



Strategi Keamanan Transaksi Elektronik dalam Pelayanan Publik Berbasis E-Government

Electronic Transaction Security Strategies in E-Government-Based Public Services

Dini Andriani^{1*}, Abd. Haris², Sumardi³

^{1,2,3} Ilmu Pemerintahan, Universitas Muhammadiyah Sinjai, Indonesia.

*Author correspondence: dini38403@gmail.com

ARTICLE INFO

Article History:

Submitted:

2025-11-21

Revised:

2025-11-24

Accepted:

2025-11-25

Published:

2025-12-01

Keywords: e-government;
electronic transactions;
security strategies; public
services;

Kata kunci: e-government;
transaksi elektronik; strategi
keamanan; pelayanan
publik;

This is an open access article
under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



ABSTRACT

Digital transformation has driven significant changes in the delivery of public services. In the era of e-government, service digitalization is aimed at creating a bureaucracy that is more transparent, efficient, and responsive. One of the most complex stages in e-government is transact, namely the phase of data exchange and electronic transactions between citizens and the government. The high sensitivity of data at this stage makes security a crucial factor. This study aims to analyze electronic transaction security strategies in e-government comprehensively. The research method used is a descriptive qualitative approach with a literature study (library research) method. The findings show that electronic transaction security in e-government is supported by the use of various technologies, including encryption, digital signatures, Public Key Infrastructure (PKI), firewalls, biometric authentication, and blockchain to ensure data confidentiality and reliability, as well as strong regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law. In addition, the readiness of human resources, both from the government and the public, is also a determining factor for success, particularly in the areas of digital literacy, information security training, and a risk-aware work culture. These three aspects complement one another in building a reliable security system.

ABSTRAK

Transformasi digital telah mendorong perubahan signifikan dalam penyelenggaraan pelayanan publik. Dalam era e-government, digitalisasi pelayanan diarahkan untuk menciptakan birokrasi yang lebih transparan, efisien, dan responsif. Salah satu tahap paling kompleks dalam e-government adalah transact, yaitu fase pertukaran data dan transaksi elektronik antara masyarakat dan pemerintah. Tingginya sensitivitas data pada tahap ini menjadikan keamanan

sebagai faktor krusial. Penelitian ini bertujuan untuk menganalisis strategi keamanan transaksi elektronik dalam e-government secara menyeluruh. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif dengan metode studi literatur (library research). Hasil penelitian menunjukkan bahwa keamanan transaksi elektronik dalam e-government didukung oleh penggunaan teknologi, mencakup penggunaan enkripsi, tanda tangan digital, Public Key Infrastructure (PKI), firewall, autentikasi biometrik, dan blockchain untuk memastikan kerahasiaan dan keandalan data. serta oleh regulasi yang kuat seperti UU ITE dan UU Perlindungan Data Pribadi. Selain itu, kesiapan sumber daya manusia, baik dari pemerintah maupun masyarakat, juga menjadi penentu keberhasilan, khususnya dalam hal literasi digital, pelatihan keamanan informasi, dan budaya kerja yang sadar risiko. Ketiga aspek tersebut saling melengkapi dalam membangun sistem keamanan yang andal.

Pendahuluan

Pesatnya Perkembangan teknologi informasi di era digital saat ini telah mendorong perubahan besar dalam berbagai bidang, termasuk pemerintahan. Konsep Electronic Government (e-government) muncul sebagai upaya strategis untuk membangun tata kelola pemerintahan yang lebih efektif, efisien, dan akuntabel, serta sebagai inovasi untuk menjawab tuntutan perubahan zaman terhadap pelayanan publik yang lebih cepat dan berbasis teknologi. Menurut Kristian et al., (2024) bahwa E- government tidak hanya sekadar digitalisasi administrasi, tetapi juga menjadi sarana penting dalam mendorong keterbukaan informasi, partisipasi publik, serta meningkatkan kepercayaan masyarakat terhadap pemerintah melalui penyediaan layanan yang lebih transparan, efisien, dan mudah diakses oleh seluruh lapisan masyarakat.

Dalam konteks pelayanan publik, kehadiran e-government semakin memperjelas peran pemerintah sebagai pelayan masyarakat. Muliawaty & Hendryawan (2020) Menjelaskan pendayagunaan e-government dalam pelayanan publik bertujuan untuk mempercepat proses pelayanan, meningkatkan koordinasi antar instansi, serta mendekatkan layanan kepada masyarakat. Pemanfaatan teknologi ini tidak hanya memperlancar hubungan antara pemerintah pusat dan daerah, tetapi juga memperkuat integrasi dengan masyarakat untuk mewujudkan prinsip *good governance*. Prinsip-prinsip *good governance* itu sendiri, yakni transparansi, akuntabilitas, keadilan, responsivitas, efisiensi, dan efektivitas, yang semuanya sangat relevan dalam membangun sistem pemerintahan modern berbasis teknologi. Namun, Joandani et al., (2019) berpendapat bahwa penerapan prinsip-prinsip tersebut dalam pelayanan e-government di Indonesia masih belum optimal. Salah satu upaya untuk memperbaiki implementasi adalah dengan memperkuat sistem dan kelembagaan berbasis peraturan perundang-undangan, serta memastikan pelaksanaannya berjalan konsisten di semua level pemerintahan melalui pengawasan dan evaluasi yang berkelanjutan.

