management Information Systems menyampaikan bahwa sistem dan teknologi informasi menjadi instrumen utama untuk meningkatkan efisiensi dalam rangka mencapai profitabilitas yang lebih tinggi, terutama jika selaras dengan perubahan praktik bisnis dan perilaku manajemen. (Laudon & Laudon, 2014).

Seiring dengan perkembangan sistem informasi, teknologi informasi sebagai penunjang

berjalannya sistem informasi juga semakin berkembang dan kompleks. Teknologi informasi tidak hanya menjadi alat tetapi juga suatu instrumen yang berperan untuk melakukan pengelolaan, penyimpanan, sampai dengan pengamanan informasi. Oleh karena itu, suatu organisasi perlu adaptif untuk terus mengikuti perkembangan teknologi informasi.

Pemanfaatan teknologi informasi tidak hanya pada sektor swasta, tetapi juga dalam sektor publik. Sejalan dengan Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), penguatan kontrol akses menjadi keharusan pada aplikasi keuangan negara, termasuk SAKTI. SAKTI adalah aplikasi terintegrasi untuk pengelolaan keuangan negara yang mencakup perencanaan, pelaksanaan anggaran, dan pelaporan, serta digunakan secara luas pada satuan kerja Kementerian/Lembaga (K/L). Untuk mencapai tujuan SPBE berupa tata kelola yang akuntabel serta integritas dan keamanan data, penyelenggaraan sistem harus didukung oleh kontrol identitas yang kuat. Ini akan menjaga kelangsungan operasi sistem dan memastikan integritas data. Klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya juga dilakukan melalui kontrol identitas dan akses, termasuk mekanisme autentikasi berlapis (MFA).

Pemerintah telah menjadi target para peretas, sebagai contoh adalah adanya kebocoran data kredensial layanan .go.id, serangan *ransomware* terhadap Pusat Data Nasional, kebocoran data NPWP, dan masih banyak kasus lainnya. Peristiwa ini dapat memberikan dampak serius terhadap kepercayaan masyarakat terhadap keamanan penyelenggaraan sistem informasi di pemerintahan. Di sisi lain, aplikasi SAKTI mencakup modul penganggaran, komitmen, pembayaran, dan pelaporan yang berisi data sensitif. Kebocoran atau manipulasi data pada aplikasi ini dapat menimbulkan risiko kerugian finansial, gangguan pada operasional pengelolaan keuangan negara, serta menurunnya kepercayaan publik terhadap pemerintah. Kondisi ini memperkuat kebutuhan autentikasi berlapis pada SAKTI.

Pada penelitian terkait E-Government yang dilakukan oleh Hazineh, et al, terdapat beberapa tantangan dalam penerapan E-Government, yang salah satunya adalah faktor organisasi. Tantangan faktor organisasi merupakan kesiapan sumber daya manusia dalam organisasi yang mencakup kurangnya kualifikasi dan pelatihan, resistensi terhadap perubahan, serta keterbatasan kemampuan terkait teknologi informasi dan komunikasi (Hazineh et al., 2022). Tantangan penerapan E-Government tidak hanya pada faktor organisasi, tetapi juga faktor eksternal, yaitu kejahatan siber. Mushtaq, Shahrukh dan Mahmood Shah pada penelitiannya menyampaikan bahwa integrasi layanan digital pada pemerintahan memberikan manfaat namun menciptakan kerentanan baru, seperti ancaman siber yang menimbulkan kekhawatiran akan perlindungan data pribadi dan data sensitif (Mushtaq & Shah, 2025). Namun, penerimaan autentikasi, khususnya MFA pada lingkungan kerja sektor publik yang bersifat wajib masih relatif kurang dieksplorasi dibanding konteks swasta yang sukarela. Kesenjangan ini menjadi dasar pengujian penerimaan MFA pada SAKTI dalam konteks penggunaan wajib.

Salah satu cara untuk menjaga keamanan data suatu aplikasi adalah dengan adanya pengelolaan terhadap individu yang memiliki otoritas untuk mengakses aplikasi. Praktik ini biasa disebut dengan Identity and Access Management yang biasa disingkat IAM. Pada penelitiannya, Singh, et al menyampaikan bahwa IAM mencakup berbagai proses, kebijakan, dan teknologi untuk memantau akses pengguna serta mengelola identitas digital, guna meningkatkan keamanan data, mengendalikan hak akses dan menjaga aplikasi dari akses ilegal (Singh et al., 2023). Penelitian terbaru terkait IAM yang dilakukan oleh Ojo, Samson dan Allan Covey menyatakan pentingnya Multi-Factor Authentication (MFA) dan Single Sign-On (SSO) dalam proses autentikasi karena memiliki peran untuk memperkuat keamanan dan pengalaman pengguna (Ojo & Covey, 2025).

Kementerian Keuangan, sebagai pengampu aplikasi SAKTI, mulai menerapkan MFA untuk meningkatkan keamanan informasi dengan mengharuskan pengguna untuk memberikan dua atau lebih faktor verifikasi guna memperoleh akses ke aplikasi SAKTI. Kebijakan ini memastikan hanya pengguna yang sah yang memperoleh akses. Penerapan MFA dilaksanakan serentak untuk seluruh pengguna aplikasi SAKTI mulai Januari 2025. Latar belakang penerapan MFA tertuang pada Nota Dinas Direktur SITP nomor ND-812/PB.8/2024 hal Penguatan Kesadaran Keamanan Informasi dan Kewaspadaan DJPb Atas Kejadian Serangan PDNS Kominfo tanggal 1 Juli 2024 (Direktorat Jenderal Perbendaharaan Kementerian Keuangan, 2024). Pengetahuan mengenai persepsi pengguna terhadap penerapan MFA penting untuk menjadi dasar perbaikan pengalaman pengguna dan penguatan tata kelola keamanan.

Penelitian mengenai persepsi pengguna terhadap MFA masih terbatas. Pada tahun 2019, Das et

al. melakukan *literature review* terkait penelitian MFA sepanjang tahun 2018 yang menunjukkan bahwa hanya sekitar 9.1% studi mengenai evaluasi pengguna terkait MFA dan tercatat bahwa tingkat adopsi MFA cenderung rendah dan penghindaran teknologi ini sangat umum ketika pengguna diwajibkan menggunakannya (Das et al., 2019). Zimmermann et al. membandingkan persepsi pengguna atas tiga skema autentikasi, yaitu password, fingerprint, dan smartphone-based dalam empat layanan. Penelitian ini menemukan bahwa tingkat kegunaan dan preferensi tertinggi terdapat pada kata sandi, disusul sidik jari, dan terendah pada smartphone-based OTP. Smartphone-based adalah skema dimana aplikasi pada telepon genggam menghasilkan OTP/token. Skema ini tidak disukai karena alasan waktu dan kerumitan tambahan serta kebutuhan perangkat (smartphone) (Zimmermann et al., 2022). Selanjutnya, Amft et al. mengungkap bahwa prosedur pemulihan MFA pada banyak platform tidak ramah pengguna dan sering kali informasi bantuan yang diberikan salah, sehingga membuat pengguna semakin frustrasi dan menurunkan kepercayaan terhadap keamanan sistem (Amft et al., 2023). Penelitian-penelitian ini menegaskan bahwa pengalaman pengguna terhadap MFA yang buruk menjadi hambatan bagi penerimaan pengguna terhadap MFA, meskipun teknologi ini diakui memberikan tingkat keamanan yang lebih tinggi.

Walaupun MFA diwajibkan pada aplikasi SAKTI dalam rangka memperkuat keamanan, keberhasilan implementasinya tidak hanya ditentukan oleh aspek keamanan. Temuan-temuan sebelumnya menegaskan bahwa pengalaman dan penerimaan pengguna menjadi hal penting karena beban penggunaan seperti langkah tambahan, waktu login yang lebih panjang, ketergantungan pada perangkat ponsel, serta prosedur pemulihan yang sulit dapat menurunkan kemudahan dan sikap pengguna terhadap aplikasi. Untuk menjelaskan penerimaan teknologi oleh pengguna, penelitian ini menggunakan kerangka Technology Acceptance Model (TAM) untuk menjelaskan bagaimana kemudahan (Perceived Ease of Use/PEOU) dan kemanfaatan (Perceived Usefulness/PU) memengaruhi sikap pengguna terhadap MFA.

