



KEAMANAN JARINGAN DALAM APLIKASI E-GOVERNMENT

Zal zabilla Azzahra Rianamanda¹, Callvin Haidiri Rahmansyah², Reinhardt Mozes Wayong³^{1,2,3} Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas PamulangE-mail: zalzabillaazzahra@gmail.com, callvinpct01@gmail.com,
reinhrdt9@gmail.com

ABSTRACT

The implementation of e-government applications has significantly transformed the delivery of public services by enabling efficient, transparent, and easily accessible digital interactions between government institutions and citizens. Despite these advantages, the increasing reliance on computer networks has made e-government systems vulnerable to various security threats that may compromise data confidentiality, system integrity, and service availability. This study aims to analyze common network security threats faced by e-government applications and to evaluate the effectiveness of layered network security mechanisms in mitigating these risks. A descriptive qualitative research method was employed using a case study approach on a simulated population administration system named SIPANDA, which represents a typical e-government environment. The results indicate that the implementation of layered network security mechanisms—such as firewalls, encryption, access control, and intrusion detection systems—plays a crucial role in enhancing system protection, resilience, and service reliability.

Keywords: *Network Security, Cybersecurity, Data protection, Detection Systems, Layered Security.*

ABSTRAK

Implementasi aplikasi e-government telah secara signifikan mengubah penyampaian layanan publik dengan memungkinkan interaksi digital yang efisien, transparan, dan mudah diakses antara lembaga pemerintah dan warga negara. Terlepas dari keuntungan ini, peningkatan ketergantungan pada jaringan komputer membuat sistem e-government rentan terhadap berbagai ancaman keamanan yang dapat membahayakan kerahasiaan data, integritas sistem, dan ketersediaan layanan. Studi ini bertujuan untuk menganalisis ancaman keamanan jaringan umum yang dihadapi oleh aplikasi e-government dan untuk mengevaluasi efektivitas mekanisme keamanan jaringan berlapis dalam mengurangi risiko ini. Metode penelitian deskriptif kualitatif digunakan dengan pendekatan studi kasus pada sistem administrasi kependudukan simulasi bernama SIPANDA, yang mewakili lingkungan e-government yang khas. Hasil menunjukkan bahwa implementasi mekanisme keamanan jaringan berlapis—seperti firewall, enkripsi, kontrol akses, dan sistem deteksi

Article History

Received: Januari 2026

Reviewed: Januari 2026

Published: Januari 2026

Plagiarism Checker No
235

Prefix DOI :

[10.8734/Kohesi.v1i2.365](https://doi.org/10.8734/Kohesi.v1i2.365)

Copyright : Author

Publish by : Kohesi



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)



intrusi—memainkan peran penting dalam meningkatkan perlindungan sistem, ketahanan, dan keandalan layanan.

Kata Kunci: *Keamanan Jaringan, Keamanan Siber, Perlindungan Data, Sistem Deteksi, Keamanan Berlapis.*

1. PENDAHULUAN

Kemajuan pesat teknologi informasi dan komunikasi telah mendorong pemerintah di seluruh dunia untuk mengadopsi sistem e-government sebagai pendekatan strategis untuk memodernisasi penyampaian layanan publik. E-government merujuk pada penggunaan teknologi digital, khususnya jaringan komputer dan aplikasi berbasis internet, untuk memberikan layanan pemerintah, bertukar informasi, dan berinteraksi dengan warga negara, bisnis, dan entitas pemerintah lainnya. Layanan seperti administrasi kependudukan, perizinan, perpajakan, pendaftaran layanan kesehatan, dan penyebaran informasi publik semakin banyak diberikan melalui platform online untuk meningkatkan efisiensi dan transparansi. Kelemahan dalam keamanan jaringan dapat dieksploitasi oleh pelaku jahat untuk melakukan akses tanpa izin, pelanggaran data, dan serangan siber yang mengganggu ketersediaan layanan. Insiden tersebut tidak hanya menyebabkan kerugian operasional dan finansial tetapi juga mengurangi kepercayaan warga negara terhadap layanan pemerintah digital.

