JURNAL SISTEM INFORMASI DAN TENOLOGI

http://www.jurnal.umk.ac.id/sitech

Analisis Kerentanan: Memanfaatkan Kerentanan dan Pengaruh Keamanan Siber pada *Cloud Computing*

Aprillia Sakinah[1], **Sangkot Khofipah**[2], **Pesah Sifrah Tripena**[3], **Maria Anjelina Dewi Karoko**[4], **Fauziyah**[5]
[12345]*Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bung Karno*

Article Info:
Dikirim: 4 Agustus 2024
Direvisi: 21 September 2024
Diterima: 3 Oktober 2024
Tersedia Online: 31 Desember 2024

Penulis Korespondensi:
Aprillia Sakinah
Universitas Bung Karno, Jakarta, Indonesia
Email: mynameapril16@gmail.com

Abstrak: *Dalam era digital yang semakin maju, cloud computing telah menjadi tulang punggung bagi banyak organisasi. Kemudahan akses, fleksibilitas, dan skalabilitas yang ditawarkan oleh teknologi ini membuatnya semakin populer. Namun, di balik segala kemudahannya, cloud computing juga membawa tantangan signifikan terkait keamanan data. Mengingat sifatnya yang terdistribusi dan multi-tenant, data yang disimpan di cloud menjadi sangat rentan terhadap berbagai ancaman siber. Analisis kerentanan terhadap sistem cloud mengungkapkan bahwa data yang berada di luar kendali langsung organisasi dapat menjadi sasaran empuk bagi pelaku kejahatan siber yang terus mengembangkan taktik serangannya. Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk menganalisis kerentanan keamanan data pada cloud computing. Fokus utama penelitian ini adalah pada tantangan dan risiko yang dihadapi data yang tersimpan di lingkungan cloud, mengingat sifatnya yang terdistribusi dan diakses oleh berbagai pihak. Dengan semakin banyaknya pengguna yang mengadopsi layanan cloud, peluang terjadinya pelanggaran data semakin meningkat. Oleh karena itu, pemahaman mendalam mengenai kerentanan keamanan pada cloud computing menjadi sangat penting untuk merancang strategi mitigasi yang efektif.*

Kata kunci: *keamanan, siber, cloud, computing, sistem*

Abstract: *In an increasingly advanced digital era, cloud computing has become the backbone of many organizations. The ease of access, flexibility, and scalability offered by this technology make it increasingly popular. However, behind all its convenience, cloud computing also brings significant challenges regarding data security. Given its distributed and multi-tenant nature, data stored in the cloud is highly vulnerable to various cyber threats. Vulnerability analysis of cloud systems reveals that data outside an organization's direct control can be an easy target for cybercriminals who continue to develop their attack tactics. This research uses a qualitative descriptive approach to analyze data security vulnerabilities in cloud computing. The main focus of this research is on the challenges and risks faced by data stored in a cloud environment, given its distributed nature and access by various parties. As more and more users adopt cloud services, the chances of data breaches are increasing. Therefore, a deep understanding of security vulnerabilities in cloud computing is very important for designing effective mitigation strategies.*

Keywords: *security, cyber, cloud, computing, systems*

1. PENDAHULUAN

Keamanan data di penyimpanan *cloud* sebagai perhatian utama karena memiliki risiko yang terkait dengan penyimpanan berita sensitif secara online. Ancaman dunia maya seperti peretasan serta pelanggaran data menyebabkan ancaman berkelanjutan terhadap kerahasiaan serta integritas data yang disimpan di lingkungan *cloud* sebagai akibatnya mempertinggi ketergantungan pada penyimpanan *cloud* buat data langsung dan bisnis. Sebab itu, tindakan keamanan yang ketat diharapkan buat mencegah akses data yang tidak legal serta kehilangan data [1].

Menurut Indonesian cloud keresahan ancaman keamanan dapat terjadi apabila data sensitif perusahaan atau organisasi atau perorangan diberikan pada pihak lain seperti penyedia jasa *cloud* tanpa disertai dengan perjanjian kerahasiaan serta keamanan data. sebab, tanpa adanya perjanjian antar kedua belah pihak bisa berpotensi diakses *hacker*. Keresahan koneksi internet yang jelek bisa menghambat akses ke data yang disimpan pada *cloud*.