Berangkat dari temuan terdahulu, terdapat celah penelitian yang mana belum ditemukan kajian yang secara spesifik menilai persepsi pengguna terhadap MFA yang bersifat wajib pada aplikasi SAKTI. Sebagian besar studi terdahulu berfokus pada sektor komersial sedangkan pada sektor publik dengan penggunaan wajib, pembahasan Perceived Security jarang dihubungkan secara eksplisit dengan kerangka penerimaan seperti TAM. Kontribusi (novelty) penelitian ini terletak pada penerapan TAM yang diperkaya dengan Perceived Security (PS) untuk menjelaskan sikap (Attitude/ATT) terhadap MFA pada aplikasi SAKTI. Perceived Security sendiri adalah tingkat dimana pengguna merasa bahwa suatu sistem aman terhadap risiko (Almaiah et al., 2023). Selain itu, penelitian ini mengukur tingkat inconvenience atau ketidaknyamanan terkait penggunaan aplikasi ketika diterapkan MFA. Tingkat inconvenience akan menjadi indeks deskriptif sebagai bahan perbaikan pengalaman pengguna yang tidak dimasukkan dalam model hipotesis.

Penelitian ini bertujuan menilai pengaruh Perceived Security (PS) terhadap Perceived Usefulness (PU) dan Perceived Ease of Use (PEOU), serta pengaruh PU dan PEOU terhadap sikap terhadap MFA (ATT) pada aplikasi SAKTI, dan menggambarkan persepsi pengguna mengenai kendala penggunaan MFA. Temuan ini dapat digunakan oleh pengelola SAKTI/Kementerian Keuangan untuk menyelaraskan aspek keamanan dan kemudahan pada mekanisme autentikasi, serta menyediakan pedoman pemulihan akun yang jelas.

URAIAN TEORI

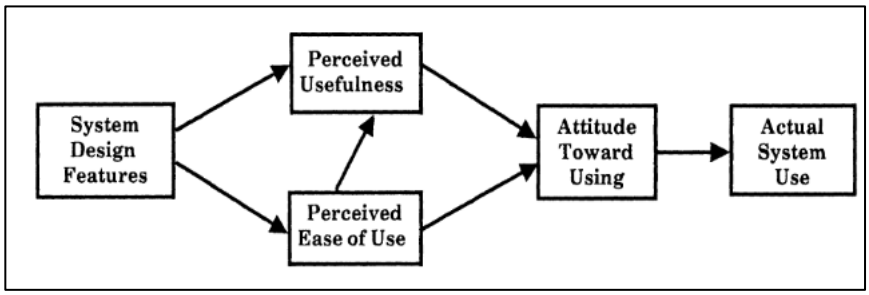
MFA merupakan suatu mekanisme autentikasi yang menerapkan berbagai prinsip autentikasi pada proses *login* ke suatu sistem melalui sejumlah perangkat, dengan tujuan mengumpulkan bukti yang cukup untuk memastikan bahwa pengguna benar-benar adalah individu yang berhak (Suleski et al., 2023). Sumber autentikasi ini dapat berasal dari interaksi manusia dengan sistem, baik melalui sistem berbasis kepercayaan, sistem berbasis pengetahuan, maupun metode lain yang memanfaatkan kredensial untuk memungkinkan pengguna membuktikan identitasnya secara sah. Umumnya, kata sandi digunakan bersama dengan autentikasi dua faktor (2FA) atau MFA, yaitu dengan mengombinasikan dua

atau lebih faktor autentikasi guna meningkatkan keamanan kredensial yang digunakan. Kredensial autentikasi dapat dikategorikan menjadi apa yang anda ketahui (faktor pengetahuan), apa yang anda miliki (faktor kepemilikan), siapa anda (faktor inherensi), dan yang terbaru, yaitu di mana anda berada (faktor lokasi). Sebagai contoh, faktor pengetahuan mencakup kata sandi, kode sandi, dan nomor PIN. Faktor kepemilikan mengacu pada kredensial yang dimiliki secara fisik seperti kunci dan kartu fisik. Faktor inherensi atau biologis seperti *fingerprint*, *hand-geometry*, retina, dan suara. Faktor lokasi mengacu pada lokasi fisik saat mengakses, namun faktor ini bukan faktor utama jenis autentikasi (Sharma & Farik, 2016).

Penerapan MFA berbasis aplikasi autentikator pada aplikasi SAKTI berimplikasi langsung pada persepsi pengguna. Adanya verifikasi tambahan ini dipandang dapat meningkatkan keamanan (Perceived Security/PS) sementara langkah tambahan, ketergantungan perangkat dan proses pemulihan MFA menambah kendala penggunaan yang dapat menurunkan PEOU. Di sisi lain, bila pengguna menilai MFA benar-benar bermanfaat untuk mencegah akses tidak sah dan mengurangi risiko penyalahgunaan, maka Perceived Usefulness (PU) akan meningkat. Dengan demikian, pengalaman pengguna saat berinteraksi dengan MFA bertindak sebagai pemicu awal yang menjelaskan keterkaitan PS dengan PU dan PEOU dalam praktik kerja sehari-hari, yang pada gilirannya membentuk sikap terhadap penggunaan (ATT) terhadap kebijakan MFA wajib di SAKTI.

Davis menyampaikan bahwa Perceived Usefulness adalah sejauh mana suatu sistem bermanfaat dalam meningkatkan kinerja pekerjaan penggunanya, sebaliknya Perceived Ease of Use mengacu pada sejauh mana sistem digunakan dengan mudah. (Davis, 1989). Dalam banyak studi, jalur PEOU → PU lazim ditemukan, namun pada konteks penggunaan wajib hubungan ini dapat melemah sehingga tetap perlu diuji untuk membuktikan relevansinya pada konteks penggunaan wajib. Beberapa studi (Almaiah et al., 2022, 2023; Zhang, 2024) mengintegrasikan indikator Perceived Security (PS) ke dalam model TAM karena keamanan dianggap sebagai manfaat inti yang memperkuat sikap pengguna terhadap suatu teknologi informasi seperti MFA. Dengan demikian, integrasi PS ke dalam model TAM dinilai relevan untuk menganalisis penerimaan MFA pada aplikasi dengan tuntutan keamanan tinggi seperti SAKTI.

Dalam kerangka TAM (Davis, 1989) dan TAM2 (Venkatesh & Davis, 2000), keyakinan inti dibentuk oleh konteks penggunaan, yang mencakup kontrol/sinyal keamanan yang dirasakan (PS), kebijakan penggunaan wajib, dan prosedur autentikasi yang diterapkan. Ketika kontrol autentikasi dirasakan bekerja (PS), persepsi ancaman menurun dan rasa kendali meningkat, sejalan dengan kerangka Technology Threat Avoidance Theory, sehingga sistem dinilai lebih bermanfaat (PS→PU) (Liang & Xue, 2009). Pada konteks layanan digital di Indonesia, temuan sejenis juga dilaporkan yang menautkan PS, PU/PEOU, dan niat penggunaan (Keni et al., 2020; Denaputri, A., & Usman, 2019; Tahar et al., 2020; Verawati et al., 2024). Pada saat yang sama, kepercayaan yang terbentuk mengurangi kecemasan dan beban kognitif (David Gefen, Elena Karahanna, 2003; McKnight et al., 2002), membuat prosedur terasa lebih mudah (PS→PEOU). Pada konteks aplikasi yang diwajibkan institusi, sinyal kebijakan dan kontrol formal (misalnya kewajiban MFA, prosedur aktivasi/pemulihan, dan dukungan helpdesk) membentuk institution-based trust yang menurunkan ketidakpastian dan mempermudah kepatuhan pengguna (McKnight et al., 2002; Perpres No. 95 Tahun 2018 tentang SPBE; Nota Dinas ND-812/PB.8/2024). Bukti e-government Indonesia juga menegaskan keterkaitan keamanan, kegunaan, dan kepercayaan dalam penerimaan layanan (Pribadi et al., 2021; Al-Kautsar Maktub et al., 2025). Pada konteks penggunaan wajib, jalur PEOU→PU tetap diuji karena kemudahan tidak selalu diterjemahkan sebagai manfaat. Dengan demikian, PS berperan di awal, memicu PU dan PEOU yang pada gilirannya membentuk sikap terhadap MFA (ATT) melalui mediasi paralel. Dengan sifatnya yang hadir di awal interaksi, PS berfungsi sebagai pemicu awal yang membentuk PU dan PEOU. Oleh karena itu, PS relevan dimodelkan sebagai variabel eksternal, bukan keluaran dari penggunaan.



