Jurnal Ekonomi, Teknologi dan Bisnis (JETBIS)
Volume 5, Number 10 October 2026, pp. 634-652
e-ISSN 2962-9330
https://doi.org/10.57185/ jetbis.v5i10.358

Peran Keamanan Siber dan Kepercayaan Digital dalam Keberhasilan Pelayanan Publik Berbasis Elektronik melalui Pengembangan Model Konseptual

Mar'atus Solikhah
STMIK LIKMI, Bandung, Indonesia
Corresponding Author: maratussholikhah615@gmail.com

Keywords:
cybersecurity; digital trust; electronic public services; e-government; DeLone and McLean model; conceptual model

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Al-Makki Publisher

Abstract

Background: Indonesia's electronic public services keep expanding, as the national SPBE index rose from 2.79 in 2023 to 3.12 in 2024, while the national cybersecurity landscape recorded more than 330 million traffic anomalies in 2024. Prior studies mostly treat security, privacy, and trust as drivers of intention to use e-government, so their joint role in explaining service success remains underexplored in Indonesia.
Objective: This article develops a conceptual model explaining how perceived cybersecurity and digital trust contribute to the success of electronic public services, including the mediating role of digital trust.
Methods: The study applies a conceptual research design using the model approach, supported by an integrative literature review of empirical studies, meta-analyses, official reports, and regulations on e-government, security, trust, and information systems success published mainly between 2016 and 2025.
Results: The synthesis yields four propositions: perceived cybersecurity relates positively to service success (P1) and to digital trust (P3), digital trust relates positively to service success (P2), and digital trust mediates the link between cybersecurity and service success (P4). The article also offers an instrument grid and a PLS-SEM testing protocol covering sample size estimation, common method bias control, and PLSpredict. No respondent data are analysed in this article.
Conclusion: Service success should be assessed through citizens' perceived security and trust, not only through technological maturity. The model provides a testable basis for future empirical studies and for SPBE policies aligned with the Personal Data Protection Law.

Kata Kunci:
keamanan siber; kepercayaan digital; pelayanan publik elektronik; e-government; model DeLone dan McLean; model konseptual

Abstrak

Latar Belakang: Pelayanan publik berbasis elektronik di Indonesia terus berkembang, ditunjukkan oleh Indeks SPBE Nasional yang naik dari 2,79 pada 2023 menjadi 3,12 pada 2024, sementara lanskap keamanan siber nasional mencatat lebih dari 330 juta anomali trafik sepanjang 2024. Penelitian terdahulu umumnya menempatkan keamanan, privasi, dan kepercayaan sebagai pendorong niat menggunakan e-government, sehingga peran bersama keduanya dalam menjelaskan keberhasilan layanan masih terbatas dikaji dalam konteks Indonesia.
Tujuan: Artikel ini bertujuan mengembangkan model konseptual yang menjelaskan kontribusi persepsi keamanan siber dan kepercayaan digital terhadap keberhasilan pelayanan publik berbasis elektronik, termasuk peran mediasi kepercayaan digital.
Metode: Penelitian menggunakan desain konseptual dengan pendekatan model yang didukung kajian literatur integratif terhadap studi empiris, meta-analisis, laporan resmi, dan regulasi terkait e-government, keamanan, kepercayaan, serta keberhasilan sistem informasi yang sebagian besar terbit pada 2016 sampai 2025.

Hasil: Sintesis menghasilkan empat proposisi, yaitu persepsi keamanan siber berhubungan positif dengan keberhasilan layanan (P1) dan kepercayaan digital (P3), kepercayaan digital berhubungan positif dengan keberhasilan layanan (P2), serta kepercayaan digital memediasi hubungan keamanan siber dan keberhasilan layanan (P4). Artikel ini juga menyajikan kisi-kisi instrumen dan protokol pengujian PLS-SEM yang mencakup estimasi ukuran sampel, pengendalian common method bias, dan PLSpredict. Artikel ini tidak menganalisis data responden.
Kesimpulan: Keberhasilan layanan perlu dinilai melalui persepsi aman dan kepercayaan masyarakat, bukan hanya kematangan teknologi. Model ini menjadi dasar yang dapat diuji bagi penelitian empiris berikutnya dan bagi kebijakan SPBE yang selaras dengan UU Pelindungan Data Pribadi.

PENDAHULUAN

Transformasi digital telah mendorong perubahan mendasar dalam penyelenggaraan pemerintahan, khususnya dalam penyediaan pelayanan publik yang lebih efektif, efisien, transparan, dan mudah diakses oleh masyarakat. Pemanfaatan teknologi informasi memungkinkan pemerintah menyediakan berbagai layanan secara elektronik, seperti administrasi kependudukan, perpajakan, perizinan, layanan kesehatan, pendidikan, hingga pengaduan masyarakat. Di Indonesia, transformasi tersebut diwujudkan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) yang diarahkan untuk mengintegrasikan proses bisnis, data, infrastruktur, dan layanan pemerintahan. Perkembangan pemerintahan digital juga menjadi perhatian global karena pemanfaatan teknologi dinilai mampu meningkatkan kapasitas pemerintah dalam memberikan pelayanan yang responsif dan berorientasi pada kebutuhan masyarakat (United Nations, 2024; OECD, 2024). Laporan United Nations (2024) mencatat bahwa proporsi penduduk dunia yang tertinggal dalam pengembangan pemerintahan digital turun dari 45% pada 2022 menjadi 22,4% pada 2024, sementara Indonesia naik dari peringkat 77 ke peringkat 64 dari 193 negara dengan nilai E-Government Development Index (EGDI) sebesar 0,7991. Perluasan layanan tersebut sekaligus meningkatkan ketergantungan pemerintah dan masyarakat pada sistem elektronik, sehingga gangguan keamanan dan menurunnya kepercayaan pengguna berpotensi langsung menghambat keberhasilan layanan.

Perkembangan pelayanan publik berbasis elektronik di Indonesia menunjukkan kemajuan yang cukup signifikan. Berdasarkan hasil evaluasi Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB), Indeks SPBE Nasional tahun 2024 mencapai 3,12 dari skala 5, meningkat dibandingkan tahun 2023 yang memperoleh nilai 2,79 (Kementerian PANRB, 2024). Evaluasi tersebut melibatkan 615 instansi pusat dan pemerintah daerah, dengan 48 instansi memperoleh predikat memuaskan. Capaian ini menunjukkan adanya peningkatan kematangan penerapan SPBE, meskipun peningkatan indeks belum secara otomatis menggambarkan bahwa seluruh layanan digital telah memenuhi harapan masyarakat, khususnya dalam aspek keamanan informasi, perlindungan data pribadi, dan kepercayaan pengguna. Oleh karena itu, keberhasilan pelayanan publik elektronik perlu dilihat tidak hanya dari tingkat penerapan teknologi, tetapi juga dari kualitas pengalaman dan rasa aman masyarakat ketika menggunakan layanan tersebut (Kementerian PANRB, 2025; United Nations, 2024). Indeks SPBE mengukur tingkat kematangan penerapan SPBE pada instansi pusat dan pemerintah daerah dengan skala 1 sampai 5, dan nilai 2,6 sampai kurang dari 3,5 termasuk predikat Baik (Kementerian PANRB, 2024). Dengan demikian, indeks ini merepresentasikan capaian institusional dan bukan persepsi pengguna layanan, sehingga

terdapat kesenjangan antara kematangan tata kelola di sisi instansi dan pengalaman aman serta kepercayaan yang dirasakan masyarakat ketika menggunakan layanan.

Di balik perkembangan tersebut, keamanan siber menjadi salah satu tantangan utama dalam penyelenggaraan pelayanan publik berbasis elektronik. Ketergantungan pemerintah terhadap sistem digital menyebabkan meningkatnya risiko serangan siber, seperti pencurian data, kebocoran informasi pribadi, ransomware, phishing, akses ilegal, dan gangguan ketersediaan sistem. Berdasarkan informasi Lanskap Keamanan Siber Indonesia Tahun 2024 yang merujuk pada pemantauan Badan Siber dan Sandi Negara (BSSN), tercatat 330.527.636 anomali trafik sepanjang tahun 2024, termasuk 26.771.610 anomali trafik yang terkait situs phishing dan 514.508 anomali terkait ransomware, serta 241 dugaan insiden kebocoran data. Anomali trafik merupakan aktivitas mencurigakan yang terdeteksi oleh sistem pemantauan, sehingga angka tersebut tidak identik dengan jumlah serangan yang berhasil maupun jumlah korban (BSSN, 2025). Data tersebut memperlihatkan bahwa ancaman siber merupakan persoalan nyata yang berpotensi mengganggu keberlangsungan layanan digital, menimbulkan kerugian bagi masyarakat, dan menurunkan reputasi institusi pemerintah. Dengan demikian, keamanan siber perlu ditempatkan sebagai bagian penting dari tata kelola pelayanan publik digital, bukan sekadar aspek teknis pengelolaan teknologi informasi (OECD, 2024).

