INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 228-236, ISSN: 3123-5573 (Online)

Analisis Risiko Keamanan Data pada Penyimpanan *Cloud Computing*

Reva Agustin[1], Rezky Awaliah Putri Achmadi[2], Rakhmadi Rahman[3]
[1,2,3]Sistem Informasi, Elektro Dan Komputer, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia
revaagustin.241031076@mahasiswa.ith.ac.id[1], rezkyawaliahputriachmadi.241031081@mahasiswa.ith.ac.id[2], rakhmadi.rahman@ith.ac.id[3]

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:

Cloud Computing, Data Security, Risk, Mitigation, Encryption, Access Control.

ABSTRACT

Cloud-based data storage has become a primary solution for data management across various industries. While cloud computing offers convenient data access and management, it also carries various risks related to data security. This study utilizes theoretical analysis methods to review relevant literature on cloud computing data security threats. The purpose of this study is to analyze threats to cloud computing data storage and provide recommendations for measures that can be implemented to minimize these threats. Data leaks, DDoS attacks, and data loss are the primary threats, according to the study findings. The use of data encryption, multi-factor authentication, and strict access control are some of the recommended mitigation strategies.

This is an open access article under the CC BY-SA license.

Article Info

Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
Cloud Computing, Keamanan Data, Risiko, Mitigasi, Enkripsi, Kontrol Akses.

ABSTRAK

Penyimpanan data berbasis cloud telah menjadi solusi utama untuk pengelolaan data di berbagai industri. Meskipun cloud computing menawarkan kemudahan akses dan pengelolaan data, itu juga membawa berbagai risiko yang terkait dengan keamanan data. Penelitian ini memanfaatkan metode analisis teori untuk meninjau berbagai literatur yang relevan mengenai ancaman keamanan data cloud computing. Tujuan dari penelitian ini adalah untuk menganalisis ancaman yang terjadi pada penyimpanan data di cloud computing serta memberikan rekomendasi untuk langkah-langkah yang dapat diterapkan untuk meminimalkan ancaman tersebut. Kebocoran data, serangan DDoS, dan kehilangan data adalah ancaman utama, menurut temuan penelitian. Penggunaan enkripsi data, otentikasi multi-faktor, dan kontrol akses yang ketat adalah beberapa strategi mitigasi yang disarankan.

This is an open access article under the CC BY-SA license.

Corresponding Author:
Reva Agustin
Institut Teknologi Bacharuddin Jusuf Habibie
Email: revaagustin.241031076@mahasiswa.ith.ac.id

Pendahuluan

Penyimpanan data berbasis cloud telah menjadi pilihan utama untuk berbagai organisasi dan individu dalam mengelola data karena kemudahan akses, efisiensi biaya, dan kapasitas penyimpanan yang tidak terbatas. Di sisi lain, cloud computing memungkinkan pengguna mengakses data dari berbagai perangkat, yang meningkatkan fleksibilitas dan mobilitas. Namun, penggunaan cloud computing membawa tantangan signifikan dalam hal keamanan data. Ini karena pengguna tidak lagi memiliki kendali penuh atas data yang disimpan.

Ancaman dari sumber luar seperti peretasan dan ancaman internal seperti kesalahan konfigurasi atau pengelolaan akses yang buruk sangat mungkin terjadi di server yang dikelola oleh penyedia layanan cloud. Penyimpanan data yang tidak dilindungi dapat menyebabkan kerugian keuangan, kerusakan reputasi, dan pelanggaran undang-undang yang dapat mengakibatkan denda atau hukuman. Oleh karena itu, penting untuk melakukan analisis menyeluruh tentang potensi bahaya yang terkait dengan penyimpanan data cloud, serta solusi mitigasi yang dapat diterapkan untuk mengatasi bahaya tersebut.

Rumusan Masalah penelitian ini adalah 1) Apa saja potensi bahaya yang terkait dengan penyimpanan data berbasis cloud computing? 2) Bagaimana integritas, kerahasiaan, dan aksesibilitas data yang disimpan dipengaruhi oleh ancaman tersebut? dan 3) Apa yang dapat dilakukan untuk mengurangi risiko dan meningkatkan keamanan data penyimpanan cloud? Tujuan dari penelitian ini adalah untuk meningkatkan pemahaman kita tentang ancaman keamanan yang terkait dengan penyimpanan data berbasis cloud computing serta mengusulkan strategi mitigasi yang berguna untuk mengurangi kerugian yang mungkin disebabkan oleh ancaman tersebut. Tujuan khusus dari penelitian ini adalah:

1. Mengidentifikasi jenis ancaman yang ada pada penyimpanan data berbasis cloud computing.
2. Mengevaluasi dampak dari risiko-risiko tersebut terhadapdata dan organisasi.
3. Untuk mengurangi risiko keamanan dan mempertahankan keandalan sistem cloud computing, berikan rekomendasi untuk langkah-langkah mitigasi yang berguna.