Sistem penyimpanan *cloud* terus menghadapi tantangan dalam memastikan keamanan facts karena information dikirimkan melalui internet dan disimpan di server jarak jauh, sehingga rentan terhadap upaya penyadapan. Akses tidak sah ke facts yang disimpan di *cloud* dapat menyebabkan pelanggaran data, kerugian finansial, kerusakan reputasi, dan konsekuensi hukum. Karena bisnis dan individu mengandalkan penyimpanan *cloud* untuk memudahkan akses ke records, mengatasi masalah keamanan statistics pada platform *cloud* menjadi semakin penting [2].

Kompleksitas pengelolaan keamanan data di penyimpanan *cloud* muncul berasal jenis data yang disimpan, perbedaan persyaratan keamanan, dan kebutuhan buat mematuhi peraturan proteksi data. Nomor kejahatan siber di *cloud computing* semakin meningkat berdasarkan data yang ada laporan yang terdapat di tahun 2021 agresi *DDoS (Distributed Denial of Service)* agresi *DDoS* artinya bentuk kejahatan siber yang menyerang layanan hosting yang terhubung menggunakan internet. serangan ini dapat Mengganggu kinerja dan performa usaha, serta mengurangi taraf kepercayaan pelanggan terhadap dapat dipercaya sistem keamanan yang dipakai sang perusahaan. serta di tahun 2022 kebocoran data banyaknya data yang ditransfer ke *cloud* membentuk situs *cloud* hosting menjadi incaran bagi pencuri data. Tim pengembangan sisi klien yang tidak terbiasa dengan fitur teknologi *cloud* berpotensi menghadapi risiko pencurian data laporan *Badan Siber dan Sandi Negara (BSSN)* tahun 2023, terjadi 403,9 juta anomali dalam lalu melintasi jaringan internet pada Indonesia sepanjang tahun 2023, meskipun jumlah ini menurun dibandingkan tahun sebelumnya yang mencapai 976,4 juta anomali. Selain itu, kegiatan *Advanced Persistent Threat (APT)* masih sangat tinggi, mencapai 4 juta kejadian sepanjang tahun 2023[3].

Sumber: LANSKAP KEAMANAN SIBER INDONESIA 2023

Gambar 1. Data Kejahatan Siber

Sesuai grafik pada gambar 1, jumlah anomali jaringan Internet pada Indonesia diperkirakan akan menurun pada tahun 2023, namun jumlah tadi masih tergolong tinggi serta aktivitas *Advanced Persistent Threat (APT)* masih meluas. Hal ini memberikan masih banyak celah yang dapat dimanfaatkan oleh pelaku kejahatan siber buat menyerang sistem *cloud computing* karena itu, diharapkan tindakan berfokus untuk memerangi kejahatan siber komputasi awan pada Indonesia.

2. PENELITIAN RELEVAN

Abiezal, dkk melakukan penelitian di tahun 2023, penelitian ini artinya buat menganalisis ancaman keamanan *cloud* waktu ini dan menyampaikan solusi buat memastikan privasi data. Penelitian ini pula akan membahas beberapa teknik dan best practices buat meningkatkan keamanan *cloud*. Metode yang dipergunakan merupakan Analisis literatur, survei, analisis data, uji coba serta analis tren. akibat penelitian ini adalah buat menjaga keamanan *cloud* di era digital, penelitian memberikan bahwa organisasi wajib mengambil tindakan agresif buat menangani ancaman siber ketika ini serta menjaga privasi data mereka. galat satu langkah penting yang dapat dilakukan ialah menerapkan praktik keamanan terbaik pada pengelolaan serta akses data *cloud* [4].

Masyhur. Zulkarnaim, dkk melakukan penelitian di tahun 2021, penelitian dengan judul Studi Literatur Keamanan serta Privasi data Sistem *Cloud Computing* pada Platform Google Drive. Penulis melakukan pencarian surat keterangan terkait dengan keamanan privasi data. Literature review merupakan sebuah metode yang sistematis, eksplisit serta reprodusibel buat melakukan identifikasi, penilaian serta sintesis terhadap karya-karya yang akan terjadi penelitian dan hasil pemikiran yang telah dihasilkan oleh para peneliti serta praktisi. sesuai yang akan terjadi asal penelitian ini, keamanan data pengguna di *Cloud computing* bisa diketahuibahwa data yang tersimpan di *Cloud computing* tidak mampu diambil dengan mudah begitu saja oleh hacker, user lain atau pun admin dari *cloudstorage*, karena data yang tersimpan di *cloudstorage* telah ter-enkripsi *Advanced Encryption Standard (AES)* yang berbasis 256 keys dimana tidak bisa diakses karena arsip tersebut telah terenkripsi [5].