Urgensi penguatan keamanan siber semakin tinggi karena pelayanan publik elektronik melibatkan pengumpulan, pemrosesan, penyimpanan, dan pertukaran data masyarakat dalam jumlah besar. Informasi seperti identitas kependudukan, alamat, data kesehatan, informasi keuangan, serta dokumen administrasi merupakan data yang memiliki nilai strategis dan harus dilindungi dari penyalahgunaan. Ketika terjadi kebocoran atau gangguan sistem, dampaknya tidak hanya berupa kerugian teknis, tetapi juga dapat menghambat akses masyarakat terhadap layanan dasar dan menimbulkan keraguan terhadap kemampuan pemerintah dalam menjaga informasi pengguna. OECD (2024) menegaskan bahwa infrastruktur digital publik perlu dibangun dengan memperhatikan interoperabilitas, keamanan, dan perlindungan privasi. Sejalan dengan itu, United Nations (2024) menekankan pentingnya pengembangan pemerintahan digital yang inklusif dan tangguh, sedangkan Gupta et al. (2025) menunjukkan bahwa aspek keamanan dan privasi memiliki hubungan penting dengan kepercayaan serta penerimaan masyarakat terhadap layanan e-government. Dari sisi regulasi, Peraturan Presiden Nomor 95 Tahun 2018 mengatur keamanan SPBE yang mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan, sedangkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mewajibkan pengendali data, termasuk badan publik, menyampaikan pemberitahuan tertulis paling lambat 3 x 24 jam apabila terjadi kegagalan pelindungan data pribadi (Republik Indonesia, 2018; Republik Indonesia, 2022). Gangguan keamanan pada layanan kependudukan, perizinan, atau perpajakan dapat menunda layanan, memaksa masyarakat kembali ke prosedur manual, dan menurunkan kesediaan untuk menggunakan layanan kembali. Oleh karena itu, persepsi keamanan berkaitan langsung dengan indikator keberhasilan layanan yang dianalisis dalam artikel ini, yaitu kepuasan, niat penggunaan berkelanjutan, dan manfaat bersih.

Selain keamanan siber, kepercayaan digital (digital trust) merupakan faktor penting yang dapat menentukan keberhasilan pelayanan publik berbasis elektronik. Kepercayaan digital merujuk pada keyakinan masyarakat bahwa sistem dan institusi penyedia layanan digital mampu mengelola informasi secara aman, menjaga kerahasiaan data, memberikan layanan secara andal, serta bertindak

secara bertanggung jawab. Masyarakat cenderung menggunakan layanan digital apabila mereka merasa bahwa informasi pribadi terlindungi, proses pelayanan dapat diandalkan, dan pemerintah memiliki kemampuan untuk menangani risiko yang mungkin terjadi. Dalam konteks e-government, kepercayaan tidak hanya berkaitan dengan teknologi yang digunakan, tetapi juga dengan persepsi terhadap integritas dan kompetensi institusi pemerintah. Penelitian Abdulkareem dan Mohd Ramli (2022) menunjukkan bahwa kepercayaan memiliki keterkaitan dengan keberhasilan penggunaan layanan e-government, sementara Hooda et al. (2023) mengidentifikasi peran kepercayaan dalam model keberhasilan sistem pemerintahan elektronik. Temuan Li dan Shang (2023) juga memperlihatkan bahwa penggunaan e-government berkaitan dengan pembentukan kepercayaan masyarakat terhadap pemerintah (Abdulkareem & Mohd Ramli, 2022; Hooda et al., 2023; Li & Shang, 2023). Untuk menjaga batas konseptual, artikel ini membedakan kedua konstruk secara tegas. Keamanan siber dipahami sebagai persepsi pengguna atas kontrol dan perlindungan teknis sistem, misalnya kerahasiaan, keutuhan, ketersediaan, dan autentikasi (National Institute of Standards and Technology, 2024), sedangkan kepercayaan digital dipahami sebagai keyakinan pengguna terhadap kemampuan (*ability*), niat baik (*benevolence*), dan integritas (*integrity*) instansi penyelenggara layanan (Alzahrani et al., 2017). Dengan pembedaan ini, keamanan merupakan karakteristik sistem yang dipersepsikan, sedangkan kepercayaan merupakan sikap terhadap institusi yang dapat terbentuk dari pengalaman aman tersebut.

Secara teoretis, hubungan antara keamanan siber, kepercayaan digital, dan keberhasilan pelayanan publik elektronik dapat dijelaskan melalui pendekatan keberhasilan sistem informasi (Information Systems Success Model) yang dikembangkan oleh DeLone dan McLean (2003). Model tersebut menjelaskan keberhasilan sistem informasi melalui sejumlah dimensi, yaitu kualitas sistem, kualitas informasi, kualitas layanan, penggunaan, kepuasan pengguna, dan manfaat bersih (net benefits). Dalam konteks penelitian ini, keamanan siber dapat diposisikan sebagai faktor yang mendukung kualitas dan keandalan sistem, sedangkan kepercayaan digital dapat dipahami sebagai faktor yang mendorong keyakinan, penerimaan, dan keberlanjutan penggunaan layanan. Keberhasilan pelayanan publik elektronik selanjutnya dapat dilihat melalui kepuasan masyarakat, intensitas penggunaan, kemudahan memperoleh layanan, serta manfaat yang dirasakan oleh pengguna. Pengembangan model tersebut sejalan dengan penelitian Abdulkareem dan Mohd Ramli (2022) serta Rahmatullah et al. (2025) yang menggunakan pendekatan keberhasilan sistem informasi untuk menjelaskan kinerja layanan e-government (Abdulkareem & Mohd Ramli, 2022; Rahmatullah et al., 2025). Perlu ditegaskan bahwa keamanan siber dan kepercayaan digital bukan dimensi asli model DeLone dan McLean (2003). Dalam artikel ini keduanya diposisikan sebagai anteseden eksternal: persepsi keamanan siber memperluas penilaian kualitas sistem, sedangkan kepercayaan digital menjadi mekanisme psikologis yang menghubungkan pengalaman menggunakan sistem dengan hasil penggunaan, sebagaimana ditunjukkan oleh meta-analisis Hooda et al. (2023). Konstruk hasil dibatasi pada tiga dimensi yang berakar pada model D&M, yaitu kepuasan pengguna, niat penggunaan berkelanjutan, dan manfaat bersih. Kemudahan pelayanan tidak dimasukkan ke dalam konstruk hasil karena lebih tepat diperlakukan sebagai anteseden dalam tradisi penerimaan teknologi (Alkraiji & Ameen, 2022; Rahmatullah et al., 2025).

Untuk memperlihatkan kondisi empiris yang melatarbelakangi penelitian, berikut disajikan beberapa data pendukung mengenai perkembangan SPBE dan ancaman keamanan siber di Indonesia.

