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

Analisis Strategi Keamanan Data pada Layanan Komputasi Awan

Mukhamad Zulfa Bakhtiar Amalani[1], Rezi Lutfayza[2], Maulana Izaki[3]

[1]Teknik Informatika, STMIK YMI Tegal, Tegal
[2]Teknik Informatika, STMIK YMI Tegal, Tegal
[3]Magister Teknik Informatika, Universitas Dian Nuswantoro, Semarang
[1,2]Jln. Pendidikan No. 1, Kelurahan Pesurungan Lor, Kota Tegal, 52142, Indonesia
[3]Jalan Imam Bonjol No. 207, Pendrikan Kidul, Kota Semarang, 50131, Indonesia
email: [1]zulfabakhtiar0107@gmail.com, [2]reziilutfayzaa03@gmail.com, [3]maulana.izaki@gmail.com

Abstract **– Data security is a vital concern in cloud computing due to significant risks to user data privacy and integrity. This study analyzes security strategies focusing on four key aspects: authentication, confidentiality, access control, and authorization. Using a literature review and analysis of security implementations by providers such as Amazon Web Services (AWS), Dell, and Oracle, this research identifies effective measures to enhance data protection. Results indicate that multi-factor authentication, robust encryption, policy-based access control, and role-based authorization effectively mitigate security risks. The study also emphasizes the need for an integrated approach to counter threats like Distributed Denial of Service (DDoS) attacks and Man-in-the-Middle attacks. By adopting standardized security frameworks, such as RSA and AES encryption, cloud services can offer enhanced protection and build user trust. This research contributes to understanding how comprehensive security strategies ensure data integrity and confidentiality in cloud environments.**

Abstrak **– Keamanan data merupakan salah satu isu krusial dalam implementasi layanan komputasi awan (cloud computing), terutama karena tingginya risiko terhadap privasi dan integritas data pengguna. Penelitian ini bertujuan untuk menganalisis strategi keamanan data yang mencakup empat aspek utama, yaitu otentikasi, kerahasiaan, kontrol akses, dan otorisasi. Metode penelitian melibatkan studi literatur dan analisis terhadap berbagai implementasi keamanan pada penyedia layanan cloud terkemuka, seperti Amazon Web Services (AWS), Dell, dan Oracle. Hasil penelitian menunjukkan bahwa kombinasi otentikasi multifaktor, enkripsi data yang kuat, pengaturan kontrol akses berbasis kebijakan, serta otorisasi berbasis peran dapat meningkatkan perlindungan data secara signifikan. Pembahasan lebih lanjut menyoroti pentingnya pendekatan keamanan yang terintegrasi untuk menghadapi ancaman seperti Distributed Denial of Service (DDoS) dan serangan Man-in-the-Middle. Kesimpulan dari penelitian ini menegaskan bahwa adopsi strategi keamanan data yang komprehensif dan berbasis standar, seperti RSA dan AES, dapat meningkatkan kepercayaan pengguna terhadap layanan komputasi awan.**

Kata Kunci **– Keamanan data, komputasi awan, otentikasi, enkripsi, kontrol akses, otorisasi.**

*) **penulis korespondensi**: Mukhamad Zulfa Bakhtiar Amalani
Email: zulfabakhtiar0107@gmail.com

I. PENDAHULUAN

Teknologi Cloud Computing merupakan salah satu paradigma komputasi modern yang telah mengubah cara perusahaan mengelola sumber daya teknologi informasi[1]. Melalui pendekatan ini, organisasi dapat memanfaatkan infrastruktur komputasi secara bersama-sama, mirip dengan model penggunaan jaringan listrik nasional. Konsep ini menawarkan efisiensi dan efektivitas biaya yang tinggi dibandingkan dengan kebutuhan untuk membangun dan memelihara infrastruktur TI secara mandiri. Selain itu, Cloud Computing memberikan fleksibilitas yang lebih besar dalam penyesuaian sumber daya sesuai kebutuhan organisasi. Dengan demikian, teknologi ini menjadi solusi yang ekonomis dan adaptif bagi berbagai sektor industri[2].

