Jurnal Informatika dan Tekonologi Komputer

E-ISSN: 2809-9230
P-ISSN: 2809-9249

Pengembangan Sistem Keamanan berbasis Cloud dengan Analisis Efek Avalanche pada Jaringan Perusahaan yang Mengadopsi Infrastruktur Cloud

Fauzan Prasetyo Eka Putra[1], Fahri Khusaini[2], Amsori[3], Khoirul Anam[4*]

[1] Informatika, Fakultas Teknik, Universitas Madura; Pamekasan, Jawa Timur; e-mail : prasetyo@unira.ac.id
[2] Informatika, Fakultas Teknik, Universitas Madura; Pamekasan, Jawa Timur; e-mail : fahrikhusaini77@gmail.com
[3] Informatika, Fakultas Teknik, Universitas Madura; Pamekasan, Jawa Timur; e-mail : amsoriabbeu2@gmail.com
[4] Informatika, Fakultas Teknik, Universitas Madura; Pamekasan, Jawa Timur; e-mail : khoirulanam44@gmail.com
* Corresponding Author : Khoirul Anam

Abstract: By adding cloud infrastructure to the company's network, there are new challenges for data security, especially related to the increasing possibility of complex cyberattacks.The main weakness of traditional systems is their inability to detect small changes in data, which can lead to data breaches.The purpose of this article is to build a cloud-based network defense system that utilizes avalanche effect analysis to enhance anomaly detection.Cryptographic algorithms with high avalanche effects are used in the simulation of cloud-based corporate networks in this study.After simulating attacks on the tested system, data is collected and then analyzed to evaluate the effectiveness and sensitivity of detection.To conduct validation tests, metrics such as detection accuracy and response time are used to compare the system's performance with conventional methods.The research results show that the use of algorithms with significant avalanche effects can enhance the system's ability to detect small suspicious changes in data, thereby reducing the likelihood of hidden attacks.The results show that adding avalanche features to the cloud defense system can enhance the company's network defense against current threats.Additionally, it has been proven that the developed system enhances operational efficiency without compromising network performance.To enhance adaptation to new attack patterns and test the system on a real implementation scale, further research must be conducted.

Keywords: Network Security, Cloud Computing, Avalanche Effect, Defense Systems, Cloud Infrastructure

Received: May 30, 2025
Revised: May 30, 2025
Accepted: July 6, 2025
Published: July 10, 2025
Curr. Ver.: July 10, 2025

Abstrak: Dengan menambahkan infrastruktur cloud ke jaringan perusahaan, ada tantangan baru untuk keamanan data, terutama terkait dengan kemungkinan serangan siber yang semakin kompleks. Kelemahan utama sistem tradisional adalah ketidakmampuan mereka untuk mendeteksi perubahan kecil dalam data, yang dapat menyebabkan kebocoran data. Tujuan dari artikel ini adalah untuk membangun sistem pertahanan jaringan berbasis cloud yang memanfaatkan analisis efek avalanche untuk meningkatkan deteksi anomali. Algoritma kriptografi dengan efek avalanche tinggi digunakan dalam simulasi jaringan perusahaan berbasis cloud dalam penelitian ini. Setelah simulasi serangan terhadap sistem yang diuji, data dikumpulkan dan kemudian dianalisis untuk mengevaluasi efektivitas dan sensitivitas deteksi. Untuk melakukan uji validasi, metrik seperti akurasi deteksi dan waktu respons digunakan untuk membandingkan kinerja sistem dengan metode konvensional. Hasil penelitian menunjukkan bahwa penggunaan algoritma dengan efek avalanche signifikan dapat meningkatkan kemampuan sistem untuk menemukan perubahan kecil yang mencurigakan dalam data, sehingga mengurangi kemungkinan serangan yang tersembunyi. Hasilnya menunjukkan bahwa menambahkan

fitur avalanche ke dalam sistem pertahanan cloud dapat meningkatkan pertahanan jaringan perusahaan terhadap ancaman saat ini. Selain itu, telah terbukti bahwa sistem yang dikembangkan meningkatkan efisiensi operasional tanpa mengurangi kinerja jaringan. Untuk meningkatkan adaptasi terhadap pola serangan baru dan menguji sistem dalam skala implementasi nyata, penelitian lebih lanjut harus dilakukan.

Kata kunci: Keamanan jaringan, Cloud Computing, Efek avalanche, Sistem pertahanan, Infrastruktur Cloud

1. Pendahuluan

Banyak bisnis telah memutuskan untuk menggunakan infrastruktur berbasis cloud sebagai akibat dari kemajuan teknologi informasi[1] yang pesat. Infrastruktur berbasis cloud memungkinkan pemrosesan dan penyimpanan data secara terdistribusi[2], [3], serta akses ke data secara real-time dari berbagai lokasi. Namun, meskipun mudah dan efektif, ada masalah besar terkait keamanan data dan pertahanan jaringan[4]. Ini terutama berlaku dalam menghadapi ancaman siber yang semakin kompleks dan canggih.