Tabel 1. Data Pendukung Perkembangan SPBE dan Ancaman Keamanan Siber di Indonesia

Indikator	Tahun	Nilai	Sumber
Indeks SPBE Nasional	2023	2,79 dari 5	Kementerian PANRB (2024)
Indeks SPBE Nasional	2024	3,12 dari 5	Kementerian PANRB (2025)
Instansi pusat dan pemerintah daerah yang dievaluasi SPBE	2024	615 instansi	Kementerian PANRB (2025)
Anomali trafik siber di Indonesia	2024	330.527.636 aktivitas	BSSN (2025)
Aktivitas phishing	2024	26.771.610 aktivitas	BSSN (2025)
Aktivitas ransomware	2024	514.508 aktivitas	BSSN (2025)
Dugaan insiden kebocoran data	2024	241 insiden	BSSN (2025)
Peringkat EGDI Indonesia	2024	64 dari 193 negara (nilai 0,7991)	United Nations (2024)

Catatan: Data anomali dan ancaman siber merupakan hasil pemantauan yang dilaporkan dalam publikasi Lanskap Keamanan Siber Indonesia Tahun 2024. Anomali trafik tidak dapat disamakan secara langsung dengan jumlah serangan yang berhasil atau jumlah korban. Sumber: Kementerian PANRB (2024, 2025) dan BSSN (2025). Data BSSN dirujuk dari dokumen resmi Lanskap Keamanan Siber Indonesia 2024 yang dirilis BSSN pada Januari 2025. Data dalam tabel ini menggambarkan konteks risiko nasional dan tidak menunjukkan bahwa pengguna layanan tertentu mengalami kegagalan layanan. Data EGDI bersumber dari United Nations (2024).

Data tersebut memperlihatkan dua kondisi yang berjalan bersamaan, yaitu meningkatnya kematangan SPBE dan masih tingginya paparan ancaman siber. Indeks kematangan institusional belum menjawab apakah masyarakat merasa aman dan percaya ketika menggunakan layanan. Oleh karena itu, masalah yang dikaji dalam artikel ini adalah bagaimana persepsi keamanan siber dan kepercayaan digital, baik secara langsung maupun melalui mekanisme mediasi, menjelaskan keberhasilan pelayanan publik berbasis elektronik.

Sejumlah penelitian terdahulu memberikan landasan bagi model ini, tetapi masing-masing memiliki keterbatasan. Abdulkareem dan Mohd Ramli (2022) menemukan bahwa kepercayaan pada e-government berkaitan dengan kinerja e-government pada pengguna layanan di Nigeria, namun belum memasukkan persepsi keamanan sebagai anteseden. Meta-analisis Hooda et al. (2023) terhadap 67 studi menunjukkan bahwa kualitas informasi, kualitas layanan, kualitas sistem, dan kepuasan pengguna memengaruhi kepercayaan e-government, sedangkan penggunaan sistem memediasi pengaruh kepercayaan terhadap niat penggunaan; studi ini tidak memisahkan keamanan dari kualitas sistem. Gupta et al. (2025) melalui MASEM terhadap 68 studi menunjukkan bahwa persepsi privasi dan keamanan, persepsi risiko, serta kepercayaan pada pemerintah dan internet membentuk kepercayaan e-government yang kemudian memengaruhi niat penggunaan, tetapi

variabel hasilnya berhenti pada niat. Di Indonesia, Rahmatullah et al. (2025) menguji model D&M pada 232 pegawai pengguna sistem e-government dan menemukan hubungan terkuat antara niat perilaku dan manfaat bersih, tetapi tidak memasukkan keamanan maupun kepercayaan. Perbandingan yang lebih rinci, termasuk konteks, variabel, metode, temuan, dan keterbatasan setiap studi, disajikan pada Tabel 4.

Berdasarkan perbandingan tersebut, celah penelitian terletak pada tiga hal. Pertama, studi yang menguji keamanan dan kepercayaan secara bersamaan, seperti Gupta et al. (2025), menempatkan niat penggunaan sebagai variabel hasil, bukan keberhasilan layanan yang mencakup kepuasan, keberlanjutan penggunaan, dan manfaat bersih. Kedua, studi keberhasilan e-government di Indonesia, seperti Rahmatullah et al. (2025), masih berfokus pada dimensi kualitas model D&M tanpa memasukkan keamanan dan kepercayaan, sementara studi Indonesia lainnya lebih menekankan adopsi dan pemanfaatan (Rachmawati et al., 2022) atau kualitas layanan elektronik dan kepuasan (Taufiqurokhman et al., 2024). Ketiga, hubungan keamanan dan kepercayaan sering disebut dalam narasi, tetapi jarang dimodelkan sebagai jalur mediasi yang menjelaskan keberhasilan layanan, khususnya setelah berlakunya UU Pelindungan Data Pribadi.

Kebaruan artikel ini terdiri atas tiga kontribusi. Pertama, artikel ini memosisikan persepsi keamanan siber sebagai anteseden eksternal model D&M yang dibedakan secara tegas dari kualitas sistem, serta kepercayaan digital sebagai mekanisme mediasi, sehingga menghasilkan jalur yang dapat diuji dari keamanan siber ke kepercayaan digital dan selanjutnya ke keberhasilan layanan. Kedua, variabel hasil dirumuskan sebagai keberhasilan layanan yang mengacu pada kepuasan, niat penggunaan berkelanjutan, dan manfaat bersih, bukan sekadar niat penggunaan sebagaimana pada Hooda et al. (2022) dan Gupta et al. (2025). Ketiga, model ditempatkan dalam konteks Indonesia setelah berlakunya UU Nomor 27 Tahun 2022, sehingga indikator keamanan dikaitkan dengan kewajiban pelindungan data pribadi yang kini mengikat penyelenggara layanan (Republik Indonesia, 2022).

Berdasarkan uraian tersebut, artikel ini bertujuan mengembangkan model konseptual yang menjelaskan (1) hubungan persepsi keamanan siber dengan keberhasilan pelayanan publik berbasis elektronik, (2) hubungan kepercayaan digital dengan keberhasilan layanan, (3) hubungan persepsi keamanan siber dengan kepercayaan digital, dan (4) peran mediasi kepercayaan digital, beserta kisi-kisi instrumen dan protokol pengujian empirisnya.

Secara teoretis, artikel ini memperluas model D&M dengan anteseden keamanan dan mekanisme kepercayaan yang relevan bagi layanan publik digital. Secara praktis, model ini memberi implikasi bagi tiga aktor. Badan Siber dan Sandi Negara dapat memanfaatkan indikator persepsi keamanan pengguna untuk melengkapi pemantauan teknis, Kementerian PANRB dapat mempertimbangkan dimensi kepercayaan dan pengalaman aman pengguna dalam evaluasi SPBE, sedangkan penyelenggara SPBE di daerah dapat memprioritaskan transparansi pelindungan data dan kanal pengaduan sebagai sarana membangun kepercayaan.

METODE PENELITIAN

Desain Penelitian (Research Design)

Penelitian ini menggunakan desain penelitian konseptual dengan pendekatan model (*model approach*) sebagaimana dirumuskan oleh Jaakkola (2020), yaitu desain yang bertujuan membangun kerangka teoretis berisi hubungan antarkonstruk yang dapat diuji secara empiris. Desain ini dipilih

karena naskah ini tidak melaporkan data responden, dan seluruh angka simulasi pada versi sebelumnya telah dihapus. Pengembangan model didukung kajian literatur integratif (*integrative review*) yang menurut Snyder (2019) sesuai untuk menyintesis temuan dari berbagai tradisi penelitian guna menghasilkan kerangka konseptual baru.

Model konseptual yang dikembangkan memuat empat proposisi (P1 sampai P4) yang diturunkan pada bagian Hasil dan Pembahasan. Proposisi dirumuskan sebagai arah hubungan yang diharapkan, bukan sebagai pernyataan signifikansi, sehingga pengujiannya diserahkan kepada penelitian empiris lanjutan.

Prosedur Kajian Literatur (Literature Review Procedure)

Penelusuran literatur dilakukan pada basis data Scopus, ScienceDirect, Emerald Insight, SpringerLink, dan Google Scholar dengan kombinasi kata kunci *e-government*, *digital government*, *trust*, *security*, *privacy*, *information systems success*, dan Indonesia. Kriteria inklusi meliputi: (1) artikel jurnal bereputasi atau meta-analisis yang terbit pada 2016 sampai 2025; (2) berada dalam konteks layanan pemerintahan elektronik; (3) memuat konstruk keamanan, privasi, kepercayaan, atau keberhasilan sistem informasi; dan (4) dapat diverifikasi melalui DOI. Rujukan fondasional di luar rentang tersebut, yaitu DeLone dan McLean (2003), tetap digunakan karena menjadi kerangka teori utama. Data kontekstual diambil dari laporan resmi United Nations, OECD, Kementerian PANRB, BSSN, dan NIST, serta peraturan perundang-undangan.