Batasan Masalah

Penelitian ini tidak akan mencakup aspek lain seperti pengelolaan aplikasi atau komputasi di cloud, tetapi akan berkonsentrasi pada analisis risiko keamanan data yang terkait dengan penyimpanan cloud computing. Studi ini juga tidak akan melakukan pengujian sistem atau eksperimen langsung, tetapi akan berfokus pada analisis teori yang didasarkan pada penelitian literatur yang relevan.

1. Tinjauan Pustaka

Cloud Computing memungkinkan pengguna mengakses sumber daya komputasi seperti penyimpanan data, aplikasi, dan pemrosesan informasi tanpa perlu mengelola infrastruktur fisik mereka sendiri. Dalam model ini, data disimpan di server yang dikelola oleh penyedia layanan cloud, yang memberikan skalabilitas dan fleksibilitas kepada pengguna. Tiga kategori utama layanan cloud computing adalah Infrastructure as a Service (IaaS), yang menyediakan infrastruktur dasar seperti server dan penyimpanan; Platform as a Service (PaaS), yang memberikan platform untuk pengembangan aplikasi tanpa memerlukan pengelolaan infrastruktur; dan Software as a Service (SaaS), yang memberikan aplikasi yang dapat diakses secara langsung melalui internet, seperti email atau aplikasi perkantoran.

Keamanan data cloud computing sangat penting karena data yang disimpan di cloud berada di luar kendali fisik pengguna dan dikelola oleh penyedia layanan cloud. Beberapa ancaman yang sering dikaitkan dengan penggunaan cloud computing adalah kebocoran data, serangan Denial of Service (DDoS), akses tidak sah, dan kehilangan data. Kebocoran data dapat terjadi jika sistem yang digunakan tidak dilindungi dengan baik atau jika terjadi kes Ketika orang yang tidak berwenang mendapatkan akses ke data sensitif, ini disebut akses tidak sah. Di sisi lain, kehilangan data dapat terjadi karena bencana alam atau kegagalan sistem yang merusak infrastruktur penyimpanan cloud.

Enkripsi data, autentikasi multi-faktor, dan kontrol akses yang ketat adalah beberapa metode keamanan yang telah dikembangkan untuk mencegah ancaman ini. Dengan mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi, enkripsi menjaga kerahasiaannya meskipun data jatuh ke tangan yang salah. Sementara itu, autentikasi multi-faktor meningkatkan keamanan dengan memerlukan dua atau lebih bukti identifikasi untuk mengakses data, sementara kontrol akses membatasi siapa yang dapat mengakses data hanya dengan izin yang telah ditentukan. Dalam hal ini, ISO/IEC 27001 dan NIST Cybersecurity Framework menjadi pedoman penting untuk manajemen dan pengurangan risiko keamanan cloud computing.

2. Metodologi Penelitian

Untuk mengeksplorasi dan menganalisis berbagai jenis risiko yang terkait dengan keamanan data dalam penyimpanan cloud computing, penelitian ini menggunakan pendekatan kualitatif dengan fokus utama pada analisis literatur. Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk menggunakan sumber teori yang sudah ada untuk menggali lebih dalam masalah yang ada daripada melakukan uji coba sistem secara langsung. Penulis tidak menggunakan eksperimen atau pengujian sistem dalam penelitian ini; sebaliknya, mereka menggunakan penelitian literatur yang relevan.

Sumber data yang digunakan dalam penelitian ini berasal dari berbagai jenis literatur, termasuk artikel jurnal ilmiah, buku, dan laporan penelitian terbaru tentang cloud computing dan keamanan data. Sumber-sumber literatur yang dipilih memiliki relevansi yang signifikan dengan topik penelitian dan telah melalui proses peer review untuk memastikan bahwa informasi yang dikumpulkan benar dan berkualitas. Hanya literatur yang diterbitkan dalam kurun waktu sepuluh tahun terakhir digunakan, kecuali literatur tersebut dianggap sangat penting dan penting dalam bidang ini, untuk memastikan bahwa informasi yang terkandung dalam literatur tetap relevan.

