Karapan Network
Journal

Vol.02, No.03, July 2026
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Studi Literatur: Strategi Migrasi dan Mekanisme Autentikasi Zero Trust untuk Mengamankan Arsitektur Microservices di Lingkungan Multi-Cloud

Radhitya Dwi Akmal Purnomo 1)[n] , Giovani Sapta Purnama A. 2)

1)2)Universitas Madura, Pamekasan, Indonesia

1)radhityadwi65@gmail.com 2) giovanisaptapurnama@gmail.com

Abstrak

Adopsi arsitektur microservices secara masif telah mendorong banyak organisasi untuk bermigrasi dari sistem monolitik menuju ekosistem terdistribusi yang dijalankan lintas beberapa penyedia layanan cloud (multi-cloud), guna menghindari ketergantungan pada satu vendor, meningkatkan resiliensi, dan memenuhi tuntutan kepatuhan regional. Namun, desentralisasi ini juga memperluas permukaan serangan secara signifikan, terutama pada fase migrasi ketika sistem legacy dan layanan microservices baru berjalan berdampingan dalam kondisi keamanan yang belum sepenuhnya matang, sehingga rentan terhadap pergerakan lateral (lateral movement) dan eskalasi akses oleh pihak yang tidak berwenang. Model keamanan berbasis perimeter tradisional terbukti tidak lagi memadai untuk lingkungan yang dinamis dan terfragmentasi semacam ini. Penelitian ini menggunakan pendekatan Tinjauan Literatur Sistematis (Systematic Literature Review/SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis berbagai strategi migrasi serta mekanisme keamanan yang relevan dalam mengamankan arsitektur microservices pada lingkungan multi-cloud. Melalui penelusuran literatur dari basis data akademik bereputasi dalam kurun lima tahun terakhir, penelitian ini mengkaji tiga domain mekanisme keamanan utama: service mesh dengan enkripsi mutual TLS (mTLS), otorisasi berbasis token melalui API gateway (OAuth2/JWT), dan arsitektur Zero Trust yang menerapkan verifikasi identitas berkelanjutan pada setiap permintaan layanan. Hasil sintesis menunjukkan bahwa tidak ada satu mekanisme tunggal yang optimal pada seluruh skenario; masing-masing pendekatan menghadirkan trade-off antara kekuatan proteksi, latensi komunikasi antar-layanan, dan kompleksitas operasional lintas-cloud. Penelitian ini turut memetakan kesenjangan riset terkait minimnya kerangka kerja migrasi yang mengintegrasikan keamanan sejak tahap perancangan (security-by-design), serta mengusulkan arah pengembangan menuju arsitektur hibrida adaptif yang menggabungkan keunggulan service mesh dan Zero Trust untuk mendukung migrasi microservices yang aman, efisien, dan dapat diskalakan pada ekosistem multi-cloud generasi mendatang.

Kata Kunci: Microservices, Multi-Cloud, System Migration, Zero Trust, Cybersecurity, Systematic Literature Analysis.

Article history: Received 6 April 2026, first decision 24 April 2026, accepted 25 August 2026, available online 30 October 2026

I. PENDAHULUAN

Transformasi arsitektur perangkat lunak dari model monolitik menuju microservices telah menjadi salah satu pergeseran paradigma paling signifikan dalam rekayasa sistem terdistribusi modern. Dengan memecah aplikasi menjadi kumpulan layanan independen yang masing-masing dapat dikembangkan, diuji, dan diskalakan secara terpisah, organisasi memperoleh fleksibilitas operasional yang jauh lebih besar dibandingkan sistem tradisional[1] Tren ini kemudian beririsan dengan adopsi strategi multi-cloud, yaitu penyebaran beban kerja pada lebih dari satu Penyedia layanan cloud publik secara simultan, yang didorong oleh kebutuhan menghindari ketergantungan pada satu vendor (vendor lock-in), meningkatkan ketahanan terhadap gangguan layanan, serta memenuhi regulasi kedaulatan data pada yurisdiksi tertentu Kombinasi microservices dan multi-cloud kini menjadi fondasi arsitektural bagi banyak platform digital berskala besar.[2][3]