Gambar 1. Technology Acceptance Model (Davis, 1989)

Kerangka konseptual tersebut dioperasionalisasikan melalui konstruk PS, PU, PEOU, dan ATT yang dimodelkan secara reflektif pada skala Likert 1–5. Daftar indikator masing-masing konstruk ditampilkan pada Tabel 1. Selain empat konstruk utama dalam model, penelitian ini juga mengamati kendala penggunaan MFA sebagai indikator kontekstual yang menggambarkan pengalaman pengguna sehari-hari (misalnya waktu tambahan, langkah ekstra, ketergantungan perangkat, dan proses pemulihan). Indikator ini tidak dimasukkan ke dalam model PLS-SEM dan hanya dilaporkan secara deskriptif untuk melengkapi interpretasi temuan.

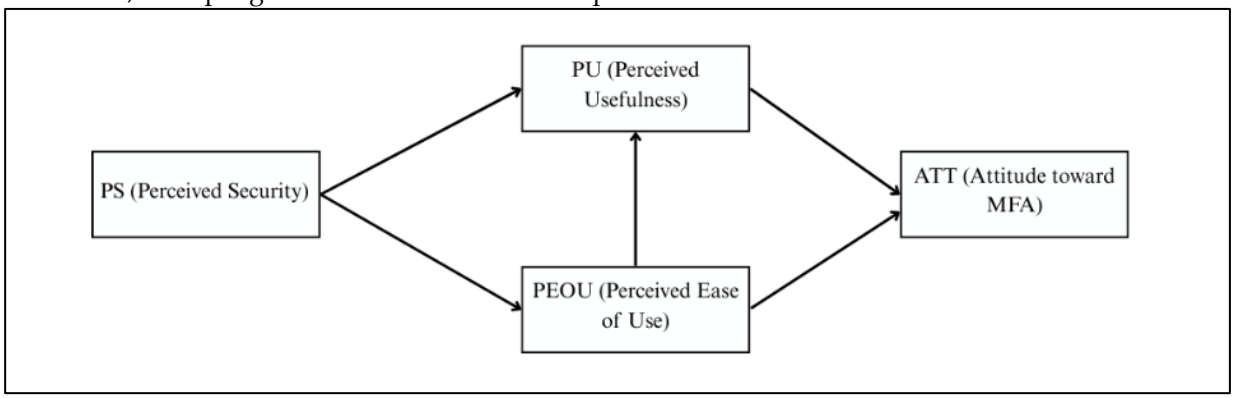
Tabel 1. Variabel dan Indikator Penelitian PLS-SEM

No	Variabel	Indikator
1	Perceived Ease of Use (PEOU)	PEOU1: Langkah MFA aplikasi SAKTI mudah dipahami.
		PEOU2: Saya tidak memerlukan banyak usaha untuk menyelesaikan MFA di aplikasi SAKTI.
		PEOU3: Proses MFA di aplikasi SAKTI ringkas dan jelas.
2	Perceived Usefulness (PU)	PU1: MFA di aplikasi SAKTI meningkatkan keamanan akses akun saya.
		PU2: MFA membantu melindungi data dan transaksi yang saya kelola di SAKTI.
		PU3: Dengan MFA, risiko penyalahgunaan akun dapat ditekan.
3	Perceived Security (PS)	PS1: Saya merasa aman saat login ke aplikasi SAKTI menggunakan MFA.
		PS2: MFA mengurangi kekhawatiran saya terhadap pengambilalihan akun.
		PS3: Dengan MFA, akses aplikasi SAKTI terasa lebih terlindungi.
4	Attitude toward MFA (ATT)	ATT1: Secara umum, saya menyukai penerapan MFA di aplikasi SAKTI.
		ATT2: Menurut saya, menggunakan MFA adalah ide yang baik.
		ATT3: Saya memiliki sikap positif terhadap kebijakan MFA di aplikasi SAKTI.

Tabel 2. Variabel dan Indikator Penelitian (Deskriptif)

No	Variabel	Indikator
1	Inconvenience (Ketidaknyamanan)	INC1: Proses MFA memakan waktu saat hendak bekerja menggunakan aplikasi SAKTI.
		INC2: MFA menambah langkah sehingga terasa kurang praktis.
		INC3: Ketergantungan ponsel/perangkat untuk MFA menyulitkan saya.
		INC4: Saat terjadi masalah, pemulihan/aktivasi ulang MFA terasa membingungkan.

Berdasarkan uraian teori, model penelitian pada Gambar 2 menguji pengaruh PS terhadap PU dan PEOU, serta pengaruh PU dan PEOU terhadap ATT.



Gambar 2. Model Penelitian

Model pada Gambar 2 mengadopsi kerangka Technology Acceptance Model (TAM) yang diperluas dengan variabel eksternal Perceived Security (PS). Dalam TAM, dua keyakinan inti, yaitu Perceived Usefulness (PU) dan Perceived Ease of Use (PEOU), membentuk Attitude toward MFA (ATT) terhadap sistem (Davis, 1989). Ekstensi TAM2 menegaskan peran faktor eksternal yang memengaruhi PU dan PEOU melalui pengaruh sosial dan proses kognitif (Venkatesh & Davis, 2000). Penelitian terbaru menunjukkan bahwa dimensi keamanan dan privasi berperan dalam penerimaan teknologi. Zhang et al. menemukan Perceived Privacy dan Perceived Security berpengaruh dalam kerangka TAM (Zhang, 2024), sementara kajian lain menambahkan trust/privacy untuk memperkaya penjelasan penerimaan (Dhagarra et al., 2020; Keni et al., 2020). Di Indonesia, modifikasi TAM dengan variabel eksternal juga pernah dilakukan, misalnya pada studi Andriani, Setyanto, & Nasiri (Andriani et al., 2020).

Dalam model ini, PS berperan di awal, ketika kontrol akan autentikasi dipersepsikan andal, persepsi risiko menurun dan rasa kendali akan meningkat sehingga sistem dinilai lebih bermanfaat (PS→PU). Pada saat yang sama, kepercayaan yang terbentuk menurunkan kecemasan dan beban kognitif sehingga langkah terasa lebih mudah (PS→PEOU). Selanjutnya, manfaat dan kemudahan yang dirasakan membentuk sikap positif terhadap MFA (PU→ATT, PEOU→ATT). Jalur PEOU→PU tetap disertakan untuk diuji karena pada konteks penggunaan wajib kemudahan tidak selalu diterjemahkan sebagai manfaat. Atas dasar itu, pengaruh PS terhadap ATT dimodelkan tidak langsung melalui mediasi paralel PU dan PEOU.

Model penelitian memosisikan PS sebagai pendorong awal yang meningkatkan PU, karena MFA dipersepsikan melindungi akun dan data, serta meningkatkan PEOU, karena rasa aman membuat proses terasa wajar dan tidak membebani (PS → PU, PS → PEOU). Sejalan bukti terdahulu, jalur PEOU → PU tetap disertakan untuk diuji pada konteks wajib. Di sisi hilir, PU dan PEOU membentuk sikap terhadap MFA (ATT) (PU → ATT, PEOU → ATT). Dengan demikian, pengaruh PS terhadap ATT tidak dimodelkan secara langsung tetapi muncul secara tidak langsung melalui PU dan PEOU (mediasi paralel).

