p-ISSN: 2502-3691
e-ISSN: 2502-4361

Strategi Keamanan Data pada Database Cloud Computing Pencegahan dan Perlindungan untuk Pengguna Layanan

Muchamad Aries Firmansyah[1*], Dinar Auranisa Moonap[2], Maulana Izaki[3]
[1,2]Teknik Informatika, Fakultas Teknik, STMIK YMI TEGAL, Tegal
[3]Magister Teknik Informatika, Universitas Dian Nuswantoro, Semarang
[1,2]Jalan Pendidikan No. 1, Kelurahan Pesurungan Lor, Kota Tegal, 52142, Indonesia
[3]Jalan Imam Bonjol No. 207, Pendrikan Kidul, Kota Semarang, 50131, Indonesia
email: [1]ariessafy09@gmail.com, [2]dinarauranisamoonap@gmail.com, [3]maulana.izaki@gmail.com

Abstract **– Cloud Computing is a strategic solution in information technology data management that offers an innovative approach to sharing computing resources over the internet. This research analyzes the security strategy of cloud database services with a focus on Confidentiality, Integrity, and Availability (CIA) aspects, using a literature study method from reputable journals. The results identified several security threats in cloud database services, including internal threats, external attacks, access control issues, illegal data recovery, network breaches, and data origin complexity. The research proposed a four-layer security structure consisting of: user interface layer, service access layer, database management layer, and data storage layer, where encryption, authentication, and access control are emphasized as critical components in protecting data confidentiality, integrity, and availability. The conclusion shows that cloud database services offer advantages in terms of minimizing infrastructure and human resources at a relatively affordable cost, but the security aspect requires special attention to handle the various threats that exist. For further development, it is recommended to conduct research using journal reference sources in a longer time span to get a more comprehensive perspective on the development of cloud database security.**

Abstrak **– Cloud Computing telah menjadi solusi strategis bagi manajemen data dalam industri teknologi informasi, menawarkan pendekatan inovatif untuk berbagi sumber daya komputasi melalui jaringan internet. Penelitian ini bertujuan menganalisis strategi keamanan layanan database cloud dengan fokus pada aspek Confidentiality, Integrity, dan Availability (CIA). Metode penelitian menggunakan studi literatur melalui pengumpulan dan analisis jurnal-jurnal terkemuka dengan kata kunci layanan database cloud . Hasil penelitian mengidentifikasi berbagai ancaman keamanan dalam layanan database cloud, seperti ancaman internal, serangan eksternal, masalah kontrol akses, pemulihan data ilegal, pelanggaran jaringan, dan kompleksitas asal data. Setiap ancaman dianalisis dengan memperhatikan mekanisme pencegahan dan dampaknya terhadap keamanan data. Struktur keamanan yang diusulkan meliputi empat lapis: lapisan antarmuka pengguna, lapisan akses layanan, lapisan manajemen database, dan lapisan penyimpanan data. Penelitian menekankan pentingnya enkripsi, otentikasi, dan kontrol akses dalam melindungi kerahasiaan, integritas, dan ketersediaan data. Kesimpulan menunjukkan bahwa layanan database cloud dapat meminimalkan infrastruktur dan sumber daya manusia dengan biaya relatif murah, namun memerlukan disarankan untuk memperluas kajian dengan menggunakan jurnal dalam rentang waktu yang lebih panjang.**

Kata Kunci **– Cloud Computing, Keamanan Database, Confidentiality, Integrity, Availability**

*) **penulis korespondensi**: Muchamad Aries Firmansyah
Email: ariessafy09@gmail.com

I. PENDAHULUAN

Industri teknologi informasi masa kini dihadapkan pada tantangan utama untuk mengelola volume data yang terus berkembang sambil menghasilkan perangkat lunak berkualitas tinggi dengan penggunaan sumber daya yang efisien dan biaya minimal [1]. Sebagai solusi, penyedia layanan internet mengembangkan Cloud Computing untuk mendukung jumlah pengguna maksimal dengan layanan yang optimal menggunakan sumber daya terbatas [2]. Cloud Computing telah menjadi teknologi yang sangat populer dalam beberapa tahun terakhir. Layanan cloud, khususnya dalam manajemen database, memiliki peran penting karena menyediakan akses terpusat ke berbagai sumber daya seperti perangkat keras, perangkat lunak, dan informasi [3]. Model layanan database berbasis cloud membebaskan pemilik aplikasi dari tugas instalasi dan pemeliharaan database, sebaliknya, penyedia layanan database bertanggungjawab penuh atas aspek teknis, sementara pemilik aplikasi cukup membayar sesuai dengan tingkat penggunaan layanan mereka. Pendekatan ini memungkinkan efisiensi dan fleksibilitas yang lebih besar dalam pengelolaan sumber daya teknologi informasi, menjadikan Cloud Computing sebagai solusi strategis bagi perusahaan yang ingin mengoptimalkan infrastruktur teknologi sekarang [4].