Penulis mencari literatur tentang bahaya yang dihadapi dalam penyimpanan data di cloud computing, dampak dari bahaya tersebut, dan solusi mitigasi yang dapat digunakan untuk meminimalkan bahaya tersebut selama pengumpulan data. Penelitian ini juga mengidentifikasi teknologi keamanan cloud computing yang melindungi data pengguna, seperti enkripsi data, autentikasi multi-faktor (MFA), dan pengelolaan kontrol akses yang baik.

Setelah pengumpulan literatur selesai, penulis menganalisis informasi tematik. Metode ini digunakan untuk mengelompokkan data berdasarkan tema-tema utama yang muncul dalam literatur yang ada, seperti jenis-jenis risiko yang dihadapi oleh pengguna cloud computing, dampaknya terhadap keamanan data, dan langkah-langkah mitigasi yang dapat diterapkan untuk mengurangi risiko-risiko tersebut. Dalam hal ini, penulis fokus pada membandingkan berbagai strategi mitigasi yang telah diterapkan di dunia industri, dan mengevaluasi seberapa efektif masing-masing solusi tersebut.

Analisis data dilakukan dengan mengidentifikasi pola- pola yang ada dalam berbagai penelitian yang telah diterbitkan sebelumnya. Penulis juga membandingkan hasil dari penelitian yang berbeda untuk menilai konsistensi dan keberhasilan langkah mitigasi yang diterapkan oleh berbagai penyedia layanan cloud dan pengguna data. Penelitian ini juga membahas kebijakan- kebijakan yang diterapkan oleh penyedia layanan cloud untuk menjaga keamanan cloud.

Secara keseluruhan, penelitian ini tidak hanya memeriksa berbagai jenis risiko yang ada, tetapi juga bagaimana setiap risiko berdampak pada organisasi dan pengguna data, serta solusi mitigasi yang dapat digunakan untuk mengurangi dampak risiko tersebut. Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang cara mengelola risiko keamanan data di cloud computing dan menemukan solusi yang dapat meningkatkan keamanan data.

3. Analisis Risiko Keamanan Data Pada Cloud Computing

Banyak organisasi, individu, dan bisnis memilih penyimpanan data berbasis cloud computing karena popularitasnya yang meningkat. Cloud computing telah mengubah cara kita mengelola data karena skalabilitas, fleksibilitas, dan penghematan biaya yang ditawarkannya. Namun, seiring dengan adopsi yang cepat, muncul berbagai risiko yang terkait dengan keamanan data, yang harus dikelola dengan hati-hati untuk menghindari dampak negatif. Ancaman ini berasal dari ancaman internal dan eksternal yang mungkin tidak selalu terlihat. Untuk itu, untuk meningkatkan keamanan data yang disimpan di cloud, sangat penting untuk melakukan analisis menyeluruh tentang jenis risiko yang ada, efeknya, dan variabel yang mempengaruhi kerentanannya.

1) Jenis Risiko

Beberapa bahaya yang paling signifikan dari cloud computing adalah sebagai berikut:

a) Kebocoran Data
Salah satu ancaman terbesar bagi cloud computing adalah kebocoran data. Karena kerentanan dalam pengelolaan akses atau kesalahan konfigurasi, orang yang tidak berwenang dapat mengakses data di cloud. Misalnya, orang yang tidak berwenang dapat mengakses data sensitif seperti data pelanggan atau data keuangan jika hak akses tidak digunakan dengan benar. Serangan peretasan atau malware juga dapat mengakses dan mencuri data yang ada di cloud, baik saat disimpan maupun saat dikirim. Data bocor dapat menyebabkan kerugian moneter, reputasi yang buruk, dan konsekuensi hukum, terutama jika data tersebut mengandung informasi pribadi yang dilindungi oleh undang-undang seperti GDPR atau CCPA.

b) Serangan DDoS (Distributed Denial of Service)
Serangan DDoS tidak mencuri data, tetapi mengganggu ketersediaan layanan cloud dengan membanjiri server dengan lalu lintas yang sangat besar. Namun, meskipun serangan ini tidak mencuri informasi, dampaknya terhadap ketersediaan layanan dapat sangat merusak. Bisnis yang bergantung pada cloud untuk penyimpanan dan akses data mungkin menghadapi downtime yang lama, yang mengganggu operasional dan produktivitas. Serangan DDoS, terutama jika pengguna atau klien tidak dapat mengakses data penting, dapat menyebabkan kerugian besar.

c) Kehilangan Data
Meskipun banyak penyedia layanan cloud menawarkan solusi backup otomatis, kesalahan dalam

pengelolaan backup atau kesalahan konfigurasi dapat menyebabkan data hilang tanpa bisa dipulihkan, serta kesalahan manusia, kerusakan perangkat keras, atau bencana alam. Selain itu, kegagalan pemulihan data setelah kerusakan sistem atau kegagalan infrastruktur cloud dapat menyebabkan hilangnya data.

