Jurnal Cakrawala Akademika (JCA)
Vol. 1 No. 4 Desember 2024
E-ISSN: 3062-9942 , Hal 1365-1373
DOI: https://doi.org/10.70182/JCA.27
https://jurnalpustakacendekia.com/index.php/jca

Mitigasi Risiko *Cybercrime* Terhadap Keamanan Sistem Komputasi Awan Pada Perusahaan

Desi Aryani
Universitas Islam Negeri Raden Fatah Palembang

Eriene Dheanda Absharina
Universitas Islam Negeri Raden Fatah Palembang

Alamat: Jalan Prof.K.H.Zainal Abidin Fikri Km.3, RW.5, 5 Ulu, Kecamatan Seberang Ulu I, Kota Palembang, Sumatera Selatan 30267

Korespondensi penulis: 212120803039@radenfatah.ac.id

Abstract *This research aims to explore and identify threats, challenges, and risk mitigation in cloud computing system security based on a systematic literature review of previous research. The literature review was conducted by collecting, selecting, and analyzing scientific articles related to trusted databases, covering the topics of cybercrime threats, data security, and risk management in cloud computing from trusted journal databases that focus on information technology security issues. The review showed that the main threats include DDoS attacks, software vulnerability exploitation, and data loss risk due to inadequate management. In addition, key challenges such as compliance with data privacy regulations, risk management, and trust in service providers are significant impediments to cloud computing implementation. Therefore, a comprehensive mitigation strategy is required, including strengthening encryption, developing security policies, and implementing an integrated risk management system. In addition, this research emphasizes the possibility of using innovative technologies, such as the use of blockchain, to improve the security of cloud computing systems in the future.*

Keywords*: Blockchain Technology, Cloud Computing, Cybercrime, Data Security, Risk Mitigation*

Abstrak. Penelitian ini bertujuan untuk mengeksplorasi dan mengidentifikasi ancaman, tantangan, serta mitigasi risiko dalam keamanan sistem komputasi awan berdasarkan tinjauan literatur sistematis dari penelitian terdahulu. Tinjauan literatur dilakukan dengan mengumpulkan, menyeleksi, dan menganalisis artikel-artikel ilmiah terkait *database* terpercaya, meliputi topik ancaman *cybercrime*, keamanan data, dan manajemen risiko dalam komputasi awan dari *database* jurnal terpercaya yang berfokus pada isu keamanan teknologi informasi. Hasil tinjauan menunjukkan bahwa ancaman utama mencakup serangan DDoS, eksploitasi kerentanan perangkat lunak, dan risiko kehilangan data

Received Desember 3, 2024; Desember 10, 2024; Accepted Desember 17, 2024
*Desi Aryani, 212120803039@radenfatah.ac.id

akibat kurangnya pengelolaan yang memadai. Selain itu, tantangan utama seperti kepatuhan terhadap regulasi privasi data, manajemen risiko, dan kepercayaan terhadap penyedia layanan menjadi penghambat utama dalam implementasi komputasi awan. Oleh karena itu, diperlukan strategi mitigasi yang komprehensif, termasuk penguatan enkripsi, pengembangan kebijakan keamanan, dan penerapan sistem manajemen risiko yang terintegrasi. Selain itu, penelitian ini menekankan kemungkinan penggunaan teknologi inovatif seperti penggunaan *blockchain* untuk meningkatkan keamanan sistem komputasi awan di masa depan.

Kata kunci: *Cybercrime*, Komputasi Awan, Keamanan Data, Mitigasi Risiko, Teknologi *Blockchain*

PENDAHULUAN

Pada era digitalisasi seperti saat ini, *cloud computing* telah menjadi solusi utama dalam mendukung transformasi digital pada perusahaan. Teknologi ini menawarkan manfaat yang signifikan, seperti efisiensi biaya, fleksibilitas dan skalabilitas dalam pengelolaan data serta aplikasi bisnis. Namun dibalik keuntungan tersebut, muncul berbagai ancaman keamanan yaitu kejahatan di internet yang meningkat, yang dapat mempengaruhi kepercayaan dan keberlanjutan operasional perusahaan. (Dheanda & Sutabri, 2023). Ancaman ini meliputi serangan siber, pencurian data, hingga eksploitasi celah keamanan pada perangkat lunak (Bhadauria et al., 2011). Di industri TI, komputasi awan adalah server virtual yang dapat diakses melalui Internet yang memungkinkan pengguna mengakses sumber daya dan layanan komputasi kapan saja dan di mana saja. Amazon Web Services (AWS), Microsoft Windows Azure, dan Google AppEngine adalah beberapa penyedia komputasi awan terkenal. Komputasi awan masih penuh dengan bahaya. Sebelum melakukan apa pun di bidang ini, keamanan, kerahasiaan, kemampuan audit, kepatuhan terhadap peraturan, dan sejumlah risiko lainnya harus diperiksa dengan cermat. (Wijoyo et al., n.d.)

