Selangor Science & Technology Review
Vol. 9, No. 2, (2025)

Tinjauan Literatur: Dampak Model Mental Pengguna Terhadap Implementasi Multi-Factor Authentication Untuk Mitigasi Risiko Password Guessing di Konteks Organisasi

Ery Triantoro[1], Setyawan Widyarto [2]
Magister Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur [1,]
Faculty of Communication, Visual Arts & Computing, Universiti Selangor[2]
e-mail: 2411600022@student.budiluhur.ac.id [1], swidyarto@unisel.edu.my [2]

Abstract: This study is a Systematic Literature Review (SLR) aimed at analyzing the impact of users' mental models on the implementation of Multi-Factor Authentication (MFA) in mitigating password guessing risks within organizational environments. A total of 200 initial articles were identified from Google Scholar using keywords related to MFA, and after the PRISMA selection process, 10 core articles were obtained for further analysis. The reviewed literature consists of publications from 2020–2025, in both Indonesian and English. The results show that expert users tend to perceive MFA as a beneficial additional security layer, while non-expert users regard it as a burdensome task. The main obstacles include a lack of understanding, low risk perception, and reliance on mobile devices. The analysis was conducted using a mental model approach to understand the differences in users' perceptions and experiences of MFA. The findings highlight the importance of aligning MFA design and policies with users' needs and understanding. Innovations such as adaptive MFA and Single Input Multi-Factor Authentication (SIMFA) are recommended to enhance both security and user convenience.

Kata Kunci: Implementasi MFA, Model Mental Pengguna, *Multi-Factor Authentication* (*MFA*), *Systematic Literature Review*

Abstract: Studi ini merupakan *Systematic Literature Review* (SLR) yang bertujuan untuk menganalisis dampak model mental pengguna terhadap implementasi *Multi-Factor Authentication* (MFA) dalam mitigasi risiko *password guessing* di lingkungan organisasi. Sebanyak 200 artikel awal diidentifikasi dari *Google Scholar* menggunakan kata kunci terkait MFA, dan setelah proses seleksi PRISMA, diperoleh 10 artikel inti yang dianalisis lebih lanjut. Literatur yang dikaji berasal dari publikasi tahun 2020–2025, baik dalam bahasa Indonesia maupun Inggris. Hasil studi menunjukkan bahwa pengguna ahli cenderung memahami MFA sebagai lapisan keamanan tambahan yang bermanfaat, sedangkan pengguna non-ahli menganggapnya sebagai tugas yang merepotkan. Hambatan utama meliputi kurangnya pemahaman, persepsi risiko yang rendah, serta ketergantungan pada perangkat seluler. Analisis dilakukan dengan pendekatan model mental untuk memahami perbedaan persepsi dan pengalaman pengguna terhadap MFA. Temuan menekankan pentingnya menyesuaikan desain dan kebijakan MFA agar selaras dengan kebutuhan dan pemahaman pengguna. Inovasi seperti MFA adaptif dan *Single Input Multi-Factor Authentication* (SIMFA) direkomendasikan guna meningkatkan keamanan sekaligus kenyamanan penggunaan.

.

1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi telah mendorong sebagian besar aktivitas manusia untuk beralih ke ranah digital, termasuk layanan berbasis web seperti perbankan daring, *e-commerce*, dan sistem uang seluler. Transformasi ini bertujuan untuk meningkatkan kenyamanan dan kepuasan pengguna. Namun, seiring dengan kemudahan akses ini, ancaman siber juga meningkat secara signifikan, menciptakan tantangan besar bagi keamanan siber [1]. Penelitian ini difokuskan pada area *computer security* sesuai dengan *scope* pada jurnal DINAMIK unisbank. Penelitian ini menggarisbawahi pentingnya pendekatan keamanan yang lebih kompresensif melalui penerapan *Multi-Factor Authentication(MFA).* Dimana metode autentikasi satu faktor (SFA) tradisional, seperti kata sandi, yang telah lama menjadi tulang punggung keamanan akses, terbukti semakin rentan terhadap berbagai serangan siber [4]. Kata sandi dapat dengan mudah diungkap atau digunakan kembali oleh pihak yang tidak bertanggung jawab.

Salah satu ancaman yang paling umum dan persisten adalah serangan *password guessing*, termasuk *brute force*, *dictionary attack*, *rainbow table*, dan rekayasa sosial (*social engineering*)

[9]. Serangan ini mengeksploitasi kelemahan kata sandi yang seringkali tidak cukup kuat atau dapat diprediksi. Mengingat sensitivitas informasi pengguna yang disimpan dan diproses oleh aplikasi daring, terutama di sektor keuangan dan organisasi, autentikasi yang lebih kuat menjadi suatu keharusan.

Sebagai respons terhadap kerentanan ini, autentikasi *Multi-Factor Authentication* (*MFA*) telah diusulkan dan diterapkan secara luas [2]. MFA meningkatkan keamanan dengan memerlukan dua atau lebih faktor verifikasi dari kategori yang berbeda, seperti "sesuatu yang diketahui" (kata sandi, PIN), "sesuatu yang dimiliki" (token, kartu pintar, perangkat seluler), dan "sesuatu yang merupakan diri pengguna" (biometrik seperti sidik jari, pengenalan wajah, suara) [6]. Pendekatan ini secara signifikan memperkuat lapisan keamanan dan mempersulit penyusup untuk mendapatkan akses tidak sah, bahkan jika salah satu faktor autentikasi telah disusupi. MFA diakui oleh regulasi internasional seperti Uni Eropa dan publikasi NIST sebagai mekanisme autentikasi yang menawarkan tingkat keamanan yang lebih tinggi [9].

Meskipun MFA menawarkan manfaat keamanan yang jelas, tingkat implementasinya masih cenderung lambat. Tantangan utama seringkali terletak pada persepsi dan pengalaman pengguna. Berbagai studi menunjukkan bahwa pengguna, terutama yang non-ahli, seringkali merasa frustrasi dan menganggap penggunaan MFA sebagai "beban" atau "tugas yang memberatkan" (*chore*). Kurangnya pemahaman tentang cara kerja MFA, persepsi yang keliru mengenai risiko daring, dan masalah usabilitas misalnya, ketergantungan pada perangkat seluler, masalah koneksi, kehabisan baterai menjadi hambatan yang signifikan [13]. Pengguna non-ahli bahkan cenderung melihat MFA sebagai "perlindungan tambahan" yang tidak perlu, dan merasa bahwa kata sandi yang digunakan sudah cukup aman.

