

Pengaruh *Public Trust* Terhadap *Platform Digital E-Government* dalam Keamanan Data Masyarakat Kelurahan Kalideres (Studi Kasus Pada Aplikasi Jaki Jakarta)

Tiara Rahmawati^{1*}, Rahma Lia Amanda², Shifa Rosa Apriyani³

^{1,2,3} Program Studi Administrasi Publik, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Islam Syekh Yusuf Tangerang, Indonesia

Email: ^{1*}tiarahmawati2005@gmail.com, ²shifarosa2005@gmail.com, ³rahmaliaamanda198@gmail.com

Published: Juli, 2026

ABSTRACT

The digital transformation of public services has encouraged governments to develop various e-government platforms to improve the effectiveness, efficiency, and quality of public service delivery. One of these innovations is the Jakarta Kini (JAKI) application developed by the Provincial Government of DKI Jakarta as an integrated public service platform. Despite the convenience it offers, the use of digital government services has also raised public concerns regarding personal data security. Citizens' perceptions of data security have become an essential factor in building public trust in digital government services. This study aims to analyze the effect of data security on public trust among JAKI users in Kalideres Village, West Jakarta. The study employed a mixed methods approach using a Sequential Explanatory Design, beginning with quantitative research followed by qualitative inquiry to strengthen the interpretation of the findings. The quantitative phase involved 101 respondents selected through purposive sampling. Data were analyzed using simple linear regression with SPSS. Subsequently, qualitative data were collected through in-depth interviews with selected informants. The results indicate that data security has a positive and significant effect on public trust. The coefficient of determination (R^2) of 0.857 indicates that data security explains 85.7% of the variation in public trust, while the remaining 14.3% is influenced by other factors outside the research model. Furthermore, the t-test confirms that data security significantly affects public trust with a significance value of <0.001 . These findings suggest that stronger perceptions of data security contribute to higher levels of public trust in digital government platforms.

Keywords: *Data Security; Public Trust; E-Government; JAKI; Digital Public Service.*

ABSTRAK

Transformasi digital dalam penyelenggaraan pelayanan publik mendorong pemerintah untuk mengembangkan berbagai platform e-government guna meningkatkan efektivitas, efisiensi, dan kualitas pelayanan kepada masyarakat. Salah satu inovasi tersebut adalah aplikasi Jakarta Kini (JAKI) yang dikembangkan oleh Pemerintah Provinsi DKI Jakarta sebagai super-app pelayanan publik. Di balik berbagai kemudahan yang ditawarkan, penggunaan aplikasi digital pemerintah menimbulkan tantangan baru berupa meningkatnya kekhawatiran masyarakat terhadap keamanan data pribadi. Persepsi masyarakat mengenai keamanan data menjadi faktor penting dalam membangun kepercayaan publik (*public trust*) terhadap layanan digital pemerintah. Penelitian ini bertujuan untuk menganalisis pengaruh keamanan data terhadap *public trust* pengguna aplikasi JAKI di Kelurahan Kalideres, Jakarta Barat. Penelitian menggunakan metode *mixed methods* dengan desain *Sequential Explanatory*, yaitu penelitian yang diawali melalui pendekatan kuantitatif kemudian dilanjutkan dengan pendekatan kualitatif untuk memperkuat interpretasi hasil. Pendekatan kuantitatif melibatkan 101 responden yang dipilih menggunakan teknik *purposive sampling*. Data dianalisis menggunakan analisis regresi linear sederhana dengan bantuan SPSS. Selanjutnya, pendekatan kualitatif dilakukan melalui wawancara mendalam kepada beberapa informan terpilih. Hasil penelitian menunjukkan bahwa keamanan data berpengaruh positif dan signifikan terhadap *public trust* masyarakat. Nilai koefisien determinasi (R^2) sebesar 0,857 menunjukkan bahwa keamanan data mampu menjelaskan 85,7% variasi *public trust* masyarakat terhadap aplikasi JAKI, sedangkan 14,3% dipengaruhi faktor lain di luar model penelitian. Hasil uji t juga menunjukkan bahwa variabel keamanan data memiliki pengaruh yang signifikan terhadap *public trust* dengan nilai signifikansi $<0,001$. Temuan penelitian menegaskan bahwa semakin tinggi persepsi masyarakat terhadap keamanan data, maka semakin tinggi pula tingkat kepercayaan masyarakat terhadap platform digital pemerintah.

Kata kunci: *keamanan data; public trust; e-government; JAKI; pelayanan publik digital.*

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong perubahan paradigma pelayanan publik dari sistem konvensional menuju pelayanan berbasis digital. Transformasi ini merupakan bagian dari implementasi electronic government (e-government) yang bertujuan meningkatkan efektivitas, efisiensi, transparansi, dan akuntabilitas penyelenggaraan pemerintahan. Melalui pemanfaatan teknologi digital, pemerintah berupaya memberikan pelayanan yang lebih cepat, mudah diakses, serta berorientasi pada kebutuhan masyarakat.