d) Akses Tidak Sah
Akses tidak sah dapat terjadi jika hak akses pengguna atau aplikasi tidak dikelola dengan ketat. Ini berlaku bahkan jika pengguna memiliki hak akses tertentu. Dalam kasus lain, kebocoran kredensial atau pengelolaan akses yang tidak terkontrol dapat memungkinkan peretas atau orang tidak sah lainnya mendapatkan akses ke data sensitif. Terutama bagi organisasi yang menyimpan data pribadi, keuangan, atau medis, serangan data ini dapat merusak integritas data dan menyebabkan kerugian besar.

e) Serangan Siber (Ancaman Internal)
Serangan insider—ancaman dari dalam organisasi—sering diabaikan. Ini mencakup orang-orang yang memiliki akses legal ke sistem dan data, seperti kontraktor, mantan kontraktor, atau karyawan saat ini. Meskipun mereka memiliki hak untuk mengakses data, mereka dapat menyalahgunakannya untuk tujuan yang merugikan, seperti mencuri, mengubah, atau bahkan menghapus data sensitif. Karena pelaku memiliki izin akses yang sah, mereka dapat dengan mudah menutupi jejak mereka, serangan insider seringkali lebih sulit dideteksi. Untuk meminimalkan risiko ini, gunakan kontrol akses berbasis peran yang ketat dan audit aktivitas pengguna yang memiliki akses ke data sensitif.

2) Dampak Dari Risiko Keamanan Data
Dampak dari risiko keamanan data dalam cloud computing bisa sangat besar, baik dari segi finansial, operasional, maupun reputasi. Dampak utama yang mungkin terjadi antara lain:

a) Kerugian Finansial
Uptime atau kebocoran data dapat menyebabkan kerugian besar. Jika terjadi kebocoran data pribadi pelanggan, seperti data kartu kredit, informasi medis, atau data pribadi lainnya, organisasi dapat dikenakan denda yang besar, terutama jika mereka melanggar peraturan perlindungan data seperti GDPR atau CCPA. Selain itu, kerugian finansial dapat meningkat karena biaya pemulihan data, downtime, dan ganti rugi yang harus dibayar kepada pihak yang dirugikan. Perusahaan harus menyediakan uang untuk memperbaiki reputasi dan menerapkan sistem keamanan yang lebih ketat, bahkan setelah peristiwa keamanan terjadi.

b) Kerusakan Reputasi
Kepercayaan pelanggan terhadap penyedia layanan cloud sangat penting. Reputasi penyedia layanan cloud dapat rusak dengan cepat jika terjadi kebocoran data atau serangan terhadap data pengguna. Pelanggan yang kehilangan data atau merasa tidak aman saat menggunakan layanan cloud lebih cenderung berpindah ke penyedia yang lebih aman daripada memperbaiki kerugian finansial. Bisnis yang terlibat dalam insiden keamanan akan kehilangan kepercayaan pelanggan dalam jangka panjang, bahkan setelah masalah teknis diselesaikan.

c) Pelanggaran Regulasi dan Hukum
Jika data sensitif bocor atau hilang, organisasi dapat dikenakan hukuman berat. Adat istiadat data, seperti GDPR di Eropa atau CCPA di California, menetapkan peraturan ketat tentang bagaimana perusahaan mengelola dan melindungi data pribadi. Organisasi dapat dikenai denda besar dan tindakan hukum jika data pribadi bocor atau hilang tanpa perlindungan yang cukup. Ini menunjukkan bahwa melanggar kebijakan perlindungan data membawa kerugian finansial yang signifikan selain mengancam keamanan.

d) Gangguan Operasional
Serangan DDoS atau kehilangan data sering menyebabkan gangguan operasional, yang mengganggu operasi bisnis. Dalam kasus ini, serangan DDoS dapat menyebabkan downtime yang lama pada layanan cloud, yang mengganggu operasi bisnis. Ketika data tidak dapat diakses atau dihapus tanpa upaya pemulihan, ini menyebabkan penurunan produktivitas, kerugian waktu, dan penurunan kinerja operasional secara keseluruhan. Beberapa sektor, seperti sektor keuangan dan kesehatan, sangat bergantung pada layanan data real-time, sehingga gangguan ini dapat berakibat fatal.