Xianrong Zeng, dkk melakukan penelitian di tahun 2014, di penelitiannya mengembangkan sebuah metode pengukuran kualitas layanan *cloud* yang CLOUDQUAL. CLOUDQUAL terdiri dari enam dimensi kualitas: *usability*, *availability*, *reliability*, *responsiveness*, *security*, dan *elasticity*. Dimensi usability, bersifat subjektif, sementara dimensi-dimensi lainnya bersifat objektif. Penelitian ini menunjukkan bahwa usability mengukur seberapa mudah, efisien, dan menyenangkannya antarmuka layanan *cloud* digunakan, serta menilai kemudahan akses fungsi layanan *cloud* melalui Application Programming Interface (API). Untuk pengguna akhir yang tidak memiliki keahlian khusus dalam cloud, antarmuka grafis (GUI) lebih disukai dibandingkan API. Selain itu, *Web User Interface* (WUI) dianggap lebih baik dari GUI, karena pengguna tidak perlu melakukan instalasi tambahan untuk menggunakan WUI, sementara GUI memerlukan instalasi *client.*

3. METODOLOGI PENELITIAN

Dalam penulisan penelitian ini, tim penulis memakai metode deskriptif kualitatif buat mendeskripsikan tentang keamanan sistem informasi di penyimpanan data *cloud computing*. Metode naratif kualitatif ialah pendekatan yang bertujuan buat menggambarkan suatu objek penelitian menggunakan memakai sampel atau data yang sudah terkumpul, serta menyimpulkan hasil yang dapat diterapkan secara awam. Metode ini dipilih sebab tim penulis bisa mengungkapkan dan menganalisis berbagai asal data serta isu yang diperoleh, sebagai akibatnya memudahkan pada pembahasan persoalan serta analisis data.

Teknik pengumpulan data yang dipergunakan yaitu studi literatur, yang merujuk pada pengumpulan data menggunakan meneliti banyak sekali sumber seperti buku, literatur, catatan, Artikel serta laporan yang relevan dengan penelitian yang dibahas [6] [7].

1. Review Literatur
   Melakukan pencarian terhadap jurnal-jurnal yang relevan mengenai keamanan penggunaan komputasi awan di berbagai platform seperti Google Scholar. Langkah selanjutnya adalah melakukan tinjauan sistematis dan naratif terhadap literatur terkait, seperti yang akan terjadi penelitian, konsep, teori, serta akibat berasal adopsi layanan *cloud* terhadap Pendidikan.
2. Studi Kasus
   Mencari contoh studi kasus terkait kemanan dalam penggunaan *cloud computing* untuk pembelajaran jarak jauh di sekolah, universitas, atau institusi pendidikan lainnya. Tujuannya adalah untuk memberikan wawasan mengenai potensi celah keamanan dalam *cloud computing*. Sistem *cloud computing* yang fleksibel menawarkan layanan berbasis internet, seperti pelatihan online dan menekankan pengembangan kualitatif serta kuantitatif dalam sains dan pendidikan. *Cloud computing* dapat mengurangi kesenjangan antara pendidikan di kampus dan pembelajaran jarak jauh. Perbedaan tersebut dapat diatasi dengan menggunakan empat lapisan yang terdapat pada *cloud computing*, yaitu sistem awan swasta (untuk sebuah organisasi), awan masyarakat (untuk beberapa organisasi), awan publik (untuk masyarakat umum), *hybrid cloud* (untuk swasta, komunitas, dan masyarakat). *Cloud computing* memiliki beberapa keuntungan, diantaranya adalah:
   a. Pengiriman berbagai layanan cepat
      Cloud computing memungkinkan pengajar untuk dengan cepat menyediakan layanan pendidikan yang dapat meningkatkan pembelajaran dan memungkinkan siswa untuk melakukan pembelajaran individual berdasarkan data kinerja. Serta bisa memaksimalkan gaya belajar yang unik pada masing – masing siswa.
   b. Pengurangan biaya

Virtualisasi dan fitur lain dari *cloud computing* memfasilitasi pemberian layanan dengan biaya yang lebih rendah daripada insfrastruktur tradisional.