Sistem manajemen basis data cloud merupakan pendekatan inovatif dalam komputasi yang menawarkan database terdistribusi sebagai layanan, bukan sekadar produk konvensional. Teknologi ini memungkinkan berbagi sumber daya, perangkat lunak, dan informasi di antara berbagai perangkat melalui jaringan, dengan internet sebagai infrastruktur utama [5]. Lingkungan komputasi awan menyediakan platform komprehensif untuk berbagi sumber daya komputasi dan menawarkan beragam layanan seperti Software as a Service (SaaS), Platform as a Service (PaaS), dan Infrastructure as a Service (IaaS). Organisasi dapat memanfaatkan model layanan ini dalam berbagai konfigurasi, termasuk lingkungan pribadi, publik, atau hibrida sesuai kebutuhan spesifik mereka. Pada dasarnya, komputasi awan dikenal dengan konsep *Everything as-a-Servic*, yang mencerminkan fleksibilitas dan kemampuan adaptif teknologi ini. Keunikan utamanya terletak pada penggunaan sumber daya terdistribusi secara global melalui jaringan luas seperti internet,

p-ISSN: 2502-3691
e-ISSN: 2502-4361

memungkinkan akses, skalabilitas, dan efisiensi yang belum pernah ada sebelumnya dalam pengelolaan dan pemanfaatan sumber daya komputasi.

Cloud Computing adalah model penyediaan layanan komputasi yang memungkinkan pengguna untuk mengakses berbagai sumber daya teknologi informasi (TI) seperti penyimpanan data, server, jaringan, perangkat lunak, dan platform pengembangan secara *on-demand* melalui internet. Model ini dirancang untuk memberikan fleksibilitas, efisiensi, dan skalabilitas tinggi, tanpa perlu investasi besar dalam infrastruktur fisik.

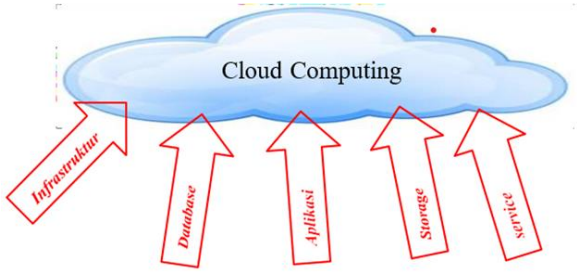

Figure 1. Lima Macam Layanan Cloud

1. Layanan *Cloud Computing*

   Ada lima layanan dalam *cloud computing* yaitu

   a) Perangkat lunak sebagai layanan (Sas), Layanan ini menyediakan infrastruktur TI seperti server, jaringan, dan penyimpanan secara virtual melalui internet. Pengguna dapat menyewa sumber daya tersebut sesuai kebutuhan tanpa harus memiliki perangkat keras fisik. Contoh layanan IaaS adalah Amazon Web Services (AWS) dan Microsoft Azure.

   b) atabase (Database as a Service, DBaaS), DBaaS memungkinkan pengguna untuk mengelola database tanpa harus menangani aspek teknis seperti pengaturan server, pembaruan perangkat lunak, atau pencadangan data. Layanan ini mendukung skalabilitas, integritas data, dan keamanan yang tinggi. Contoh DBaaS meliputi Google Cloud SQL dan MongoDB Atlas.

   c) Aplikasi (Software as a Service, SaaS), SaaS memberikan akses ke aplikasi perangkat lunak melalui internet tanpa perlu instalasi di perangkat pengguna. Layanan ini umumnya digunakan untuk aplikasi berbasis web seperti pengelolaan dokumen, perangkat lunak akuntansi, atau CRM (Customer Relationship Management). Contoh layanan SaaS adalah Google Workspace dan Salesforce.

   d) Storage (Storage as a Service), Layanan ini memungkinkan pengguna menyimpan, mengakses, dan mengelola data mereka di cloud. Penyimpanan cloud sangat fleksibel, memungkinkan penggunanya untuk menambah atau mengurangi kapasitas penyimpanan sesuai kebutuhan. Contoh penyedia layanan ini adalah Dropbox, Google Drive, dan Amazon S3.

   e) Service (Platform as a Service, PaaS), PaaS menyediakan platform pengembangan dan penerapan aplikasi. Layanan ini mencakup alat pengembangan, sistem operasi, dan infrastruktur yang diperlukan, sehingga memudahkan pengembang untuk membangun aplikasi tanpa perlu memikirkan pengelolaan infrastruktur. Contoh PaaS adalah Heroku dan Google App Engine.

