(2025), 3 (7): 403–414 **Scientica** 3021-8209

Jurnal Ilmiah Sains dan Teknologi

Aspek Keamanan Sistem Informasi Digital dalam Pelayanan Perizinan Berbasis Online Single Submission (OSS) pada Instansi Pemerintahan

Tengku Maura Safa Ramadhanti, Muhammad Raihan, Muhammad Rizky Ramadhandi, Fazri Fadhilah Tambunan
Universitas Islam Negeri Sumatera Utara
mauradhanti@gmail.com,rayhanmhd654@gmail.com, dhandisecond@gmail.com, fazrifadhilah21@gmail.com

Abstract (English)

The digital transformation of public services has encouraged the implementation of the Online Single Submission (OSS) system as a primary platform for licensing services in government institutions. OSS aims to improve efficiency, transparency, and ease of access for licensing services for the public and business actors. However, the adoption of digital systems also presents significant challenges related to information system security, particularly data protection, system reliability, and public trust. This study aims to analyze the aspects of digital information system security in OSS-based licensing services within government institutions. The research employs a qualitative approach using a literature review method by examining scientific journals, books, regulations, and official documents relevant to information system security and e-government implementation. The findings indicate that OSS information system security is influenced by information security policies, access control mechanisms, personal data protection, human resource competencies, and technological infrastructure support. Furthermore, risks such as data breaches and unauthorized access may hinder public trust in OSS services. Therefore, strengthening information security governance is essential to ensure the sustainability and reliability of digital licensing services.

Article History
Submitted: 20 December 2025
Accepted: 29 December 2025
Published: 30 December 2025

Key Words
Information system security, OSS, licensing services, e-government, literature review

Abstrak (Indonesia)

Transformasi pelayanan publik melalui sistem informasi digital mendorong penerapan Online Single Submission (OSS) sebagai platform pelayanan perizinan pada instansi pemerintahan. OSS bertujuan meningkatkan efisiensi, transparansi, dan kemudahan akses layanan perizinan bagi masyarakat dan pelaku usaha. Namun, implementasi sistem digital ini juga menghadirkan tantangan terkait keamanan sistem informasi, terutama perlindungan data pribadi, keandalan sistem, serta kepercayaan publik. Penelitian ini bertujuan untuk menganalisis aspek keamanan sistem informasi digital dalam pelayanan perizinan berbasis OSS pada instansi pemerintahan. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan studi literatur, melalui penelaahan jurnal ilmiah, buku, peraturan perundang-undangan, dan dokumen resmi yang relevan. Hasil kajian menunjukkan bahwa keamanan sistem informasi OSS dipengaruhi oleh kebijakan keamanan informasi, pengendalian akses, perlindungan data pribadi, kompetensi sumber daya manusia, dan dukungan infrastruktur teknologi. Selain itu, risiko kebocoran data dan akses tidak sah berpotensi menghambat kepercayaan publik terhadap layanan OSS. Oleh karena itu, penguatan tata kelola keamanan sistem informasi diperlukan untuk menjamin keberlanjutan dan keandalan pelayanan perizinan digital.

Sejarah Artikel
Submitted: 20 December 2025
Accepted: 29 December 2025
Published: 30 December 2025

Kata Kunci
Keamanan sistem informasi, OSS, pelayanan perizinan, e-government, studi literatur

Latar Belakang

Perkembangan teknologi informasi telah mendorong transformasi pelayanan publik di berbagai instansi pemerintahan melalui penerapan sistem E-Government, termasuk dalam proses pelayanan perizinan usaha. Sistem Online Single Submission (OSS) menjadi platform utama dalam penyelenggaraan perizinan berbasis digital di Indonesia, yang dirancang untuk menyederhanakan proses, meningkatkan efisiensi, transparansi, serta

mempercepat waktu penyelesaian izin melalui integrasi semua layanan perizinan dalam satu sistem elektronik terpusat. OSS mengubah mekanisme layanan perizinan yang sebelumnya manual menjadi digital, sehingga memungkinkan pelaku usaha untuk mengajukan permohonan perizinan secara daring tanpa harus datang langsung ke kantor Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (DPMPTSP) setempat. Penelitian sebelumnya menunjukkan bahwa implementasi OSS berdampak positif terhadap percepatan dan kualitas layanan perizinan di berbagai daerah, meskipun terdapat tantangan pada aspek sosialisasi dan infrastruktur teknologi[1].

Namun, seiring dengan peningkatan penggunaan layanan perizinan digital, muncul pula tantangan baru di bidang keamanan sistem informasi. Sistem OSS yang bersifat daring dan terintegrasi rentan terhadap ancaman keamanan informasi seperti akses tidak sah, kebocoran data pribadi, serta serangan siber jika tidak dilengkapi dengan mekanisme proteksi yang memadai. Keamanan sistem informasi dalam konteks E-Government tidak hanya mencakup aspek teknis seperti enkripsi dan kontrol akses, tetapi juga aspek manajemen risiko, kesadaran pengguna, serta kebijakan tata kelola keamanan data. Penelitian mengenai keamanan informasi pada e-government menunjukkan bahwa sektor ini sering kali menghadapi ancaman serangan seperti phishing, DDoS, dan ransomware yang dapat mengganggu ketersediaan layanan publik jika mitigasi yang tepat tidak diterapkan[2].

OSS memfasilitasi pertukaran data sensitif antara pemerintah dan pengguna layanan, termasuk informasi identitas pelaku usaha dan dokumen penting perizinan. Ketidakmampuan sistem dalam menjamin kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data dapat menurunkan kepercayaan publik dan mengganggu kelancaran proses layanan perizinan. Karena itu, aspek keamanan sistem informasi digital menjadi faktor kritis yang harus diperhatikan dalam penelitian maupun praktik pelayanan perizinan berbasis OSS untuk melindungi data dan meningkatkan kepercayaan stakeholder terhadap layanan digital pemerintah. Kajian keamanan sistem informasi ini menjadi penting untuk mengidentifikasi dan memetakan berbagai risiko potensial yang dapat mengancam data dan layanan perizinan digital. Melalui kajian tersebut, dapat dirumuskan strategi perlindungan yang efektif dan berkelanjutan dalam penerapan OSS pada DPMPTS di berbagai daerah, guna menjamin keamanan, keandalan, serta kepercayaan masyarakat terhadap layanan perizinan elektronik[3].