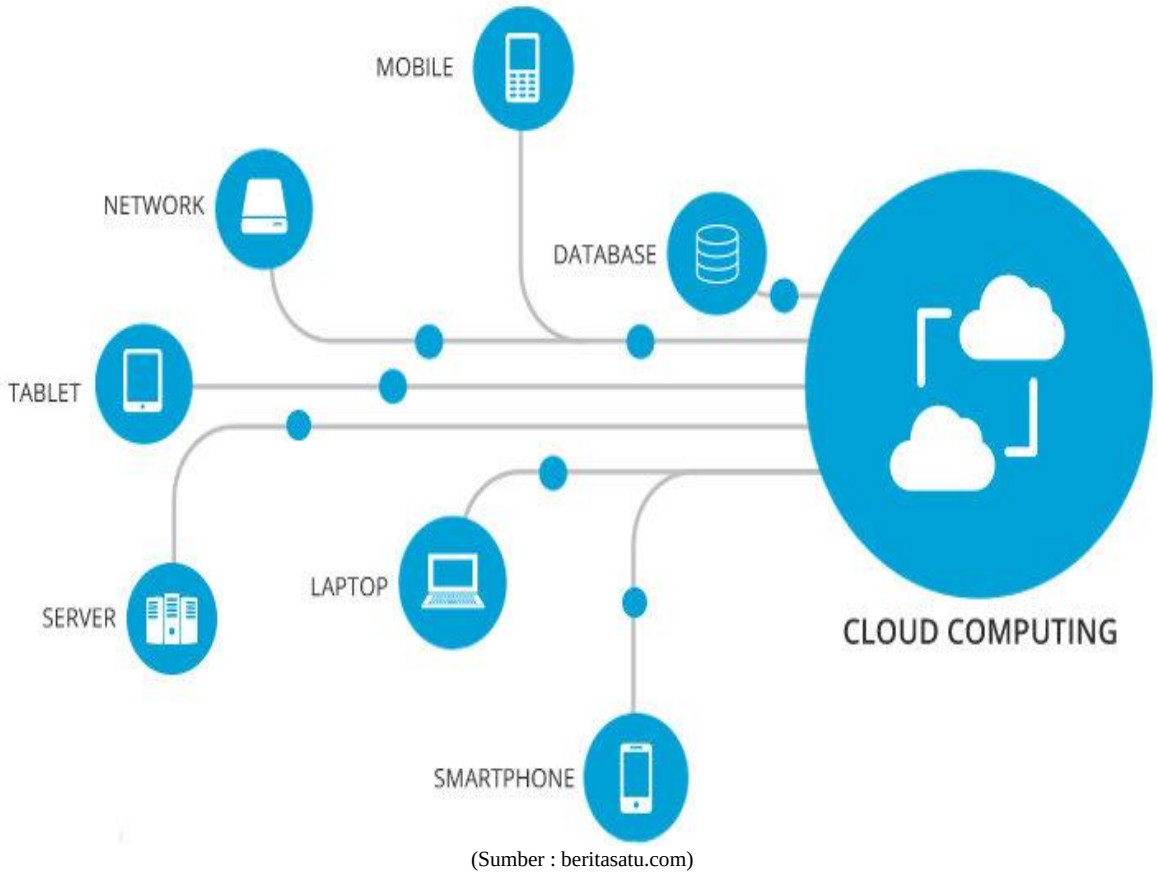
c. Pengurangan risiko dan peningkatan keamanan
Keamanan *cloud* membantu staf IT mengurangi risiko dengan memastikan konsistensi kebijakan keamanan dan penegakan hukum, skalabilitas tinggi dan peningkatan kinerja.

d. Pengembangan pengajaran dan perluasan kolaborasi
Sistem pendidikan berbasis *cloud computing* menawarkan berbagai layanan yang dapat memperluas lingkungan belajar interaktif untuk siapa pun, dan dimana saja. Selain itu, layanan *cloud computing* juga dapat menyederhanakan proses administrasi fakultas atau sekolah.