Pengembangan Hipotesis

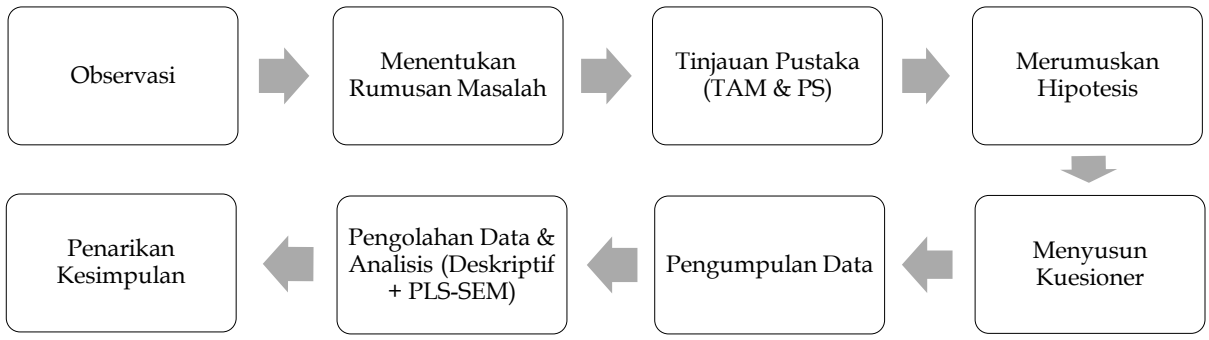
Dengan mengacu pada Gambar 2 serta penjelasan hubungan antar variabel pada bagian Kajian Teori, hipotesis penelitian adalah sebagai berikut:

1. H1: PEOU berpengaruh positif terhadap PU.
2. H2: PU berpengaruh positif terhadap ATT.
3. H3: PEOU berpengaruh positif terhadap ATT.
4. H4: PS berpengaruh positif terhadap PU.
5. H5: PS berpengaruh positif terhadap PEOU.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei dan desain *cross-sectional*. Metode survei dipilih karena penelitian ini menghimpun persepsi pengguna dalam jumlah tertentu pada satu periode waktu untuk menilai penerimaan MFA pada SAKTI. Pemodelan dilakukan dengan Partial Least Squares Structural Equation Modeling (PLS-SEM) karena konstruk dalam studi ini bersifat reflektif dan ukuran sampel relatif kecil (N=69). Pendekatan ini dipilih untuk tujuan analisis yang eksplanatori dan prediktif, sekaligus lebih toleran terhadap kemungkinan ketidaknormalan distribusi data dan memadai untuk menguji beberapa jalur kausal secara simultan. Dalam menyelesaikan penelitian ini terdapat beberapa tahapan proses yang digambarkan pada Gambar 3.

Gambar 3. Alur Proses Penelitian



Populasi sasaran dalam penelitian ini mencakup pengguna aplikasi SAKTI pada beberapa K/L. Kriteria partisipasi meliputi: (i) pengguna Aplikasi SAKTI aktif sekurang-kurangnya satu bulan terakhir; (ii) pernah melakukan login menggunakan MFA; dan (iii) menyetujui partisipasi. Kriteria pengecualian diterapkan sebelum pengisian dimana responden yang tidak memenuhi syarat partisipasi atau tidak menyetujui partisipasi tidak dilibatkan. Kemudian setelah pengisian kuesioner, kriteria yang dikecualikan mencakup respons yang kurang dari 80% terisi, berpola tidak wajar (duplikat), atau menunjukkan inkonsistensi pada saat dilakukan screening.

Teknik pengambilan sampel menggunakan non-probability purposive sampling. Non-probability berarti pemilihan responden tidak acak, sehingga peluang setiap anggota populasi untuk terpilih tidak diketahui (Etikan et al., 2016). Purposive berarti responden dipilih secara sengaja karena memenuhi kriteria inklusi yang relevan, yaitu pengguna SAKTI yang telah menggunakan MFA dan aktif sekurang-kurangnya satu bulan (Tongco, 2007). Pencarian responden dilakukan melalui jejaring internal peneliti yang sesuai dengan kriteria yang telah dijelaskan sebelumnya dimana partisipasi berasal dari sejumlah K/L yang terjangkau oleh peneliti. Konsekuensinya, temuan terutama menggambarkan kondisi kelompok yang diteliti dan tidak dimaksudkan mewakili seluruh populasi pengguna SAKTI (Yin, 2018). Halaman awal kuesioner memuat informed consent (tujuan, kerahasiaan, sifat sukarela, hak

menghentikan partisipasi). Survei anonim dan tidak mengumpulkan data identitas pribadi responden.

Pengumpulan data menghasilkan 70 respons, dan setelah penyaringan kualitas data, 69 respons dinyatakan valid (N = 69) dan digunakan dalam analisis. Ukuran sampel mengacu pada Hair et al., 10-times rule dalam PLS-SEM menyatakan bahwa ukuran sampel minimum adalah 10 kali jumlah panah terbanyak yang menuju satu konstruk endogen (Hair et al., 2017). Dalam model ini ATT menerima 2 panah dari PU dan PEOU sehingga ambang minimal adalah 20 responden. Ukuran sampel penelitian berjumlah 69 sehingga melebihi ambang tersebut dan dinilai memadai untuk estimasi menggunakan SmartPLS. Aturan ini bersifat *rule of thumb* sehingga tetap dianjurkan pelaporan hasil yang lengkap dan transparansi prosedur pembersihan data.

Data dikumpulkan melalui kuesioner daring berskala Likert 1–5 (1 = Sangat Tidak Setuju, 2 = Tidak Setuju, 3 = Netral, 4 = Setuju, dan 5 = Sangat Setuju) yang mengukur Perceived Ease of Use (PEOU) dan Perceived Usefulness (PU) yang diadaptasi dari TAM (Davis, 1989; Venkatesh & Davis, 2000), serta Attitude (ATT) yang mengikuti praktik pengukuran dalam studi TAM (Davis, 1989). Perceived Security (PS) dirumuskan dari literatur yang menautkan dimensi keamanan dengan penerimaan teknologi (Almaiah et al., 2023; Zhang, 2024) yang kemudian disesuaikan dalam konteks MFA di SAKTI. Uji coba awal dilakukan untuk memastikan kejernihan butir dan memeriksa indikasi kolinearitas antar indikator serta umpan balik dari uji coba digunakan untuk penyelarasan redaksi sebelum pengumpulan data utama. Selain itu, studi ini mencatat inconvenience atau ketidaknyamanan sebagai indeks deskriptif yang akan menggambarkan ketidaknyamanan yang dirasakan pengguna seperti waktu tambahan, langkah ekstra, ketergantungan perangkat, dan proses pemulihan. Variabel ini tidak dimasukkan dalam model struktural dan berfungsi melengkapi interpretasi temuan.

