E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 3 No 7 Tahun 2024, Hal 23-97

TEKNIK PELESTARIAN PRIVASI DATA DI DATABASE CLOUD

Raisida Salwa, Muhammad Irwan Padli Nasution
Fakultas Ekonomi Dan Bisnis Islam Universitas Islam Negeri Sumatera Utara
Korespondensi Penulis: rysdslw@gmail.com

Abstrack. *In an era technological advancement and internet proliferation, data privacy whitin the realm of cloud computing is increasingly emphasized. This article discusses varios aspects related to data privacy, such as safeguarding user identities, maintaining information confidentiality, and managing data usage. The research methodology employed is a qualitative approach, focusing on case study analyses to comprehend how data privacy is upheld whitin cloud database systems. The article also identifies attributes of privacy preservation, including the use of encryption, audit processes, implementation of secure data transfer protocols, and trustworthy key management. The utilization of cryptographic technology stands aout as a key aspect in ensuring security and confidentiality whitin cloud storage environments.*
Keyword: *Privacy, Privacy Preservation, Cloud, Cloud Data Storage*

Abstrak. Dalam era kemajuan teknologi dan internet, privasi data di dalam lingkungan cloud computing semakin ditekankan.Artikel ini membahas berbagai aspek yang terkait dengan privasi data, seperti perlindungan identitas pengguna, kerahasiaan informasi dan penggunaan data. Metode penelitian yang digunakan adalah pendekatan kualitatif yang menekankan pada analisis studi kasus untuk memahami bagaimana privasi data dipertahankan di dalam database cloud. Artikel ini juga mengidentifikasi atribut pelestarian privasi, termasuk penggunaan enkripsi, proses audit, penerapan protokol transfer data yang aman, serta manajemen kunci yang terpercaya. Penggunaan teknologi kriptografi menjadi salah satu aspek utama dalam menjaga keamanan serta kerahasiaan informasi di lingkungan penyimpanan cloud.
Kata kunci: Privasi, Pelestarian Privasi, Cloud, Penyimpanan Data Cloud

LATAR BELAKANG

Privasi data dapat dijelaskan dengan berbagai aspek, termasuk privasi identitas yaitu, merahasiakan identitas pengguna, kecuali bagi entitas yang berwenang, privasi data yaitu menjaga kerahasiaan data, kecuali untuk pengguna berwenang, dan privasi penggunaan, adalah menyembunyikan aktivitas pengguna, kecuali bagi pihak yang berwenang. Dengan perkembangan cepat internet dan bidang informatika, perlindungan privasi semakin penting di ranah digital. Serangan terhadap privasi bisa mengakibatkan gangguan pada layanan penyimpanan cloud, yang berpotensi menimbulkan kerugian finansial baik bagi pengguna maupun penyedia layanan. Hal ini membantu membatasi akses terhadap data sensitif seperti kata sandi, informasi identitas, dan infromasi lainnya yang dapat membahayakan pemerintah, organisasi, atau masyarakat jika jatuh ke tangan yang salah.

Cloud sering kali diartikan sebagai representasi metaforis dari internet yang umumnya dikenal, tetapi ketika digabungkan dengan computing, maka maknanya akan menjadi luas. Computing cloud adalah paradigma baru yang sangat otomatis dan didasarkan pada utilitas, yang mencakup server, alokasi layanan untuk jaringan computer melalui internet, memfasilitasi penerapan manajemen data yang aman dengan mudah dan fleksibel. Hal ini menyebabkan tersedianya standart ketersediaan tinggi, interoperabilitas, dan skalabilitas yang berkelanjutan untuk perangkat keras dan perangkat lunak, yang memastikan kerahasiaan data. Penyimpanan Cloud adalah sistem yang memungkinkan pengguna untuk menyimpan data sensitif dan pribadi mereka secara aman, memungkinkan akses dari mana saja, kapan saja dan dari perangkat apapun yang sah.

Dalam konteks ini, artikel ini bertujuan untuk membahas pendekatan yang digunakan untuk mengatasi teknik pelestarian privasi data. Latar belakang privasi data akan menjadi landasan bagi pembaca untuk memahami urgensi dari pembahasan ini.