3. Analisis Data: Mengumpulkan data dari berbagai sumber seperti buku dan jurnal untuk mengevaluasi dan mempelajari implementasi keamanan komputasi awan.
4. Kajian Teoritis: Kajian teoritis ini bertujuan untuk menyelidiki faktor-faktor risiko, strategi perlindungan data, teknologi keamanan yang relevan, serta kebijakan dan regulasi yang memengaruhi implementasi keamanan dalam konteks penyimpanan *cloud.*

4. HASIL DAN PEMBAHASAN

Cloud computing adalah sebuah layanan penyimpanan berbasis internet yang memungkinkan pengguna untuk meyimpan data secara online seperti pada gambar 2. Peningkatan penggunaan layanan *cloud* sangat signifikan karena fasilitasnya yang luas dan aksebilitas yang praktis. Dengan tingginya penggunaan layanan *cloud*, keamanan data pengguna menjadi aspek yang sangat penting dan harus diprioritaskan oleh penyedia layanan cloud. Oleh karena itu, penyedia layanan *cloud* harus memastikan bahwa data pengguna terlindungi dengan baik. Sebagai contoh langkah-langkah keamanan data *cloud* dapat diterapkan untuk melawan potensi peretas yang berusaha mengakses dan mencuri data pengguna [8].



(Sumber : beritasatu.com)

Gambar 2. Mode *Cloud computing*

Ancaman Keamanan pada Penyimpanan *Cloud*

1. Ancaman seperti serangan siber, pencurian data, atau akses tidak sah
Sangat penting buat tahu jenis kejahatan siber ini buat melindungi sistem perbankan syariah dan menjaga kerahasiaan berita keuangan. Pencurian data ialah galat satu bentuk kejahatan siber yang paling umum. Pencurian data dapat dilakukan melalui serangan siber yang ditujukan buat mendapatkan akses tidak legal ke berita sensitif seperti nomor kartu kredit, data keuangan, serta berita eksklusif [9].

2. Analisis dampak ancaman terhadap kerahasiaan, integritas, dan ketersediaan data.
   Mengingat bahwa keamanan siber adalah sistem yang berfungsi buat melindungi isu sistem asal agresi siber (cyberattack) atau segala jenis kejahatan siber (cybercrime), keamanan siber memiliki tiga komponen utama, yaitu Confidentiality(kerahasiaan), Integrity (integritas), Availability (ketersediaan). contoh keamanan siber berfungsi menjadi pedoman untuk kebijakan keamanan informasi dalam sebuah organisasi menjadi sasaran penyelenggaraan keamanan siber [10].

Kontrol Keamanan dan Mitigasi Risiko

1. Kontrol keamanan fisik, teknis, serta administratif untuk melindungi penyimpanan *cloud* model Matriks Risiko mengikuti definisi ISO-27001 perihal paparan risiko. Ini berarti bahwa buat melakukan pengukuran risiko *cloud* computing, pemilik usaha harus menemukan aset eksklusif dan ancaman keamanan teratas terhadap *cloud* computing. di antara konsep yang paling penting untudipertimbangkan pada sini artinya domain keamanan fisik serta logis, dan batas domain yang terkait. Model ini menganggap 3 kategori kontrol: teknis, administratif, serta fisik. Selain itu, contoh mendeskripsikan kontrol ini buat setiap aspek sumber daya komputasi *cloud* [11].
2. Enkripsi data, autentikasi kuat, dan pemantauan keamanan sebagai mitigasi risiko.
   - Enkripsi data: : Data yang dikirim melalui jaringan Internet of Things wajib dienkripsi buat menjaga rahasia serta integritas dalamnya [12].
   - Autentikasi: Sebelum diberikan izin buat mengakses jaringan atau berinteraksi dengan perangkat lainnya, sangat krusial buat memastikan bahwa setiap perangkat yang akan terhubung ke jaringan diidentifikasi dan diauntentikasi dengan benar[12].
   - Pemantauan keamanan: buat mendeteksi serangan atau kegiatan yang mencurigakan pada jaringan, sistem pemantauan dan deteksi ancaman keamanan sangat penting buat dilaksanakan. Ini juga bisa meliputi penggunaan solusi keamanan mirip *Intrusion Detection System (IDS)* atau *Security Information and Event Management (SIEM)* [12].

Tantangan dan Rekomendasi

Tantangan pada menjaga keamanan data pada lingkungan *cloud* yang kompleks beberapa problem utama yang terkait menggunakan proteksi data sensitif termasuk akses yang tidak legal, kompromi identitas, serta kemungkinan data hilang. Meskipun pertumbuhan yang cepat dalam adopsi layanan *cloud* telah membawa poly manfaat, kekhawatiran perihal keamanan dan privasi data yang disimpan dan diproses pada *cloud* [13].