Kajian Teori

1. Sistem Informasi Digital dan Pelayanan Publik

Transformasi digital dalam pelayanan publik merupakan langkah strategis pemerintah untuk menjawab tuntutan masyarakat akan layanan yang cepat, transparan, dan akuntabel. Salah satu wujud nyata dari transformasi ini adalah penerapan sistem informasi digital dalam bidang perizinan, seperti Online Single Submission (OSS)**.** Kehadiran OSS menjadi bagian penting dari implementasi e-Government yang bertujuan menyederhanakan proses perizinan usaha yang sebelumnya bersifat manual, berbelit, dan memakan waktu lama.

[1] Dewi, R., Priyanti, H., Aisyah, T., & Hasyem, M. (2025). Implementasi e-Government berbasis Online Single Submission (OSS) dalam upaya meningkatkan kualitas layanan publik digital. Jurnal Pemerintahan dan Politik, 10(3), 579–593.

[2] Novianto, F. (2023). Analisis keamanan informasi pada e-government menggunakan COBIT 5 framework. CyberSecurity dan Forensik Digital, 6(1).

[3] Syahfitra, A. (2020). E-Government dalam pelaksanaan One Stop Service (OSS). Jurnal Administrasi dan Sains Pemerintahan.

OSS dirancang sebagai sistem perizinan terintegrasi yang memungkinkan pelaku usaha mengajukan berbagai izin secara elektronik melalui satu platform. Dengan sistem ini, masyarakat tidak lagi harus mendatangi banyak instansi secara langsung, karena proses pengajuan, verifikasi, hingga penerbitan izin dapat dilakukan secara daring. Hal ini secara signifikan meningkatkan efisiensi pelayanan publik, baik dari sisi waktu, biaya, maupun tenaga, sekaligus meminimalkan potensi praktik maladministrasi.

Selain efisiensi, OSS juga mendorong transparansi dan akuntabilitas dalam penyelenggaraan pelayanan publik. Setiap tahapan perizinan dapat dipantau secara real time oleh pemohon, sehingga mengurangi ketidakpastian informasi. Pemerintah pun memiliki rekam jejak digital yang jelas terkait proses pengambilan keputusan, yang dapat digunakan sebagai dasar evaluasi dan pengawasan. Dengan demikian, OSS tidak hanya berfungsi sebagai alat pelayanan, tetapi juga sebagai instrumen tata kelola pemerintahan yang lebih baik.

Penerapan OSS mensyaratkan pengelolaan data yang terstruktur dan terotomatisasi. Sistem ini mengelola berbagai jenis data, mulai dari data permohonan izin, database pelaku usaha, hingga integrasi data antar kementerian dan lembaga. Interoperabilitas antar instansi menjadi kunci utama agar pertukaran data dapat berjalan efektif dan akurat. Jika dikelola dengan baik, OSS berpotensi besar mendukung iklim investasi, meningkatkan kepercayaan publik, serta memperkuat kualitas pelayanan publik di era digital[4]. Pengertian dan Dimensi Keamanan Sistem Informasi Keamanan sistem informasi merupakan aspek fundamental dalam penyelenggaraan layanan publik berbasis digital, khususnya pada layanan perizinan elektronik. Secara konseptual, keamanan sistem informasi didefinisikan sebagai kemampuan sistem dalam melindungi confidentiality, integrity, dan availability yang dikenal sebagai CIA Triad. Confidentiality menekankan perlindungan data agar hanya dapat diakses oleh pihak yang berwenang, integrity memastikan keutuhan dan keakuratan data tetap terjaga, sedangkan availability menjamin sistem dan layanan dapat diakses kapan pun dibutuhkan oleh pengguna. Ketiga elemen ini menjadi dasar utama dalam membangun sistem informasi yang andal dan terpercaya.

2. Pengertian dan Dimensi Keamanan Sistem Informasi

Dalam konteks layanan perizinan digital, keamanan informasi memiliki peran yang sangat krusial karena sistem mengelola data sensitif, seperti identitas pelaku usaha, data usaha, serta dokumen legal. Ancaman terhadap sistem dapat berasal dari faktor internal, seperti kelalaian pengguna atau penyalahgunaan akses oleh pihak berwenang, maupun faktor eksternal, seperti serangan siber, peretasan, dan malware. Oleh karena itu, penerapan keamanan sistem informasi tidak dapat hanya bergantung pada teknologi semata.

Aspek teknis keamanan, seperti penggunaan enkripsi untuk melindungi data, firewall untuk membatasi lalu lintas jaringan, serta kontrol akses berbasis hak pengguna, merupakan lapisan penting dalam melindungi sistem. Namun, teknologi tersebut harus didukung oleh aspek non-teknis yang mencakup kebijakan keamanan informasi, standar operasional prosedur, dan tata kelola organisasi yang jelas. Kebijakan keamanan berfungsi sebagai pedoman bagi seluruh pemangku kepentingan dalam mengelola dan menggunakan sistem, sementara prosedur yang terstandar membantu meminimalkan risiko kesalahan manusia.

