Journal of Renewable Energy and Smart Device (JORESD)

ISSN: 3026-216X
Vol. 3, No. 1, May 2025

Strategi Pemulihan Data dalam Sistem Terdistribusi terhadap Ancaman Siber (Studi pada Jurusan Teknik Informatika dan Komputer

Muhammad Zulfahrizi Zubair[1], Veronika Asri Tandirerung[2*], Sarmila Aulia[3], Hilda Anria[4], Bagus Ardiansyah[5], Bunga Mawar Jamaluddin[6]

[1,2,3,4,5,6]Universitas Negeri Makassar
[(*)]Coresponding Author E-mail: veronika.asri@unm.ac.id

ARTICLE HISTORY

Received :
Revised :
Accepted :

ABSTRACT

Ancaman siber menjadi tantangan utama dalam pengelolaan data pada sistem terdistribusi, khususnya di lingkungan akademik seperti jurusan teknik. Artikel ini bertujuan untuk mengidentifikasi permasalahan keamanan data yang dihadapi serta merancang strategi pemulihan data yang efektif terhadap potensi serangan siber. Metode yang digunakan adalah studi kualitatif melalui observasi, wawancara, dan analisis dokumentasi di lingkungan jurusan teknik. Hasil penelitian menunjukkan bahwa sistem saat ini belum memiliki mekanisme pemulihan data yang memadai dan rentan terhadap serangan seperti ransomware dan distributed denial-of-service (DDoS). Strategi pemulihan data yang diusulkan meliputi penerapan backup data terjadwal, penggunaan teknologi enkripsi, segmentasi jaringan, serta peningkatan literasi keamanan siber bagi pengelola sistem. Dengan menerapkan strategi ini, ketahanan sistem terhadap ancaman siber dapat ditingkatkan secara signifikan, sekaligus menjamin kontinuitas layanan data dan informasi akademik. Studi ini memberikan kontribusi praktis bagi pengembangan kebijakan keamanan data di lingkungan pendidikan tinggi yang semakin terdigitalisasi.

Keywords: Pemulihan Data, Sistem Terdistribusi, Ancaman Siber, Keamanan Informasi, Redundansi Data

1. PENDAHULUAN

Di era digital yang semakin kompleks, sistem terdistribusi telah menjadi tulang punggung infrastruktur teknologi informasi, termasuk dalam lingkungan akademik seperti jurusan Teknik Informatika dan Komputer. Sistem ini memungkinkan penyimpanan dan pengolahan data secara terdistribusi di berbagai node, meningkatkan efisiensi dan ketersediaan layanan. Namun, peningkatan konektivitas dan kompleksitas ini juga membawa risiko keamanan yang signifikan, terutama terhadap ancaman siber yang dapat mengganggu integritas, ketersediaan, dan kerahasiaan data[1].

Tingginya jumlah pengguna internet di Indonesia yang mencapai sekitar 204,7 juta pengguna atau tingkat penetrasi sebesar 73,3 persen per Januari 2022, semestinya diiringi dengan kebijakan keamanan siber yang matang dan terintegrasi[11]. Sayangnya, kondisi keamanan siber di Indonesia masih sangat lemah dan menghadapi banyak paradoks kebijakan. Pemilihan satu arah kebijakan sering kali mengorbankan arah lain, sementara terdapat argumen yang kuat untuk menggabungkan keduanya. Lebih lanjut, kemajuan teknologi telah membawa konflik ke ranah dunia maya, menciptakan medan cyber yang pada akhirnya tetap dapat berujung pada dampak fisik. Selain itu, keamanan siber juga meninjau aktivitas internet oleh anak-anak dan mengidentifikasi lima kategori risiko utama yang mereka hadapi: risiko konten, risiko kontak, anak-anak sebagai target konsumen, risiko ekonomi, dan risiko privasi online[8].Serangan seperti Distributed Denial of Service (DDoS), malware, dan ransomware telah menjadi

ancaman nyata yang dapat menyebabkan kerugian besar, baik secara finansial maupun reputasi[2].