Pentingnya memahami model mental pengguna menjadi krusial dalam menjembatani kesenjangan antara keamanan yang kuat dan pengalaman pengguna yang baik. Model mental pengguna mengacu pada bagaimana individu memahami dan berinteraksi dengan teknologi, termasuk persepsi terhadap risiko dan mekanisme keamanan. [16] Masih sedikit penelitian yang secara spesifik menyelidiki pemahaman dan penggunaan MFA oleh pengguna, dengan fokus pada model mental dan perilaku sosial mereka dalam konteks lingkungan kerja atau organisasi. Kesenjangan penelitian ini menimbulkan urgensi untuk menganalisis bagaimana persepsi dan pemahaman pengguna mempengaruhi keputusan untuk mengimplementasi atau menolak MFA, terutama dalam skenario mitigasi risiko *password guessing* yang terus berkembang. Jika langkah-langkah keamanan terlalu kompleks, masalah usabilitas dapat muncul, yang pada gilirannya dapat membuat pengguna frustrasi dan bahkan menyebabkan penolakan terhadap penggunaan MFA. Tinjauan literatur ini bertujuan untuk mengeksplorasi secara mendalam dampak model mental pengguna terhadap implementasi MFA untuk mitigasi risiko *password guessing* di konteks organisasi. Sebagian SLR sebelumnya lebih menekankan pada aspek teknis, kerangka kerja MFA, atau tantangan implementasi umum tanpa menggali secara mendalam pemahaman pengguna terhadap MFA. Kontribusi spesifik dari SLR ini adalah mengisi celah tersebut dengan menyoroti pengaruh model mental pengguna terhadap keberhasilan implementasi MFA, serta memetakan perbedaan persepsi antara pengguna ahli dan non-ahli, termasuk titik frustrasi, konteks organisasi, dan strategi peningkatan usabilitas. Studi ini menghadirkan pendekatan baru yang lebih berpusat pada pengguna, yang belum banyak dijelajahi secara sistematis pada kajian sebelumnya.

Kondisi penelitian saat ini telah mulai mengakui pentingnya menyeimbangkan keamanan dan usabilitas. Upaya terkini berfokus pada pengembangan kerangka MFA yang lebih adaptif dan ramah pengguna. Hal ini mencakup implementasi MFA ambang (*threshold MFA*) yang memungkinkan pengguna memilih faktor autentikasi secara fleksibel untuk mendeteksi penipuan yang lebih akurat dan keamanan yang adaptif terhadap ancaman *password guessing*, serta desain antarmuka pengguna yang lebih intuitif untuk memudahkan proses pendaftaran dan verifikasi. Kerangka MFA yang adaptif, seperti mengintegrasikan deteksi perilaku

pengguna berdasarkan lokasi atau peramban yang digunakan, juga sedang dikembangkan untuk mengurangi alarm palsu dan meningkatkan pengalaman pengguna secara keseluruhan. Namun, meskipun ada kemajuan dalam aspek teknis dan adaptabilitas, penelitian lebih lanjut masih diperlukan untuk memastikan implementasi yang luas dan efektif di kalangan pengguna non-ahli, serta untuk mengatasi "rasa tidak suka" pengguna terhadap MFA agar sistem yang aman benar-benar dapat dimanfaatkan secara optimal.

2. METODE PENELITIAN

Penelitian ini mengimplementasi pendekatan *Systematic Literatur Review* (SLR) untuk menganalisis secara komprehensif literatur yang relevan mengenai dampak model mental pengguna terhadap implementasi *Multi-Factor Authentication* (*MFA*), khususnya dalam konteks mitigasi risiko *password guessing* di lingkungan organisasi. Pendekatan ini memungkinkan identifikasi, evaluasi, dan sintesis bukti-bukti dari studi-studi terdahulu secara transparan dan metodis, sehingga dapat menjawab kesenjangan penelitian yang telah diidentifikasi.

Formulasi Permasalahan yang Lebih Rinci Meskipun MFA secara luas diakui sebagai solusi keamanan yang superior untuk mengatasi kerentanan autentikasi satu faktor seperti *password guessing*, tingkat implementasi dan penerimaannya di kalangan pengguna, terutama non-ahli, masih menjadi tantangan signifikan. Sumber-sumber menunjukkan adanya frustrasi dan persepsi negatif terhadap MFA, yang sering dianggap sebagai "tugas yang memberatkan" (*chore*). Kurangnya pemahaman pengguna tentang cara kerja MFA, persepsi risiko yang keliru, serta masalah *usability* yang disebabkan oleh ketergantungan perangkat dan kompleksitas proses, menghambat implementasi yang luas.

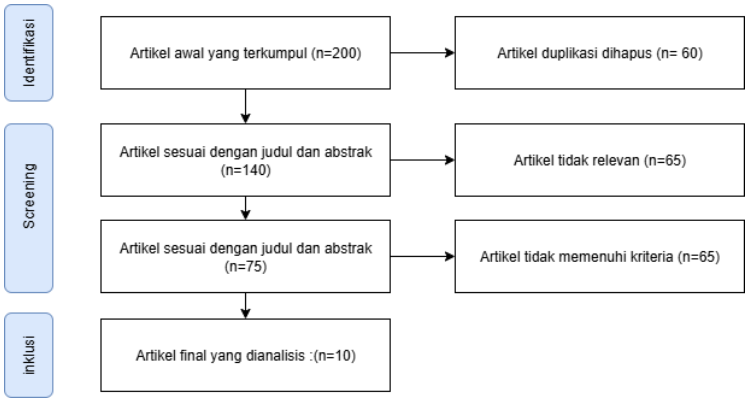
Di sisi lain, para ahli memiliki pemahaman yang lebih baik tentang MFA sebagai lapisan keamanan tambahan yang bermanfaat. Penelitian sebelumnya kurang secara spesifik mengeksplorasi bagaimana model mental pengguna yaitu pemahaman internal mereka tentang bagaimana sistem bekerja dan apa yang dilindunginya memengaruhi keputusan implementasi MFA dalam konteks organisasi, di mana kebijakan IT seringkali mewajibkan penggunaannya. Selanjutnya penelitian tinjauan literatur ini akan memformulasikan pertanyaan-pertanyaan kunci berikut:

1. Bagaimana persepsi risiko daring pengguna (terutama terkait serangan *password guessing*) memengaruhi kesediaan mereka untuk mengimplementasi MFA?
2. Bagaimana model mental pengguna (baik ahli maupun non-ahli) terhadap mekanisme dan fungsi MFA memengaruhi pengalaman dan penerimaan mereka?
3. Apa saja hambatan *usability* dan faktor-faktor penerimaan pengguna yang paling sering dilaporkan terkait implementasi MFA, terutama dalam lingkungan organisasi?
4. Bagaimana konteks organisasi (misalnya, kewajiban IT, pelatihan) memodifikasi dampak model mental pengguna terhadap implementasi MFA?
5. Apa saja rekomendasi dan solusi inovatif yang telah diajukan dalam literatur untuk meningkatkan implementasi MFA dengan mempertimbangkan model mental dan pengalaman pengguna?

Bahan/Data Bahan/data untuk tinjauan literatur ini akan bersumber dari publikasi ilmiah yang telah melalui tinjauan *peer-reviewed*. Ini mencakup artikel jurnal, makalah konferensi, dan laporan teknis dari basis data akademik terkemuka Google Scholar. Batasan waktu pencarian akan difokuskan pada literatur yang diterbitkan dalam lima tahun terakhir (2020-2025) untuk memastikan relevansi riset MFA saat ini.

Penelitian ini mengikuti alur *Systematic Literature Review* (SLR) yang dimodifikasi dengan pendekatan berbasis model mental pengguna, serta mengimplementasi tahapan

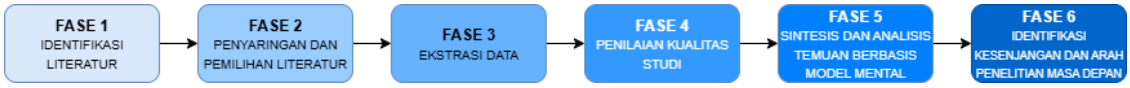
PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) untuk menjamin keterlacakan proses seleksi literatur. Diagram PRISMA mencakup empat tahap utama:



Gambar 1. Diagram PRISMA

- **Identifikasi:** Sebanyak 200 artikel awal diperoleh dari hasil pencarian menggunakan kombinasi kata kunci seperti "*Multi-Factor Authentication*," "*password guessing*," dan "*information system*"
- **Penyaringan:** Setelah proses penghapusan duplikat (60 artikel), sebanyak 140 artikel disaring berdasarkan judul dan abstrak dan 65 diantaranya dikeluarkan karena tidak relevan.
- **Uji Kelayakan:** Sebanyak 75 artikel dievaluasi secara penuh, dan 65 di antaranya dikeluarkan karena tidak memenuhi kriteria inklusi.
- **Inklusi:** Sebanyak 10 artikel yang relevan dimasukkan ke dalam analisis akhir.

Metode yang penelitian ini mengikuti alur *Systematic Literatur Review* (*SLR*) yang dimodifikasi untuk secara khusus menyoroti aspek model mental pengguna, seperti yang diinspirasi oleh studi-studi yang menginvestigasi persepsi pengguna. Alur penelitian ini akan dibagi menjadi enam fase utama seperti pada Gambar 2 berikut ini:



Gambar 2. Alur Penelitian

1. **Fase 1: Identifikasi Literatur**

Strategi Pencarian Kata Kunci: Menggunakan kombinasi kata kunci yang relevan dalam bahasa Inggris dan Indonesia, seperti "*Multi-Factor Authentication*" ATAU "MFA", "*User perception*" ATAU "*User mental model*" ATAU "*User experience*" ATAU "*Usability*" ATAU "*Acceptance*" ATAU "*Adoption*" ATAU "*Frustration*" ATAU "*Chore*", "*Password guessing*" ATAU "*Cybersecurity risk perception*", "*Organizational context*" ATAU "*Workplace*" ATAU "*Enterprise*". Basis Data Pencarian dilakukan pada basis data yang telah disebutkan di atas.

2. **Fase 2: Penyaringan dan Pemilihan Literatur**

Kriteria Inklusi Artikel disertakan jika: Fokus utama atau sebagian signifikan membahas MFA, Menganalisis persepsi, pengalaman, model mental, usabilitas, atau penerimaan pengguna terhadap MFA, Mengeksplorasi implementasi MFA dalam konteks mitigasi risiko siber, khususnya *password guessing*, Berada dalam konteks penggunaan pribadi atau organisasi (dengan prioritas pada organisasi), Diterbitkan dalam bahasa Inggris atau Indonesia,

Merupakan artikel jurnal, prosiding konferensi, atau laporan teknis. Kriteria Eksklusi artikel dikecualikan jika: Hanya berfokus pada aspek teknis MFA tanpa membahas pengguna, Merupakan ulasan literatur umum tanpa analisis mendalam tentang model mental/persepsi pengguna, Tidak relevan dengan konteks keamanan siber atau autentikasi, merupakan bab buku, paten.

3. **Fase 3: Ekstraksi Data**

Dari setiap artikel yang dipilih informasi kunci akan diekstrak termasuk: tahun dan jenis publikasi, jenis MFA yang diteliti, metodologi penelitian yang digunakan (misalnya, survei, wawancara, eksperimen, studi kasus), demografi partisipan (jika ada, misalnya, ahli vs. non-ahli, seperti dalam), temuan terkait persepsi risiko pengguna, temuan terkait model mental pengguna tentang cara kerja MFA, temuan tentang hambatan usabilitas dan alasan penolakan/frustrasi pengguna, implikasi atau rekomendasi untuk peningkatan implementasi MFA.