Analisis efek avalanche[5] adalah salah satu cara untuk menguji ketahanan sistem kriptografi dalam infrastruktur cloud. Efek avalanche adalah perubahan besar pada output kriptografi yang disebabkan oleh perubahan kecil pada input. Efek avalanche yang ideal menunjukkan kekuatan algoritma kriptografi yang digunakan dalam sistem pertahanan. Oleh karena itu, membangun sistem pertahanan berbasis cloud yang berfokus pada analisis efek[6] avalanche menjadi penting dan relevan, terutama untuk menjamin keamanan data perusahaan yang bergantung pada infrastruktur cloud.

Beberapa studi penelitian sebelumnya telah mendiskusikan masalah ini. Misalnya, penelitian yang dilakukan oleh Arshad et al. (2020) mengevaluasi seberapa baik algoritma kriptografi[7] bekerja dalam lingkungan cloud dengan menghitung seberapa besar efek avalanche yang dihasilkan oleh masing-masing algoritma. Studi lain yang dilakukan oleh Khan et al. (2019) menemukan bahwa penggunaan algoritma kriptografi adaptif dapat meningkatkan resistensi sistem cloud terhadap serangan brute-force dan side-channel[4]. Namun, analisis efek avalanche tidak selalu dikaitkan dengan strategi pertahanan sistem secara menyeluruh pada jaringan perusahaan.

Penelitian ini bertujuan untuk merancang sistem keamanan[8] yang kuat untuk mengenkripsi data dan tahan terhadap gangguan dari luar, seperti yang ditunjukkan oleh fitur efek avalanche. Oleh karena itu, fokus utama penelitian ini adalah menggabungkan elemen keamanan jaringan [9]dan kriptografi dalam sistem pertahanan berbasis cloud yang tangguh.

3. Metode Penelitian

Mengembangkan dan menguji sistem keamanan berbasis cloud dengan fokus pada analisis efek avalanche, penelitian ini menggunakan metode "eksperimen kuantitatif". Lima tahapan metode penelitian terdiri dari (1) penelitian literatur, (2) desain sistem keamanan, (3) penerapan infrastruktur cloud simulasi, (4) pengujian efek avalanche, dan (5) analisis hasil.

3.1. Kajian Literatur

Studi meneliti teori, teknik, dan teknologi terkait keamanan cloud, efek avalanche dalam kriptografi, dan algoritma enkripsi yang biasa digunakan pada sistem informasi perusahaan[10]. Untuk menjamin validitas ilmiah, literatur[11] diambil dari jurnal yang terindeks Scopus dan SINTA.

3.2. Desain Sistem Keamanan

Arsitektur berbasis cloud hybrid, yang disimulasikan dengan layanan cloud open-source seperti OpenStack atau Nextcloud[12], melengkapi sistem keamanan dengan modul enkripsi

data yang mendukung uji efek avalanche seperti AES (Advanced Encryption Standard)[13], Blowfish[14], dan Serpent[15].

3.3. Pelaksanaan

Setelah perancangan selesai, sistem diimplementasikan dalam lingkungan virtual dengan menggunakan server cloud simulasi[16], [17].Untuk menguji bagaimana sistem mempertahankan kerahasiaan data dan merespon perubahan, skenario pengiriman dan penyimpanan data dilakukan.

3.4. Evaluasi Efek Avalanche

Pengujian efek avalanche dilakukan dengan mengubah satu bit pada input plaintext[17] dan melihat seberapa banyak perubahan terjadi pada output ciphertext[18]. Untuk mengetahui sejauh mana efek avalanche bekerja pada algoritma[19], [20] yang digunakan, persentase perubahan bit dihitung. Rumus yang digunakan adalah sebagai berikut:

Efektivitas Avalanche (%) = jumlah bit yang berubah pada ciphertext dan total bit ciphertext dibagi 100 %. Setiap algoritma diuji selama tiga puluh iterasi untuk menghasilkan nilai efek avalanche rata-rata yang stabil[20].

3.5. Evaluasi Hasil

Untuk membandingkan performa masing-masing algoritma, data hasil pengujian dianalisis secara kuantitatif. Analisis ini mencakup efektivitas efek avalanche, efisiensi waktu enkripsi[21], [22], dan konsumsi sumber daya sistem. Hasil akhir akan menentukan algoritma yang paling ideal untuk keamanan data perusahaan[23], [24] berbasis cloud.

