E-ISSN 3032-601X & P-ISSN 3032-7105
Vol. 1, No. 4, Tahun 2024

MISTER

Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research

Jurnal Penelitian Multidisiplin dalam Ilmu Pengetahuan, Teknologi dan Pendidikan

UNIVERSITAS SERAMBI MEKKAH
KOTA BANDA ACEH
mister@serambimekkah.ac.id

Journal of Multidisciplinary Inquiry in Science Technology and Educational Research

Journal of MISTER

Vol. 1, No. 4, Tahun 2024

Pages: 1997-2004

Keamanan Cloud Computing Tantangan dan Solusi

Yossi Indrawati Syuhardi, Eko Tri Asmoro

Prodi Teknik Informatika, Universitas Indraprasta PGRI

Article in Journal of MISTER

Available at	:	https://jurnal-serambimekkah.org/index.php/mister/index
DOI	:	https://doi.org/10.32672/mister.v1i4.2171

How to Cite this Article

APA	:	Syuhardi, Y. I., & Asmoro, E. T. (2024). Keamanan Cloud Computing Tantangan dan Solusi. *MISTER: Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research*, *1*(4), 1997 – 2004. https://doi.org/10.32672/mister.v1i4.2171
Others Visit	:	https://jurnal-serambimekkah.org/index.php/mister/index

ISSN 3032-7105 ISSN 3032-601X

Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research
UNIVERSITAS SERAMBI MEKKAH
https://jurnal-serambimekkah.org/index.php/mister

e-ISSN 3032-601X & p-ISSN 3032-7105
Vol. 1 No. 4, Tahun 2024
Doi: 10.32672/mister.v1i4.2171
Hal. 1997-2004

Keamanan Cloud Computing Tantangan dan Solusi

Yossi Indrawati Syuhardi[1], Eko Tri Asmoro[2*]
Prodi Teknik Informatika, Universitas Indraprasta PGRI[1,2]

[*]Email Korespodensi: asmorotrieko@gmail.com

Diterima: 23-08-2024 | Disetujui: 24-08-2024 | Diterbitkan: 25-08-2024

ABSTRACT

Cloud computing has become a key technology in digital transformation, offering significant benefits in terms of scalability, flexibility, and cost efficiency. However, the adoption of cloud computing also presents substantial security challenges, including risks to data security, identity and access management, regulatory compliance, insider threats, and isolation issues in multi-tenant environments. These challenges can lead to data breaches, unauthorized access, and non-compliance with international security standards. Proposed solutions include the use of data encryption, implementation of multi-factor authentication and Zero Trust architecture, regular security audits, security awareness training, and isolation technologies such as Virtual Private Cloud (VPC). By adopting these measures, organizations can minimize cloud security risks and fully leverage the benefits of cloud technology.

Keywords*: Cloud Computing Security, Security Challenges, Identity And Access Management*

ABSTRAK

Cloud computing telah menjadi teknologi kunci dalam transformasi digital, memberikan keuntungan besar dalam hal skalabilitas, fleksibilitas, dan efisiensi biaya. Namun, adopsi cloud computing juga membawa tantangan keamanan yang signifikan, termasuk risiko terhadap keamanan data, manajemen identitas dan akses, kepatuhan terhadap regulasi, ancaman insider, dan masalah isolasi di lingkungan multi-tenant. Tantangan-tantangan ini dapat mengakibatkan kebocoran data, akses tidak sah, dan ketidakpatuhan terhadap standar keamanan internasional. Solusi yang diusulkan meliputi penggunaan enkripsi data, penerapan autentikasi multi-faktor dan arsitektur Zero Trust, audit keamanan berkala, pelatihan kesadaran keamanan, dan teknologi isolasi seperti Virtual Private Cloud (VPC). Dengan mengadopsi langkah-langkah ini, organisasi dapat meminimalkan risiko keamanan cloud dan memanfaatkan sepenuhnya manfaat teknologi cloud.