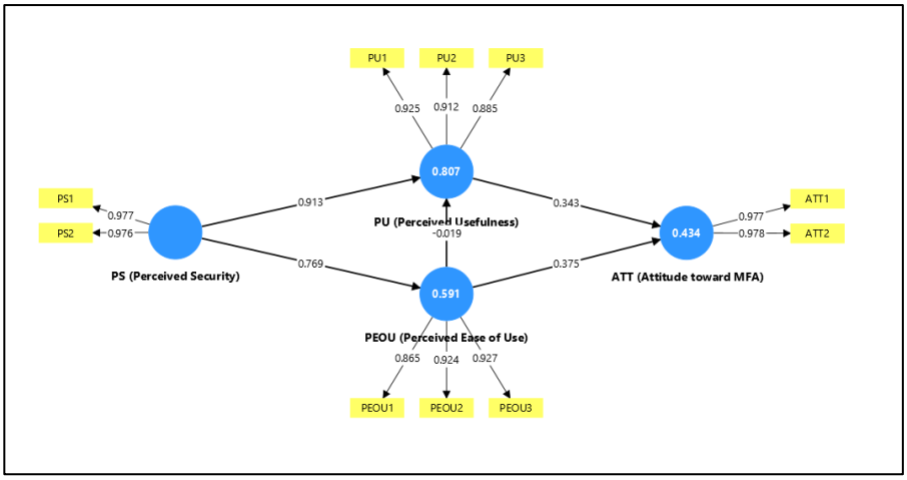
Analisis menggunakan PLS-SEM di SmartPLS v4. Seluruh konstruk dimodelkan reflektif pada skala Likert 1–5. Evaluasi meliputi model pengukuran (outer loadings, reliabilitas, AVE, validitas diskriminan) dan model struktural (koefisien jalur, R^2, f^2, specific indirect effects). Signifikansi diuji dengan bootstrapping 5000 subsampel. Evaluasi relevansi prediktif (Q^2) melalui teknik blindfolding tidak dilakukan pada penelitian ini karena keterbatasan teknis pada proyek SmartPLS.

HASIL PENELITIAN

Pengujian dilakukan secara bertahap dimulai dari model pengukuran lalu model struktural. Pada tahap model pengukuran untuk konstruk reflektif, diperiksa kualitas indikator melalui outer loading, reliabilitas internal (Cronbach's alpha, ρA, dan Composite Reliability), serta validitas konvergen (AVE). Selanjutnya diuji validitas diskriminan menggunakan kriteria Fornell–Larcker dan HTMT. Kolinearitas pada tingkat indikator diperiksa melalui outer VIF. Setelah model pengukuran memadai, analisis berlanjut ke model struktural dengan mengecek kolinearitas antar-prediktor (inner VIF), daya jelaskan konstruk endogen (R^2), serta ukuran efek lokal (f^2). Signifikansi hubungan dievaluasi dengan bootstrapping (jumlah subsampel memadai), termasuk uji efek tidak langsung (mediasi).

Ringkasan hasil utama

Perceived Security (PS) berpengaruh kuat dan signifikan terhadap Perceived Usefulness (PU) dan Perceived Ease of Use (PEOU) ($p < 0{,}001$ untuk keduanya). PU dan PEOU berpengaruh positif terhadap sikap terhadap MFA (ATT) dan keduanya signifikan (PU → ATT: $p = 0{,}010$; PEOU → ATT: $p = 0{,}011$), sedangkan PEOU → PU tidak terbukti pada konteks penggunaan wajib ($p = 0{,}870$). Secara keseluruhan, ketika keamanan dipersepsikan memadai, pengguna menilai MFA lebih bermanfaat dan lebih mudah digunakan, yang pada akhirnya membentuk sikap positif terhadap kebijakan MFA. Hasil perhitungan SmartPLS tergambar pada Gambar 4.



Gambar 4. Hasil Perhitungan SmartPLS 4

Kualitas pengukuran: reliabilitas dan validitas

Dalam PLS-SEM, validitas konvergen dievaluasi melalui: (i) outer loading indikator yang idealnya ≥ 0,70, (ii) signifikansi loading berdasarkan bootstrapping, dan (iii) AVE ≥ 0,50 untuk setiap konstruk (Hair, 2019; Hair & Ringle, 2022). Berdasarkan hasil SmartPLS, mayoritas loading indikator berada ≥ 0,70 dan seluruh loading yang dipertahankan signifikan kemudian AVE tiap konstruk > 0,50 (Tabel 3). Pada tahap perapihan, dua butir (ATT3 dan PS3) dihapus untuk memperbaiki konvergensi dan mengurangi redundansi sehingga indikator tersisa merefleksikan konstruk secara memadai.

Tabel 3. Construct Reliability and Validity

Variabel/Konstruk	Cronbach_alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	AVE
ATT	0,954	0,954	0,977	0,956
PEOU	0,89	0,897	0,932	0,820
PS	0,952	0,952	0,976	0,954
PU	0,893	0,893	0,933	0,823

Tabel 3 memperlihatkan seluruh konstruk telah memenuhi reliabilitas internal dan validitas konvergen. Nilai cronbach's alpha, rho_A, dan rho_C seluruhnya berada di atas ambang rekomendasi (≥ 0,70). Hasil AVE yang seluruhnya lebih besar dari 0,50 menguatkan validitas konvergen. Dengan demikian, indikator yang dipertahankan merepresentasikan konstruk ATT, PEOU, PS, PU dengan baik sesuai pedoman PLS-SEM (Hair, 2019; Hair & Ringle, 2022).Validitas diskriminan dinilai dengan kriteria Fornell–Larcker. Akar AVE di diagonal lebih besar daripada korelasi antarkonstruk (Tabel 4), sehingga konstruk-konstruk dapat dibedakan.

Tabel 4. Discriminant Validity

Variabel/Konstruk	ATT	PEOU	PS	PU
ATT	0.978			
PEOU	0.609	0.906		
PS	0.666	0.769	0.977	
PU	0.599	0.683	0.898	0.907

Akar AVE pada diagonal selalu lebih tinggi daripada korelasi antarkonstruk, sehingga validitas diskriminan terpenuhi. Korelasi PS–PU = 0,898 tergolong tinggi, tetapi tetap di bawah akar AVE masing-masing, sehingga PS dan PU tetap berbeda menurut data (Fornell & Larcker, 1981; Henseler et al., 2015). Validitas diskriminan juga diuji menggunakan Heterotrait–Monotrait Ratio (HTMT). Hasilnya ditunjukkan pada tabel berikut.

Tabel 5. Discriminant Validity-HTMT

Variabel/Konstruk	ATT	PEOU	PS	PU
ATT				
PEOU	0,657			
PS	0,699	0,835		
PU	0,648	0,763	**0,973**	

Sebagian besar nilai HTMT <0,90 sehingga memenuhi kriteria validitas diskriminan (Henseler et al., 2015). Namun, hubungan antara PS dan PU memiliki nilai HTMT sebesar 0,973 yang melampaui ambang batas. Hal ini mengindikasikan adanya potensi tumpang tindih persepsi antara keamanan dan kemanfaatan. Dengan kata lain, bagi responden, manfaat MFA pada SAKTI banyak dimaknai sebagai fungsi perlindungan yang diberikannya. Temuan ini konsisten dengan peran PS sebagai pemicu awal yang menonjol dalam membentuk keyakinan inti pengguna, dan diperhatikan dalam interpretasi hasil.

Pada evaluasi kolinearitas tingkat indikator, beberapa butir menunjukkan outer VIF di atas ambang umum. Mengikuti praktik PLS-SEM, indikator bermasalah dievaluasi dan kemudian diputuskan untuk mengeluarkan indikator ATT3 dan PS3. Setelah pemangkasan, nilai VIF menunjukkan kolinearitas indikator berada pada tingkat yang terkendali. Penghapusan ATT3 dan PS3 efektif menurunkan VIF yang semula sangat tinggi pada evaluasi awal.

Tabel 6. Collinearity statistics (VIF) – Outer model

Indikator	VIF
ATT1	5,916
ATT2	5,916
PEOU1	2,114
PEOU2	3,129
PEOU3	3,303
PS1	5,671
PS2	5,671
PU1	3,360
PU2	3,109
PU3	2,171

Nilai tertinggi berada pada kisaran 5,7–5,9, sedangkan indikator lain berada sekitar 2,1–3,4. Nilai sebelum pemangkasan mencapai sekitar 9 pada sebagian butir. Ini menunjukkan redundansi indikator sudah terkendali dan tidak ada masalah kolinearitas berlebihan pada level indikator (Hair, 2019; Hair & Ringle, 2022). Selanjutnya dilakukan pengecekan pada inner VIF. Kriteria umum yang direkomendasikan adalah VIF < 5 agar estimasi jalur stabil (Hair, 2019; Hair & Ringle, 2022). Seluruh nilai inner VIF berada di bawah ambang 5. Dengan demikian, estimasi koefisien jalur pada model struktural dinilai stabil dan tidak terdistorsi oleh multikolinearitas.

