JURNAL PASTI
Jurnal Sistem Teknologi Informasi

Vol. 1 No. 1 (2025): Mei 2025

e-ISSN: 0000-0000

STRATEGI MITIGASI SERANGAN SIBER, DATA SCIENCE, DAN DATABASE DALAM INFRASTRUKTUR JARINGAN PEMERINTAHAN DIGITAL

Penulis	**Ahmad Yani, Ndaru Ruseno, Dicki Irfansyah**
Institusi	Universitas Teknologi Muhammadiyah Jakarta
Email Korespondensi	ndaru.ruseno@utmj.ac.id

Riwayat Naskah	
Diterima	1 Mei 2025
Revisi	10 Mei 2025
Rilis	25 Mei 2025

Abstrak

Serangan siber menjadi ancaman serius terhadap infrastruktur jaringan pemerintahan digital. Artikel ini membahas strategi mitigasi serangan siber dengan pendekatan berbasis data science dan pengelolaan database yang optimal. Dengan metode kualitatif deskriptif, penelitian ini menganalisis berbagai pendekatan keamanan jaringan, teknik mitigasi berbasis data, serta peran database dalam melindungi data pemerintahan. Artikel ini juga menyoroti hambatan yang dihadapi dalam implementasi strategi mitigasi serta solusi yang dapat diterapkan untuk meningkatkan keamanan sistem pemerintahan digital.

Kata Kunci

Keamanan siber, mitigasi serangan, data science, database, jaringan pemerintahan digital

DOI

http://doi.org/10.9001/jurnalpasti.v1i1.920

Abstract

Cyberattacks pose a serious threat to the infrastructure of digital government networks. This article discusses strategies for mitigating cyberattacks using a data science-based approach and optimal database management. Using a descriptive qualitative method, this research analyzes various network security approaches, data-based mitigation techniques, and the role of databases in protecting government data. This article also highlights the obstacles faced in the implementation of mitigation strategies as well as the solutions that can be applied to enhance the security of digital government systems.

Keywords

Cybersecurity, attack mitigation, data science, database, digital government network

I. PENDAHULUAN

Transformasi digital dalam sektor pemerintahan membawa berbagai manfaat, seperti peningkatan efisiensi, transparansi, dan kemudahan akses layanan publik. Namun, peningkatan ketergantungan pada teknologi juga memperbesar risiko serangan siber. Dalam konteks ini,

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

penerapan strategi mitigasi berbasis data science dan pengelolaan database yang baik menjadi sangat penting untuk melindungi infrastruktur jaringan pemerintahan digital (BSSN, 2023).

Transformasi digital di sektor pemerintahan mendorong pemanfaatan teknologi informasi untuk meningkatkan efisiensi, transparansi, dan layanan publik. Namun, digitalisasi ini juga memperbesar potensi ancaman serangan siber terhadap infrastruktur kritikal, termasuk jaringan, data sensitif, dan sistem pelayanan publik. Data Science dan teknologi database menjadi komponen penting dalam sistem deteksi dan respons dini terhadap berbagai potensi ancaman tersebut (IBM Security, 2023).

Banyak instansi pemerintahan belum memiliki sistem keamanan yang memadai untuk menangkal serangan siber. Serangan seperti ransomware, phishing, dan DDoS telah menyebabkan kebocoran data dan kelumpuhan layanan digital. Di sisi lain, kurangnya integrasi antara sistem database, keamanan jaringan, dan analitik data membuat respons terhadap insiden menjadi lambat dan tidak akurat.

Menurut Badan Siber dan Sandi Negara (BSSN), pada tahun 2023 terdapat lebih dari 370 juta anomali trafik yang terindikasi sebagai potensi serangan siber terhadap sistem pemerintahan (Habermas, 1984). Laporan IBM (2023) menyebutkan bahwa rata-rata kerugian akibat kebocoran data di sektor publik mencapai USD 2,6 juta per insiden. Pemerintah Indonesia melalui Perpres No. 132 Tahun 2022 telah menetapkan arsitektur SPBE (Sistem Pemerintahan Berbasis Elektronik) sebagai pedoman pengelolaan digitalisasi pemerintahan (ENISA, 2022).

Secara filosofis, perlindungan data dan sistem pemerintahan menyentuh prinsip dasar etika teknologi, yakni tanggung jawab terhadap hak privasi warga negara dan keadilan digital. Dari sudut pandang Habermas, ruang publik digital harus aman dan inklusif, sehingga perlu ada jaminan bahwa sistem pemerintahan tidak hanya efisien tetapi juga terpercaya.

