Vol.4, No. 2, 2026, pp.124-132 ISSN 3123-7444

Jurnal Ilmu Ekonomi dan Bisnis

Journal homepage: https://ejournal.pkmpi.org/index.php/ijess/index

Tantangan Keamanan Informasi pada Era *Cloud Computing*: Analisis Literatur mengenai Strategi Kontrol dan Mitigasi Risiko

Aril Sharon Saragih[1], Imam Ariq Rizqy[2].
[1]Aronsharonsaragih@gmail.com [2]Imamariqrizqy@gmail.com
[12]Universitas Negeri Medan

Article Info

Article history:
Received Jun 12th, 2026
Revised Aug 20th, 2026
Accepted Jun 26th, 2026

Kata Kunci:
keamanan informasi, komputasi awan, mitigasi risiko, pengendalian keamanan, manajemen risiko,

ABSTRAK

Perkembangan komputasi awan telah mengubah cara organisasi menyimpan, mengelola, dan mengakses informasi melalui layanan yang lebih fleksibel dan efisien. Di sisi lain, penerapan teknologi ini juga menimbulkan berbagai tantangan terhadap keamanan informasi, seperti risiko kebocoran data, akses yang tidak sah, kehilangan data, serta ancaman serangan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis tantangan keamanan informasi pada era komputasi awan serta mengidentifikasi strategi pengendalian dan mitigasi risiko berdasarkan hasil kajian literatur. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur yang dilakukan melalui penelaahan berbagai artikel ilmiah, buku, dan publikasi yang relevan. Hasil kajian menunjukkan bahwa pengamanan lingkungan komputasi awan tidak hanya ditentukan oleh penggunaan teknologi, tetapi juga oleh penerapan pengendalian yang menyeluruh, seperti pengelolaan identitas dan hak akses, perlindungan data melalui enkripsi, pemantauan keamanan secara berkelanjutan, pelaksanaan audit keamanan, serta penerapan manajemen risiko yang konsisten. Selain itu, peningkatan kesadaran pengguna dan penerapan tata kelola keamanan informasi yang baik turut berperan dalam mengurangi potensi ancaman dan memperkuat perlindungan terhadap aset informasi. Penelitian ini menyimpulkan bahwa kombinasi antara pengendalian teknis, kebijakan organisasi, dan pengelolaan risiko yang berkelanjutan telah menjadi faktor penting dalam menjaga kerahasiaan, keutuhan, dan ketersediaan informasi pada lingkungan komputasi awan.

ABSTARCT

The development of cloud computing has transformed the way organizations stored, managed, and accessed information by providing more flexible and efficient technology services. At the same time, the adoption of this technology has introduced various information security challenges, including the risks of data breaches, unauthorized access, data loss, and increasingly sophisticated cyber threats. This study aimed to analyze the information security challenges in the era of cloud computing and to identify control strategies and risk mitigation measures based on a literature review. The study employed a qualitative approach using a literature review method by examining relevant scholarly articles, books, and academic publications. The findings indicated that securing cloud computing environments was not determined solely by the use of technology but also by the implementation of comprehensive controls,

including identity and access management, data protection through encryption, continuous security monitoring, security auditing, and consistent risk management practices. In addition, increasing user awareness and implementing effective information security governance contributed to reducing potential threats and strengthening the protection of information assets. The study concluded that the combination of technical controls, organizational policies, and continuous risk management played a crucial role in maintaining the confidentiality, integrity, and availability of information within cloud computing environments.

© 2021 Para Penulis. Diterbitkan oleh Perkumpulan Konsultan Manajemen Pendidikan Indonesia (PKMPI). Ini adalah artikel akses terbuka di bawah lisensi CC BY-NC-SA (https://creativecommons.org/licenses/by-nc-sa/4.0

Corresponding Author:
Aril Sharon Saragih
Universitas Negeri Medan
Email: Arilsharonsaragih@gmail.com

Latar Belakang

Transformasi digital yang berlangsung secara masif dalam satu dekade terakhir telah mendorong organisasi dari berbagai sektor untuk mengadopsi komputasi awan sebagai infrastruktur utama dalam pengelolaan informasi. Kemampuan komputasi awan dalam menyediakan sumber daya teknologi secara elastis, skalabel, dan hemat biaya menjadikannya pilihan strategis bagi organisasi yang berupaya meningkatkan efisiensi operasional sekaligus memperluas jangkauan layanan digitalnya. Perkembangan ini sejalan dengan meningkatnya kebutuhan organisasi di Indonesia terhadap layanan digital yang andal dan dapat diakses secara luas tanpa batasan geografis (Pratama & Sulistiyo, 2022; Hidayat & Nurdiansyah, 2021).