Meski membawa banyak manfaat seperti kemudahan akses layanan dan percepatan administrasi, implementasi e-government juga dihadapkan pada berbagai tantangan. Seperti yang dikemukakan oleh Risnandar (2014) Yakni permasalahan utama yang dihadapi di antaranya adalah keterbatasan infrastruktur teknologi, kurangnya sumber daya manusia khusus di bidang IT, dan minimnya dukungan anggaran. Untuk mengatasinya, perlu dilakukan pengadaan sarana prasarana serta penguatan kapasitas teknis sumber daya manusia di instansi pemerintah, termasuk pelatihan intensif dan penyediaan perangkat kerja yang memadai. Selain hambatan teknis, Kurhayadi (2019) Menambahkan bahwa keberhasilan implementasi e-government di Indonesia juga dipengaruhi oleh budaya kerja birokrasi yang masih konvensional serta rendahnya literasi digital di kalangan masyarakat. Dalam praktiknya, layanan e-government sering kali hanya sebatas penyediaan informasi melalui situs resmi tanpa ada optimalisasi interaksi dan pelayanan publik berbasis teknologi yang partisipatif dan responsif. Perubahan paradigma birokrasi dan peningkatan kualitas pelayanan berbasis e-public menjadi syarat mutlak dalam mewujudkan e-government yang efektif dan berorientasi pada kebutuhan masyarakat digital saat ini.

Secara historis, pengembangan e-government di Indonesia sebetulnya telah melalui perjalanan panjang, dimulai sejak diterbitkannya Instruksi Presiden No. 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government. Seiring waktu, dengan bantuan teknologi seperti aplikasi Vos Viewer, dapat diketahui bahwa terminologi e-government, implementasi e-government, dan faktor keberhasilan menjadi fokus utama perkembangan di Indonesia. Keberhasilan implementasi e-government sangat bergantung pada kolaborasi aktif antara pemerintah dan masyarakat, sehingga partisipasi masyarakat harus terus didorong untuk memastikan keberlanjutan sistem ini, terutama melalui edukasi digital dan penguatan peran warga dalam proses pengambilan keputusan layanan publik berbasis teknologi. (Amrozi et al., 2022).

Seiring perkembangannya, layanan yang disediakan melalui sistem e-government semakin beragam. Indrajit (2016) dalam bukunya menjelaskan sedikitnya terdapat tiga bentuk utama layanan e-government yang dikembangkan, yaitu *publish*, *interact*, dan *transact*. Pelayanan *publish* merupakan tahapan paling dasar di mana pemerintah hanya menyediakan informasi kepada masyarakat secara satu arah, tanpa adanya interaksi. Informasi yang disajikan biasanya berupa berita, data statistik, regulasi, dan panduan layanan, yang dapat diakses dengan mudah melalui situs resmi atau aplikasi pemerintah. Ini menjadi fondasi awal bagi pemerintah dalam membangun transparansi kepada masyarakat.

Tahap berikutnya adalah *interact*, di mana terjadi komunikasi dua arah antara pemerintah dan masyarakat. Pada tahap ini, masyarakat tidak hanya menerima informasi, tetapi juga dapat berinteraksi aktif dengan pemerintah, misalnya melalui forum diskusi daring, layanan pengaduan, hingga penggunaan chatbot berbasis kecerdasan buatan untuk membantu penyelesaian kebutuhan informasi. Interaksi ini membuka peluang besar dalam memperkuat partisipasi masyarakat dalam proses pemerintahan.

Tahap yang ketiga adalah transact, yang merupakan tahap paling kompleks dalam implementasi e-government, yaitu tahap di mana layanan digital memungkinkan masyarakat untuk melakukan transaksi elektronik secara penuh dengan pemerintah. Transaksi ini mencakup berbagai aktivitas penting seperti pembayaran pajak, pendaftaran izin usaha, pengajuan klaim layanan publik, hingga penerbitan dokumen resmi dalam bentuk digital. Kompleksitas tahap ini tidak hanya terletak pada volume transaksi yang besar, tetapi juga pada tingginya tingkat sensitivitas data yang dipertukarkan dan nilai finansial yang terlibat dalam setiap transaksi. Karena melibatkan data pribadi, data keuangan, hingga dokumen legal yang bersifat rahasia, tahap transact membutuhkan sistem keamanan informasi yang sangat kuat. Sistem ini harus mampu melindungi seluruh proses transaksi dari berbagai ancaman seperti pencurian data, peretasan, manipulasi informasi, serta pelanggaran privasi. Tanpa adanya sistem keamanan yang handal, layanan transact dalam e-government berisiko mengalami kebocoran data, penyalahgunaan identitas, penyimpangan prosedur, hingga berkurangnya kepercayaan masyarakat terhadap layanan digital pemerintah (Sadar, 2023).

Sejumlah penelitian sebelumnya telah menyoroti pentingnya teknologi keamanan seperti enkripsi, tanda tangan digital, Public Key Infrastructure (PKI), firewall, dan autentikasi biometrik dalam melindungi transaksi elektronik. Namun, kajian tersebut umumnya masih terfokus pada aspek teknis atau aspek hukum secara parsial. Belum banyak penelitian yang membahas strategi keamanan transaksi elektronik secara komprehensif dengan mengintegrasikan pendekatan teknologi, regulasi, dan kesiapan sumber daya manusia sebagai satu kesatuan sistem keamanan yang berkelanjutan dalam e-government. Dengan kata lain, terdapat research gap pada kajian tentang bagaimana ketiga pilar tersebut saling melengkapi dan membentuk arsitektur keamanan transaksi yang menyeluruh.