4. **Fase 4: Penilaian Kualitas Studi**

Dalam proses peninjauan literatur secara sistematis setiap artikel yang telah lolos uji kelayakan awal dievaluasi kualitasnya berdasarkan sejumlah indikator, antara lain relevansi topik terhadap tujuan SLR, kejelasan metodologi penelitian seperti penggunaan wawancara, survei, atau eksperimen, serta informasi mengenai karakteristik partisipan, misalnya apakah responden merupakan pengguna ahli atau non-ahli. Penilaian juga mencakup ketepatan analisis terhadap model mental dan persepsi risiko yang dikaji, serta kontribusi artikel dalam memberikan solusi atau rekomendasi terkait pengembangan *Multi-Factor Authentication* (MFA). Artikel yang tidak secara eksplisit menjelaskan elemen-elemen tersebut atau hanya bersifat teknis tanpa kontribusi konseptual maupun praktis tidak diikutsertakan dalam proses sintesis akhir.

5. **Fase 5: Sintesis dan Analisis Temuan Berbasis Model Mental**

Merupakan kontribusi modifikasi metode yang signifikan dalam tinjauan literatur yang diteliti saat ini. Data yang diekstrak dianalisis dan disintesis melalui lensa model mental pengguna dan persepsi risiko, dengan mengimplementasi kategorisasi yang terinspirasi dari analisis yang berfokus pada pemetaan kesenjangan antara desain MFA yang menekankan keamanan dan pemahaman/harapan pengguna yang seringkali mengutamakan kenyamanan. Lima dimensi analisis utama diterapkan sebagai **perbandingan model mental ahli vs. non-ahli,** dimana hal tersebut untuk membedakan bagaimana pengguna ahli dan non-ahli memahami MFA. Ahli menganggap MFA sebagai lapisan tambahan yang berguna sementara non-ahli menganggap MFA sebagai beban atau keamanan yang tidak perlu. Selanjutnya **identifikasi titik frustrasi pengguna,** yang mengidentifikasi secara spesifik sumber-sumber frustrasi yang dialami pengguna misalnya, ketergantungan pada perangkat seluler, masalah koneksi, *time-consuming*. Kemudian **korelasi persepsi risiko dan implementasi** yang menganalisis bagaimana pemahaman atau kesalahpahaman pengguna tentang risiko siber termasuk *password guessing* memengaruhi keputusan mereka untuk mengimplementasi atau menolak MFA. **Dampak dalam konteks organisasi** yang mengeksplorasi bagaimana lingkungan kerja dimana MFA menjadi kebijakan wajib, sehingga dukungan IT memengaruhi perilaku implementasi MFA, dibandingkan dengan penggunaan pribadi. Terakhir **analisis rekomendasi peningkatan usabilitas** dimana mensintesis solusi yang diusulkan dalam literatur untuk meningkatkan usabilitas MFA, seperti peningkatan edukasi pengguna, eliminasi ketergantungan perangkat tunggal, dan komunikasi risiko yang lebih efektif.

6. **Fase 6: Identifikasi Kesenjangan dan Arah Penelitian Masa Depan**

Berdasarkan sintesis dan analisis, kesenjangan dalam literatur diidentifikasi masuk area di mana penelitian tentang model mental pengguna MFA masih terbatas. Seperti, kurangnya studi tentang dampak budaya atau demografi pada model mental pengguna MFA untuk peningkatan usabilitas yang perlu divalidasi secara empiris. Identifikasi tersebut akan menjadi

dasar untuk menyarankan arah penelitian di masa depan yang relevan untuk mengatasi masalah implementasi MFA.

Penulisan ini bertujuan untuk memberikan pandangan yang mendalam dan terstruktur tentang peran model mental pengguna dalam implementasi MFA serta memungkinkan identifikasi *pain points* spesifik dan mengarahkan pada rekomendasi yang lebih berorientasi pengguna untuk meningkatkan keamanan autentikasi di lingkungan digital.

3 HASIL DAN PEMBAHASAN

Implementasi Metodologi *Systematic Literatur Review* (*SLR*)

Metodologi *Systematic Literatur Review* (*SLR*), yang dimodifikasi dengan fokus pada model mental pengguna, diimplementasikan melalui serangkaian fase yang sistematis dan transparan:

1. **Fase 1: Identifikasi Literatur** Pada fase ini, strategi pencarian kata kunci yang komprehensif diterapkan pada basis data akademik Google Scholar. Kata kunci yang digunakan meliputi kombinasi istilah-istilah seperti "*Multi-Factor Authentication*" ATAU "MFA", dikombinasikan dengan "*User experience*" ATAU "*Usability*" ATAU "*Acceptance*" ATAU "*Chore*", serta "*Password guessing*" dan "*Organizational context*". Batasan waktu pencarian difokuskan pada literatur yang diterbitkan dalam lima tahun terakhir (2020-2025) untuk memastikan relevansi dengan kondisi terkini riset MFA. Proses ini menghasilkan kumpulan awal 200 artikel potensial. [20]

2. **Fase 2: Penyaringan dan Pemilihan Literatur** Artikel-artikel yang teridentifikasi kemudian melalui proses penyaringan ketat berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi mencakup fokus utama pada MFA, analisis persepsi/pengalaman/model mental/usabilitas pengguna, eksplorasi implementasi MFA dalam konteks mitigasi risiko siber khususnya *Password guessing*, relevansi dengan konteks organisasi, serta publikasi dalam bahasa Inggris atau Indonesia sebagai artikel jurnal, prosiding konferensi, atau laporan teknis. Artikel yang hanya berfokus pada aspek teknis MFA tanpa pembahasan pengguna, atau tinjauan literatur umum tanpa analisis model mental mendalam, dikecualikan. Proses ini melibatkan peninjauan judul, abstrak, dan kemudian teks lengkap untuk memastikan relevansi dan kualitas sehingga menghasilkan 10 kumpulan artikel inti yang memenuhi persyaratan tinjauan sistematis.

3. **Fase 3: Ekstraksi Data** Dari setiap artikel yang terpilih, informasi kunci diekstraksi secara terstruktur. Data yang diekstraksi meliputi tahun publikasi, jenis MFA yang diteliti, metodologi penelitian yang digunakan, temuan terkait persepsi risiko pengguna, temuan tentang model mental pengguna terhadap mekanisme dan fungsi MFA, hambatan usabilitas dan faktor penerimaan pengguna, serta implikasi atau rekomendasi untuk peningkatan implementasi MFA. Tertuang dalam 2 tabel berikut ini:

Tabel 1. Hasil Penyeringan dan Pemilihan Literatur

No.	Tahun	Topik Utama	Jenis MFA	Metodologi	Temuan Khusus
1	2020	Eksplorasi model mental pengguna terhadap MFA	*Password, OTP, Biometrics, Behavior-based* [17]	Wawancara semi-terstruktur, kualitatif	Ahli menganggap MFA berguna; non-ahli melihatnya sebagai beban
2	2021	*SIMFA* (*Single Channel Input*	Suara, Gerakan,	Desain sistem dan	Otentikasi paralel melalui saluran tunggal.