METODE PENELITIAN

Dalam mendukung eksploitasi konsep pelestarian privasi data di database cloud. Artikel ini mengambil pendekatan penelitian kualitatif dengan fokus pada studi kasus. Pendekatan kualitatif dipilih karena memberikan ruang yang lebih luas untuk memahami konteks dan dinamika sebenarnya dari proses pelestarian privasi data. Studi kasus dipilih sebagai desain penelitian dipilih karena memungkinkan analisis mendalam terhadap beberapa organisasi yang telah berhasil melestarikan privasi data di database cloud.

Artikel ini bertujuan untuk memberikan pemahaman yang mendalam tentang tantangan dalam keamanan, baik dari perspektif perangkat lunak maupun perangkat keras, untuk melindungi data di lingkungan cloud, dengan tujuan meningkatkan keamanan data dan privasi dalam lingkungan cloud yang dapat dipercaya.

HASIL DAN PEMBAHASAN

A. Sistem Manajemen Basis Data Cloud

Sistem manajemen basis data cloud merupakan sebuah sistem basis data terdistribusi yang menyediakan layanan komputasi daripada sekedar produk. Hal ini melibatkan pembagian sumber daya, perangkat lunak, dan informasi di antara beberapa perangkat melalui jaringan, terutama internet. Lingkungan computing cloud menyediakan platform untuk ini. Pengguna computing cloud melibatkan berbagi sumber daya terdistribusi di seluruh dunia melalui jaringan luar seperti internet yang dapat menimbulkan berbagai masalah keamanan. Berbeda dengan computer pribadi yang memberikan kontrol penuh atas data dan proses, lingkungan cloud menggunakan data dan layanan aplikasi dari penyedia layanan cloud lainnya. Oleh karena itu, keamanan menjadi perhatian utama bagi penyedia layanan database cloud untuk menjaga kerahasiaan data. Artikel ini menyoroti kekhawatiran tentang keamanan dan upaya pencegahan dalam penyediaan layanan basis data di cloud.

Penyimpanan cloud adalah layanan inti dalam arsitektur computing cloud yang memfasilitasi pengguna untuk menyimpan dan berbagai data melalui internet. Beberapa keunggulan penyimpanan cloud termasuk pencadangan di luar lokasi, akses file yang aman dan efisien, ruang penyimpanan yang tidak terbatas, serta biaya penggunaan yang rendah. Namun, ketika data dan aplikasi bisnis dialihkan kepada pihak ketiga, kekhawatiran tentang keamanan dan privasi muncul.

Keamanan data secara konsisten menjadi fokus utama dalam teknologi informasi. Perlindungan data dan privasi menjadi dua perhatian utama pengguna terhadap teknologi cloud. Cloud merujuk pada infrastruktur perangkat keras dan perangkat lunak di pusat data yang menyediakan berbagai layanan melalui jaringan atau internet untuk memenuhi pengguna. Kemanan data menjadi isu yang serius dalam computing cloud karena data tersebar di berbagai perangkat penyimpnanan termasuk server, PC, dan reangkat seluler seperti jaringan sensor nirkabel dan ponsel cerdas. Untuk meningkatkan adopsi computing cloud oleh pengguna dan perusahaan, masalah keamanan pengguna harus diselesaikan terlebih dahulu sehingga lingkungan cloud dapat dipercaya. Perlindungan dan keamanan data menjadi faktor kunci dalam upaya mendapatkan kepercayaan pengguna dan keberhasilan penggunaan teknologi cloud. Tantangan keamanan dalam cloud mencakup ancaman, kehilangan data, gangguan layanan, dan serangan berbahaya dari pihak luar. Perlindungan data yang konsisten sangat penting untuk mencegah pelanggaran data dan kehilangan informasi sensitif. Itulah mengapa privasi data cloud harus menjadi prioritas utama bagi organisasi dalam era digital.