Pada *Database*, penyampaian layanan oleh penyedia layanan *cloud* sangat penting karena lingkungan *cloud* memberikan akses ke perangkat lunak, perangkat keras, dan informasi lainnya yang terpusat (Keislaman & Sains, 2018). Dengan *database* sebagai model layanan, pemilik aplikasi tidak perlu memasang dan memelihara *database* itu sendiri; sebaliknya, ini dilakukan oleh penyedia layanan *database*, dan pemilik aplikasi dikenakan biaya terkait dengan penggunaan layanan tersebut. Sistem manajemen basis

data *cloud* adalah basis data terdistribusi yang memberikan komputasi sebagai layanan, bukan produk. Ini adalah penyebaran perangkat lunak, sumber daya, dan informasi antara beberapa perangkat melalui jaringan, yang sebagian besar terdiri dari internet. Platform untuk berbagi sumber daya komputasi dan layanan seperti SaaS, PaaS, dan IaaS disediakan oleh lingkungan komputasi *cloud*, yang dapat digunakan oleh perusahaan jenis *hybrid*, publik, atau pribadi(Marliana, 2019). Karena komputasi awan digunakan bersama sumber daya yang tersebar di seluruh dunia melalui jaringan luas, seperti internet, di lingkungan terbuka, komputasi awan akan menimbulkan berbagai masalah keamanan untuk *cloud* dan aplikasinya. Konsekuensinya, komputasi awan dikenal sebagai *Everything as-a-service*. Memiliki kontrol penuh atas data dan proses di komputer pribadi, tetapi di *cloud* menggunakan data dan layanan aplikasi dari beberapa penyedia layanan *cloud* lainnya (Daffa Ilyasa, n.d.).

Penerapan komputasi awan di lingkungan perusahaan memberikan berbagai keuntungan strategis. Melalui pengelolaan data yang terpusat dan penggunaan teknologi canggih, perusahaan dapat meningkatkan kolaborasi antar tim, mempercepat pengambilan keputusan, dan mengoptimalkan proses bisnis (Farizy Emi Sita Eriana et al., n.d.). Namun, ancaman terhadap keamanan data menjadi perhatian utama, terutama mengingat risiko kebocoran data, serangan siber, dan akses tidak sah yang semakin kompleks. Oleh karena itu, keamanan sistem komputasi awan menjadi isu kritis yang harus dikelola dengan serius oleh perusahaan dengan menerapkan mitigasi risiko (Novianti Indah Putri et al., 2022). Ancaman utama yang dihadapi perusahaan dalam penggunaan komputasi awan mencakup serangan *Distributed Denial of Service* (DDoS), eksploitasi kerentanan perangkat lunak, serta risiko kehilangan data akibat kurangnya manajemen keamanan yang memadai. Selain itu, tantangan lain seperti kepatuhan terhadap regulasi privasi data, manajemen risiko, dan membangun kepercayaan terhadap penyedia layanan *cloud* menjadi faktor yang mempengaruhi adopsi teknologi ini. Meskipun terdapat berbagai tantangan, potensi besar yang ditawarkan oleh komputasi awan dalam mendukung inovasi dan pertumbuhan bisnis tidak dapat diabaikan. Penggunaan teknologi baru seperti *blockchain* dapat membantu perusahaan dalam meningkatkan keamanan dan keandalan sistem *cloud*. Selain itu, penerapan strategi mitigasi risiko yang komprehensif, termasuk enkripsi data yang kuat, pengembangan

kebijakan keamanan, dan integrasi sistem manajemen risiko, menjadi langkah penting untuk melindungi data perusahaan dan memastikan keberlangsungan operasional.

Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi dan menganalisis ancaman serta tantangan dalam keamanan sistem komputasi awan berdasarkan tinjauan literatur yang sistematis. Fokus utama penelitian adalah mengidentifikasi ancaman utama, tantangan, serta strategi mitigasi yang dapat diterapkan untuk mendukung penggunaan komputasi awan yang aman dan efisien di lingkungan perusahaan. Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan yang berarti tentang pentingnya pengelolaan risiko dan strategi keamanan dalam mendukung adopsi teknologi komputasi awan secara optimal.