Selain itu, tata kelola organisasi yang baik diperlukan untuk memastikan adanya pembagian peran dan tanggung jawab yang jelas dalam pengelolaan keamanan sistem. Dengan mengintegrasikan aspek teknologi, manajemen, dan tata kelola, keamanan sistem

[4] Sari, C. F., & Rahayu, S. A. P. (2025). Analisis Penerapan OSS Berbasis Risiko dalam Mewujudkan Kepastian Hukum bagi Investor di Indonesia. JURNAL ILMIAH NUSANTARA, 2(3), 577-591.

informasi dalam layanan perizinan digital dapat terjaga secara optimal. Hal ini pada akhirnya akan meningkatkan kepercayaan publik terhadap layanan digital pemerintah serta mendukung keberlanjutan transformasi digital dalam pelayanan publik[5]. Beberapa dimensi utama aspek keamanan sistem informasi:

1. Kerahasiaan (Confidentiality): Menjamin bahwa data sensitif (mis. data pemohon perizinan) hanya dapat diakses oleh pihak berwenang.
2. Integritas (Integrity): Menjamin bahwa data tidak berubah secara tidak sah selama penyimpanan atau transmisi.
3. Ketersediaan (Availability): Menjamin bahwa sistem informasi OSS selalu dapat diakses oleh pengguna ketika diperlukan.

Konsep ini penting untuk menjamin bahwa layanan OSS tidak hanya berorientasi pada kecepatan proses, tetapi juga mampu memberikan tingkat keamanan dan kepercayaan yang tinggi bagi seluruh stakeholder, termasuk pemerintah, pelaku usaha, dan masyarakat sebagai pengguna layanan.

3. Keamanan dalam E-Government dan Layanan Publik Digital

Dalam konteks pelayanan publik digital, keamanan sistem informasi tidak dapat dipisahkan dari konsep tata kelola pemerintahan yang baik (good governance). Penerapan e-government melalui sistem seperti Online Single Submission (OSS) menempatkan teknologi informasi sebagai tulang punggung layanan publik, sehingga setiap gangguan atau kelemahan keamanan akan berdampak langsung pada kualitas layanan yang diterima masyarakat. Keamanan sistem informasi berfungsi sebagai fondasi yang menjamin bahwa proses digitalisasi pelayanan publik berjalan sesuai dengan prinsip transparansi, akuntabilitas, dan perlindungan hak pengguna.

Kepercayaan pengguna menjadi faktor kunci dalam keberhasilan layanan e-government. Masyarakat dan pelaku usaha hanya akan memanfaatkan layanan perizinan berbasis OSS apabila mereka meyakini bahwa data pribadi dan informasi usaha yang disampaikan dikelola secara aman dan tidak disalahgunakan. Apabila terjadi insiden keamanan, seperti kebocoran data atau penyalahgunaan akses, tingkat kepercayaan publik terhadap instansi pemerintah dapat menurun secara signifikan. Kondisi ini berpotensi menghambat adopsi layanan digital dan mendorong pengguna kembali ke mekanisme pelayanan konvensional yang dianggap lebih aman, meskipun kurang efisien.

Selain aspek kepercayaan, keamanan sistem informasi juga berpengaruh terhadap keberlanjutan layanan publik digital. Sistem OSS yang tidak memiliki mekanisme pengamanan yang memadai rentan terhadap gangguan teknis dan serangan siber, seperti serangan Distributed Denial of Service (DDoS) yang dapat menyebabkan layanan tidak tersedia dalam periode tertentu. Gangguan terhadap ketersediaan layanan ini tidak hanya merugikan pengguna, tetapi juga dapat menghambat aktivitas ekonomi, terutama bagi pelaku usaha yang bergantung pada kecepatan proses perizinan. Oleh karena itu, keamanan sistem informasi menjadi faktor strategis dalam menjaga kontinuitas layanan publik digital.

Perlindungan data pribadi merupakan dimensi lain yang tidak kalah penting dalam keamanan e-government. OSS memproses berbagai data sensitif, termasuk identitas pelaku usaha, informasi legalitas, dan dokumen pendukung perizinan. Pengelolaan data tersebut harus sesuai dengan prinsip perlindungan data pribadi dan regulasi yang berlaku. Lemahnya pengamanan data dapat membuka peluang terjadinya pencurian identitas, pemalsuan dokumen, serta penyalahgunaan informasi untuk kepentingan pihak yang tidak bertanggung jawab. Hal ini menunjukkan bahwa keamanan sistem informasi tidak hanya

[5] Magnusson, L., Iqbal, S., & Elm, P. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. International Journal of Information Security, 24, Article 177.

berdampak pada aspek teknis, tetapi juga memiliki implikasi hukum dan etika.

Dengan demikian, keamanan dalam e-government dan layanan publik digital seperti OSS harus dipandang sebagai tanggung jawab menyeluruh yang melibatkan aspek teknologi, organisasi, dan kebijakan. Penguatan keamanan sistem informasi perlu dilakukan secara berkelanjutan melalui penerapan standar keamanan, peningkatan kompetensi sumber daya manusia, serta pengawasan dan evaluasi yang konsisten. Pendekatan yang komprehensif ini diharapkan mampu menciptakan layanan publik digital yang aman, andal, dan dipercaya oleh masyarakat, sehingga tujuan transformasi digital dalam pemerintahan dapat tercapai secara optimal.[6].

4. Tata Kelola Keamanan Informasi dalam Sistem Pemerintah

Tata kelola keamanan informasi dalam sistem pemerintahan memiliki peran strategis dalam menjamin bahwa penerapan teknologi informasi, khususnya pada layanan perizinan berbasis Online Single Submission (OSS), berjalan secara aman, terkontrol, dan berkelanjutan. Tata kelola ini berfungsi sebagai kerangka kerja yang mengatur bagaimana kebijakan keamanan dirumuskan, diimplementasikan, serta diawasi dalam organisasi publik. Tanpa tata kelola yang jelas dan terstruktur, upaya pengamanan sistem informasi berpotensi menjadi tidak konsisten dan tidak efektif dalam menghadapi berbagai ancaman keamanan digital.

Salah satu komponen utama dalam tata kelola keamanan informasi adalah manajemen risiko. Instansi pemerintah perlu mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan yang berpotensi mengganggu operasional sistem OSS, baik yang bersumber dari faktor internal seperti kesalahan manusia maupun faktor eksternal seperti serangan siber. Proses manajemen risiko ini memungkinkan organisasi untuk menentukan prioritas pengamanan dan mengalokasikan sumber daya secara tepat sesuai tingkat risiko yang dihadapi. Dengan demikian, pengendalian keamanan dapat difokuskan pada area yang paling kritis terhadap keberlangsungan layanan perizinan digital.