Keamanan informasi adalah upaya melindungi data dan sistem dari akses atau tindakan tidak sah guna menjaga kerahasiaan, integritas, dan ketersediaannya[12]. Tujuannya untuk menjaga kerahasiaan, integritas, dan ketersediaan data, sehingga informasi tetap akurat, tidak diubah tanpa izin, dan dapat diakses oleh pihak yang berhak saat dibutuhkan. Peran keamanan siber semakin penting seiring dengan peningkatan penggunaan komputer seperti desktop, laptop, ponsel pintar, server, dan perangkat Internet of Things (IoT), serta penggunaan jaringan komputer seperti Internet dalam kehidupan sehari-hari. Keamanan informasi memainkan peran kunci dalam manajemen perusahaan, karena menangani kerahasiaan, privasi, integritas, dan ketersediaan salah satu sumber daya terpenting[5].

Oleh karena itu, dalam konteks sistem terdistribusi, perhatian terhadap aspek keamanan informasi menjadi semakin penting sebagai respons terhadap meningkatnya ancaman digital[6]. Pengembangan strategi keamanan data yang efektif tidak hanya memerlukan pendekatan teknis, tetapi juga menuntut integrasi aspek kebijakan, regulasi, dan pendidikan pengguna. Model seperti NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) telah menjadi acuan penting karena mampu menggabungkan pendekatan preventif dan responsif secara sistematis dalam menghadapi ancaman siber[7].Efektivitas program kesadaran keamanan siber dapat diukur secara internal dan eksternal bagi sebuah organisasi. Pengukuran efisiensi internal dapat mencakup kesadaran endpoint, pemantauan proaktif terhadap ancaman dan kerentanan, arsitektur keamanan, tata kelola keamanan siber, serta kepatuhan hukum dan regulasi[9].

Pendidikan tinggi telah menjadi target yang menguntungkan bagi serangan siber, dengan banyak institusi yang sudah mengalami insiden berdampak tinggi[10]. Meskipun berbagai upaya telah dilakukan untuk meningkatkan keamanan sistem terdistribusi, masih terdapat tantangan dalam mengembangkan strategi pemulihan data yang efektif setelah terjadinya serangan siber[1]. Banyak institusi pendidikan, termasuk jurusan Teknik Informatika dan Komputer, mengalami tantangan dalam pemulihan data akibat serangan siber. Hal ini terutama disebabkan oleh kurangnya protokol pemulihan data yang terintegrasi dan adaptif terhadap berbagai jenis ancaman. Keberadaan ancaman siber yang sering terjadi seperti hacking, cracking, ATM skimming, cybersquatting, terorisme, pinjaman online, kejahatan carding (credit card fraud), malware (virus/bots/worm), human trafficking phishing (internet banking fraud), dan serangan siber lainnya semakin meningkat seiring dengan perkembangan teknologi informasi[13]. Penelitian menunjukkan bahwa serangan phishing dapat menyebabkan kerugian signifikan bagi mahasiswa dengan mengakses dan mengungkap informasi sensitif[14].

Penelitian sebelumnya telah menemukan sejumlah metode yang dapat diterapkan guna memperkuat perlindungan pada sistem terdistribusi. Sebagai contoh, teknologi deteksi intrusi yang mengandalkan pola tanda tangan dan deteksi anomali, serta integrasi metode pembelajaran mesin, telah banyak digunakan sebagai strategi utama dalam memperkuat keamanan pada sistem distribusi Linux[3]. Selain itu, penerapan sistem keamanan jaringan berbasis cybersecurity, seperti Intrusion Detection Systems (IDS) SNORT dan penerapan Artificial Intelligence (AI) dalam mendeteksi ancaman berbasis perilaku, telah menunjukkan efektivitas dalam mengurangi ancaman siber pada infrastruktur TI[4]. Meskipun berbagai pendekatan telah dikembangkan, masih terdapat kesenjangan dalam implementasi strategi pemulihan data yang komprehensif dan adaptif terhadap berbagai jenis serangan siber. Penelitian sebelumnya umumnya lebih berfokus pada tindakan preventif dan deteksi serangan siber, sementara strategi pemulihan data pasca pelanggaran masih minim dikaji secara komprehensif, terutama dalam mencakup area pemulihan pelanggan, proses, karyawan, dan regulasi[15].