METODE PENELITIAN

Penelitian ini menganalisis ancaman dan tantangan keamanan dalam sistem komputasi awan perusahaan dengan menggunakan metodologi tinjauan literatur yang sistematis. Tujuan dari metode tinjauan literatur adalah untuk mengumpulkan, menganalisis, dan merangkum temuan penelitian sebelumnya serta menilai perspektif para ahli yang tercermin dalam berbagai karya ilmiah. (Achmad Mukhlis et al., 2023). Diharapkan metode ini dapat memberikan gambaran menyeluruh tentang masalah keamanan yang dihadapi perusahaan saat menggunakan teknologi komputasi awan serta strategi mitigasi yang dapat diterapkan.

Penelitian dimulai dengan mengumpulkan artikel ilmiah dari sumber-sumber terpercaya seperti Google Scholar, ScienceDirect, dan IEEE Xplore. Keamanan komputasi *cloud*, ancaman *cyber* di *cloud*, perlindungan data di komputasi *cloud*, dan manajemen risiko *cloud* adalah beberapa kata kunci yang relevan yang digunakan dalam proses pencarian. Kemudian kriteria inklusi digunakan untuk memilih artikel yang berfokus pada ancaman keamanan dan tantangan penggunaan komputasi awan. Ini termasuk masalah seperti manajemen risiko, kebocoran data, serangan siber, dan kepatuhan terhadap peraturan privasi. Dalam analisis, artikel yang tidak relevan atau tidak berbasis penelitian diabaikan.

Selanjutnya, literatur yang dipilih dianalisis secara menyeluruh untuk mengidentifikasi ancaman yang sering terjadi, kesulitan dalam menerapkan keamanan

cloud, dan strategi mitigasi yang efektif. Analisis juga mencakup pemeriksaan regulasi yang berlaku serta kemungkinan penggunaan teknologi baru, seperti *blockchain* untuk meningkatkan keamanan sistem *cloud*. Kesimpulan dari analisis ini dikumpulkan untuk memberikan gambaran menyeluruh tentang masalah ini. Metode pada penelitian ini diharapkan dapat membantu perusahaan memahami dan mengelola risiko keamanan sistem komputasi awan dengan lebih baik.

HASIL DAN PEMBAHASAN

Ancaman Pada Sistem Komputasi Awan

Berikut beberapa ancaman keamanan pada sistem komputasi awan:

1. ***Distribution Denial of Service* (DDoS)**

   Serangan DDoS (*Denial of Service*) adalah satu ancaman terbesar dalam dunia keamanan *cyber* saat ini. Serangan DDoS memanfaatkan jaringan komputer yang terdistribusi secara geografis untuk secara bersamaan mengirimkan lalu lintas yang besar ke sebuah target dengan tujuan untuk mengganggu atau menghentikan layanan yang diberikan oleh target tersebut. Serangan ini memanfaatkan kelemahan infrastruktur jaringan target, seperti *bandwidth* atau sumber daya komputasi, dan membanjiri target dengan permintaan lalu lintas yang melebihi kapasitas normal jaringan. Serangan DDoS ini telah diperburuk oleh kemajuan teknologi(Puspitasari et al., 2024). Dengan semakin banyaknya perangkat yang terhubung ke internet, baik melalui *Internet of Things* (IoT), komputer pribadi, atau perangkat *mobile*, potensi untuk membentuk botnet yang besar untuk melancarkan serangan meningkat. Botnet ini biasanya terdiri dari ribuan hingga jutaan perangkat yang dikompromikan dan dikendalikan tanpa sepengetahuan pemiliknya. Serangan DDoS dapat memiliki konsekuensi finansial yang signifikan bagi korban selain masalah teknis. Karena *downtime* yang tidak terduga pada layanan, perusahaan dapat mengalami kerugian besar, yang dapat mempengaruhi reputasi dan kepercayaan pelanggan. Industri keamanan *cyber* terus mengembangkan strategi dan teknologi baru untuk melawan serangan DDoS. Ini termasuk penggunaan sistem deteksi dini yang lebih canggih, pendekatan yang berbeda untuk mitigasi lalu lintas, dan layanan perlindungan

DDoS yang diberikan oleh penyedia layanan keamanan atau CDN (Rahman et al., 2024).