Kata kunci: Keamanan Cloud Computing, Tantangan Keamanan, Manajemen Identitas Dan Akses

e-ISSN3032-601X & p-ISSN3032-7105

PENDAHULUAN

Dalam beberapa tahun terakhir, *cloud computing* telah menjadi landasan utama bagi banyak organisasi dalam mendukung transformasi digital mereka. Dengan adopsi teknologi *cloud,* organisasi dapat mengakses sumber daya komputasi yang fleksibel dan skalabel, yang memungkinkan mereka untuk berinovasi lebih cepat, mengurangi biaya operasional, dan meningkatkan efisiensi. Namun, seiring dengan meningkatnya penggunaan layanan cloud, muncul pula tantangan yang signifikan terkait dengan keamanan data dan sistem. Salah satu tantangan utama dalam cloud computing adalah masalah keamanan (Srivastava & Sudhish, 2015). Salah satu tantangan utama dalam cloud computing adalah masalah keamanan, yang mencakup risiko pencurian data, serangan siber, dan kurangnya kontrol atas informasi yang disimpan di lingkungan cloud, sehingga memerlukan strategi mitigasi yang efektif untuk menjaga keamanan data (Mishra et al., 2020).

Situasi ini memerlukan pemahaman komprehensif tentang lanskap keamanan untuk memastikan organisasi dapat secara efektif melindungi informasi sensitif sambil memanfaatkan manfaat lingkungan komputasi awan. Pemahaman ini melibatkan pengenalan kerentanan unik yang terkait dengan arsitektur cloud, termasuk meningkatnya risiko akses tidak sah dan kompleksitas pengelolaan keamanan di berbagai model layanan, yang harus diatasi untuk membangun kepercayaan pelanggan dan memastikan integritas data di lingkungan cloud (Behl, 2011). Selain itu, sifat komputasi awan yang beragam menuntut agar organisasi tidak hanya menerapkan langkah-langkah keamanan yang kuat namun juga mengadopsi pendekatan adaptif terhadap tata kelola keamanan yang dapat secara efektif merespons lanskap ancaman yang terus berkembang dan persyaratan kepatuhan yang melekat pada layanan cloud (Sambaiah.G, 2020). Untuk mencapai hal ini, organisasi harus memprioritaskan penilaian risiko menyeluruh dan mengembangkan kerangka keamanan khusus yang mengintegrasikan praktik terbaik dari paradigma keamanan tradisional dan cloud, sehingga dapat mengatasi ancaman yang ada dan yang muncul yang ditimbulkan oleh lingkungan komputasi awan yang dinamis.

Perpindahan dari infrastruktur IT tradisional ke lingkungan cloud mengubah lanskap keamanan secara mendasar. Di lingkungan cloud, data tidak lagi disimpan dan dikelola secara lokal di pusat data milik organisasi, melainkan di infrastruktur yang dikelola oleh penyedia layanan cloud. Hal ini menimbulkan kekhawatiran baru tentang kontrol dan visibilitas data, terutama dalam konteks manajemen akses, kepatuhan terhadap regulasi, serta perlindungan terhadap ancaman siber. Dalam lingkungan cloud, layanan keamanan yang diberikan oleh penyedia cloud harus dapat menjamin kerahasiaan, integritas, dan ketersediaan data. Namun, penting untuk diingat bahwa penawaran default dari penyedia cloud publik biasanya tidak mencerminkan kebutuhan spesifik keamanan dan privasi organisasi, sehingga penyesuaian terhadap lingkungan cloud mungkin diperlukan untuk memenuhi persyaratan tersebut (Jansen & Grance, 2011).

Hal ini memerlukan pendekatan proaktif di mana organisasi melakukan pemantauan dan evaluasi terus-menerus terhadap langkah-langkah keamanan cloud mereka untuk memastikan keselarasan dengan kebutuhan operasional dan persyaratan peraturan, serta untuk mengatasi setiap kerentanan yang muncul dalam penggunaan layanan cloud publik. Selain itu, tata kelola keamanan yang efektif di lingkungan cloud mengharuskan organisasi untuk mengadopsi strategi komprehensif yang mencakup tidak hanya penerapan teknologi keamanan canggih namun juga penetapan kebijakan dan protokol keamanan yang jelas yang disesuaikan dengan konteks operasional unik dan profil risiko mereka, untuk memastikan bahwa langkah-langkah perlindungan data diterapkan secara konsisten di seluruh sistem dan layanan berbasis cloud.

