CLOUD COMPUTING PEMAHAMAN MODEL LAYANAN IaaS, PaaS, SaaS, DAN ASPEK KEAMANAN

Muhammad Faris Alifiansyah[1], Hermansyah[2] , Nabilanisa Agustin[3] , Muhammad Zibril Tafa Tabia[4] , Muhammad Rivan Surya[5] , Muhammad Ridho Ramadhan[6] , Muhammad Raeyhan[7] , Muhammad Fikri[8], Muhammad Encep[9]

[1]Computer Sciene, Universitas Djuanda Bogor, farisalifiansyah@gmail.com

[2]Computer Sciene, Universitas Djuanda Bogor, syahhermansy@gmail.com

[3]Computer Sciene, Universitas Djuanda Bogor, nabilanisa1108@gmail.com

[4]Computer Sciene, Universitas Djuanda Bogor, i.2510056@unida.ac.id

[5]Computer Sciene, Universitas Djuanda Bogor, i.2510393@unida.ac.id

[6]Computer Sciene, Universitas Djuanda Bogor, i.2510184@unida.ac.id

[7]Computer Sciene, Universitas Djuanda Bogor, muhammadraeyhanrey@gmail.com

[8]Computer Sciene, Universitas Djuanda Bogor, i.2510162@unida.ac.id

[9]Coresponding Author, Universitas Djuanda Bogor, ahmadpoac@unida.ac.id

ABSTRAK

Cloud Computing adalah teknologi yang memungkinkan pengguna menyimpan dan mengakses data melalui internet. Teknologi ini semakin populer karena lebih hemat biaya dan fleksibel. Ada tiga jenis layanan utama dalam cloud, yaitu IaaS (Infrastructure as a Service), PaaS (Platform as a Service), dan SaaS (Software as a Service). Banyak orang masih bingung membedakan ketiganya dan khawatir tentang keamanan data di cloud. Penelitian ini bertujuan untuk menjelaskan perbedaan antara ketiga model layanan tersebut dan bagaimana cara keamanan data dijaga di masing-masing model. Penelitian dilakukan dengan meninjau berbagai sumber seperti artikel jurnal, laporan teknis, dan keamanan siber.. Hasil analisis menunjukkan bahwa perbedaan utama ketiga model terletak pada tingkat kendali dan tanggung jawab keamanan. Pada IaaS, pengguna menyewa infrastruktur dasar seperti server dan jaringan, lalu bertanggung jawab atas keamanan sistem operasi, aplikasi, dan data mereka sendiri. Pada PaaS, penyedia layanan sudah mengelola platform seperti sistem operasi dan database, sehingga pengguna hanya perlu menjaga keamanan aplikasi dan data yang mereka buat. Sedangkan pada SaaS, semua hal teknis dan keamanan dikelola oleh penyedia layanan, sementara pengguna hanya mengatur siapa yang boleh mengakses dan menjaga data yang dimasukkan. Penelitian ini tidak melakukan uji keamanan langsung, melainkan menganalisis konsep dan pembagian tanggung jawab antara penyedia dan pengguna. Kesimpulannya, tidak ada model layanan yang paling aman secara mutlak. Keamanan data di cloud tergantung pada seberapa baik pengguna memahami model layanan yang digunakan dan seberapa jelas pembagian tanggung jawab keamanan antara pengguna dan penyedia layanan.

Kata kunci: Cloud Computing, IaaS, PaaS, SaaS, Keamanan Data

PENDAHULUAN

Cloud Computing kini telah menjadi bagian penting dari dunia digital dan bisnis modern. Teknologi ini tidak lagi dianggap sebagai hal baru, tetapi sudah menjadi pondasi utama dalam strategi digital banyak perusahaan. Penggunaan layanan cloud terus meningkat karena memberikan banyak keuntungan seperti fleksibilitas, kemudahan menambah kapasitas (skalabilitas), dan penghematan biaya. Berdasarkan laporan CloudZero (2025), pengeluaran perusahaan di bidang teknologi informasi kini banyak dialihkan ke layanan berbasis cloud. Secara umum, layanan cloud terbagi menjadi tiga jenis, yaitu Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). Ketiga model ini menawarkan tingkat layanan yang berbeda-beda sehingga setiap organisasi bisa memilih sesuai dengan kebutuhan mereka.