2. Eksploitasi Kerentanan Perangkat Lunak

Ancaman lainnya pada sistem komputasi awan adalah eksploitasi kerentanan perangkat lunak. Ada celah dalam kode perangkat lunak yang memungkinkan pelaku kejahatan siber mengakses sistem secara ilegal, mencuri data, atau mengganggu layanan. Ketergantungan pada aplikasi pihak ketiga yang tidak memenuhi standar keamanan yang memadai, konfigurasi sistem yang buruk, dan pembaruan perangkat lunak yang tidak rutin merupakan beberapa faktor yang memperburuk eksploitasi ini.

Serangan seperti injeksi kode atau serangan yang menggunakan kelemahan dalam repositori dan *framework* aplikasi dapat memanfaatkan kerentanan perangkat lunak. Sampai terjadi pelanggaran keamanan yang signifikan, ancaman ini sering kali tidak terdeteksi. Perangkat lunak tidak 100% aman, tetapi dapat dirancang dan dikembangkan dengan pikiran aman. Komponen kontrol keamanan diperlukan untuk mengurangi dampak eksploitasi. (Dewi & Sn, 2012).

3. Tantangan Pada Sistem Komputasi Awan

Tantangan pada sistem komputasi awan yang memungkinkan ialah kebocoran data, pencurian identitas, dan serangan dunia maya. Tantangan tersebut membutuhkan pendekatan yang cermat dan komprehensif dalam desain arsitektur sistem (Novianti Indah Putri et al., 2022).

Solusi Untuk Penggunaan Sistem Komputasi Awan Pada Perusahaan

Untuk mencapai tingkat keamanan yang komprehensif, peneliti mengusulkan untuk menerapkan perlindungan berlapis yang diterapkan yang dimana lapisan tersebut saling melengkapi satu sama lain. Penggunaan enkripsi data tingkat tinggi, seperti Standar Enkripsi Tinggi (AES) dengan kunci 256-bit, memberikan perlindungan yang kuat terhadap data baik saat dikirim maupun disimpan. Selain itu, sistem deteksi dan pencegahan intrusi (IDS/IPS) berbasis pembelajaran mesin memungkinkan deteksi pola

serangan baru secara *real-time*, sementara autentikasi multifaktor (MFA) memastikan bahwa hanya pengguna yang sah yang dapat mengakses data perusahaan.

Sistem pengelolaan akses dan identitas (IAM) juga penting karena memungkinkan perusahaan untuk mengatur hak akses berdasarkan peran pengguna, sehingga mengurangi risiko akses tidak sah. Selain itu, arsitektur *zero trust* memastikan bahwa semua pengguna dan perangkat harus diverifikasi sebelum dapat mengakses sistem.

Audit keamanan berkala juga sangat penting untuk mengidentifikasi kerentanan yang dapat digunakan oleh pihak yang tidak berwenang. Teknik keamanan *multi-tenancy*, yang memungkinkan isolasi data pengguna meskipun menggunakan sumber daya yang sama, juga merupakan komponen penting dalam menjaga privasi dan keamanan data.

Diharapkan bahwa langkah-langkah ini, bersama dengan pelatihan lebih lanjut tentang keamanan siber, akan meningkatkan kesadaran dan kemampuan karyawan untuk menghindari serangan berbasis kesalahan manusia. Perlindungan terhadap serangan yang lebih canggih dapat diperkuat dengan *firewall* generasi baru yang dapat menganalisis lalu lintas jaringan secara menyeluruh. Bisnis dapat menjaga integritas data, meningkatkan kepercayaan pengguna terhadap layanan berbasis *cloud*, dan mengelola risiko keamanan sistem komputasi awan dengan lebih efisien dengan menerapkan solusi-solusi ini secara menyeluruh.

Penelitian ini memberikan gagasan penting untuk solusi inovatif dalam menangani masalah dan ancaman keamanan informasi dalam sistem berbasis komputasi awan. Mengingat kompleksitas penerapan teknologi *cloud*, yang mencakup penyimpanan data dan akses melalui layanan *cloud*, fokus utamanya adalah meningkatkan tingkat keamanan dan privasi data secara signifikan. Perangkat lunak dan perangkat keras yang disimpan secara dapat diakses jarak jauh oleh setiap pengguna melalui layanan *cloud*. Arsitektur sistem yang dikembangkan didasarkan pada pertimbangan elemen penting yang berkaitan dengan keamanan data. Fondasi utama dari lapisan perlindungan yang kuat adalah teknologi mutakhir seperti enkripsi data, sistem deteksi intrusi, dan kontrol akses yang ketat. Lapisan perlindungan ini dirancang untuk memberikan perlindungan menyeluruh terhadap berbagai potensi ancaman sambil menjaga integritas dan kerahasiaan data.