		MFA) – US Patent US10904246	Input Tunggal [5]	dokumentasi paten	
3	2021	MFA untuk aplikasi *mobile money*	*PIN, OTP, Prototipe Mobile*	*Prototyping evolusioner*	Rentan terhadap rekayasa sosial & MITM; sistem G-MoMo dikembangkan.
4	2021	Threshold MFA (T-MFA)	*Adaptive selection of n-of-t factors* [9]	Desain protokol, evaluasi formal	T-MFA tingkatkan fleksibilitas dan kegunaan.
5	2021	Skema SELAMAT untuk Industrial IoT	*Smartcard, OTP, Biometrics*	*Formal analysis* (AVISPA, BAN *logic*)	Skema ringan dan aman untuk perangkat industri lintas *platform*.
6	2022	MFA untuk transaksi keuangan berbasis *cloud*	*OTP, PIN*, Kartu, *Biometrics*	Pengembangan sistem, analisis kinerja	Keamanan transaksi finansial menjadi prioritas tinggi.
7	2023	Tinjauan sistematis tentang MFA dan tantangan	Semua jenis (*OTP, biometrics, knowledge, adaptive*) [6]	*Review* literatur	Sorotan pada risiko kebocoran data biometrik dan kebutuhan adaptivitas.
8	2023	*Framework multi-layer MFA* untuk *cloud*	Kombinasi *multilayer (biometrik, OTP, behavior)*	Desain & pengujian *framework*	Kegunaan penting; antarmuka intuitif dibutuhkan.
9	2024	Integrasi MFA dan *Machine Learning* untuk transaksi keuangan *online*	*PIN, OTP, biometrik, ML detection* [6]	*Framework*, evaluasi keamanan	Kata sandi tidak cukup; perlu ML & faktor tambahan adaptif

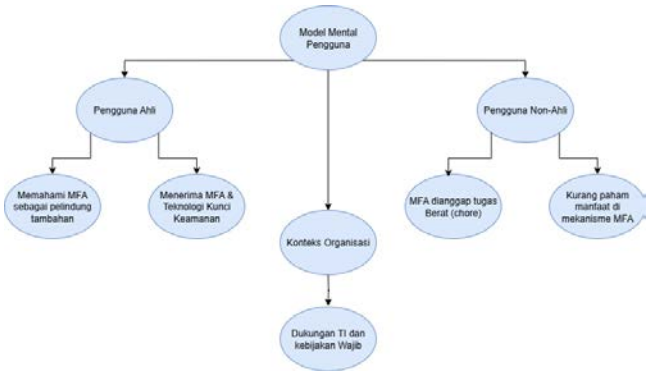
Tabel 2. Ekstraksi Data Penelitian MFA

No.	Aspek	Temuan dan Tantangan
1	Persepsi Pengguna	MFA dianggap membebani, terutama oleh non-ahli; kesadaran ancaman tinggi, mitigasi rendah [2,14]
2	Hambatan Usabilitas	Pendaftaran sulit, ketergantungan perangkat, adaptasi rendah, kompleksitas teknis [17,8,10]
3	Faktor Penerimaan	Sistem adaptif, T-MFA, antarmuka intuitif, pemakaian ML meningkatkan kegunaan [6,9,7]

4	Rekomendasi Peningkatan	Perbaikan UI, eliminasi ketergantungan mobile, edukasi pengguna, pemulihan akun lebih baik [3]

4. **Fase 4: Penilaian Kualitas Studi** setiap artikel dinilai berdasarkan relevansi topik, kejelasan metodologi, karakteristik partisipan, analisis terhadap model mental dan persepsi risiko, serta kontribusi pada solusi MFA. Artikel yang tidak memenuhi indikator tersebut atau hanya bersifat teknis tanpa dimensi pengguna dikeluarkan dari sintesis. Analisis akhir difokuskan pada sintesis kritis berbasis model mental, dengan memetakan kesenjangan antara desain keamanan MFA dan ekspektasi kenyamanan pengguna, yang menghasilkan lima dimensi utama sebagai dasar interpretasi temuan dan arah rekomendasi pengembangan sistem MFA yang lebih adaptif dan ramah pengguna.

5. **Fase 5: Sintesis dan Analisis Temuan Berbasis Model Mental** merupakan inti dari kontribusi modifikasi metodologi dan bagaimana masalah penelitian dipecahkan. Data yang diekstraksi tidak hanya dirangkum, tetapi dianalisis dan disintesis secara kritis melalui lensa model mental pengguna dan persepsi risiko, dengan mengimplementasi kategorisasi yang terinspirasi oleh studi. Analisis berfokus pada pemetaan kesenjangan antara desain MFA yang menekankan keamanan dan pemahaman/harapan pengguna yang seringkali mengutamakan kenyamanan. Lima dimensi analisis utama diterapkan:



Gambar 3. Sintesis model mental pengguna terhadap MFA

Perbandingan Model Mental Ahli vs. Non-Ahli: Penelitian ini mengkonfirmasi bahwa terdapat perbedaan signifikan dalam model mental antara pengguna ahli dan non-ahli. Pengguna ahli cenderung memahami MFA sebagai "lapisan verifikasi tambahan yang berguna" dan "lapisan pelindung berganda". Pengguna ahli memiliki pemahaman sistematis tentang cara kerja MFA dan manfaat keamanannya. Pengguna ahli juga lebih menyukai teknologi modern seperti kunci keamanan fisik dan notifikasi seluler untuk MFA. Sebaliknya, pengguna non-ahli melihat MFA sebagai "layanan keamanan" atau "keamanan tambahan" tanpa pemahaman mendalam tentang implementasi internal atau faktor-faktor di baliknya. Non-Ahli sering menganggap MFA sebagai "tugas yang memberatkan" (*chore*) dan akan memilih untuk tidak menggunakannya jika ada pilihan. Non-Ahli merasa MFA menambah beban kerja dan tidak melihat banyak manfaat tambahan, bahkan tidak yakin apa yang sebenarnya dilindungi oleh MFA. Di lingkungan organisasi, pengguna non-ahli cenderung hanya mengimplementasi MFA jika diwajibkan oleh manajemen TI. [2]

