PROSIDING Seminar Nasional SISFOTEK ISSN 2597-3584 (Media Online)
Sistem Informasi dan Teknologi
website : www.seminar.iaii.or.id | email : seminar@iaii.or.id

Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia

Rafli Al Ihsan[1], Binastya Anggara Sekti[2]
[1]Teknik Informatika, Fakultas Ilmu Komputer, STMIK Palangka Raya
[2]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Esa Unggul
alihsannn.skilvul@gmail.com, anggara@esaunggul.ac.id

Abstract

In the digital era, data security has become a crucial issue for many countries, including Indonesia, especially after the hacker attack on Indonesia's National Data Center exposed the vulnerability of the system and its impact on national security and public trust. This journal aims to investigate the importance of data security in the digital era with a focus on the hacker attack that occurred on the PDN. This research uses the literature study method to explore the importance of data security, analyze the level of vulnerability of the National Data Center to cyberattacks, its impact on government stability and operations, and formulate strategies and policies that can be implemented to strengthen data defense. The results show that in addition to improved security technology, strict policies and good human resource education, inter-agency cooperation and international collaboration are also very important in building a resilient security system.

Keywords: Data security, hacker attacks, Indonesia National Data Center, inter-agency cooperation, international collaboration

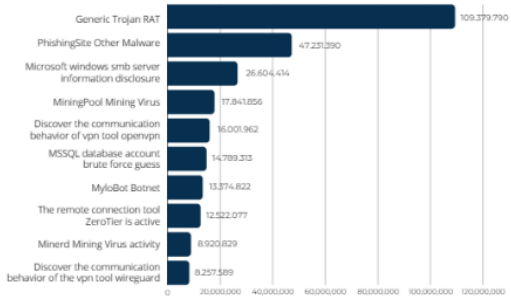
Abstrak

Dalam era digital, keamanan data menjadi isu krusial bagi banyak negara, termasuk Indonesia, terutama setelah serangan hacker terhadap Pusat Data Nasional Indonesia yang mengungkap kerentanan sistem dan dampaknya terhadap keamanan nasional serta kepercayaan publik. Jurnal ini bertujuan untuk menyelidiki pentingnya keamanan data dalam era digital dengan fokus pada serangan hacker yang terjadi pada PDN. Penelitian ini menggunakan metode studi literatur untuk mengeksplorasi pentingnya keamanan data, menganalisis tingkat kerentanan Pusat Data Nasional terhadap serangan siber, dampaknya terhadap stabilitas dan operasional pemerintahan, serta merumuskan strategi dan kebijakan yang dapat diimplementasikan untuk memperkuat pertahanan data. Hasil penelitian menunjukkan bahwa selain peningkatan teknologi keamanan, kebijakan yang ketat dan pendidikan sumber daya manusia yang baik, kerjasama antar instansi dan kolaborasi internasional juga sangat penting dalam membangun sistem keamanan yang tangguh.

Kata kunci: Keamanan data, serangan hacker, Pusat Data Nasional Indonesia, kerjasama antar instansi, kolaborasi internasional.

1. Pendahuluan

Dalam era digital yang semakin maju, keamanan data menjadi salah satu isu paling krusial yang dihadapi oleh banyak negara, termasuk Indonesia [1]. Data telah menjadi aset berharga yang berpengaruh besar terhadap berbagai sektor, mulai dari pemerintahan, bisnis, hingga kehidupan sehari-hari masyarakat. Penggunaan teknologi informasi dan komunikasi yang terus berkembang pesat membawa manfaat besar, namun juga memunculkan tantangan baru dalam hal perlindungan data. Perkembangan ini membuat keamanan data tidak hanya menjadi tanggung jawab individu atau perusahaan, tetapi juga menjadi prioritas nasional [2].