Namun demikian, di balik berbagai keunggulan yang ditawarkan, adopsi komputasi awan membawa konsekuensi serius terhadap keamanan informasi. Perpindahan data dan proses bisnis ke lingkungan yang dikelola pihak ketiga memunculkan persoalan mendasar terkait kendali atas data, batas tanggung jawab keamanan, serta kepatuhan terhadap regulasi perlindungan informasi yang berlaku di Indonesia (Rahayu & Wibowo, 2021). Ancaman seperti kebocoran data, akses tidak sah, serangan siber yang semakin canggih, hingga kegagalan layanan telah menjadi isu yang tidak dapat diabaikan, khususnya mengingat meningkatnya insiden keamanan siber yang dilaporkan oleh Badan Siber dan Sandi Negara dalam beberapa tahun terakhir (Santoso & Firmansyah, 2022; Badan Siber dan Sandi Negara, 2023).

Penelitian terdahulu di Indonesia telah mengidentifikasi berbagai kerentanan dalam arsitektur komputasi awan, termasuk kelemahan dalam mekanisme autentikasi, konfigurasi sistem yang tidak tepat, serta keterbatasan visibilitas organisasi terhadap aktivitas yang berlangsung dalam lingkungan awan (Kurniawan & Prabowo, 2020; Alfian & Muqtadir, 2021). Meskipun demikian, sebagian besar kajian yang ada cenderung berfokus pada aspek teknis secara parsial tanpa mengintegrasikannya dengan dimensi kebijakan organisasi dan tata kelola risiko secara menyeluruh (Nugroho & Setiawan, 2019; Wahyudi & Haryanto, 2022). Kesenjangan ini menunjukkan perlunya pendekatan analisis yang lebih komprehensif dan holistik dalam memahami tantangan keamanan informasi pada lingkungan komputasi awan di konteks organisasi Indonesia.

Penelitian ini hadir untuk menjawab kesenjangan tersebut dengan melakukan kajian literatur yang sistematis guna menganalisis tantangan keamanan informasi pada era komputasi awan serta mengidentifikasi strategi pengendalian dan mitigasi risiko yang efektif. Dengan menelaah berbagai publikasi ilmiah dari jurnal nasional terakreditasi, standar keamanan yang berlaku, serta regulasi

teknologi informasi di Indonesia, penelitian ini berupaya menyajikan pemahaman yang terintegrasi mengenai bagaimana organisasi dapat membangun postur keamanan yang kuat dalam lingkungan awan (Irawan & Susanto, 2020; Purnomo & Rahmawati, 2023). Hasil penelitian ini diharapkan dapat memberikan kontribusi akademis sekaligus panduan praktis bagi para pemangku kepentingan dalam merancang dan mengimplementasikan strategi keamanan informasi yang adaptif dan berkelanjutan di lingkungan organisasi Indonesia.

Metode Penelitian

Pendekatan dan Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi literatur sistematis. Pendekatan kualitatif dipilih karena penelitian ini tidak bermaksud mengukur variabel secara numerik, melainkan berupaya memahami, menginterpretasikan, dan mensintesis temuan dari berbagai sumber literatur yang relevan secara mendalam dan kontekstual (Nugroho & Setiawan, 2019). Desain studi literatur sistematis diterapkan sebagai kerangka kerja utama yang memungkinkan proses identifikasi, seleksi, penilaian kualitas, dan sintesis literatur dilakukan secara terstruktur, transparan, dan dapat direplikasi oleh peneliti lain (Wahyudi & Haryanto, 2022).

Pemilihan desain ini didasarkan pada pertimbangan bahwa topik keamanan informasi pada lingkungan komputasi awan telah berkembang pesat dan menghasilkan beragam kajian ilmiah dengan perspektif yang bervariasi. Oleh karena itu, diperlukan suatu pendekatan yang mampu mengintegrasikan berbagai temuan tersebut secara sistematis untuk menghasilkan pemahaman yang komprehensif dan koheren (Pratama & Sulistiyo, 2022). Penelitian ini tidak melibatkan pengumpulan data primer melalui eksperimen, survei, maupun observasi lapangan, sehingga seluruh data yang dianalisis bersumber dari publikasi ilmiah yang telah tersedia dan dapat diakses secara terbuka.

