Infinity Engineering Journal
Vol. 2 No. 1, Feb (2026), pp. 36-44

ISSN 3090-5621 (online)
Published by Yayasan Cinta Negara Indonesia

Pendekatan Keamanan Cloud Computing Berbasis Zero Trust dan Enkripsi: Tinjauan Sistematis Literatur Lima Tahun Terakhir

Nadia Amelia[1], Dafa Setiawan[2], Rais Affaruq Zunnurain[3]
[1,2] Fakultas Teknologi dan Bisnis, Program Studi Teknologi Informasi
[3] Fakultas Teknologi dan Bisnis, Program Studi Bisnis Digital
Universitas Putra Abadi Langkat

A R T I C L E I N F O

Article history:
Received: Jan 02, 2026
Revised: Jan 12, 2026
Accepted: Jan 22, 2026

Keywords:
Cloud Computing
Enkripsi
Keamanan Cloud
Systematic Literature Review
Zero Trust

ABSTRAK

Perkembangan cloud computing yang pesat telah mendorong peningkatan pemanfaatan teknologi ini di berbagai sektor, namun di sisi lain juga memunculkan risiko keamanan data dan ancaman siber yang semakin kompleks. Model keamanan tradisional berbasis perimeter dinilai tidak lagi memadai untuk melindungi lingkungan cloud yang bersifat dinamis, terdistribusi, dan terbuka. Oleh karena itu, pendekatan Zero Trust dan enkripsi berkembang sebagai strategi keamanan yang lebih adaptif dan komprehensif. Penelitian ini bertujuan untuk mengkaji secara sistematis perkembangan penelitian terkait penerapan Zero Trust dan enkripsi dalam keamanan cloud computing selama lima tahun terakhir. Metode yang digunakan adalah Systematic Literature Review (SLR) dengan menganalisis artikel ilmiah dari basis data bereputasi seperti IEEE, Scopus, ScienceDirect, dan Springer. Hasil kajian menunjukkan bahwa Zero Trust efektif dalam memperkuat kontrol akses dan autentikasi berkelanjutan, sementara enkripsi berperan penting dalam menjaga kerahasiaan dan integritas data pada berbagai kondisi penggunaan. Namun demikian, implementasi kedua pendekatan ini masih menghadapi tantangan berupa kompleksitas teknis, biaya, serta dampak terhadap performa sistem. Penelitian ini menyimpulkan bahwa integrasi Zero Trust dan enkripsi memiliki potensi besar dalam meningkatkan keamanan cloud computing, sekaligus membuka peluang penelitian lanjutan terkait pengembangan model keamanan terintegrasi yang lebih efisien dan adaptif.

Corresponding Author:
Nadia Amelia
Fakultas Teknologi Dan Bisnis, Program Studi Teknologi Informasi
Universitas Putra Abadi Langkat
Jl. Letjen R. Soeprapto No.10, Sumatera Utara 20814. Indonesia
Email: nadiaamelia28016@gmail.com

1. PENDAHULUAN

Cloud computing telah menjadi fondasi teknologi informasi modern karena menawarkan skala layanan yang fleksibel, efisiensi biaya, dan kemampuan akses data kapan saja dan dari mana saja (Satrinia, Yutia, & Matin, 2024). Implementasi layanan komputasi awan kini meluas ke berbagai sektor industri, seperti kesehatan, keuangan, pendidikan, dan pemerintahan, sebagai bagian dari transformasi digital global yang menghadirkan produktivitas dan efisiensi operasional (Alkadrie & Fitroh, 2024).

Namun, seiring meningkatnya adopsi cloud computing, risiko atas keamanan data dan ancaman siber juga meningkat secara signifikan. Lingkungan cloud cenderung menyimpan data pengguna dan aplikasi di infrastruktur milik pihak ketiga dengan model multi-tenant, yang membuka ruang serangan baru seperti pelanggaran data, akses tidak sah, kehilangan data, dan serangan siber terkoordinasi (Desi Alexander, 2025).

Model keamanan tradisional berbasis perimeter atau perimeter-based security sudah tidak lagi cukup efektif dalam konteks cloud computing yang dinamis. Metode ini mengandalkan lapisan pertahanan di sekitar jaringan internal yang kini mudah dilampaui oleh ancaman berbasis identitas

pengguna, cloud services, dan API yang terus berubah. Hal ini menimbulkan kebutuhan akan model keamanan yang lebih adaptif dan responsif terhadap ancaman tanpa batasan wilayah jaringan tradisional.

Dalam konteks ini, pendekatan Zero Trust muncul sebagai paradigma keamanan yang menekankan prinsip never trust, always verify, yaitu tidak mempercayai entitas mana pun —baik di dalam maupun di luar jaringan— tanpa verifikasi autentikasi dan otorisasi yang konsisten (Ahmadi, 2024). Zero Trust memfokuskan pada kontrol akses kontekstual, segmentasi mikro, dan autentikasi terus menerus untuk meminimalkan risiko intrusi, terutama pada layanan cloud yang terdistribusi dan dinamis.