Keamanan jaringan memainkan peran penting dalam memastikan kerahasiaan, integritas, dan ketersediaan informasi dalam sistem e-government. Tanpa kontrol keamanan yang memadai, serangan berbasis jaringan seperti intersepsi data, serangan penolakan layanan (denial-of-service), dan upaya intrusi dapat berdampak buruk pada kinerja sistem. Oleh karena itu, memahami ancaman keamanan jaringan dan menerapkan mekanisme perlindungan yang efektif sangat penting untuk keberlanjutan inisiatif e-government. Penelitian ini berfokus pada analisis masalah keamanan jaringan dalam aplikasi e-government dan mengevaluasi peran mekanisme keamanan jaringan berlapis dalam mengurangi potensi risiko.

Perkembangan pesat teknologi informasi dan komunikasi telah mendorong pemerintah di seluruh dunia untuk mengadopsi sistem e-government guna meningkatkan penyampaian layanan publik. E-government memungkinkan pemerintah untuk menyediakan layanan seperti administrasi kependudukan, perizinan, perpajakan, dan penyebaran informasi publik melalui platform digital, mengurangi kompleksitas birokrasi dan meningkatkan efisiensi.

Terlepas dari manfaat tersebut, sistem e-government sangat bergantung pada jaringan komputer, sehingga rentan terhadap berbagai ancaman keamanan siber. Sistem ini memproses dan menyimpan data warga negara yang sensitif, termasuk informasi identitas pribadi dan



catatan administrasi. Keamanan jaringan yang lemah dapat menyebabkan akses tidak sah, pelanggaran data, dan serangan penolakan layanan, yang dapat mengganggu layanan publik dan mengikis kepercayaan warga terhadap inisiatif pemerintahan digital. Oleh karena itu, memastikan keamanan jaringan yang kuat merupakan persyaratan penting untuk keberhasilan implementasi e-government.

2. METODE PENELITIAN

Studi ini menggunakan metodologi penelitian deskriptif kualitatif dengan pendekatan studi kasus untuk menganalisis keamanan jaringan dalam aplikasi e-government. Objek analisis adalah sistem e-government simulasi bernama SIPANDA (Sistem Informasi Administrasi Kependudukan), yang dirancang untuk mewakili platform layanan publik online tipikal yang dioperasikan oleh lembaga pemerintah. Sistem ini diasumsikan dapat diakses melalui jaringan publik dan terhubung ke basis data internal pemerintah yang berisi data warga negara yang sensitif.

Proses penelitian terdiri dari tiga tahap utama. Pertama, dilakukan tinjauan pustaka untuk meneliti studi-studi sebelumnya yang berkaitan dengan e-government, ancaman keamanan jaringan, dan kerangka kerja keamanan siber. Tahap ini memberikan landasan teoritis untuk mengidentifikasi masalah keamanan umum dan praktik terbaik dalam melindungi sistem pemerintahan digital. Kedua, arsitektur dan aliran data sistem SIPANDA dianalisis untuk mengidentifikasi potensi kerentanan jaringan yang dapat dieksploitasi oleh penyerang. Ketiga, potensi ancaman keamanan diidentifikasi dan dianalisis berdasarkan vektor serangan umum yang menargetkan aplikasi e-government.

Evaluasi mekanisme keamanan jaringan dilakukan berdasarkan prinsip-prinsip inti keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan (triad CIA). Kerangka kerja ini memungkinkan studi untuk secara sistematis menilai bagaimana berbagai kontrol keamanan berkontribusi pada perlindungan data, pencegahan akses tidak sah, dan keberlanjutan layanan publik. Meskipun penelitian ini tidak melibatkan pengujian kuantitatif atau pengujian penetrasi teknis, pendekatan kualitatif memberikan wawasan komprehensif tentang tantangan keamanan jaringan dan strategi mitigasi yang tepat dalam lingkungan e-government.

3. HASIL DAN PEMBAHASAN

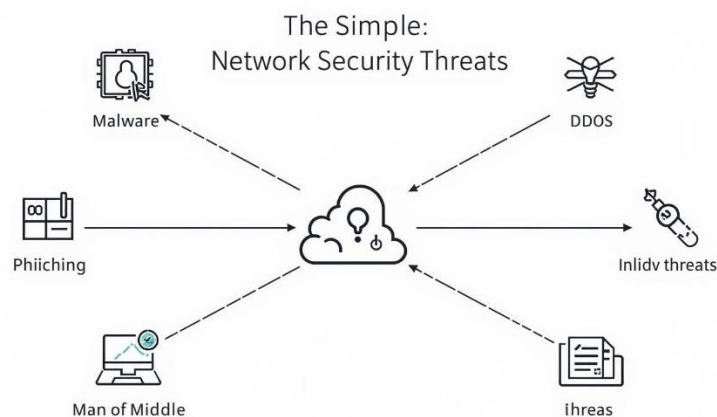
Bagian ini membahas hasil analisis terhadap sistem e-government simulasi SIPANDA dengan menitikberatkan pada identifikasi ancaman keamanan jaringan serta evaluasi penerapan mekanisme keamanan jaringan berlapis. Pembahasan dilakukan secara deskriptif berdasarkan