2. Karakteristik cloud computing

   a) On-Demand Self-Service. Pengguna dapat mengakses layanan komputasi seperti penyimpanan, aplikasi, atau server secara mandiri kapan saja tanpa memerlukan interaksi langsung dengan penyedia layanan. Hal ini memberikan kemudahan dan fleksibilitas dalam mengelola kebutuhan komputasi.

   b) Broad Network Access. Layanan cloud dapat diakses melalui jaringan internet dari berbagai perangkat, seperti komputer, laptop, tablet, dan smartphone. Akses yang luas ini memungkinkan mobilitas pengguna, sehingga mereka dapat bekerja dari mana saja dan kapan saja selama terhubung ke internet.

   c) Resource Pooling. Sumber daya komputasi seperti penyimpanan, memori, dan prosesor dikumpulkan dan didistribusikan secara dinamis di antara banyak pengguna. Dengan menggunakan teknologi virtualisasi, sumber daya dapat dialokasikan secara efisien sesuai kebutuhan pengguna, tanpa mereka mengetahui lokasi fisik sumber daya tersebut.

   d) Elastisitas yang cepat. Kapabilitas dapat disediakan dan dilepaskan secara elastis, dalam beberapa kasus secara otomatis, untuk menyesuaikan dengan cepat ke luar dan ke dalam yang sesuai dengan permintaan. Bagi konsumen, kemampuan yang tersedia untuk penyediaan seringkali tampak tidak terbatas dan dapat disesuaikan dalam jumlah berapa pun dan kapan pun.

   e) Layanan terukur. Sistem cloud secara otomatis mengontrol dan mengoptimalkan penggunaan sumber daya dengan memanfaatkan kapabilitas pengukuran pada beberapa tingkat abstraksi yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, bandwidth, dan akun pengguna aktif). Penggunaan sumber daya dapat dipantau, dikendalikan, dan dilaporkan, memberikan transparansi bagi penyedia dan konsumen layanan yang digunakan.

3. Layanan Cloud Database

   Layanan database menyediakan secara otomatis konsumen bisa meminta fungsionalitas dari layanan khusus yang dihosting di Cloud. Ada banyak layanan basis data lain yang tersedia saat ini tetapi layanan database berbeda dari basis data tradisional karena arsitekturnya memiliki dua atribut utama yaitu: Berorientasi layanan karena fasilitas basis data tersedia dalam bentuk layanan. Model interaksi layanan mandiri pelanggan karena organisasi

p-ISSN: 2502-3691
e-ISSN: 2502-4361

diizinkan untuk menggunakan, mengonfigurasi, dan menyebarkan layanan database Cloud itu sendiri tanpa dukungan TI apa pun dan tanpa membeli perangkat keras apa pun untuk tujuan yang ditentukan. Tiga fase utama dalam arsitektur layanan database secara keseluruhan lihat gambar 2.