Identifikasi Titik Frustrasi Pengguna: Baik ahli maupun non-ahli sama-sama mengungkapkan frustrasi terhadap penggunaan MFA, seringkali menyebutnya sebagai *'chore'*. Titik frustrasi utama yang diidentifikasi meliputi ketergantungan pada perangkat seluler, yang dianggap sebagai hambatan terbesar bagi perluasan MFA. Masalah-masalah spesifik yang

dilaporkan meliputi masalah koneksi internet, perangkat kehabisan baterai, ketidakmampuan mengakses perangkat dalam waktu singkat, atau perangkat hilang. Kurangnya pemahaman pengguna tentang metode pemulihan akun yang aman setelah kehilangan perangkat juga menjadi masalah. [17],[8]

Korelasi Persepsi Risiko dan Implementasi: Ditemukan bahwa meskipun pengguna secara umum menyadari ancaman keamanan *online* (terutama *phishing* dan *password guessing*), banyak yang gagal mengambil tindakan mitigasi yang tepat, termasuk penggunaan alat keamanan. Hal ini seringkali disebabkan oleh ketidakmampuan mereka dalam memahami mitigasi risiko dan perlindungan data, yang pada akhirnya menghambat implementasi MFA. Para ahli menunjukkan pemahaman yang lebih baik tentang risiko dan upaya untuk melindungi data mereka. [14,2]

Dampak Konteks Organisasi: Dalam konteks organisasi, MFA seringkali diwajibkan, yang mana menjadi pendorong implementasi di kalangan non-ahli. Lingkungan kerja dengan dukungan TI yang berdedikasi dapat membantu mengurangi kerentanan yang timbul dari masalah seperti kehilangan perangkat, karena adanya personel dukungan yang dapat membantu proses pemulihan. Hal ini menunjukkan bahwa kebijakan organisasi dan dukungan teknis memainkan peran krusial dalam mengatasi hambatan implementasi MFA.

Analisis Rekomendasi Peningkatan Usabilitas: Literatur menyarankan beberapa solusi inovatif untuk meningkatkan implementasi MFA seperti peningkatan edukasi pengguna dalam hal ini perlu adanya edukasi yang lebih proaktif dan efektif mengenai kesadaran risiko dan pengembangan *self-efficacy* melalui antarmuka pengguna. [18] Eliminasi ketergantungan perangkat tunggal dengan mengembangkan teknologi verifikasi baru seperti *Secure Element*, atestasi jarak jauh menggunakan *Trusted Platform Modules* (*TPM*), dan *environment fingerprinting* dapat mengurangi ketergantungan pada perangkat seluler. Kemudian peningkatan prosedur pemulihan yang penting untuk memperkenalkan dan menyederhanakan mekanisme pemulihan akun bagi pengguna rata-rata, terutama saat perangkat pendamping hilang. Terakhir Desain antarmuka yang lebih intuitif yang memudahkan penemuan fitur pendaftaran MFA misalnya, memunculkan *prompt* setelah autentikasi kata sandi pertama yang berhasil atau menempatkan pengaturan MFA di lokasi yang lebih mudah ditemukan.

6. **Fase 6: Identifikasi Kesenjangan dan Arah Penelitian Masa Depan** Dari sintesis ini, beberapa kesenjangan penelitian teridentifikasi. Studi tentang dampak model mental pengguna MFA masih terbatas pada faktor budaya atau demografi. Validasi empiris dari rekomendasi peningkatan usabilitas yang diusulkan masih perlu untuk dilakukan. Selain itu, diperlukan penelitian lebih lanjut untuk memeriksa perbedaan antara teknologi MFA spesifik dapat meningkatkan usabilitas tanpa menambah kompleksitas, seperti yang disarankan dalam beberapa penelitian terkait MFA. [15]

Pemecahan Masalah dan Kontribusi Signifikan

Metodologi *Systematic Literatur Review* (*SLR*) secara efektif memecahkan masalah penelitian dengan menyediakan pemahaman yang terstruktur dan mendalam tentang mengapa tingkat implementasi MFA masih rendah meskipun manfaat keamanannya superior, khususnya dalam konteks mitigasi risiko *password guessing* di organisasi. Dengan secara mengekstraksi dan mensintesis temuan dari berbagai studi melalui lensa model mental pengguna baik ahli maupun non-ahli, penelitian ini berhasil memetakan kesenjangan kritis antara tujuan keamanan sistem dan realitas pengalaman serta pemahaman pengguna.

Kontribusi Signifikan Penelitian:

1. **Sintesis Model Mental yang Baru dan Bernuansa:** Kontribusi utama penelitian ini adalah sintesis terstruktur dari temuan-temuan terfragmentasi mengenai model mental

pengguna MFA. Dengan membedakan secara jelas antara pemahaman ahli dan non-ahli, penelitian ini menyediakan pandangan yang lebih terhadap hambatan psikologis dan persepsi terhadap MFA. Hal ini melampaui pernyataan umum bahwa implementasi MFA lambat dengan menjelaskan mengapa fenomena ini terjadi dari sudut pandang kognitif pengguna.

2. **Identifikasi Titik Frustrasi Pengguna yang Spesifik:** Melalui analisis terperinci, penelitian ini secara eksplisit mengidentifikasi titik sakit (*pain points*) pengguna MFA, seperti ketergantungan pada perangkat seluler, masalah koneksi, dan kurangnya mekanisme pemulihan yang intuitif. Hal tersebut memberikan gambaran yang jelas tentang area-area yang memerlukan intervensi desain atau kebijakan.
3. **Pemahaman Praktis untuk Perancangan dan Kebijakan:** Berdasarkan identifikasi model mental yang tidak selaras dan titik frustrasi, penelitian ini menyajikan rekomendasi yang konkret dan dapat ditindaklanjuti untuk pengelola TI, pengembang, dan pembuat kebijakan. Rekomendasi ini mencakup peningkatan edukasi pengguna, penyederhanaan antarmuka, diversifikasi faktor autentikasi di luar ketergantungan seluler, dan perbaikan prosedur pemulihan akun. Hal ini secara langsung mendukung pengembangan solusi MFA yang lebih berpusat pada pengguna dan efektif.