Kualitas model struktural

Koefisien determinasi (R^2) pada konstruk endogen berada pada kategori sedang sampai tinggi (Hair & Ringle, 2022).

Tabel 7. R-square – Overview

Variabel/Konstruk	R^2	R^2_adj
ATT	0,434	0,417
PEOU	0,591	0,585

PU	0,807	0,801

Tabel 7 menunjukkan ATT = 0,434 berada pada kategori sedang, PEOU = 0,591 pada sedang–tinggi, sedangkan PU = 0,807 pada tinggi. Pola ini konsisten dengan peran PS di sisi awal yang kuat dalam menjelaskan PU, serta kontribusi bersama PEOU dan PU dalam membentuk ATT (Hair & Ringle, 2022).

Besarnya pengaruh (f^2) menunjukkan PS sangat dominan di awal, sedangkan PEOU dan PU berkontribusi pada sikap. Kategori mengikuti panduan Cohen (Cohen, 1988), dimana pengaruh kecil sekitar 0,02, sedang sekitar 0,15, besar sekitar 0,35, rujukan ini juga digunakan oleh Hair dan Ringle (Hair & Ringle, 2022).

Tabel 8. F-square – Matrix

Dari	Ke	f^2
PEOU	ATT	0,133
PS	PEOU	1,445
PS	PU	1,762
PU	ATT	0,111
PEOU	PU	0,001

Tabel 9 menunjukkan pengaruh PS → PU (1,762) dan PS → PEOU (1,445) tergolong sangat besar. Pengaruh PEOU → ATT (0,133) dan PU → ATT (0,111) kecil hingga sedang tetapi tetap berarti. Pengaruh PEOU → PU (0,001) sangat kecil dan sejalan dengan hasil jalur yang tidak signifikan. Efek PEOU → ATT (0,133) dan PU → ATT (0,111) berada pada tingkat kecil menuju sedang namun relevan. PEOU → PU (0,001) praktis tidak berarti, selaras dengan uji jalur yang tidak signifikan (Cohen, 1988).

Uji hipotesis

Sebagai kelanjutan dari evaluasi R^2 dan besarnya pengaruh (f^2), pengujian hipotesis pada model struktural dilakukan melalui *bootstrapping* 5.000 subsampel. Hasilnya, empat jalur signifikan. H1 (PEOU → PU) tidak didukung. Dengan demikian, H2, H3, H4, dan H5 didukung pada tingkat signifikansi $p < 0,05$.

Tabel 9. Path coefficients – Mean, STDEV, T, p

Jalur	O	M	STDEV	T	P
PEOU → ATT	0,375	0,358	0,147	2,551	0,011
PEOU → PU	-0,019	0,000	0,118	0,164	0,870
PS → PEOU	0,769	0,757	0,093	8,271	0,000
PS → PU	0,913	0,904	0,083	10,941	0,000
PU → ATT	0,343	0,357	0,133	2,582	0,010

Empat jalur signifikan dengan arah sesuai teori. PS terbukti mendorong PU dan PEOU secara kuat, sementara PEOU dan PU bersama-sama meningkatkan ATT. Jalur PEOU → PU tidak signifikan pada konteks MFA yang wajib dan berorientasi keamanan, menandakan manfaat lebih bergantung pada persepsi aman ketimbang kemudahan prosedural (Davis, 1989; King & He, 2006; Legris et al., 2003). Terkait efek tidak langsung dan mediasi, PS berpengaruh pada ATT sepenuhnya melalui mediator PU dan PEOU. Jalur berantai PS → PEOU → PU → ATT tidak signifikan.

Analisis mediasi menunjukkan bahwa PS memengaruhi ATT secara tidak langsung melalui dua jalur paralel yang signifikan. Pertama, PS → PU → ATT dengan $\beta\_ind = 0,313$, $t = 2,690$, $p = 0,007$. Kedua, PS → PEOU → ATT dengan $\beta\_ind = 0,288$, $t = 2,266$, $p = 0,023$. Temuan ini berarti ketika keamanan dipersepsikan memadai, pengguna menilai MFA lebih bermanfaat dan lebih mudah digunakan, sehingga sikap terhadap kebijakan menjadi lebih positif. Jalur berantai PS → PEOU → PU → ATT tidak signifikan ($p = 0,878$), sehingga peningkatan manfaat yang memicu sikap tidak bergantung pada kemudahan terlebih dahulu, sejalan dengan konteks MFA yang wajib dan berorientasi keamanan.

Berdasarkan evaluasi R^2 dan f^2 (Tabel 7–8), keputusan hipotesis ditentukan pada tahap uji jalur

menggunakan *bootstrapping* 5.000 subsampel. Kriteria penerimaan merujuk praktik pelaporan PLS-SEM: koefisien searah dengan hipotesis dan nilai p < 0,05 (Hair, 2019; Hair & Ringle, 2022).

Tabel 12. Hasil Hipotesis

Kode	Pernyataan Hipotesis	Koefisien (β)	p value	Keputusan
H1	PEOU → PU (positif)	-0,019	0,870	Tidak didukung
H2	PU → ATT (positif)	0,343	0,010	Didukung
H3	PEOU → ATT (positif)	0,375	0,011	Didukung
H4	PS → PU (positif)	0,913	0,000	Didukung
H5	PS → PEOU (positif)	0,769	0,000	Didukung

Secara substantif, PS bertindak sebagai pendorong awal yang kuat terhadap PU dan PEOU. Keduanya kemudian membentuk ATT, sementara hubungan PEOU → PU tidak muncul pada konteks ini. Temuan ini konsisten dengan implementasi MFA yang wajib dan berorientasi keamanan, sehingga manfaat dipersepsikan terutama dari sisi perlindungan.

Penelitian ini juga mengumpulkan data terkait ketidaknyamanan yang dirasakan oleh responden ketika menggunakan MFA. Berikut adalah rangkuman dari jawaban responden terhadap ketidaknyamanan:

Tabel 13. Rangkuman Indikator Inconvenience/Ketidaknyamanan

Indikator	Skor paling sering	Frekuensi	Persentase (%)
Proses MFA memakan waktu saat hendak bekerja di SAKTI.	4	20	29
MFA menambah langkah sehingga terasa kurang praktis.	3	20	29
Ketergantungan ponsel/perangkat untuk MFA menyulitkan saya.	2	18	26.1
Saat terjadi masalah, pemulihan/aktivasi ulang MFA terasa membingungkan.	5	18	26.1

Secara ringkas, pernyataan 1 paling sering diberi skor 4 (29,0%), pernyataan 2 paling sering 3 (29,0%), pernyataan 3 paling sering 2 (26,1%), dan pernyataan 4 paling sering 5 (26,1%). Pola ini menunjukkan adanya persepsi beban waktu dan dan tambahan langkah pada MFA, ketergantungan perangkat yang cukup dirasakan, serta kebingungan pada pemulihan. Temuan ini selaras dengan hasil struktural bahwa PEOU → ATT signifikan, sehingga beban tersebut berpotensi menekan sikap terhadap kebijakan MFA.

Masukan terbuka dari responden menguatkan pola yang sama, terutama pada tahap autentikasi (input OTP manual dan waktu tunggu), kebutuhan perangkat kedua, serta banyaknya langkah login. Oleh karena itu, pengurangan friksi pada empat aspek tersebut dengan memangkas waktu dan jumlah langkah, menyediakan faktor autentikasi cadangan yang tidak selalu bergantung pada satu perangkat, dan memperjelas prosedur pemulihan diharapkan dapat meningkatkan PEOU dan pada gilirannya memperkuat ATT.