Berdasarkan analisis permasalahan yang telah dikemukakan sebelumnya, penelitian ini akan difokuskan pada strategi pemulihan data dalam sistem terdistribusi yang relevan dengan

kebutuhan institusi pendidikan tinggi, khususnya di lingkungan Jurusan Teknik Informatika dan Komputer. Fokus utama penelitian ini adalah merumuskan strategi yang efektif dalam menghadapi berbagai jenis serangan siber seperti Distributed Denial of Service (DDoS), malware, dan ransomware yang semakin kompleks dan merugikan. Selain itu, strategi yang dikembangkan diharapkan mampu bersifat adaptif terhadap dinamika dan perubahan lingkungan sistem terdistribusi, yang mencakup tantangan teknis maupun non-teknis di ruang lingkup institusi pendidikan. Penelitian ini juga mempertimbangkan keterbatasan sumber daya yang sering dihadapi oleh jurusan, baik dari segi infrastruktur, personel teknis, maupun kebijakan institusional, sehingga strategi yang dirancang tidak hanya bersifat teoritis, tetapi juga realistis untuk diterapkan.

Penelitian ini akan mengusulkan strategi pemulihan data yang mengintegrasikan teknologi deteksi dan pencegahan intrusi, enkripsi data, serta manajemen identitas dan akses yang efektif. Pendekatan ini akan dirancang dengan menyesuaikan kebutuhan dan karakteristik lingkungan akademik, khususnya di institusi pendidikan tinggi seperti Jurusan Teknik Informatika dan Komputer. Tujuan utamanya adalah untuk meningkatkan ketahanan sistem terdistribusi terhadap berbagai bentuk ancaman siber dan memastikan kontinuitas layanan pendidikan, terutama dalam aspek pengelolaan dan perlindungan data yang krusial.

Sebagai langkah awal, penelitian ini akan dilakukan melalui penyebaran kuesioner kepada mahasiswa Jurusan Teknik Informatika dan Komputer sebagai subjek penelitian. Metode ini dipilih untuk menggali persepsi, pengalaman, serta pemahaman mahasiswa terhadap strategi pemulihan data dalam konteks sistem terdistribusi dan ancaman siber. Selain itu, kuesioner ini juga bertujuan untuk menilai tingkat kesiapan mahasiswa dalam menghadapi insiden keamanan siber, serta sejauh mana mereka memahami pentingnya upaya pemulihan data. Hasil dari penyebaran kuesioner tersebut akan dianalisis secara kuantitatif dan digunakan sebagai dasar dalam perumusan strategi pemulihan data yang tepat sasaran, realistis, dan sesuai dengan kondisi nyata di lingkungan akademik.