Penekanan pada Usabilitas sebagai Pilar Keamanan: Penelitian ini secara tegas memperkuat gagasan bahwa keamanan yang efektif hanya dapat dicapai dengan meningkatkan usabilitas alat keamanan. Dengan menyoroti bagaimana model mental pengguna secara langsung memengaruhi perilaku implementasi, penelitian ini menekankan bahwa aspek manusia sama pentingnya dengan aspek teknis dalam mencapai postur keamanan yang kuat.

4. KESIMPULAN

Tinjauan literatur ini secara komprehensif menyimpulkan bahwa model mental pengguna merupakan faktor krusial yang secara signifikan memengaruhi tingkat implementasi dan efektivitas *Multi-Factor Authentication*(*MFA*) sebagai strategi mitigasi risiko password guessing di lingkungan organisasi. Penelitian ini secara langsung menjawab permasalahan fundamental terkait lambatnya implementasi MFA, di tengah kebutuhan mendesak akan peningkatan keamanan siber, dengan menyoroti kesenjangan persepsi dan pengalaman pengguna yang menjadi penghambat utama.

Berdasarkan analisis hasil penelitian, dapat disimpulkan hal-hal sebagai berikut:

a. MFA terbukti secara fundamental meningkatkan keamanan siber dibandingkan otentikasi satu faktor (SFA) tradisional. Hal tersebut secara signifikan mengurangi kerentanan terhadap serangan *password guessing* seperti *phishing*, pencurian identitas, *rainbow table*, *dictionary attack*, dan *social engineering*. MFA mensyaratkan dua atau lebih faktor otentikasi dari kategori yang berbeda, meliputi: "sesuatu yang Anda ketahui" (seperti kata sandi atau PIN), "sesuatu yang Anda miliki" (seperti token atau perangkat seluler yang menghasilkan OTP), dan "sesuatu yang Anda adalah" (seperti biometrik berupa sidik jari, pengenalan wajah, atau pola suara).
b. Model mental pengguna secara langsung memengaruhi implementasi MFA. Pengguna ahli memiliki pemahaman yang lebih baik tentang cara kerja MFA, pengguna ahli melihatnya sebagai lapisan otentikasi tambahan yang bermanfaat untuk perlindungan berlapis, dan cenderung mengimplementasi teknologi modern seperti kunci keamanan atau notifikasi seluler, serta bersedia melindungi akun bernilai tinggi pengguna ahli dengan MFA. Sebaliknya, pengguna non-ahli seringkali tidak merasakan manfaat tambahan dari MFA dan memandangnya sebagai keamanan tambahan tanpa kejelasan tentang apa yang sebenarnya dilindungi. Mereka kerap menganggap MFA sebagai tugas yang merepotkan (*chore*) dan cenderung memilih untuk tidak menggunakannya

jika diberi pilihan, meskipun implementasinya sering terjadi di lingkungan kerja karena penegakan kebijakan TI. Pengguna non-ahli juga sering kesulitan membedakan antara otentikasi dua faktor (2FA) dan *muti-factor authentication* (MFA). Terlepas dari tingkat keahlian, kedua kelompok pengguna menyatakan frustrasi terkait ketergantungan pada perangkat seluler, seperti masalah koneksi, baterai habis, atau perangkat yang hilang, yang menciptakan ketidakseimbangan antara keamanan dan usabilitas.

Penelitian ini telah memecahkan masalah penelitian dengan secara komprehensif menganalisis bagaimana pemahaman mendalam tentang model mental pengguna dapat menjadi kunci untuk meningkatkan implementasi dan efektivitas MFA. Inovasi-inovasi MFA yang diidentifikasi dari tinjauan literatur ini menawarkan solusi yang selaras dengan tantangan model mental pengguna seperti Otentikasi *Muti-factor* Adaptif menggunakan biometrik yang dapat dibatalkan (*cancelable biometrics*) dan OTP melalui notifikasi *push* dianggap lebih aman dan efisien daripada SMS atau email. *Single Input, Multi-Factor Authentication(SIMFA)* yang menerima satu masukan pengguna misalnya, suara, gerakan, atau teks dan memprosesnya secara paralel melalui berbagai saluran otentikasi pengetahuan dan non-pengetahuan dapat mengurangi beban pengguna sambil meningkatkan keamanan secara signifikan. Inovasi-inovasi tersebut, yang muncul dari pemahaman model mental, secara langsung mengatasi masalah implementasi yang lambat dengan menawarkan solusi yang lebih fleksibel, efisien, dan mengurangi beban pengguna, sekaligus mempertahankan atau meningkatkan tingkat keamanan siber secara keseluruhan.

Tinjauan literatur sistematis menyimpulkan bahwa model mental pengguna merupakan faktor krusial yang memengaruhi tingkat implementasi dan efektivitas *Multi-Factor Authentication* (MFA) sebagai strategi mitigasi risiko *password guessing* di lingkungan organisasi. Studi tinjauan literatur sistematis mengungkap bahwa persepsi pengguna non-ahli terhadap MFA sebagai beban, serta ketergantungan pada perangkat seluler, menjadi hambatan utama adopsi, meskipun secara teknis MFA terbukti mampu meningkatkan keamanan siber secara signifikan. Pengguna ahli cenderung mengadopsi MFA secara sadar dan melihatnya sebagai perlindungan berlapis, sementara pengguna non-ahli hanya menerapkan MFA jika diwajibkan oleh organisasi. Inovasi berbasis pemahaman model mental pengguna, seperti MFA adaptif dan *Single Input Multi-Factor Authentication* (SIMFA), direkomendasikan untuk menyeimbangkan aspek keamanan dan kenyamanan. Batasan studi tinjauan literatur sistematis terletak pada ruang lingkup data yang digunakan, yaitu hanya mengkaji 10 artikel ilmiah terpilih dari literatur akademik *peer-reviewed* yang berfokus pada rentang tahun 2020–2025 dan konteks organisasi. Studi tinjauan literatur sistematis belum mencakup data empiris primer atau pengalaman langsung dari sektor-sektor di luar organisasi berbasis TI. Temuan dan rekomendasi dalam kajian berpotensi digeneralisasi ke sektor lain seperti layanan keuangan digital, pendidikan daring, dan sistem kesehatan berbasis *cloud*, dengan mempertimbangkan penyesuaian konteks dan karakteristik pengguna masing-masing. Penelitian lanjutan disarankan untuk menguji temuan ini secara lintas sektor melalui studi empiris yang lebih luas dan inklusif.