4. Hasil dan Pembahasan

4.1. Membangun Sistem Keamanan Berbasis Cloud

Penelitian ini menggunakan platform open-source yang biasa digunakan dalam simulasi jaringan perusahaan untuk membangun sistem keamanan[25] berbasis cloud[26]. Platform ini memungkinkan pengujian dengan berbagai skenario yang relevan untuk implementasi dunia nyata. Sistem ini menggunakan tiga algoritma kriptografi simetris—Advanced Encryption Standard (AES), Blowfish, dan Serpent—untuk mengenkripsi data yang dikirim antar node jaringan[27], [28]. Karakteristik kriptografi masing-masing algoritma memungkinkan penilaian seberapa baik dan efektif masing-masing algoritma dalam melindungi data di lingkungan cloud[29].

Untuk menguji kemampuan sistem ini, data dikirim dalam bentuk file biner, dokumen, dan teks yang telah dienkripsi. Proses enkripsi dan dekripsi dilakukan menggunakan metode kriptografi simetris, yang menggunakan kunci yang sama untuk kedua proses, memastikan kecepatan dan efisiensi pengolahan data. Hasilnya menunjukkan bahwa sistem dapat mengenkripsi dan mendekripsi seluruh file dengan benar tanpa kehilangan integritas data. Selain itu, pengujian dilakukan dengan menggunakan alat monitoring jaringan seperti Wireshark[30], yang dapat memeriksa lalu lintas data jaringan. Hasil pemantauan menunjukkan bahwa data yang terenkripsi tidak memiliki pola yang konsisten atau mudah dianalisis. Hal ini menunjukkan bahwa sistem berfungsi dengan baik untuk menyembunyikan data asli dari pihak yang tidak berwenang. Selain itu, proses ini memastikan bahwa data tidak dapat ditangkap dalam bentuk yang dapat dipahami oleh pihak luar, bahkan jika mereka berhasil mengakses lalu lintas jaringan.

Untuk meningkatkan keamanan jaringan perusahaan yang menggunakan infrastruktur cloud, penerapan sistem ini sangat penting[31]. Ini karena data sering berpindah antar server dan lokasi di lingkungan cloud, yang meningkatkan risiko kebocoran data. Dengan menggunakan algoritma kriptografi yang efektif seperti AES, Blowfish, dan Serpent, sistem ini mampu mengurangi risiko ini dan memastikan bahwa data yang dikirim antar server tetap aman[32]. Ini juga menunjukkan bahwa teknologi kriptografi berbasis cloud dapat diandalkan untuk melindungi data sensitif di dunia digital yang semakin terhubung[33], [34].

Untuk membangun sistem keamanan berbasis cloud, penelitian ini menggunakan platform open-source yang umum digunakan dalam simulasi jaringan perusahaan. Platform ini memungkinkan pengujian dengan berbagai skenario yang terkait dengan implementasi dunia nyata[35]. Tiga algoritma kriptografi simetris digunakan oleh sistem ini: Advanced Encryption Standard (AES), Blowfish, dan Serpent. Algoritma ini mengenkripsi data yang dikirim antar node jaringan. Penilaian seberapa baik dan efektif masing-masing algoritma dalam melindungi data di lingkungan cloud dimungkinkan oleh karakteristik kriptografi yang dimiliki algoritma tersebut.

Data dikirim dalam bentuk teks, file biner, dan dokumen yang telah dienkripsi untuk menguji kemampuan sistem ini. Metode kriptografi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, memastikan kecepatan dan efisiensi pengolahan data. Hasil penelitian menunjukkan bahwa sistem dapat dengan benar mengenkripsi dan mendekripsi setiap file tanpa kehilangan integritas data. Selain itu, pengujian dilakukan dengan menggunakan alat pemantauan jaringan seperti Wireshark, yang dapat memeriksa lalu lintas data jaringan. Hasil pemantauan menunjukkan bahwa data yang terenkripsi tidak memiliki pola yang konsisten dan mudah dianalisis. Hal ini menunjukkan bahwa sistem bekerja dengan baik untuk mencegah orang yang tidak berwenang mengakses data asli. Selain itu, proses ini memastikan bahwa data tidak dapat ditangkap dalam bentuk yang dapat dipahami oleh orang lain, bahkan jika mereka dapat mengakses lalu lintas jaringan[36].

Sistem ini sangat penting untuk diterapkan untuk meningkatkan keamanan jaringan perusahaan yang menggunakan infrastruktur cloud. Ini karena data sering berpindah antar server dan lokasi di cloud, yang meningkatkan risiko kebocoran data. Namun, sistem ini mampu mengurangi risiko ini dan memastikan bahwa data yang dikirim antar server tetap aman dengan menggunakan algoritma kriptografi yang efektif seperti AES, Blowfish, dan Serpent. Ini juga menunjukkan bahwa teknologi kriptografi berbasis cloud dapat diandalkan untuk melindungi data sensitif di dunia digital yang semakin terhubung[7].