Perusahaan teknologi terkemuka, seperti Google, Amazon, Cisco, IBM, dan Dell, telah melakukan investasi yang signifikan dalam pengembangan teknologi Cloud Computing[3]. Investasi tersebut ditujukan untuk menyediakan berbagai solusi cloud yang dapat memenuhi kebutuhan bisnis dan individu. Salah satu keunggulan utama teknologi ini adalah kemampuannya untuk mengurangi waktu dan biaya dalam pengelolaan sistem informasi. Selain itu, teknologi ini menawarkan akses ke infrastruktur teknologi informasi yang dapat disesuaikan dengan kebutuhan pengguna[4]. Infrastruktur tersebut dirancang agar tetap aman, efisien, dan hemat biaya, sehingga menjadi solusi yang relevan untuk berbagai sektor.

Cloud Computing menawarkan berbagai model yang dapat disesuaikan dengan kebutuhan spesifik organisasi[5]. Berdasarkan lokasi, teknologi ini terdiri atas empat tipe utama, yaitu *public cloud* yang dikelola oleh vendor eksternal, *private cloud* yang digunakan secara eksklusif oleh organisasi, *hybrid cloud* yang menggabungkan keduanya, serta *community cloud* yang berbagi infrastruktur antar organisasi serupa. Dari sisi layanan, Cloud Computing dapat diklasifikasikan menjadi tiga model utama: *Software as a Service* (SaaS), *Platform as a Service* (PaaS), dan *Infrastructure as a Service* (IaaS)[6]. Ketiga model layanan tersebut dirancang untuk memberikan tingkat kontrol, fleksibilitas, dan efisiensi yang berbeda sesuai kebutuhan pengguna. Dengan pendekatan ini, Cloud

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

Computing mampu memenuhi kebutuhan yang beragam, baik untuk organisasi kecil maupun skala besar[7].

Gambar 1 Arsitektur Cloud Computing

Cloud Computing dapat diklasifikasikan berdasarkan lokasi dan jenis layanan yang ditawarkan. Dari segi lokasi, terdapat empat model utama: public cloud (dikelola vendor eksternal), private cloud (infrastruktur khusus satu organisasi), hybrid cloud (kombinasi private dan public), dan community cloud (berbagi infrastruktur antar organisasi serupa). Sedangkan berdasarkan layanan, Cloud Computing dibedakan menjadi tiga kategori: Infrastructure as a Service (IaaS) yang menyediakan sumber daya komputasi dasar, Platform as a Service (PaaS) yang menawarkan platform pengembangan lengkap, dan Software as a Service (SaaS) yang memberikan akses langsung ke aplikasi melalui internet.

II. PENELITIAN YANG TERKAIT

Penelitian sebelumnya dengan judul **"Implementasi Cloud Computing terhadap Keamanan Layanan Publik"**, yang ditulis oleh Endang Suhendar. Teknologi cloud computing menjadi salah satu pendekatan revolusioner yang memungkinkan pengelolaan data lebih efisien dan fleksibel. Jurnal ini menyoroti pentingnya keamanan data dalam pelayanan publik, dengan menekankan perlunya strategi mitigasi ancaman, serta pengembangan langkah penerapan layanan cloud yang efektif dan efisien[8].

Penelitian terkait dengan judul **"Analisis Dampak Cloud Computing terhadap Keamanan Sistem dan Data"**, yang ditulis oleh Razman Rifany, Mario Dwi Prakoso, Pandu Dwi Laksono. Penelitian ini memberikan kontribusi signifikan pada identifikasi risiko keamanan dalam penerapan teknologi cloud computing, seperti ancaman akses tidak sah dan kebocoran data. Jurnal ini menekankan pentingnya strategi mitigasi yang meliputi autentikasi, enkripsi data, dan pemilihan layanan cloud yang terpercaya. Dengan pendekatan analisis yang komprehensif, penelitian ini membuka wawasan tentang tantangan utama keamanan cloud, serta menawarkan langkah-langkah praktis untuk melindungi integritas data dan sistem[9].