Namun demikian, fleksibilitas yang ditawarkan oleh kombinasi ini tidak datang tanpa konsekuensi. Desentralisasi kontrol dan meningkatnya jumlah titik komunikasi antar-layanan secara langsung memperluas permukaan serangan (attack surface) sistem .[4][5] Fase migrasi dari sistem monolitik menuju microservices merupakan periode yang sangat rentan, karena pada tahap ini komponen legacy dan layanan baru sering kali harus berjalan berdampingan (coexistence) dengan tingkat kematangan kontrol keamanan yang tidak seragam[6]. Penyerang yang berhasil mengompromikan satu layanan dengan keamanan lemah dapat memanfaatkan celah ini untuk melakukan pergerakan lateral menuju layanan lain yang lebih kritis, terutama apabila organisasi masih mengandalkan model keamanan berbasis perimeter jaringan.[7][8]

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.pp-pp

Berbagai upaya mitigasi telah diusulkan dalam literatur, mulai dari penerapan service mesh yang menyediakan enkripsi komunikasi antar-layanan secara transparan, mekanisme otorisasi berbasis token pada lapisan API gateway, hingga pergeseran paradigma menuju arsitektur Zero Trust yang tidak lagi mengasumsikan kepercayaan implisit berdasarkan lokasi jaringan.[9] Meskipun demikian, kajian terdahulu menunjukkan bahwa literatur mengenai keamanan microservices masih sangat terfragmentasi, dengan sedikit penelitian yang secara spesifik mengaitkan strategi migrasi dengan pemilihan mekanisme keamanan yang tepat pada konteks multi-cloud [10].

Penelitian ini bertujuan untuk menjembatani kesenjangan tersebut melalui Tinjauan Literatur Sistematis (SLR) terhadap strategi migrasi dan mekanisme keamanan microservices mutakhir pada lingkungan multi-cloud.[11] Kontribusi utama studi ini meliputi penyusunan taksonomi mekanisme keamanan yang relevan, evaluasi trade-off antara tingkat proteksi dengan kompleksitas operasional dan latensi, serta identifikasi arah penelitian masa depan yang strategis.[12]

II. TINJAUAN PUSTAKA

Microservices didefinisikan sebagai gaya arsitektur yang menyusun aplikasi sebagai kumpulan layanan kecil yang saling berkomunikasi melalui antarmuka berbasis pesan (message-passing API), di mana setiap layanan dapat dikembangkan dan dieksekusi secara independen [13]. Survei tahunan komunitas cloud-native mencatat bahwa adopsi container dan orkestrasi berbasis Kubernetes terus meningkat secara konsisten pada lingkungan produksi perusahaan, sejalan dengan menguatnya tren penyebaran beban kerja pada lebih dari satu penyedia layanan cloud sekaligus [14]. Lingkungan multi-cloud menambah lapisan kompleksitas tersendiri karena setiap penyedia memiliki model identitas, kebijakan jaringan, dan mekanisme kontrol akses yang berbeda [15].

Migrasi dari sistem monolitik menuju microservices bukan sekadar persoalan teknis pemecahan kode, melainkan melibatkan pertimbangan menyeluruh terhadap atribut kualitas perangkat lunak seperti skalabilitas, keterpisahan (coupling), dan kinerja [16][17]. Survei industri menunjukkan bahwa banyak organisasi memulai migrasi tanpa kerangka kerja metodologis yang matang, sehingga keputusan mengenai batas layanan (service boundary) dan mekanisme komunikasi antar-layanan sering kali diambil secara ad hoc[18]. Minimnya pertimbangan keamanan pada tahap perencanaan migrasi ini kerap kali baru disadari setelah sistem berjalan pada lingkungan produksi.