Gambar 1. Trafic Anomali

Sumber : Lanskap Keamanan Indonesia Siber 2023

Serangan hacker pada Pusat Data Nasional Indonesia beberapa waktu lalu menyoroti betapa rentannya sistem keamanan data yang ada saat ini. Pusat Data Nasional, yang menyimpan informasi sensitif dan vital bagi kelangsungan pemerintahan dan masyarakat, menjadi target utama bagi pelaku kejahatan siber [3]. Serangan ini tidak hanya mengganggu operasional pemerintahan tetapi juga menimbulkan ancaman serius terhadap keamanan nasional dan kepercayaan publik. Kejadian ini menunjukkan bahwa masih ada celah yang bisa dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab [4].

Keamanan data dalam era digital harus dipandang sebagai investasi jangka panjang yang memerlukan perhatian khusus dari pemerintah dan seluruh lapisan masyarakat [5]. Implementasi teknologi keamanan yang canggih dan up-to-date, serta peningkatan kesadaran akan pentingnya menjaga kerahasiaan data, menjadi langkah-langkah esensial yang harus segera diambil [6]. Selain itu, regulasi dan kebijakan yang tegas dalam penanganan dan pencegahan serangan siber perlu disusun dan dijalankan dengan konsisten. Pemerintah, sebagai pemegang kendali utama atas data nasional, harus berperan aktif dalam menginisiasi dan mengawasi pelaksanaan langkah-langkah ini[7].

Serangan hacker yang terjadi juga memberikan pelajaran berharga tentang pentingnya kolaborasi dan koordinasi antara berbagai pihak dalam menjaga keamanan data [8]. Kerjasama antara pemerintah, sektor swasta, dan masyarakat luas sangat diperlukan untuk membangun ekosistem keamanan data yang tangguh. Selain itu, pendidikan dan pelatihan mengenai keamanan siber harus ditingkatkan untuk menciptakan sumber daya manusia yang kompeten dan mampu menghadapi tantangan di era digital[9].

Refleksi terhadap serangan hacker pada Pusat Data Nasional Indonesia menegaskan kembali urgensi untuk memperkuat sistem keamanan data. Keamanan data bukan hanya soal melindungi informasi dari tangan-tangan yang tidak berwenang, tetapi juga menjaga stabilitas dan kepercayaan dalam pemerintahan serta melindungi kepentingan nasional [10]. Dalam konteks ini, investasi dalam teknologi keamanan, kebijakan yang ketat, dan peningkatan kesadaran masyarakat menjadi langkah-langkah penting yang harus segera diambil untuk memastikan keamanan data di era digital ini [11].

Jurnal ini bertujuan untuk membahas pentingnya keamanan data dalam era digital, dengan mengambil refleksi dari serangan hacker pada Pusat Data Nasional Indonesia. Melalui analisis literatur dari berbagai sumber, jurnal ini akan mengidentifikasi tantangan dan strategi dalam meningkatkan keamanan data. Selain itu, jurnal ini juga akan memberikan rekomendasi untuk pencegahan serangan serupa di masa mendatang.

2. Metode Penelitian

Penelitian ini akan menggunakan metode studi literatur tentang pentingnya keamanan data dalam era digital, dengan fokus pada refleksi terhadap serangan hacker pada Pusat Data Nasional Indonesia. Studi literatur ini akan melibatkan pengumpulan dan analisis berbagai sumber sekunder seperti jurnal ilmiah, buku, laporan pemerintah, dan artikel berita yang relevan. Tujuan utama dari pendekatan ini adalah untuk mendapatkan pemahaman mendalam mengenai konsep keamanan data, tantangan yang dihadapi, serta langkah-langkah mitigasi yang telah diimplementasikan di berbagai negara. Selain itu, penelitian ini juga akan meninjau studi kasus serangan hacker yang terjadi di Indonesia dan negara lain untuk mengidentifikasi pola, dampak, dan strategi yang efektif dalam mengatasi ancaman siber. Analisis ini akan memberikan gambaran komprehensif tentang upaya yang perlu dilakukan untuk meningkatkan keamanan data nasional di Indonesia

3. Hasil dan Pembahasan

Manajemen keamanan data merupakan disiplin yang berfokus pada perlindungan data dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data tersebut [7]. Teori ini mencakup berbagai aspek, termasuk kebijakan, prosedur, serta teknologi yang digunakan untuk mengelola risiko yang berhubungan dengan informasi digital. Salah satu kerangka kerja utama dalam manajemen keamanan data adalah Confidentiality, Integrity, and Availability (CIA) Triad, yang menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data. Ketiga elemen ini menjadi dasar dalam merancang strategi keamanan data yang komprehensif [4].