Penelitian terdahulu dengan judul **"Analisis Keamanan pada Cloud Computing",** yang ditulis oleh Charles Josua Napitupulu. Penelitian ini mengulas secara mendalam berbagai tantangan dan strategi keamanan pada teknologi Cloud Computing, yang telah menjadi tren utama di era digital. Jurnal ini memberikan kontribusi signifikan dengan menganalisis resiko dan solusi terkait keamanan data, termasuk enkripsi, pengelolaan akses, dan kebutuhan standar global dalam menjaga integritas data. Dengan pendekatan yang komprehensif[10].

III. METODE PENELITIAN

A. Otentikasi

Otentikasi dalam cloud computing bertujuan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data yang disediakan oleh penyedia layanan cloud. Proses otentikasi ini melibatkan pembuktian identitas pengguna kepada penyedia layanan sebelum mereka dapat mengakses informasi yang tersimpan di cloud. Pada implementasinya, layanan cloud publik dan privat sering memanfaatkan desain berbasis RSA untuk mendukung berbagai model otentikasi, seperti autentikasi dua faktor, berbasis pengetahuan, dan adaptif. Salah satu contoh penerapan adalah Amazon Web Services (AWS), yang memprioritaskan keamanan dalam transfer informasi rahasia antara server web dan browser, termasuk dalam lingkungan private cloud virtual. AWS mengintegrasikan berbagai skema otentikasi, termasuk autentikasi multifaktor, manajemen akses, dan pengelolaan identitas, untuk meningkatkan perlindungan data dan akses pengguna.

B. Kerahasian dalam Cloud Computing

Kerahasiaan merupakan salah satu aspek keamanan yang sangat penting untuk melindungi data pengguna dalam layanan cloud computing. Upaya menjaga kerahasiaan dilakukan melalui proses enkripsi plaintext menjadi teks sandi sebelum data disimpan di cloud. Metode ini dirancang untuk memastikan bahwa data pengguna terlindungi, sehingga bahkan penyedia layanan cloud sekalipun tidak dapat membaca atau memodifikasi data yang tersimpan. Salah satu contoh penerapan adalah solusi dari Dell, yang menyediakan perlindungan data dengan enkripsi yang dapat diterapkan baik melalui perangkat lunak maupun perangkat keras. Selain itu, Dell menggunakan Transparent File Encryption untuk mengontrol akses pengguna terhadap data. Wuala cloud juga menawarkan mekanisme enkripsi, di mana data dienkripsi terlebih dahulu di perangkat pengguna sebelum dikirimkan ke cloud, memastikan bahwa bahkan penyedia layanan tidak memiliki akses ke data tersebut.

C. Kontrol Akses

Kontrol akses merupakan salah satu mekanisme keamanan krusial untuk memastikan perlindungan data dalam cloud computing. Mekanisme ini dirancang untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data yang tersimpan di cloud. Berbagai metode pengamanan dapat diterapkan untuk mendukung kontrol akses yang efektif, termasuk *Intrusion Detection System* (IDS), firewall, dan pengaturan hak akses (*privilege*). Firewall, misalnya, dapat dikonfigurasi untuk hanya mengizinkan konten yang telah difilter sesuai kebijakan keamanan pengguna untuk melewati jaringan cloud. Selain itu, firewall sering kali diintegrasikan dengan zona demiliterisasi (*Demilitarized Zone* atau DMZ) guna menambahkan lapisan keamanan ekstra untuk melindungi data dari ancaman eksternal. Implementasi metode-metode ini memastikan bahwa akses

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

data di cloud computing tetap aman dan terkendali sesuai dengan kebijakan yang telah ditetapkan.

D. Otorisasi

Otorisasi dalam cloud computing merupakan elemen penting yang memastikan bahwa pengguna memiliki akses yang sesuai saat mereka menggunakan berbagai layanan cloud. Proses otorisasi ini biasanya dilakukan setelah langkah otentikasi untuk memberikan kontrol tambahan terhadap akses data. Salah satu contoh implementasi otorisasi adalah *Oracle Database Vault*, sebuah solusi keamanan yang ditawarkan oleh Oracle untuk melindungi data aplikasi pengguna administratif. Metode ini memungkinkan penerapan kebijakan otorisasi yang dirancang untuk menjaga privasi pengguna, sehingga mereka dapat menetapkan kebijakan akses dan privasi sesuai kebutuhan. Dengan pendekatan ini, data pengguna terlindungi secara efektif dari akses yang tidak sah, memastikan keamanan yang lebih baik dalam lingkungan cloud computing.