Analisis dilakukan melalui tiga tahap. Pertama, setiap studi terpilih dipetakan berdasarkan konteks, metode, variabel, temuan utama, dan keterbatasannya (Tabel 4). Kedua, temuan dibandingkan untuk mengidentifikasi pola yang konsisten, temuan yang bertentangan, dan celah konseptual. Ketiga, hasil sintesis diturunkan menjadi proposisi dan model konseptual sesuai pendekatan model (Jaakkola, 2020). Karena kajian bersifat integratif dan bukan tinjauan sistematis, studi yang dipilih tidak dimaksudkan sebagai sensus literatur, dan keterbatasan ini dinyatakan pada bagian akhir artikel.

Rancangan Pengujian Empiris yang Diusulkan (Proposed Empirical Testing Protocol)

Agar model dapat diuji, artikel ini menyusun protokol pengujian empiris bagi penelitian lanjutan. Populasi yang disarankan dibatasi pada pengguna satu jenis layanan dan satu lokus, misalnya pengguna layanan administrasi kependudukan daring di satu kabupaten atau kota, karena persepsi keamanan dan kepercayaan dapat berbeda antarjenis layanan, seperti layanan kependudukan, perpajakan, dan kesehatan.

Teknik *purposive sampling* disarankan untuk menjamin pengalaman responden, dengan konsekuensi berupa keterbatasan generalisasi yang perlu dinyatakan sebagai keterbatasan penelitian. Rekrutmen dapat dilakukan melalui kanal resmi layanan, media sosial instansi, dan titik layanan tatap muka, dengan pertanyaan penyaring (*screening question*) di awal kuesioner.

Kriteria responden yang disarankan meliputi:

1. Berusia minimal 18 tahun.
2. Pernah menggunakan pelayanan publik berbasis elektronik yang disediakan oleh instansi pemerintah.
3. Memiliki pengalaman menggunakan layanan tersebut minimal satu kali dalam enam bulan terakhir.

4. Mampu menyebutkan jenis layanan dan langkah yang pernah dilakukan, yang diverifikasi melalui pertanyaan penyaring.
5. Bersedia berpartisipasi sebagai responden penelitian.

Ukuran sampel minimum dihitung dengan dua cara. Analisis daya statistik untuk regresi berganda dengan dua prediktor, $f^2 = 0{,}15$, $\alpha = 0{,}05$, dan *power* 0,80 menghasilkan kebutuhan minimum 68 responden. Metode *inverse square root* (Kock & Hadaya, 2018) dengan koefisien jalur minimum yang diharapkan sebesar 0,20 pada $\alpha = 0{,}05$ menghasilkan kebutuhan minimum 155 responden. Oleh karena itu, penelitian lanjutan disarankan menargetkan sedikitnya 200 kuesioner valid untuk mengantisipasi data yang tidak lengkap, serta melaporkan jumlah kuesioner yang disebar, kembali, dan layak dianalisis.

Instrumen Penelitian (Research Instrument)

Instrumen yang diusulkan berupa kuesioner terstruktur dengan skala Likert lima tingkat (Tabel 2). Setiap indikator dioperasionalkan ke dalam butir pernyataan yang diadaptasi dari sumber rujukan sebagaimana disajikan pada Tabel 3. Butir yang diadaptasi dari sumber berbahasa Inggris perlu melalui penerjemahan dan penerjemahan balik, uji keterbacaan, serta uji coba awal pada sekitar 30 responden dengan karakteristik serupa sebelum pengumpulan data utama.

Tabel 2. Skala Pengukuran Likert Lima Tingkat yang Diusulkan

Skor	Keterangan
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Instrumen penelitian terdiri atas tiga variabel, yaitu keamanan siber, kepercayaan digital, dan keberhasilan pelayanan publik berbasis elektronik. Indikator pengukuran setiap variabel dirumuskan sebagai berikut.

a. Keamanan Siber (X1)

Keamanan siber merupakan persepsi pengguna mengenai kemampuan sistem pelayanan publik elektronik dalam melindungi informasi, menjaga integritas data, dan memastikan layanan dapat diakses secara aman. Indikator mengacu pada prinsip kerahasiaan, keutuhan, dan ketersediaan dalam NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology, 2024) serta keamanan SPBE dalam Perpres Nomor 95 Tahun 2018 (Republik Indonesia, 2018), dan dirumuskan sebagai persepsi keamanan (*perceived security*) agar dapat dinilai oleh responden awam. Indikator yang digunakan meliputi:

1. Kerahasiaan data (*confidentiality*), yaitu kemampuan sistem dalam menjaga informasi pribadi pengguna agar tidak diakses oleh pihak yang tidak berwenang.
2. Integritas data (*integrity*), yaitu kemampuan sistem dalam menjaga keakuratan dan keutuhan informasi yang tersimpan maupun diproses.
3. Ketersediaan sistem (*availability*), yaitu kemampuan sistem untuk tetap dapat diakses ketika masyarakat membutuhkan layanan.

4. Autentikasi dan kontrol akses (*authentication and access control*), yaitu mekanisme untuk memastikan bahwa akses terhadap sistem hanya diberikan kepada pihak yang memiliki kewenangan.
5. Pelindungan data pribadi, yaitu persepsi bahwa sistem menerapkan pelindungan data pribadi sesuai UU Nomor 27 Tahun 2022.

b. Kepercayaan Digital (X2)

Kepercayaan digital merupakan keyakinan pengguna bahwa sistem dan penyelenggara pelayanan publik elektronik mampu menyediakan layanan secara aman, andal, transparan, dan bertanggung jawab. Indikator X2 difokuskan pada keyakinan terhadap institusi penyelenggara berdasarkan dimensi kemampuan, niat baik, dan integritas (Alzahrani et al., 2017; Alkraiji & Ameen, 2022), sehingga tidak tumpang tindih dengan indikator teknis X1. Indikator yang digunakan meliputi:

1. Kompetensi (*competence*), yaitu keyakinan pengguna terhadap kemampuan instansi pemerintah dalam mengelola dan menyediakan layanan digital.
2. Integritas (*integrity*), yaitu keyakinan bahwa penyelenggara layanan menjalankan proses pelayanan secara jujur dan bertanggung jawab.
3. Niat baik (*benevolence*), yaitu keyakinan bahwa penyelenggara layanan bertindak demi kepentingan masyarakat pengguna.
4. Keyakinan terhadap layanan digital, yaitu tingkat kepercayaan pengguna dalam melakukan transaksi atau menyampaikan informasi melalui sistem pelayanan publik elektronik.

c. Keberhasilan Pelayanan Publik Berbasis Elektronik (Y)

Keberhasilan pelayanan publik berbasis elektronik merupakan tingkat keberhasilan sistem dalam memberikan manfaat dan memenuhi kebutuhan masyarakat melalui pemanfaatan teknologi informasi. Konstruk ini dibatasi pada dimensi hasil model D&M, yaitu kepuasan pengguna, niat penggunaan berkelanjutan, dan manfaat bersih, dan diusulkan dimodelkan sebagai konstruk formatif tingkat kedua (DeLone & McLean, 2003; Rahmatullah et al., 2025). Indikator yang digunakan meliputi:

1. Kepuasan pengguna (*user satisfaction*), yaitu tingkat kepuasan masyarakat terhadap pengalaman menggunakan pelayanan publik elektronik.
2. Penggunaan berkelanjutan (*continuance intention*), yaitu keinginan masyarakat untuk terus menggunakan layanan digital pada masa mendatang.
3. Manfaat bersih (*net benefits*), yaitu manfaat yang dirasakan masyarakat, seperti penghematan waktu, biaya, tenaga, serta peningkatan aksesibilitas pelayanan.