Kajian sistematis terhadap ratusan publikasi mengenai keamanan microservices mengungkap bahwa ancaman spoofing dan denial-of-service merupakan dua kategori serangan yang paling banyak dibahas dalam literatur [19]. Spesifikasi keamanan resmi dari lembaga standar turut menegaskan bahwa strategi keamanan microservices perlu mencakup verifikasi identitas layanan, enkripsi komunikasi, serta kontrol akses berbasis kebijakan yang konsisten di seluruh siklus hidup aplikasi [20][21]. Tinjauan multivokal terhadap literatur akademik maupun sumber industri turut menemukan bahwa sebagian besar solusi keamanan yang diusulkan berfokus pada pencegahan, sementara kemampuan deteksi dan pemulihan pascaserangan masih jarang dibahas secara mendalam [22].

Salah satu pendekatan teknis yang banyak diadopsi untuk mengamankan komunikasi antar-layanan adalah penerapan service mesh, yaitu lapisan infrastruktur khusus yang menangani routing, observabilitas, dan keamanan trafik tanpa mengubah kode aplikasi itu sendiri.[23] Service mesh seperti Istio dan Linkerd menyediakan enkripsi mutual TLS (mTLS) secara otomatis pada seluruh komunikasi antar-pod, sehingga setiap layanan wajib membuktikan identitasnya melalui sertifikat digital sebelum sesi komunikasi dibuka. Studi performa menunjukkan bahwa penerapan service mesh pada lingkungan multi-cloud tidak menimbulkan penalti kinerja yang signifikan pada level data plane, meskipun terdapat variasi penggunaan sumber daya tergantung konfigurasi dan karakteristik masing-masing penyedia cloud [24].

Selain service mesh, lapisan API gateway turut berperan penting sebagai titik kontrol terpusat untuk autentikasi dan otorisasi permintaan yang masuk ke dalam ekosistem microservices.[25] Protokol OAuth2 dan JSON Web Token (JWT) banyak diadopsi karena memungkinkan verifikasi identitas yang bersifat stateless, di mana setiap token membawa klaim otorisasi yang dapat divalidasi tanpa memerlukan pemanggilan balik ke server pusat secara berulang [26][27]. Pendekatan ini secara signifikan mengurangi beban komputasi pada arsitektur terdistribusi, namun tetap menyisakan tantangan terkait manajemen siklus hidup token, termasuk pencabutan akses secara real-time ketika terjadi indikasi kompromi kredensial.[28]Pergeseran paradigma paling mendasar dalam literatur terkini adalah adopsi arsitektur Zero Trust, yang secara eksplisit meniadakan asumsi kepercayaan implisit berdasarkan lokasi jaringan dan mewajibkan autentikasi serta otorisasi pada setiap permintaan, tanpa memandang apakah permintaan tersebut berasal dari dalam atau luar batas jaringan organisasi [29]. Kajian mengenai optimalisasi infrastruktur cloud networking melalui integrasi Software Defined Network (SDN) dan Network Function Virtualization (NFV) menunjukkan bahwa virtualisasi fungsi jaringan dapat mempermudah orkestrasi kebijakan konektivitas lintas-penyedia layanan cloud secara terprogram [30][31]. Tinjauan mengenai regulasi siber dan kebijakan keamanan jaringan generasi kelima dari perspektif nasional maupun internasional menggarisbawahi bahwa aspek kepatuhan terhadap kerangka regulasi lintas-