Sistem ini dirancang untuk beradaptasi dengan perilaku jaringan cloud yang kompleks selain bergantung pada kekuatan algoritma enkripsi. Misalnya, sistem tetap dapat menjaga konsistensi dan keamanan data melalui proses re-enkripsi yang cepat ketika terjadi perpindahan data antar server karena load balancing atau replikasi otomatis. Metode ini sangat penting mengingat skala dan fleksibilitas infrastruktur cloud modern, yang membutuhkan sistem keamanan yang dapat disesuaikan yang tidak mengganggu kinerja jaringan secara keseluruhan[37].

Selain itu, penggabungan sistem keamanan ini dengan perangkat pengelolaan log audit dan pemantauan lalu lintas memungkinkan administrator jaringan untuk mendeteksi aktivitas mencurigakan secara proaktif. Sistem dapat mengidentifikasi pola serangan yang berpotensi membahayakan, seperti upaya brute force atau manipulasi data, dengan menggunakan data log yang terekam. Informasi ini sangat penting untuk keputusan tentang peningkatan sistem, pembaruan algoritma keamanan, dan penyesuaian kebijakan akses data di cloud[3].

Adanya arsitektur sistem yang mendukung skalabilitas dan kompatibilitas dengan berbagai platform cloud (baik publik maupun privat) membuat sistem ini layak digunakan bukan hanya oleh perusahaan besar tetapi juga oleh UMKM dan lembaga pemerintah yang sedang beralih ke layanan digital berbasis cloud. Ini memperkuat posisi sistem sebagai solusi keamanan data yang aplikatif, ekonomis, dan responsif terhadap kebutuhan transformasi digital yang cerdas.

4.2. Evaluasi Efek Avalanche

Setiap algoritma diuji 30 kali pada tahap pengujian efek avalanche untuk mendapatkan hasil yang lebih stabil dan representatif[38]. Pengujian ini dilakukan dengan mengubah satu bit plaintext sebelum dienkripsi, dan kemudian, setelah proses enkripsi, melihat jumlah bit yang berubah pada ciphertext. Efek avalanche adalah fitur kriptografi di mana perubahan kecil pada input (seperti perubahan satu bit) menghasilkan perubahan besar pada output. Ini membuat algoritma lebih aman untuk analisis pola[39].

Hasil pengujian menunjukkan bahwa Blowfish menghasilkan efek avalanche tertinggi, yaitu 51,37%, meskipun hanya ada perubahan satu bit pada teks plain, lebih dari setengah bit pada teks cipher, menunjukkan bahwa Blowfish sangat sensitif terhadap perubahan input. Sifat ini sangat diinginkan dalam algoritma kriptografi karena menyulitkan pihak yang tidak berwenang untuk menganalisis pola dan memprediksi teks plain. Di sisi lain, dengan nilai 48,92% dan 49,81%, masing-masing AES dan Serpent menunjukkan performa avalanche yang luar biasa; keduanya berada di kisaran yang dianggap ideal untuk algoritma kriptografi yang aman[40].

Tabel 1. Efek Avalanche dan Performa Rata-rata Algoritma

Algoritma	Efek Avalanche (%)	Waktu Enkripsi (ms)	Konsumsi CPU (%)
AES	48.92	12.4	21.5
Blowfish	51.37	9.8	19.2
Serpent	49.81	15.2	23.1

Dalam penelitian ini, waktu enkripsi Blowfish lebih lama daripada waktu enkripsi AES, meskipun Blowfish memiliki efek avalanche yang sedikit lebih besar daripada AES, Serpent menggunakan lebih banyak CPU dan memiliki waktu enkripsi yang lebih lama, yang membuatnya kurang efisien untuk digunakan pada sistem yang membutuhkan kecepatan tinggi.

Secara keseluruhan, pengujian ini menunjukkan bahwa meskipun ketiga algoritma yang diuji sangat baik untuk efek avalanche, pemilihan algoritma bergantung pada keamanan, efisiensi, dan jumlah sumber daya yang tersedia. Sementara AES masih unggul dalam adopsi industri dan integrasi sistem perangkat keras, Blowfish menawarkan kombinasi efisiensi dan keamanan terbaik. Oleh karena itu, ketika seseorang membuat keputusan untuk memilih algoritma yang tepat, mereka harus mempertimbangkan kebutuhan khusus dari aplikasi atau sistem yang akan digunakan.

4.3. Analisis Efisiensi dan Kinerja

Selain menguji parameter keamanan melalui efek avalanche, sistem juga diuji untuk efisiensi dengan mengukur waktu enkripsi dan penggunaan sumber daya CPU. Waktu enkripsi adalah komponen penting dalam pengoperasian sistem kriptografi di dunia nyata, terutama pada jaringan perusahaan yang membutuhkan kecepatan pengolahan data. Hasil pengujian menunjukkan bahwa Blowfish memiliki waktu enkripsi paling singkat, yaitu 9.8 milidetik per proses enkripsi. Dengan kinerja ini, Blowfish sangat cocok untuk produksi yang membutuhkan efisiensi tinggi tetapi tetap aman. Selain itu, Blowfish memiliki penggunaan CPU terendah sebesar 19,2%, yang menjadikannya pilihan yang bagus untuk aplikasi yang membutuhkan pemrosesan cepat tetapi tetap hemat daya.