e-ISSN3032-601X & p-ISSN3032-7105

Selain itu, sifat multi-tenant dari lingkungan cloud publik, di mana beberapa organisasi berbagi infrastruktur yang sama, menambah kompleksitas dalam menjamin isolasi dan keamanan data. Organisasi perlu memastikan bahwa data mereka terlindungi dari akses yang tidak sah, baik dari pihak eksternal maupun dari tenant lain yang menggunakan layanan yang sama. Dalam upaya untuk menghadapi tantangan keamanan yang muncul dari adopsi cloud computing, beberapa penelitian telah mengusulkan kerangka kerja manajemen identitas dan akses, enkripsi data, kompartementasi data, serta integrasi blockchain sebagai solusi yang menjanjikan (Deorankar & Khobragade, 2020). Namun, meskipun berbagai teknik dan sistem sedang dikembangkan untuk meningkatkan keamanan dan privasi, tantangan yang berkaitan dengan kepercayaan pengguna dan kebocoran data tetap menjadi perhatian utama, mengingat bahwa data sensitif sering kali disimpan dan dikelola oleh pihak ketiga di luar kendali organisasi.

Kehadiran ancaman siber yang terus berkembang, seperti serangan ransomware, DDoS, dan ancaman insider, juga menjadi perhatian utama dalam keamanan cloud. Selain itu, ketidakpastian dalam memastikan kepatuhan terhadap berbagai regulasi dan standar keamanan global memperparah risiko yang dihadapi oleh organisasi dalam adopsi cloud. Ketika organisasi bertransisi ke komputasi awan, mereka harus menavigasi kompleksitas ini sambil memastikan bahwa kerangka keamanan mereka tidak hanya kuat namun juga cukup fleksibel untuk beradaptasi dengan lanskap ancaman yang terus berkembang dan perubahan tuntutan peraturan, sehingga mendorong lingkungan cloud yang aman yang dapat mendukung tujuan operasional mereka (Sreelatha et al., 2020). Mengingat tantangan-tantangan ini, penyelarasan strategis antara langkah-langkah keamanan dan tujuan organisasi sangat penting untuk memitigasi risiko secara efektif dan melindungi data sensitif dari ancaman eksternal dan internal, menekankan pentingnya proses penilaian risiko yang berkelanjutan dan praktik keamanan adaptif untuk menjaga kepercayaan dan integritas di dalam perusahaan. sistem berbasis cloud. Mengingat perlunya peningkatan kewaspadaan, organisasi semakin menyadari pentingnya mengintegrasikan teknologi keamanan canggih, seperti pembelajaran mesin dan kecerdasan buatan, untuk meningkatkan postur keamanan cloud mereka dan secara proaktif mengidentifikasi potensi ancaman sebelum mereka dapat mengeksploitasi kerentanan.

Dengan latar belakang ini, penting bagi organisasi untuk memahami tantangan keamanan yang dihadapi dalam penggunaan cloud computing dan mengembangkan strategi yang komprehensif untuk mengatasinya. Organisasi perlu memastikan bahwa langkah-langkah keamanan yang diterapkan mampu melindungi data dan sistem mereka dari ancaman yang ada, sekaligus memanfaatkan manfaat yang ditawarkan oleh cloud computing.

METODE PENELITIAN

Metode penelitian dengan literature review adalah pendekatan yang digunakan untuk mengumpulkan, menganalisis, dan menginterpretasikan informasi dari berbagai sumber literatur yang relevan dengan topik penelitian. Metode ini bertujuan untuk mendapatkan pemahaman yang mendalam tentang topik yang diteliti, mengidentifikasi kesenjangan penelitian, dan memberikan landasan teori yang kuat untuk penelitian lebih lanjut. Metode literature review sangat penting dalam penelitian karena memberikan gambaran yang komprehensif tentang topik yang diteliti dan membantu memastikan bahwa penelitian yang dilakukan memiliki dasar yang kuat.

e-ISSN3032-601X & p-ISSN3032-7105

HASIL

Tantangan Keamanan Data

Salah satu tantangan terbesar yang dihadapi dunia digital saat ini adalah masalah keamanan data. Masalah ini semakin mendalam dengan meningkatnya aktivitas kejahatan siber yang memanfaatkan kelemahan dalam sistem pengumpulan dan penyimpanan data, mengakibatkan risiko penyalahgunaan informasi pribadi yang terus meningkat (Alvi Sholikhatin et al., 2020). Selain itu, kesadaran pengguna tentang perlindungan data pribadi yang diperlukan untuk mencegah kejahatan ini belum sepenuhnya berkembang, sehingga mereka sering kali menjadi korban akibat kurangnya kehati-hatian dalam membagikan informasi sensitif di internet (Soemitro et al., 2023). Kondisi ini menuntut perhatian serius dari semua pihak, termasuk pemerintah dan penyedia layanan digital, dalam mengedukasi masyarakat mengenai risiko yang ada serta pentingnya menjaga privasi data pribadi mereka agar tidak jatuh ke tangan yang salah (Syailendra, 2021).