yurisdiksi turut menjadi pertimbangan penting dalam mendesain mekanisme keamanan pada lingkungan multi-cloud [32][33]. Perbandingan kinerja protokol WebSocket dan MQTT pada konteks pengiriman notifikasi push menunjukkan bahwa karakteristik masing-masing protokol perlu disesuaikan dengan kebutuhan spesifik aplikasi, sebuah prinsip yang juga berlaku pada pemilihan mekanisme komunikasi antar-microservices [34]. Evaluasi kinerja perangkat jaringan seperti router pada infrastruktur penghubung memberikan gambaran bahwa stabilitas lapisan jaringan dasar turut menentukan keberhasilan implementasi mekanisme keamanan tingkat aplikasi di atasnya [35][36]. Analisis kinerja jaringan 5G menegaskan bahwa peningkatan kapasitas dan penurunan latensi jaringan akses turut membuka peluang sekaligus tantangan baru bagi keandalan komunikasi layanan terdistribusi yang tersebar secara geografis [37][38]. Studi mengenai privasi dan keamanan penerapan teknologi terhubung dalam kehidupan sehari-hari turut mengingatkan bahwa efisiensi operasional kerap kali diprioritaskan di atas mekanisme keamanan yang kuat [39]. Perancangan jaringan nirkabel berbasis mesh untuk smart city memberikan preseden mengenai bagaimana arsitektur jaringan terdistribusi dengan banyak node dapat dikelola secara efisien [40][41], sementara eksplorasi integrasi teknologi kuantum dan fiber optik untuk keamanan jaringan masa depan memberikan wawasan mengenai arah jangka panjang penguatan lapisan transport komunikasi yang mendasari ekosistem multi-cloud [42].

III. METODE

Penelitian ini mengadopsi pendekatan Tinjauan Literatur Sistematis (Systematic Literature Review/SLR) yang mengikuti pedoman metodologis yang lazim digunakan dalam rekayasa perangkat lunak, dengan fokus utama pada evaluasi komprehensif terhadap strategi migrasi dan mekanisme keamanan microservices pada lingkungan multi-cloud. Metode ini tidak melibatkan eksperimen maupun implementasi sistem baru, melainkan berfokus pada meta-analisis mendalam terhadap arsitektur keamanan, metrik kinerja, dan temuan dari studi-studi primer terdahulu yang relevan dan kredibel. Kerangka kerja penelitian dirancang melalui empat tahapan utama, yang diuraikan sebagai berikut:

A. Perumusan Kriteria dan Pengumpulan Literatur

Tahap pertama berfokus pada penelusuran literatur ilmiah dari basis data akademik global terkemuka, khususnya IEEE Xplore, ACM Digital Library, ScienceDirect, dan Google Scholar, dengan bantuan perangkat lunak seperti Publish or Perish. Pencarian dilakukan menggunakan kombinasi kata kunci spesifik seperti "microservices security multi-cloud", "zero trust microservices architecture", dan "API gateway authentication cloud-native". Untuk memastikan kualitas dan relevansi, proses penyaringan menerapkan kriteria inklusi yang ketat, meliputi:

1. **Relevansi Topik:** Literatur harus secara eksplisit membahas mekanisme migrasi atau keamanan pada arsitektur microservices, dengan konteks penerapan pada lebih dari satu penyedia layanan cloud.
2. **Kredibilitas Sumber:** Pengumpulan data dibatasi pada jurnal ilmiah bereputasi (peer-reviewed journals) dan prosiding konferensi internasional guna menjamin validitas temuan yang disintesis.
3. **Kebaruan (Novelty):** Prioritas utama diberikan pada publikasi dalam rentang waktu lima tahun terakhir untuk menangkap tren teknologi cloud-native dan ancaman siber terkini.

B. Prosedur Ekstraksi dan Analisis Data

Literatur yang lolos verifikasi tahap pertama kemudian ditetapkan sebagai data primer untuk dianalisis menggunakan metode analisis isi (content analysis) dengan pendekatan deskriptif kualitatif. Pada tahap ini, setiap artikel dibedah secara kritis untuk mengekstraksi parameter teknis yang membedakan satu mekanisme keamanan dengan mekanisme lainnya. Ekstraksi data secara spesifik difokuskan pada pengumpulan variabel berikut:

1. **Strategi Migrasi:** Mengidentifikasi pendekatan dekomposisi sistem monolitik dan pola transisi yang digunakan.
2. **Mekanisme Keamanan:** Menganalisis pendekatan yang digunakan, seperti service mesh dengan mTLS, API gateway berbasis token (OAuth2/JWT), atau arsitektur Zero Trust.
3. **Metrik Kinerja:** Menilai besaran latensi, overhead komputasi, dan kompleksitas operasional yang ditimbulkan oleh masing-masing mekanisme saat diterapkan lintas-cloud.
4. **Cakupan Mitigasi Ancaman:** Mengevaluasi sejauh mana mekanisme tersebut mampu mencegah pergerakan lateral dan akses tidak sah antar-layanan.