AES, standar internasional yang disetujui oleh National Institute of Standards and Technology (NIST) dan didukung oleh hampir semua perangkat keras dan aplikasi saat ini, tetap jauh lebih baik daripada Blowfish, terutama dalam hal penerimaan industri. AES menawarkan keseimbangan yang baik antara kecepatan, keamanan, dan dukungan luas di berbagai platform, dengan waktu enkripsi hanya 12.4 milidetik dan penggunaan CPU sebesar 21,5%[41]. Karena keunggulan ini, AES menjadi pilihan utama dalam banyak aplikasi yang mengutamakan kestabilan dan keterandalan[42], meskipun sedikit lebih lambat dibandingkan Blowfish.

Meskipun memiliki kinerja terendah dari ketiganya, Serpent masih cukup baik untuk bisnis besar yang membutuhkan tingkat keamanan yang lebih tinggi. Serpent masih berada di ambang batas yang dapat diterima untuk kebanyakan aplikasi bisnis dengan waktu enkripsi 15.2 milidetik dan konsumsi CPU 23.1%. Meskipun Serpent sedikit lebih lambat dan menggunakan sumber daya lebih banyak dibandingkan AES dan Blowfish, ia tetap menawarkan tingkat keamanan yang luar biasa. Oleh karena itu, Serpent mungkin menjadi pilihan yang baik untuk sistem yang mengutamakan tingkat keamanan yang lebih tinggi, meskipun perlu diperhatikan seberapa efisien ia dilaksanakan[43].

4.4. Efek Keamanan Infrastruktur Cloud

Sistem keamanan harus dirancang agar mampu beroperasi secara optimal dalam lingkungan hybrid—yang merupakan kombinasi cloud publik dan privat—dalam konteks infrastruktur cloud modern[44], [45]. Perusahaan banyak menggunakan lingkungan hybrid karena memberikan fleksibilitas dalam mengelola beban kerja, skalabilitas sumber daya, dan kendali atas data sensitif. Namun, model ini menimbulkan masalah baru dalam hal keamanan data yang berpindah antar domain dengan berbagai tingkat perlindungan. Oleh karena itu, sistem keamanan yang diimplementasikan harus memiliki kemampuan untuk memastikan bahwa data tetap aman dan rahasia baik saat disimpan maupun saat dikirim antar node atau layanan[46].

Penerapan algoritma kriptografi dengan efek avalanche tinggi adalah salah satu metode yang berhasil untuk meningkatkan sistem keamanan infrastruktur cloud[47]. Efek avalanche adalah sifat algoritma enkripsi di mana perubahan kecil pada input (plaintext), seperti satu bit, akan menghasilkan perubahan besar dan tidak terkendali pada output (ciphertext). Pola ciphertext menjadi tidak dapat ditebak atau dianalisis secara statistik karena sifat ini. Akibatnya, upaya penyusupan data dengan metode seperti brute force atau serangan berbasis pola menjadi lebih sulit. Penelitian ini menguji algoritma seperti Blowfish, Serpent, dan AES. Algoritma-algoritma ini menunjukkan kemampuan untuk menghasilkan tingkat avalanche yang tinggi dan meningkatkan perlindungan terhadap ancaman yang bergantung pada pencocokan pola.

Selain itu, sistem yang dikembangkan mendukung enkripsi dinamis terhadap node jaringan yang berubah-ubah, yang umum terjadi di lingkungan cloud karena fitur otomatisasi seperti auto-scaling, load balancing, atau migrasi VM[36]. Mekanisme ini memungkinkan sistem untuk secara otomatis mengenkripsi ulang data ketika terjadi perubahan arsitektur atau perpindahan node, tanpa mengganggu alur komunikasi[48], [49]. Dengan demikian, kemungkinan kebocoran data selama transmisi dapat diminimalkan. Sistem adaptif semacam ini menunjukkan kemampuan tinggi untuk menjaga keamanan data secara berkelanjutan di tengah dinamika arsitektur cloud[50]. Perlindungan ini sangat penting untuk mencegah serangan seperti man-in-the-middle dan sniffing, yang sering menggunakan titik lemah selama perpindahan data antar komponen cloud.