Selain itu, teknik enkripsi merupakan bagian penting dari strategi keamanan data cloud. Enkripsi secara signifikan meningkatkan kerahasiaan data baik dalam penyimpanan (data at rest) maupun ketika berpindah antar sistem (data in transit), sehingga hanya pengguna yang terautentikasi yang dapat membaca atau memproses informasi sensitif tersebut (Purba Lia et al., 2025).

Karena perkembangan ancaman siber dan teknologi keamanan terus cepat berubah, kajian yang sistematis terhadap penelitian terdahulu atas penerapan Zero Trust dan enkripsi dalam cloud computing sangat diperlukan. Tinjauan sistematis literatur dalam lima tahun terakhir dapat memberikan gambaran tren, praktik terbaik, tantangan, serta gap penelitian yang bisa dijadikan arah studi lanjutan.

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah: Bagaimana perkembangan pendekatan Zero Trust dalam keamanan cloud computing selama lima tahun terakhir? Bagaimana peran dan jenis enkripsi yang digunakan dalam pengamanan cloud computing? Apa kelebihan dan tantangan penerapan Zero Trust dan enkripsi pada lingkungan cloud? Apa celah penelitian (research gap) yang masih terbuka untuk studi lanjutan?

Sejalan dengan rumusan masalah, penelitian ini memiliki tujuan sebagai berikut:1. Menganalisis tren penelitian keamanan cloud berbasis Zero Trust dalam lima tahun terakhir. 2. Mengidentifikasi penerapan dan efektivitas teknik enkripsi dalam pengamanan cloud computing. 3. Mengevaluasi kelebihan dan tantangan dari pendekatan Zero Trust dan enkripsi. 4. Menyusun rekomendasi dan arah penelitian selanjutnya berdasarkan gap yang ditemukan.

Penelitian ini diharapkan dapat memperkaya kajian akademik tentang keamanan cloud computing, khususnya dengan fokus pada Zero Trust dan enkripsi, serta menjadi rujukan bagi peneliti dan akademisi lainnya yang tertarik mendalami topik ini. Secara praktis, hasil penelitian ini diharapkan membantu praktisi TI, arsitek keamanan informasi, dan organisasi dalam memahami karakteristik, kelebihan, dan keterbatasan dari pendekatan Zero Trust dan teknik enkripsi untuk merumuskan strategi keamanan cloud yang lebih efektif dan adaptif.

2. METODE

2.1. Jenis Penelitian

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR), yaitu metode penelitian yang bertujuan untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil-hasil penelitian terdahulu secara sistematis dan terstruktur berdasarkan pertanyaan penelitian yang telah dirumuskan. Pendekatan SLR dipilih karena mampu memberikan gambaran komprehensif mengenai perkembangan penelitian, tren, serta celah penelitian terkait keamanan cloud computing berbasis Zero Trust dan enkripsi dalam lima tahun terakhir. SLR memungkinkan peneliti untuk melakukan kajian literatur secara objektif dan transparan melalui tahapan yang terdokumentasi dengan baik, sehingga hasil sintesis yang diperoleh dapat dipertanggungjawabkan secara akademik. Metode ini juga banyak digunakan dalam penelitian di bidang teknologi informasi dan keamanan siber untuk memetakan perkembangan pendekatan dan teknologi yang terus berubah secara cepat (Kitchenham et al., 2020; Page et al., 2021).

2.2. Tahapan Systematic Literature Review

Pelaksanaan Systematic Literature Review dalam penelitian ini dilakukan melalui beberapa tahapan utama yang disusun secara sistematis sebagai berikut:

2.2.1. Perumusan Pertanyaan Penelitian

Tahap awal SLR dimulai dengan perumusan pertanyaan penelitian yang jelas dan terfokus. Pertanyaan penelitian disusun untuk mengarahkan proses pencarian dan seleksi literatur,

khususnya yang berkaitan dengan penerapan pendekatan Zero Trust dan teknik enkripsi dalam keamanan cloud computing. Perumusan pertanyaan penelitian yang tepat berperan penting dalam menentukan relevansi dan kualitas literatur yang dikaji (Kitchenham et al., 2020).

2.2.2. Strategi Pencarian Literatur

Pada tahap ini, dilakukan penyusunan strategi pencarian literatur dengan menentukan kata kunci utama dan kombinasi istilah yang relevan dengan topik penelitian. Strategi pencarian dirancang untuk memperoleh artikel yang komprehensif dan relevan, serta meminimalkan risiko terlewatnya penelitian penting yang sesuai dengan fokus kajian (Snyder, 2019).

2.2.3. Penentuan Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi ditetapkan untuk menyaring literatur yang sesuai dengan tujuan penelitian. Tahapan ini bertujuan untuk memastikan bahwa hanya artikel yang relevan, berkualitas, dan sesuai dengan ruang lingkup penelitian yang dianalisis lebih lanjut (Page et al., 2021).