Survei menunjukkan bahwa kesadaran masyarakat akan pentingnya menjaga kerahasiaan informasi pribadi mereka di media sosial masih relatif rendah. Banyak pengguna tidak sepenuhnya menyadari potensi risiko yang terkait dengan pembagian data pribadi, yang menyebabkan mereka dengan mudah terjebak dalam praktik yang dapat membahayakan keamanan data mereka, seperti berbagi informasi sensitif tanpa memeriksa pengaturan privasi atau menggunakan kata sandi yang mudah ditebak. Selain itu, perlunya pendidikan yang lebih efektif mengenai manajemen privasi dan keamanan data pribadi di berbagai platform digital sangat penting untuk meningkatkan tindakan pencegahan yang diambil oleh pengguna saat berinteraksi secara online. Sebagai bagian dari strategi pendidikan ini, workshop yang menekankan kelebihan dan kekurangan penggunaan media sosial serta tantangan keamanan yang dihadapi pengguna dapat memainkan peran penting dalam meningkatkan pemahaman masyarakat mengenai perangkat yang mereka gunakan dan konsekuensi dari tindakan mereka di dunia digital (Agir & Mohd Matore, 2022).

Tantangan Manajemen Identitas dan Akses (IAM)

Manajemen identitas dan akses telah menjadi bidang yang semakin penting dalam lingkungan teknologi informasi modern. Munculnya struktur internal yang kompleks di organisasi besar, ditambah dengan kebutuhan usaha kecil dan menengah untuk menjamin keamanan tanpa beban infrastruktur yang mahal, mendorong perlunya praktik yang efektif dalam manajemen layanan teknologi informasi untuk mempertahankan kualitas layanan yang tinggi. Hal ini penting karena organisasi berusaha untuk tetap kompetitif sambil menjaga aset informasi mereka dan memastikan kelangsungan layanan di tengah tantangan keamanan yang terus berkembang (Hadiana et al., 2021).

Selain itu, meningkatnya harapan dari pengguna untuk meningkatkan kualitas layanan dan tekanan simultan dari badan pengatur untuk proses kontrol akses yang terdokumentasi menyoroti kebutuhan mendesak bagi organisasi untuk meningkatkan sistem manajemen identitas mereka agar dapat secara efektif menyeimbangkan persyaratan keamanan, biaya, dan kepatuhan (Becker & Drew, 2005). Selain itu, integrasi tata kelola identitas dengan manajemen akses istimewa menghadirkan pendekatan yang menjanjikan bagi organisasi untuk memperkuat kerangka keamanan mereka, memungkinkan mereka mengelola dan mengontrol akses ke data sensitif dengan lebih efektif sekaligus menyederhanakan proses. Selain itu, organisasi juga harus menyadari bahwa metode verifikasi identitas tradisional tidak memadai dalam lanskap digital, sehingga memerlukan penerapan praktik manajemen identitas yang lebih canggih

e-ISSN3032-601X & p-ISSN3032-7105

dan terstandarisasi yang tidak hanya meningkatkan keamanan tetapi juga memfasilitasi kolaborasi di berbagai platform dan yurisdiksi (Parveen et al., 2021).

Ketika organisasi semakin memperluas layanan mereka secara online, penerapan praktik manajemen identitas yang kuat menjadi sangat penting dalam menjaga informasi sensitif dan menjaga kepercayaan pengguna, yang diperburuk dengan tantangan untuk memastikan bahwa hanya individu yang berwenang yang memiliki akses ke data dan sumber daya penting (Smith & McKeen, 2011). Untuk mengatasi tantangan ini, kerangka manajemen identitas dan akses yang komprehensif harus dikembangkan, yang tidak hanya mencakup solusi teknologi tetapi juga kebijakan dan proses yang diperlukan untuk beradaptasi dengan sifat dinamis lingkungan organisasi dan harapan pengguna (Devlekar & Ramteke, 2021). Selain itu, evolusi manajemen identitas memerlukan eksplorasi menyeluruh terhadap keterbatasan yang melekat pada model saat ini, serta pengembangan pendekatan inovatif yang dapat beradaptasi dengan beragam lingkungan dan kasus penggunaan yang ada dalam lanskap digital saat ini, yang pada akhirnya mendorong terciptanya sistem yang lebih aman dan efisien. ekosistem organisasi.