Tantangan Keamanan:

Tugas utama, serta sama pentingnya bagi penyedia layanan *cloud*, artinya memastikan bahwa layanan yang tersedia buat persiapan data tersedia secara memadai serta mudah diakses oleh pengguna. contohnya, penyedia layanan *cloud* bisa penekanan di problem keamanan data pada *cloud (multi-tenancy*, kehilangan kendali, dan kepercayaan) buat memastikan perkara ini terkendali serta memberikan solusi optimal ketika masalah ada [14].

Untuk menghindari risiko, Anda perlu melindungi tidak hanya penyimpanan data Anda, namun pula data yang disimpan, dikirimkan, atau diproses. untuk menaikkan keamanan komputasi awan, penting buat menyediakan otentikasi, otorisasi, serta kontrol akses untuk data yang disimpan pada awan [14].

Tiga bidang utama dalam keamanan data adalah :

1. Kerahasiaan: Kerentanan kunci wajib diperiksa buat memastikan bahwa data Anda terlindungi dari serangan. oleh sebab itu, Anda harus melakukan uji keamanan buat melindungi data Anda asal pengguna dursila, termasuk pembuatan skrip lintas situs dan mekanisme kontrol akses [14].
2. Integritas: Buat mengklaim keamanan data klien, hanya sejumlah mungil asal daya energi yang tersedia yang dipergunakan. Pengguna tidak boleh menyimpan berita eksklusif mirip kata sandi buat memastikan integritas [14].
3. Ketersediaan: Ketersediaan adalah masalah paling penting di beberapa organisasi di mana waktu henti menjadi perhatian utama [14].

Keamanan data dan informasi merupakan tantangan utama dalam layanan *cloud*. Mengenkripsi data dan informasi pengguna *cloud* adalah salah satu metode untuk melindungi data dan informasi mereka.

(Sumber: linkedin.com)

Gambar 3. *Data security*

Cloud computing memungkinkan pengguna untuk terhubung dengan server yang dihosting di Internet guna menyimpan dan memproses data seperti pada gambar 3. Ini memberi mereka kemampuan untuk menggunakan teknologi komputer tanpa perlu menginstalnya di perangkat mereka sendiri. *Cloud* computing menghadirkan tantangan keamanan yang lebih akbar. Tantangan-tantangan ini terbagi dalam 2 kategori akbar yakni duduk perkara keamanan penyedia *cloud* serta duduk perkara keamanan pelanggan [15]. Tantangan dan solusi keamanan *cloud computing* menimbulkan berbagai masalah keamanan dan privasi, antara lain:

1. Pengalihdayaan: Pengguna bisa kehilangan kendali control atas data mereka. Oleh karena itu, diperlukan mekanisme yang tepat untuk mencegah penyedia *cloud* menggunakan data pelanggan dengan cara yang tidak sesuai dengan kesepakatan.
2. Skalabilitas dan Tanggung Jawab Bersama: Terdapat kompromi antara skalabilitas dan tanggung jawab keamanan dalam penerapan yang tidak terkoordinasi dengan baik.
3. Virtualisasi: Harus ada mekanisme untuk memastikan isolasi yang kuat, pembagian yang terkontrol, serta komunikasi antar mesin virtual. Hal ini bisa dicapai menggunakan memakai sistem kontrol akses yang fleksibel untuk menerapkan kebijakan akses yang mengatur kontrol serta membuatkan VM di dalam host *cloud*.
4. Multi-tenancy: Menyediakan lingkungan multi-tenant yang aman memerlukan pertimbangan duduk perkara mirip kebijakan akses, penyediaan serta akses aplikasi, serta proteksi data.
5. Perjanjian Tingkat Layanan: Tujuan utamanya ialah buat menciptakan taraf baru dalam negosiasi kontrak antara penyedia serta konsumen layanan dan memantau pemenuhannya selama implementasi.
6. Heterogenitas: Penyedia *cloud* yang berbeda dapat menerapkan metode dan pendekatan keamanan yang bervariasi untuk melindungi data, sehingga menimbulkan tantangan dalam hal integrasi.

Rekomendasi Keamanan

Rekomendasi buat praktik terbaik keamanan, pembinaan kesadaran, serta kerja sama antara pengguna serta penyedia *cloud* pada menaikkan kesadaran perihal praktik keamanan data terbaik serta menaikkan pemahaman ihwal ancaman keamanan potensial, mirip serangan phishing atau rekayasa sosial [16].