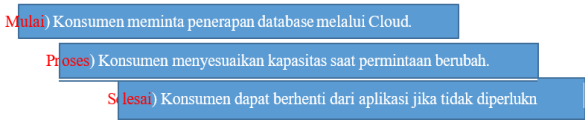

Figure 2 Lapisan Keamanan

4. Struktur Empat Lapis Keamanan Layanan Database
   Model yang ditunjukkan pada gambar 3. menggunakan struktur sistem empat lapis, setiap lapis melakukan tugasnya sendiri untuk memastikan keamanan data dari lapisan Cloud.
   a. Lapisan pertama: Lapisan ini berfungsi sebagai titik awal interaksi pengguna dengan sistem. Dalam lapisan ini, mekanisme autentikasi seperti *Single Sign-On* (SSO) diterapkan untuk memastikan bahwa hanya pengguna yang sah dapat mengakses sistem. Dengan menyediakan kontrol akses berbasis identitas, lapisan ini bertujuan melindungi sistem dari penyusupan dan memastikan keamanan data sejak awal proses interaksi.
   b. Lapisan kedua: Lapisan aplikasi bertanggung jawab untuk mengelola kontrol akses, menjalankan layanan web, dan menangani unggahan data. Dalam lapisan ini, *Access Control* digunakan untuk memastikan bahwa hanya pengguna tertentu yang dapat mengakses data atau fitur tertentu. Selain itu, web server berperan sebagai penghubung antara antarmuka pengguna dan database backend. Fitur unggah data juga diawasi untuk memastikan bahwa data yang dimasukkan ke dalam sistem aman dan bebas dari potensi ancaman.
   c. Lapisan ketiga lapisan ini berperan sebagai pusat penyimpanan data yang dikelola di lingkungan cloud atau server lokal. Tugas utama lapisan ini adalah menyediakan penyimpanan yang aman dan efisien untuk mendukung operasi sistem. Selain itu, lapisan ini memastikan ketersediaan dan konsistensi data, sehingga dapat diakses kapan saja oleh aplikasi atau pengguna yang berwenang.
   d. Lapisan keempat Lapisan penyimpanan data adalah lini terakhir pertahanan dalam sistem keamanan. Di sini, data dilindungi melalui enkripsi untuk mencegah akses tidak sah. Integritas data juga dijaga agar tetap utuh dan tidak dimodifikasi oleh pihak yang tidak berwenang. Selain itu, lapisan ini menyediakan mekanisme pemulihan data yang memungkinkan sistem untuk mengembalikan data yang hilang atau rusak akibat kegagalan perangkat keras atau serangan siber.

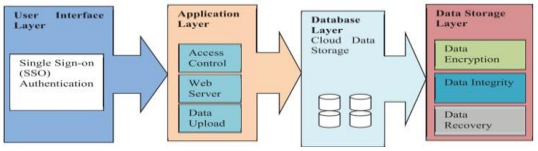

Figure 3 Model layanan keamanan

5. Prinsip Keamanan Informasi
   Keamanan sistem informasi bertujuan untuk menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk perangkat keras , perangkat lunak, informasi / data, dan telekomunikasi). Konsep keamanan kerahasiaan, integritas dan ketersediaan juga disebut triad CIA.
   a. Kerahasiaan informasi biasanya dilihat sebagai jaminan bahwa informasi sensitif hanya diakses oleh pengguna yang berwenang. Tugas ini dapat dicapai dengan berbagai mekanisme seperti enkripsi dan kontrol akses.
   b. Integritas informasi biasanya dilihat sebagai jaminan bahwa informasi tidak di rubah oleh pengguna yang tidak sah sedemikian rupa sehingga pengguna yang sah yang akan dapat merubahnya. Tugas ini dapat dicapai dengan berbagai mekanisme seperti tanda tangan digital dan kode otentikasi pesan.
   c. Ketersediaan adalah tugas untuk memastikan bahwa suatu sistem menyediakan layanannya kepada penggunanya kapan saja. Biasanya sebuah sistem mencakup banyak mekanisme untuk memastikan ketersediaannya, seperti penggunaan beberapa sumber daya independen dan beberapa jalur komunikasi.

II. METODE PENELITIAN

Hasil Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur untuk menganalisis isu-isu terkait keamanan database cloud sebagai layanan (*Database as a Service* atau DBaaS). Pendekatan ini dilakukan dengan mengumpulkan, menganalisis, dan mensintesis berbagai jurnal ilmiah, artikel, dan laporan teknis yang membahas aspek keamanan dalam DBaaS.

III. HASIL DAN PEMBAHASAN

Layanan database cloud harus memperhatikan berbagai ancaman dan pencegahan dilihat dari aspek keamanan (CIA) secara menyeluruh, dapat dilihat pada tabel 1.

No	Ancaman	pencegahan	cia
1	Ancaman Orang Dalam	· Karyawan dapat · memanfaatkan data sensitif dan rahasia . Manajemen dan penilaian rantai pasokan yang ketat diperlukan	*Confidenciality*