2.2.4. Seleksi dan Penyaringan Artikel

Artikel yang diperoleh dari proses pencarian kemudian diseleksi melalui beberapa tahap, yaitu pemeriksaan judul, abstrak, dan teks lengkap. Proses ini dilakukan secara bertahap untuk mengeliminasi artikel yang tidak relevan, duplikat, atau tidak memenuhi kriteria yang telah ditetapkan sebelumnya (Xiao & Watson, 2019).

2.2.5. Analisis dan Sintesis Data

Tahap akhir adalah analisis dan sintesis data dari artikel terpilih. Pada tahap ini, informasi penting seperti pendekatan keamanan yang digunakan, metode enkripsi, kelebihan, tantangan, serta temuan utama diekstraksi dan dianalisis secara kualitatif. Hasil analisis kemudian disintesis untuk menjawab pertanyaan penelitian dan mengidentifikasi pola serta celah penelitian yang masih terbuka (Snyder, 2019).

2.3. Sumber Data dan Strategi Pencarian

Sumber data dalam penelitian ini diperoleh dari berbagai database ilmiah bereputasi, antara lain IEEE Xplore, Scopus, ScienceDirect, dan SpringerLink. Pemilihan database tersebut didasarkan pada reputasi, kelengkapan, serta relevansinya terhadap bidang teknologi informasi dan keamanan siber. Rentang waktu publikasi artikel yang dikaji dibatasi pada lima tahun terakhir, yaitu dari tahun 2020 hingga 2025, dengan tujuan untuk memperoleh hasil penelitian yang mutakhir dan relevan dengan perkembangan terkini dalam keamanan cloud computing. Kata kunci pencarian yang digunakan dalam proses penelusuran literatur antara lain: cloud computing security, Zero Trust Architecture, cloud encryption, data security in cloud, dan Zero Trust and encryption. Kombinasi kata kunci tersebut digunakan dengan bantuan operator Boolean (AND, OR) untuk memperluas dan mempersempit hasil pencarian sesuai kebutuhan penelitian (Kitchenham et al., 2020).

2.4. Kriteria Inklusi dan Eksklusi

Untuk menjaga kualitas dan relevansi literatur yang dianalisis, penelitian ini menetapkan kriteria inklusi dan eksklusi sebagai berikut:

2.4.1. Kriteria Inklusi:

a. Artikel jurnal internasional dan nasional bereputasi.
b. Artikel yang membahas keamanan cloud computing dengan fokus pada Zero Trust, enkripsi, atau keduanya.
c. Artikel yang dipublikasikan dalam rentang waktu lima tahun terakhir (2020–2025).
d. Artikel yang tersedia dalam teks lengkap (full text).

2.4.2. Kriteria Eksklusi:

a. Artikel non-ilmiah seperti opini, blog, white paper, atau laporan tanpa proses peer-review.
b. Artikel yang tidak secara spesifik membahas keamanan cloud computingz
c. Artikel duplikat yang muncul pada lebih dari satu database.

Penerapan kriteria ini bertujuan untuk memastikan bahwa literatur yang dianalisis memiliki kualitas ilmiah yang baik serta relevan dengan tujuan penelitian (Page et al., 2021).

3. HASIL DAN PEMBAHASAN

3.1. Karakteristik Literatur yang Dianalisis

Berdasarkan proses seleksi dan penyaringan literatur yang telah dilakukan melalui pendekatan Systematic Literature Review (SLR), diperoleh sejumlah artikel ilmiah yang memenuhi kriteria inklusi dan relevan dengan topik keamanan cloud computing berbasis Zero Trust dan enkripsi. Karakteristik literatur yang dianalisis dalam penelitian ini mencakup distribusi jumlah artikel per tahun, jenis publikasi, serta fokus utama penelitian yang dibahas dalam masing-masing artikel.

3.1.1. Jumlah Artikel per Tahun

Distribusi jumlah artikel berdasarkan tahun publikasi menunjukkan adanya tren peningkatan penelitian terkait keamanan cloud computing dalam lima tahun terakhir. Pada periode awal (2020–2021), jumlah publikasi masih relatif terbatas dan umumnya berfokus pada penguatan keamanan data cloud secara umum, termasuk isu privasi dan kontrol akses. Namun, mulai tahun 2022 hingga 2024, terjadi peningkatan signifikan jumlah artikel yang secara khusus membahas pendekatan Zero Trust dan integrasi teknik enkripsi dalam lingkungan cloud. Peningkatan jumlah publikasi ini mencerminkan meningkatnya perhatian akademisi dan praktisi terhadap ancaman keamanan siber yang semakin kompleks serta kebutuhan akan model keamanan yang lebih adaptif dibandingkan pendekatan tradisional. Tren tersebut sejalan dengan perkembangan arsitektur cloud yang semakin terdistribusi dan berbasis layanan (service-oriented architecture) (Alkadi et al., 2022; Rose, Borchert, Mitchell, & Connelly, 2020).