4.5. Manfaat dan Relevansi Penelitian

Hasil penelitian ini menggunakan pendekatan kuantitatif terhadap efek avalanche untuk membantu pengembangan sistem keamanan berbasis cloud[37], yang biasanya hanya digunakan dalam kajian teoritis. Studi ini juga memberikan rekomendasi teknis tentang algoritma kriptografi terbaik untuk diterapkan pada jaringan perusahaan yang menggunakan infrastruktur cloud.[51]

5. Kesimpulan

Studi ini menghasilkan sistem keamanan berbasis cloud yang menggunakan tiga algoritma kriptografi simetris—AES, Blowfish, dan Serpent—untuk mengenkripsi data di jaringan bisnis. Penelitian ini menunjukkan melalui pendekatan kuantitatif bahwa algoritma Blowfish unggul dalam kecepatan enkripsi dan efisiensi penggunaan CPU sambil tetap menjaga tingkat keamanan yang tinggi melalui efek avalanche yang besar. Selain itu, telah terbukti bahwa sistem yang dikembangkan memiliki kemampuan untuk menjaga integritas data selama proses transmisi dan penyimpanan. Selain itu, sistem ini berhasil mengaburkan pola data asli dari pihak yang tidak berwenang. Sistem ini dinilai layak untuk digunakan dalam lingkungan bisnis yang menerapkan infrastruktur cloud hybrid karena didukung oleh pengujian melalui platform simulasi cloud dan alat pemantauan jaringan.

Studi ini membuka pintu untuk pengembangan lebih lanjut, meskipun temuan menunjukkan bahwa Blowfish memberikan kinerja terbaik. Salah satunya adalah memeriksa kinerja algoritma kriptografi lain, seperti Camellia atau Twofish, dalam skala besar dan dalam lingkungan produksi nyata. Teknologi kecerdasan buatan (AI) juga dapat meningkatkan sistem keamanan dengan mengubah algoritma kriptografi sesuai dengan lalu lintas dan ancaman jaringan. Untuk menilai keandalan dan stabilitas sistem dalam situasi dunia nyata, sangat

disarankan untuk melakukan pengujian tambahan pada infrastruktur cloud nyata yang memiliki beban kerja yang kompleks. Metode ini dapat digunakan untuk terus mengembangkan sistem keamanan cloud yang fleksibel dan kuat untuk menghadapi tantangan keamanan data yang semakin kompleks di era digital saat ini.

Daftar Pustaka

[1] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[2] "PERAN TEKNOLOGI CLOUD COMPUTING DALAM TRANSFORMASI INFRASTRUKTUR TI PERUSAHAAN".

[3] J. Pendidikan and D. Konseling, "Keamanan Data dan Transaksi dalam Pemanfaatan Cloud sebagai Service."

[4] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *INDOTECH Indonesian Journal of Education And Computer Science*, vol. 1, no. 3, p. 2023.

[5] J. S. G. Sinaga, Nehemia Sitorus, and Steven Lukas Samosir, "Analisis Kinerja Algoritma Hash pada Keamanan Data: Perbandingan Antara SHA-256, SHA-3, dan Blake2," *JURNAL QUANCOM: QUANTUM COMPUTER JURNAL*, vol. 2, no. 2, pp. 9–16, Dec. 2024, doi: 10.62375/jqc.v2i2.432.

[6] R. Abi Assyarif, G. Eka Yuliastuti, and C. Nurina Prabiantissa Institut Teknologi Adi Tama Surabaya, "Implementasi Kombinasi Algoritma Rot13 dan Vernam Cipher untuk Keamanan Data Teks."

[7] J. Informasi and P. Sains Dan Teknologi, "Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer".

[8] J. Ferlyzon, I. Kanedi, and R. Supardi, "Penerapan Snort Sebagai Sistem Keamanan Jaringan," *Jl. Meranti Raya No. 32 Kota Bengkulu*, vol. 21, no. 1, p. 341139, 2025.

[9] O. Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi Faris Jawad, R. Amanda Amalia, T. Sutan Nadzarudien, P. Sistem Informasi, and S. Tinggi Ilmu Komputer Cipta Karya Informatika, "Optimizing Security And Monitoring Infrastructure Networks At The Bekasi DPRD Office," 2023.

[10] M. Rizal Yahya, "PENGARUH BUSINESS INTELLIGENCE DAN CLOUD COMPUTING TERHADAP KEAMANAN SISTEM INFORMASI (Studi Pada BUMN di Provinsi Aceh)," 2023.

[11] S. Aflia Alkadrie, S. Hidayatullah Jakarta, and T. Selatan, "Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review," 2024.

[12] M. F. Khoer and N. Heryana, "TINJAUAN SISTEMATIK LITERATUR TENTANG CLOUD COMPUTING DAN ANALISIS DATA: ARSITEKTUR DAN METODOLOGI," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4989.