Tabel 3. Kisi-Kisi Instrumen yang Diusulkan

Konstruk	Indikator	Contoh Butir	Sumber Adaptasi
Persepsi Keamanan Siber (X1)	Kerahasiaan	Saya yakin data pribadi saya pada layanan ini tidak dapat diakses pihak yang tidak berwenang.	National Institute of Standards and Technology (2024); Gupta et al. (2025)
	Keutuhan data	Informasi yang saya kirim melalui layanan ini tersimpan tanpa perubahan yang tidak sah.	National Institute of Standards and Technology (2024)

Konstruk	Indikator	Contoh Butir	Sumber Adaptasi
	Ketersediaan	Layanan ini dapat diakses ketika saya membutuhkannya.	Republik Indonesia (2018)
	Autentikasi	Layanan ini memverifikasi identitas saya sebelum memberikan akses.	National Institute of Standards and Technology (2024)
	Pelindungan data pribadi	Penyelenggara menjelaskan cara data pribadi saya dikelola dan dilindungi.	Republik Indonesia (2022)
Kepercayaan Digital (X2)	Kemampuan	Instansi penyelenggara mampu mengelola layanan digital ini dengan baik.	Alzahrani et al. (2017)
	Niat baik	Instansi penyelenggara bertindak demi kepentingan masyarakat pengguna.	Alzahrani et al. (2017); Alkraiji dan Ameen (2022)
	Integritas	Instansi penyelenggara jujur dalam menyampaikan informasi tentang layanan.	Alzahrani et al. (2017)
	Keyakinan umum	Saya bersedia menyampaikan data pribadi melalui layanan ini.	Hooda et al. (2022); Gupta et al. (2025)
Keberhasilan Pelayanan Publik Elektronik (Y)	Kepuasan pengguna	Secara keseluruhan saya puas dengan layanan ini.	DeLone dan McLean (2003); Rahmatullah et al. (2025)
	Niat penggunaan berkelanjutan	Saya akan terus menggunakan layanan ini pada masa mendatang.	Alkraiji dan Ameen (2022)
	Manfaat bersih	Layanan ini menghemat waktu dan biaya saya dalam mengurus keperluan administrasi.	DeLone dan McLean (2003); Rahmatullah et al. (2025)

Catatan: setiap indikator disarankan diukur dengan dua sampai tiga butir; contoh butir perlu diuji keterbacaan dan diuji coba sebelum digunakan.

Teknik Pengumpulan Data dan Etika Penelitian yang Diusulkan (Proposed Data Collection and Ethics)

Pada penelitian lanjutan, data primer dikumpulkan melalui kuesioner daring, sedangkan literatur dan laporan resmi berfungsi sebagai data sekunder pendukung, bukan sebagai teknik pengujian proposisi.

Penyebaran kuesioner dilakukan melalui satu kanal utama yang ditetapkan sejak awal, dengan periode pengumpulan data yang dicantumkan secara pasti, yaitu tanggal mulai dan tanggal selesai. Sebelum mengisi kuesioner, responden menerima lembar penjelasan dan memberikan persetujuan (*informed consent*). Data dikumpulkan tanpa identitas langsung, disimpan pada penyimpanan terenkripsi yang hanya dapat diakses peneliti, dan dimusnahkan setelah masa retensi berakhir. Persetujuan etik atau surat pengecualian dari komite etik institusi perlu diperoleh sebelum pengumpulan data dimulai.

Data yang terkumpul selanjutnya diperiksa untuk memastikan kelengkapan jawaban, kesesuaian karakteristik responden dengan kriteria sampel, serta konsistensi pengisian kuesioner. Jawaban yang tidak lengkap atau tidak memenuhi kriteria penelitian tidak disertakan dalam proses analisis. Data dengan pola jawaban seragam atau waktu pengisian yang tidak wajar juga dikeluarkan dari analisis.

Prosedur Penelitian (Research Procedure)

Prosedur penelitian dilaksanakan melalui beberapa tahapan yang sistematis untuk memastikan bahwa proses penelitian berjalan sesuai dengan tujuan dan rancangan yang telah ditetapkan. Tahapan 1 dan 2 telah dilaksanakan dalam artikel ini, tahapan 3 dilaksanakan dalam bentuk kisi-kisi instrumen (Tabel 3), sedangkan tahapan 4 sampai 7 merupakan protokol bagi penelitian lanjutan.

Tahapan penelitian meliputi:

1. **Identifikasi masalah dan studi literatur.** Peneliti mengidentifikasi permasalahan terkait keamanan siber dan kepercayaan digital dalam pelayanan publik elektronik, kemudian mengkaji teori dan penelitian terdahulu sebagai dasar pengembangan model penelitian.
2. Pengembangan model dan proposisi. Peneliti menetapkan variabel penelitian, menyusun hubungan antarvariabel, serta merumuskan proposisi mengenai pengaruh keamanan siber dan kepercayaan digital terhadap keberhasilan pelayanan publik elektronik.
3. **Penyusunan instrumen penelitian.** Peneliti menyusun kuesioner berdasarkan indikator masing-masing variabel dengan menggunakan skala Likert lima tingkat.
4. **Pengujian instrumen.** Kuesioner ditelaah untuk memastikan kesesuaian indikator dengan konsep penelitian, kejelasan bahasa, dan kemudahan pemahaman responden. Uji coba wajib dilakukan pada sekitar 30 responden dengan karakteristik serupa, dan hasilnya dilaporkan sebelum pengumpulan data utama.
5. **Pengumpulan data.** Kuesioner disebarkan kepada masyarakat yang memenuhi kriteria sampel hingga jumlah responden yang dibutuhkan terpenuhi.
6. **Pengolahan dan analisis data.** Data yang telah terkumpul diperiksa, dikodekan, dan dianalisis menggunakan perangkat lunak SmartPLS dengan pendekatan PLS-SEM.
7. **Interpretasi hasil dan penarikan kesimpulan.** Peneliti menginterpretasikan hasil pengujian model pengukuran dan model struktural, menguji hipotesis, serta menyusun kesimpulan berdasarkan hasil analisis.

Teknik Analisis Data (Data Analysis Technique)

Teknik analisis data menggunakan pendekatan *Partial Least Squares Structural Equation Modeling* (PLS-SEM) dengan bantuan perangkat lunak SmartPLS. Metode PLS-SEM dipilih karena dapat digunakan untuk menguji hubungan antarvariabel laten secara simultan, mengevaluasi kualitas instrumen pengukuran, serta menganalisis kemampuan variabel independen dalam menjelaskan variabel dependen. PLS-SEM dipilih karena orientasi model yang bersifat prediktif, adanya konstruk tingkat kedua, dan kemungkinan data tidak berdistribusi normal (Hair et al., 2019; Hair et al., 2022). Versi SmartPLS yang digunakan wajib dilaporkan.

Analisis data dilakukan melalui beberapa tahapan berikut.

a. Analisis Statistik Deskriptif

Analisis statistik deskriptif digunakan untuk menggambarkan karakteristik responden dan kecenderungan jawaban terhadap setiap variabel penelitian. Karakteristik responden dapat meliputi jenis kelamin, kelompok usia, tingkat pendidikan, pekerjaan, jenis layanan publik elektronik yang digunakan, serta frekuensi penggunaan layanan. Analisis ini juga digunakan untuk memperoleh gambaran umum mengenai persepsi responden terhadap keamanan siber, kepercayaan digital, dan keberhasilan pelayanan publik elektronik.

b. Evaluasi Model Pengukuran (Outer Model)

Evaluasi *outer model* dilakukan untuk menguji validitas dan reliabilitas instrumen penelitian. Pengujian meliputi:

1. **Convergent validity**, dievaluasi melalui nilai *outer loading* dengan nilai yang diharapkan ≥ 0,70 dan nilai *Average Variance Extracted* (AVE) ≥ 0,50.
2. **Discriminant validity**, dievaluasi untuk memastikan bahwa setiap variabel memiliki perbedaan empiris dengan variabel lainnya. Pengujian dapat menggunakan kriteria *Heterotrait-Monotrait Ratio* (HTMT), dengan ambang konservatif di bawah 0,85 karena konstruk keamanan dan kepercayaan berdekatan secara konseptual, serta dilengkapi kriteria Fornell dan Larcker dan *cross loading*.
3. **Reliability test**, dilakukan untuk mengukur konsistensi internal indikator menggunakan nilai *Cronbach's Alpha* dan *Composite Reliability*. Nilai ≥ 0,70 secara umum menunjukkan reliabilitas yang memadai.

c. Evaluasi Model Struktural (Inner Model)

Evaluasi *inner model* dilakukan untuk menganalisis hubungan antarvariabel laten dan mengukur kemampuan model dalam menjelaskan variabel dependen. Pengujian meliputi:

1. **Collinearity test**, menggunakan nilai *Variance Inflation Factor* (VIF) untuk mengetahui adanya potensi multikolinearitas antarvariabel prediktor.
2. **Coefficient of Determination (R^2)**, digunakan untuk mengetahui seberapa besar kemampuan variabel keamanan siber dan kepercayaan digital dalam menjelaskan keberhasilan pelayanan publik berbasis elektronik.
3. **Effect Size (f^2)**, digunakan untuk mengetahui besarnya kontribusi masing-masing variabel independen terhadap variabel dependen.
4. **Predictive power**, dievaluasi menggunakan PLSpredict melalui nilai Q^2predict, RMSE, dan MAE yang dibandingkan dengan model pembanding regresi linear (Shmueli et al., 2019).
5. **Common method bias**, diuji melalui *full collinearity* VIF dengan ambang 3,3 serta diantisipasi secara prosedural melalui pemisahan bagian kuesioner dan jaminan anonimitas (Tehseen et al., 2017).

d. Pengujian Hipotesis (Hypothesis Testing)

Pengujian hipotesis dilakukan menggunakan prosedur *bootstrapping* pada SmartPLS dengan jumlah subsampel yang memadai, yaitu 10.000 subsampel. Pengujian dilakukan dengan memperhatikan nilai koefisien jalur (*path coefficient*), nilai *t-statistic*, dan *p-value* untuk mengetahui arah, kekuatan, serta signifikansi hubungan antarvariabel.

Hipotesis dinyatakan didukung apabila hubungan antarvariabel memiliki arah positif sesuai dengan hipotesis dan nilai signifikansi memenuhi kriteria pengujian, yaitu *p-value* < 0,05. Hasil pengujian tersebut digunakan untuk menentukan apakah keamanan siber dan kepercayaan digital memiliki pengaruh yang signifikan terhadap keberhasilan pelayanan publik berbasis elektronik. Karena proposisi bersifat berarah, uji satu arah (*one tailed*) digunakan dan dilengkapi interval kepercayaan *bias corrected*. Pengujian mediasi (P4) dilakukan melalui signifikansi efek tidak langsung hasil *bootstrapping* (Hair et al., 2019).

Melalui tahapan analisis tersebut, penelitian lanjutan diharapkan dapat memberikan gambaran empiris mengenai kontribusi keamanan siber dan kepercayaan digital dalam meningkatkan keberhasilan pelayanan publik berbasis elektronik.

HASIL DAN PEMBAHASAN

Sintesis Penelitian Terdahulu

Tabel 4 merangkum studi utama yang menjadi dasar pengembangan model. Pola pertama yang konsisten adalah bahwa kepercayaan memiliki peran sentral dalam penggunaan e-government, baik pada tingkat meta-analisis (Hooda et al., 2022; Hooda et al., 2023; Gupta et al., 2025) maupun pada studi di tingkat negara (Abdulkareem & Mohd Ramli, 2022; Alkraiji & Ameen, 2022). Pola kedua adalah bahwa persepsi keamanan dan privasi lebih sering diuji sebagai pembentuk kepercayaan daripada sebagai penentu langsung keberhasilan layanan (Alzahrani et al., 2017; Gupta et al., 2025). Namun, temuan tidak sepenuhnya seragam. Santa et al. (2019) tidak menemukan hubungan langsung antara kepercayaan pada layanan daring dan kepuasan pengguna layanan pemerintah untuk bisnis di Arab Saudi, karena pengaruh tersebut berlangsung melalui efektivitas sistem. Di Jakarta, Taufiqurokhman et al. (2024) menemukan bahwa kualitas layanan elektronik membangun kepercayaan dan kepuasan publik, tetapi kepercayaan tidak memediasi hubungan kualitas layanan dengan kepuasan. Temuan ini menunjukkan bahwa peran kepercayaan terhadap keberhasilan layanan bergantung pada konteks dan perlu diuji, bukan diasumsikan.

Tabel 4. Perbandingan Penelitian Terdahulu yang Menjadi Dasar Model

Studi	Konteks dan Metode	Variabel Utama	Temuan Utama	Keterbatasan bagi Model Ini
Alzahrani et al. (2017)	Tinjauan sistematis literatur 2000 sampai 2014	Anteseden kepercayaan e-government	Faktor warga, pemerintah, dan teknologi, termasuk keamanan, membentuk kepercayaan	Belum menghubungkan kepercayaan dengan keberhasilan layanan
Santa et al. (2019)	Survei pengguna layanan pemerintah untuk bisnis, Arab Saudi	Kepercayaan, kualitas sistem, informasi, layanan, efektivitas operasional, kepuasan	Pengaruh kepercayaan terhadap kepuasan berlangsung melalui efektivitas sistem; tidak ada pengaruh langsung	Konteks layanan bisnis; keamanan tidak diukur terpisah
Abdulkareem dan Mohd Ramli (2022)	Survei pengguna e-government, Nigeria	Kepercayaan e-government, model D&M, nilai publik	Kepercayaan berkaitan dengan kinerja e-government	Keamanan tidak dimodelkan sebagai anteseden
Alkraiji dan Ameen (2022)	Survei 780 mahasiswa pengguna layanan penerimaan, Arab Saudi	Kualitas layanan, kepercayaan, kepuasan, loyalitas	Kepercayaan pada pemerintah berpengaruh langsung paling kuat terhadap loyalitas	Responden muda dan satu jenis layanan
Hooda et al. (2022)	MASEM terhadap 90 studi	UTAUT dan kepercayaan e-government	Kepercayaan berperan sentral bagi niat dan perilaku penggunaan	Variabel hasil berupa penggunaan, bukan keberhasilan layanan
Rachmawati et al. (2022)	Survei 158 responden, DKI Jakarta	Faktor personal, keandalan, kepercayaan, adopsi	Kepercayaan dan faktor personal memengaruhi adopsi dan pemanfaatan e-government	Fokus adopsi; keamanan tidak diukur
Hooda et al. (2023)	MASEM terhadap 67 studi	Model D&M dan kepercayaan e-government	Kualitas dan kepuasan memengaruhi kepercayaan; penggunaan memediasi kepercayaan terhadap niat	Keamanan tidak dipisahkan dari kualitas sistem
Li dan Shang (2023)	Survei warga, Tiongkok	Penggunaan e-government dan kepercayaan pada pemerintah	Penggunaan meningkatkan kepercayaan secara tidak langsung melalui penilaian integritas, kinerja, dan responsivitas pemerintah	Arah hubungan dari penggunaan ke kepercayaan menunjukkan kemungkinan hubungan timbal balik
Taufiqurokhman et	Survei 262 pengguna	Kualitas layanan	Kualitas layanan	Keamanan tidak

Studi	Konteks dan Metode	Variabel Utama	Temuan Utama	Keterbatasan bagi Model Ini
al. (2024)	layanan digital, Jakarta; SmartPLS 4	elektronik, kepercayaan publik, kepuasan	membangun kepercayaan dan kepuasan; kepercayaan tidak memediasi	dipisahkan dari kualitas layanan
Gupta et al. (2025)	MASEM terhadap 68 studi	Privasi dan keamanan, risiko, kepercayaan, niat	Privasi dan keamanan membentuk kepercayaan e-government yang memengaruhi niat	Variabel hasil berhenti pada niat penggunaan
Rahmatullah et al. (2025)	Survei 232 pegawai pengguna e-government, Indonesia	Kualitas informasi, sistem, layanan, niat, kepuasan, manfaat bersih	Hubungan terkuat terjadi antara niat perilaku dan manfaat bersih	Tidak memasukkan keamanan dan kepercayaan

Sumber: Disarikan penulis dari studi yang dirujuk.

Pengembangan Proposisi

Proposisi 1 (P1): persepsi keamanan siber berhubungan positif dengan keberhasilan pelayanan publik berbasis elektronik. Dalam model D&M, kualitas sistem menentukan kepuasan dan manfaat yang dirasakan pengguna (DeLone & McLean, 2003). Persepsi bahwa data terjaga kerahasiaannya, informasi tidak berubah tanpa izin, dan layanan tetap tersedia merupakan bagian dari pengalaman kualitas sistem yang dirasakan pengguna layanan publik (National Institute of Standards and Technology, 2024). Meskipun demikian, bukti empiris lebih banyak menunjukkan pengaruh keamanan terhadap kepercayaan daripada terhadap keberhasilan layanan secara langsung (Gupta et al., 2025). Penjelasan alternatifnya, persepsi keamanan mungkin sudah tercakup dalam penilaian kualitas sistem atau bekerja melalui kepercayaan, sehingga P1 diharapkan bernilai positif tetapi lebih lemah dibandingkan jalur tidak langsung.