Kesenjangan tersebut menegaskan urgensi untuk melakukan penelitian yang mampu mengkaji strategi keamanan transaksi elektronik secara holistik. Penguatan keamanan transaksi dalam e-government sangat penting bukan hanya untuk menjaga integritas dan kerahasiaan data, tetapi juga sebagai fondasi dalam membangun kepercayaan publik, memperluas adopsi layanan digital, serta memastikan keberlanjutan transformasi digital dalam pemerintahan. Dalam konteks meningkatnya ancaman siber dan semakin kompleksnya transaksi digital, kebutuhan terhadap strategi keamanan yang terintegrasi menjadi semakin mendesak. Oleh karena itu, artikel ini bertujuan untuk menganalisis dan menggali lebih dalam berbagai strategi keamanan yang dapat diterapkan guna menjaga keabsahan, integritas, kerahasiaan, serta keandalan transaksi elektronik dalam sistem e-government. Dengan membahas secara komprehensif berbagai pendekatan teknis, prosedural, dan kebijakan yang relevan, diharapkan artikel ini dapat memberikan gambaran menyeluruh mengenai upaya-upaya yang perlu dilakukan untuk memastikan setiap transaksi digital antara masyarakat dan pemerintah berlangsung dengan aman, transparan, dan terpercaya.

Kajian Literatur

E-Government dan Pelayanan Publik Elektronik

E-Government (SPBE atau Sistem Pemerintahan Berbasis Elektronik) didefinisikan sebagai pemanfaatan teknologi informasi dan komunikasi (TIK) oleh pemerintah untuk meningkatkan efisiensi, transparansi, dan aksesibilitas pelayanan publik (Djabbari et al., 2024; Nurfadillah et al., 2025). Widiyaningrum (2020) menyatakan bahwa “melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat”. Di sisi regulasi di Indonesia, peraturan penting adalah PP No. 82 Tahun 2012 mengenai penyelenggaraan sistem dan transaksi elektronik. Sebagaimana disebutkan dalam kajian, strategi e-government meliputi pengaturan interoperabilitas dan transaksi antar portal pemerintahan untuk mengamankan pertukaran informasi antar instansi (Nur, 2018).

Risiko dan Tantangan Keamanan dalam Transaksi Elektronik di E-Government

Salah satu tantangan utama dalam implementasi e-government adalah keamanan data dan transaksi elektronik. (Ibrahim et al., 2020) dalam kajian pustaka sistematis menyoroti bahwa sektor keamanan menjadi fokus kritis karena banyaknya informasi yang harus dikelola dengan tingkat sensitivitas yang cukup tinggi. Tantangan Keamanan dalam Transaksi Elektronik di E-Government salah satunya adalah aspek perlindungan data pribadi juga menjadi isu sentral. Iswandari (2021) menekankan bahwa data keamanan, yang bersifat privasi dari masyarakat, sangat penting dalam sistem e-government, dan kepercayaan publik akan sangat dipengaruhi oleh isu keamanan data. Selain itu, menurut Kurniawan, Simanjuntak and Limbong, (2022) digitalisasi pelayanan publik menghadapi masalah regulasi perlindungan data karena pengaturan yang berhubungan dengan perlindungan data pribadi saat ini di Indonesia sifatnya hanya parsial dan sektoral.

Strategi Keamanan dan Teknik Analisis

Dalam literatur keamanan sistem e-government, terdapat pendekatan teknis seperti penetration testing dan vulnerability assessment. Studi komparatif oleh (Kurniawan et al., 2022) membandingkan kedua teknik ini dalam konteks SPBE, menunjukkan bahwa kedua metode penting untuk mengevaluasi keamanan sistem informasi dan kerentanan sebelum diimplementasikan pada layanan publik. Selain itu, strategi keamanan yang lebih mutakhir melibatkan penggunaan teknologi blockchain. (Elisa et al., 2023) mengusulkan kerangka sistem e-government berbasis blockchain untuk menjamin integritas dan privasi data, serta mengurangi risiko single point of failure yang rentan terhadap serangan siber seperti DDoS. Dalam varian lain, konsorsium blockchain juga diusulkan sebagai solusi desentralisasi untuk menjaga keamanan dan kerahasiaan transaksi dalam sistem pemerintahan elektronik.

Kepatuhan Hukum dan Tata Kelola Data

Keamanan transaksi elektronik dalam e-government tidak hanya teknis, tetapi juga bersifat legal dan kebijakan. Keberadaan UU ITE (Undang-Undang No. 11 Tahun 2008) merupakan landasan hukum untuk transaksi elektronik di Indonesia dan memberikan payung legal bagi pengelolaan data publik dan

pribadi dalam e-government. Iswandari (2021) menunjukkan bahwa meskipun e-government berpotensi mendukung good governance, jika jaminan hukum terhadap data pribadi belum kuat, kepercayaan publik bisa terganggu. Selain itu, dari sudut kebijakan, Kurniawan, Simanjuntak and Limbong (2022) menekankan urgensi pengesahan RUU Perlindungan Data Pribadi sebagai bagian dari strategi keamanan dalam digitalisasi layanan publik.