Selain manajemen risiko, audit keamanan informasi merupakan instrumen penting dalam tata kelola keamanan sistem pemerintah. Audit dilakukan untuk menilai kesesuaian antara kebijakan keamanan yang telah ditetapkan dengan praktik pengamanan yang diterapkan di lapangan. Melalui audit keamanan secara berkala, instansi pemerintah dapat mendeteksi kelemahan sistem, mengevaluasi efektivitas kontrol keamanan, serta memastikan kepatuhan terhadap regulasi dan standar yang berlaku. Hasil audit juga dapat menjadi dasar dalam perbaikan berkelanjutan terhadap sistem keamanan OSS.

Penegakan standar keamanan informasi internasional, seperti ISO/IEC 27001[7], juga menjadi bagian integral dari tata kelola keamanan informasi di sektor publik. Penerapan standar ini membantu instansi pemerintah dalam membangun sistem manajemen keamanan informasi yang sistematis dan terukur. Namun, keberhasilan tata kelola keamanan tidak hanya bergantung pada aspek teknis, melainkan juga pada koordinasi yang efektif antara unit teknis dan manajemen. Kolaborasi ini diperlukan agar kebijakan keamanan dapat dipahami dan dijalankan secara konsisten di seluruh lini organisasi. Dengan tata kelola keamanan informasi yang kuat, integritas OSS sebagai platform pelayanan perizinan digital dapat terjaga dan kepercayaan publik terhadap layanan pemerintah dapat ditingkatkan.

5. Ancaman, Risiko, dan Tantangan Keamanan pada OSS

Ancaman keamanan pada sistem Online Single Submission (OSS) merupakan konsekuensi dari sifat sistem yang berbasis daring dan terintegrasi dengan berbagai layanan

[6] Choi, M., Lee, J., & Hwang, K. (2018). Information systems security (ISS) of e-government for sustainability: A dual path model of ISS influenced by institutional isomorphism.
[7] "ISO/IEC 27001:2022 - Information Security Management Systems," accessed December 30, 2025, https://www.iso.org/standard/27001.

pemerintahan lainnya. Akses tidak sah menjadi salah satu risiko utama, terutama apabila mekanisme autentikasi dan pengelolaan hak akses tidak diterapkan secara ketat. Celah ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memperoleh atau memanipulasi data perizinan, yang pada akhirnya dapat merugikan pengguna dan menurunkan kredibilitas layanan publik digital.

Selain itu, serangan siber seperti Distributed Denial of Service (DDoS) dan malware berpotensi mengganggu ketersediaan layanan OSS. Serangan DDoS dapat menyebabkan sistem tidak dapat diakses dalam jangka waktu tertentu, sehingga menghambat proses pengajuan dan penerbitan izin. Sementara itu, malware dapat menyusup melalui perangkat pengguna atau sistem internal apabila tidak dilengkapi dengan pengamanan yang memadai, yang berisiko menimbulkan kebocoran data atau kerusakan sistem.

Tantangan lain yang dihadapi dalam implementasi OSS adalah ketergantungan pada infrastruktur jaringan dan tingkat literasi keamanan digital pengguna. Gangguan jaringan telekomunikasi dapat berdampak langsung pada kinerja layanan, khususnya di wilayah dengan infrastruktur teknologi yang belum merata. Selain itu, praktik keamanan yang lemah, seperti penggunaan kata sandi yang mudah ditebak atau berbagi kredensial, meningkatkan risiko pencurian identitas (credential theft). Oleh karena itu, upaya pengamanan OSS perlu dilakukan secara menyeluruh melalui penerapan kontrol teknis, seperti autentikasi berlapis dan enkripsi data, serta kontrol non-teknis berupa peningkatan kesadaran dan kompetensi sumber daya manusia. Pendekatan terpadu ini penting untuk meminimalkan risiko keamanan dan menjaga keandalan layanan perizinan digital.

6. Perlindungan Data Pribadi dan Regulasi

Perlindungan data pribadi merupakan aspek fundamental dalam keamanan sistem informasi digital, terutama pada layanan publik berbasis Online Single Submission (OSS) yang mengelola data warga dan pelaku usaha dalam jumlah besar. Sistem OSS memproses berbagai jenis data sensitif, seperti identitas pengguna, informasi usaha, dokumen legal, serta data administratif lainnya yang wajib dijaga kerahasiaan dan keamanannya. Oleh karena itu, pengelolaan data dalam OSS harus dilakukan secara bertanggung jawab dan sesuai dengan prinsip perlindungan data pribadi.

Keberadaan regulasi seperti Undang-Undang Perlindungan Data Pribadi memberikan landasan hukum yang jelas bagi instansi pemerintah dalam mengelola dan melindungi data pengguna layanan digital. Regulasi ini menuntut adanya prinsip legalitas, transparansi, pembatasan tujuan, serta keamanan dalam setiap tahapan pemrosesan data, mulai dari pengumpulan, penyimpanan, hingga penghapusan data. Kegagalan dalam memenuhi prinsip-prinsip tersebut dapat menimbulkan risiko hukum bagi instansi pemerintah serta merugikan hak-hak subjek data.

Selain kepatuhan terhadap regulasi, perlindungan data pribadi juga berkaitan erat dengan aspek etika dan kepercayaan publik. Masyarakat akan lebih bersedia memanfaatkan layanan perizinan digital apabila mereka merasa yakin bahwa data pribadinya dikelola secara aman dan tidak disalahgunakan. Oleh karena itu, instansi pemerintah perlu menerapkan kebijakan perlindungan data yang jelas, memperkuat mekanisme pengamanan teknis, serta meningkatkan kesadaran aparatur terhadap pentingnya perlindungan data pribadi. Upaya ini menjadi bagian integral dalam membangun sistem OSS yang aman, patuh hukum, dan berorientasi pada perlindungan hak pengguna.[8].