PEMBAHASAN

Hasil pengujian hipotesis menunjukkan bahwa empat jalur dalam model diterima, sedangkan satu jalur tidak didukung. Jalur PEOU → PU (H1) tidak signifikan (p = 0,870), berbeda dengan PU → ATT (H2) (p = 0,010), PEOU → ATT (H3) (p = 0,011), PS → PU (H4) (p < 0,001), dan PS → PEOU (H5) (p <

0,001) yang signifikan positif. Dengan demikian, manfaat MFA (PU) lebih banyak dipengaruhi oleh persepsi keamanan (PS) daripada persepsi kemudahan (PEOU), sedangkan sikap terhadap MFA (ATT) terbentuk dari gabungan pengalaman kemudahan dan persepsi manfaat.

Tidak signifikannya PEOU → PU pada konteks MFA yang wajib menunjukkan bahwa pengguna memaknai manfaat terutama sebagai perlindungan dari akses tidak sah, bukan sebagai keluaran dari kemudahan prosedural. Pola ini konsisten dengan jalur PS → PU yang kuat serta dengan temuan sebelumnya bahwa adopsi MFA cenderung rendah ketika pengguna diwajibkan (Das et al., 2019), dan bahwa skema smartphone-based OTP dinilai paling rendah karena waktu tambahan dan kerumitan langkah (Zimmermann et al., 2022). Hambatan pada tahap pemulihan yang kurang ramah pengguna turut memperkuat beban penggunaan tanpa serta-merta menurunkan persepsi manfaat yang berorientasi keamanan (Amft et al., 2021).

Fenomena ini selaras dengan data lapangan, di mana responden menyampaikan kendala penggunaan MFA SAKTI. Hasil deskriptif Likert menunjukkan keluhan utama pada aspek waktu, banyaknya langkah, ketergantungan perangkat, dan pemulihan akun. Misalnya, 29% responden menilai proses MFA memakan waktu (skor 4), sedangkan 26,1% menilai pemulihan membingungkan (skor 5). Kendala semacam ini menekan persepsi kemudahan, tetapi tidak mengurangi peran keamanan dalam membentuk manfaat yang dirasakan. Artinya, meskipun prosedur MFA dianggap kurang praktis, responden tetap menilai keberadaannya bermanfaat untuk melindungi data dan akun mereka.

Secara teoretis, hasil ini menegaskan kerangka Technology Acceptance Model (TAM) (Davis, 1989) yang menyatakan bahwa PU dan PEOU membentuk sikap pengguna, serta ekstensi TAM2 yang membuka ruang masuknya faktor eksternal (Venkatesh & Davis, 2000). Pada penelitian ini, PS diposisikan sebagai variabel eksternal yang kuat dalam memengaruhi PU dan PEOU. Hal ini sejalan dengan penelitian Zhang et al. (2024) yang menekankan peran privacy dan security dalam memperkuat TAM, serta studi Dhagarra et al. (2020) yang menunjukkan bahwa trust dan keamanan memengaruhi penerimaan teknologi kesehatan (Dhagarra et al., 2020; Zhang, 2024). Keni et al. (2020) di Indonesia juga membuktikan pengaruh positif keamanan, kemudahan, dan manfaat terhadap niat menggunakan mobile payment (Keni et al., 2020).

Dengan demikian, PS berperan sebagai variabel eksternal kunci yang terlebih dahulu mengangkat PU dan PEOU, sedangkan jalur PEOU → PU tidak universal dan bergantung pada cara pengguna mendefinisikan manfaat dalam domain yang sensitif terhadap keamanan. Hal ini memperkaya penerapan TAM pada sektor publik yang regulatif dan menegaskan pentingnya memodelkan faktor keamanan ketika autentikasi menjadi kebijakan institusional.

Tidak signifikannya PEOU → PU dapat dipahami dari karakter mandatory use pada MFA SAKTI di instansi pemerintah. Dalam lingkungan yang menuntut kepatuhan, pengguna menilai manfaat terutama dari fungsi perlindungan dan pengendalian risiko, bukan dari kemudahan prosedur. Dengan demikian, PEOU lebih berperan membentuk sikap daripada menjadi sumber utama PU. Pola ini sejalan dengan kajian TAM pada konteks non-sukarela yang menunjukkan melemahnya pengaruh kemudahan terhadap manfaat, sementara faktor yang merepresentasikan nilai inti tugas dan kontrol organisasi lebih menentukan penilaian manfaat (King & He, 2006; Legris et al., 2003). Hal ini sekaligus menjelaskan mengapa PS → PU tampak sangat kuat pada temuan studi ini.

Temuan ini juga konsisten dengan literatur usable security. Sejumlah studi menunjukkan bahwa MFA meningkatkan keamanan tetapi menambah beban waktu, kebutuhan perangkat, dan kerumitan proses yang memengaruhi PEOU (Amft et al., 2023; Ciolino et al., 2019; Reese et al., 2020; Reynolds et al., 2018). Namun, meski beban autentikasi nyata dirasakan, pengguna tetap cenderung menerima MFA ketika aspek keamanannya dinilai tinggi. Hasil ini memperluas gagasan usable security di lingkungan layanan publik dimana PS perlu dipertahankan tinggi melalui kontrol autentikasi yang kredibel, sementara PEOU ditingkatkan dengan memangkas waktu dan jumlah langkah login, menyediakan faktor cadangan yang tidak bergantung pada satu perangkat, serta memperjelas panduan pemulihan. Pendekatan ini menjaga manfaat yang dipersepsikan sebagai keamanan sekaligus meningkatkan kemudahan, yang menurut hasil jalur berdampak langsung pada ATT.

Berdasarkan hasil tersebut, terdapat beberapa arah perbaikan yang wajar untuk konteks MFA SAKTI. Prioritasnya adalah mengurangi beban prosedur sehingga kemudahan penggunaan meningkat tanpa mengorbankan aspek keamanan. Langkah yang dapat ditempuh antara lain meringkas jumlah

tahapan autentikasi, mempercepat alur (misalnya melalui *push approval*), menyediakan pilihan autentikasi yang tidak sepenuhnya bergantung pada satu perangkat, serta menghadirkan petunjuk pemulihan akun yang ringkas dan mudah dipahami. Perbaikan ini diperkirakan dapat mengangkat PEOU dan pada akhirnya memperkuat sikap positif (ATT), sementara manfaat (PU) tetap terjaga karena PS sudah menjadi pengaruh dominan di dalam model.

PENUTUP

Studi ini menunjukkan bahwa Perceived Security (PS) secara konsisten menaikkan Perceived Usefulness (PU) dan Perceived Ease of Use (PEOU). PU dan PEOU bersama membentuk sikap terhadap MFA (ATT), sedangkan jalur PEOU ke PU tidak terdukung pada konteks penggunaan wajib. Temuan deskriptif mengenai waktu tambahan, langkah ekstra, ketergantungan perangkat, dan pemulihan yang membingungkan selaras dengan peran PEOU terhadap ATT, sementara efek tidak langsung mengindikasikan bahwa PS memengaruhi ATT melalui PU dan PEOU.

Hasil ini menegaskan PS sebagai variabel eksternal kunci dalam perluasan TAM untuk autentikasi sektor publik. Cara pengguna memaknai manfaat lebih berorientasi pada perlindungan daripada kemudahan sehingga hubungan PEOU ke PU menjadi kondisional pada konteks mandatory. Kontribusi studi terletak pada penempatan PS sebagai pemicu awal keyakinan inti (PU dan PEOU) serta pada penguatan jembatan antara TAM dan gagasan usable security di lingkungan yang regulatif.

Bagi pengelola SAKTI, diharapkan dapat mempertahankan kredibilitas keamanan sambil meningkatkan pengalaman pengguna. Strategi yang disarankan meliputi peringkasan jumlah tahapan autentikasi, percepatan alur login melalui mekanisme seperti push approval, penyediaan faktor autentikasi cadangan yang tidak sepenuhnya bergantung pada satu perangkat, penyusunan panduan pemulihan yang ringkas dan mudah diakses, serta komunikasi manfaat keamanan yang jelas di titik antarmuka. Implementasi sebaiknya disertai pemantauan metrik adopsi dan beban penggunaan seperti waktu login, tingkat kegagalan verifikasi, dan permintaan pemulihan agar PEOU meningkat tanpa menurunkan PS.