Implikasi Kepercayaan Publik dan Adopsi Layanan

Keamanan transaksi elektronik sangat terkait dengan kepercayaan masyarakat terhadap e-government. Dalam studi budaya, Abunadi (2013) menunjukkan bahwa kepercayaan dalam internet sebagai media komunikasi dengan pemerintah adalah faktor signifikan yang mempengaruhi penerimaan transaksi elektronik (e-transactions) oleh warga. Lebih jauh, kualitas situs web e-government juga penting. Sebagai contoh, Alshehri et al. (2012) menggunakan model UTAUT (Unified Theory of Acceptance and Use of Technology) dan menemukan bahwa Website Quality memiliki dampak signifikan pada penerimaan layanan e-government oleh masyarakat.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur (library research). Pendekatan ini bertujuan untuk mendeskripsikan dan menganalisis berbagai konsep, teori, serta hasil penelitian terdahulu yang berkaitan dengan implementasi e-government dalam pelayanan publik, khususnya terkait upaya-upaya strategis dalam memperkuat keamanan transaksi elektronik antara pemerintah dan masyarakat. Sumber data dalam penelitian ini berasal dari literatur sekunder, yang meliputi artikel jurnal nasional, buku akademik, laporan penelitian, serta dokumen resmi pemerintah. Pemilihan sumber dilakukan berdasarkan kriteria relevansi terhadap topik pembahasan. Pengumpulan data dilakukan melalui penelusuran literatur dari berbagai database ilmiah seperti Google Scholar, ResearchGate, serta dari situs resmi lainnya. Data yang terkumpul kemudian dianalisis menggunakan teknik analisis isi, dengan mengidentifikasi tema-tema utama, mengklasifikasikan informasi berdasarkan fokus kajian, serta mensintesis hasil temuan untuk membangun argumentasi yang mendukung tujuan penulisan artikel ini.

Hasil dan Pembahasan

Dalam konteks pelayanan publik berbasis digital, transaksi elektronik antara pemerintah dan masyarakat telah menjadi bagian tak terpisahkan dari proses birokrasi modern. Berbagai jenis layanan publik kini dapat diakses secara daring, lebih dari itu berbagai jenis transaksi juga dapat dilakukan secara digital antara pemerintah dan masyarakat secara luas, contohnya seperti pembayaran pajak melalui e-billing, proses pengadaan barang dan jasa melalui e-procurement, pengurusan izin, dan verifikasi dokumen secara digital. Transformasi ini memperlihatkan arah perkembangan sistem pemerintahan menuju efisiensi dan kemudahan akses layanan yang tidak lagi terbatas ruang dan waktu, sekaligus mencerminkan pergeseran paradigma pelayanan publik ke arah sistem yang lebih cepat, transparan, dan berbasis teknologi. Di sisi lain, digitalisasi juga menghadirkan bentuk interaksi baru dalam ruang virtual yang sarat dengan

tantangan, khususnya dalam hal menjaga keandalan dan keamanan informasi yang dipertukarkan. Karena itu, isu keamanan dalam transaksi elektronik menjadi semakin vital untuk memastikan kepercayaan publik terhadap e-government tetap terjaga (Supriyanto, 2016).

Pentingnya perlindungan data dan transaksi dalam e-government tidak bisa diremehkan. Transaksi yang dilakukan melalui jaringan publik menghadirkan risiko kebocoran data, pemalsuan dokumen, hingga penyalahgunaan akses oleh pihak tidak berwenang. Vania et al., (2023) menjelaskan bahwa strategi keamanan tidak bisa dilepaskan dari regulasi yang mengatur perlindungan data dan transaksi digital. Di Indonesia, berbagai regulasi telah diterbitkan untuk mendukung keamanan dalam transaksi elektronik, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi (UU PDP) yang baru disahkan. Regulasi ini memberikan landasan hukum yang penting, menjadi pedoman dalam merancang sistem perlindungan data yang terstandar, serta mendorong akuntabilitas penyelenggara sistem elektronik.

Meskipun demikian, implementasinya masih menghadapi tantangan di lapangan. Ketimpangan antara norma yang diatur dan kapasitas lembaga pelaksana, termasuk sumber daya manusia, membuat sistem keamanan digital belum sepenuhnya efektif dan merata di seluruh instansi. Bahkan hingga kini, menurut Najwa, (2024) Lembaga Sertifikasi Keandalan (LSK) yang diamanatkan UU ITE masih belum terbentuk, padahal lembaga ini memiliki peran penting dalam memberikan jaminan keandalan atas transaksi elektronik. Tanpa lembaga tersebut, pengguna layanan digital tidak memiliki rujukan resmi dalam menilai tingkat keamanan sistem, yang pada akhirnya dapat menghambat kepercayaan dan adopsi publik terhadap layanan digital pemerintah.