KESIMPULAN

Komputasi awan di era digital memberikan berbagai keuntungan seperti efisiensi, fleksibilitas, dan skalabilitas, tetapi juga menimbulkan risiko signifikan, termasuk ancaman *cybercrime*, kebocoran data, dan serangan DDoS. Untuk menghadapi tantangan ini, perusahaan perlu menerapkan strategi mitigasi risiko yang komprehensif, seperti penguatan enkripsi, autentikasi multifaktor, dan audit keamanan berkala. Selain itu, teknologi inovatif seperti *blockchain* dan sistem manajemen risiko terintegrasi dapat meningkatkan keamanan data dan operasional perusahaan. Dengan langkah-langkah ini, perusahaan dapat memanfaatkan potensi besar komputasi awan sambil menjaga keamanan dan kepercayaan terhadap sistem.

DAFTAR PUSTAKA

Achmad Mukhlis, Baiq Laila Alfila, & Aliya Zhafira Wastuyana. (2023). Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review. *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer*, *3*(2), 143–152. https://doi.org/10.55606/juisik.v3i2.496

Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S., & Author, C. (2011). *A Survey on Security Issues in Cloud Computing*. https://www.researchgate.net/publication/51940172

Daffa Ilyasa, N. (n.d.). *Keamanan dan Privasi Pada Cloud Computing Sebagai Tempat Penyimpanan Data Masa Kini Latar Belakang*. https://doi.org/10.13140/RG.2.2.11425.28003

Dewi, E. K., & Sn, A. (2012). ANALISIS KEAMANAN SISTEM PERANGKAT LUNAK. In *Seminar Nasional Aplikasi Teknologi Informasi*.

Dheanda, E., & Sutabri, T. (2023). ANALISIS MODEL DIGITAL FORENSIC READINESS INDEX (DiFRI) UNTUK MENCEGAH CYBERCRIME. *Blantika : Multidisciplinary Jornal*, *1*(2). https://blantika.publikasiku.id/191

Farizy Emi Sita Eriana Jl Surya Kencana No, S., Gd, P. A., & Pamulang Tangerang Selatan -Banten, U. (n.d.). *Universitas Pamulang Sistem Informasi Cloud Computing = Komputasi Awan i CLOUD COMPUTING = KOMPUTASI AWAN*. www.unpam.ac.id

Keislaman, S., & Sains, D. (2018). Analisis Kesuksesan Sistem Informasi E-KKN LP2M UIN Raden Fatah Palembang dengan Menggunakan Model Delone dan Mclean. *Jurnal Intelektualita: Keislaman, Sosial, Dan Sains*, *7*(2), 2303–2952. https://doi.org/10.19109/intelektualita.v7i2.2732

Marliana, M. (2019). *KEAMANAN DAN PENCEGAHAN DATABASE CLOUD COMPUTING UNTUK PENGGUNA LAYANAN*. *3*(2).

Novianti Indah Putri, Iswanto, Dandun Widhiantoro, Zen Munawar, & Heru Soerjono. (2022). Penerapan Manajemen Resiko Pada Komputasi Awan. *TEMATIK*, *9*(2), 144–151. https://doi.org/10.38204/tematik.v9i2.1074

Puspitasari, V., Abdillah, M. Z., Alfa, M. A., Steyer, D., & Neyman, S. N. (2024). Deteksi dan Respons Terhadap Ddos Attacks pada Website Dinamis. *Jurnal Ilmu Teknik*, *1*(4), 18–25. https://doi.org/10.62017/tektonik

Rahman, R., Odja, G. R. S., & Artikel, S. (2024). *Technology Sciences Insights Journal Analisis dan Pencegahan Serangan DDoS Pada Jaringan Skala Besar INFORMASI ARTIKEL ABSTRAK*.

Wijoyo SSKom, A., Fatimah, S., Widianti, Y., & Fadillah, M. (n.d.). *Keamanan Data dalam Sistem Informasi Manajemen: Risiko dan Strategi Perlindungan*. https://jurnalmahasiswa.com/index.php/teknobis