2. Metodologi

Penelitian ini menggunakan pendekatan kuantitatif dengan metode analisis deskriptif yang bertujuan untuk mengukur dan menganalisis persepsi serta pemahaman mahasiswa terhadap strategi pemulihan data dalam sistem terdistribusi terhadap ancaman siber. Objek dalam penelitian ini adalah strategi pemulihan data yang relevan dengan konteks akademik di Jurusan Teknik Informatika dan Komputer, Universitas Negeri Makassar. Fokus penelitian mencakup efektivitas strategi dalam menghadapi berbagai bentuk serangan siber seperti DDoS, malware, dan ransomware, kemampuan adaptasi terhadap perubahan lingkungan sistem terdistribusi, serta pertimbangan terhadap keterbatasan sumber daya yang tersedia. Populasi dalam penelitian ini adalah seluruh mahasiswa aktif Jurusan Teknik Informatika dan Komputer, sedangkan sampel ditentukan secara acak sederhana dengan mempertimbangkan keterwakilan angkatan dan minat terhadap bidang keamanan informasi. Instrumen penelitian berupa kuesioner tertutup berbasis skala Likert, yang dirancang untuk mengeksplorasi aspek pengetahuan, kesiapan, dan pengalaman mahasiswa dalam menghadapi gangguan keamanan digital serta pemulihan data. Teknik pengumpulan data dilakukan melalui penyebaran kuesioner secara daring menggunakan Google Form. Selanjutnya, data dianalisis menggunakan teknik statistik deskriptif dengan bantuan perangkat lunak SPSS, guna memperoleh gambaran umum mengenai kecenderungan jawaban responden yang akan menjadi dasar dalam merumuskan strategi pemulihan data yang tepat, kontekstual, dan aplikatif.

3. HASIL DAN PEMBAHASAN

Descriptive Statistics

Descriptive Statistics

	Valid	Missing	Median	Mean	Std. Deviation	Range	Minimum	Maximum	Sum
SPD	100	0	3,750	3,717	0.679	3,000	2,000	5,000	371,750
PMS	100	0	2,500	2,975	1,031	3,000	1,500	4,500	297,500
KMS	100	0	3,500	3,520	0.631	3,250	1,750	5,000	352,000
PSPD	100	0	4,000	4,110	0.677	2,500	2,500	5,000	411,000

Gambar 1. Statistik Deskriptif Indikator Penelitian

Gambar 1 menunjukkan statistik deskriptif dari empat variabel utama dalam penelitian terkait Strategi Pemulihan Data dalam Sistem Terdistribusi terhadap Ancaman Siber, yaitu SPD (Strategi Pemulihan Data), PMS (Persepsi Mahasiswa terhadap Sistem), KMS (Keamanan Media Simpan), dan PSPD (Persepsi terhadap Sistem Pemulihan Data).

Variabel PSPD mencatat rata-rata tertinggi sebesar 4,110, yang mengindikasikan bahwa responden sangat positif terhadap sistem pemulihan data yang ada. Disusul oleh SPD (3,717), KMS (3,520), dan yang paling rendah adalah PMS (2,975), menunjukkan bahwa persepsi terhadap sistem secara umum masih tergolong sedang.

Nilai standar deviasi terbesar terdapat pada PMS (1,031), menunjukkan adanya keragaman persepsi mahasiswa terhadap sistem yang digunakan, sementara KMS memiliki standar deviasi terendah (0,631), mencerminkan konsistensi penilaian terhadap keamanan media simpan. Dari segi total skor (sum), PSPD kembali menempati posisi tertinggi (411.000), memperkuat posisi indikator ini sebagai aspek yang paling mendapat perhatian dan kepercayaan dari responden. Sementara itu, nilai minimum terendah terdapat pada PMS (1.500), yang menandakan adanya responden yang menilai sangat rendah terhadap sistem yang digunakan.

Secara keseluruhan, data ini menggambarkan bahwa sistem pemulihan data dalam konteks sistem terdistribusi dipandang efektif oleh mahasiswa, namun perlu ada peningkatan pada aspek sistem yang mereka gunakan, terutama dalam membangun persepsi dan pengalaman pengguna terhadap sistem tersebut.