Proposisi 2 (P2): kepercayaan digital berhubungan positif dengan keberhasilan pelayanan publik berbasis elektronik. Kepercayaan mengurangi ketidakpastian ketika warga menyerahkan data pribadi kepada sistem pemerintah, sehingga mendorong kepuasan dan keberlanjutan penggunaan (Hooda et al., 2022; Alkraiji & Ameen, 2022). Temuan ini sejalan dengan Abdulkareem dan Mohd Ramli (2022) yang menghubungkan kepercayaan dengan kinerja e-government. Sebaliknya, Santa et al. (2019) menunjukkan bahwa pengaruh kepercayaan terhadap kepuasan dapat sepenuhnya berlangsung melalui efektivitas sistem. Perbedaan ini kemungkinan dipengaruhi jenis layanan. Pada layanan yang bersifat wajib, pengguna tetap menggunakan layanan meskipun tingkat kepercayaannya rendah, sehingga kepercayaan lebih tercermin pada kepuasan dan manfaat yang dirasakan daripada pada frekuensi penggunaan.

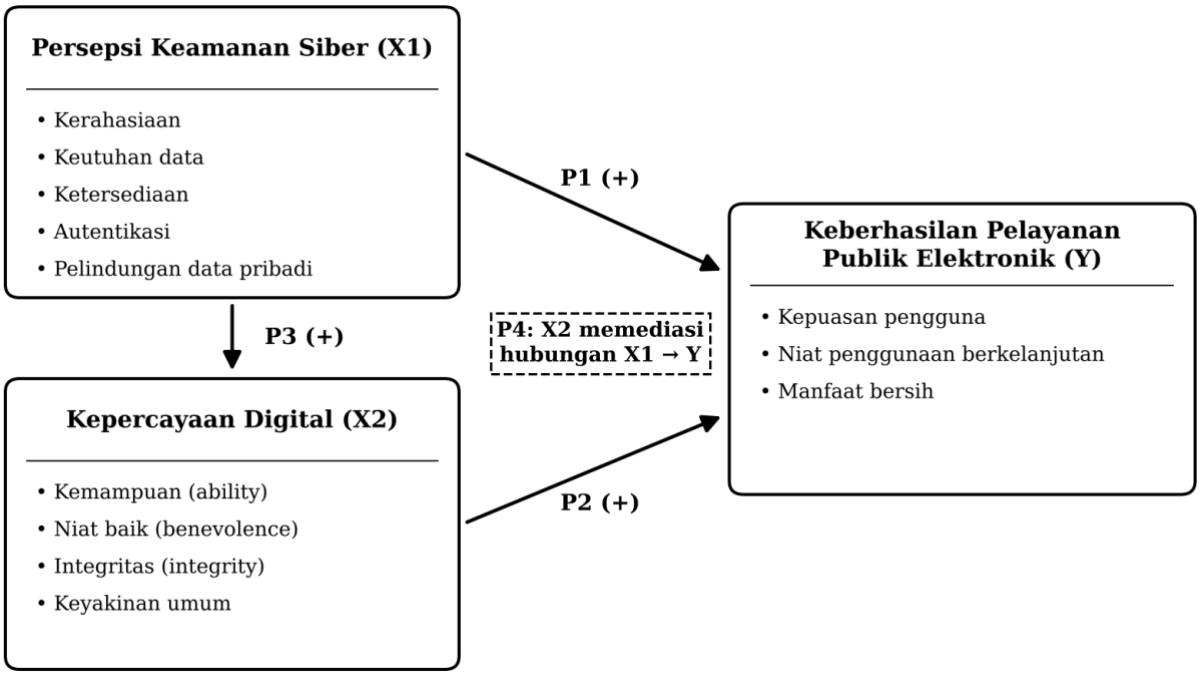
Proposisi 3 (P3): persepsi keamanan siber berhubungan positif dengan kepercayaan digital. Meta-analisis Gupta et al. (2025) dan tinjauan Alzahrani et al. (2017) sama-sama menempatkan keamanan dan privasi sebagai pembentuk kepercayaan e-government. Dalam konteks Indonesia, berlakunya UU Nomor 27 Tahun 2022 menjadikan pelindungan data pribadi sebagai kewajiban hukum, sehingga pengalaman aman yang dirasakan pengguna dapat menjadi dasar keyakinan terhadap kemampuan dan integritas penyelenggara (Republik Indonesia, 2022). Namun, Li dan Shang (2023) menemukan bahwa pengalaman menggunakan layanan juga membentuk kepercayaan, sehingga hubungan ini perlu ditafsirkan secara hati-hati karena pada desain potong lintang arah sebaliknya tidak dapat disingkirkan.

Proposisi 4 (P4): kepercayaan digital memediasi hubungan antara persepsi keamanan siber dan keberhasilan pelayanan publik berbasis elektronik. Gabungan P1 sampai P3 mengarah pada

mekanisme mediasi parsial, yaitu keamanan memengaruhi keberhasilan secara langsung melalui pengalaman sistem yang andal dan secara tidak langsung melalui terbentuknya kepercayaan. Logika ini didukung oleh temuan bahwa kepercayaan memediasi hubungan kualitas e-government dengan partisipasi elektronik (Abdulkareem et al., 2022) dan bahwa pengaruh kepercayaan terhadap niat bekerja melalui penggunaan sistem (Hooda et al., 2023). Di sisi lain, Taufiqurokhman et al. (2024) tidak menemukan mediasi kepercayaan pada hubungan kualitas layanan elektronik dan kepuasan. Oleh karena itu, P4 dirumuskan sebagai mediasi parsial yang harus diuji, dan jalur mediasi inilah yang membedakan model ini dari studi sebelumnya yang memperlakukan keamanan dan kepercayaan secara terpisah.

Model Konseptual

Gambar 1 menyajikan model konseptual hasil sintesis. Model memuat dua anteseden, yaitu persepsi keamanan siber dan kepercayaan digital, serta satu konstruk hasil, yaitu keberhasilan pelayanan publik berbasis elektronik yang terdiri atas kepuasan pengguna, niat penggunaan berkelanjutan, dan manfaat bersih. Jalur P1 sampai P3 merupakan hubungan langsung, sedangkan P4 merupakan jalur tidak langsung dari keamanan siber ke keberhasilan layanan melalui kepercayaan digital. Kisi-kisi instrumen untuk menguji model disajikan pada Tabel 3.



Gambar 1. Model Konseptual Peran Keamanan Siber dan Kepercayaan Digital dalam Keberhasilan Pelayanan Publik Berbasis Elektronik

Sumber: Disusun penulis berdasarkan DeLone dan McLean (2003), Hooda et al. (2023), dan Gupta et al. (2025).

Implikasi Teoretis dan Praktis

Secara teoretis, model ini memperluas model D&M dengan memisahkan persepsi keamanan dari kualitas sistem dan menempatkan kepercayaan sebagai mekanisme yang menghubungkan pengalaman aman dengan keberhasilan layanan. Model juga merespons temuan yang tidak seragam

mengenai pengaruh kepercayaan (Santa et al., 2019; Taufiqurokhman et al., 2024) dengan mengusulkan pengujian jalur langsung dan tidak langsung secara bersamaan.

Secara praktis, tiga implikasi dapat diturunkan sebagai agenda pengujian dan bukan sebagai rekomendasi yang telah dibuktikan secara empiris. Pertama, BSSN bersama penyelenggara layanan dapat melengkapi indikator teknis, seperti jumlah anomali trafik, dengan indikator persepsi keamanan pengguna yang diukur secara berkala. Kedua, Kementerian PANRB dapat mempertimbangkan dimensi kepercayaan dan kepuasan pengguna sebagai pelengkap Indeks SPBE yang saat ini mengukur kematangan institusional. Ketiga, penyelenggara SPBE di daerah perlu memastikan prosedur pemberitahuan kegagalan pelindungan data pribadi dalam 3 x 24 jam sesuai UU Nomor 27 Tahun 2022 serta menyediakan kanal pengaduan yang responsif, dengan indikator evaluasi berupa waktu pemberitahuan dan waktu penyelesaian pengaduan (Republik Indonesia, 2022; OECD, 2024).