Aspek hukum lainnya yang cukup krusial adalah kejelasan status dokumen digital di mata hukum. Dalam beberapa kasus, perbedaan tafsir antara UU ITE dan KUH Perdata menimbulkan ketidakpastian hukum, khususnya terkait pembuktian sah dokumen elektronik di pengadilan. Ketidakjelasan ini dapat memperlemah posisi hukum dalam sengketa digital dan menghambat proses hukum secara keseluruhan. Hal ini mencerminkan bahwa selain memperkuat infrastruktur digital, pemerintah juga perlu menyelaraskan seluruh aturan agar tidak terjadi tumpang tindih atau kekosongan hukum yang bisa dimanfaatkan oleh pelaku kejahatan digital. Dalam kondisi ini, kejelasan legalitas tidak hanya berdampak pada penegakan hukum, tetapi juga pada tingkat adopsi teknologi oleh pengguna layanan. Ketika hukum masih bersifat ambigu, masyarakat dan pelaku usaha cenderung enggan menggunakan layanan digital secara maksimal (Siburian, 2021).

Selain dari segi regulasi dan kebijakan oleh pemerintah, Strategi yang tak kalah penting dalam keamanan transaksi dalam pelayanan public adalah penggunaan teknologi yang tepat. Dari sisi teknologi, mencakup berbagai pendekatan yang komprehensif. Dalam penelitian yang dilakukan oleh Izzah & Sugandha (2021) Menyebutkan bahwa salah satu bentuk perlindungan yang dapat dilakukan yakni penggunaan tanda tangan elektronik yaitu sebagai alat

validasi yang kuat terhadap keaslian dokumen digital, memberikan jaminan otentikasi serta integritas dokumen yang ditandatangani secara sah. Penggunaan tanda tangan elektronik yang tersertifikasi memungkinkan proses administrasi berjalan dengan lebih aman, karena hanya pihak berwenang yang dapat menandatangani dokumen, dengan rekam jejak digital yang tidak dapat dimanipulasi serta dapat dilacak secara transparan. Tanda tangan digital yang didukung oleh sertifikat elektronik juga memungkinkan efisiensi dalam pengesahan dokumen lintas instansi tanpa memerlukan kehadiran fisik, sehingga mempercepat pelayanan publik. Ini membuktikan bahwa keamanan digital bukan hanya isu teknis, tetapi juga berkaitan erat dengan legalitas dan kepercayaan dalam proses pemerintahan.

Salah satu model yang juga dianggap efektif adalah konsep pertahanan berlapis atau *defense in depth*, yang mencakup perlindungan dari sisi jaringan, aplikasi, perangkat keras, serta kebijakan internal dan pelatihan SDM. Teknologi seperti firewall, enkripsi data, VPN, autentikasi biometrik, hingga sistem monitoring akses berbasis log file, menjadi bagian penting dalam sistem pertahanan ini. Pendekatan berlapis memungkinkan deteksi dini dan mitigasi risiko yang lebih baik, karena celah keamanan tidak hanya bergantung pada satu titik proteksi. Dengan adanya beberapa lapisan pengamanan, serangan siber yang berhasil menembus satu lapisan masih dapat ditahan oleh lapisan lainnya. Hal ini memberikan waktu lebih bagi tim keamanan untuk merespons, sekaligus meningkatkan ketahanan sistem terhadap berbagai bentuk ancaman yang terus berkembang. (Novianto, 2020).

Untuk melindungi data yang sensitif, Feriyanto (2024) Menjelaskan bahwa teknologi kriptografi berbasis *Public Key Infrastructure* (PKI) patut digunakan. Dengan sistem ini, hanya pengguna yang memiliki kunci privat yang dapat membuka informasi yang dienkripsi, memastikan bahwa data tidak dapat diakses oleh pihak lain selama proses. Sertifikat digital dan algoritma tanda tangan digital juga memberikan verifikasi identitas terhadap pihak-pihak yang terlibat dalam transaksi, serta memastikan integritas pesan tetap utuh selama proses transmisi data. Dalam konteks layanan publik, hal ini sangat penting untuk menghindari pemalsuan identitas maupun duplikasi layanan yang dapat merugikan masyarakat maupun pemerintah. Pemerintah juga telah mulai menggunakan protokol keamanan seperti *Secure Socket Layer* (SSL) untuk melindungi komunikasi data di situs resmi pelayanan publik.

Bentuk teknologi lainnya ialah sistem *blockchain*, yang mulai diperkenalkan sebagai teknologi pendukung keamanan dalam sistem e-government. Dengan kemampuan menyimpan data secara terdistribusi dan tidak dapat diubah, *blockchain* dipercaya mampu mengurangi risiko manipulasi serta meningkatkan transparansi dalam transaksi digital. Teknologi ini juga memungkinkan pencatatan yang bersifat permanen dan terverifikasi secara otomatis oleh sistem. Beberapa inisiatif awal telah dilakukan, seperti verifikasi sertifikat pendidikan dan pencatatan data medis yang lebih aman berkat penerapan *blockchain*, terutama karena setiap perubahan data dapat dilacak secara akurat melalui jejak digital yang terenkripsi. Suryawijaya (2023) menjelaskan bahwa sistem ini memungkinkan adanya jejak digital permanen atas semua perubahan data, yang

hanya bisa dilakukan berdasarkan konsensus, sehingga keabsahan dan integritas informasi lebih terjamin. Namun demikian, penggunaan *blockchain* juga menuntut pengembangan kapasitas SDM yang memahami cara kerja dan risikonya, karena teknologi ini relatif baru dan kompleks, serta memerlukan pemahaman teknis yang mendalam, termasuk pengelolaan infrastruktur, keamanan kriptografi, dan pengambilan keputusan berbasis algoritma konsensus yang tidak lazim digunakan dalam sistem tradisional.