Descriptive Statistics

Descriptive Statistics

	Valid	Missing	Median	Mean	Std. Deviation	Variance	Range	Minimum	Maximum	Sum
SPD1	100	0	5,000	4,040	1,717	2,948	4,000	1,000	5,000	404,000
SPD2	100	0	4,000	3,770	0.802	0.644	4,000	1,000	5,000	377,000
SPD3	100	0	4,000	3,830	0.829	0.688	4,000	1,000	5,000	383,000
SPD4	100	0	3,000	3,230	0.908	0.825	4,000	1,000	5,000	323,000
PMS1	100	0	4,000	3,470	0.771	0.595	4,000	1,000	5,000	347,000
PMS2	100	0	1,000	2,480	1,941	3,767	4,000	1,000	5,000	248,000
KMS1	100	0	4,000	3,630	0.861	0.741	4,000	1,000	5,000	363,000
KMS2	100	0	3,000	3,290	0.902	0.814	4,000	1,000	5,000	329,000
KMS3	100	0	3,000	3,250	0.914	0.836	4,000	1,000	5,000	325,000
KMS4	100	0	4,000	3,910	0.793	0.628	3,000	2,000	5,000	391,000
PSPD 1	100	0	4,000	4,020	0.791	0.626	3,000	2,000	5,000	402,000
PSPD 2	100	0	4,000	4,060	0.814	0.663	3,000	2,000	5,000	406,000
PSPD 3	100	0	4,000	4,180	0.757	0.573	2,000	3,000	5,000	418,000
PSPD 4	100	0	4,000	4,180	0.796	0.634	3,000	2,000	5,000	418,000

Gambar 2. Statistik Deskriptif Item Penyataan Penelitian

Gambar 2 ini menunjukkan statistik deskriptif dari sub-indikator dalam empat variabel utama yang berkaitan dengan strategi pemulihan data dalam sistem terdistribusi terhadap

ancaman siber, yaitu SPD (Strategi Pemulihan Data), PMS (Persepsi Mahasiswa terhadap Sistem), KMS (Keamanan Media Simpan), dan PSPD (Persepsi terhadap Sistem Pemulihan Data).

Sub-indikator PSPD4 mencatat rata-rata tertinggi (4,180), diikuti oleh SPD1 (4,040), yang menandakan bahwa mahasiswa memberikan penilaian sangat positif terhadap efektivitas pemulihan data dan keandalan sistem dalam menghadapi gangguan siber. Sebaliknya, PMS2 (2,480) menunjukkan bahwa masih ada keraguan mahasiswa terhadap aspek sistem yang digunakan.

SPD1 juga memiliki standar deviasi tertinggi (1,717), mencerminkan perbedaan pandangan yang cukup signifikan mengenai strategi pemulihan yang digunakan. Sedangkan PSPD3 (0,757) memiliki penyebaran nilai yang paling seragam. Dari total skor, PSPD4 dan PSPD2 (418.000) menjadi yang tertinggi, menunjukkan konsistensi persepsi positif terhadap sistem pemulihan data.

Data ini secara umum menunjukkan bahwa meskipun mahasiswa menilai tinggi strategi dan sistem pemulihan data, terdapat aspek teknis dan sistem yang masih membutuhkan penguatan, khususnya dalam membangun kepercayaan dan persepsi terhadap sistem yang digunakan dalam menghadapi ancaman siber.

4. KESIMPULAN DAN SARAN

Penelitian ini menyoroti pentingnya strategi pemulihan data dalam sistem terdistribusi di lingkungan akademik, khususnya di Jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar, sebagai respons terhadap meningkatnya ancaman siber. Berdasarkan hasil kuesioner, dapat disimpulkan bahwa mahasiswa memiliki kebutuhan dan ketergantungan tinggi terhadap teknologi, serta menyadari pengaruh signifikan yang dimiliki oleh sistem informasi terhadap kegiatan harian mereka. Namun, ditemukan pula bahwa masih terdapat kendala teknis seperti gangguan jaringan dan kekhawatiran terhadap keamanan data yang menunjukkan perlunya penguatan sistem pemulihan data.

Berdasarkan hasil penelitian ini, disarankan agar penelitian selanjutnya dapat menguji secara langsung efektivitas strategi pemulihan data yang telah dirumuskan, khususnya dalam menghadapi skenario serangan nyata seperti DDoS, malware, dan ransomware. Selain itu, penting untuk memperluas ruang lingkup penelitian dengan menambahkan variabel lain seperti kesiapan institusi, pelatihan sumber daya manusia, serta dukungan kebijakan yang dapat memperkuat penerapan strategi tersebut.