Penelitian ini menggunakan sampel terbatas dan non probability sehingga generalisasi terutama berlaku pada konteks yang serupa, dan pengukuran berfokus pada konstruk inti sehingga manfaat non keamanan belum tergali luas. Riset berikutnya dapat menambahkan konstruk seperti trust dan resistance to change, memperkaya indikator PU yang menyoroti efisiensi proses, membandingkan berbagai skema MFA, melakukan studi longitudinal untuk menilai dinamika pasca perbaikan UX, serta menguji model alternatif seperti mediasi dan moderator agar pemisahan PS, PU, dan PEOU semakin tegas. Diharapkan temuan penelitian ini membantu pengelola aplikasi SAKTI untuk mengetahui tingkat rasa aman yang dirasakan pengguna sekaligus beban penggunaan dari para pengguna serta memperkaya literatur penerimaan teknologi pada konteks autentikasi berlapis yang wajib di sektor publik.

REFERENSI

Al-Kautsar Maktub, M., Handayani, P. W., & Sunarso, F. P. (2025). Citizen acceptance and use of the Jakarta Kini (JAKI) e-government: Extended unified model for electronic government adoption. *Heliyon*, *11*(2), e42078. https://doi.org/10.1016/j.heliyon.2025.e42078

Almaiah, M. A., Al-otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the Role of Perceived Risk, Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. *Sustainability*, *15*(9908), 1–17. https://doi.org/10.3390/su15139908

Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., Alkhalaf, S., Al-Rahmi, W. M., Al-sharaieh, S., & Aldhyani, T. H. H. (2022). Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia. *Electronics (Switzerland)*, *11*(23), 1–22. https://doi.org/10.3390/electronics11233926

Amft, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023). "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 3138–3152. https://doi.org/10.1145/3576915.3623180

Andriani, R., Setyanto, A., Nasiri, A., Informatika, M. T., Korespondensi, P., Studi, K. R., & Equation, S. (2020). *EVALUASI SISTEM INFORMASI MENGGUNAKAN TECHNOLOGY ACCEPTANCE MODEL DENGAN PENAMBAHAN VARIABEL EVALUATION OF INFORMATION SYSTEM USING TECHNOLOGY ACCEPTANCE*. *7*(3), 531–538. https://doi.org/10.25126/jtiik.20207850

Ciolino, S., Parkin, S., & Dunphy, P. (2019). Of Two Minds about Two-Factor : Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling This paper is included in the Proceedings of the. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, 339–356.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*.

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). *Evaluating User Perception of Multi-Factor Authentication: A Systematic Review*. http://arxiv.org/abs/1908.05901

David Gefen, Elena Karahanna, D. W. S. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, *27*(No.1), 51–90.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.5962/bhl.title.33621

Denaputri, A., & Usman, O. (2019). Effect of Perceived Trust, Perceived Security, Perceived Usefulness and Perceived Ease of use on Customers' Intention to Use Mobile Payment Annisa. *Harvard Business Review*, *1*.

Dhagarra, D., Goswami, M., & Kumar, G. (2020). *Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective*. *January*.

Direktorat Jenderal Perbendaharaan Kementerian Keuangan. (2024). *Multi-Factor Authentication (MFA) pada SAKTI*. https://djpb.kemenkeu.go.id/kppn/kotabumi/id/sakti/user-sakti/multi-factor-authentication-mfa-pada-sakti.html

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). *Comparison of Convenience Sampling and Purposive Sampling*. *5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, Vol. 18, No. 1 (Feb., 1981), Pp. 39-50*, *18*(1), 39–50.

Hair, J. F. (2019). *When to use and how to report the results of PLS-SEM*. *April 2019*. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Hult, G. T. M., & Ringle, C. M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (Second edi). SAGE Publications.

Hair, J. F., & Ringle, C. M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (Issue January). SAGE Publications, Inc.

Hazineh, S. A. S., Eleyan, D., & Alkhateeb, M. (2022). E-Government: Limitations And Challenges: A General Framework For To Consider In Both Developed And Developing Countries. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *11*(01), 97–103.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43 (1)*(January), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Keni, K., Tjoe, H., Wilson, N., & Negara, E. S. (2020). *The Effect of Perceived Security , Ease of Use and Perceived Usefulness on Intention to Use Towards Mobile Payment Services in Indonesia*. *478*(Ticash), 78–84.

King, W. R., & He, J. (2006). A meta-analysis of the Technology Acceptance Model A meta-analysis of the technology acceptance model. *Information & Management*, *43*(March), 740–755. https://doi.org/10.1016/j.im.2006.05.003

Laudon, K. C., & Laudon, J. P. (2014). Manajemen Information System: Managing the Digital Firm. In *Pearson/Prentice Hall*.

Legris, P., Ingham, J., & Collerette, P. (2003). *Why do people use information technology ? A critical review of the technology acceptance model Why do people use information technology ? A critical review of the*

technology acceptance model. *7206*(October 2017). https://doi.org/10.1016/S0378-7206(01)00143-4

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly: Management Information Systems*, *33*(1), 71–90. https://doi.org/10.2307/20650279

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Mushtaq, S., & Shah, M. (2025). Mitigating Cybercrimes in E-Government Services: A Systematic Review and Bibliometric Analysis. *Digital*, *5*(1). https://doi.org/10.3390/digital5010003

Ojo, S., & Covey, A. (2025). Identity and Access Management (IAM) Authentication Methods: Importance of Multi-Factor Authentication (MFA) and Single Sign-On (SSO) and Access Control. *Petsymposium.Org*, 0–11. https://doi.org/10.20944/preprints202503.1830.v1

Pribadi, U., Iqbal, M., & Restiane, F. (2021). Factors Affecting Trust in E-Government. *Journal of Government and Civil Society*, *Vol.5*, *No.*(Oktober 2021), 263–276. https://doi.org/https://doi.org/10.31000/jgcs.v5i2.4848

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2020). A Usability Study of Five Two-Factor Authentication Methods. *Proceedings of the 29th USENIX Security Symposium*, 127–143.

Reynolds, J., Smith, T., Reese, K., Dickinson, L., Ruoti, S., & Seamons, K. (2018). A Tale of Two Studies : The Best and Worst of YubiKey Usability. *2018 IEEE Symposium on Security and Privacy (SP)*, 872–888. https://doi.org/10.1109/SP.2018.00067

Sharma, N., & Farik, M. (2016). Security Gaps In Authentication Factor Credentials. *International Journal of Scientific & Technology Research*, *5*(11), 116–120.

Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*, *8*(4), 30–38. https://doi.org/10.24018/ejeng.2023.8.4.3074

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*. https://doi.org/10.1177/20552076231177144

Tahar, A., Riyadh, H. A., Sofyani, H., & Purnomo, W. E. (2020). Perceived ease of use, perceived usefulness, perceived security and intention to use e-filing: The role of technology readiness. *Journal of Asian Finance, Economics and Business*, *7*(9), 537–547. https://doi.org/10.13106/JAFEB.2020.VOL7.NO9.537

Tongco, M. D. C. (2007). *Purposive Sampling as a Tool for Informant Selection*. *5*, 147–158.

Venkatesh, V., & Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Verawati, L., Syaeful Anwar, M., & Afiati, L. (2024). Intention To Use Mobile Banking Application: Empirical Evidence From Indonesia. *The International Journal of Business Review (The Jobs Review)*, *7*(1), 29–40. https://doi.org/10.17509/tjr.v7i1.72773

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. SAGE Publications, Inc.

Zhang, Y. (2024). Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors. *International Journal of Information Management Data Insights*, *4*(2), 100270. https://doi.org/10.1016/j.jjimei.2024.100270

Zimmermann, V., Gerber, P., & Stöver, A. (2022). *That Depends - Assessing User Perceptions of Authentication Schemes across Contexts of Use*. http://arxiv.org/abs/2209.13958