[8] Suryana, T. F., Rahmawati, A. A., Ramdanti, N. S., & Safitri, A. N. (2025). Transformasi Digital dalam Pelayanan Publik: Tinjauan Yuridis terhadap SPBE di Indonesia. CONSTITUO: Journal of State and Political Law Research, 4(1), 37-53.

Metode Penelitian

1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (literature review). Pendekatan ini dipilih karena penelitian berfokus pada pengkajian konsep, teori, dan temuan ilmiah yang berkaitan dengan aspek keamanan sistem informasi digital dalam pelayanan perizinan berbasis OSS. Melalui studi literatur, peneliti dapat memahami secara komprehensif bagaimana keamanan sistem informasi diterapkan dalam konteks e-government, khususnya layanan perizinan digital, berdasarkan hasil penelitian terdahulu yang relevan dan terpercaya.

2. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kepustakaan (library research) yang bersifat deskriptif-analitis. Penelitian ini bertujuan untuk menggambarkan dan menganalisis aspek keamanan sistem informasi digital, seperti kerahasiaan data, integritas sistem, dan ketersediaan layanan, berdasarkan kajian terhadap jurnal ilmiah, artikel penelitian, dan publikasi akademik. Dengan pendekatan ini, peneliti tidak melakukan pengumpulan data lapangan, melainkan mengandalkan data sekunder yang diperoleh dari sumber pustaka untuk mengidentifikasi pola, konsep, serta tantangan keamanan sistem OSS dalam pelayanan publik.

3. Sumber Data, Teknik Pengumpulan, dan Analisis Data

Sumber data dalam penelitian ini berupa jurnal nasional dan internasional yang membahas keamanan sistem informasi, e-government, pelayanan publik digital, serta implementasi OSS atau sistem perizinan berbasis teknologi informasi. Jurnal diperoleh melalui Google Scholar, portal jurnal nasional, dan repositori akademik lainnya dengan kriteria publikasi relevan dan kredibel.

Teknik pengumpulan data dilakukan dengan penelusuran dan seleksi literatur, kemudian dilanjutkan dengan proses klasifikasi dan pencatatan data sesuai fokus penelitian. Data yang telah terkumpul dianalisis menggunakan analisis isi (content analysis), yaitu dengan mengkaji, membandingkan, dan menginterpretasikan hasil penelitian terdahulu untuk menemukan kesamaan, perbedaan, serta kesimpulan terkait aspek keamanan sistem informasi digital dalam pelayanan perizinan berbasis OSS. Hasil analisis tersebut digunakan sebagai dasar untuk menarik kesimpulan dan memberikan gambaran teoretis mengenai keamanan sistem OSS pada instansi pemerintahan.

Hasil dan Pembahasan

1. Keamanan Sistem Informasi dalam Konteks Pelayanan Publik Digital

Transformasi pelayanan perizinan melalui pemanfaatan sistem informasi digital, seperti Online Single Submission (OSS), merupakan bagian integral dari implementasi e-government yang terus dikembangkan oleh instansi pemerintahan di Indonesia. Digitalisasi pelayanan publik ini bertujuan untuk mempercepat proses birokrasi, meningkatkan efisiensi waktu dan biaya, serta memperluas akses masyarakat terhadap layanan perizinan tanpa dibatasi oleh ruang dan waktu. Dengan adanya OSS, proses pengajuan izin usaha yang sebelumnya dilakukan secara manual dan memerlukan kehadiran fisik di kantor pemerintahan kini dapat dilaksanakan secara daring melalui satu platform terintegrasi, sehingga memberikan kemudahan bagi pelaku usaha dan meningkatkan efektivitas kinerja birokrasi.

Meskipun demikian, pemanfaatan sistem informasi digital dalam pelayanan publik tidak terlepas dari berbagai tantangan, terutama yang berkaitan dengan aspek keamanan sistem informasi. OSS sebagai sistem perizinan elektronik mengelola dan menyimpan data dalam jumlah besar, termasuk data pribadi pemohon, informasi usaha, serta dokumen legal yang bersifat sensitif. Kondisi ini menjadikan keamanan sistem informasi sebagai elemen

krusial yang harus diperhatikan secara serius, karena setiap kelemahan dalam sistem dapat berpotensi menimbulkan risiko kebocoran data, penyalahgunaan informasi, maupun gangguan terhadap ketersediaan layanan. Oleh karena itu, keamanan sistem informasi tidak hanya dipandang sebagai persoalan teknis, tetapi juga sebagai faktor strategis dalam menjamin kualitas dan keberlanjutan pelayanan publik digital.

Dalam konteks pelayanan publik digital, keamanan sistem informasi memiliki keterkaitan erat dengan tingkat kepercayaan pengguna terhadap layanan yang disediakan oleh pemerintah. Kepercayaan masyarakat dan pelaku usaha akan terbentuk apabila mereka meyakini bahwa data dan informasi yang disampaikan melalui sistem OSS dikelola secara aman, terlindungi, dan tidak disalahgunakan. Apabila terjadi insiden keamanan, seperti kebocoran data atau gangguan sistem, kepercayaan publik terhadap instansi pemerintah dapat menurun secara signifikan. Penurunan kepercayaan ini berpotensi menghambat tingkat adopsi layanan digital dan mendorong pengguna untuk kembali menggunakan mekanisme pelayanan konvensional yang dinilai lebih aman, meskipun kurang efisien.

Selain aspek kepercayaan, keamanan sistem informasi juga berperan penting dalam menjaga keberlangsungan dan keandalan layanan publik digital. Sistem OSS yang tidak memiliki mekanisme pengamanan yang memadai rentan terhadap berbagai ancaman siber, seperti serangan malware, peretasan, maupun serangan Distributed Denial of Service (DDoS) yang dapat mengganggu ketersediaan layanan. Gangguan tersebut tidak hanya berdampak pada pengguna layanan, tetapi juga dapat menghambat aktivitas ekonomi dan investasi, mengingat proses perizinan merupakan salah satu faktor penentu dalam kelancaran kegiatan usaha. Dengan demikian, keamanan sistem informasi menjadi prasyarat utama agar layanan perizinan digital dapat beroperasi secara stabil dan berkelanjutan.