Keterbatasan Penelitian

Artikel ini memiliki beberapa keterbatasan. Pertama, model belum diuji dengan data empiris sehingga proposisi belum dapat diklaim sebagai temuan. Kedua, kajian bersifat integratif sehingga pemilihan studi tidak sekomprehensif tinjauan sistematis. Ketiga, protokol pengujian yang diusulkan menggunakan desain potong lintang dan data persepsi, sehingga hubungan kausal dan kemungkinan hubungan timbal balik antara kepercayaan dan penggunaan perlu diuji dengan desain longitudinal. Keempat, model belum memasukkan variabel lain yang relevan, seperti kualitas informasi, literasi digital, dan persepsi risiko.

KESIMPULAN

Artikel ini menyimpulkan bahwa keberhasilan pelayanan publik berbasis elektronik perlu dijelaskan melalui dua faktor yang saling berkaitan, yaitu persepsi pengguna terhadap keamanan siber dan kepercayaan digital terhadap institusi penyelenggara. Sintesis literatur menghasilkan empat proposisi yang menempatkan persepsi keamanan siber sebagai anteseden langsung keberhasilan layanan sekaligus pembentuk kepercayaan digital, serta kepercayaan digital sebagai mediator. Model ini menjawab tujuan penelitian dengan menyediakan kerangka yang dapat diuji beserta kisi-kisi instrumen dan protokol pengujiannya.

Berdasarkan simpulan tersebut, terdapat dua saran. Bagi pemerintah dan penyelenggara SPBE, pengukuran keberhasilan layanan perlu melengkapi indikator kematangan institusional dengan indikator persepsi keamanan, kepercayaan, dan kepuasan pengguna, serta memastikan kepatuhan terhadap UU Pelindungan Data Pribadi. Bagi penelitian selanjutnya, model perlu diuji secara empiris pada satu jenis layanan dan lokus tertentu menggunakan protokol PLS-SEM yang diusulkan, termasuk pengujian mediasi, serta dikembangkan dengan variabel kualitas sistem, kualitas informasi, literasi digital, dan persepsi risiko. Keterbatasan utama artikel ini adalah belum adanya pengujian empiris dan sifat kajian yang integratif.

PENDANAAN

Penulis menyatakan bahwa tidak ada dukungan finansial yang diterima untuk pelaksanaan penelitian ini dan/atau penerbitan artikel ini.

KONFLIK KEPENTINGAN

Penulis menyatakan bahwa penelitian ini dilakukan tanpa adanya hubungan komersial atau finansial yang dapat ditafsirkan sebagai potensi konflik kepentingan.

KONTRIBUSI PENULIS

Mar'atus Solikhah merupakan penulis tunggal yang bertanggung jawab atas konseptualisasi, penelusuran dan sintesis literatur, pengembangan model, penulisan naskah awal, serta revisi naskah.

PERNYATAAN PENGGUNAAN KECERDASAN ARTIFISIAL GENERATIF

Penulis menyatakan bahwa kecerdasan artifisial (AI) generatif digunakan untuk membantu memperbaiki kejelasan bahasa dan struktur naskah. Angka ilustratif yang terdapat pada versi naskah sebelumnya bukan hasil pengolahan data responden dan telah dihapus seluruhnya dari naskah revisi ini, sehingga naskah revisi tidak memuat data numerik hasil pengolahan statistik. Seluruh rujukan telah diperiksa keberadaannya melalui DOI atau laman resmi, dan penulis bertanggung jawab penuh atas keakuratan isi, kutipan, dan integritas naskah.

REFERENSI

Abdulkareem, A. K., & Mohd Ramli, R. (2022). Does trust in e-government influence the performance of e-government? An integration of information system success model and public value theory. *Transforming Government: People, Process and Policy, 16*(1), 1–17. https://doi.org/10.1108/TG-01-2021-0001

Abdulkareem, A. K., Abdulkareem, Z. J., Ishola, A. A., & Akindele, I. T. (2022). Does e-government impact e-participation? The influence of trust in e-government. *International Review of Public Administration, 27*(2), 91–110. https://doi.org/10.1080/12294659.2022.2071540

Alkraiji, A., & Ameen, N. (2022). The impact of service quality, trust and satisfaction on young citizen loyalty towards government e-services. *Information Technology & People, 35*(4), 1239–1270. https://doi.org/10.1108/ITP-04-2020-0229

Alzahrani, L., Al-Karaghouli, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review, 26*(1), 164–175. https://doi.org/10.1016/j.ibusrev.2016.06.004

Badan Siber dan Sandi Negara. (2025). *Lanskap keamanan siber Indonesia tahun 2024*. https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. *Information Systems Frontiers, 27*(3), 1089–1105. https://doi.org/10.1007/s10796-024-10497-8

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications.

Hooda, A., Gupta, P., Jeyaraj, A., Giannakis, M., & Dwivedi, Y. K. (2022). The effects of trust on behavioral intention and use behavior within e-government contexts. *International Journal of Information Management, 67*, Article 102553. https://doi.org/10.1016/j.ijinfomgt.2022.102553

Hooda, A., Gupta, P., Jeyaraj, A., & Dwivedi, Y. K. (2023). Clarifying the role of e-government trust in e-government success models: A meta-analytic structural equation modeling approach. *Australasian Journal of Information Systems, 27*. https://doi.org/10.3127/ajis.v27i0.4079

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*(1), 18–26. https://doi.org/10.1007/s13162-020-00161-0

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2024). *Keputusan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 13 Tahun 2024 tentang Hasil Evaluasi Sistem Pemerintahan Berbasis Elektronik pada Instansi Pusat dan Pemerintah Daerah Tahun 2023*.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2025, January 6). *Indeks SPBE nasional meningkat, Menteri Rini: Penguatan integrasi pelayanan publik berbasis digital*. https://www.menpan.go.id/posts/indeks-spbe-nasional-meningkat-menteri-rini-penguatan-integrasi-pelayanan-publik-berbasis-digital

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal, 28*(1), 227–261. https://doi.org/10.1111/isj.12131

Li, Y., & Shang, H. (2023). How does e-government use affect citizens' trust in government? Empirical evidence from China. *Information & Management, 60*(7), Article 103844. https://doi.org/10.1016/j.im.2023.103844

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Organisation for Economic Co-operation and Development. (2024). *Digital public infrastructure for digital governments*. OECD Publishing. https://doi.org/10.1787/ff525dc8-en

Rachmawati, Aswar, K., Sumardjo, M., & Wiguna, M. (2022). Personal and reliability factors affecting adoption and utilization of e-government: An effect of intention to use. *Problems and Perspectives in Management, 20*(2), 281–290. https://doi.org/10.21511/ppm.20(2).2022.23

Rahmatullah, R., Habibi, A., Khaeruddin, K., Yaqin, L. N., Alharmali, T. M., Fauzee, M. S. O., & Mahat, J. (2025). A study of user satisfaction and net benefits in Indonesia through the DeLone and McLean model for e-government success. *Discover Sustainability, 6*(1), 1–18. https://doi.org/10.1007/s43621-025-01645-4

Republik Indonesia. (2018). *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*.

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Santa, R., MacDonald, J. B., & Ferrer, M. (2019). The role of trust in e-Government effectiveness, operational effectiveness and user satisfaction: Lessons from Saudi Arabia in e-G2B. *Government Information Quarterly, 36*(1), 39–50. https://doi.org/10.1016/j.giq.2018.10.007

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *European Journal of Marketing, 53*(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Taufiqurokhman, T., Satispi, E., Andriansyah, A., Murod, M., & Sulastri, E. (2024). The impact of e-service quality on public trust and public satisfaction in e-government public services. *International Journal of Data and Network Science, 8*(2), 765–772. https://doi.org/10.5267/j.ijdns.2024.1.002

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences, 4*(2), 142–168. https://doi.org/10.20547/jms.2014.1704202

United Nations Department of Economic and Social Affairs. (2024). *United Nations e-government survey 2024: Accelerating digital transformation for sustainable development*. United Nations.