C. Evaluasi Komparatif dan Klasifikasi Tematik

Setelah data diekstraksi, langkah selanjutnya adalah melakukan analisis secara tematik dengan mengklasifikasikan literatur berdasarkan pendekatan teknis utama ke dalam tiga domain: mekanisme berbasis service mesh dan mTLS, mekanisme berbasis token/otorisasi pada API gateway, dan mekanisme berbasis arsitektur Zero Trust. Evaluasi komparatif dilakukan untuk mengukur trade-off antara Tingkat Keamanan dan Efisiensi Operasional (latensi komunikasi dan kompleksitas konfigurasi lintas-cloud). Hasil perbandingan ini direpresentasikan dalam bentuk tabulasi pada bagian Hasil.

D. Sintesis Temuan dan Identifikasi Celah Penelitian

Tahap akhir dari metodologi ini melibatkan sintesis komprehensif dari seluruh temuan komparatif untuk menarik kesimpulan umum mengenai strategi migrasi dan mekanisme keamanan mana yang paling unggul dan aplikatif untuk skenario multi-cloud. Selain merumuskan solusi optimal saat ini, tahapan ini juga ditujukan untuk memetakan celah penelitian (research gap) yang masih belum terpecahkan, khususnya menuju integrasi keamanan yang adaptif dan terintegrasi lintas-platform pada generasi arsitektur microservices berikutnya.

IV. HASIL

Penelitian ini berhasil mengekstraksi dan mensintesis data dari korpus literatur primer mengenai mekanisme keamanan microservices yang diterapkan pada lingkungan multi-cloud. Fokus analisis diarahkan pada kemampuan masing-masing mekanisme dalam mencegah pergerakan lateral dan akses tidak sah selama dan setelah proses migrasi berlangsung. Hasil studi menunjukkan bahwa tanpa mekanisme verifikasi identitas yang konsisten di setiap titik komunikasi, kerentanan pada satu layanan dapat dengan cepat dieksploitasi untuk mengompromikan layanan lain yang lebih kritis dalam ekosistem terdistribusi.

Taksonomi Mekanisme Keamanan untuk Arsitektur Microservices Multi-Cloud

Berdasarkan analisis literatur, mekanisme keamanan microservices pada lingkungan multi-cloud diklasifikasikan ke dalam tiga domain teknis yang memiliki karakteristik operasional berbeda:

1. **Service Mesh dan Mutual TLS (mTLS):**
   Pendekatan ini menempatkan lapisan keamanan pada infrastruktur jaringan layanan itu sendiri melalui sidecar proxy, tanpa memerlukan modifikasi kode aplikasi. Setiap layanan diberikan identitas kriptografis unik, dan seluruh komunikasi antar-layanan diwajibkan melalui sesi mTLS yang saling terverifikasi. Keunggulan utama pendekatan ini adalah konsistensi penegakan kebijakan keamanan secara transparan di seluruh klaster, meskipun memerlukan sumber daya komputasi tambahan untuk proses enkripsi dan dekripsi pada setiap sidecar proxy.
2. **Mekanisme Otorisasi Berbasis Token pada API Gateway:**
   Pendekatan ini memusatkan autentikasi dan otorisasi pada titik masuk (entry point) sistem, di mana setiap permintaan klien harus menyertakan token akses yang sah sebelum diteruskan ke layanan internal. Skema ini relatif ringan dari sisi komputasi internal karena validasi token bersifat stateless, namun bergantung pada keandalan satu titik kontrol terpusat yang berpotensi menjadi target serangan tersendiri apabila tidak diperkuat dengan redundansi yang memadai.
3. **Arsitektur Zero Trust:**
   Pendekatan paling komprehensif yang mengintegrasikan verifikasi identitas berkelanjutan, kontrol akses berbasis kebijakan granular (fine-grained), dan asumsi bahwa tidak ada entitas baik di dalam maupun di luar jaringan yang secara default dapat dipercaya. Implementasinya pada lingkungan multi-cloud sering kali mengombinasikan identitas berbasis sertifikat pada level workload dengan kebijakan otorisasi dinamis yang dievaluasi secara real-time pada setiap permintaan layanan.