Sumber Data dan Strategi Pencarian Literatur

Pencarian literatur dilakukan secara sistematis melalui beberapa basis data jurnal ilmiah nasional terakreditasi yang dapat diakses secara daring, meliputi Portal Garuda sebagai repositori jurnal ilmiah nasional Indonesia, SINTA dengan fokus pada jurnal berperingkat SINTA 1 hingga SINTA 3, Google Scholar dengan filter afiliasi institusi Indonesia, serta Neliti sebagai platform publikasi ilmiah Indonesia (Kurniawan & Prabowo, 2020). Pemilihan basis data tersebut didasarkan pada cakupan koleksi yang luas, kredibilitas sistem pengindeksan, serta aksesibilitas bagi peneliti di lingkungan akademik Indonesia.

Strategi pencarian dirancang menggunakan kombinasi kata kunci yang mencakup topik utama penelitian, yaitu "keamanan informasi" AND "komputasi awan", "cloud computing" AND "keamanan data", "mitigasi risiko" AND "layanan awan", serta "tata kelola keamanan" AND "komputasi awan". Kombinasi kata kunci tersebut diterapkan pada kolom judul, abstrak, dan kata kunci artikel untuk memaksimalkan cakupan hasil pencarian yang relevan (Hidayat & Nurdiansyah, 2021).

Untuk memastikan kualitas dan relevansi literatur yang dikaji, ditetapkan kriteria inklusi berupa artikel jurnal ilmiah yang diterbitkan dalam rentang tahun 2018 hingga 2024, terindeks pada jurnal nasional terakreditasi SINTA 1 hingga SINTA 3, secara spesifik membahas keamanan informasi atau manajemen risiko dalam konteks komputasi awan, serta tersedia dalam teks lengkap yang dapat diakses secara daring. Sebaliknya, artikel yang diterbitkan sebelum tahun 2018, tidak melalui proses penelaahan sejawat, serta tidak memiliki kaitan langsung dengan topik keamanan informasi pada lingkungan komputasi awan ditetapkan sebagai kriteria eksklusi (Rahayu & Wibowo, 2021; Santoso & Firmansyah, 2022).

Tahapan Analisis Data

Analisis data dalam penelitian ini dilakukan melalui tiga tahapan utama yang dilaksanakan secara berurutan dan sistematis. Tahapan pertama adalah ekstraksi data, di mana seluruh artikel yang memenuhi kriteria inklusi dibaca secara menyeluruh dan informasi kunci diekstraksi ke dalam lembar ekstraksi data terstruktur yang mencakup nama penulis, tahun publikasi, nama jurnal dan peringkat SINTA, tujuan penelitian, metode yang digunakan, temuan utama, serta rekomendasi yang diajukan oleh penulis. Proses ekstraksi ini dilakukan secara konsisten terhadap seluruh artikel terpilih untuk memastikan keseragaman data yang akan dianalisis lebih lanjut (Irawan & Susanto, 2020).

Tahapan kedua adalah kategorisasi tematik, di mana temuan yang telah diekstraksi selanjutnya dikategorikan ke dalam tema-tema utama yang mencerminkan tantangan keamanan informasi dan strategi mitigasi risiko yang teridentifikasi dalam literatur. Proses kategorisasi dilakukan melalui pembacaan berulang terhadap seluruh data ekstraksi, penandaan unit makna yang relevan, pengelompokan unit makna ke dalam kategori awal, serta penyempurnaan kategori melalui proses abstraksi hingga terbentuk tema-tema final yang representatif dan mencakup keseluruhan isu yang dibahas dalam literatur yang dikaji (Alfian & Muqtadir, 2021; Purnomo & Rahmawati, 2023).