IV. HASIL DAN PEMBAHASAN

terdapat empat kategori utama mekanisme pengamanan yang efektif untuk melindungi data dalam cloud computing. Pertama, otentikasi merupakan langkah penting untuk memastikan hanya pengguna yang sah dapat mengakses data, dengan metode seperti autentikasi dua faktor, berbasis pengetahuan, adaptif, dan multifaktor, seperti yang diterapkan oleh AWS. Kedua, kerahasiaan data dijaga melalui enkripsi sebelum penyimpanan di cloud menggunakan metode seperti Transparent File Encryption dan Full Disk Encryption. Enkripsi ini memastikan bahwa data tidak dapat diakses atau dimodifikasi oleh pihak yang tidak berwenang, bahkan oleh penyedia layanan cloud. Ketiga, kontrol akses dilakukan dengan memanfaatkan firewall, Intrusion Detection System (IDS), dan pengaturan hak akses, yang memastikan bahwa hanya pengguna berwenang yang dapat mengakses data. Penambahan zona demiliterisasi (Demilitarized Zone atau DMZ) juga memberikan lapisan perlindungan tambahan. Keempat, otorisasi digunakan setelah otentikasi untuk membatasi akses data berdasarkan kebijakan tertentu, dengan salah satu contoh implementasi berupa Oracle Database Vault yang melindungi data pengguna administratif.

Pembahasan penelitian ini menyoroti pentingnya penerapan langkah-langkah pengamanan yang terintegrasi guna menghadapi ancaman keamanan seperti Distributed Denial of Service (DDoS) dan Man-in-the-Middle Attacks. Pernyataan dalam jurnal ini menegaskan bahwa kombinasi metode otentikasi yang kuat, enkripsi data yang efektif, kontrol akses yang ketat, dan kebijakan otorisasi yang fleksibel dapat meningkatkan kepercayaan pengguna terhadap layanan cloud computing. Selain itu, penulis merekomendasikan peningkatan keamanan melalui pengelolaan kontrol administratif, pengaturan akses jaringan yang lebih baik, dan penerapan enkripsi berbasis standar seperti RSA dan AES. Dengan implementasi yang menyeluruh, layanan cloud computing dapat diandalkan untuk melindungi data pengguna dari berbagai ancaman keamanan.

Mekanisme Pengamanan	Deskripsi	Contoh Implementasi
Otentikasi	Proses untuk memastikan hanya pengguna yang sah yang dapat mengakses data.	Autentikasi multifaktor (AWS), autentikasi berbasis pengetahuan.
Kerahasiaan	Melindungi data melalui enkripsi sebelum penyimpanan di cloud agar tidak dapat diakses pihak tak berwenang.	*Transparent File Encryption* (Dell), *Full Disk Encryption*.
Kontrol Akses	Mengatur hak akses sehingga hanya pengguna yang berwenang dapat mengakses data.	*Intrusion Detection System* (IDS), firewall, zona DMZ.
Otorisasi	Mengatur izin pengguna berdasarkan kebijakan setelah proses otentikasi selesai.	*Oracle Database Vault*, kebijakan berbasis akses.