Mekanisme Mitigasi terhadap Pergerakan Lateral dan Akses Tidak Sah

Pergerakan lateral pada arsitektur microservices terjadi ketika penyerang yang berhasil mengompromikan satu layanan memanfaatkan kepercayaan implisit antar-layanan untuk mengakses sumber daya lain yang lebih sensitif. Mekanisme keamanan modern membongkar permasalahan ini melalui dua pilar utama:

1. **Verifikasi Identitas Berkelanjutan:**
   Dengan penerapan mTLS dan Zero Trust, setiap permintaan antar-layanan wajib disertai bukti identitas kriptografis yang valid. Jika penyerang mencoba menyamar sebagai layanan sah dari pod atau node yang telah dikompromikan, mekanisme verifikasi akan mendeteksi ketidaksesuaian sertifikat atau klaim identitas, sehingga permintaan tersebut akan ditolak sebelum dapat menjangkau layanan tujuan.
2. **Segmentasi Mikro dan Kebijakan Akses Granular:**
   Pendekatan mikrosegmentasi membatasi komunikasi antar-layanan hanya pada jalur yang secara eksplisit diizinkan oleh kebijakan keamanan, alih-alih mengandalkan kepercayaan menyeluruh dalam satu segmen jaringan. Dengan demikian, meskipun satu layanan berhasil dikompromikan, kemampuan penyerang untuk bergerak menuju layanan lain menjadi sangat terbatas, sehingga membatasi dampak insiden keamanan secara signifikan.

Evaluasi Kinerja dan Analisis Perbandingan Data

Keamanan yang maksimal selalu membawa konsekuensi terhadap kompleksitas operasional dan latensi komunikasi. Dalam lingkungan multi-cloud, trade-off antara kekuatan proteksi dan efisiensi operasional menjadi indikator

keberhasilan implementasi yang krusial. Tabel 1 menyajikan sintesis data komparatif dari berbagai studi literatur primer.

Tabel 1. Analisis Perbandingan Mekanisme Keamanan Microservices pada Lingkungan Multi-Cloud

Parameter Evaluasi	**Service Mesh (mTLS)**	**API Gateway (OAuth2/JWT)**	**Zero Trust Architecture**
Metode Verifikasi	*Sertifikat per-layanan (mutual TLS)*	*Validasi token / klaim akses*	*Verifikasi identitas + kebijakan kontekstual berkelanjutan*
Cakupan Mitigasi Pergerakan Lateral	Tinggi: enkripsi & autentikasi di seluruh trafik internal	Sedang: hanya mengontrol titik masuk eksternal	Sangat Tinggi: penegakan kebijakan pada setiap permintaan, internal maupun eksternal
Overhead Komputasi	Sedang (beban tambahan pada sidecar proxy)	Rendah (validasi token bersifat ringan)	Tinggi (evaluasi kebijakan kontekstual berkelanjutan)
Kompleksitas Konfigurasi Lintas-Cloud	Sedang (perlu sinkronisasi sertifikat antar klaster)	Rendah hingga Sedang	Tinggi (perlu integrasi identity provider lintas-platform)
Latensi Komunikasi	Minimal hingga sedang	Minimal	Sedang (tergantung kecepatan evaluasi kebijakan)
Keandalan Skalabilitas	Baik untuk topologi layanan padat	Sangat baik untuk klien eksternal dalam jumlah besar	Baik, namun bergantung pada kematangan infrastruktur identitas

Analisis Trade-off Kompleksitas dan Skalabilitas

Data pada Tabel 1 menegaskan bahwa pemilihan mekanisme keamanan tidak boleh dilakukan secara seragam tanpa mempertimbangkan konteks. Permasalahan utama pada implementasi sebelumnya adalah penerapan Zero Trust murni pada seluruh lapisan komunikasi tanpa mempertimbangkan dampaknya terhadap latensi layanan yang sensitif terhadap waktu respons.