Di Indonesia, perkembangan e-government semakin didukung oleh meningkatnya penggunaan internet. Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa jumlah pengguna internet pada tahun 2025 mencapai sekitar 229 juta jiwa atau sekitar 80,66% dari total populasi nasional. Tingginya penetrasi internet memberikan peluang besar bagi pemerintah untuk memperluas penyelenggaraan pelayanan publik berbasis digital. Namun demikian, meningkatnya aktivitas digital masyarakat juga diikuti oleh berbagai ancaman keamanan siber, seperti pencurian data pribadi, phishing, penyalahgunaan identitas digital, hingga kebocoran data yang berpotensi menurunkan tingkat kepercayaan masyarakat terhadap layanan digital pemerintah.

Salah satu implementasi e-government di Indonesia adalah aplikasi Jakarta Kini (JAKI) yang dikembangkan oleh Pemerintah Provinsi DKI Jakarta. JAKI merupakan platform pelayanan publik yang mengintegrasikan berbagai layanan pemerintahan, mulai dari administrasi kependudukan, pengaduan masyarakat, layanan kesehatan, informasi transportasi, bantuan sosial, hingga informasi kebencanaan dalam satu aplikasi. Integrasi berbagai layanan tersebut diharapkan mampu meningkatkan kualitas pelayanan publik sekaligus memperkuat hubungan antara pemerintah dan masyarakat melalui pemanfaatan teknologi digital.

Meskipun demikian, penggunaan aplikasi digital pemerintah mengharuskan masyarakat memberikan berbagai informasi pribadi, seperti identitas, nomor telepon, lokasi, serta data administratif lainnya. Kondisi tersebut menyebabkan masyarakat semakin memperhatikan aspek keamanan data sebelum menggunakan layanan digital pemerintah. Berbagai kasus kebocoran data yang terjadi di Indonesia dalam beberapa tahun terakhir turut meningkatkan kekhawatiran masyarakat terhadap perlindungan data pribadi. Apabila pemerintah tidak mampu menjamin keamanan informasi pengguna, maka tingkat penerimaan masyarakat terhadap layanan digital pemerintah dapat menurun.

Dalam perspektif administrasi publik, kepercayaan masyarakat (public trust) merupakan salah satu indikator penting keberhasilan implementasi e-government. OECD menjelaskan bahwa kepercayaan publik dibangun melalui kemampuan pemerintah dalam menyediakan pelayanan yang andal, transparan, akuntabel, responsif, dan berintegritas. Pada konteks pemerintahan digital, dimensi tersebut semakin erat kaitannya dengan kemampuan pemerintah dalam menjaga keamanan sistem informasi serta melindungi data pribadi masyarakat. Oleh karena itu, keamanan data tidak lagi dipandang hanya sebagai aspek teknis, tetapi juga menjadi faktor strategis dalam membangun legitimasi pemerintah di era digital.

Berbagai penelitian terdahulu menunjukkan bahwa keamanan sistem dan perlindungan privasi memiliki hubungan yang erat dengan kepercayaan masyarakat terhadap layanan e-government. Penelitian sebelumnya lebih banyak membahas kualitas layanan digital dan kepuasan pengguna, sedangkan penelitian yang secara khusus mengkaji pengaruh keamanan data terhadap public trust pada platform digital pemerintah masih relatif terbatas, khususnya pada tingkat masyarakat kelurahan sebagai pengguna langsung layanan publik digital. Kesenjangan tersebut menunjukkan perlunya penelitian yang secara khusus mengkaji hubungan antara keamanan data dan public trust dalam penggunaan aplikasi JAKI.

Penelitian ini bertujuan menganalisis pengaruh keamanan data terhadap public trust masyarakat pengguna aplikasi JAKI di Kelurahan Kalideres, Jakarta Barat. Hasil penelitian diharapkan dapat memberikan kontribusi akademis dalam pengembangan kajian digital governance dan e-government, sekaligus menjadi bahan evaluasi bagi Pemerintah Provinsi DKI Jakarta dalam meningkatkan keamanan sistem informasi serta memperkuat kepercayaan masyarakat terhadap pelayanan publik berbasis digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan *mixed methods* dengan desain *Sequential Explanatory*, yaitu penelitian yang diawali dengan pengumpulan dan analisis data kuantitatif, kemudian dilanjutkan dengan pendekatan kualitatif untuk memperdalam interpretasi hasil kuantitatif. Desain ini dipilih karena mampu

memberikan pemahaman yang lebih komprehensif mengenai hubungan antara keamanan data dan *public trust* masyarakat terhadap penggunaan aplikasi JAKI.

Penelitian dilaksanakan di Kelurahan Kalideres, Kecamatan Kalideres, Kota Administrasi Jakarta Barat. Lokasi penelitian dipilih karena masyarakat di wilayah tersebut telah memanfaatkan aplikasi JAKI sebagai salah satu media pelayanan publik digital yang disediakan oleh Pemerintah Provinsi DKI Jakarta.