hasil pengamatan dan analisis terhadap potensi risiko keamanan yang muncul pada lingkungan jaringan e-government. Hasil yang diperoleh kemudian didiskusikan untuk menunjukkan keterkaitan antara ancaman yang teridentifikasi dengan efektivitas mekanisme perlindungan jaringan yang diterapkan dalam menjaga kerahasiaan, integritas, dan ketersediaan layanan publik.

3.1 Ancaman Keamanan Jaringan yang Teridentifikasi

Hasil analisis menunjukkan bahwa sistem SIPANDA menghadapi sejumlah ancaman keamanan jaringan yang umum dijumpai pada implementasi e-government. Salah satu ancaman utama adalah akses tidak sah ke dalam sistem. Ancaman ini muncul akibat kelemahan pada proses autentikasi, pengelolaan kata sandi yang kurang optimal, serta konfigurasi layanan jaringan yang tidak sepenuhnya aman. Akses tidak sah dapat memberikan peluang bagi pihak yang tidak berwenang untuk memperoleh atau memanipulasi data kependudukan yang bersifat sensitif, sehingga berpotensi menimbulkan kerugian bagi individu maupun instansi pemerintah.

Ancaman berikutnya berkaitan dengan keamanan data selama proses transmisi. Sistem e-government bergantung pada komunikasi berbasis jaringan publik, sehingga data yang dikirimkan antara pengguna dan server berisiko disadap apabila tidak dilindungi dengan teknik pengamanan yang memadai. Intersepsi data dapat terjadi melalui berbagai metode, seperti penyadapan lalu lintas jaringan atau serangan perantara, yang memungkinkan penyerang memperoleh informasi penting, termasuk data identitas pribadi dan kredensial pengguna.



Gambar 1. Analisis Keamanan Jaringan

3.2 Analisis Mekanisme Keamanan Jaringan Berlapis

Untuk mengatasi berbagai ancaman tersebut, penerapan mekanisme keamanan jaringan berlapis menjadi strategi yang penting dalam sistem SIPANDA. Pendekatan ini menempatkan



beberapa lapisan pengamanan yang saling melengkapi, sehingga risiko serangan dapat diminimalkan meskipun salah satu lapisan mengalami kegagalan.

Firewall berfungsi sebagai lapisan perlindungan awal yang mengatur dan memfilter lalu lintas jaringan berdasarkan kebijakan keamanan tertentu. Dengan adanya firewall, akses dari sumber yang mencurigakan dapat dibatasi, sehingga mengurangi kemungkinan terjadinya serangan langsung ke sistem. Pada lapisan berikutnya, penerapan enkripsi berperan dalam melindungi data yang dikirimkan melalui jaringan agar tidak dapat dibaca atau diubah oleh pihak yang tidak berwenang.

Berdasarkan hasil analisis, kombinasi berbagai mekanisme keamanan jaringan berlapis terbukti meningkatkan tingkat perlindungan sistem SIPANDA secara signifikan. Pendekatan ini tidak hanya mampu mengurangi potensi dampak serangan keamanan, tetapi juga memperkuat ketahanan sistem serta menjamin keberlangsungan layanan e-government yang andal dan aman.

3.3 Implikasi Penerapan Keamanan Jaringan terhadap Keandalan Layanan E-Government

Hasil pembahasan pada subbagian sebelumnya menunjukkan bahwa ancaman keamanan jaringan memiliki dampak langsung terhadap kinerja dan keberlangsungan layanan e-government. Oleh karena itu, penerapan mekanisme keamanan jaringan yang tepat tidak hanya berfungsi sebagai upaya perlindungan teknis, tetapi juga memberikan implikasi strategis terhadap keandalan dan kualitas layanan publik yang disediakan. Pada sistem SIPANDA, integrasi keamanan jaringan berlapis berkontribusi dalam menciptakan lingkungan layanan yang lebih stabil, aman, dan terpercaya bagi pengguna.