3) Faktor-faktor yang Mempengaruhi Kerentanannya
Banyak hal, seperti teknologi, manajemen, dan kebijakan, dapat mempengaruhi kerentanannya terhadap risiko tersebut. Beberapa faktor yang meningkatkan kerentanannya antara lain:
a) Pengelolaan Akses Yang Buruk Pengelolaan hak akses yang buruk merupakan faktor utama penyebab

kebocoran atau akses tidak sah. Pengguna seringkali diberi akses lebih banyak daripada yang mereka butuhkan untuk menyelesaikan tugas, yang memungkinkan pihak yang tidak berwenang mengakses data. Selain itu, masalah ini diperburuk dengan penggunaan kata sandi yang tidak kuat atau kredensial yang bocor.

b) Kesalahan Konfigurasi Sistem Konfigurasi sistem cloud yang salah dapat membuat data tidak aman. Misalnya, jika penyedia layanan cloud atau pengguna gagal mengatur pengaturan enkripsi atau kontrol akses dengan benar, data yang disimpan di cloud sangat rentan terhadap serangan atau kebocoran.

c) Kebijakan Keamanan Yang Lemah Kebijakan keamanan yang tidak jelas atau tidak ditegakkan dengan baik dapat menyebabkan masalah serius. Organisasi lebih mudah mengalami insiden yang merusak integritas dan kerahasiaan data jika tidak memiliki kebijakan dan prosedur yang ketat untuk audit keamanan, pengelolaan data, dan pemulihan data.

d) Kurangnya Pelatihan dan Kesadaran Keamanan
Tanpa pelatihan yang memadai, karyawan atau pengguna cloud dapat melakukan kesalahan yang meningkatkan kelentanannya terhadap ancaman. Ini termasuk tidak mematuhi kebijakan keamanan, menggunakan kata sandi yang buruk, atau tidak menyadari potensi serangan sosial seperti phishing, yang dapat digunakan oleh peretas untuk mendapatkan akses tidak sah.

2. Mitigasi Risiko Dan Solusi Keamanan

Mengatasi berbagai ancaman keamanan cloud computing membutuhkan pendekatan yang menyeluruh dan strategi mitigasi yang efektif. Sangat penting bagi organisasi untuk menerapkan langkah-langkah keamanan yang kuat untuk mencegah ancaman terhadap data yang disimpan di cloud. Bagian ini akan membahas berbagai metode mitigasi yang dapat digunakan untuk melindungi data dari ancaman saat ini, serta solusi keamanan yang perlu dipertimbangkan untuk memastikan data tetap aman, rahasia, dan tersedia.

a) Enkripsi Data

Gambar 1. Enkripsi Data

Proses enkripsi data mengubah data yang dapat dibaca oleh manusia menjadi format yang tidak dapat dipahami tanpa kunci dekripsi. Ini adalah langkah pertama yang sangat penting dalam melindungi data sensitif. Data at rest, yang merupakan data yang disimpan di cloud, dan data in transit, yang merupakan data yang dikirimkan ke dan dari server cloud, harus dienkripsi dalam dua tahap dalam konteks komputasi cloud. Enkripsi Data at Rest: Enkripsi data at rest melindungi data yang disimpan di server cloud dengan mengubahnya menjadi bentuk terenkripsi. Orang yang dapat mengakses data yang sudah terenkripsi tidak dapat melakukannya, meskipun mereka memiliki kunci dekripsi yang tepat. Ini penting karena cloud computing sering melibatkan penyimpanan data besar. Melindungi data ini dari akses yang tidak sah sangat penting.

Enkripsi Data in Transit: Protokol enkripsi yang kuat seperti SSL/TLS juga harus digunakan untuk melindungi data yang dikirim dari perangkat pengguna ke cloud. Ini memastikan bahwa data yang dikirim melalui jaringan aman dari ancaman seperti serangan Man-in-the-Middle (MITM), di mana pihak ketiga mencoba menghentikan komunikasi dan mendapatkan akses ke data yang sedang dipindahkan. Selain itu, enkripsi membantu organisasi memenuhi peraturan perlindungan data pribadi seperti GDPR, yang mengharuskan organisasi mengambil langkah- langkah yang cukup untuk melindungi data sensitif.

b) Autentikasi Multi-Factor (MFA)

Gambar 2. MFA

Autentikasi multi-faktor (MFA) adalah metode terbaik untuk mencegah akses tidak sah ke data karena mengharuskan pengguna memberikan lebih dari satu bukti identitas saat mencoba mengakses data atau layanan tertentu. MFA biasanya mencakup dua atau lebih faktor berikut:

informasi yang diketahui, seperti PIN atau kata sandi
item yang dimiliki: contohnya, perangkat otentikasi
informasi biometrik seperti sidik jari atau pengenalan wajah