Tantangan Kepatuhan dan Regulasi

Semakin banyak perusahaan yang memperluas pengiriman layanan dan data mereka secara online, mereka harus dapat memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi dan sumber daya sensitive. Hal ini ditegaskan dengan meningkatnya pengawasan peraturan dan perlunya proses manajemen akses yang transparan yang tidak hanya mematuhi undang-undang yang ada namun juga mengantisipasi kebutuhan di masa depan dalam lanskap hukum yang berubah dengan cepat. Hal ini ditegaskan dengan meningkatnya pengawasan peraturan dan perlunya proses manajemen akses yang transparan yang tidak hanya mematuhi undang-undang yang ada namun juga mengantisipasi persyaratan di masa depan dalam lanskap hukum yang berubah dengan cepat, karena organisasi harus bergulat dengan kompleksitas undang-undang perlindungan data pribadi di berbagai negara. yurisdiksi. Seiring berkembangnya peraturan ini, organisasi harus menerapkan strategi komprehensif yang mencakup perlindungan data dan pertimbangan etis, yang pada akhirnya bertujuan untuk menumbuhkan kepercayaan dan keamanan dalam sistem manajemen identitas mereka sekaligus memitigasi risiko yang terkait dengan pelanggaran data dan akses tidak sah ke informasi pribadi (Santosa & Perwira Redi, 2021).

Tantangan Ancaman Insider

Ancaman dari dalam (*insider threats*) merupakan salah satu tantangan utama dalam manajemen identitas dan akses. Ancaman orang dalam ini dapat terwujud dalam berbagai cara, termasuk kelalaian karyawan, niat jahat, atau penyalahgunaan hak akses, sehingga menimbulkan risiko signifikan terhadap aset informasi organisasi dan keseluruhan postur keamanan. Mengatasi risiko-risiko ini memerlukan pendekatan multifaset yang tidak hanya mencakup solusi teknologi yang kuat namun juga kerangka tata kelola yang efektif dan pemantauan berkelanjutan untuk mendeteksi dan memitigasi potensi ancaman dari dalam sebelum ancaman tersebut dapat menimbulkan kerugian (Alsowail & Al-Shehari, 2021).

Selain itu, organisasi harus menyadari bahwa hanya mengandalkan langkah-langkah teknologi saja tidaklah cukup; mereka juga harus menumbuhkan budaya kesadaran dan tanggung jawab keamanan di kalangan karyawan, karena hal ini dapat secara signifikan mengurangi kemungkinan ancaman orang dalam yang berasal dari kelalaian atau penilaian yang buruk. Selain itu, penerapan program pelatihan karyawan komprehensif yang mendidik staf tentang potensi implikasi tindakan mereka dan menanamkan rasa

e-ISSN3032-601X & p-ISSN3032-7105

akuntabilitas dapat berfungsi sebagai tindakan pencegahan terhadap meningkatnya ancaman dari dalam, yang pada akhirnya meningkatkan ketahanan organisasi terhadap risiko tersebut.

Tantangan Isolasi dan *Multi-Tenancy*

Sebagai organisasi semakin memperluas layanan dan data mereka secara digital, kebutuhan untuk manajemen identitas dan akses yang komprehensif semakin mendesak. Kebutuhan ini sangat penting dalam lingkungan multi-penyewa, di mana isolasi data pengguna dan perlindungan informasi sensitif di berbagai klien menjadi hal yang sangat penting untuk menghindari potensi pelanggaran kerahasiaan dan integritas. Dalam konteks seperti ini, memastikan bahwa kontrol akses tersegmentasi dengan tepat dan adanya mekanisme pemantauan yang ketat adalah hal yang penting untuk mencegah akses tidak sah dan menjaga kepatuhan terhadap standar peraturan, karena implikasi dari pelanggaran data dapat melampaui organisasi yang terkena dampak dan berdampak pada semua penyewa di dalamnya.

Di lingkungan cloud publik, di mana beberapa organisasi berbagi infrastruktur yang sama, ada kekhawatiran tentang isolasi data yang tidak memadai antara tenant. Risiko ini dapat menyebabkan kebocoran data antar organisasi yang menggunakan layanan cloud yang sama.