Lebih lanjut, keamanan sistem informasi dalam pelayanan publik digital juga berkaitan dengan tanggung jawab pemerintah dalam melindungi hak-hak warga negara, khususnya hak atas perlindungan data pribadi. Penerapan OSS menuntut adanya pengelolaan data yang sesuai dengan prinsip kerahasiaan, integritas, dan ketersediaan informasi. Hal ini menegaskan bahwa transformasi digital dalam pelayanan publik tidak cukup hanya berfokus pada peningkatan efisiensi dan kemudahan layanan, tetapi juga harus diimbangi dengan upaya penguatan keamanan sistem informasi secara menyeluruh. Dengan pengelolaan keamanan yang optimal, sistem OSS diharapkan mampu mendukung terciptanya pelayanan publik digital yang aman, terpercaya, dan berorientasi pada kepentingan masyarakat[9].

2. Faktor-faktor Keamanan yang Mempengaruhi Layanan Digital

Berdasarkan hasil kajian literatur dalam konteks e-government, terdapat beberapa faktor informasi keamanan yang signifikan mempengaruhi kepercayaan publik dan adopsi sistem layanan digital seperti OSS. Penelitian literature review oleh Febrianty, Hilman, & Yazid 2024)[10] mengidentifikasi bahwa aspek teknologi, organisasi, dan lingkungan merupakan tiga dimensi utama yang mempengaruhi keamanan layanan e-government.

Keamanan sistem informasi dalam implementasi e-government, khususnya layanan perizinan digital seperti OSS, dipengaruhi oleh berbagai dimensi yang saling berkaitan, yaitu dimensi teknologi, organisasi, dan lingkungan. Faktor teknologi mencakup aspek

[9] Dewi, R., Priyanti, H., Aisyah, T., & Hasyem, M. (2025). Implementasi E-Government Berbasis Online Single Submission (OSS) Dalam Upaya Meningkatkan Kualitas Layanan Publik Digital. Jurnal Pemerintahan Dan Politik, 10(3), 579-593.

[10] Febrianty, D., Hilman, M., & Yazid, S. (2024). Information Security Factors and Strategies in Enhancing E-Government Adoption in the Public Sector of Developing Countries: A Literature Review. The Indonesian Journal of Computer Science, 13(6).

perlindungan teknis yang berfungsi sebagai lapisan pertama pengamanan sistem, seperti penggunaan enkripsi data untuk menjaga kerahasiaan informasi, penerapan kontrol akses berbasis hak pengguna, serta mekanisme deteksi dan pencegahan ancaman siber. Aspek ini berperan penting dalam melindungi sistem dari serangan teknis dan kebocoran data.

Namun demikian, keberhasilan keamanan sistem tidak hanya ditentukan oleh faktor teknologi. Dimensi organisasi memiliki peran yang sangat signifikan karena berkaitan langsung dengan bagaimana sistem dikelola dan dijalankan. Dimensi ini mencakup keberadaan kebijakan keamanan informasi yang jelas, penerapan manajemen risiko secara sistematis, serta pembentukan budaya keamanan di dalam instansi pengelola sistem. Tanpa dukungan kebijakan dan komitmen organisasi yang kuat, teknologi keamanan yang canggih pun berpotensi tidak berjalan secara optimal.

Selain itu, dimensi lingkungan juga turut memengaruhi tingkat keamanan layanan e-government. Dimensi ini meliputi regulasi perlindungan data, lingkungan hukum yang berlaku, serta persepsi publik terhadap keamanan dan keandalan layanan digital pemerintah. Persepsi masyarakat yang positif akan meningkatkan tingkat kepercayaan dan partisipasi dalam penggunaan layanan digital. Studi ini menunjukkan bahwa faktor non-teknis, seperti kebijakan organisasi dan persepsi publik, sering kali memberikan dampak yang lebih besar dibandingkan faktor teknis dalam menentukan keberhasilan keamanan e-government secara keseluruhan.

3. Teknik Analisis Keamanan dan Implikasinya

Berbagai kajian teknis pada sistem informasi e-government menunjukkan bahwa pengujian keamanan sistem diperlukan untuk mengetahui kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Misalnya, studi komparatif oleh Ayyas, Fauzi, & Widodo[11] membahas metode analisis keamanan seperti penetration testing dan vulnerability assessment dalam konteks sistem e-government. Penetration testing adalah teknik di mana penguji mencoba mengeksploitasi celah keamanan secara aktif untuk menilai seberapa kuat sistem tersebut terhadap serangan nyata, sedangkan vulnerability assessment memetakan potensi kelemahan sistem secara sistematis.

Studi ini menunjukkan bahwa penggunaan kombinasi metode evaluasi keamanan, seperti kajian literatur dan analisis teknis, memiliki peran yang sangat penting dalam menilai tingkat keamanan sistem informasi digital publik. Kedua metode tersebut saling melengkapi dalam membantu mengidentifikasi berbagai potensi kerentanan, baik yang bersifat teknis maupun konseptual, sebelum sistem digunakan secara luas oleh masyarakat. Dengan adanya evaluasi sejak tahap awal, risiko gangguan layanan dan kebocoran data dapat diminimalkan secara lebih efektif.

Kajian literatur memungkinkan peneliti untuk memahami pola ancaman, kelemahan sistem, serta praktik terbaik (best practices) dalam keamanan sistem informasi yang telah diterapkan pada berbagai layanan e-government sebelumnya. Melalui pendekatan ini, dapat diidentifikasi faktor-faktor kunci yang memengaruhi keberhasilan pengamanan sistem, termasuk aspek kebijakan, tata kelola, dan kesiapan sumber daya manusia. Sementara itu, analisis teknis berfokus pada identifikasi celah keamanan pada infrastruktur dan aplikasi, sehingga potensi serangan siber dapat dideteksi lebih dini.