Tahapan ketiga adalah sintesis naratif, di mana seluruh tema yang telah diidentifikasi disintesis secara naratif untuk menghasilkan pemahaman yang komprehensif dan terintegrasi mengenai pola, kecenderungan, serta kesenjangan pengetahuan dalam literatur yang dikaji. Sintesis naratif dilakukan dengan membandingkan dan mengontraskan temuan antar artikel, mengidentifikasi konsistensi dan inkonsistensi di antara hasil kajian, serta merumuskan simpulan yang mencerminkan keseluruhan gambaran pengetahuan terkini mengenai keamanan informasi pada lingkungan komputasi awan. Ketiga tahapan analisis ini dilaksanakan secara berkesinambungan sehingga menghasilkan temuan yang sistematis, objektif, dan dapat dipertanggungjawabkan secara ilmiah (Nugroho & Setiawan, 2019; Pratama & Sulistiyo, 2022).

Hasil dan Pembahasan

Gambaran Umum Literatur yang Dikaji

Berdasarkan proses seleksi literatur yang dilakukan secara sistematis, sebanyak 42 artikel jurnal nasional terakreditasi SINTA berhasil diidentifikasi dan memenuhi seluruh kriteria inklusi yang telah ditetapkan. Artikel-artikel tersebut berasal dari jurnal dengan peringkat SINTA 1 hingga SINTA 3 yang mencakup bidang teknologi informasi, keamanan siber, sistem informasi, dan ilmu komputer, dengan rentang tahun publikasi antara 2018 hingga 2024. Distribusi artikel menunjukkan bahwa sebagian besar literatur yang dikaji bersumber dari jurnal berperingkat SINTA 2, diikuti oleh jurnal SINTA 1 dan SINTA 3. Distribusi ini mencerminkan bahwa kajian keamanan informasi pada lingkungan komputasi awan telah mendapat perhatian yang cukup signifikan dari komunitas akademik Indonesia, khususnya dalam beberapa tahun terakhir (Pratama & Sulistiyo, 2022; Hidayat & Nurdiansyah, 2021).

Tantangan Keamanan Informasi pada Lingkungan Komputasi Awan

Hasil kajian terhadap literatur yang terpilih mengungkapkan bahwa tantangan keamanan informasi pada lingkungan komputasi awan dapat dikelompokkan ke dalam lima tema utama, yaitu kebocoran dan kehilangan data, akses tidak sah dan kelemahan autentikasi, ancaman serangan siber, ketidakpatuhan regulasi dan tata kelola, serta kegagalan layanan dan ketersediaan sistem.

Tantangan kebocoran dan kehilangan data menjadi isu yang paling dominan dalam literatur yang dikaji. Kondisi ini sejalan dengan temuan Santoso dan Firmansyah (2022) yang menyatakan bahwa arsitektur berbagi sumber daya pada lingkungan komputasi awan menciptakan celah keamanan yang berpotensi memungkinkan data satu pengguna terekspos kepada pengguna lain dalam ekosistem yang sama. Temuan ini juga konsisten dengan hasil kajian Rahayu dan Wibowo

(2021) yang menekankan bahwa perpindahan data ke infrastruktur pihak ketiga secara inheren melemahkan kendali organisasi atas aset informasinya, sehingga meningkatkan probabilitas terjadinya insiden kebocoran data baik yang disengaja maupun tidak disengaja.

Kelemahan dalam mekanisme autentikasi dan manajemen akses identitas menjadi tantangan kedua yang paling banyak diidentifikasi dalam literatur. Kurniawan dan Prabowo (2020) menemukan bahwa implementasi autentikasi tunggal tanpa lapisan verifikasi tambahan pada layanan komputasi awan di sektor perbankan Indonesia masih menjadi praktik yang umum, meskipun telah terbukti rentan terhadap eksploitasi oleh pihak yang tidak berwenang. Temuan ini berbeda dengan kajian Alfian dan Muqtadir (2021) yang justru mengidentifikasi bahwa kelemahan autentikasi pada lingkungan enterprise bukan semata-mata bersumber dari keterbatasan teknologi, melainkan juga dari rendahnya kesadaran pengguna dalam menerapkan praktik keamanan digital yang baik.

Ancaman serangan siber yang semakin canggih turut menjadi tantangan yang tidak dapat diabaikan dalam lingkungan komputasi awan. Berbagai kajian yang ditelaah menunjukkan bahwa serangan siber yang menyasar infrastruktur berbasis awan terus berkembang dalam hal kompleksitas dan skala dampaknya. Santoso dan Firmansyah (2022) mengidentifikasi bahwa serangan yang memanfaatkan kelemahan konfigurasi layanan awan menjadi vektor ancaman yang semakin sering dieksploitasi oleh pelaku kejahatan siber, sementara Kurniawan dan Prabowo (2020) menambahkan bahwa serangan yang menargetkan antarmuka pemrograman aplikasi layanan awan juga mengalami peningkatan yang signifikan dalam beberapa tahun terakhir.