Pembahasan

Data di cloud rentan terhadap berbagai bentuk serangan, baik dari luar maupun dari dalam. Hal ini disebabkan oleh akses yang lebih luas dan sering kali kurangnya visibilitas langsung oleh organisasi terhadap data mereka. Enkripsi data, baik saat transit maupun saat istirahat, menjadi solusi utama untuk melindungi data dari akses yang tidak sah. Selain itu, penerapan teknologi seperti Data Loss Prevention (DLP) dan Security Information and Event Management (SIEM) dapat membantu dalam memonitor dan mendeteksi ancaman terhadap data di cloud.

Kesulitan dalam mengelola akses ke sistem cloud sering kali menyebabkan terjadinya kebocoran data atau akses yang tidak sah. Pengelolaan identitas yang lemah dapat memperbesar risiko ini. Penerapan IAM yang kuat, termasuk penggunaan MFA dan Zero Trust Architecture, dapat membantu memastikan bahwa hanya pengguna yang sah yang dapat mengakses data sensitif. Sistem IAM juga perlu dikonfigurasi dengan kebijakan akses berbasis peran untuk membatasi akses hanya pada data yang relevan dengan tugas pengguna.

Memastikan kepatuhan terhadap regulasi internasional adalah tantangan besar, terutama ketika data disimpan dan diproses di berbagai wilayah dengan regulasi yang berbeda. Organisasi dapat menggunakan layanan cloud yang menawarkan sertifikasi dan kepatuhan terhadap standar internasional seperti ISO 27001, SOC 2, dan GDPR. Selain itu, melakukan audit keamanan secara rutin dan bekerja sama dengan penyedia cloud untuk memastikan kepatuhan juga menjadi langkah penting.

Ancaman insider tetap menjadi tantangan karena pelaku memiliki akses yang sah ke sistem cloud dan sering kali tidak terdeteksi hingga kerusakan telah terjadi. Implementasi sistem pengawasan dan analitik yang kuat untuk mendeteksi aktivitas yang mencurigakan dari dalam organisasi dapat mengurangi risiko serangan insider. Pelatihan dan peningkatan kesadaran keamanan di kalangan karyawan juga sangat penting untuk mengurangi ancaman ini.

Risiko terkait isolasi data di lingkungan multi-tenant cloud dapat menyebabkan kebocoran data antara tenant yang berbeda jika tidak dikelola dengan benar. Menggunakan Virtual Private Cloud (VPC) dan micro-segmentation untuk memastikan isolasi data yang ketat antara tenant adalah langkah kunci.

e-ISSN3032-601X & p-ISSN3032-7105

Selain itu, penyedia cloud perlu memastikan bahwa infrastruktur mereka memiliki kontrol keamanan yang kuat untuk mencegah kebocoran data antar tenant. Keamanan cloud computing menghadirkan tantangan yang kompleks namun dapat diatasi dengan penerapan solusi yang tepat. Organisasi perlu secara proaktif mengadopsi langkah-langkah keamanan yang komprehensif, termasuk enkripsi data, manajemen identitas yang kuat, dan kepatuhan terhadap regulasi. Dengan pendekatan yang tepat, risiko keamanan di cloud dapat diminimalkan, memungkinkan organisasi untuk memanfaatkan sepenuhnya manfaat dari teknologi cloud tanpa mengorbankan keamanan data mereka.

KESIMPULAN

Keamanan dalam cloud computing adalah salah satu aspek paling kritis yang perlu diperhatikan oleh organisasi yang mengadopsi teknologi ini. Meskipun cloud computing menawarkan berbagai keuntungan seperti skalabilitas, fleksibilitas, dan efisiensi biaya, tantangan keamanan yang menyertainya tidak dapat diabaikan. Untuk memanfaatkan sepenuhnya manfaat cloud computing, organisasi harus mengadopsi strategi keamanan yang komprehensif dan proaktif. Ini melibatkan penerapan teknologi keamanan yang canggih, kepatuhan terhadap regulasi yang berlaku, serta edukasi dan pelatihan karyawan. Dengan pendekatan yang tepat, tantangan keamanan cloud dapat diatasi, memungkinkan organisasi untuk mengoperasikan infrastruktur mereka di cloud dengan aman dan efisien.