p-ISSN: 2502-3691
e-ISSN: 2502-4361

2	Penyerang dari luar Berbahaya	· Serangan · berbahaya oleh peretas. Tidak adanya otentikasi, otorisasi dan akuntansi kontrol dapat mengakibatkan serangan	*Confidenciality*
3	Masalah Kontrol Akses	Pemilik data tidak dapat menentukan atau mengubah kebijakan sesuai kebutuhan. · Peningkatan biaya pengembangan dan analisis terjadi saat pengelolaan pengguna dan akses *granular* kontrol diterapkan	*Confidenciality*
4	Pemulihan Data Ilegal dari Perangkat Penyimpanan	· Lakukan *degaussing*, pemusnahan dan penimpaan data untuk menghindari kebocoran data. · Pemulihan data oleh sumber berbahaya jika tidak dibuang dengan benar	*Confidencialit y*
5	Pelanggaran Jaringan	Data yang mengalir melalui jaringan (internet) rentan terhadap keadaan berbahaya dan masalah kinerja jaringan. · Kemungkinan penyebab kegagalan jaringan adalah: kesalahan konfigurasi, kurangnya isolasi sumber daya, kelangsungan bisnis yang buruk atau belum teruji, rencana pemulihan bencana, modifikasi lalu lintas jaringan	*Confidencialit y*
6	Asal Data	· Kompleksitas · dan kepekaan waktu dalam metadata asal. Perhitungan intensif terlibat dalam mendapatkan riwayat yang dibutuhkan. · Algoritma cepat, log otomatis diperlukan	*Confidencialit y*
7	Kegagalan Rantai Pasokan	Keamanan bergantung pada pihak ketiga saat data dialihdayakan	*Confidencialit y*
8	Lokalitas Data	· Masalah kepatuhan dan keamanan data, undang-undang privasi melarang perpindahan data sensitif antar negara. · Masalah yang dihadapi ketika tidak ada yang bertanggung jawab atas data di lokasi penyimpanan data *independen*	*Confidencialit y*
9	Yurisdiksi yang Bervariasi	Resiko dan batasan yang dihadapi ketika data pelanggan tunduk pada yurisdiksi hukum beberapa negara. · Data dalam situasi ini dapat diakses oleh banyak pihak	*Confidencialit y*
10	*Arsitektur Proxy*	· Mengurangi kebutuhan penggunaan komponen perantara. Metadata dipindahkan ke database.	*Confidentialit y*

p-ISSN: 2502-3691
e-ISSN: 2502-4361

		Mesin enkripsi dijalankan oleh setiap klien. · Skalabilitas, keamanan dan konsistensi data	
11	Homo-morphic penuh	· kueri terenkripsi data algoritma dimungkinkan. · Evaluasi Algoritma digunakan selain pembuatan kunci, enkripsi dan dekripsi	*Confidentiality*
12	Penyimpanan data	· Enkripsi sisi · klien dengan · cepat digunakan. Menggunakan Algoritma SHA-512 untuk kontrol integritas. AES-256 digunakan untuk enkripsi. · Pengguna tidak lagi harus mengelola kunci secara manual.	*Integrity*
13	Pemeriksaan Integritas	· Modifikasi konfigurasi, akses dan file data merupakan ancaman terhadap integritas data. · Membutuhkan akurasi dan integritas data	*Integrity*
14	*Data Lock-In*	· Pelanggan tidak dapat memindahkan data dari satu situs ke situs lainnya. · Kegagalan layanan yang disediakan oleh satu vendor akan mengakibatkan hilangnya data secara keseluruhan. · Perlu API standar untuk dijalankan di bawah platform setiap penyedia	*Availability*
15	Pendekatan Pencadangan	· Server cadangan disimpan di lokasi yang jauh. · Meode enkripsi dan dekripsi tradisional digunakan dengan dua langkah autentikasi. · Enkripsi dilakukan selama operasi pencadangan.	*Availability*

IV. KESIMPULAN

Penelitian ini mengidentifikasi aspek keamanan layanan database cloud berdasarkan kerangka CIA (Confidentiality, Integrity, dan Availability). Layanan cloud database ini menawarkan keunggulan dalam mengoptimalkan infrastruktur dan sumber daya manusia dengan biaya yang relatif terjangkau. Mengingat berbagai keunggulan yang ditawarkan oleh penyedia layanan cloud, calon pengguna yang berencana migrasi database perlu memperhatikan faktor keamanan dengan seksama. Untuk penelitian selanjutnya, disarankan untuk memperluas kajian dengan melakukan tinjauan jurnal dalam rentang waktu yang lebih panjang, sehingga dapat mengumpulkan referensi yang lebih komprehensif untuk menganalisis aspek Confidentiality, Integrity, dan Availability secara mendalam.

DAFTAR PUSTAKA

Journal Article

[1] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in iot-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, 2021.

[2] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions," *Comput. Commun.*, 2023.

[3] W. N. Hussein, H. N. Hussain, H. N. Hussain, and A. Q. Mallah, "A deployment model for IoT devices based on fog computing for data management and analysis," *Wirel. Pers. Commun.*, pp. 1–13, 2023.

[4] D. Lepore, N. Testi, and E. Pasher, "Building inclusive smart cities through innovation intermediaries," *Sustainability*, vol. 15, no. 5, p. 4024, 2023.

[5] A. Amaithi Rajan and V. V, "Systematic survey: secure and privacy-preserving big data analytics in cloud," *J. Comput. Inf. Syst.*, vol. 64, no. 1, pp. 136–156, 2024.