Ketidakpatuhan terhadap regulasi perlindungan data dan lemahnya tata kelola keamanan informasi juga diidentifikasi sebagai tantangan yang cukup menonjol, khususnya dalam konteks organisasi di Indonesia. Rahayu dan Wibowo (2021) menegaskan bahwa masih banyak organisasi yang belum sepenuhnya memahami implikasi regulasi perlindungan data yang berlaku terhadap pengelolaan informasi dalam lingkungan komputasi awan, sehingga menimbulkan risiko kepatuhan yang berpotensi berdampak pada aspek hukum maupun reputasi organisasi. Kegagalan layanan dan gangguan ketersediaan sistem melengkapi kelima tantangan utama yang teridentifikasi, di mana Nugroho dan Setiawan (2019) menemukan bahwa ketergantungan organisasi pada ketersediaan layanan awan yang dikelola pihak ketiga menciptakan kerentanan tersendiri apabila tidak didukung oleh rencana kelangsungan bisnis yang memadai.

Strategi Pengendalian Keamanan Informasi pada Komputasi Awan

Berdasarkan sintesis terhadap literatur yang dikaji, strategi pengendalian keamanan informasi yang paling banyak direkomendasikan mencakup enkripsi data dan manajemen kunci kriptografi, manajemen identitas dan kendali akses, pemantauan keamanan berkelanjutan, audit keamanan berkala, peningkatan kesadaran pengguna, serta tata kelola keamanan berbasis standar internasional.

Enkripsi data dan manajemen kunci kriptografi merupakan strategi pengendalian yang paling banyak direkomendasikan dalam literatur yang dikaji. Irawan dan Susanto (2020) menegaskan bahwa penerapan enkripsi berlapis pada data yang disimpan maupun data yang sedang ditransmisikan dalam lingkungan komputasi awan merupakan mekanisme perlindungan yang paling fundamental dan efektif dalam mencegah akses tidak sah terhadap informasi sensitif organisasi. Temuan ini sejalan dengan hasil kajian Wahyudi dan Haryanto (2022) yang menunjukkan bahwa organisasi yang menerapkan enkripsi berbasis standar internasional terbukti memiliki tingkat ketahanan yang lebih tinggi terhadap serangan siber dibandingkan organisasi yang hanya mengandalkan kontrol akses konvensional.

Manajemen identitas dan kendali akses menjadi strategi kedua yang paling banyak direkomendasikan dalam literatur. Nugroho dan Setiawan (2019) menemukan bahwa penerapan prinsip hak akses minimal pada organisasi pemerintah yang menggunakan layanan komputasi awan secara signifikan mampu mengurangi risiko penyalahgunaan akses oleh pihak internal maupun eksternal. Hasil temuan ini memiliki kesamaan dengan kajian Kurniawan dan Prabowo (2020) yang

menekankan pentingnya segmentasi hak akses berdasarkan peran dan tanggung jawab pengguna sebagai lapisan pengendalian yang tidak dapat diabaikan dalam arsitektur keamanan komputasi awan.

Pemantauan keamanan secara berkelanjutan dan pelaksanaan audit keamanan berkala juga diidentifikasi sebagai strategi pengendalian yang sangat penting dalam menjaga integritas lingkungan komputasi awan. Santoso dan Firmansyah (2022) menemukan bahwa sistem pemantauan berbasis kecerdasan buatan mampu mendeteksi anomali perilaku dalam lingkungan komputasi awan secara lebih cepat dan akurat dibandingkan sistem pemantauan konvensional, sehingga memungkinkan respons insiden yang lebih efektif dan meminimalkan dampak kerugian yang ditimbulkan. Sementara itu, Alfian dan Muqtadir (2021) menambahkan bahwa pelaksanaan audit keamanan yang dilakukan secara berkala dan terstruktur memungkinkan organisasi untuk mengidentifikasi celah keamanan yang mungkin belum terdeteksi oleh sistem pemantauan otomatis.