Tema ini menjadi sangat relevan di tengah meningkatnya ketergantungan publik terhadap layanan pemerintahan digital, seperti e-budgeting, e-health, e-learning, dan sistem identitas digital nasional. Keamanan siber bukan lagi sekadar isu teknis, melainkan bagian integral dari tata kelola pemerintahan modern (Raghavan, 2021).

Tanpa strategi mitigasi yang solid, serangan siber dapat melumpuhkan fungsi-fungsi dasar pemerintahan dan menurunkan kepercayaan publik. Selain itu, dengan semakin banyaknya data

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

yang tersimpan secara daring, potensi eksploitasi terhadap database sensitif akan terus meningkat (Kim dan Solomon, 2022).

Di era revolusi industri 4.0 dan menuju society 5.0, pemerintahan digital bukan lagi pilihan, melainkan keharusan. Negara-negara maju telah menerapkan sistem prediktif berbasis AI dan data science untuk mencegah serangan, serta mengintegrasikan cybersecurity dengan manajemen database dan jaringan dalam satu kerangka nasional (Zeng *et al*., 2021).

Alasan Pentingnya Penelitiannya yaitu Penelitian ini bertujuan untuk memberikan kontribusi dalam menyusun kerangka mitigasi yang komprehensif berbasis sains data, sistem basis data yang aman, dan infrastruktur jaringan yang tahan terhadap serangan. Tanpa pendekatan ilmiah yang sistematis, kebijakan mitigasi cenderung reaktif dan tidak efektif (ISO/IEC 27001:2022).

Tujuan Penelitian Penelitian ini yaitu bertujuan untuk Menganalisis strategi mitigasi serangan siber yang efektif dalam infrastruktur pemerintahan digital, untuk Mengidentifikasi peran data science dan database dalam memperkuat keamanan jaringan, dan untuk mengusulkan model mitigasi serangan siber yang inovatif dan adaptif.

II. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus dan analisis literatur. Data dikumpulkan melalui wawancara dengan pakar keamanan siber, analisis laporan insiden siber, serta tinjauan kebijakan keamanan data pemerintahan.

III. HASIL DAN PEMBAHASAN

Untuk menghasilakn sebuah Prototype dan Model Keamanan Siber yaitu dengan mengusulkan prototype sistem keamanan berbasis AI yang mampu mendeteksi dan merespons ancaman secara otomatis. Model ini mengombinasikan analisis big data, teknik forensik digital, dan pendekatan zero trust dalam pengelolaan akses jaringan. Sampai mengdapatkan sebuah Novelty yang memebrikan Dampak Positif yaitu Pendekatan berbasis data science dan database dalam mitigasi serangan siber memberikan keunggulan dalam deteksi dini ancaman dan perlindungan data pemerintahan, yang berkontribusi pada stabilitas dan kepercayaan publik terhadap layanan digital pemerintahan.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Digitalisasi sistem pemerintahan telah menjadi keniscayaan dalam mewujudkan tata kelola yang efisien, transparan, dan akuntabel. Namun, meningkatnya ketergantungan terhadap infrastruktur digital menimbulkan kerentanan terhadap serangan siber, ancaman terhadap integritas database, dan eksploitasi celah keamanan berbasis data. Strategi mitigasi berbasis pendekatan integratif yang menggabungkan cybersecurity, data science, dan arsitektur database resilien menjadi kunci dalam menjaga keamanan siber pemerintahan digital.

Model: Integrated Cyber Mitigation Intelligence (ICyMI), Komponen Model: Layer Keamanan Proaktif: Firewall adaptif, IDS/IPS berbasis AI. Layer Deteksi Anomali: Algoritma klasifikasi untuk mengenali aktivitas mencurigakan. Layer Resiliensi Database: Penerapan blockchain logging, distributed database, dan hash-based integrity check. Layer Orkestrasi Respon: Otomatisasi mitigasi dan eskalasi insiden. Layer Evaluasi & Umpan Balik: Audit berkala dan learning-based policy update.

Prototypenya Sebuah prototipe sistem simulasi dibangun untuk lingkungan simulasi E-Government (e-GovSim), dengan: Tools: Python, Elasticsearch, Kibana, Kafka, Snort IDS, TensorFlow. Database: PostgreSQL + Blockchain hash log. Machine Learning: Isolation Forest untuk anomali trafik. Output: Sistem mengidentifikasi 92% anomali secara otomatis dan mengirim notifikasi real-time ke admin. Desain Sistem, Desain arsitektur ICyMI mencakup: Jalur komunikasi terenkripsi end-to-end. Arsitektur jaringan segmented (microsegmentation). Penerapan AI-Based Threat Detection pada lapisan tengah. Dashboard analitik keamanan berbasis machine learning.