Kerahasiaan (confidentiality) berkaitan dengan upaya untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Untuk mencapai kerahasiaan, berbagai teknik seperti enkripsi, kontrol akses, dan otentikasi digunakan. Enkripsi, misalnya, mengubah data menjadi format yang tidak bisa dibaca tanpa kunci dekripsi yang benar, sehingga melindungi informasi dari akses yang tidak sah. Kontrol akses dan otentikasi, di sisi lain, memastikan bahwa hanya individu yang berhak yang dapat mengakses dan memodifikasi data [11].

Integritas (integrity) menekankan pentingnya menjaga keakuratan dan konsistensi data selama siklus hidupnya [9]. Ini berarti bahwa data harus dilindungi dari perubahan yang tidak sah, baik itu disebabkan oleh kesalahan manusia, kegagalan sistem, atau serangan siber. Implementasi checksum, hash functions, dan digital signatures adalah beberapa metode yang digunakan untuk memastikan integritas data. Dengan metode ini, setiap perubahan data yang tidak sah dapat terdeteksi dengan cepat, memungkinkan organisasi untuk mengambil tindakan korektif segera.

Ketersediaan (availability) mengacu pada kemampuan untuk memastikan bahwa data dan sistem informasi

selalu dapat diakses dan digunakan ketika dibutuhkan [4]. Ancaman terhadap ketersediaan dapat datang dari berbagai sumber, termasuk serangan denial-of-service (DoS), kegagalan perangkat keras, atau bencana alam. Untuk mengatasi ancaman ini, organisasi perlu mengimplementasikan strategi seperti redundancy, failover systems, dan disaster recovery planning. Dengan langkah-langkah ini, gangguan pada akses data dapat diminimalkan dan operasi bisnis dapat terus berjalan tanpa hambatan.

Selain CIA Triad, teori manajemen keamanan data juga mencakup aspek-aspek seperti manajemen risiko dan kepatuhan terhadap regulasi [12]. Manajemen risiko melibatkan identifikasi, evaluasi, dan mitigasi risiko yang berkaitan dengan data. Proses ini memerlukan penilaian yang terus-menerus terhadap ancaman dan kerentanan, serta implementasi kontrol yang sesuai untuk mengurangi risiko tersebut. Kepatuhan terhadap regulasi, seperti GDPR, HIPAA, atau UU ITE, mengharuskan organisasi untuk menerapkan langkah-langkah perlindungan data yang spesifik dan memastikan bahwa mereka mematuhi standar hukum yang berlaku.

Manajemen keamanan data menekankan pentingnya pendekatan yang sistematis dan proaktif dalam melindungi informasi. Dengan mengintegrasikan teknologi canggih, kebijakan yang kuat, dan kesadaran keamanan di seluruh organisasi, risiko yang terkait dengan data dapat diminimalkan [4]. Ini tidak hanya melindungi aset digital, tetapi juga memastikan bahwa organisasi dapat memenuhi tanggung jawabnya terhadap pemangku kepentingan dan regulator, sambil mempertahankan kepercayaan dan reputasi di pasar.