Melakukan autentikasi multifaktor (MFA) secara wajib pada setiap titik akses ke data sensitif akan meningkatkan tingkat keamanan dan mencegah banyak jenis serangan yang umum terjadi, seperti phishing dan brute force, karena mengurangi risiko akses yang tidak sah meskipun kredensial utama (seperti kata sandi) bocor atau dicuri.

c) Kontrol Akses yang Ketat

Gambar 3. Kontrol Akses

Pengendalian hak akses yang buruk merupakan penyebab utama kebocoran data dan akses tidak sah di cloud computing. Pengaturan kontrol akses yang ketat sangat penting untuk memastikan bahwa hanya orang yang berwenang yang dapat mengakses informasi sensitif. Untuk menjalankan kontrol akses dengan lebih efisien, beberapa tindakan harus dilakukan:

1) Prinsip Least Privilege digunakan, yang berarti bahwa pengguna hanya memiliki akses ke data yang mereka butuhkan untuk menyelesaikan tugas mereka. Ini mengurangi kemungkinan pengguna menyalahgunakan akses.
2) Kontrol Akses Berbasis Peran (RBAC): RBAC memungkinkan penyedia layanan cloud membatasi akses data berdasarkan peran atau jabatan pengguna. Misalnya, hanya staf IT yang memiliki akses penuh ke data server, sedangkan staf non-IT hanya memiliki akses terbatas pada data yang berkaitan dengan pekerjaan mereka.
3) Audit dan Pemantauan Akses: Melakukan audit rutin terhadap hak akses yang ada memungkinkan organisasi untuk mendeteksi dan menangani potensi ancaman lebih cepat.

Kontrol akses yang ketat akan melindungi data dari serangan internal atau akses yang tidak sah dari luar.

d) Pengelolaan Keamanan Jaringan dan Sistem

Gambar 4. Keamanan Jaringan

Keamanan jaringan dan pengelolaan sistem cloud adalah langkah-langkah mitigasi keamanan penting selain pengelolaan data dan hak akses. Untuk mencegah akses yang tidak sah ke jaringan cloud mereka, setiap penyedia layanan cloud harus menerapkan firewall yang kuat. Anda dapat mengkonfigurasi firewall ini untuk mencegah trafik yang tidak dikenal atau berpotensi berbahaya.

1) Segregasi Jaringan: Agar data yang lebih sensitif dilindungi dengan lebih baik, penyedia layanan cloud harus mengisolasi berbagai jaringan. Selain itu, segmentasi jaringan membantu mengurangi dampak serangan DDoS dengan memastikan bahwa serangan terhadap satu segmen tidak mempengaruhi seluruh sistem.
2) Pemantauan Real-Time: Sistem pemantauan ancaman secara real-time sangat penting agar mereka dapat mendeteksi dan merespons ancaman baru dengan cepat. Penyedia layanan cloud harus memiliki alat pengawasan yang dapat mengidentifikasi tindakan yang mencurigakan, seperti percobaan login yang gagal atau pengiriman data yang tidak sah. Sistem cloud menjadi lebih tahan terhadap serangan dengan memantau dan melakukan pembaruan secara teratur. Dengan demikian, mereka dapat bertindak cepat jika terjadi sesuatu.

e) Penggunaan Teknologi Backup dan Pemulihan Data

Gambar 5. Backup Recovery

Keamanan data bukan hanya mencegah serangan atau kebocoran data, tetapi juga strategi pemulihan jika terjadi kerusakan. Salah satu cara terbaik untuk mengurangi risiko kehilangan data adalah dengan melakukan backup secara teratur. Backup Otomatis: Banyak penyedia layanan cloud menawarkan solusi backup otomatis yang memastikan bahwa data penting selalu tercadangkan dalam beberapa salinan di tempat yang berbeda. Backup ini harus dilakukan secara berkala dan disimpan dalam format terenkripsi untuk menjaga kerahasiaan. Pemulihan Bencana (Disaster Recovery): Penyedia layanan cloud juga harus memiliki rencana pemulihan bencana. Rencana pemulihan bencana harus mencakup pendekatan untuk pemulihan data dalam waktu yang singkat untuk menghindari penundaan yang lama. Ini akan memastikan bahwa data dapat dipulihkan dengan cepat dalam kasus data hilang atau rusak. Pemulihan yang cepat dan efektif setelah insiden dapat mengurangi kerugian finansial yang disebabkan oleh downtime dan kehilangan data.

f) Implementasi Kebijakan Keamanan yang Jelas

Gambar 6. Kebijakan Keamanan

Sangat penting bagi penyedia layanan cloud dan pengguna untuk menetapkan kebijakan keamanan untuk mengatur perlindungan data. Penyedia layanan cloud harus memiliki prosedur yang jelas tentang bagaimana mereka melindungi data pengguna, dan pengguna juga harus mengikuti kebijakan yang sama untuk mengelola data mereka sendiri.