Hasil dari kajian literatur dan analisis teknis tersebut dapat dijadikan dasar yang kuat dalam merancang strategi pengamanan sistem OSS pada instansi pemerintahan. Strategi ini mencakup peningkatan perlindungan terhadap ancaman siber, penguatan mekanisme kontrol akses, serta pengelolaan data pengguna secara aman. Dengan penerapan strategi

[11] Ayyas, M., Fauzi, A., & Widodo, S. (2024). Studi komparatif teknik analisis keamanan sistem informasi e-government: Penetration testing vs vulnerability assessment. SATIN – Sains dan Teknologi Informasi, 9(2), 1–11.

yang tepat, sistem OSS diharapkan mampu menjaga integritas, kerahasiaan, dan keandalan data, sekaligus meningkatkan kepercayaan masyarakat terhadap layanan perizinan digital pemerintah.

4. Tantangan Keamanan pada Pelayanan Perizinan OSS

Meskipun Online Single Submission (OSS) dirancang sebagai solusi digital untuk meningkatkan efisiensi dan efektivitas pelayanan perizinan, berbagai kajian literatur menunjukkan bahwa implementasi sistem ini masih menghadapi tantangan keamanan yang cukup kompleks, terutama dalam konteks negara berkembang. Tantangan tersebut tidak hanya berkaitan dengan aspek teknis sistem informasi, tetapi juga mencakup dimensi organisasi, sumber daya manusia, serta lingkungan regulasi dan sosial. Kompleksitas ini menjadikan keamanan OSS sebagai isu strategis yang memerlukan perhatian serius dari instansi pemerintahan agar manfaat digitalisasi dapat dirasakan secara optimal oleh masyarakat dan pelaku usaha.

Salah satu tantangan utama dalam pelayanan perizinan berbasis OSS adalah rendahnya tingkat kepercayaan publik terhadap keamanan data pribadi yang dikelola oleh sistem digital pemerintah. OSS memproses dan menyimpan berbagai data sensitif, seperti identitas pemohon, informasi usaha, dan dokumen legal, sehingga kekhawatiran masyarakat terhadap potensi kebocoran atau penyalahgunaan data menjadi hal yang wajar. Apabila instansi pemerintah tidak mampu memberikan jaminan keamanan yang memadai, persepsi negatif terhadap layanan digital dapat berkembang dan menghambat partisipasi publik dalam penggunaan OSS. Hal ini sejalan dengan temuan Febrianty et al. (2024) yang menegaskan bahwa masalah keamanan informasi merupakan salah satu faktor utama yang memengaruhi tingkat adopsi dan kepercayaan publik terhadap layanan e-government.

Selain persoalan kepercayaan, risiko akses tidak sah dan kebocoran informasi juga menjadi tantangan signifikan dalam pengelolaan OSS. Kelemahan pada mekanisme autentikasi, pengendalian hak akses, serta pengelolaan akun pengguna dapat membuka peluang bagi pihak yang tidak berwenang untuk mengakses atau memanipulasi data perizinan. Ancaman ini tidak hanya berasal dari serangan eksternal, seperti peretasan dan malware, tetapi juga dari faktor internal, seperti kelalaian pengguna atau penyalahgunaan kewenangan oleh aparat yang memiliki akses sistem. Oleh karena itu, tantangan keamanan OSS bersifat multidimensional dan tidak dapat diselesaikan hanya dengan pendekatan teknis semata.

Tantangan lainnya berkaitan dengan pengembangan dan pemeliharaan sistem yang aman dan andal. OSS sebagai sistem terintegrasi membutuhkan infrastruktur teknologi informasi yang stabil, pembaruan sistem secara berkala, serta mekanisme pemantauan keamanan yang berkelanjutan. Namun, keterbatasan anggaran, ketimpangan infrastruktur teknologi antar daerah, serta minimnya tenaga ahli di bidang keamanan siber sering kali menjadi kendala dalam menjaga tingkat keamanan sistem secara optimal. Kondisi ini berpotensi meningkatkan kerentanan sistem terhadap gangguan teknis maupun serangan siber, yang pada akhirnya dapat mengganggu ketersediaan layanan perizinan digital.

Lebih lanjut, rendahnya tingkat kesadaran dan literasi keamanan digital di kalangan pengguna dan aparatur pemerintah juga menjadi tantangan yang tidak dapat diabaikan. Praktik keamanan yang lemah, seperti penggunaan kata sandi yang mudah ditebak, berbagi kredensial akun, atau kurangnya kewaspadaan terhadap upaya phishing, dapat meningkatkan risiko terjadinya pelanggaran keamanan. Tanpa adanya upaya sistematis untuk meningkatkan pemahaman dan kesadaran terhadap praktik keamanan digital, kelemahan pada faktor manusia (human factor) akan terus menjadi celah yang sulit dikendalikan dalam sistem OSS.

Berdasarkan berbagai tantangan tersebut, penguatan kebijakan keamanan dan tata kelola sistem informasi menjadi langkah yang sangat penting dalam mengoptimalkan

pelayanan perizinan berbasis OSS. Kebijakan perlindungan data pribadi yang jelas, penerapan standar keamanan informasi, serta peningkatan kapasitas sumber daya manusia di bidang keamanan siber perlu dilakukan secara terpadu dan berkelanjutan. Upaya ini sejalan dengan tujuan pemerintah daerah dalam menghadirkan layanan publik digital yang tidak hanya efisien dan mudah diakses, tetapi juga aman, andal, dan terpercaya. Dengan pendekatan keamanan yang komprehensif, OSS diharapkan mampu menjadi instrumen pelayanan perizinan yang mendukung pertumbuhan ekonomi sekaligus menjaga kepercayaan publik terhadap transformasi digital pemerintahan.