Pada tahap kuantitatif, populasi penelitian adalah seluruh masyarakat Kelurahan Kalideres yang pernah menggunakan aplikasi JAKI. Karena jumlah populasi tidak diketahui secara pasti (*unknown population*), maka jumlah sampel ditentukan menggunakan rumus *Lemeshow* dengan tingkat kepercayaan 95% dan margin of error sebesar 10%. Hasil perhitungan menunjukkan jumlah sampel minimum sebanyak 96 responden, kemudian dibulatkan menjadi 100 responden untuk mengantisipasi data yang tidak valid. Dalam pelaksanaannya, penelitian berhasil memperoleh 101 responden yang memenuhi kriteria penelitian. Teknik pengambilan sampel menggunakan *purposive sampling* dengan kriteria responden berusia minimal 17 tahun, berdomisili di Kelurahan Kalideres, pernah menggunakan aplikasi JAKI, dan bersedia menjadi responden penelitian.

Variabel independen dalam penelitian ini adalah Keamanan Data (X) yang diadaptasi dari konsep *Internet Users' Information Privacy Concerns* (IUIPC) yang dikembangkan oleh Malhotra, Kim, dan Agarwal (2004). Variabel ini diukur melalui lima dimensi, yaitu *collection*, *control*, *awareness*, *system security*, dan *risk of misuse*. Sementara itu, variabel dependen adalah Public Trust (Y) yang mengacu pada indikator OECD (2022), meliputi *reliability*, *responsiveness*, *openness*, *integrity*, dan *fairness*. Seluruh indikator diukur menggunakan skala Likert lima tingkat.

Instrumen penelitian terlebih dahulu diuji melalui *pilot test* terhadap 30 responden. Hasil pengujian menunjukkan seluruh item pernyataan valid sehingga layak digunakan pada penelitian utama. Selanjutnya, pengumpulan data dilakukan melalui penyebaran kuesioner secara daring menggunakan Google Form. Data kuantitatif dianalisis menggunakan perangkat lunak SPSS versi 26 melalui uji validitas, uji reliabilitas, analisis statistik deskriptif, uji asumsi klasik, koefisien determinasi (R^2), uji F, uji t, serta analisis regresi linear sederhana. Tahap kualitatif dilakukan melalui wawancara mendalam terhadap beberapa informan untuk menjelaskan hasil analisis kuantitatif secara lebih komprehensif.

Tabel 1. Operasional Variabel Penelitian

Variabel	Dimensi	Indikator	No. Item	Skala
Keamanan Data (X)	Collection	Pengumpulan data sesuai kebutuhan layanan	1	Likert
		Transparansi tujuan pengumpulan data	2	Likert
	Control	Kebebasan pengguna mengontrol data	3	Likert
		Persetujuan penggunaan data	4	Likert
	Awareness	Pemahaman terhadap kebijakan privasi	5	Likert
		Pengetahuan keamanan data aplikasi	6	Likert
	System Security	Keamanan sistem aplikasi	7	Likert
		Perlindungan terhadap kebocoran data	8	Likert
	Risk of Misuse	Risiko penyalahgunaan data	9	Likert
		Keamanan akses informasi pribadi	10	Likert
Public Trust (Y)	Reliability	Keandalan aplikasi	11	Likert
		Konsistensi pelayanan	12	Likert
	Responsiveness	Kecepatan respons	13	Likert

		Tanggapan terhadap kebutuhan masyarakat	14	Likert
	Openness	Keterbukaan informasi	15	Likert
		Transparansi sistem	16	Likert
	Integrity	Kejujuran pemerintah	17	Likert
		Tanggung jawab perlindungan data	18	Likert
	Fairness	Kesetaraan pelayanan	19	Likert
		Akses layanan tanpa diskriminasi	20	Likert

Sumber: Diolah Peneliti berdasarkan Malhotra et al. (2004), OECD (2022), dan Wirtz et al. (2022).

HASIL DAN PEMBAHASAN

Hasil Penelitian

3.1 Hasil Uji Validitas

Uji validitas dilakukan untuk mengetahui sejauh mana setiap item pernyataan mampu mengukur variabel yang diteliti. Suatu instrumen dinyatakan valid apabila nilai r hitung lebih besar daripada r tabel pada tingkat signifikansi 5%. Sebelum penyebaran kuesioner kepada sampel utama, peneliti telah melakukan *pilot test* terhadap 30 responden. Hasil pengujian awal menunjukkan bahwa seluruh item memenuhi kriteria validitas sehingga layak digunakan pada penelitian utama. Selanjutnya, uji validitas dilakukan kembali terhadap data penelitian yang diperoleh dari 101 responden.

Tabel 1. Hasil Uji Validitas

Variabel	Item Pernyataan	R hitung	R tabel	Keterangan
Keamanan Data (X)	Item X01	0,908	0,195	Valid
	Item X02	0,785	0,195	Valid
	Item X03	0,825	0,195	Valid
	Item X04	0,868	0,195	Valid
	Item X05	0,884	0,195	Valid
	Item X06	0,790	0,195	Valid
	Item X07	0,741	0,195	Valid
	Item X08	0,761	0,195	Valid
	Item X09	0,638	0,195	Valid
	Item X10	0,870	0,195	Valid
Public Trust (Y)	Item Y01	0,846	0,195	Valid
	Item Y02	0,782	0,195	Valid
	Item Y03	0,887	0,195	Valid
	Item Y04	0,849	0,195	Valid
	Item Y05	0,866	0,195	Valid
	Item Y06	0,848	0,195	Valid
	Item Y07	0,794	0,195	Valid