5. SARAN

Rekomendasi Akademik

Penelitian di masa depan harus fokus pada pengembangan dan pengujian metodologi edukasi serta komunikasi risiko yang lebih efektif, terutama yang disesuaikan untuk pengguna non-ahli, guna meningkatkan kesadaran dan persepsi nilai keamanan MFA. Selanjutnya Perlu

dilakukan studi lebih lanjut untuk merancang sistem MFA yang inheren mudah digunakan dan intuitif, meminimalkan kompleksitas yang memicu frustrasi dan resistensi pengguna[19]. Terakhir eksplorasi dan pengembangan teknologi alternatif untuk MFA misalnya, *Secure Element*, *remote attestation*, atau *environment fingerprinting* penting untuk mengurangi ketergantungan pada perangkat seluler yang rentan terhadap masalah konektivitas atau daya.

Rekomendasi Tindak Lanjut Nyata

Rekomendasi desain yang diusulkan dalam tinjauan ini perlu divalidasi melalui studi empiris dan survei kuesioner berskala besar untuk memastikan validitas eksternal di populasi pengguna yang lebih luas, melengkapi wawasan mendalam dari studi kualitatif. Penelitian selanjutnya dapat mengeksplorasi secara rinci perbedaan dalam pengalaman pengguna dan tingkat implementasi antara teknologi MFA yang spesifik, serta mengumpulkan data demografi untuk memahami bagaimana faktor-faktor sosial-budaya memengaruhi implementasi MFA.

DAFTAR PUSTAKA

[1] A. H. Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, “Current multi-factor of authentication: Approaches, requirements, attacks and challenges,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 1, pp. 1–19, 2023, doi: 10.14569/IJACSA.2023.0140119.

[2] S. Das, B. Wang, A. Kim, and L. J. Camp, “MFA is a necessary chore! Exploring user mental models of multi-factor authentication technologies,” in *Proc. 53rd Hawaii Int. Conf. Syst. Sci. (HICSS-53)*, 2020, pp. 5782–5791.

[3] D. Prabakaran and S. Ramachandran, “Multi-factor authentication for secured financial transactions in cloud environment,” *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1781–1798, 2022.

[4] M. A. Nugraha, D. Arisandi, and N. J. Perdana, “Pengamanan website e-commerce menggunakan multi-factor authentication,” *J. Ilmu Komputer dan Sistem Informasi*, vol. 9, no. 1, pp. 158–162, [n.d.].

[5] S. Chari, Z. Gu, H. Huang, and D. Pendarakis, “Single channel input multi-factor authentication via separate processing pathways,” U.S. Patent 10,904,246 B2, Feb. 2, 2021.

[6] A. M. Aburbeian and M. Fernández-Veiga, “Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning,” *AI*, vol. 5, no. 1, pp. 177–194, 2024, doi: 10.3390/ai5010010.

[7] A. M. Mostafa *et al.*, “Strengthening cloud security: An innovative multi-factor multi-layer authentication framework for cloud user authentication,” *Appl. Sci.*, vol. 13, no. 19, Art. 10871, 2023, doi: 10.3390/app131910871.

[8] G. Ali, M. A. Dida, and A. E. Sam, “A secure and efficient multi-factor authentication algorithm for mobile money applications,” *Future Internet*, vol. 13, no. 12, Art. 299, 2021, doi: 10.3390/fi13120299.

[9] W. Li, H. Cheng, P. Wang, and K. Liang, “Practical threshold multi-factor authentication,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3573–3588, 2021, doi: 10.1109/TIFS.2021.3081263.

[10] H. Khalid, S. J. Hashim, S. M. Syed Ahmad, F. Hashim, and M. A. Chaudhary, “SELAMAT: A new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems,” *Sensors*, vol. 21, no. 4, Art. 1428, 2021.

[11] S. AlJanah, N. Zhang, and S. W. Tay, “A multi-factor homomorphic encryption-based method for authenticated access to IoT devices,” *arXiv preprint*, arXiv:2307.03291, 2023.

[12] S. AlJanah, N. Zhang, and S. W. Tay, “M2I: Multi-factor multi-level and interaction-based authentication framework for IoT,” *arXiv preprint*, 2022.

[13] B. Yang, X. Li, Y. Xie, and H. Yu, “AI-oriented two-phase multi-factor authentication in SAGINs,” *arXiv preprint*, arXiv:2303.17833, 2023.

[14] W. d. R. Bezerra, P. A. Costa, and R. D. Alves, “Characteristics and main threats about multi-factor authentication: A survey,” *arXiv preprint*, 2022.

[15] T. Suleski, J. Nielsen, and J. Edberg, “A review of multi-factor authentication in the Internet of Healthcare Things,” *Digital Health*, vol. 9, pp. 1–12, 2023, doi: 10.1177/20552076231177144.

[16] S. Mali, “Assessing the effectiveness of multi-factor authentication in cloud-based big data environments,” *IoT and Cloud Computing*, vol. 12, no. 2, 2024.

[17] E. Marasco, R. Ghiass, and A. Ross, “Biometric multi-factor authentication: On the usability of the FingerPIN scheme,” *Security and Privacy*, vol. 5, no. 1, pp. 1–12, 2022.

[18] M. Saleh and A. Abdel-Hamid, “A blockchain-based multi-factor authentication framework for IoT devices,” *Sensors*, vol. 23, no. 4, Art. 1890, 2023.

[19] A. I. Abubakar, N. Hashim, and Y. Yahya, "A lightweight multi-factor authentication protocol for resource-constrained environments," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, 2022.
[20] R. Chatterjee and M. Green, "The security of modern password expiration: An MFA perspective," in *Proc. IEEE Symp. Security and Privacy*, 2021, pp. 1–15.