Walaupun penggunaan cloud semakin meluas, tantangan terbesar yang dihadapi banyak perusahaan dan pengguna adalah keamanan data. Banyak orang masih beranggapan bahwa penyedia layanan cloud bertanggung jawab penuh atas keamanan data mereka. Padahal, kenyataannya keamanan di cloud merupakan tanggung jawab bersama (shared responsibility) antara penyedia layanan dan pengguna. Hal ini berarti ada bagian keamanan yang menjadi tugas penyedia, dan ada pula yang menjadi tanggung jawab pengguna. Seperti dijelaskan oleh (Firmansyah, 2025), peran dan tanggung jawab pengguna berbeda tergantung pada jenis layanan cloud yang digunakan..

Penelitian ini dilakukan untuk membantu menjelaskan perbedaan utama dari ketiga jenis layanan cloud tersebut dengan cara yang sederhana dan mudah dipahami. Pendekatan yang digunakan adalah studi literatur, yaitu dengan meninjau berbagai sumber seperti artikel, laporan teknis, dan penelitian sebelumnya. Tujuan dari studi ini adalah memberikan pemahaman yang lebih jelas tentang perbedaan fungsi antara IaaS, PaaS, dan SaaS, serta bagaimana pembagian tanggung jawab keamanan data diterapkan pada masing-masing model.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur. Tujuan utamanya adalah untuk mengumpulkan, menilai, dan menyimpulkan informasi dari berbagai sumber yang sudah ada mengenai perbedaan layanan cloud computing (IaaS, PaaS, SaaS) (Pemanfaatan Cloud Computing, 2025). Yang paling penting keamanan data aspek paling krusial dalam penerapan layanan cloud computing, terutama karena data pengguna disimpan dan dikelola oleh pihak ketiga (penyedia layanan cloud) (Analisis Risiko Keamanan Data pada Platform Cloud

Computing, 2024). Metode studi literatur dipilih karena memungkinkan peneliti menganalisis konsep dan sistem keamanan cloud yang sudah dipublikasikan sebelumnya tanpa harus melakukan pengumpulan data langsung dari lapangan.

Proses pengumpulan data dilakukan dengan cara mencari dan membaca berbagai literatur secara sistematis dari sumber-sumber digital seperti Google Scholar, ResearchGate, dan berbagai portal jurnal ilmiah yang telah terindeks. Dalam proses pencarian, peneliti menggunakan beberapa kata kunci seperti Cloud Computing, IaaS vs PaaS vs SaaS, Keamanan Data Cloud, Cloud Security Model, dan Shared Responsibility Model.

Data yang ditemukan kemudian dianalisis menggunakan metode analisis isi secara kualitatif. dua fokus utama, yaitu:

1. Perbandingan fitur dan tingkat kontrol antara layanan IaaS, PaaS, dan SaaS.
2. Pembagian tanggung jawab keamanan antara penyedia layanan dan pengguna.

Setelah itu, data dari berbagai sumber dibandingkan untuk menemukan perbedaan mendasar dan dampaknya terhadap keamanan data di masing-masing model layanan cloud. Hasil dari analisis ini kemudian disajikan dalam bagian hasil dan pembahasan agar pembaca dapat memahami perbedaan fungsi dan tanggung jawab keamanan pada setiap jenis layanan cloud dengan lebih mudah.

HASIL DAN PEMBAHASAN

Cloud computing memliki 3 layanan IaaS, PaaS, dan SaaS , namun cloud compuing tidak luput dari keamanan data oleh karena itu kami disini akan menjalaskan hasil dari penilitian. Mengenai pengertian, perbedaan dan system keamanan pada cloud computing.

A. CLOUD COMPUTING

Cloud Computing adalah teknologi penting yang telah mengubah cara kita dalam mengakses dan mengelola data serta layanan komputer. Secara sederhana, cloud computing berarti menggunakan internet untuk menyimpan, mengelola, dan memproses data, tanpa harus memakai server fisik atau computer pribadi sendiri (Riana, 2020). Dengan teknologi ini, pengguna tidak perlu membeli atau merawat perangkat keras besar, karena bisa menyewa sumber daya dari penyedia layanan cloud sesuai kebutuhan. Sistem pembayaran biasanya menggunakan model *pay-as-you-go*, yaitu bayar sesuai dengan pemakaian (Zahra dkk., 2023).

Cloud computing bekerja dengan cara "memvirtualisasikan" sumber daya fisik menjadi layanan digital yang bisa digunakan bersama-sama. Maksudnya, satu

sistem besar milik penyedia cloud bisa dipakai oleh banyak pengguna secara bersamaan, tetapi tetap menjaga keamanan dan privasi masing-masing data (Sistem Informasi FT UNESA, 2025).