Item Y08	0,850	0,195	Valid
Item Y09	0,842	0,195	Valid
Item Y10	0,914	0,195	Valid

Sumber: Data primer yang diolah, 2026

Berdasarkan Tabel 1, seluruh item pada variabel Keamanan Data dan Public Trust memiliki nilai r hitung lebih besar dari r tabel (0,195), sehingga seluruh pernyataan dinyatakan valid. Nilai r hitung pada Keamanan Data berkisar antara 0,638–0,908, sedangkan pada Public Trust antara 0,782–0,914. Meskipun Item X09 memiliki nilai validitas terendah (0,638), nilainya tetap memenuhi kriteria validitas. Hasil ini menunjukkan bahwa seluruh indikator mampu merepresentasikan konstruk yang diukur secara tepat dan konsisten. Dengan demikian, instrumen penelitian memiliki tingkat ketepatan pengukuran yang baik sehingga layak digunakan sebagai alat pengumpulan data dan dapat dilanjutkan pada tahap uji reliabilitas, analisis deskriptif, serta pengujian hipotesis.

3.2 Hasil Uji Reliabilitas

Setelah instrumen dinyatakan valid, tahap berikutnya adalah menguji reliabilitas untuk mengetahui tingkat konsistensi instrumen penelitian. Pengujian reliabilitas dilakukan menggunakan metode **Cronbach's Alpha** dengan batas minimum sebesar 0,60. Nilai Cronbach's Alpha yang melebihi batas tersebut menunjukkan bahwa instrumen memiliki tingkat konsistensi yang baik dalam mengukur variabel penelitian.

Tabel 2. Hasil Uji Reliabilitas

Variabel	Jumlah Item	Cronbach's Alpha	Keterangan
Keamanan Data (X)	10	0,954	Reliabel
Public Trust (Y)	10	0,967	Reliabel

Sumber: Data primer yang diolah, 2026

Berdasarkan Tabel 2, variabel Keamanan Data memiliki nilai Cronbach's Alpha sebesar 0,954, sedangkan Public Trust sebesar 0,967. Kedua nilai tersebut melebihi batas minimum 0,60, sehingga seluruh indikator dinyatakan sangat reliabel dan layak digunakan. Nilai Cronbach's Alpha yang mendekati 1 menunjukkan bahwa setiap indikator memiliki konsistensi internal yang sangat baik dengan tingkat kesalahan pengukuran yang rendah. Pada variabel Keamanan Data, indikator pengumpulan data, kontrol data, kesadaran pengguna, keamanan sistem, dan risiko penyalahgunaan data secara konsisten mengukur persepsi keamanan data. Sementara itu, pada variabel Public Trust, indikator reliability, responsiveness, openness, integrity, dan fairness secara konsisten menggambarkan tingkat kepercayaan masyarakat. Dengan demikian, instrumen penelitian memiliki reliabilitas yang sangat tinggi sehingga layak digunakan dalam analisis statistik selanjutnya.

3.3 Hasil Analisis Statistik Deskriptif

Analisis statistik deskriptif dilakukan untuk memberikan gambaran umum mengenai karakteristik data penelitian berdasarkan nilai minimum, maksimum, rata-rata (*mean*), dan standar deviasi dari masing-masing variabel. Analisis ini bertujuan untuk mengetahui kecenderungan persepsi responden terhadap Keamanan Data dan Public Trust sebelum dilakukan pengujian hipotesis.

Tabel 3. Hasil Analisis Statistik Deskriptif

Variabel / Statistics	N	Minimum	Maximum	Mean	Std. Deviation
Keamanan Data (X)	101	10,00	50,00	38,45	5,21
Public Trust (Y)	101	10,00	50,00	37,92	5,54
Valid N (listwise)	101				

Sumber: Data primer yang diolah, 2026

Berdasarkan Tabel 3, variabel Keamanan Data memiliki nilai minimum 10, maksimum 50, rata-rata 38,45, dan standar deviasi 5,21, yang menunjukkan bahwa sebagian besar responden memberikan penilaian positif terhadap keamanan data pada aplikasi JAKI. Variabel Public Trust memiliki nilai minimum 10, maksimum 50, rata-rata 37,92, dan standar deviasi 5,54, sehingga menunjukkan tingkat kepercayaan masyarakat yang juga tergolong baik. Rata-rata Keamanan Data yang sedikit lebih tinggi dibandingkan Public Trust mengindikasikan bahwa kepercayaan masyarakat tidak hanya dipengaruhi oleh keamanan data, tetapi juga oleh faktor lain, seperti kualitas layanan, kemudahan penggunaan, dan respons pemerintah. Selain itu, standar deviasi kedua variabel yang lebih kecil dari nilai rata-rata menunjukkan bahwa jawaban responden relatif seragam dan memiliki variasi yang rendah.

3.4 Hasil Analisis Regresi Linear Sederhana

Analisis regresi linear sederhana dilakukan untuk mengetahui pengaruh variabel Keamanan Data (X) terhadap Public Trust (Y) pada pengguna aplikasi JAKI di Kelurahan Kalideres. Sebelum dilakukan pengujian hipotesis, model regresi telah memenuhi asumsi normalitas sehingga layak digunakan untuk menganalisis hubungan antara kedua variabel penelitian. Pengujian regresi meliputi koefisien determinasi (R^2), uji kelayakan model (Uji F), uji parsial (Uji t), dan persamaan regresi linear sederhana.