V. KESIMPULAN

Kesimpulan dari penelitian ini menegaskan bahwa perlindungan data dalam cloud computing dapat dicapai secara optimal melalui penerapan metode pengamanan yang komprehensif. Evaluasi terhadap empat aspek utama, yaitu otentikasi, kerahasiaan, kontrol akses, dan otorisasi, menunjukkan bahwa pendekatan-pendekatan ini efektif dalam mengatasi berbagai tantangan keamanan, termasuk ancaman terhadap privasi dan integritas data. Penulis juga merekomendasikan langkah-langkah tambahan, seperti pengelolaan hak akses yang efisien, penggunaan enkripsi berbasis standar seperti RSA dan AES, serta implementasi sistem backup yang memadai untuk memitigasi risiko kehilangan data. Dengan mengadopsi langkah-langkah ini, layanan cloud computing dapat memberikan jaminan keamanan yang lebih baik bagi penggunanya. Oleh karena itu, penerapan metode pengamanan yang terintegrasi dan sesuai kebutuhan sangat penting untuk meningkatkan kepercayaan dan keberlanjutan penggunaan teknologi cloud computing dalam berbagai sektor.

UCAPAN TERIMA KASIH

Penghargaan yang setinggi-tingginya disampaikan kepada STMIK Tegal atas fasilitas dan dukungan yang telah diberikan selama proses penelitian ini. Terima kasih juga ditujukan kepada para ahli di bidang keamanan data

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

yang telah memberikan masukan berharga serta kepada tim teknologi informasi yang mendukung proses analisis teknis penelitian ini.

Apresiasi khusus disampaikan kepada keluarga, rekan sejawat, dan semua pihak yang telah memberikan dukungan moral maupun profesional selama pelaksanaan penelitian ini.

Semoga hasil penelitian ini dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan data dalam layanan komputasi awan dan menjadi acuan bagi penelitian lebih lanjut di masa mendatang.

DAFTAR PUSTAKA

[1] E. Barus, K. M. Pardede, and J. A. Putri Br. Manjorang, "Transformasi Digital: Teknologi Cloud Computing dalam Efisiensi Akuntansi," *J. Sains dan Teknol.*, vol. 5, no. 3, pp. 904–911, 2024, doi: 10.55338/saintek.v5i3.2862.

[2] Julia, M. I. Mutahari, Renaldi, and Saepullah, "Analisis Kinerja Basis Data Terdistribusi dalam Linkungan Cloud Computing," *Karimah Tauhid*, vol. 3, no. 2, pp. 1771–1782, 2024, doi: 10.30997/karimahtauhid.v3i2.11907.

[3] T. Gunawan, "Peran Teknologi Cloud Computing Dalam Transformasi Infrastruktur Ti Perusahaan," *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 3, pp. 11393–11401, 2024.

[4] S. Bahri, "Analisa Kebutuhan Cloud Computing Dalam Mendukung Bisnis Perusahaan," *Inform. Eng. Sci. J.*, vol. 9, no. 2, pp. 1–4, 2019.

[5] R. P. Anugrah, I. Yatini, and M. A. Nugroho, "Implementasi Openstack Untuk Infrastruktur Private Cloud Computing," *J. Inf. Syst. Manag.*, vol. 4, no. 1, pp. 36–41, 2022, doi: 10.24076/joism.2022v4i1.768.

[6] Z. Masyhur, A. Rizaldy, and P. Kartini, "Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive," *J. Software, Hardw. Inf. Technol.*, vol. 1, no. 2, pp. 31–38, 2021, doi: 10.24252/shift.v1i2.15.

[7] D. Salsabilla, R. N. Awaliyah, S. Nuraisyah, and A. N. Muslihah, "Cloud Computing untuk Pengelolaan Keuangan : Analisis Efisiensi dan Efektivitas," vol. 3, no. 5, pp. 4046–4054, 2024.

[8] E. Suhendar, "Tinjauan Sistematis : Implementasi Cloud Computing Terhadap Keamanan Layanan Publik," *Smart Comp Jurnalnya Orang Pint. Komput.*, vol. 11, no. 4, pp. 599–606, 2022, doi: 10.30591/smartcomp.v11i4.4245.

[9] R. Rifany, M. D. Prakoso, and P. D. Laksono, "Analisis Dampak Cloud Computing terhadap Keamanan Sistem dan Data," vol. 8, no. 2502, pp. 01–06, 2023.

[10] T. Jaringan, I. Print, I. Online, C. J. Napitupulu, and U. S. Utara, "InfoTekJar : Jurnal Nasional Informatika dan Analisis Keamanan pada Cloud Computing," vol. 2, pp. 2–4, 2023.