3.1 Tingkat kerentanan keamanan data di Pusat Data Nasional Indonesia terhadap serangan hacker

Tingkat kerentanan keamanan data di Pusat Data Nasional Indonesia dapat diukur melalui beberapa indikator utama, seperti kualitas infrastruktur teknologi, kebijakan keamanan siber, dan kesiapan sumber daya manusia dalam menghadapi ancaman siber [13]. Infrastruktur teknologi di Pusat Data Nasional, meskipun canggih, masih memiliki beberapa kelemahan yang bisa dimanfaatkan oleh hacker. Misalnya, penggunaan perangkat lunak yang belum diperbarui secara rutin atau sistem keamanan yang tidak mengikuti standar internasional bisa menjadi celah yang dimanfaatkan oleh pelaku kejahatan siber [14].

Kebijakan keamanan siber yang diterapkan di Pusat Data Nasional juga menjadi faktor penting dalam menentukan tingkat kerentanan [15]. Regulasi dan kebijakan yang tidak komprehensif atau kurang tegas dalam pelaksanaannya dapat meningkatkan risiko terjadinya serangan [16]. Misalnya, kebijakan yang tidak mewajibkan enkripsi data sensitif atau tidak mengatur mekanisme tanggap darurat ketika terjadi pelanggaran keamanan bisa memperbesar peluang terjadinya serangan siber yang berhasil. Selain itu, kurangnya koordinasi antara berbagai instansi pemerintah juga dapat memperlemah sistem keamanan secara keseluruhan[12].

Kesiapan sumber daya manusia di Pusat Data Nasional dalam menghadapi ancaman siber juga menjadi penentu utama tingkat kerentanan. Tenaga ahli yang tidak terlatih dengan baik atau tidak memiliki pengetahuan yang cukup mengenai teknik-teknik terbaru dalam keamanan siber akan kesulitan dalam mendeteksi dan merespons serangan [17]. Selain itu, rendahnya kesadaran dan pemahaman pegawai tentang pentingnya praktik keamanan dasar, seperti pengelolaan kata sandi yang baik dan deteksi phishing, dapat menambah kerentanan terhadap serangan.

Selain faktor internal, faktor eksternal seperti meningkatnya frekuensi dan kompleksitas serangan siber di seluruh dunia juga berkontribusi terhadap tingginya tingkat kerentanan. Hacker terus mengembangkan metode dan teknik baru untuk menembus sistem keamanan yang ada, dan Pusat Data Nasional harus selalu siap menghadapi ancaman yang semakin canggih ini [3]. Serangan yang dilakukan oleh kelompok hacker internasional yang terorganisir dengan baik seringkali menggunakan teknik-teknik yang sangat kompleks, yang memerlukan upaya ekstra dalam hal deteksi dan pencegahan.

Meskipun Pusat Data Nasional Indonesia telah melakukan berbagai upaya untuk meningkatkan keamanan data, tingkat kerentanannya masih cukup tinggi [15]. Hal ini disebabkan oleh kombinasi dari kelemahan infrastruktur teknologi, kebijakan keamanan siber yang belum optimal, kesiapan sumber daya manusia yang kurang, dan meningkatnya ancaman dari serangan siber yang semakin kompleks. Untuk mengurangi tingkat kerentanan ini, diperlukan upaya yang lebih terintegrasi dan berkelanjutan dalam semua aspek yang telah disebutkan, termasuk peningkatan teknologi, penguatan kebijakan, pelatihan sumber daya manusia, dan peningkatan koordinasi antar instansi terkait.

3.2 Dampak serangan hacker terhadap Pusat Data Nasional Indonesia

Serangan hacker terhadap Pusat Data Nasional Indonesia memiliki dampak signifikan terhadap keamanan nasional [14]. Ketika data sensitif, termasuk informasi pemerintah, strategi militer, dan data pribadi warga negara, diretas dan diakses oleh pihak yang tidak berwenang, hal ini bisa mengakibatkan kerentanan serius dalam keamanan negara. Informasi yang bocor dapat digunakan untuk melakukan berbagai tindakan yang mengancam keamanan, seperti spionase, sabotase, dan manipulasi informasi. Kejadian semacam ini tidak hanya merugikan secara langsung, tetapi juga mengurangi kemampuan pemerintah dalam menjaga stabilitas dan keamanan nasional [13].