3.1.2. Jenis Publikasi

Berdasarkan jenis publikasinya, literatur yang dianalisis didominasi oleh artikel jurnal internasional bereputasi yang diterbitkan pada jurnal bidang teknologi informasi, keamanan siber, dan sistem komputasi awan. Selain itu, beberapa artikel berasal dari prosiding konferensi internasional yang membahas inovasi terbaru terkait arsitektur Zero Trust dan mekanisme enkripsi cloud. Dominasi artikel jurnal menunjukkan bahwa topik keamanan cloud berbasis Zero Trust dan enkripsi telah menjadi fokus penelitian yang matang dan berkelanjutan, bukan sekadar isu teknis jangka pendek. Artikel jurnal umumnya menyajikan analisis yang lebih mendalam, baik dari sisi konseptual maupun implementatif, dibandingkan dengan publikasi non-ilmiah atau laporan teknis (Sarker, 2021).

3.1.3. Fokus Penelitian

Ditinjau dari fokus penelitian, literatur yang dianalisis dapat dikelompokkan ke dalam beberapa tema utama. Pertama, penelitian yang berfokus pada konsep dan arsitektur Zero Trust, termasuk prinsip dasar, model implementasi, serta adaptasinya dalam lingkungan cloud computing. Studi dalam kategori ini menekankan pentingnya verifikasi identitas berkelanjutan dan segmentasi mikro untuk mengurangi risiko akses tidak sah (Kindervag et al., 2021).

Kedua, penelitian yang menitikberatkan pada penerapan teknik enkripsi, baik untuk data yang tersimpan (data at rest), data yang ditransmisikan (data in transit), maupun data yang sedang diproses (data in use). Fokus utama dari penelitian ini adalah peningkatan kerahasiaan dan integritas data cloud melalui algoritma enkripsi yang aman dan efisien (Alasmary et al., 2022).

Ketiga, beberapa penelitian mengombinasikan pendekatan Zero Trust dan enkripsi sebagai strategi keamanan terpadu. Penelitian dalam kelompok ini menyoroti sinergi antara kontrol akses berbasis identitas dan perlindungan data kriptografis untuk menghadapi ancaman keamanan cloud yang semakin kompleks. Namun, masih ditemukan keterbatasan kajian yang membahas evaluasi komprehensif efektivitas integrasi kedua pendekatan tersebut dalam skala besar, sehingga membuka peluang penelitian lanjutan (Zhang et al., 2023).

3.2. Pendekatan Zero Trust dalam Keamanan Cloud Computing

3.2.1. Konsep dan Prinsip Zero Trust

Zero Trust merupakan paradigma keamanan modern yang dikembangkan untuk menjawab keterbatasan model keamanan tradisional berbasis perimeter. Pendekatan ini didasarkan pada prinsip utama never trust, always verify, yang berarti setiap entitas—baik pengguna, perangkat, maupun aplikasi—harus selalu diverifikasi sebelum diberikan akses, tanpa memandang lokasi atau asal koneksi (Rose et al., 2020).

Dalam konteks cloud computing yang bersifat terdistribusi dan dinamis, Zero Trust menekankan beberapa prinsip fundamental, antara lain autentikasi dan otorisasi berkelanjutan,

penerapan hak akses minimum (least privilege access), serta pemantauan aktivitas secara real-time. Prinsip-prinsip ini bertujuan untuk meminimalkan potensi penyalahgunaan akses dan membatasi dampak serangan apabila terjadi pelanggaran keamanan (Kindervag et al., 2021).

Pendekatan Zero Trust juga memanfaatkan identitas sebagai pusat kontrol keamanan, sehingga keputusan akses tidak hanya bergantung pada lokasi jaringan, tetapi juga mempertimbangkan konteks seperti identitas pengguna, kondisi perangkat, dan tingkat sensitivitas data yang diakses. Hal ini menjadikan Zero Trust lebih relevan dibandingkan pendekatan keamanan konvensional dalam lingkungan cloud yang bersifat tanpa batas fisik (Alkadi et al., 2022).

3.2.2. Model Implementasi Zero Trust pada Cloud

Implementasi Zero Trust dalam lingkungan cloud umumnya dilakukan melalui beberapa komponen utama, yaitu identity and access management (IAM), segmentasi mikro (micro-segmentation), kebijakan akses berbasis konteks, serta pemantauan dan analisis aktivitas secara berkelanjutan. Model ini memungkinkan organisasi untuk membatasi akses hanya pada sumber daya yang benar-benar dibutuhkan oleh pengguna atau aplikasi tertentu (Zhang et al., 2023).

Pada arsitektur cloud, Zero Trust sering diintegrasikan dengan layanan keamanan bawaan penyedia cloud, seperti kontrol identitas, manajemen kunci kriptografi, dan kebijakan keamanan berbasis API. Pendekatan ini mendukung pengamanan beban kerja (workloads), aplikasi, serta data yang tersebar di berbagai layanan cloud, baik public cloud, private cloud, maupun hybrid cloud (Sharma & Chen, 2021).