Penerapan firewall, enkripsi, kontrol akses, dan sistem deteksi intrusi terbukti mampu meningkatkan tingkat kepercayaan terhadap sistem dengan meminimalkan risiko kebocoran data dan gangguan layanan. Perlindungan terhadap kerahasiaan data kependudukan memastikan bahwa informasi pribadi warga negara tetap terjaga, sementara mekanisme pengamanan terhadap integritas sistem mencegah terjadinya perubahan data yang tidak sah.

Implikasi lain yang muncul adalah meningkatnya efisiensi operasional dan kesiapan sistem dalam menghadapi potensi insiden keamanan. Dengan adanya pemantauan jaringan secara berkelanjutan dan kebijakan keamanan yang terstruktur, administrator sistem dapat melakukan respons yang lebih cepat terhadap ancaman yang terdeteksi. Hal ini membantu mengurangi waktu henti layanan serta meminimalkan dampak gangguan terhadap proses pelayanan publik.

Secara keseluruhan, penerapan keamanan jaringan yang komprehensif pada sistem e-government seperti SIPANDA memberikan kontribusi signifikan terhadap peningkatan keandalan



layanan dan kepercayaan pengguna. Temuan ini menegaskan bahwa aspek keamanan jaringan harus menjadi bagian integral dalam perancangan dan pengelolaan sistem e-government, bukan hanya sebagai pelengkap, tetapi sebagai fondasi utama dalam mendukung transformasi layanan publik berbasis digital.

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa aplikasi e-government memiliki tingkat ketergantungan yang tinggi terhadap infrastruktur jaringan komputer, sehingga menjadikannya rentan terhadap berbagai ancaman keamanan. Studi pada sistem simulasi SIPANDA menunjukkan bahwa ancaman utama yang dihadapi meliputi akses tidak sah, intersepsi data selama transmisi, serta serangan gangguan layanan seperti denial-of-service dan distributed denial-of-service. Ancaman-ancaman tersebut berpotensi mengganggu kerahasiaan data, integritas sistem, dan ketersediaan layanan publik.

Penerapan mekanisme keamanan jaringan berlapis terbukti menjadi pendekatan yang efektif dalam meminimalkan risiko keamanan pada sistem e-government. Kombinasi penggunaan firewall, enkripsi data, kontrol akses berbasis peran, serta sistem deteksi intrusi mampu meningkatkan tingkat perlindungan sistem secara menyeluruh. Mekanisme ini tidak hanya mencegah terjadinya pelanggaran keamanan, tetapi juga meningkatkan ketahanan sistem terhadap serangan yang bersifat kompleks dan berkelanjutan.

Selain itu, implementasi keamanan jaringan yang komprehensif memberikan dampak positif terhadap keandalan dan kontinuitas layanan e-government. Sistem menjadi lebih stabil, responsif, dan mampu mempertahankan ketersediaan layanan meskipun berada dalam kondisi ancaman keamanan. Hal ini berkontribusi pada peningkatan kepercayaan masyarakat terhadap layanan publik berbasis digital serta mendukung keberhasilan transformasi pemerintahan menuju sistem yang lebih transparan dan efisien.

Secara keseluruhan, hasil penelitian ini menegaskan bahwa keamanan jaringan merupakan komponen fundamental dalam pengembangan dan pengelolaan aplikasi e-government. Oleh karena itu, perencanaan keamanan yang matang dan penerapan mekanisme pengamanan berlapis perlu menjadi prioritas utama guna menjamin keberlangsungan layanan publik yang aman, andal, dan berkelanjutan.



DAFTAR PUSTAKA

- [1] S. Alenezi dan A. Almuqren, "Cybersecurity readiness in e-government platforms," Sustainability, vol. 14, no. 9, 2022.
<https://doi.org/10.3390/su14095231>
- [2] S. Alotaibi dan A. Almagwashi, "Information assurance for e-government systems," Journal of Information Security, vol. 14, no. 1, pp. 1-12, 2023.
<https://doi.org/10.4236/jis.2023.141001>
- [3] M. Rogers, "Cyber risk management in government digital services," Computers & Security, vol. 124, 2023.
<https://doi.org/10.1016/j.cose.2023.102996>
- [4] N. Kshetri, "Cybersecurity and public sector digital transformation," IT Professional, vol. 23, no. 1, pp. 45-52, 2021.
<https://doi.org/10.1109/MITP.2020.3035366>