Beberapa peraturan penting yang harus diikuti adalah:
1) Prosedur pengelolaan data: Menciptakan peraturan yang mengatur penyimpanan, perlindungan, dan akses data pengguna.
2) Penyusunan kebijakan pemulihan data: Peraturan yang mengatur bagaimana data akan dipulihkan jika hilang atau rusak.
3) Pendidikan dan pelatihan keamanan: mengajarkan pengguna cloud tentang cara melindungi data mereka dan mengatasi pelanggaran.

Kesimpulan

Dalam penelitian ini, berbagai ancaman keamanan data yang terkait dengan penyimpanan berbasis cloud computing telah dibahas, serta strategi mitigasi yang dapat diterapkan untuk mengurangi dampak dari ancaman tersebut. Meskipun cloud computing menawarkan banyak keuntungan dalam hal efisiensi biaya, skalabilitas, dan kemudahan akses, ada sejumlah ancaman yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan data yang disimpan di cloud. Beberapa ancaman utama yang dihadapi oleh pengguna dan penyedia layanan cloud adalah kebocoran data, serangan DDoS, kehilangan data, dan akses yang tidak sah. Kebocoran data, yang biasanya disebabkan oleh kesalahan konfigurasi atau ketahanan terhadap serangan peretas, dapat menyebabkan kerugian finansial, reputasi, dan kepatuhan hukum yang signifikan. Selain itu, serangan DDoS yang bertujuan untuk mengurangi ketersediaan layanan cloud dapat menyebabkan downtime yang lama, mengganggu operasi bisnis yang bergantung pada ketersediaan data secara real-time. Kehilangan data karena kerusakan sistem atau bencana alam yang merusak infrastruktur penyimpanan cloud juga merupakan risiko yang signifikan karena data yang disimpan di cloud sangat penting untuk kelangsungan operasional suatu organisasi. Akses tidak sah, baik yang disebabkan oleh kebocoran kredensial atau kesalahan dalam pengelolaan hak akses, dapat merusak integritas data dan menyebabkan kerugian yang signifikan.

Penelitian ini merekomendasikan beberapa metode mitigasi yang terbukti berhasil untuk mengurangi efek dari risiko-risiko tersebut. Salah satunya adalah enkripsi data, yang sangat penting untuk melindungi data yang disimpan dan dikirim melalui jaringan dari orang yang tidak berhak. Ini memastikan bahwa data sensitif tetap aman meskipun kebocoran data terjadi. Untuk meningkatkan keamanan akses, autentikasi multi-faktor (MFA) memastikan bahwa hanya pengguna yang sah yang dapat mengakses data sensitif, menambah lapisan keamanan tambahan yang mengurangi kemungkinan akses tidak sah, yang sering menjadi celah dalam sistem keamanan. Selain itu, kontrol akses yang ketat harus diterapkan untuk membatasi siapa yang dapat mengakses data dan apa yang dapat mereka lakukan dengannya. Kebijakan penting untuk mencegah orang yang tidak berwenang menyalahgunakan akses mereka, atau bahkan orang dalam yang memiliki akses sah tetapi menyalahgunakan kewenangannya. Pengelolaan hak akses berbasis peran (RBAC) dapat digunakan untuk memastikan bahwa setiap pengguna atau aplikasi hanya dapat mengakses data yang relevan dengan peran atau tanggung jawabnya.

Meskipun langkah-langkah mitigasi ini menurunkan risiko, tidak ada sistem yang dapat menghilangkan semua ancaman yang mungkin. Oleh karena itu, perusahaan dan penyedia layanan cloud harus terus melakukan pemantauan keamanan secara real-time untuk mendeteksi dan merespons potensi ancaman lebih awal. Ini dapat mencakup penggunaan sistem deteksi ancaman dan pengelolaan log untuk menemukan aktivitas yang mencurigakan dan segera melaporkannya kepada pihak yang berwenang. Selain itu, penyedia layanan cloud harus mematuhi standar keamanan internasional seperti ISO/IEC 27001 dan NIST Cybersecurity Framework, yang memberikan pedoman lengkap untuk pengelolaan keamanan data. Audit keamanan dan pembaruan sistem yang berkala sangat penting untuk memastikan bahwa sistem cloud aman dari ancaman baru.