Akses data cloud oleh pihak ketiga seperti penyedia layanan cloud atau lembaga pemerintah dapat menimbulkan risiko keamanan, seperti akses tidak sah atau pelanggaran data. Untuk mengatasi risiko tersebut, berbagai Undang-Undang da peraturan, seperti GDPR, CCPA, dan HIPAA, telah diberlakukan untuk mengatur perlindungan data dan privasi pengguna.

B. Privasi Data

Masalah privasi data terus berkembang sebagai ancaman bagi layanan cloud computing dalam berbagai bentuk. Seiring dengan itu, para akademis telh fokus pada pengembangan teknik pelestarian privasi untuk mengatasi risiko tersebut. Awalnya, mereka menciptakan berbagai kerangka dan strategi tanpa mengidentifikasi jenis ancaman secara khusus. Beberapa studi survei kemudian difokuskan pada kategorisasi jenis ancaman privasi untuk penyimpanan cloud. Enkripsi, kontrol akses, dan audit menjadi atribut umum yang digunakan di berbagai kategoris. Selain itu, pemeriksaan integritas dan pencarian kata kunci digunakan untuk melindungi privasi penyimpanan cloud.

Protokol pemeriksaan integritas data jarak jauh meryupakan teknologi baru yang menyediakan alat verifikasi untuk memastikan privasi data saat diambil dari penyimpanan cloud. Penulis juga mengem bangkan metodologi rekontruksi metadata dinamis untuk menyortir metadata dalam database penyimpanan cloud. Penulis fokus pada teknik tradisional seperti enkripsi, krontrol akses, dan audit tanpa menyebutkan atribut baru dan canggih. Metode pelestarian dibagi menjadi empat kelompok: Peringkat, anonimasi. Probabilitas, dan kriptografi. Kriptografi dan enkripsi digunakan bersamaan dengan tindakan menjaga privasi lainnya, sementara probabilitas menciptakan metode yang menghasilkan hasil yang konsisten untuk mengatasi ancaman kebocoran data.

Anonimasi data melibatkan atau pengubahan data pengguna sehingga identitas pemilik data tidak terungkap, melindungi identifikasi peserta asli dan mengurangi kerentanan terhadap serangan pencurian identitas. Metode pemeringkatan menerapkan algoritma unik pada data untuk menjaga privasi data dan mencapai temuan yang paling tepat. Pemisahan data pengguna dan aktivitas cloud merupakan opsi baru, di mana saling percaya antara pihak penting untuk memastikan pekerjaan yang tepat waktu dan bebas kesalahan.

Disisi lain, pendekatan kepercayaan perangkat keras dan pembuatan sistem peraturan dan hukum juga dianggap penting dalam memerangi kemungkinan bahaya dalam sistem cloud computing.

C. Pencegahan Privasi Data

Langkah-langkah pencegahan dan perlindungan dapat diambil dalam berbagai aspek untuk mengatasi masalah tersebut, termasuk dalam aspek kemanan privasi data. Privasi memiliki signifikan yang besar dalam cloud computing karena preferensi privasi setiap individu berbeda. Dengan menjaga privasi data, setiap orang dapat mengontrol siapa yang memiliki akses atau mengubah informasi sesuai kebutuhan dan keinginannya. Dari perspektif penggunaan layanan cloud, beberapa faktor penting harus dipertimbangkan, seperti kontrol terhadap sistem dan data, kemampuan untuk menggunakan banyak identitas dan autentikasi untuk transaksi penting. Semua hal ini penting bagi individu agar privasi informasinya yang disampaikan kepada penyedia layanan cloud tetap aman.

Selain itu, bagi penyedia layanan cloud sendiri, beberapa aspek yang harus diperhatikan antara lain adalah menyediakan fasilitas untuk mengelola data pribadi pengguna, menerapkan enkripsi pada setiap data yang menyipan informasi pribadi pengguna, mengelola pengolahan dan penyimpanan data, mengendalikan pengidentifikasi unik, serta mengelola persyaratan privasi dan kemanan secara eksplisit antara penyedia layanan cloud dan pengguna.