3.3.1 Koefisien Determinasi (R^2)

Koefisien determinasi digunakan untuk mengetahui seberapa besar kemampuan variabel independen dalam menjelaskan perubahan variabel dependen. Semakin besar nilai koefisien determinasi, maka semakin besar pula kemampuan model dalam menjelaskan hubungan antarvariabel penelitian.

Tabel 4. Hasil Koefisien Determinasi (Model Summary)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,926	0,857	0,855	4,282

Sumber: Output SPSS Versi 26, Data Primer Diolah Tahun 2026.

Berdasarkan Tabel 4, nilai koefisien korelasi (R) sebesar 0,926 menunjukkan bahwa hubungan antara Keamanan Data dan Public Trust sangat kuat. Nilai R Square sebesar 0,857 mengindikasikan bahwa 85,7% variasi Public Trust dapat dijelaskan oleh Keamanan Data, sedangkan 14,3% sisanya dipengaruhi faktor lain, seperti kualitas layanan digital, kemudahan penggunaan, kualitas informasi, pengalaman pengguna, dan kecepatan respons pemerintah. Nilai Adjusted R Square sebesar 0,855

menunjukkan bahwa model regresi memiliki tingkat ketepatan yang tinggi. Temuan ini menegaskan bahwa keamanan data merupakan faktor dominan dalam membangun kepercayaan masyarakat terhadap aplikasi JAKI, sehingga peningkatan keamanan data menjadi strategi penting dalam mendukung keberhasilan layanan publik digital.

3.3.2 Uji Kelayakan Model (Uji F)

Uji F dilakukan untuk mengetahui apakah model regresi yang digunakan layak (*goodness of fit*) dalam menjelaskan hubungan antara variabel Keamanan Data dengan Public Trust. Model regresi dinyatakan layak apabila memiliki nilai signifikansi kurang dari 0,05.

Tabel 5. Hasil Uji F (ANOVA)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10870,950	1	10870,950	592,893	<,001 ^b
	Residual	1815,208	99	18,335		
	Total	12686,158	100			

a. Dependent Variable: Public Trust

b. Predictors: (Constant), Keamanan Data

Sumber: Output SPSS Versi 26, Data Primer Diolah Tahun 2026.

Berdasarkan hasil pengujian diperoleh nilai F hitung sebesar 592,893 dengan tingkat signifikansi 0,000. Nilai signifikansi tersebut lebih kecil daripada taraf signifikansi sebesar 0,05 sehingga model regresi dinyatakan layak digunakan dalam penelitian ini. Dengan demikian, model mampu menjelaskan hubungan antara Keamanan Data dan Public Trust secara signifikan.

Besarnya nilai F menunjukkan bahwa variasi Public Trust secara keseluruhan dapat dijelaskan oleh variabel Keamanan Data. Hasil ini mengindikasikan bahwa model regresi memiliki tingkat kecocokan (*goodness of fit*) yang sangat baik. Dengan kata lain, model yang dibangun telah sesuai dengan data empiris sehingga mampu menjelaskan fenomena yang terjadi pada masyarakat pengguna aplikasi JAKI.

Selain itu, hasil uji F juga memperkuat bahwa model penelitian memiliki kemampuan yang baik dalam menjelaskan hubungan antarvariabel. Oleh karena itu, model regresi layak digunakan sebagai dasar dalam pengujian hipotesis melalui uji parsial (uji t).

3.3.3 Uji Parsial (Uji t)

Uji parsial dilakukan untuk mengetahui apakah variabel Keamanan Data secara individual memiliki pengaruh yang signifikan terhadap Public Trust masyarakat pengguna aplikasi JAKI.

Tabel 6. Hasil Uji t (Coefficients)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,284	1,355		,948	,346
	Keamanan Data	,957	,039	,926	24,349	<,001

a. Dependent Variable: Public Trust

Sumber: Output SPSS Versi 26, Data Primer Diolah Tahun 2026.

Berdasarkan Tabel 6, variabel Keamanan Data memiliki nilai t hitung sebesar 24,349, lebih besar dari t tabel sebesar 1,984, dengan nilai signifikansi 0,000 (<0,05). Hasil ini menunjukkan bahwa Keamanan Data berpengaruh positif dan signifikan terhadap Public Trust, sehingga hipotesis penelitian diterima. Koefisien regresi yang bernilai positif mengindikasikan bahwa semakin tinggi persepsi masyarakat

terhadap keamanan data, semakin tinggi pula tingkat kepercayaan mereka terhadap aplikasi JAKI. Sebaliknya, rendahnya persepsi keamanan data dapat menurunkan kepercayaan masyarakat. Temuan ini menunjukkan bahwa keberhasilan implementasi JAKI tidak hanya bergantung pada inovasi teknologi, tetapi juga pada kemampuan pemerintah menjaga kerahasiaan, integritas, dan keamanan data pribadi pengguna.