Selain itu, penerapan Zero Trust pada cloud juga melibatkan proses evaluasi risiko secara dinamis. Setiap permintaan akses dievaluasi berdasarkan kebijakan keamanan yang telah ditetapkan, sehingga akses dapat dibatasi atau dihentikan secara otomatis apabila terdeteksi perilaku mencurigakan. Model ini memberikan fleksibilitas dan ketahanan keamanan yang lebih tinggi dibandingkan sistem statis berbasis perimeter (NIST, 2020).

3.2.3. Manfaat Zero Trust dalam Mengurangi Risiko Keamanan

Penerapan pendekatan Zero Trust dalam cloud computing memberikan berbagai manfaat signifikan dalam mengurangi risiko keamanan. Salah satu manfaat utama adalah kemampuan untuk meminimalkan risiko akses tidak sah melalui mekanisme verifikasi berlapis dan kontrol akses berbasis identitas. Dengan demikian, potensi penyalahgunaan kredensial dan serangan berbasis identitas dapat ditekan secara efektif (Kindervag et al., 2021).

Selain itu, Zero Trust mampu mengurangi dampak serangan siber dengan membatasi pergerakan lateral penyerang di dalam sistem cloud. Melalui segmentasi mikro dan prinsip least privilege, ruang gerak penyerang menjadi lebih sempit meskipun berhasil menembus salah satu komponen sistem (Alkadi et al., 2022).

Manfaat lainnya adalah peningkatan visibilitas dan kemampuan pemantauan aktivitas pengguna dan aplikasi secara menyeluruh. Dengan pemantauan berkelanjutan, organisasi dapat mendeteksi ancaman lebih dini dan merespons insiden keamanan secara cepat dan tepat. Hal ini menjadikan Zero Trust sebagai pendekatan strategis yang efektif untuk meningkatkan ketahanan keamanan cloud computing di tengah meningkatnya kompleksitas ancaman siber (Zhang et al., 2023).

3.3. Peran Enkripsi dalam Keamanan Cloud Computing

Enkripsi merupakan salah satu mekanisme fundamental dalam menjaga keamanan dan kerahasiaan data pada lingkungan cloud computing. Mengingat data cloud disimpan dan diproses pada infrastruktur milik pihak ketiga, enkripsi berperan sebagai lapisan perlindungan utama untuk mencegah akses tidak sah, kebocoran data, serta penyalahgunaan informasi sensitif. Dalam praktiknya, enkripsi diterapkan pada berbagai kondisi data, mulai dari data yang disimpan, ditransmisikan, hingga diproses (Alasmary et al., 2022).

3.3.1. Jenis Enkripsi dalam Cloud Computing

Berdasarkan kondisi data, penerapan enkripsi dalam cloud computing umumnya dibedakan menjadi tiga jenis utama, yaitu data at rest, data in transit, dan data in use. Enkripsi data at rest bertujuan untuk melindungi data yang tersimpan dalam media penyimpanan cloud, seperti basis data, object storage, dan backup. Dengan enkripsi ini, data tetap berada dalam bentuk tidak terbaca meskipun terjadi akses tidak sah terhadap media penyimpanan. Pendekatan ini sangat penting dalam

mencegah kebocoran data akibat kegagalan sistem atau pelanggaran keamanan internal (Singh & Chatterjee, 2021).

Enkripsi data in transit diterapkan untuk melindungi data yang sedang dikirimkan melalui jaringan, baik antar pengguna dan layanan cloud maupun antar komponen dalam infrastruktur cloud itu sendiri. Enkripsi ini bertujuan untuk mencegah serangan seperti man-in-the-middle dan penyadapan jaringan, yang sering terjadi pada sistem berbasis internet (Kumar et al., 2023).

Sementara itu, enkripsi data in use merupakan pendekatan yang relatif lebih baru dan kompleks, di mana data tetap berada dalam keadaan terenkripsi saat sedang diproses. Teknik ini umumnya diimplementasikan melalui confidential computing atau homomorphic encryption, yang memungkinkan pemrosesan data tanpa harus mendekripsinya terlebih dahulu. Pendekatan ini dinilai sangat menjanjikan dalam meningkatkan keamanan data cloud, meskipun masih menghadapi tantangan dari sisi performa dan kompleksitas implementasi (Ménard et al., 2021).

3.3.2. Algoritma Enkripsi yang Umum Digunakan

Dalam implementasinya, berbagai algoritma enkripsi digunakan untuk mengamankan data pada layanan cloud. Salah satu algoritma yang paling umum digunakan adalah Advanced Encryption Standard (AES), yang dikenal memiliki tingkat keamanan tinggi dan efisiensi yang baik untuk enkripsi data dalam jumlah besar. AES banyak diterapkan untuk enkripsi data at rest karena kemampuannya dalam menjaga kerahasiaan data secara efektif (Alasmary et al., 2022).

Selain algoritma simetris, algoritma enkripsi asimetris seperti RSA dan Elliptic Curve Cryptography (ECC) juga digunakan, terutama untuk proses pertukaran kunci dan autentikasi. ECC semakin banyak digunakan dalam lingkungan cloud karena menawarkan tingkat keamanan yang setara dengan RSA namun dengan ukuran kunci yang lebih kecil, sehingga lebih efisien dari sisi komputasi (Kumar et al., 2023).