D. Model Pelestarian Privasi Data di Cloud

Mengidentifikasi atribut penyimpanan data cloud yang mempertahankan privasi. Untuk menyusun kerangka kerja yang komprehensif dalam menjaga privasi data penyimpanan cloud,

semua atribut yang berkontruksi dalam menjaga privasi harus dipertimabangkan. Bagian ini mengidentifikasi atribut-atribut yang dapat mengurangi dampak pelanggaran privasi. Berbagai database, termasuk Science Direct, IEEE, Springer, Wiley, Googgle scoholar, dan MDPI digunakan untuk mengidentifikasi studi yang membahas pemeliharaan privasi dalam penyimpanan data cloud.

Artikel ini menggabungkan atribut privasi yang mencerminakan penemuan terbaru dari para pakar keamanan siber. Atribut-atribut ini di kelompokan dalam kategori dalam sebuah taksonomi, yaitu: manajemen desain, manajemen kunci, manajemen pengujian, manajemen ancaman, dan manajemen kinerja. Setiap kategori mencakup atribut-atribut tertentu yang penting untuk menjaga privasi data.

Dengan pertumbuhan layanan cloud conputing, memperbaiki kerentanan dan kesalahan sistem privasi telah menjadi upaya yang memakan waktu dan tidak menjamin kepastian. Perlindungan informasi pribadi merupakan bagian penting dari desain teknik pelestarian privasi, yang memungkinkan perancang sistem untuk mengatasi kekurangan yang dapat membahayakan operasi sistem. Namun tanpa keterlibatan desainer dalam teknologi baru yang dapat mengurangi dampak keseluruhan dari bahaya privasi teknik pelestarian privasi tetap rentan terhadap berbagai resiko.

Pencapaian privasi adalah aspek penting dalam mengevaluasi teknik pelestarian privasi yang mencerminkan keberhasilan atau konsekuensi dari fungsi-fungsi tertentu.berbagai tindakan privasi dapat menghasilkan pencapaian privasi yang beragam, seperti mencegah penipuan data oleh pihak yang tidak berwewenang atau mencegah otoritas pihak ketiga untuk mengungkapkan data tanpa izin.komponen kerangka kerja baru yang diusulkan mencakup peserta, pendaftaran, pemrosesan data, teknik kriptografi, audit, fungsi pengontrol data kemasan eksternal, penggabungan, dan segmentasi data, serta penyimpanan multi-cloud.

Pelestarian privasi yang memungkinkan pembuatan lingkungan database cloud pribadi dengan opsi pelestarian privasi yang realistis. Skema enkripsi tiga kali lipat diusulkan untuk meningktakan privasi dan efisiensi teknik secara keseluruhan, dengan tujuan menciptakan database cloud pribadi yang dapat menjalankan perintah pada data terenkripsi tanpa memberikan tekanan tambahan pada penyedia layanan cloud atau pengguna. Hasil eksperimen menunjukkan pengurangan signifikan dalam biaya komputasi untuk operasi enkripsi/deskripsi sambil menjaga privasi data yang dialihdayakan.

Model konseptual untuk pelestarian privasi penyimpanan cloud melibatkan sejumlah teknik dan pendekatan untuk memastikan kerahasiaan dan keamanan data yang di simpan di cloud. Beberapa contoh yang menggambarkan kerangka kerja ini:

1. Enkripsi Data: Penyedia penyimpanan cloud menggunakan algoritma enkripsi untuk melindungi data saat disimpan dan dalam perjalanan, sehingga mencegah akses yang tidak sah
2. Audit yang menjaga privasi: Teknik bukti tanpa pengetahuan memungkinkan pengguna memverifikasi integritas data tanpa mengungkap kontennya, sehingga memastikan privasi
3. Protokol transfer data yang aman: Memnfaatkan protocol aman seperti SSL/TLS selama transfer data menjamin enkripsi dan integritas data
4. Kebijakan privasi dan transparansi: Penyedia penyimpanan cloud harus menjaga kebijakan privasi yang transparan dan mengungkapkan praktik penanganan data untuk membangun kepercayaan pengguna
5. Manajemen kunci yang aman: Menerapkan praktik yang kuat untuk menjaga kunci enkripsi dan mencegah akses tidak sah ke data
6. Otentifikasi aman dan manajemen identitas: Menerapkan mekanisme otentikasi yang kuat dan manajemen identitas yang tepat untuk mencegah akses tidak sah
7. Deteksi anomali: Mengidentifikasi aktivitas tidak biasa atau pola akses yang mencurigakan yang mungkin mengindikasikan pelanggaran privasi