Kesimpulan

Berdasarkan hasil studi di atas, dapat disimpulkan bahwa keamanan sistem informasi digital merupakan aspek krusial dalam pelaksanaan pelayanan perizinan berbasis Online Single Submission (OSS) berperan penting dalam meningkatkan efisiensi, transparansi, dan kemudahan pelayanan publik, namun juga menghadapi berbagai tantangan keamanan informasi seperti perlindungan data pribadi, kerahasiaan informasi, integritas data, serta ketersediaan sistem. Literatur yang dianalisis menunjukkan bahwa penerapan kebijakan keamanan informasi, penggunaan teknologi pengamanan yang memadai, serta peningkatan kompetensi sumber daya manusia menjadi faktor penentu dalam menjaga keandalan sistem OSS. Dengan pengelolaan keamanan yang baik, sistem OSS dapat mendukung pelayanan perizinan yang aman, terpercaya, dan berkelanjutan.

Meskipun penelitian ini memberikan gambaran komprehensif mengenai aspek keamanan sistem informasi digital dalam pelayanan perizinan berbasis Online Single Submission (OSS) pada instansi pemerintahan, terdapat beberapa keterbatasan yang perlu diperhatikan. Pertama, penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur, sehingga seluruh temuan dan kesimpulan didasarkan pada data sekunder yang diperoleh dari jurnal ilmiah, buku, regulasi, dan dokumen resmi.

Keterbatasan ini menyebabkan penelitian tidak melibatkan data empiris lapangan, seperti wawancara dengan aparatur pengelola OSS, observasi langsung terhadap sistem, maupun pengalaman pengguna layanan. Akibatnya, penelitian belum dapat menggambarkan kondisi keamanan OSS secara faktual dan spesifik pada instansi pemerintahan tertentu. Kedua, penelitian ini tidak melakukan pengujian teknis terhadap sistem OSS, seperti penetration testing, vulnerability assessment, atau audit keamanan sistem secara langsung. Oleh karena itu, penelitian belum mampu mengidentifikasi tingkat kerentanan teknis OSS secara nyata, melainkan hanya mengandalkan temuan dan rekomendasi dari penelitian terdahulu. Hal ini membatasi kemampuan penelitian dalam memberikan evaluasi keamanan yang bersifat operasional dan teknis.

Ketiga, ruang lingkup penelitian masih bersifat umum dan konseptual, karena membahas keamanan sistem informasi OSS dalam konteks instansi pemerintahan secara luas. Penelitian ini belum membedakan secara mendalam variasi tingkat kesiapan keamanan antar instansi atau daerah, yang pada praktiknya dapat dipengaruhi oleh perbedaan sumber daya manusia, infrastruktur teknologi, dan dukungan anggaran. Keempat, penelitian ini belum secara spesifik mengukur persepsi dan tingkat kepercayaan publik terhadap keamanan layanan OSS melalui instrumen penelitian kuantitatif, seperti survei atau kuesioner. Padahal, aspek kepercayaan publik merupakan variabel penting dalam keberhasilan adopsi layanan e-government dan sangat berkaitan dengan isu keamanan sistem informasi.

Dengan adanya keterbatasan tersebut, hasil penelitian ini lebih tepat dipahami sebagai kajian konseptual dan teoretis yang memberikan landasan pemahaman mengenai pentingnya keamanan sistem informasi dalam pelayanan perizinan berbasis OSS. Penelitian selanjutnya diharapkan dapat melengkapi keterbatasan ini dengan melakukan studi empiris,

pengujian teknis sistem, serta analisis persepsi pengguna untuk memperoleh gambaran yang lebih utuh dan aplikatif.

Daftar Pustaka

Ayyas, M., Fauzi, A., & Widodo, S. (2024). Studi komparatif teknik analisis keamanan sistem informasi e-government: Penetration testing vs vulnerability assessment. SATIN – Sains dan Teknologi Informasi, 9(2), 1–11.

Choi, M., Lee, J., & Hwang, K. (2018). Information systems security (ISS) of e-government for sustainability: A dual path model of ISS influenced by institutional isomorphism.

Dewi, R., Priyanti, H., Aisyah, T., & Hasyem, M. (2025). Implementasi E-Government Berbasis Online Single Submission (OSS) Dalam Upaya Meningkatkan Kualitas Layanan Publik Digital. Jurnal Pemerintahan Dan Politik, 10(3), 579-593.

Febrianty, D., Hilman, M., & Yazid, S. (2024). Information Security Factors and Strategies in Enhancing E-Government Adoption in the Public Sector of Developing Countries: A Literature Review. The Indonesian Journal of Computer Science, 13(6).

"ISO/IEC 27001:2022 - Information Security Management Systems." Accessed December 30, 2025. https://www.iso.org/standard/27001.

Magnusson, L., Iqbal, S., & Elm, P. (2025). Information security governance in the public sector: Investigations, approaches, measures, and trends. International Journal of Information Security, 24, Article 177.

Maulan, Puteri, and Nining Fitriani. "E-GOVERNMENT AND PUBLIC TRUST: EXAMINING THE IMPACT OF DIGITAL TRANSPARENCY ON CITIZEN ENGAGEMENT IN SOUTHEAST ASIA." *Dinamika: Jurnal Manajemen Sosial Ekonomi* 5 (May 2025): 242–52. https://doi.org/10.51903/shq0s821.

Novianto, F. (2023). Analisis keamanan informasi pada e-government menggunakan COBIT 5 framework. CyberSecurity dan Forensik Digital, 6(1).

Sari, C. F., & Rahayu, S. A. P. (2025). Analisis Penerapan OSS Berbasis Risiko dalam Mewujudkan Kepastian Hukum bagi Investor di Indonesia. JURNAL ILMIAH NUSANTARA, 2(3), 577-591.

Suryana, T. F., Rahmawati, A. A., Ramdanti, N. S., & Safitri, A. N. (2025). Transformasi Digital dalam Pelayanan Publik: Tinjauan Yuridis terhadap SPBE di Indonesia. CONSTITUO: Journal of State and Political Law Research, 4(1), 37-53.

Syahfitra, A. (2020). E-Government dalam pelaksanaan One Stop Service (OSS). Jurnal Administrasi dan Sains Pemerintahan.