[13] R. Octian Nafis and M. Sidqon, "Jurnal Rekayasa Sistem Informasi dan Teknologi Volume 2, No 1-Agustus 2024 e-ISSN : 3025-888X RANCANG BANGUN SISTEM E-ARSIP BERBASIS WEBSITE MENGGUNAKAN METODE ENKRIPSI AES (Advanced Encryption Standard) STUDI KASUS KPU SIDOARJO."

[14] H. Alabdulrazzaq and M. N. Alenezi, "Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 14, no. 1, Apr. 2022, doi: 10.17762/ijcnis.v14i1.5262.

[15] L. Biondi, N. Gomes, R. S. Maior, and S. C. Soares, "Revisiting 'The Malicious Serpent': Phylogenetically Threatening Stimulus Marked in the Human Brain," *Emotion Review*, Apr. 2024, doi: 10.1177/17540739241277942.

[16] B. R. Allo *et al.*, "PERAN TEKNOLOGI CLOUD COMPUTING DALAM TRANSFORMASI INFRASTRUKTUR TI PERUSAHAAN: STUDI ANALISIS IMPLEMENTASI DI INDUSTRI MANUFAKTUR."

[17] A. Jacovi, A. Caciularu, O. Goldman, and Y. Goldberg, "Stop Uploading Test Data in Plain Text: Practical Strategies for Mitigating Data Contamination by Evaluation Benchmarks," May 2023, [Online]. Available: http://arxiv.org/abs/2305.10160

[18] M. Li, L. Wilke, J. Wichelmann, T. Eisenbarth, R. Teodorescu, and Y. Zhang, "A Systematic Look at Ciphertext Side Channels on AMD SEV-SNP," 2022, doi: 10.1109/SP46214.2022.00112.

[19] R. Abi Assyarif, G. Eka Yuliastuti, and C. Nurina Prabiantissa Institut Teknologi Adi Tama Surabaya, "Implementasi Kombinasi Algoritma Rot13 dan Vernam Cipher untuk Keamanan Data Teks."

[20] T. Indriyani, P. Dinasti Airlangga, F. Jaka, I. T. Adhi, and T. Surabaya, "Enkripsi Data Dengan Mengunakan Metode ECC (Elliptic Curve Cryptography)."

[21] A. F. Kusuma, S. Agustini, M. Hakimah, M. Kurniawan, I. T. Adhi, and T. Surabaya, "SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Implementasi Algoritma Caesar Cipher dan Rivest Shamir Adleman Super Enkripsi Teks Pesan dengan Karakter ASCII", doi: 10.31284/p.snestik.2024.5714.

[22] K. Marlin, K. Mere, A. Fitri, D. Santyo Nugroho, and D. Koerniawati, "PERAN TEKNOLOGI CLOUD COMPUTING DALAM MENINGKATKAN EFISIENSI DAN KEAMANAN PROSES AKUNTANSI: TINJAUAN TERHADAP PERUBAHAN PARADIGMA DALAM MANAJEMEN DATA KEUANGAN," *Jurnal Darma Agung*, no. 2, pp. 1044–1055, 2024, doi: 10.46930/ojsuda.v32i2.4152.

[23] "PERENCANAAN IMPLEMENTASI KOMPUTASI AWAN PADA INFRASTRUKTUR TEKNOLOGI DAN SISTEM INFORMASI DI UMPR".

[24] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *Jurnal Sistim Informasi dan Teknologi*, pp. 82–87, Jan. 2024, doi: 10.60083/jsisfotek.v5i4.329.

[25] D. Setiawan, M. Charlie Pratama, and D. Arisandi, "IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN RULE-BASED IDS PADA PT NETKRIDA TUAH CAKRAWALA," *JOISIE Journal Of Information System And Informatics Engineering*, vol. 7, no. 2, pp. 381–389, 2023.

[26] S. A. Calix, "cloud-computing-security-for-multi-cloud-service-providers-controls-and-techniques-in-our-modern-threat-landscape", doi: 10.5281/zenodo.7084251.

[27] D. Ardiani, A. H. Jatmika, and A. Zubaidi, "Modifikasi Protokol Routing DSDV Menggunakan Algoritma Dynamic-power transmission untuk Mengurangi Interferensi Sinyal dalam Pengiriman Data Berdasarkan Tingkat Kepadatan Node di Jaringan MANET Modification of DSDV Routing Protocol Using Dynamic-power transmission Algorithm to Reduce Signal Interference in Data Delivery Based on Node Density Level in MANET." [Online]. Available: http://jcosine.if.unram.ac.id/

[28] J. Informasi and P. Sains Dan Teknologi, "Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer".

[29] N. Dharmawan, Gani Indriyanta, and I Kadek Dendy Senapartha, "ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS," *Jurnal Terapan Teknologi Informasi*, vol. 6, no. 2, pp. 121–130, Oct. 2022, doi: 10.21460/jutei.2022.62.214.