8. Audit keamanan rutin: Melakukan audit kemanan berkala untuk mengidentifikasi kerentanan dan memastikan peningkatan berkelanjutan atas tindakan pelestarian privasi dalam sistem penyimpanan cloud

Contoh-contoh ini mencakup beberapa elemen dan teknik dasar dalam kerangka konseptual untuk menjaga privasi penyimpanan cloud, yang bertujuan untuk melindungi data pengguna dan menjaga kerahasiaan di lingkungan penyimpanan cloud.

Dan kriptografi adalah teknik yang krusial dan banyak digunakan dalam konteks keamanan. Dengan menggunakan kunci dan algoritma enkripsi, teks biasa diubah menjadi teks tersandi. Ini adalah salah satu teknik keamanan yang paling aman, dan sering digunakan dalam penyimpanan data melalui cloud. Teknik kriptografi yang saat ini tersedia lebih realistis dan mampu mencapai berbagai tujuan, termasuk menjaga kerahasiaan dan integritas data.

KESIMPULAN

Kesimpulan ditulis secara singkat yaitu mampu menjawab tujuan atau permasalahan penelitian dengan menunjukkan hasil penelitian, bahwa pelestarian privasi data di database cloud sangat penting dalam menghadapi tantangan keamanan dan privasi yang terus berkembang di era digital. Berbagai teknik seperti enkripsi data, kontrol akses, audit, dan manajemen kunci digunakan untuk menjaga kerahasiaan data dan integritas data. Selain itu, pentingnya kebijakan privasi, transparansi, otentifikasi yang aman, deteksi anomali juga ditekankan sebagai langkah-langkah penting dalam memastikan privasi data dalam lingkungan penyimanan cloud. Dengan melakukan pendekatan ini, diharapkan bahwa penyedia layanan cloud dan pengguna dapat bekerja sama untuk menciptakan lingkungan cloud yang aman dan dapat dipercaya semua pihak yang terlibat.

DAFTAR PUSTAKA

Sun, Y,. Zhang, J., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing.

Taofik I., Irawan, A. (2023). Analisis Keamanan dan Perlindungan Data pada Komputasi Awan dalam Ruang Lingkup Pendidikan.

Wang, H. (2010). Privacy-Preservering Data Sharing in Cloud Computing. Journal of Computer Science and Technology, 25(3), 401-414.

Revathi, T, S., A, Gayathri., J, Kalaivani, Mary, S, C., Danilo, P., & M, A. (2021).Cloud-Assisted Privacy-Preserving Method for Healthcare Using Adaptive Fractional Brain Storm Integrated Whale Optimization Algorithm. Hindawi: Security and Communication Network.

Azzaoui, A, E., Chen, H., Kim, S, H., Pan, Y., & Park, J, H. (2022). Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preservering in Medical Supply Chain Systems. Sensors, 2022,22, 1371.

Abdul, R., & Rizvi, S, S. (2017). Privacy Preservering Model: A New Scheme for Auditing Cloud Stakeholders. Journal of Cloud Computing: Advances, Ssytems and Applications.

Riyadi, F, S., Syefudin., Gunawan., & Murtopo, A, A. (2023). Analisis Keamanan dan Privasi Data Pada Layanan Cloud Computing dengan Menggunakan Teknik Kriptografi. JTech, 11(2), 93-100.

Singh, N., & Singh, K, A. (2017). Data Privacy Protection Mechanisms in the Cloud.

Marliana, M. (2020). Keamanan dan Pencegahan Database Cloud Computing untuk Pengguna Layanan. Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi.

Tantowi, L., Wijayanti, L. (2023). Peluang dan Tantangan Penyimpanan Cloud Storage Pada Dokumen Digital. Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip dan Dokumentasi, 15 (1).