REFERENSI

[1] A. F. D. Suryawan, F. G. D. Putra, V. A. Lovely, and A. Setiawan, “Keamanan IoT dan Sistem Terdistribusi,” *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 10, 2024, doi: 10.47134/pjise.v1i3.2619.

[2] A. Aryapranata, Y. Al Rasyid, Y. P. Agsena, and S. Hermanto, “Keamanan Siber dalam Era Digital : Tantangan dan Solusi,” vol. 8, no. 2, pp. 109–114, 2024.

[3] S. Mufti Prasetiyo, S. Familia Ulu, H. Simatupang, and J. K. Nahak, “BIIKMA : Buletin Ilmiah Ilmu Komputer dan Multimedia Keamanan Siber Pada Distribusi Linux: Studi Kasus Dan Solusi Efektif,” vol. 2, no. 1, pp. 72–76, 2024, [Online]. Available: www.divakaraoke.co.id

[4] P. A. Khairunnisa, N. Annisa, and Y. J. Parhusip, “Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia,” vol. 4, pp. 9–16, 2024.

[5] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, “Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal,” J. Cybersecurity

Priv., vol. 1, no. 2, Art. no. 2, Jun. 2021, doi: 10.3390/jcp1020012.
[6] Muslim, A. Sephira, M. H. Abrar, S. L. S. P. Angin, and H. Hidayatullah, “Analisis Keamanan Siber (Cyber Security) Dalam Era Digital ‘Tantangan Dan Strategi Pengamanan,’” J. Ilmu Komput. Revolusioner, vol. 8, no. 2, Art. no. 2, Feb. 2024, Accessed: Apr. 02, 2024. [Online]. Available: https://com.ojs.co.id/index.php/jikr/article/view/116
[7] R. P. Azhari, *“Metodologi Penelitian dalam Pengembangan Keamanan Data untuk Sistem Informasi,”* Preprint, 2024
[8] Aziz, A. (2023). Pentingnya pengetahuan cyber security untuk publik dan negara (The importance of cyber security knowledge for the public and the country). Jurnal Prosiding SAINTEK: Sains Dan Teknolog, 2(1), 75–82
[9] Dube, D. P., & Mohanty, R. P. (2022). Application of grounded theory in construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models. Organizational Cybersecurity Journal: Practice, Process and People, (ahead-of-print). https://doi.org/10.1108/OCJ-04-2022-0009
[10] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.
[11] A. H. Simorangkir and A. J. S. Runturambi, “Budaya & Masyarakat Digital dalam Ketahanan Siber di Indonesia: Sebuah Adaptasi dari Pendekatan Capacity Maturity Model (CMM),” *J. Manaj. dan Pendidik. Ilmu Sos.*, vol. 5, no. 4, pp. 922–934, Jun.–Jul. 2024, doi: 10.38035/jmpis.v5i4.
[12] S. Nurul, S. Anggrainy, and S. Aprelyani, “Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi, dan network (Literature Review SIM),” *J. Ekon., Manaj., dan Sist. Inform.*, vol. 3, no. 5, pp. 564–577, May 2022, doi: 10.31933/jemsi.v3i5.
[13] S. Parulian, D. A. Pratiwi, dan M. C. Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia," *Telecommunications, Networks, Electronics, and Computer Technologies*, vol. 1, no. 2, pp. 85–92, Des. 2021.
[14] B. Gumay, A. Hendrawan, & F. Kusumah, "Analisis dampak ancaman cybercrime terhadap data mahasiswa pada serangan web phising siak uika", Infotech Journal, vol. 10, no. 2, p. 297-305, 2024. https://doi.org/10.31949/infotech.v10i2.11463
[15] Z. Mohammed, "Data breach recovery areas: An exploration of organization's recovery strategies for surviving data breaches," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 2, no. 1, pp. 41–59, 2022. doi: 10.1108/OCJ-05-2021-0014.