3.5 Hasil Analisis Kualitatif

Tabel 7. Profil Informan

No.	Kode Responden	Kategori Public Trust	Keterangan
1.	R 16	Tinggi	Pengguna aktif aplikasi JAKI
2.	R 13	Sedang	Pengguna aplikasi JAKI
3.	R 15	Rendah	Pengguna aplikasi JAKI

Sumber: Data primer diolah peneliti (2026).

Setelah analisis kuantitatif menunjukkan bahwa Keamanan Data berpengaruh positif dan signifikan terhadap Public Trust, penelitian dilanjutkan dengan wawancara mendalam terhadap tiga informan yang mewakili tingkat kepercayaan tinggi (R16), sedang (R13), dan rendah (R15). Seluruh informan menilai keamanan data sebagai aspek penting dalam penggunaan aplikasi JAKI, namun tingkat kepercayaan dipengaruhi oleh pengalaman penggunaan, transparansi pengelolaan data, dan manfaat layanan. Informan R16 meyakini data pribadinya aman karena aplikasi dikelola pemerintah dan belum pernah mengalami penyalahgunaan data. Sebaliknya, R13 dan R15 masih mengharapkan penjelasan yang lebih transparan mengenai mekanisme pengumpulan, penyimpanan, dan penggunaan data pribadi. R15 juga menilai manfaat aplikasi belum optimal sehingga memengaruhi tingkat kepercayaan. Temuan ini menunjukkan bahwa Public Trust dibangun melalui kombinasi keamanan data, transparansi pengelolaan informasi, pengalaman penggunaan, dan kualitas layanan yang diberikan pemerintah.

3.7 Integrasi Hasil Kuantitatif dan Kualitatif

Sesuai dengan desain Sequential Explanatory Mixed Methods, hasil penelitian kuantitatif dan kualitatif diintegrasikan untuk memperoleh pemahaman yang lebih komprehensif mengenai hubungan antara Keamanan Data dan *Public Trust*. Hasil analisis kuantitatif menunjukkan bahwa Keamanan Data berpengaruh positif dan signifikan terhadap *Public Trust*, sedangkan hasil wawancara memberikan penjelasan mengenai alasan di balik hubungan tersebut.

Integrasi kedua jenis data menunjukkan bahwa tingginya *public trust* tidak hanya dipengaruhi oleh keberadaan sistem keamanan aplikasi, tetapi juga oleh pengalaman pengguna, transparansi pengelolaan data pribadi, serta manfaat layanan yang dirasakan. Informan dengan tingkat kepercayaan tinggi memiliki persepsi positif terhadap seluruh dimensi keamanan data dan merasakan manfaat nyata dari aplikasi. Sebaliknya, informan dengan tingkat kepercayaan sedang dan rendah mengharapkan adanya peningkatan transparansi mengenai pengelolaan data pribadi serta penyempurnaan kualitas layanan aplikasi.

Temuan tersebut memperkuat hasil analisis kuantitatif bahwa keamanan data merupakan faktor penting dalam membentuk *public trust*. Namun demikian, hasil wawancara juga menunjukkan bahwa peningkatan kepercayaan masyarakat memerlukan pendekatan yang lebih komprehensif, yaitu melalui penguatan keamanan sistem, peningkatan keterbukaan informasi mengenai perlindungan data pribadi, serta pengembangan kualitas pelayanan publik digital agar lebih responsif terhadap kebutuhan masyarakat.

Pembahasan

Hasil penelitian menunjukkan bahwa Keamanan Data berpengaruh positif dan signifikan terhadap Public Trust pada pengguna aplikasi Jakarta Kini (JAKI) di Kelurahan Kalideres. Analisis kuantitatif menunjukkan hubungan yang sangat kuat antara kedua variabel, sedangkan hasil wawancara memperkuat bahwa keamanan data menjadi pertimbangan utama masyarakat dalam menggunakan layanan publik digital. Temuan ini menunjukkan bahwa persepsi terhadap keamanan data tidak hanya

meningkatkan keinginan masyarakat menggunakan aplikasi JAKI, tetapi juga memperkuat kepercayaan terhadap pemerintah sebagai penyedia layanan digital. Hasil ini sejalan dengan Governance Theory yang menekankan pentingnya akuntabilitas, transparansi, efektivitas, dan perlindungan hak masyarakat dalam penyelenggaraan pemerintahan digital. Dalam konteks tersebut, perlindungan data pribadi merupakan bentuk tanggung jawab pemerintah untuk menjamin keamanan informasi pengguna sekaligus meningkatkan kualitas tata kelola pemerintahan digital (OECD, 2022; Venkatesh et al., 2023; Dwivedi et al., 2023).

Hasil wawancara menunjukkan bahwa responden dengan tingkat kepercayaan tinggi meyakini aplikasi JAKI telah dikelola secara baik sehingga data pribadi mereka aman. Sebaliknya, responden dengan tingkat kepercayaan sedang dan rendah masih mengharapkan transparansi yang lebih besar mengenai mekanisme pengumpulan, penyimpanan, penggunaan, dan perlindungan data pribadi. Temuan ini mengindikasikan bahwa kepercayaan masyarakat tidak hanya dibangun melalui penerapan teknologi keamanan, tetapi juga melalui keterbukaan informasi dari pemerintah. Kondisi tersebut mendukung konsep Public Trust yang menyatakan bahwa kepercayaan publik dibangun melalui dimensi reliability, responsiveness, openness, integrity, dan fairness, di mana keterbukaan informasi dan integritas dalam pengelolaan data menjadi elemen penting dalam pelayanan publik digital (OECD, 2022; Janssen et al., 2023; AlHogail, 2024).