Untuk kebutuhan enkripsi data in use, teknik homomorphic encryption dan secure enclave mulai banyak diteliti dan dikembangkan. Meskipun teknik ini belum diadopsi secara luas, potensinya dalam mendukung pemrosesan data yang aman tanpa mengorbankan privasi menjadikannya fokus penting dalam penelitian keamanan cloud terkini (Ménard et al., 2021).

3.3.3. Integrasi Enkripsi dengan Layanan Cloud

Integrasi enkripsi dengan layanan cloud umumnya dilakukan melalui mekanisme keamanan bawaan yang disediakan oleh penyedia cloud, seperti layanan key management system (KMS), hardware security module (HSM), serta kebijakan keamanan berbasis identitas. Integrasi ini memungkinkan pengelolaan kunci enkripsi secara terpusat dan aman, sehingga risiko kebocoran kunci dapat diminimalkan (Sharma & Chen, 2021).

Selain itu, enkripsi sering dikombinasikan dengan pendekatan keamanan lain, seperti Zero Trust Architecture, untuk membentuk sistem keamanan cloud yang lebih komprehensif. Dalam konteks ini, enkripsi berfungsi sebagai pelindung data, sementara Zero Trust mengatur kontrol akses dan verifikasi identitas secara berkelanjutan. Kombinasi kedua pendekatan tersebut dinilai mampu meningkatkan ketahanan sistem cloud terhadap berbagai bentuk ancaman siber (Zhang et al., 2023). Dengan demikian, enkripsi tidak hanya berperan sebagai mekanisme teknis, tetapi juga sebagai komponen strategis dalam arsitektur keamanan cloud computing modern yang menekankan prinsip kerahasiaan, integritas, dan keandalan data.

3.4. Analisis Kelebihan dan Tantangan

Penerapan pendekatan Zero Trust dan enkripsi dalam keamanan cloud computing menawarkan berbagai kelebihan yang signifikan, namun juga menghadirkan sejumlah tantangan dan keterbatasan yang perlu dikaji secara kritis. Analisis ini penting untuk memberikan pemahaman yang seimbang mengenai efektivitas kedua pendekatan tersebut dalam konteks lingkungan cloud yang kompleks dan dinamis.

3.4.1. Kelebihan Zero Trust dan Enkripsi

Salah satu kelebihan utama pendekatan Zero Trust adalah kemampuannya dalam mengurangi risiko akses tidak sah melalui mekanisme verifikasi identitas dan otorisasi yang dilakukan secara berkelanjutan. Dengan prinsip least privilege access dan segmentasi mikro, Zero Trust mampu membatasi ruang gerak penyerang dan mencegah pergerakan lateral dalam sistem cloud, sehingga dampak serangan dapat diminimalkan secara signifikan (Rose et al., 2020; Kindervag et al., 2021). Selain itu, Zero Trust memberikan peningkatan visibilitas dan kontrol terhadap aktivitas pengguna

dan aplikasi di lingkungan cloud. Pemantauan yang bersifat kontekstual dan real-time memungkinkan deteksi dini terhadap perilaku mencurigakan, sehingga respons keamanan dapat dilakukan secara lebih cepat dan tepat (Alkadi et al., 2022).

Sementara itu, enkripsi berperan penting dalam menjaga kerahasiaan dan integritas data cloud. Penerapan enkripsi pada data at rest, data in transit, dan data in use memastikan bahwa informasi sensitif tetap terlindungi meskipun terjadi pelanggaran keamanan pada infrastruktur cloud. Enkripsi juga mendukung kepatuhan terhadap regulasi perlindungan data, seperti perlindungan privasi dan keamanan informasi pengguna (Alasmary et al., 2022).

Kombinasi Zero Trust dan enkripsi dinilai mampu membentuk sistem keamanan yang berlapis (defense in depth), di mana Zero Trust berfokus pada kontrol akses dan verifikasi identitas, sedangkan enkripsi melindungi data secara kriptografis. Sinergi ini meningkatkan ketahanan keamanan cloud secara keseluruhan terhadap berbagai jenis ancaman siber (Zhang et al., 2023).

3.4.2. Tantangan Implementasi

Meskipun menawarkan berbagai kelebihan, implementasi Zero Trust dan enkripsi dalam lingkungan cloud juga menghadapi tantangan yang tidak dapat diabaikan. Salah satu tantangan utama adalah kompleksitas implementasi. Penerapan Zero Trust membutuhkan perubahan arsitektur keamanan secara menyeluruh, termasuk integrasi sistem manajemen identitas, kebijakan akses berbasis konteks, serta mekanisme pemantauan berkelanjutan. Kompleksitas ini sering kali menjadi hambatan bagi organisasi dengan sumber daya teknis yang terbatas (Sharma & Chen, 2021).