DAFTAR PUSTAKA

Agir, N., & Mohd Matore, M. E. @ E. (2022). Literasi dan Kewarganegaraan Digital: Konsep dan Strategi Implementasi dalam Pendidikan di Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *7*(3), e001367. https://doi.org/10.47405/mjssh.v7i3.1367

Alsowail, R. A., & Al-Shehari, T. (2021). A Multi-Tiered Framework for Insider Threat Prevention. *Electronics*, *10*(9), 1005. https://doi.org/10.3390/electronics10091005

Alvi Sholikhatin, S., Fitrianingsih, W., & Dhiyaulhaq, S. (2020). WORKSHOP STRATEGI PENINGKATAN POPULARITAS KONTEN SERTA MENJAGA KEAMANAN DATA PRIBADI DI BERBAGAI PLATFORM MEDIA SOSIAL. *SELAPARANG Jurnal Pengabdian Masyarakat Berkemajuan*, *4*(1), 251. https://doi.org/10.31764/jpmb.v4i1.2929

Becker, M., & Drew, M. (2005). Overcoming the challenges in deploying user provisioning/identity access management backbone. *BT Technology Journal*, *23*(4), 71–79. https://doi.org/10.1007/s10550-006-0009-x

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. *2011 World Congress on Information and Communication Technologies*, 217–222. https://doi.org/10.1109/WICT.2011.6141247

Deorankar, A. V., & Khobragade, K. T. (2020). A Review on Various Data Sharing Strategies for Privacy of Cloud Storage. *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, 98–101. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00019

Devlekar, S., & Ramteke, V. (2021). Identity and Access Management: High-level Conceptual Framework. *Revista Gestão Inovação e Tecnologias*, *11*(4), 4885–4897. https://doi.org/10.47059/revistageintec.v11i4.2511

Hadiana, A. I., Putra, E. K., & Melina, M. (2021). Tinjauan Mengenai Potensi Information Technology Infrastructure Library (ITIL) pada Model Layanan Teknologi Informasi di Usaha Kecil Mikro dan Menengah (UMKM). *Informatics and Digital Expert (INDEX)*, *2*(2). https://doi.org/10.36423/index.v2i02.582

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing*. https://doi.org/10.6028/NIST.SP.800-144

Mishra, S., Kumar Sharma, S., & A. Alowaidi, M. (2020). Multilayer Self-defense System to Protect Enterprise Cloud. *Computers, Materials & Continua*, *66*(1), 71–85. https://doi.org/10.32604/cmc.2020.012475

Parveen, S., Ahmad, S., & Khan, M. A. (2021). Integration of Identity Governance and Management Framework within Universities for Privileged Users. *International Journal of Advanced Computer Science and Applications*, *12*(6). https://doi.org/10.14569/IJACSA.2021.0120664

Sambaiah.G. (2020). Imperative Requirements for Data Security in Cloud Computing. *International Journal of Engineering Research And*, *V9*(07). https://doi.org/10.17577/IJERTV9IS070455

Santosa, A. A., & Perwira Redi, A. A. N. (2021). Pemilihan Platform Tanda Tangan Digital Berdasarkan Faktor Keberlanjutan Selama Pandemi COVID-19 Menggunakan Metode AHP. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *12*(2). https://doi.org/10.31849/digitalzone.v12i2.8014

Smith, H. A., & McKeen, J. D. (2011). The Identity Management Challenge. *Communications of the Association for Information Systems*, *28*. https://doi.org/10.17705/1CAIS.02811

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum*, *5*(1), 155–167. https://doi.org/10.37276/sjh.v5i1.272

Sreelatha, G., Babu, A. V., & Midhunchakkarvarthy, D. (2020). A Survey on Cloud Attack Detection using Machine Learning Techniques. *International Journal of Computer Applications*, *175*(34), 21–27. https://doi.org/10.5120/ijca2020920887

Srivastava, S., & Sudhish, P. S. (2015). Security in cloud computing systems: A review of challenges and solutions for security in distributed computing environments. *2015 39th National Systems Conference (NSC)*, 1–5. https://doi.org/10.1109/NATSYS.2015.7489088

Syailendra, M. R. (2021). PERLINDUNGAN DATA PRIBADI TERHADAP TINDAKAN PENYEBARAN SEX TAPE MENURUT HUKUM POSITIF DI INDONESIA. *Jurnal Muara Ilmu Sosial, Humaniora, Dan Seni*, *5*(2), 440. https://doi.org/10.24912/jmishumsen.v5i2.12506.2021