Temuan penelitian ini juga konsisten dengan berbagai penelitian sebelumnya yang menyatakan bahwa keamanan data merupakan determinan utama keberhasilan implementasi e-government dan smart government. Masyarakat cenderung memberikan kepercayaan yang lebih tinggi ketika pemerintah mampu menjamin kerahasiaan data pribadi serta meminimalkan risiko penyalahgunaan informasi. Perlindungan privasi yang kuat juga meningkatkan penerimaan masyarakat terhadap layanan digital pemerintah sekaligus mendorong penggunaan layanan secara berkelanjutan (Mensah et al., 2020; Sharma et al., 2021; Abu-Shanab, 2022; Alenezi, 2023; Al-Rahmi et al., 2024; Chatterjee et al., 2024).

Meskipun demikian, penelitian ini menunjukkan bahwa Keamanan Data hanya menjelaskan 85,7% variasi Public Trust, sedangkan 14,3% sisanya dipengaruhi oleh faktor lain. Berdasarkan hasil wawancara, faktor-faktor tersebut meliputi kemudahan penggunaan aplikasi, kualitas layanan, kecepatan respons terhadap pengaduan, stabilitas sistem, serta transparansi tindak lanjut layanan. Temuan ini menunjukkan bahwa peningkatan keamanan data saja belum cukup untuk membangun kepercayaan masyarakat secara optimal apabila tidak diimbangi dengan peningkatan kualitas pelayanan publik secara menyeluruh. Oleh karena itu, Pemerintah Provinsi DKI Jakarta perlu terus memperkuat keamanan siber, melakukan pembaruan sistem secara berkala, meningkatkan transparansi pengelolaan data pribadi, serta memperbaiki kualitas layanan digital agar kepercayaan masyarakat terhadap aplikasi JAKI semakin meningkat. Secara keseluruhan, penelitian ini menegaskan bahwa keberhasilan transformasi pelayanan publik digital tidak hanya ditentukan oleh inovasi teknologi, tetapi juga oleh kemampuan pemerintah dalam mengelola data pribadi secara aman, transparan, akuntabel, dan berorientasi pada kebutuhan masyarakat (Hair et al., 2024; Field, 2025; Criado & Gil-Garcia, 2024).

KESIMPULAN DAN SARAN

Kesimpulan penelitian ini menunjukkan bahwa Keamanan Data berpengaruh positif dan signifikan terhadap Public Trust pada pengguna aplikasi Jakarta Kini (JAKI) di Kelurahan Kalideres. Hasil analisis kuantitatif membuktikan bahwa semakin tinggi persepsi masyarakat terhadap keamanan data yang diterapkan pada aplikasi JAKI, maka semakin tinggi pula tingkat kepercayaan masyarakat terhadap layanan publik digital yang diselenggarakan oleh Pemerintah Provinsi DKI Jakarta. Variabel Keamanan Data mampu menjelaskan sebesar 85,7% variasi Public Trust, sedangkan sisanya dipengaruhi oleh faktor lain di luar model penelitian. Temuan ini menunjukkan bahwa keamanan data merupakan faktor penting dalam membangun dan mempertahankan kepercayaan masyarakat terhadap layanan digital pemerintah.

Hasil analisis kualitatif memperkuat temuan tersebut dengan menunjukkan bahwa keamanan data tidak hanya dipandang sebagai aspek teknis, tetapi juga sebagai faktor strategis yang memengaruhi kepercayaan masyarakat terhadap aplikasi JAKI. Informan yang memiliki tingkat kepercayaan tinggi menilai bahwa pengelolaan data pada aplikasi JAKI telah memberikan rasa aman, sedangkan informan dengan tingkat kepercayaan sedang dan rendah masih mengharapkan peningkatan transparansi terkait mekanisme pengelolaan dan perlindungan data pribadi. Oleh karena itu, Pemerintah Provinsi DKI Jakarta

disarankan untuk terus meningkatkan keamanan sistem informasi, melakukan audit keamanan secara berkala, memperkuat transparansi pengelolaan data pengguna, serta meningkatkan kualitas layanan dan kecepatan respons terhadap pengaduan. Peneliti selanjutnya juga disarankan untuk menambahkan variabel lain yang berpotensi memengaruhi Public Trust dan memperluas cakupan lokasi penelitian agar diperoleh hasil yang lebih komprehensif dan memiliki tingkat generalisasi yang lebih tinggi.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada seluruh responden pengguna aplikasi Jakarta Kini (JAKI) di Kelurahan Kalideres yang telah berpartisipasi dalam penelitian ini, serta kepada para informan yang bersedia meluangkan waktu untuk memberikan informasi dan pengalaman terkait penggunaan aplikasi JAKI. Ucapan terima kasih juga disampaikan kepada semua pihak yang telah memberikan dukungan, bantuan, dan fasilitas selama proses penelitian sehingga penelitian ini dapat diselesaikan dengan baik dan memberikan kontribusi bagi pengembangan pelayanan publik digital di Indonesia.