Bagi kita sebagai mahasiswa atau pengguna pemula, cloud computing bisa diibaratkan sebagai cara baru menggunakan teknologi tanpa harus memiliki komputer dengan spesifikasi tinggi. Misalnya, kita bisa menjalankan program, menyimpan file, atau membuat aplikasi langsung dari layanan cloud. Dengan begitu, kita tidak perlu fokus pada pengelolaan perangkat keras, melainkan cukup memanfaatkan layanan digital yang sudah tersedia. Hal ini membuat kegiatan komputasi menjadi lebih mudah, efisien, bisa dilakukan bersama (kolaboratif), dan dapat diakses dari mana saja.

Cloud computing memiliki 3 jenis layanan yaitu IaaS, PaaS, dan SaaS:

1. IaaS (Infrasructure as a service)

   Infrastructure as a Service merupakan model layanan *cloud* di mana pengguna menyewa infrastruktur komputasi dasar seperti server virtual, media penyimpanan data, dan jaringan—dari penyedia layanan. Model ini menggeser paradigma pengadaan TI dari investasi perangkat keras (hardware) fisik yang mahal menjadi model biaya operasional berbasis pemakaian (pay-as-you-go).

   IaaS menawarkan fleksibilitas yang tinggi, memungkinkan pengguna untuk menjalankan berbagai aplikasi dan sistem operasi sesuai kebutuhan spesifik, serta memfasilitasi pengembangan proyek komputasi berskala besar (Suliman, 2021).

   Meskipun model IaaS kini telah banyak digunakan di berbagai industri, fleksibilitas tersebut diimbangi dengan tingkat tanggung jawab pengguna yang signifikan. Walaupun penyedia layanan mengelola infrastruktur fisik, pengguna IaaS tetap memegang kendali dan tanggung jawab penuh untuk menginstal, mengkonfigurasi, dan mengelola sistem operasi serta seluruh aplikasi yang dijalankan di atas infrastruktur yang disewa tersebut (Dimitri, 2020). Titik tanggung jawab inilah yang memunculkan tantangan krusial pada sistem perlindungan data dan privasi. Studi mengidentifikasi bahwa kelemahan utama IaaS adalah tingginya risiko pelanggaran data, yang diakibatkan oleh arsitektur berbagi sumber daya antar pengguna (*multi-tenancy*). Selain itu, model ini juga rentan terhadap ancaman dari serangan *Denial of Service* (DoS) dan penyalahgunaan akses oleh pihak internal yang memiliki hak administratif (Kumar et al., 2023).

2. PaaS (Platform as a service)

   Platform as a Service adalah model layanan komputasi awan di mana penyedia layanan menyediakan sebuah platform pengembangan yang lengkap. Platform ini tidak hanya mencakup infrastruktur dasar (seperti server, hardware, dan jaringan), tetapi juga kerangka kerja perangkat lunak (software framework), database, dan runtime yang diperlukan untuk mendukung siklus hidup pembangunan dan pengoperasian aplikasi (Wulf dkk., 2021). Dengan demikian, pengguna mendapatkan lingkungan yang siap guna (*ready-to-use*) dan dapat langsung fokus pada pembuatan serta pengelolaan aplikasi dan data mereka. Tanggung jawab untuk mengelola infrastruktur dasarnya, seperti sistem operasi, *runtime*, atau pemeliharaan *server*, dialihkan sepenuhnya kepada penyedia layanan. Meskipun model ini menyederhanakan proses pengembangan, PaaS sering menghadapi kerentanan keamanan spesifik, terutama terkait risiko akses tidak sah (*unauthorized access*), sehingga diperlukan implementasi model keamanan yang dirancang khusus untuk mengatasi tantangan tersebut (Santoso, 2024). PaaS lebih menempatkan tanggung jawab pada penyedia layanan dan pengelolaan infrastruktur dasar (server, storage, jaringan) sekaligus platform pengembangan (runtime, framework, database). jadi pengguna tidak hanya mendapatkan infrastruktur tetapi juga platform pengembangan yang terkelola. Hal ini memungkinkan kita (terutama pengembang aplikasi) untuk mengurangi beban teknis pengaturan infrastruktur dan middleware, dan lebih memfokuskan sumberdaya pada pengembangan dan inovasi aplikasi.