Selain dari segi regulasi dan penerapan beberapa teknologi, faktor manusia juga menjadi kunci keberhasilan strategi keamanan transaksi elektronik dalam e-government. Karena tidak cukup hanya dengan membangun sistem yang canggih; aparatur sipil negara harus dilatih secara berkala dalam hal literasi digital dan pemahaman terhadap prosedur keamanan informasi. Pelatihan ini penting untuk membentuk pola pikir yang tanggap terhadap ancaman siber dan meningkatkan kedisiplinan dalam pengelolaan data sensitif. Penelitian yang dilakukan oleh (Supriyanto, 2016) menunjukkan bahwa SDM yang sadar akan pentingnya privasi dan keamanan informasi dapat mencegah kebocoran data sejak awal, karena sebagian besar insiden keamanan berasal dari kesalahan manusia, baik disengaja maupun tidak. Oleh karena itu, pendekatan keamanan tidak bisa bersifat parsial, melainkan harus menyeluruh dari sisi teknis, regulatif, dan kapasitas organisasi. Program pelatihan yang berkesinambungan serta insentif terhadap kepatuhan keamanan informasi harus menjadi bagian dari strategi keamanan nasional, termasuk pengawasan rutin dan evaluasi terhadap penerapan standar operasional di setiap instansi pemerintah.

Namun, meskipun berbagai strategi telah dijalankan, evaluasi terhadap keberhasilan implementasi menunjukkan bahwa masih terdapat sejumlah tantangan besar. Keterbatasan sumber daya, rendahnya literasi digital masyarakat, serta kurangnya koordinasi antar instansi sering kali menyebabkan kebijakan tidak berjalan secara konsisten dan berkelanjutan. Selain itu, keberhasilan strategi keamanan juga sangat tergantung pada kemauan politik dan komitmen pemimpin institusi dalam menjadikan keamanan sebagai prioritas dalam pelayanan publik, termasuk dalam hal alokasi anggaran, penegakan regulasi internal, serta dukungan terhadap inovasi teknologi keamanan yang terus berkembang di era digital saat ini. (Effendy & Oktiani, 2024).

Dalam beberapa kasus, pemerintah daerah yang menerapkan sistem digital secara menyeluruh telah menunjukkan hasil positif, terutama dalam efisiensi pelayanan, pengurangan waktu tunggu, dan meningkatnya kepercayaan masyarakat. Namun, menurut Sihotang & Hoessein, (2025) keberhasilan ini belum terjadi secara merata, sehingga perlu adanya kebijakan nasional yang lebih tegas dan dukungan anggaran yang cukup untuk memperluas praktik baik ini ke seluruh daerah. Pemerintah pusat juga harus memastikan adanya pendampingan teknis dan standarisasi sistem untuk menjaga kualitas layanan digital di semua wilayah. Di sisi lain, tantangan eksternal seperti serangan siber dari pihak luar juga mengharuskan sistem keamanan digital terus diperbarui sesuai dengan ancaman yang berkembang dari waktu ke waktu. Hal ini menuntut pembaruan kebijakan dan peningkatan kapasitas teknis secara berkelanjutan agar sistem tetap tangguh dan adaptif.

lebih lanjut, tantangan infrastruktur juga menjadi penghambat utama dalam penerapan keamanan transaksi elektronik di Indonesia. Keterbatasan akses internet di wilayah-wilayah tertentu, khususnya daerah terpencil, serta kurangnya perangkat teknologi yang memadai di beberapa instansi pemerintah menyebabkan ketimpangan dalam penerapan layanan e-government. Ketimpangan ini berdampak langsung pada kualitas dan keamanan sistem, karena daerah dengan infrastruktur yang terbatas cenderung tidak memiliki perlindungan digital yang optimal. Risiko kebocoran data, kegagalan sistem, hingga penyalahgunaan informasi menjadi lebih tinggi pada wilayah yang tidak memiliki sarana dan prasarana pendukung yang memadai. Oleh karena itu, pembangunan infrastruktur digital secara merata harus menjadi agenda prioritas pemerintah, agar sistem keamanan transaksi elektronik dapat diterapkan secara konsisten di seluruh daerah, tanpa meninggalkan wilayah yang tertinggal secara teknologi (Lestari et al., 2021).

Untuk itu, Saputra et al., (2019) merekomendasikan percepatan pembentukan lembaga pelaksana keamanan digital seperti LSK, peningkatan kerja sama lintas sektor antara pemerintah dan pihak swasta dalam membangun ekosistem keamanan digital nasional, serta peningkatan literasi digital masyarakat secara menyeluruh. Pemerintah juga perlu lebih aktif dalam mengembangkan sistem otentikasi yang kuat serta memastikan setiap data yang dikumpulkan dan disimpan mendapat perlindungan maksimal sesuai ketentuan perundang-undangan. Terakhir, dibutuhkan pemantauan dan evaluasi secara berkala terhadap semua sistem digital yang digunakan dalam layanan publik, agar potensi kerentanan bisa dideteksi sejak dini dan segera diatasi sebelum berkembang menjadi ancaman serius yang dapat mengganggu integritas dan keandalan pelayanan kepada masyarakat (Savitri et al., 2024).