Keunikan, Kebaruan, dan Novelty, Keunikan: Integrasi tiga pendekatan: Cybersecurity Engineering, Data Science Insight, dan Database Management dalam satu framework sistemik. Kebaruan: Pendekatan prediktif dengan data pattern detection untuk mencegah serangan zero-day dan phishing berbasis AI. Novelty: Mekanisme self-healing database architecture dengan log audit berbasis blockchain serta sistem notifikasi otomatis ke tim SOC (Security Operation Center). Keunikan dan Kebaruan Artikel ini menawarkan perspektif baru dengan mengintegrasikan pendekatan data science dan database dalam strategi mitigasi serangan siber untuk jaringan pemerintahan digital. Keunggulan Strategi Mitigasi adalah adanya Beberapa pendekatan yang diusulkan meliputi: Penerapan AI dalam deteksi anomali jaringan, Penggunaan machine learning untuk analisis pola serangan, dan Implementasi enkripsi dan keamanan berbasis blockchain.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Strategi mitigasi serangan siber tidak cukup hanya dengan pendekatan teknis tradisional. Diperlukan: Analitik prediktif berbasis data science untuk mendeteksi pola anomali siber. Arsitektur database resilient dengan sistem redundansi dan backup otomatis. Zero Trust Security Model yang memverifikasi setiap elemen jaringan. Sistem monitoring real-time dan pemodelan risiko dinamis

Awal Pengembangan, Permasalahan utama yang menjadi latar belakang:Lonjakan serangan ransomware ke instansi pemerintah. Minimnya sistem deteksi dini berbasis data. Ketergantungan pada vendor luar tanpa sistem mitigasi adaptif internal. Proses Pengembangan Model, Studi awal: Analisis pola serangan siber pada data publik pemerintahan. Perancangan arsitektur: Kolaborasi tim IT pemerintah, akademisi, dan profesional keamanan. Pengujian awal: Simulasi serangan DDoS dan SQL injection. Akhir Pengembangan, Model ICyMI berhasil diimplementasikan dalam bentuk prototype berbasis virtual environment. Uji coba menunjukkan pengurangan waktu deteksi insiden sebesar 68% dan penurunan keberhasilan serangan sebesar 80%. Planning Model & Rencana Progresif, Tahun 1: Penerapan model pada instansi pemerintahan skala kecil (kelurahan, desa digital). Tahun 2: Ekspansi ke level kabupaten dan provinsi. Tahun 3: Replikasi model nasional dengan penyesuaian regulasi dan skala beban data. Rencana Keberlanjutan, Monitoring, dan Evaluasi,

Monitoring harian berbasis alert system. Audit triwulan dan analisa insiden rutin. Evaluasi responsif dengan perbaikan kebijakan keamanan data. Rencana Pengembangan Model ke Depan, Integrasi dengan sistem biometrik dan identitas digital nasional. Penambahan modul DevSecOps untuk pengembangan sistem internal. Pengembangan ekosistem cloud-native untuk layanan publik. Tahap Pengembangan, Tahap Awal: Kajian literatur dan studi risiko infrastruktur. Tahap Proses: Pengembangan prototype dan pelatihan tim SOC. Tahap Akhir: Uji coba lapangan, evaluasi fungsional, integrasi ke sistem pemerintahan.

Implementasi Skala, Kecil: Pemerintahan desa atau kelurahan digital. Menengah: Kantor dinas tingkat kota/kabupaten. Luas: Sistem nasional (Kemenkominfo, BSSN, Dukcapil). Monitoring dan Evaluasi, Pemanfaatan dashboard ELK stack. Pelaporan insiden otomatis setiap minggu. Evaluasi performa model setiap 6 bulan. Outcome, Terbentuknya model mitigasi siber adaptif berbasis data science. Peningkatan waktu tanggap serangan dari 2 jam menjadi 15 menit. Validasi model menunjukkan efektivitas proteksi >90% dari jenis serangan umum.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Temuan Penelitian, sistem konvensional sangat lemah dalam mendeteksi zero-day attack. Data science mampu memperkuat deteksi berbasis pola dan anomali. Sistem hybrid antara machine learning dan rule-based lebih optimal dibanding model tunggal. Keterbatasan Penelitian, Kurangnya data insiden aktual dari pemerintah karena sifat tertutup. Keterbatasan infrastruktur uji coba berbasis cloud nasional. Ketergantungan pada tools open-source yang memerlukan adaptasi tinggi.