Cloud computing menjadi salah satu teknologi jaringan penyimpanan data yang sedang berkembang pesat ketika ini, tidak sporadis data yang disimpan pada *cloud computing* merupakan data penting serta rahasia yang tidak semua orang bisa mengaksesnya. Oleh sebab itu, keamanan data menjadi sangat penting. poly pakar dan

praktisi menyatakan bahwa *Enterprise Computing* merupakan suatu duduk perkara sudah selesai, cenderung stabil serta statis, serta tidak memerlukan peningkatan yang signifikan.

Perkembangan ilmu pengetahuan dan teknologi terbaru sudah mempermudah serta memudahkan melakukan tugas sehari-hari yang tak dapat dilakukan di saat yang bersamaan. Dalam global teknologi isu serta komunikasi, pemanfaatan software *cloud computing* menjadi salah satu pilihan terbaik buat mengatasi permasalahan di atas [17].

Keamanan pada lingkungan *cloud computing* perlu mempertimbangkan beberapa hal utama yang melibatkan perusahaan, organisasi dan institusi yang menggunakan layanan *cloud* [18], beberapa rekomendasi yang perlu dipertimbangkan diantaranya:

1. Kemungkinan Kebocoran Data (Data Leakage)
   Kebocoran data bisa terjadi bila data yang disimpan di *cloud* tidak dikelola menggunakan baik ancaman tadi bisa timbul berasal penggunaan tidak legal oleh karyawan, kesalahan pada konfigurasi, atau agresi siber yang berhasil. Memastikan enkripsi data yang efektif serta penerapan manajemen perizinan yang ketat artinya langkah krusial buat mencegah kebocoran data.
2. Pentingnya Kepatuhan Regulasi
   Banyak organisasi harus mematuhi hukum tertentu yang berkaitan menggunakan privasi data, seperti GDPR pada Uni Eropa atau HIPAA di Amerika perkumpulan. Menyelaraskan penyimpanan serta manajemen data pada *cloud* menggunakan persyaratan hukum artinya tantangan besar.
3. Keamanan API (*Application Programming Interface*)
   banyak software *cloud* mengandalkan barah buat interaksi. Tantangan keamanan terkait dengan penggunaan api meliputi melindungi asal agresi mirip pencurian kunci barah, penolakan layanan, atau pendayagunaan melalui antarmuka yang tidak aman.
4. Pemantauan dan Deteksi Ancaman
   Mengenali potensi ancaman siber dan tindakan mencurigakan pada lingkungan *cloud* bisa menjadi tantangan. Memantau dengan efektif serta memahami pola sikap yang normal dan tidak biasa bisa membantu mengidentifikasi agresi siber secara lebih cepat.
5. Keamanan Akses dan Identitas
   Perlunya memastikan bahwa hanya entitas yang berwenang yang dapat mengakses data dan asal daya pada lingkungan *cloud*. Manajemen identitas serta akses yang sesuai, termasuk penggunaan otentikasi ganda, pengaturan kiprah, dan pemantauan kegiatan akses, menjadi sangat penting buat mencegah akses yang tidak legal.

5. KESIMPULAN

Cloud computing sudah merevolusi cara kita mengelola data dan perangkat lunak. Fleksibilitas, skalabilitas, dan efisiensi biaya yang ditawarkannya membentuk teknologi ini semakin populer pada kalangan usaha. namun, di balik segala kemudahannya, *cloud* computing pula menghadirkan tantangan tersendiri, terutama pada hal keamanan siber. Analisis kerentanan terhadap sistem *cloud* berkata sejumlah kelemahan yang dapat dimanfaatkan oleh para pelaku kejahatan siber. Kerentanan-kerentanan ini bisa muncul dari berbagai sumber, mulai dari konfigurasi yang keliru, kelemahan di *software*, sampai kesalahan manusia. agresi siber yang berhasil dapat mengakibatkan kerugian finansial yang akbar, kerusakan reputasi, serta bahkan pelanggaran privasi data pelanggan. buat mengatasi tantangan keamanan siber di lingkungan *cloud*, diperlukan pendekatan yang komprehensif. Organisasi perlu menerapkan langkah-langkah keamanan yang ketat, mirip enkripsi data, autentikasi multi-faktor, dan pemantauan aktivitas yang mencurigakan. Selain itu, penting juga buat melakukan pembaruan perangkat lunak secara berkala serta memberikan *training* keamanan kepada karyawan. dengan demikian, organisasi bisa meminimalkan risiko agresi siber dan melindungi aset digital mereka.