Dengan strategi yang tepat, sistem transaksi elektronik dalam pelayanan publik berbasis e-government dapat menjadi pilar utama menuju pemerintahan yang lebih transparan, efisien, dan aman secara digital. Namun, keamanan transaksi elektronik dalam e-government bukan sekadar persoalan teknis atau administratif, melainkan menyangkut keberlanjutan kepercayaan antara pemerintah dan masyarakat di era digital. Untuk itu, pendekatan yang komprehensif yang mencakup regulasi yang kuat, teknologi yang andal, dan kesiapan sumber daya manusia harus menjadi prioritas utama. Tanpa komitmen dan kolaborasi lintas sektor yang berkelanjutan, potensi digitalisasi justru bisa berubah menjadi risiko yang dapat merugikan berbagai pihak. Setiap inovasi layanan publik berbasis elektronik harus dirancang dengan perspektif keamanan yang memadai. Keamanan yang terjaga menjadi kunci agar e-government dapat tumbuh secara berkelanjutan.

Kesimpulan

Strategi keamanan transaksi elektronik dalam pelayanan publik berbasis e-government harus mencakup tiga pilar utama: teknologi, regulasi, dan sumber daya manusia. Dari sisi teknologi, strategi mencakup penggunaan enkripsi, tanda tangan digital, Public Key Infrastructure (PKI), firewall, autentikasi biometrik, dan blockchain untuk memastikan kerahasiaan dan keandalan data. Dari aspek regulasi, keberadaan UU ITE, UU Perlindungan Data Pribadi, serta PP No. 71

Tahun 2019 menjadi dasar hukum penting. Namun, implementasi masih menghadapi tantangan seperti belum terbentuknya Lembaga Sertifikasi Keandalan (LSK) dan belum sinkronnya beberapa aturan. Sementara dari aspek sumber daya manusia, peningkatan literasi digital, pelatihan keamanan informasi, dan budaya sadar risiko menjadi kunci keberhasilan pelaksanaan strategi keamanan. Dengan mengintegrasikan ketiga aspek tersebut secara berkelanjutan, e-government dapat berkembang menjadi sistem pelayanan publik yang tidak hanya efisien dan transparan, tetapi juga aman dan terpercaya. Keamanan transaksi elektronik adalah kunci utama untuk menjaga kepercayaan publik serta keberlanjutan transformasi digital dalam tata kelola pemerintahan modern.

Referensi

- Abunadi, I. (2013). Influence of Culture on e-Government Acceptance in Saudi Arabia. *Computers and Society*.
<https://api.semanticscholar.org/CorpusID:60893292>
- Alshehri, M., Drew, S., Alhussain, T., & AlGhamdi, R. (2012). The Effects of Website Quality on Adoption of E-Government Service: An Empirical Study Applying UTAUT Model Using SEM. *ArXiv*, *abs/1211.2410*.
<https://api.semanticscholar.org/CorpusID:11731551>
- Amrozi, Y., Aini, N., & Munadhiroh, Z. (2022). Peta Perkembangan E-Government di Indonesia. *JSI: Jurnal Sistem Informasi (E-Journal)*, *14*(1), 2465-2472.
<https://doi.org/10.18495/jsi.v14i1.16635>
- Djabbari, M. H., B., I., Nugroho, T. C., Amiruddin, I., & Yanto, E. (2024). Implementasi E-Government dalam Pelayanan Publik Berbasis Website di Desa Tondowolio Kabupaten Kolaka. *Kolaborasi: Jurnal Administrasi Publik*, *10*(2), 1-10. <https://doi.org/https://doi.org/10.26618/kjap.v10i2.15588>
- Effendy, M. Y., & Oktiani, H. (2024). Literasi digital keamanan siber pada remaja menghadapi social engineering. *Jurnal Wacana Publik*, *18*(01), 35-42.
- Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005-1015. <https://doi.org/10.1007/s11276-018-1883-0>
- Feriyanto, O. (2024). Kemudahan dan keamanan transaksi e-commerce dan inovasi pembayaran digital. *Jurnal Star*, *XXI*(1), 24-32.
- Ibrahim, A., Arie, A., & Abdullah, S. Do. (2020). KEAMANAN UNTUK PENERAPAN LAYANAN PUBLIK PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE): SEBUAH KAJIAN PUSTAKA SISTEMATIS. *Indonesian Journal on Information System*, *5*(2), 135-143.
<https://doi.org/https://doi.org/10.36549/ijis.v5i2.105>
- Indrajit, R. E. (2016). Konsep dan Strategi Electronic Government. In *Electronic Government*. Andi Yogyakarta.

- Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. *Jurnal Hukum IUS QUIA IUSTUM*, 28(1), 115-138. <https://doi.org/10.20885/iustum.vol28.iss1.art6>
- Izzah, A. N. El, & Sugandha, W. (2021). Penggunaan Tanda Tangan Elektronik Dalam Penyelenggaraan E-Government Guna Mewujudkan Pelayanan Publik Yang Efisien. *Journal of Law, Society, and Islamic Civilization*, 9(1), 1-9. <https://doi.org/10.20961/jolsic.v9i1.52836>
- Joandani, G. K., Pribadi, R., & Suryono, C. A. (2019). Kajian Potensi Pengembangan Ekowisata Sebagai Upaya Konservasi Mangrove Di Desa Pasar Banggi , Kabupaten Rembang. *OF MARINE RESEARCH*, 8(1), 117-126.
- Kristian, I., Nuradhawati, R., & Ristala, H. (2024). Jurnal academia praja. *Jurnal Academia Praja*, 7(2), 252-263.
- Kurhayadi. (2019). Dampak Sistem E-Government Terhadap Kualitas Pelayanan Publik Di Indonesia. *AKSELERASI: Jurnal Ilmiah Nasional*, 1(3), 25-34. <https://doi.org/10.54783/jin.v1i3.549>
- Kurniawan, T., Simanjuntak, N. C., & Limbong, S. U. (2022). Urgensi Pengesahan Rancangan Undang- Undang Perlindungan Data Pribadi Dalam Digitalisasi Pelayanan Publik Guna Mewujudkan Smart Government. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 2(2), 265-281. <https://doi.org/https://doi.org/10.15294/ipmhi.v2i2.55032>
- Lestari, P. A., Tasyah, A., Syofira, A., Rahmayani, C. A., Cahyani, R. D., & Tresiana, N. (2021). *Inovasi Pelayanan Publik Berbasis Digital (E-Government) Di Era Pandemi Covid-19*. Jurnal Ilmu Administrasi: Media Pengembangan Ilmu dan Praktek Administrasi. <https://jia.stialanbandung.ac.id/index.php/jia/article/view/808/>
- Muliawaty, L., & Hendryawan, S. (2020). Peranan e-government dalam pelayanan publik (studi kasus: Mal pelayanan publik Kabupaten Sumedang). *Jurnal Ilmu Administrasi*, 11(2), 101-112.
- Novianto, F. (2020). Evaluation of E-Government Information Security Using the Defense in Depth Model. *Cyber Security Dan Forensik Digital*, 3(1), 14-19. <https://doi.org/10.14421/csecurity.2020.3.1.1962>
- Nur, E. (2018). PENERAPAN E-GOVERNMENT PUBLIK PADA SETIAP SKPD BERBASIS PELAYANAN DI KOTA PALU. *Jurnal Penelitian Komunikasi Dan Opini Publik*, 18(3), 265-280. <https://doi.org/https://doi.org/10.33299/jpkop.18.3.331>
- Nurfadillah, A., Nursamsir, & Mardiana. (2025). Penerapan E-Government pada Sektor Pelayanan Publik (Studi Kasus Aplikasi OpenSID di Desa Tondowolio Kecamatan Tanggetada Kabupaten Kolaka). *PENA BANGSA: BISNIS DAN TATA KELOLA PUBLIK ADAPTIF*, 1(1), 1-14.

<https://doi.org/10.69616/pb.v1i1.256>

- Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, 2(1), 8-16. <https://doi.org/10.32520/albahts.v2i1.3044>
- Risnandar. (2014). ANALISIS E-GOVERNMENT DALAM PENINGKATAN PELAYANAN PUBLIK PADA DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI SULAWESI TENGAH. *Katalogis*, 2(7), 192-199.
- Sadar. (2023). *E-GOVERNMENT (KONSEP, IMPLEMENTASI DAN EVALUASI E-GOVERNMENT DI INDONESIA)*.
- Saputra, S. L., Gultom, E., & Suwandono, A. (2019). Eksistensi Lembaga Sertifikasi Keandalan Untuk Mendukung Kegiatan E-Commerce Dalam Menghadapi Era Industri 4.0 Ditinjau Dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan Dan Ke-PPAT-An*, 2(2), 200-212. <https://doi.org/10.24198/acta.v2i2.238>
- Savitri, A. S., Hukum, F., Udayana, U., Eka, A. A. I., Yanti, K., Hukum, F., & Udayana, U. (2024). KEAMANAN DATA TRANSAKSI ELEKTRONIK DALAM KONTEKS BISNIS DIGITAL. *Jurnal Kertha Wicara*, 14(01), 11-18.
- Siburian, H. K. (2021). Legalitas Tanda Tangan Elektronik Dalam Perjanjian Jual Beli Lewat Media Internet (E-Commerce) Ditinjau Dari Undang - Undang Nomor. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Judge : Jurnal Hukum*, 2(02), 24-31. <https://doi.org/10.54209/judge.v2i02.60>
- Sihotang, M., & Hoessein, Z. A. (2025). Transformasi Politik Hukum dalam Penguatan Regulasi Cyber Law di Indonesia. *Jurnal Syntax Admiration*, 6(1), 586-596.
- Supriyanto, E. E. (2016). Kebijakan Inovasi Teknologi Informasi (IT) Melalui Program Elektronik Government dalam Meningkatkan Kualitas Pelayanan Publik di Indonesia. *Jurnal Ilmu Pemerintahan : Kajian Ilmu Pemerintahan Dan Politik Daerah*, 1(1), 141-161. <https://doi.org/10.24905/jip.v1i1.438>
- Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55-68. <https://doi.org/10.21787/jskp.2.2023.55-68>
- Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654-666. <https://doi.org/10.58344/jmi.v2i3.157>
- Widiyaningrum, W. Y. (2020). KAJIAN TEORITIS : STRATEGI PENGEMBANGAN E-GOVERNMENT DALAM PELAYANAN ADMINISTRASI. *PAJOUL (Pakuan*

Justice Journal Of Law, 1(2), 18-33.
<https://doi.org/https://doi.org/10.33751/pajoul.v1i2.2879>