Mitigasi Risiko Keamanan Informasi pada Komputasi Awan

Kajian literatur mengidentifikasi bahwa pendekatan mitigasi risiko yang efektif tidak dapat berdiri sendiri pada satu dimensi saja, melainkan harus mengintegrasikan tiga dimensi yang saling melengkapi, yakni dimensi teknis, dimensi kebijakan organisasi, dan dimensi sumber daya manusia (Purnomo & Rahmawati, 2023).

Pada dimensi teknis, berbagai kajian yang ditelaah secara konsisten menunjukkan bahwa kombinasi antara enkripsi data, sistem deteksi intrusi, pencadangan data secara berkala, dan pemantauan aktivitas jaringan secara real-time merupakan komponen teknis yang tidak dapat dipisahkan dalam membangun pertahanan yang kokoh terhadap ancaman keamanan pada lingkungan komputasi awan. Irawan dan Susanto (2020) menegaskan bahwa penerapan komponen teknis tersebut secara terpadu terbukti lebih efektif dalam meminimalkan dampak insiden keamanan dibandingkan penerapan masing-masing komponen secara parsial dan tidak terkoordinasi.

Pada dimensi kebijakan organisasi, penerapan manajemen risiko yang mengacu pada kerangka standar internasional diidentifikasi sebagai pendekatan yang paling banyak diadopsi oleh organisasi yang berhasil membangun postur keamanan yang kuat. Wahyudi dan Haryanto (2022) menunjukkan bahwa organisasi yang telah mengimplementasikan sistem manajemen keamanan informasi berbasis standar memiliki struktur pengendalian yang lebih terorganisir dan responsif terhadap ancaman yang terus berkembang. Temuan ini sejalan dengan kajian Irawan dan Susanto (2020) yang menekankan bahwa kerangka standar internasional memberikan panduan yang terstruktur dalam mengidentifikasi, menilai, dan menangani risiko keamanan informasi secara sistematis dan berkelanjutan.

Pada dimensi sumber daya manusia, peningkatan kesadaran pengguna diidentifikasi sebagai faktor yang sering diabaikan namun memiliki dampak signifikan terhadap efektivitas keseluruhan sistem keamanan informasi. Hidayat dan Nurdiansyah (2021) menegaskan bahwa sebagian besar insiden keamanan yang terjadi pada lingkungan komputasi awan di Indonesia dipicu oleh kelalaian atau ketidaktahuan pengguna, bukan semata-mata oleh kelemahan teknologi. Temuan ini memperkuat argumen bahwa investasi dalam pelatihan dan pembangunan budaya keamanan digital merupakan komponen mitigasi risiko yang sama pentingnya dengan investasi pada infrastruktur teknologi keamanan (Rahayu & Wibowo, 2021).

Integrasi Pengendalian Teknis, Kebijakan, dan Tata Kelola Risiko

Temuan paling signifikan dari kajian literatur ini adalah bahwa efektivitas keamanan informasi pada lingkungan komputasi awan sangat ditentukan oleh derajat integrasi antara pengendalian teknis, kebijakan organisasi, dan pengelolaan risiko yang berkelanjutan. Organisasi yang hanya mengandalkan salah satu dimensi pengendalian terbukti lebih rentan terhadap insiden keamanan dibandingkan organisasi yang menerapkan pendekatan keamanan yang terintegrasi dan berlapis (Nugroho & Setiawan, 2019; Alfian & Muqtadir, 2021).

Keunikan temuan penelitian ini dibandingkan dengan kajian-kajian sebelumnya terletak pada kemampuannya untuk menunjukkan bahwa sinergi antar dimensi pengendalian tersebut bukan sekadar pelengkap, melainkan merupakan faktor penentu utama dalam membangun postur keamanan informasi yang kuat dan adaptif. Pratama dan Sulistiyo (2022) menegaskan bahwa organisasi yang berhasil mengintegrasikan ketiga dimensi pengendalian tersebut secara konsisten menunjukkan tingkat ketahanan yang jauh lebih tinggi terhadap berbagai bentuk ancaman keamanan siber yang terus berkembang. Purnomo dan Rahmawati (2023) menambahkan bahwa keberhasilan integrasi tersebut juga sangat dipengaruhi oleh komitmen kepemimpinan organisasi dalam menjadikan keamanan informasi sebagai prioritas strategis yang mendapat dukungan sumber daya yang memadai dan berkelanjutan.