3. SaaS (Software as a service)

   Software as a Service adalah bagian dari komputasi awan yang terdiri dari aplikasi untuk digunakan oleh end user. Pengguna software dapat langsung menggunakan dan memanfaatkan software tersebut tanpa harus mengeluarkan biaya pengembangan atau pengadaan terlebih dahulu. Selain itu pengguna juga hanya membayar biaya sewa selama masih menggunakan software tersebut. (Dinata & Afrianto, 2023)
   Meskipun SaaS menawarkan kemudahan, platform SaaS juga menyimpan data sensitif pelanggan dan bisnis di cloud, sehingga rentan terhadap serangan siber dan pelanggaran data. (Chillapalli, 2022)

   SaaS merupakan model layanan di mana aplikasi perangkat lunak

disediakan oleh penyedia layanan cloud dan dapat diakses oleh pengguna melalui internet, tanpa pengguna harus mengelola infrastruktur atau platform di bawahnya. (Juroihan dkk., 2024)

B. KEAMANAN DATA CLOUD COMPUTING

Keamanan cloud computing didefinisikan sebagai sebuah disiplin komprehensif yang mengintegrasikan aspek teknologi, kebijakan, dan praktik manajemen risiko yang bertujuan untuk melindungi data serta layanan dalam ekosistem *cloud* yang terdistribusi. Fokus utama disiplin ini mencakup upaya berkelanjutan untuk mengidentifikasi, menganalisis, dan mengatasi berbagai isu keamanan yang timbul secara spesifik pada setiap model layanan, baik itu IaaS, PaaS, maupun SaaS (Achar, 2022).

Dalam praktiknya, lingkungan cloud menghadapi beragam ancaman yang dapat diklasifikasikan ke dalam dua kelompok besar. Pertama, ancaman internal, yang dapat berasal dari penyedia layanan itu sendiri atau dari pengguna lain yang berbagi infrastruktur dalam arsitektur multi-tenancy. Kedua, ancaman eksternal, yang merujuk pada serangan yang dilakukan oleh pihak luar seperti peretas atau entitas berbahaya lainnya (Abdulsalam & Hedabou, 2022, dalam Parast, 2022). Studi juga menyoroti adanya kerentanan spesifik dalam arsitektur keamanan, di mana sebagian besar model gagal menyediakan mekanisme autentikasi dua arah (mutual authentication) antara klien dan *cloud*, sehingga membuka celah terhadap risiko impersonasi layanan (AlAhmad dkk., 2021).

Untuk mitigasi risiko tersebut, tujuan keamanan cloud (cloud security objectives) meliputi pencegahan akses tidak sah ke infrastruktur cloud serta perlindungan data pelanggan (termasuk manajemen identitas). Upaya ini diwujudkan melalui penggunaan solusi keamanan seperti enkripsi SSL/TLS dan kontrol akses intrusi yang diterapkan oleh penyedia layanan (Tahirkheli et al., 2021). Keberhasilan penerapan keamanan cloud pada akhirnya tidak hanya ditentukan oleh kapabilitas teknis dan strategi mitigasi ancaman, tetapi juga sangat bergantung pada pemahaman organisasi dan pengguna terhadap model tanggung jawab bersama (shared responsibility model).

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, kesimpulan utamanya adalah perbedaan antara IaaS, PaaS, dan SaaS terletak pada seberapa besar kendali yang dipegang pengguna dan siapa yang bertanggung jawab atas keamanan. Pada IaaS, pengguna mendapat kendali paling besar (seperti menyewa server kosong), sehingga tanggung jawab keamanannya juga paling besar, termasuk mengamankan sistem

operasi dan data. Pada PaaS, tanggung jawabnya dibagi: penyedia layanan mengamankan platform (sistem operasi dan database), sementara pengguna fokus mengamankan aplikasi dan data yang mereka buat sendiri. Pada SaaS, penyedia layanan mengamankan hampir segalanya, namun pengguna tetap bertanggung jawab untuk menjaga keamanan akun (siapa yang boleh masuk) dan data yang mereka masukkan ke aplikasi.

Temuan terpenting dari penelitian ini adalah tidak ada satu pun model layanan cloud yang "paling aman" secara mutlak. Keamanan data sangat bergantung pada pemahaman pengguna terhadap "Model Tanggung Jawab Bersama" (Shared Responsibility Model). Banyak masalah keamanan terjadi bukan karena teknologinya yang lemah, melainkan karena pengguna keliru menganggap bahwa semua aspek keamanan sudah diurus oleh penyedia layanan.