Dampak lainnya adalah gangguan terhadap operasional pemerintahan. Pusat Data Nasional yang diserang dapat mengalami downtime atau gangguan dalam sistem yang mengelola berbagai layanan publik. Hal ini dapat mengakibatkan terganggunya pelayanan kepada masyarakat, seperti sistem administrasi kependudukan, layanan kesehatan, dan infrastruktur kritis lainnya [9]. Ketidakmampuan pemerintah untuk memberikan layanan yang efektif dapat menimbulkan ketidakpuasan

di kalangan masyarakat dan menghambat berbagai program pembangunan yang sedang berjalan.

Kepercayaan publik terhadap pemerintah juga mengalami penurunan drastis akibat serangan hacker ini. Masyarakat akan merasa bahwa data pribadi mereka tidak aman dan pemerintah tidak mampu melindungi informasi mereka dari ancaman siber [18]. Penurunan kepercayaan ini dapat berdampak pada berbagai aspek, termasuk penurunan partisipasi masyarakat dalam program pemerintah dan penurunan kepatuhan terhadap peraturan yang ada. Kepercayaan publik yang rendah juga bisa mempengaruhi stabilitas politik dan sosial dalam jangka panjang.

Selain itu, serangan hacker terhadap Pusat Data Nasional juga bisa merusak citra internasional Indonesia. Dalam era globalisasi ini, reputasi keamanan siber suatu negara sangat mempengaruhi kepercayaan negara lain, investor, dan mitra dagang. Jika Indonesia dianggap tidak mampu melindungi data nasionalnya, hal ini bisa menghambat kerjasama internasional dan investasi asing, yang pada gilirannya dapat mempengaruhi pertumbuhan ekonomi negara. Citra internasional yang buruk juga bisa mempengaruhi posisi Indonesia dalam berbagai forum global terkait keamanan siber dan teknologi[19].

Serangan hacker terhadap Pusat Data Nasional Indonesia membawa dampak yang luas dan mendalam. Keamanan nasional terancam, operasional pemerintahan terganggu, kepercayaan publik menurun, dan citra internasional rusak[5]. Oleh karena itu, sangat penting bagi pemerintah untuk mengambil langkah-langkah yang tegas dan komprehensif dalam meningkatkan keamanan data dan sistem informasi nasional. Hal ini termasuk investasi dalam teknologi keamanan canggih, pengembangan kebijakan yang kuat, serta peningkatan kapasitas sumber daya manusia dalam bidang keamanan siber.

3.3 Strategi dan kebijakan untuk memperkuat keamanan data

Untuk memperkuat keamanan data di Pusat Data Nasional Indonesia dalam menghadapi ancaman siber, diperlukan berbagai strategi dan kebijakan yang komprehensif dan terintegrasi. Salah satu strategi utama adalah meningkatkan infrastruktur keamanan siber melalui investasi dalam teknologi canggih. Penggunaan sistem enkripsi tingkat tinggi, firewall yang diperbarui secara rutin, serta deteksi intrusi otomatis adalah beberapa langkah teknis yang bisa diambil. Selain itu, penerapan teknologi berbasis kecerdasan buatan (AI) untuk mendeteksi dan merespon ancaman siber secara real-time dapat membantu mencegah serangan sebelum merusak system [17].

Kebijakan yang kuat juga sangat penting dalam upaya memperkuat keamanan data. Pemerintah perlu mengembangkan dan mengimplementasikan regulasi yang ketat terkait keamanan siber[1]. Regulasi ini harus mencakup standar keamanan minimum yang harus dipatuhi oleh semua instansi pemerintah, serta mekanisme pemantauan dan penegakan yang efektif. Kebijakan yang jelas mengenai penanganan insiden siber, termasuk prosedur tanggap darurat dan pelaporan insiden, juga harus diterapkan untuk memastikan bahwa setiap serangan dapat ditangani dengan cepat dan efisien.