[30] R. Soepeno, "Wireshark: An Effective Tool for Network Analysis", doi: 10.13140/RG.2.2.34444.69769.

[31] B. W. Aulia, M. Rizki, P. Prindiyana, and S. Surgana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi*, vol. 1, no. 1, pp. 9–20, Dec. 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.

[32] C. A. Pinuyut, E. Utami, and A. H. Muhammad, "ANALISIS KINERJA ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) TERMODIFIKASI DALAM ENRKIPSI DAN DEKRIPSI DATA (PERFORMANCE ANALYSIS OF MODIFIED ADVANCED ENCRYPTION STANDART (AES) ALGORITHM FOR ENCRYPTING AND DECRYPTING DATA)."

[33] R. Panji Anugrah, I. Yatini, and M. Agung Nugroho, "IMPLEMENTASI OPENSTACK UNTUK INFRASTRUKTUR PRIVATE CLOUD COMPUTING (STUDI KASUS UNTUK FASILITAS MAHASISWA UTDI)."

[34] A. P. Meriani, "Perbandingan Data Warehouse Cloud Computing Menggunakan Konvensional Berbasis Kriptopgafi." [Online]. Available: https://www.researchgate.net/publication/369001529

[35] R. Fauzi, Y. Muhyidin, and D. Singasatia, "Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS)," 2023.

[36] A. Fauzi, A. Maharani Putri, F. Fitriyani, R. Astriyani, V. Arisana, and Y. Indah Cahyani, "Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis", doi: 10.38035/jkmt.v2i2.

[37] S. Pitriyani and R. Firdaus, "Pengembangan Data Base Terdistribusi untuk Aplikasi Cloud Computing".

[38] M. Dzaky Nurfaishal and Y. Akbar, "Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping," 2024. [Online]. Available: https://journal.stmiki.ac.id

[39] D. Ramalinda and A. Rachmat Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," *Journal of International Multidisciplinary Research*, [Online]. Available: https://journal.banjaresepacific.com/index.php/jimr

[40] J. S. G. Sinaga, Nehemia Sitorus, and Steven Lukas Samosir, "Analisis Kinerja Algoritma Hash pada Keamanan Data: Perbandingan Antara SHA-256, SHA-3, dan Blake2," *JURNAL QUANCOM: QUANTUM COMPUTER JURNAL*, vol. 2, no. 2, pp. 9–16, Dec. 2024, doi: 10.62375/jqc.v2i2.432.

[41] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," vol. 6, no. 1.

[42] P. S. Curlin, J. Heiges, C. Chan, and T. S. Lehman, "A Survey of Hardware-Based AES SBoxes: Area, Performance, and Security," *ACM Comput Surv*, vol. 57, no. 9, pp. 1–37, Sep. 2025, doi: 10.1145/3724114.

[43] M. Bima, P. Sansaya, and A. Farisi, "2 ND MDP STUDENT CONFERENCE (MSC) 2023 PERBANDINGAN KINERJA ALGORITMA KANDIDAT AES DALAM ENKRIPSI DAN DEKRIPSI FILE DOKUMEN".

[44] M. Rizal Yahya, "PENGARUH BUSINESS INTELLIGENCE DAN CLOUD COMPUTING TERHADAP KEAMANAN SISTEM INFORMASI (Studi Pada BUMN di Provinsi Aceh)," 2023.

[45] P. Ananda Khairunnisa *et al.*, "Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia," *Jurnal Ilmu Teknik dan Informatika*, vol. 4, pp. 9–16, doi: 10.51903/teknik.

[46] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "ANALISIS KEAMANAN JARINGAN SISTEM INFORMASI SEKOLAH MENGGUNAKAN PENETRATION TEST DAN ISSAF," *Transmisi*, vol. 24, no. 3, pp. 83–91, Aug. 2022, doi: 10.14710/transmisi.24.3.83-91.

[47] "Analisis Keamanan dan Kenyamanan pada Cloud Computing Dwina Satrinia #1 , Syifa Nurgaida Yutia #2 , Iik Muhamad Malik Matin #3", doi: 10.52661.

[48] K. Tauhid and ; | Juroihan, "Integrasi Cloud Computing untuk Analisis Big Data," 2024.

[49] M. Kaleem *et al.*, "New Efficient Cryptographic Techniques For Cloud Computing Security Migration Letters New Efficient Cryptographic Techniques For Cloud Computing Security," vol. 21, no. S11, pp. 13–28, 2024, [Online]. Available: www.migrationletters.com

[50] I. Dwiputra and I. Afrianto, "Evaluasi berbagai Keamanan Sistem Cloud Computing: Suatu Tinjauan Literatur."

[51] H. Risky Kurniawan, I. Nur Sofiyanto, and M. Faqih Habiburrohman, "Analisis Risiko Keamanan Data pada Platform Cloud Computing," pp. 18–2024.