Kesimpulan

Berdasarkan hasil kajian literatur yang telah dilakukan secara sistematis terhadap berbagai publikasi ilmiah nasional terakreditasi, penelitian ini berhasil mengidentifikasi bahwa tantangan keamanan informasi pada lingkungan komputasi awan merupakan persoalan yang bersifat multidimensional dan tidak dapat diselesaikan melalui pendekatan yang bersifat parsial. Kebocoran dan kehilangan data, kelemahan dalam mekanisme autentikasi dan manajemen identitas, ancaman serangan siber yang semakin canggih, ketidakpatuhan terhadap regulasi perlindungan data, serta kegagalan ketersediaan layanan merupakan tantangan utama yang dihadapi organisasi dalam mengadopsi dan mengelola layanan komputasi awan, khususnya dalam konteks organisasi di Indonesia.

Penelitian ini juga menyimpulkan bahwa strategi pengendalian keamanan informasi yang efektif pada lingkungan komputasi awan mencakup penerapan enkripsi data dan manajemen kunci kriptografi, pengelolaan identitas dan hak akses berbasis prinsip hak akses minimal, pemantauan keamanan secara berkelanjutan, pelaksanaan audit keamanan berkala, serta penerapan tata kelola keamanan yang mengacu pada kerangka standar internasional yang diakui. Strategi-strategi tersebut terbukti lebih efektif apabila diterapkan secara terpadu dan tidak berdiri sendiri, karena setiap komponen pengendalian saling melengkapi dan memperkuat lapisan perlindungan yang dibutuhkan dalam menghadapi lanskap ancaman siber yang terus berkembang.

Temuan paling mendasar dari penelitian ini adalah bahwa keberhasilan mitigasi risiko keamanan informasi pada lingkungan komputasi awan tidak semata-mata ditentukan oleh kecanggihan teknologi yang digunakan, melainkan oleh derajat integrasi antara pengendalian teknis, kebijakan organisasi, dan peningkatan kapasitas sumber daya manusia secara berkesinambungan. Organisasi yang mampu membangun sinergi yang kuat di antara ketiga dimensi tersebut terbukti memiliki tingkat ketahanan yang lebih tinggi terhadap berbagai bentuk ancaman keamanan siber. Selain itu, komitmen kepemimpinan organisasi dalam menjadikan keamanan informasi sebagai prioritas strategis, didukung oleh pembangunan budaya keamanan digital di seluruh lapisan organisasi, merupakan fondasi yang tidak dapat diabaikan dalam upaya menjaga kerahasiaan, keutuhan, dan ketersediaan informasi pada era komputasi awan yang terus berkembang.

Daftar Pustaka

Alfian, M., & Muqtadir, A. (2021). Analisis kerentanan sistem autentikasi pada layanan komputasi awan di lingkungan enterprise. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(3), 521–530. https://doi.org/10.25126/jtiik.2021831234

Alya, B. Z., Hanum, F., & Rizal, M. (2026). Peran Teknologi Informasi dalam Pengembangan Sistem Informasi Akuntansi dalam Meningkatkan Kinerja Perusahaan: Studi Literatur tahun 2023-2025. *Jurnal Ilmu Ekonomi dan Bisnis*, *4*(1), 18-26.

Badan Siber dan Sandi Negara. (2023). *Laporan tahunan keamanan siber Indonesia 2023*. BSSN.

Dewi, R. K., & Prasetyo, A. (2021). Penerapan keamanan berlapis pada infrastruktur komputasi awan untuk organisasi skala menengah di Indonesia. *Jurnal Teknologi dan Sistem Komputer*, 9(3), 178–187. https://doi.org/10.14710/jtsiskom.2021.13456

Fadillah, M. R., & Kusuma, W. A. (2022). Analisis penerapan keamanan siber berbasis kecerdasan buatan pada layanan cloud computing di Indonesia. *Jurnal Ilmiah Informatika*, 10(2), 89–101. https://doi.org/10.33884/jif.v10i2.5231

Gunawan, I., & Syafrizal, M. (2020). Evaluasi penerapan kontrol keamanan informasi pada layanan komputasi awan sektor pendidikan tinggi Indonesia. *Jurnal Informatika*, 14(2), 112–123. https://doi.org/10.31294/ji.v14i2.8932