Salah satu elemen yang juga harus dipertimbangkan adalah rencana pemulihan data dan bencana. Ini karena bencana alam, kegagalan perangkat keras, atau serangan dapat menyebabkan kehilangan data atau mengganggu operasional cloud. Penyedia layanan cloud harus memiliki rencana pemulihan data yang kuat untuk memulihkan data yang hilang atau rusak secepat mungkin. Kesimpulannya, meskipun cloud computing menawarkan banyak keuntungan dalam pengelolaan dan penyimpanan data, penting bagi organisasi dan penyedia layanan cloud untuk memahami ancaman yang ada dan menerapkan langkah mitigasi yang tepat untuk melindungi data yang disimpan di cloud. Dengan menerapkan enkripsi, autentikasi multi-faktor, kontrol akses yang ketat, dan pemantauan dan pemulihan sistem yang efektif, organisasi dan penyedia layanan cloud dapat mengurangi dampak dari ancaman tersebut dan meningkatkan keamanan. Penyedia layanan cloud harus terus

memperbarui dan mengembangkan teknologi keamanan yang lebih canggih untuk menghadapi ancaman yang semakin meningkat. Selain itu, mereka harus memperkuat kerja sama antara penyedia layanan cloud dan pelanggan untuk menjaga keamanan data.

Referensi :

Anggraini, I. R., & Rahardjo, S., "Analisis Penggunaan Metode CRC dan Checksum untuk Verifikasi Integritas Data pada Sistem Penyimpanan Berkas," *Jurnal Informatika Universitas Pamulang*, 2021.

Bessani, A., Sousa, J., & Correia, M., "Fault and Intrusion Tolerance in the Cloud," *IEEE Cloud Computing*, 2022.

Gunawan, R. A., & Kristalina, T., "Implementasi Checksum dalam Deteksi Kesalahan Data pada File Teks," *Jurnal Teknik ITS*, 2020.

Hakim, M. I., & Simanjuntak, E. F., "Evaluasi Strategi Disaster Recovery System pada Infrastruktur Cloud Berbasis OpenStack," *Jurnal RESTI*, 2023.

Kurniawan, N. R., & Kusuma, D., "Pengembangan Sistem Backup Otomatis untuk Meningkatkan Ketahanan Data," *Jurnal Ilmiah Komputer dan Informatika KOMPUTA*, 2021.

Maulana, M., Riduan, M. S., Ripandi, M. A., Maulida, M., & Feriadi, "Pengertian Sistem Berkas," *Scribd*, 2021.

Putri, R. N., Wibowo, T. M., & Syafei, E. Y., "Pengaruh Redundansi Data Terhadap Ketersediaan Sistem File Berbasis Cloud," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 2022.

Sharma, A., Bhardwaj, K., & Singh, R., "Enhancing Cloud File System Performance and Reliability with Adaptive Redundancy Techniques," *Computer Standards & Interfaces*, 2021.

Subedi, P. A., & Jha, S., "Data Integrity Verification with Improved Checksum Algorithms in Distributed Storage," *Journal of Systems and Software*, 2021.

Santoso, T. R., "Analisis Perbandingan Teknologi RAID untuk Redundansi Sistem File," *Jurnal Teknologi dan Informasi (JATI)*, 2021.

Syahputra, D. P., & Rahmat, L. I., "Pemanfaatan Snapshot Backup untuk Meningkatkan Ketahanan Data dalam Server File Linux," *Jurnal JTIIK*, 2022.

Wicaksono, F. K., & Firmansyah, D. A., "Rancang Bangun Sistem Pemulihan Data Berbasis Snapshot dan Replikasi Lokal," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK)*, 2019.

Wang, R., & Zhang, X., "Error Recovery in Distributed File Systems: Recent Advances and Future Trends," *Journal of Parallel and Distributed Computing*, 2022.

Zhao, Y., Wu, H., Lu, C., & Zhang, H., "Design and Implementation of a Reliable File Storage System Based on Redundant Technologies," *IEEE Access*, 2021.

ISO/IEC 27001:2013 – Information Security Management Systems International Organization for Standardization (ISO), "ISO/IEC 27001:2013: Information Security Management Systems – Requirements," ISO, 2013.

NIST Cybersecurity Framework - National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," NIST, 2018. [Online]. Available: https://www.nist.gov/cyberframework.

Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," 2020.

Yadav, S. P., "Security Risks and Mitigation in Cloud Computing," *International Journal of Computer Applications*, 2019.

Rohit, S. P., "Cloud Computing Security Risks and Mitigation," *Journal of Information Security*, 2020.

Bessani, A., & Sousa, J., "Fault and Intrusion Tolerance in the Cloud," *IEEE Cloud Computing*, 2022.