DAFTAR REFERENSI

- Abu-Shanab, E. (2022). Factors influencing citizens' adoption of smart government services: The role of trust, privacy, and security. *International Journal of Electronic Government Research*, 18(4), 1–17.
- Abu-Shanab, E. (2022). Smart government implementation and citizens' trust: The role of privacy and data protection. *International Journal of Public Administration*.
- Alenezi, M. (2023). Data privacy, cybersecurity, and public trust in digital government services. *Information*, 14(9), 485. <https://doi.org/10.3390/info14090485>
- AlHogail, A. (2024). Citizens' trust in digital government: The role of privacy, transparency, and cybersecurity. *Sustainability*, 16(3), 1184. <https://doi.org/10.3390/su16031184>
- Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2024). Factors affecting citizens' adoption of digital government services: A systematic review. *Heliyon*, 10(2), e24156. <https://doi.org/10.1016/j.heliyon.2024.e24156>
- Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165–176. <https://doi.org/10.1016/j.jsis.2007.12.002>
- Chatterjee, S., Rana, N. P., Dwivedi, Y. K., & Sharma, A. (2024). Understanding citizen trust and adoption of digital public services: A systematic review. *Government Information Quarterly*, 41(2), 101965.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Criado, J. I., & Gil-Garcia, J. R. (2024). Digital government transformation: Trends, challenges, and future directions. *Government Information Quarterly*, 41(1), 101932.
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges, and implications of generative conversational AI for research, practice, and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>
- Field, A. (2025). *Discovering statistics using IBM SPSS Statistics* (6th ed.). Sage Publications.
- Hadita, A., Agustina, N., & Bella, S. (2025). Kepuasan pengguna aplikasi Pasti Oke melalui kualitas pelayanan e-government di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Garut. *Jurnal Algoritma*, 22(1), 1002–1012.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2024). *Multivariate data analysis* (9th ed.). Cengage Learning.
- Jan Kooiman. (2003). *Governing as governance*. SAGE Publications.
- Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2023). Trust, transparency, and artificial intelligence in digital government: A research agenda. *Government Information Quarterly*, 40(4), 101889.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>

- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.5465/amr.1995.9508080335>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.8>
- Mensah, I. K. (2020). Citizens' trust, risk, and intention to adopt e-government services: Evidence from developing countries. *International Journal of Public Administration*.
- Mensah, I. K., Zeng, G., & Luo, C. (2020). E-government services adoption: The role of perceived privacy, security, and trust. *Telematics and Informatics*, 53, 10139.
- Organisation for Economic Co-operation and Development. (2005). *E-government for better government*. OECD Publishing. <https://doi.org/10.1787/9789264018341-en>
- Organisation for Economic Co-operation and Development. (2009). *Rethinking e-government services: User-centred approaches*. OECD Publishing. <https://doi.org/10.1787/9789264059412-e>
- Organisation for Economic Co-operation and Development. (2022). *Building trust to reinforce democracy: Main findings from the 2021 OECD survey on drivers of trust in public institutions*. OECD Publishing. <https://doi.org/10.1787/b407f99c-en>
- Organisation for Economic Co-operation and Development. (2024). *Digital government*. OECD. <https://www.oecd.org/en/topics/digital-government.html>
- Pribadi, U., Iqbal, M., & Restiane, F. (2021). Factors affecting trust in e-government. *Journal of Government and Civil Society*, 5(2), 263–284. <https://doi.org/10.31000/jgcs.v5i2.4848>
- Rahman, F. (2021). Kerangka hukum perlindungan data pribadi dalam penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia. *Jurnal Legislasi Indonesia*, 18(1), 81–102.
- Sharma, S. K., Al-Badi, A., Rana, N. P., & Al-Azizi, L. (2021). Digital government adoption: The role of privacy, trust, and perceived security. *Transforming Government: People, Process and Policy*, 15(4), 603–621.
- Sharma, S., Singh, G., & Sharma, R. (2021). Data privacy and citizen trust in digital government services. *Government Information Quarterly*.
- Sugiyono. (2022). *Metode penelitian kuantitatif, kualitatif, dan kombinasi (mixed methods)*. Alfabeta.
- Syahroni, F., Ardiansyah, Pribadi, U., Rafi, M., & Amri, P. (2023). Factors affecting trust and use of e-government: The case of Banda Aceh City, Aceh Province. *Jurnal Ilmu Pemerintahan: Kajian Ilmu Pemerintahan dan Politik Daerah*, 8(2), 72–85. <https://doi.org/10.24905/jip.8.2.2023.72-85>
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. (2022). *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196*.
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2023). Unified theory of acceptance and use of technology: Advances and future directions. *Journal of the Association for Information Systems*, 24(2), 325–356.
- Wenjuan, L. (2021). The role of trust and risk in citizens' e-government services adoption: A perspective of the extended UTAUT model. *Sustainability*, 13(14), 7671. <https://doi.org/10.3390/su13147671>
- Widiani, Y. N., & Abdullah. (2018). Pengaruh kualitas layanan e-government terhadap kepuasan pengguna aplikasi e-Filing. *Jurnal Administrasi Publik*.
- Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*.