DAFTAR PUSTAKA

[1] M. Hossain, R. Khan, S. Al Noor, and R. Hasan, "Jugo: A Generic Architecture for Composite Cloud as a Service," Institute of Electrical and Electronics Engineers (IEEE), Jan. 2017, pp. 806–809. doi: 10.1109/cloud.2016.0112.

[2] G. Manogaran, C. Thota, and M. V. Kumar, "MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing," in Procedia Computer Science, Elsevier B.V., 2016, pp. 128–133. doi: 10.1016/j.procs.2016.05.138.

[3] Direktorat Operasi Keamanan Siber, "LANSKAP KEAMANAN SIBER INDONESIA 2023," Jakarta, Dec. 2023.

[4] M. E. Abiezal and I. Afrianto, "Tinjauan Literatur: Keamanan Cloud di Era Digital Menangani Ancaman Saat Ini dan Memastikan Privasi Data." [Online]. Available: https://www.researchgate.net/publication/368542573

[5] Z. Masyhur, A. Rizaldy, P. Kartini, and D. Publikasi, "Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive," 2021.

[6] B. G. Sudarsono, I. Zulkarnain, E. Buulolo, and D. P. Utomo, "Analisa Penerapan Metode MOOSRA dan MOORA dalam Keputusan Pemilihan Lokasi Usaha," Building of Informatics, Technology and Science (BITS), vol. 4, no. 3, pp. 1456–1463, Dec. 2022, doi: 10.47065/bits.v4i3.2696.

[7] A. G. Santika, R. G. Whendasmoro, and I. Zulkarnain, "Aplikasi Manajemen Komplain Gedung Plaza Setiabudi Menggunakan Framework Ionic," Eksplorasi Teknologi Enterprise & Sistem Informasi (EKSTENSI), vol. 1, no. 1, p. 037045, 2022, [Online]. Available: https://journal.fikom.site/ekstensiCommonsAttribution4.0

[8] P. M. Kumar, "Enhanced Cloud Data Security Using AES Algorithm," 2019. [Online]. Available: https://www.researchgate.net/publication/334963833

[9] J. L. Keuangan et al., "Asy-Syarikah," vol. 5, no. 2, p. 2023, [Online]. Available: http://journal.uiad.ac.id/index.php/asy-syarikah

[10] P. Keamanan Siber Dalam Mengatasi Konten Negatif, L. Siagian, A. Budiarto, and P. Strategi Pertahanan Udara Universitas Pertahanan, "THE ROLE OF CYBER SECURITY IN OVERCOME NEGATIVE CONTENTS TO REALIZE NATIONAL INFORMATION RESILIENCE."

[11] "jitter_herdian,+03+Rusdan_JitterAgustus19_20191128".

[12] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, "Jurnal Sistim Informasi dan Teknologi https://jsisfotek.org/index.php Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," vol. 5, no. 2, 2023, doi: 10.37034/jsisfotek.v5i1.232.

[13] "Jurnal+Suhada+Kohesi".

[14] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," in Procedia Computer Science, Elsevier B.V., 2015, pp. 204–209. doi: 10.1016/j.procs.2015.04.171.

[15] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," in Procedia Computer Science, Elsevier B.V., 2014, pp. 357–362. doi: 10.1016/j.procs.2014.08.053.

[16] F. Indriyajati, M. Margarith, S. Damiana Jawa, and H. Utomo, "Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia Article Info ABSTRAK," vol. 02, no. 01, pp. 59–66, doi: 10.58812/smb.v2i01.

[17] A. Nugroho, "PELATIHAN PEMANFAATAN GOOGLE DRIVE UNTUK MANAJEMEN DOKUMEN DAN FILE DI PEMERINTAHAN DESA SIDOWANGI KABUPATEN MAGELANG".

[18] A. Wijoyo, A. R. Silalahi, A. Raihan, P. Arrasyid, and R. Diana, "Sistem Informasi Manajemen Berbasis Cloud", [Online]. Available: https://jurnalmahasiswa.com/index.php/teknobis