REFERENSI

CloudZero. (2025). 90+ cloud computing statistics: A 2025 market snapshot. **https://www.cloudzero.com/blog/cloud-computing-statistics/**

Firmansyah, M. A. (2025). Strategi keamanan data pada database cloud computing pencegahan dan perlindungan untuk pengguna layanan. Jurnal BATIRSI, 8(2). **https://e-journal.stmik-tegal.ac.id/index.php/batirsi/article/download/81/61/242**

Analisis Risiko Keamanan Data pada Platform Cloud Computing. (2024). Senatib, 5(1), 71– 83. **https://www.ojs.udb.ac.id/Senatib/article/download/4634/3092**

Suliman, M. E. (2021). A Brief Analysis of Cloud Computing Infrastructure as a Service (IaaS). **https://www.researchgate.net/publication/349297686_A_Brief_Analysis_of_Cloud_Computing_Infrastructure_as_a_ServiceIaaS**

Pemanfaatan Cloud Computing dalam Pengembangan Kecerdasan Buatan - Systematic Literature Review. (2025). Jurnal BUSITI, 4(2). https://jurnal.fikom.umi.ac.id/index.php/BUSITI/article/download/2813/pdf

Sistem Informasi FT UNESA. (2025, Maret 2). Mengenal Cloud Computing: Pengertian, Tipe, dan Fungsinya. FT UNESA. **https://si.ft.unesa.ac.id/post/mengenal-cloud-computing-pengertian-tipe-dan-fungsinya**

Zahra, A. F., Kusuma, Z. H., Putra, I. D., Arifin, R. F., Fadhila, Z. N., Amrozi, Y., & Rozzika,
C. (2023). Penelitian Cloud computing pada Industri, Pendidikan, Kesehatan, Transportasi, dan Perbankan. Jurnal Teknologi Informasi, 9(2), 163–171. https://journal.uta45jakarta.ac.id/index.php/JKTE/article/download/7732/2940

Dimitri, N. (2020). Pricing cloud IaaS computing services. Journal of Cloud Computing:Advances,Systems and Applications https://doi.org/10.1186/s13677-020-00161-2

Wulf, F., Westner, M., & Strahringer, S. (2021). IaaS, PaaS, or SaaS? The Why of Cloud ComputingDeliveryModelSelection. https://scholarspace.manoa.hawaii.edu/items/526aeb05-41e6-42e5-936a-64a742e1f733

Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in Our Modern Threat Landscape. https://www.academia.edu/90477930/Cloud_Computing_Security_for_Multi_Cloud_Service_Providers_Controls_and_Techniques_in_our_Modern_Threat_Landscape

Parast, F. K. (2022). Cloud Computing Security: A Survey of Service-Based Models. Computers&Security,Elsevier. https://www.sciencedirect.com/science/article/pii/S0167404821003977

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and Privacy in Cloud Computing: Technical Review. Future Internet, 14(1), 11. MDPI. https://doi.org/10.3390/fi14010011

AlAhmad, A. S., Aziz, K., & Zainal, A. (2021). Mobile Cloud Computing Models Security Issues: A Systematic Review. Journal of Network and Computer Applications, 191, 103152. Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S1084804521001673

Riana, E. (2020). Implementasi Cloud Computing Technology dan Dampaknya Terhadap Kelangsungan Bisnis Perusahaan Dengan Menggunakan Metode Agile dan Studi Literatur. https://doi.org/10.30865/jurikom.v7i3.2192

Dinata, F. C., & Afrianto, I. (2023). Tinjauan Literatur: Penerapan Cloud Computing pada Sistem Pemesanan Cafe Menggunakan Software As A Service (SaaS).Universitas KomputerIndonesia. https://www.researchgate.net/publication/368562243_Tinjauan_Literatur_Pener

apan_
Cloud_Computing_pada_Sistem_Pemesanan_Cafe_Menggunakan_Software_As_A_Service_SaaS.pdf

Kurniawan, S., Ruseno, N., Irfansyah, D., & Santoso, G. (2025). Analisis Tren Teknologi Cloud Computing dalam E-Business dan E-Commerce untuk Optimalisasi Operasional. https://doi.org/10.9001/jurnalpasti.v1i1.917

Chillapalli, N. T. R. (2022). Software as a Service (SaaS) in E-Commerce: The Impact of Cloud Computing on Business Agility. Sarcouncil Journal of Engineering and Computer Sciences, https://sarcouncil.com/download-article/SJECS-2022.pdf

Juroihan, M., Khoirul Fikri, W., Mohdo, L., Fikri, M., Nuansa, R., & Encep, M. (2024). Integrasi Cloud Computing untuk Analisis Big Data. Karimah Tauhid, 3(4), 4387-4399. https://doi.org/10.30997/karimahtauhid.v3i4.12679

Kumar, S., Rajlingam, A., & Gokila, B. (2023). Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies. https://jscer.org/wp-content/uploads/2023-Volume%206-Issue%208/Study%20Analysis%20of%20Cloud%20Security%20Challenges%20and%20Issues%20in%20Cloud%20Computing%20Technologies%20five.pdf

Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., & Kim, K-Il. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. https://doi.org/10.3390/electronics10151811