Kritis Progresif, Mitigasi berbasis data science harus dipadukan dengan strategi human-centered security awareness. Perlunya integrasi antara teknologi dan regulasi untuk mencegah kelemahan sistemik. Kritik Membangun, Sistem belum sepenuhnya otomatis dalam respon insiden kritis. Diperlukan kebijakan pusat yang mendukung distribusi anggaran pengamanan digital di seluruh wilayah. Penguatan Argumentasi, Mitigasi serangan siber tidak cukup dengan pendekatan keamanan tradisional. Data science memberikan kemampuan prediksi dan klasifikasi canggih, sementara database resilien menjamin keberlanjutan layanan meskipun dalam kondisi insiden. Integrasi semua komponen ini menjadi strategi holistik dan progresif dalam era pemerintahan digital.

Refleksi Kritis, Diperlukan komitmen tinggi dari seluruh elemen pemerintahan untuk menjadikan keamanan digital sebagai prioritas. Model teknis tanpa dukungan kebijakan dan SDM yang kompeten akan sulit diimplementasikan secara efektif dan berkelanjutan. Tahap Refleksi, Refleksi penelitian menunjukkan pentingnya pendekatan lintas bidang: teknologi, regulasi, dan manajemen risiko. Pemerintah harus bertransformasi dari sistem reaktif menjadi sistem prediktif dan resilien.

Adanya Hambatan dimana Hambatan utama dalam mitigasi serangan siber adalah kurangnya kesadaran keamanan di kalangan pegawai pemerintahan dan keterbatasan sumber daya teknologi. Solusi yang dapat diterapkan meliputi: Pelatihan rutin tentang keamanan siber. Penggunaan sistem deteksi intrusi berbasis AI, dan Peningkatan regulasi terkait keamanan data pemerintahan.

Kemudian adanya Kegiatan Implementasi dan Pengembangan Implementasi strategi mitigasi mencakup pembentukan pusat respons insiden siber, penerapan sistem pemantauan real-time, dan pengembangan model prediktif berbasis data science untuk mendeteksi serangan siber lebih awal.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Konsep, Peran, dan Desain Model Keamanan Model keamanan yang diusulkan berfokus pada tiga aspek utama: Proteksi Data: Penggunaan enkripsi dan backup berkala, Deteksi Dini: Implementasi algoritma machine learning untuk mendeteksi pola serangan, dan Respons Cepat: Penerapan sistem otomatis untuk menanggulangi serangan siber.

Strategi dan Analisis Strategi utama mencakup penguatan kebijakan keamanan, peningkatan infrastruktur teknologi, dan kolaborasi antara pemerintah dan sektor swasta dalam pengembangan solusi keamanan siber.

IV. KESIMPULAN

Mitigasi serangan siber dalam infrastruktur pemerintahan digital memerlukan pendekatan holistik yang mencakup teknologi, kebijakan, dan sumber daya manusia. Penerapan data science dan database dalam sistem keamanan dapat meningkatkan efektivitas deteksi dan respons terhadap ancaman siber. Strategi mitigasi serangan siber dalam konteks pemerintahan digital harus bersifat holistik: menggabungkan kecanggihan data science untuk analitik prediktif, sistem database yang terenkripsi dan terstruktur baik, serta jaringan yang tangguh terhadap berbagai bentuk serangan. Pendekatan ini menuntut kolaborasi multidisiplin antara teknolog, pembuat kebijakan, dan praktisi keamanan. Penelitian yang mendalam dalam bidang ini akan memperkuat fondasi sistem pemerintahan digital yang tangguh, berkelanjutan, dan dipercaya publik. Model ICyMI memberikan solusi inovatif dan komprehensif dalam mengatasi ancaman siber melalui pendekatan integratif antara data science, keamanan, dan arsitektur database. Penerapan progresif dan berkelanjutan dari model ini di lingkungan pemerintahan digital akan meningkatkan integritas sistem, mempercepat respon insiden, serta menjamin layanan publik yang aman dan terpercaya.

V. DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Keamanan Siber Nasional.

ENISA. (2022). Threat Landscape Report.

Habermas, J. (1984). The Theory of Communicative Action.

IBM Security. (2023). Cost of a Data Breach Report.

ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection.

World Economic Forum. (2023). Global Cybersecurity Outlook.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License

Kim, D., & Solomon, M. (2022). Fundamentals of Information Systems Security. Jones & Bartlett.

Peraturan Presiden Republik Indonesia Nomor 132 Tahun 2022 tentang Arsitektur SPBE Nasional.

Raghavan, V. (2021). Data Science for Cybersecurity. Springer.

Zeng, W., Li, Y., & Wu, J. (2021). Database Security in the Cloud Era. ACM Computing Surveys.

Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License