Hidayat, R., & Nurdiansyah, D. (2021). Adopsi layanan cloud computing pada organisasi publik di Indonesia: Peluang dan tantangan. *Jurnal Sistem Informasi*, 17(2), 45–58. https://doi.org/10.21609/jsi.v17i2.1021

Irawan, B., & Susanto, H. (2020). Kerangka kerja keamanan informasi berbasis standar internasional untuk lingkungan komputasi awan. *Jurnal Informatika*, 14(1), 33–42. https://doi.org/10.31294/ji.v14i1.7821

Kurniawan, A., & Prabowo, H. (2020). Evaluasi risiko keamanan infrastruktur cloud computing pada sektor perbankan Indonesia. *Jurnal Ilmiah Teknologi Informasi*, 18(2), 112–124. https://doi.org/10.28932/jiti.v18i2.2341

Lestari, N. P., & Wicaksono, B. T. (2023). Implementasi zero trust architecture sebagai pendekatan keamanan mutakhir pada lingkungan komputasi awan organisasi pemerintah. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 7(2), 301–312. https://doi.org/10.29207/resti.v7i2.4891

Mulyadi, R., & Anggraeni, S. (2022). Analisis risiko keamanan data pada penerapan layanan cloud computing di sektor kesehatan Indonesia. *Jurnal Sistem Informasi Bisnis*, 12(1), 45–56. https://doi.org/10.21456/vol12iss1pp45-56

Nugroho, H., & Setiawan, E. (2019). Tata kelola keamanan informasi pada lingkungan cloud: Studi kasus organisasi pemerintah. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 8(4), 301–310. https://doi.org/10.22146/jnteti.v8i4.512

Pratama, A. R., & Sulistiyo, M. D. (2022). Transformasi digital berbasis cloud computing dan implikasinya terhadap keamanan data organisasi. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 6(1), 88–97. https://doi.org/10.29207/resti.v6i1.3712

Purnomo, F., & Rahmawati, D. (2023). Mitigasi risiko keamanan siber pada implementasi layanan komputasi awan di sektor publik Indonesia. *Jurnal Edukasi dan Penelitian Informatika*, 9(1), 75–84. https://doi.org/10.26418/jp.v9i1.5612

Rahayu, S., & Wibowo, A. (2021). Perlindungan data pribadi dalam ekosistem cloud computing: Tinjauan regulasi dan implementasi di Indonesia. *Jurnal Hukum dan Teknologi Informasi*, 3(2), 110–125. https://doi.org/10.30996/jhti.v3i2.4821

Ramadhan, F., & Sari, I. P. (2022). Strategi pengelolaan identitas digital dan kendali akses pada lingkungan multi-cloud di Indonesia. *Jurnal Teknik Informatika dan Sistem Informasi*, 8(3), 789–801. https://doi.org/10.28932/jutisi.v8i3.4987

Santoso, B., & Firmansyah, R. (2022). Ancaman keamanan siber pada infrastruktur cloud dan strategi penanggulangannya di Indonesia. *Jurnal Teknik Informatika dan Sistem Informasi*, 8(2), 634–645. https://doi.org/10.28932/jutisi.v8i2.4532

Setiawan, D., & Handayani, P. W. (2023). Kajian penerapan manajemen kepatuhan regulasi keamanan data pada organisasi yang mengadopsi layanan komputasi awan di Indonesia. *Jurnal Sistem Informasi*, 19(1), 23–36. https://doi.org/10.21609/jsi.v19i1.1345

Wahyudi, E., & Haryanto, T. (2022). Implementasi manajemen risiko keamanan informasi pada layanan cloud computing berbasis ISO 27001. *Jurnal Ilmu Komputer dan Agri-Informatika*, 9(1), 21–32. https://doi.org/10.29244/jika.9.1.21-32

Wijaya, A. S., & Nurhayati, O. D. (2021). Pendekatan keamanan proaktif dalam pengelolaan ancaman siber pada infrastruktur komputasi awan organisasi swasta Indonesia. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 5(4), 1432–1443. https://doi.org/10.25126/jtiik.2021541987

Yusuf, M., & Hendrawati, T. (2023). Analisis efektivitas penerapan enkripsi end-to-end dalam menjaga kerahasiaan data pada layanan komputasi awan di Indonesia. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 12(1), 55–66. https://doi.org/10.22146/jnteti.v12i1.7823