Dari sisi biaya, penerapan Zero Trust dan enkripsi tingkat lanjut, seperti confidential computing atau homomorphic encryption, memerlukan investasi yang cukup besar, baik dalam hal infrastruktur, lisensi perangkat lunak, maupun pengembangan sumber daya manusia. Hal ini dapat menjadi kendala terutama bagi organisasi skala kecil dan menengah yang memiliki keterbatasan anggaran (Singh & Chatterjee, 2021).

Selain itu, tantangan performa sistem juga menjadi perhatian penting. Proses enkripsi dan dekripsi, khususnya pada data in use, dapat menimbulkan beban komputasi tambahan yang berdampak pada penurunan kinerja aplikasi cloud. Beberapa penelitian menunjukkan bahwa peningkatan tingkat keamanan sering kali berbanding terbalik dengan efisiensi sistem, sehingga diperlukan kompromi antara keamanan dan performa (Ménard et al., 2021).

3.4.3. Keterbatasan dalam Penelitian Terdahulu

Analisis terhadap penelitian terdahulu menunjukkan adanya beberapa keterbatasan yang masih perlu dikaji lebih lanjut. Pertama, sebagian besar penelitian masih berfokus pada pendekatan Zero Trust atau enkripsi secara terpisah, sementara kajian yang membahas integrasi keduanya secara komprehensif dalam skala besar masih relatif terbatas (Zhang et al., 2023).

Kedua, banyak penelitian yang bersifat konseptual atau berbasis simulasi, sehingga belum sepenuhnya merepresentasikan tantangan implementasi di lingkungan cloud nyata yang kompleks dan heterogen. Kurangnya studi empiris dan evaluasi jangka panjang menjadi salah satu celah penelitian yang signifikan (Alkadi et al., 2022).

Ketiga, aspek non-teknis seperti kesiapan organisasi, faktor manusia, dan kebijakan tata kelola keamanan masih kurang mendapat perhatian dalam penelitian keamanan cloud berbasis Zero Trust dan enkripsi. Padahal, faktor-faktor tersebut memiliki peran penting dalam menentukan keberhasilan implementasi keamanan cloud secara menyeluruh (Sarker, 2021).

3.5. Research Gap dan Peluang Penelitian

Berdasarkan hasil analisis literatur yang telah dilakukan, dapat diidentifikasi sejumlah kekosongan penelitian (research gap) serta peluang pengembangan penelitian terkait keamanan cloud computing berbasis Zero Trust dan enkripsi. Identifikasi ini penting untuk memberikan kontribusi ilmiah yang berkelanjutan dan relevan dengan perkembangan teknologi keamanan cloud di masa depan.

3.5.1. Kekosongan Penelitian

Pertama, sebagian besar penelitian terdahulu masih membahas Zero Trust dan enkripsi secara terpisah. Studi mengenai Zero Trust umumnya berfokus pada aspek kontrol akses, autentikasi berkelanjutan, dan segmentasi mikro, sementara penelitian enkripsi lebih menekankan pada perlindungan data dari sisi kriptografi. Kajian yang mengintegrasikan kedua pendekatan tersebut

secara komprehensif dalam satu kerangka keamanan cloud masih relatif terbatas (Zhang et al., 2023; Alkadi et al., 2022).

Kedua, banyak penelitian yang bersifat konseptual atau berbasis simulasi, sehingga belum sepenuhnya merepresentasikan kondisi implementasi di lingkungan cloud nyata yang berskala besar dan heterogen. Minimnya studi empiris yang menguji efektivitas Zero Trust dan enkripsi pada sistem cloud produksi menjadi celah penelitian yang signifikan, khususnya dalam konteks beban kerja dinamis dan multi-tenant (Sharma & Chen, 2021).

Ketiga, aspek evaluasi performa dan efisiensi sistem masih kurang mendapatkan perhatian mendalam. Beberapa penelitian mengakui adanya penurunan performa akibat penerapan mekanisme keamanan tingkat lanjut, seperti enkripsi data in use, namun belum banyak yang memberikan analisis kuantitatif atau solusi optimasi yang terukur untuk mengatasi permasalahan tersebut (Ménard et al., 2021).

Keempat, literatur yang ada masih relatif terbatas dalam membahas aspek non-teknis, seperti kesiapan organisasi, faktor manusia, dan tata kelola keamanan (security governance). Padahal, keberhasilan penerapan Zero Trust dan enkripsi tidak hanya ditentukan oleh teknologi, tetapi juga oleh kebijakan, kompetensi sumber daya manusia, serta budaya keamanan dalam organisasi (Sarker, 2021).

3.5.2. Peluang Pengembangan Model Keamanan Cloud di Masa Depan

Berdasarkan kekosongan penelitian yang teridentifikasi, terdapat beberapa peluang penelitian yang dapat dikembangkan di masa depan. Salah satu peluang utama adalah pengembangan model keamanan cloud terintegrasi yang menggabungkan Zero Trust dan enkripsi dalam satu arsitektur yang adaptif dan kontekstual. Model ini diharapkan mampu memberikan perlindungan menyeluruh terhadap akses dan data, sekaligus mempertahankan performa sistem cloud (Zhang et al., 2023).