Pendidikan dan pelatihan sumber daya manusia merupakan komponen penting dalam strategi keamanan data. Pusat Data Nasional perlu memastikan bahwa semua pegawainya memiliki pemahaman yang kuat tentang praktik keamanan siber dan dilatih untuk mengenali dan merespon ancaman potensial. Program pelatihan reguler, sertifikasi dalam bidang keamanan siber, dan peningkatan kesadaran akan pentingnya menjaga kerahasiaan data adalah beberapa langkah yang bisa diambil. Selain itu, kolaborasi dengan institusi pendidikan untuk mengembangkan kurikulum keamanan siber dapat membantu membangun generasi baru yang siap menghadapi tantangan siber [9].

Kerjasama dan koordinasi antar berbagai instansi pemerintah dan sektor swasta juga sangat diperlukan. Pembentukan tim tanggap darurat siber nasional yang melibatkan berbagai pemangku kepentingan dapat membantu mempercepat respons terhadap serangan dan meminimalkan dampaknya [13]. Selain itu, kerjasama internasional dengan negara-negara lain dan organisasi global dalam berbagi informasi tentang ancaman siber dan praktik terbaik dalam keamanan data dapat memperkuat pertahanan siber nasional.

Dalam memastikan bahwa strategi dan kebijakan yang diimplementasikan tetap relevan dan efektif, diperlukan evaluasi dan penyesuaian secara berkala [8]. Penilaian risiko yang rutin, audit keamanan, dan simulasi serangan siber dapat membantu mengidentifikasi kelemahan dalam sistem dan menguji kesiapan respon terhadap insiden. Dengan pendekatan yang proaktif dan adaptif, Pusat Data Nasional Indonesia dapat terus memperkuat pertahanannya terhadap ancaman siber yang terus berkembang, memastikan keamanan data nasional, dan menjaga kepercayaan publik.

4. Kesimpulan

Keamanan data dalam era digital menjadi sangat penting, terutama bagi entitas vital seperti Pusat Data Nasional Indonesia. Serangan hacker yang berhasil menembus sistem ini dapat memiliki dampak serius terhadap keamanan nasional, operasional pemerintahan, kepercayaan publik, dan citra internasional Indonesia. Oleh karena itu, strategi yang komprehensif dan kebijakan yang kuat diperlukan untuk memperkuat pertahanan data nasional. Meningkatkan infrastruktur teknologi dengan sistem keamanan canggih, seperti enkripsi dan deteksi intrusi otomatis, merupakan langkah awal yang penting. Selain itu, pengembangan regulasi yang ketat dan penerapan kebijakan yang jelas mengenai penanganan insiden siber akan membantu memastikan bahwa sistem keamanan tetap kuat dan responsif terhadap ancaman. Pendidikan dan pelatihan sumber daya

manusia juga sangat penting dalam strategi keamanan data. Dengan meningkatkan pemahaman dan kesadaran pegawai mengenai praktik keamanan siber, serta menyediakan program pelatihan reguler, Pusat Data Nasional dapat membangun tim yang siap menghadapi ancaman siber. Kolaborasi dan koordinasi antara berbagai instansi pemerintah, sektor swasta, dan mitra internasional akan memperkuat upaya pertahanan siber. Tim tanggap darurat siber nasional dan kerjasama internasional dalam berbagi informasi tentang ancaman dan praktik terbaik akan membantu dalam menghadapi tantangan yang semakin kompleks. Pendekatan yang proaktif, integratif, dan adaptif dalam mengimplementasikan strategi dan kebijakan keamanan siber akan memastikan bahwa Pusat Data Nasional Indonesia dapat melindungi data sensitif dan menjaga stabilitas serta kepercayaan publik. Upaya berkelanjutan dan penyesuaian rutin terhadap kebijakan dan teknologi keamanan akan memperkuat pertahanan data nasional di era digital yang terus berkembang.