Selain itu, penelitian lanjutan dapat difokuskan pada pemanfaatan teknologi kecerdasan buatan dan pembelajaran mesin untuk mendukung Zero Trust, khususnya dalam analisis perilaku pengguna dan deteksi anomali secara otomatis. Integrasi pendekatan ini berpotensi meningkatkan akurasi deteksi ancaman dan mengurangi ketergantungan pada kebijakan keamanan statis (Alkadi et al., 2022).

Peluang lainnya adalah pengembangan dan evaluasi mekanisme enkripsi yang lebih efisien, seperti optimasi homomorphic encryption atau penerapan confidential computing, agar dapat digunakan secara luas tanpa menurunkan performa sistem secara signifikan. Penelitian di bidang ini menjadi penting seiring meningkatnya kebutuhan pemrosesan data sensitif di lingkungan cloud (Ménard et al., 2021).

Terakhir, penelitian di masa depan juga perlu mengkaji pendekatan holistik yang mengintegrasikan aspek teknis dan non-teknis, termasuk tata kelola keamanan, kepatuhan regulasi, serta kesiapan organisasi. Pendekatan ini diharapkan dapat menghasilkan model keamanan cloud yang tidak hanya kuat secara teknis, tetapi juga realistis dan berkelanjutan dalam penerapannya (Sarker, 2021).

4. KESIMPULAN

Berdasarkan hasil Systematic Literature Review terhadap publikasi lima tahun terakhir, dapat disimpulkan bahwa pendekatan Zero Trust dan enkripsi merupakan dua pilar utama dalam strategi keamanan cloud computing modern yang saling melengkapi. Zero Trust berkembang sebagai respons atas kelemahan model keamanan berbasis perimeter dengan menekankan prinsip never trust, always verify, penerapan autentikasi berkelanjutan, serta kontrol akses berbasis identitas dan konteks, sehingga efektif dalam menurunkan risiko serangan lateral dan kebocoran data di lingkungan cloud yang dinamis (Rose et al., 2020; Kindervag et al., 2021). Sementara itu, enkripsi—baik untuk data at rest, data in transit, maupun data in use—berperan krusial dalam menjaga kerahasiaan dan integritas data, dengan pemanfaatan algoritma kriptografi modern serta integrasi layanan key management yang disediakan oleh penyedia cloud (Zhang et al., 2022; Alasmary et al., 2023). Meskipun demikian, temuan literatur juga menunjukkan adanya tantangan signifikan, seperti kompleksitas implementasi Zero Trust, peningkatan biaya operasional, potensi penurunan performa akibat proses enkripsi, serta keterbatasan penelitian empiris yang menguji efektivitas integrasi kedua pendekatan secara holistik di lingkungan multi-cloud dan hybrid cloud. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan model keamanan cloud terintegrasi yang menggabungkan Zero Trust dan enkripsi secara adaptif, melakukan evaluasi berbasis studi kasus

dan eksperimen nyata, serta mengeksplorasi peran teknologi pendukung seperti kecerdasan buatan dan confidential computing. Secara praktis, hasil penelitian ini diharapkan dapat menjadi acuan bagi organisasi dan penyedia layanan cloud dalam merancang strategi keamanan yang lebih komprehensif, berkelanjutan, dan sesuai dengan tingkat risiko serta kebutuhan operasional masing-masing organisasi.

DAFTAR PUSTAKA

Alasmary, W., Alhaidari, F., & Alsubaie, N. (2022). Encryption techniques for securing data in cloud computing: A comprehensive review. *Journal of Cloud Computing*, 11(1), 1–18. https://doi.org/10.1186/s13677-022-00315-9

Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2022). A systematic review of cloud computing security challenges and solutions. *Journal of Network and Computer Applications*, 196, 103246. https://doi.org/10.1016/j.jnca.2021.103246

Kindervag, J., Balaouras, S., & Hines, S. (2021). Implementing Zero Trust security in modern cloud environments. *IEEE Security & Privacy*, 19(4), 44–52. https://doi.org/10.1109/MSEC.2021.3075375

Ménard, D., Gomis, J., & Sirdey, R. (2021). Confidential computing and data protection in cloud environments. *IEEE Security & Privacy*, 19(5), 56–64. https://doi.org/10.1109/MSEC.2021.3090112

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sarker, I. H. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 8(1), 1–29. https://doi.org/10.1186/s40537-021-00438-6

Sharma, P., & Chen, Y. (2021). Zero Trust based cloud security framework for distributed environments. *Future Internet*, 13(7), 1–18. https://doi.org/10.3390/fi13070182

Singh, A., & Chatterjee, K. (2021). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 179, 102995. https://doi.org/10.1016/j.jnca.2020.102995

Zhang, Y., Chen, X., & Li, J. (2023). Integrating Zero Trust and encryption mechanisms for cloud data security. *Future Generation Computer Systems*, 140, 12–24. https://doi.org/10.1016/j.future.2022.10.014