Daftar Rujukan

[1] S. B. Far and A. I. Rad, "Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges," *J. Metaverse* , vol. 2, no. 1, pp. 8–15, 2022.

[2] I. Kickbusch *et al.*, "The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world," *Lancet*, vol. 398, no. 10312, pp. 1727–1776, 2021, doi: 10.1016/S0140-6736(21)01824-9.

[3] E. Sundari, "TRANSFORMASI PEMBELAJARAN DI ERA DIGITAL: MENGINTEGRASIKAN TEKNOLOGI DALAM PENDIDIKAN MODERN," *Cendekia Pendidik.*, vol. 3, no. 6, pp. 101–112, 2024.

[4] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber Di Era Digital," *J. Bus. Entrep.*, vol. 11, no. 1, p. 23, 2023, doi: 10.46273/jobe.v11i1.365.

[5] N. A. Perifanis and F. Kitsios, "Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review," *Inf.*, vol. 14, no. 2, 2023, doi: 10.3390/info14020085.

[6] S. A. M. Babys, "Ancaman Perang Siber di Era Digital dan Solusi Keamanan Indonesia," *J. Oratio Directa*, vol. 3, no. 1, pp. 425–442, 2021, [Online]. Available: https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163

[7] B. T. Azzahrah, M. Naufal, R. Hamdi, R. Raynee, and Z. Layla, "Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi," vol. 8, pp. 23934–23943, 2024.

[8] R. firdaus M. Aulia Fitra Purba, "Peran dan Tantangan Sistem Informasi Manajemen dalam Era Digital : Tinjauan Literatur The Role and Challenges of Management Information Systems in the Digital Age : A Literature Review," *JICN J. Intelek dan Cendikiawan Nusant.*, vol. 01, no. 03, pp. 4302–4309, 2024.

[9] E. Ahyani and E. M. Dhuhani, "Transformasi Digital dalam Manajemen Perkantoran Pendidikan: Sebuah Kajian Literatur," *J. Vision. Penelit. dan Pengemb. dibidang Adm. Pendidik.*, vol. 12, no. 1, p. 205, 2024, doi: 10.33394/vis.v12i1.10785.

[10] M. Yudistira and Ramadhan, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo," *Unes Law Rev.*, vol. 5, no. 4, pp. 3802–3815, 2023, [Online]. Available: https://doi.org/10.31933/unesrev.v5i4

[11] E. Budi, D. Wira, and A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[12] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," *SAMMAJIVA J. Penelit. Bisnisdan Manaj.*, vol. 1, no. 2, p. 186, 2023.

[13] E. Kalim, "Tantangan Dan Solusi Dalam Pengelolaan Arsip Di Era Digital," *J. Ekon. dan Bisnis Digit.*, vol. 02, no. 01, pp. 16–20, 2023.

[14] Aan Setiadarma, Ahmad Zaki Abdullah, Priyono Sadjijo, and Dwi Firmansyah, "Tinjauan Literatur Transformasi Sosial dalam Era Virtual," *Khatulistiwa J. Pendidik. dan Sos. Hum.*, vol. 4, no. 1, pp. 232–244, 2024, doi: 10.55606/khatulistiwa.v4i1.2930.

[15] M. Faqih Febriansyah, R. Setiawan, and T. Sutabri, "IJM: Indonesian Journal of Multidisciplinary Kemudahan dan Keamanan Dalam Rumah Pintar: Tinjauan Terhadap Teknologi Smart Home," *IJM Indones. J. Multidiscip.*, vol. 2, pp. 24–31, 2024, [Online]. Available: https://journal.csspublishing/index.php/ijm

[16] S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia," *Telecommun. Networks, Electron. Comput. Technol.*, vol. 1, no. 2, pp. 85–92, 2021.

[17] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

[18] A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustain.*, vol. 13, no. 6, pp. 1–19, 2021, doi: 10.3390/su13063196.

[19] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.