Hasil sintesis literatur menunjukkan bahwa kombinasi hibrida antara service mesh berbasis mTLS untuk komunikasi internal antar-layanan dengan penegakan kebijakan Zero Trust pada titik-titik kritis memberikan rasio efisiensi terbaik. Pendekatan ini mampu memberikan proteksi yang kuat terhadap pergerakan lateral tanpa membebani seluruh sistem dengan overhead evaluasi kebijakan kontekstual pada setiap permintaan, sehingga lebih sesuai untuk skala operasional multi-cloud yang besar dan heterogen.

Implikasi terhadap Stabilitas dan Keberlanjutan Migrasi

Secara lebih luas, mekanisme keamanan yang tepat secara implisit meningkatkan kelancaran proses migrasi itu sendiri. Dengan menerapkan verifikasi identitas sejak awal fase migrasi, organisasi dapat menghindari kondisi "lubang keamanan transisi" yang sering muncul ketika sistem legacy dan microservices baru berjalan berdampingan tanpa kebijakan akses yang konsisten. Hal ini menghasilkan proses migrasi yang lebih terkendali, mencegah insiden kebocoran data selama masa transisi, serta memastikan bahwa fondasi keamanan yang dibangun dapat terus diandalkan setelah sistem sepenuhnya berjalan pada arsitektur microservices multi-cloud.

V. PEMBAHASAN

Analisis komprehensif terhadap korpus literatur terkini menegaskan bahwa transisi strategi keamanan dari model perimeter statis menuju mekanisme verifikasi identitas yang adaptif merepresentasikan evolusi fundamental dalam mitigasi risiko pada ekosistem microservices multi-cloud. Temuan ini menunjukkan bahwa keamanan sistem terdistribusi tidak lagi dapat dipandang sebagai tanggung jawab eksklusif lapisan jaringan, melainkan tantangan manajemen identitas yang harus diselesaikan pada setiap titik komunikasi guna memecahkan masalah persisten mengenai kepercayaan implisit dan heterogenitas platform.

Mekanisme Adaptif dan Manajemen Identitas Berkelanjutan

Tinjauan sistematis mengungkap bahwa serangan yang canggih tidak dapat dimitigasi secara efektif hanya melalui kontrol akses statis pada titik masuk sistem, karena penyerang sering kali memanfaatkan layanan internal yang sah

namun lemah keamanannya untuk bergerak lebih jauh ke dalam sistem. Solusi yang robust memerlukan pendekatan verifikasi yang adaptif terhadap dinamika beban kerja, di mana setiap sesi komunikasi divalidasi berdasarkan parameter identitas dan konteks secara real-time.

Komparasi Kinerja Kecerdasan Komputasional

Analisis mendalam terhadap taksonomi mekanisme menyoroti peran krusial pendekatan berbasis kecerdasan komputasional dalam memecahkan kompleksitas pemilihan kebijakan keamanan yang optimal pada lingkungan multi-cloud yang dinamis.

1. **Deteksi Anomali Berbasis Pembelajaran Mesin:** Pendekatan ini menawarkan kemampuan mengidentifikasi pola komunikasi antar-layanan yang menyimpang dari perilaku normal, sehingga dapat mendeteksi indikasi pergerakan lateral pada tahap awal sebelum dampaknya meluas, tanpa memerlukan aturan statis yang kaku.
2. **Penilaian Kepercayaan Adaptif (Adaptive Trust Scoring):** Algoritma penilaian kepercayaan yang menyesuaikan tingkat akses berdasarkan riwayat perilaku dan konteks permintaan menunjukkan keunggulan dalam menyeimbangkan keamanan dengan pengalaman pengguna, meskipun menuntut investasi awal yang lebih tinggi pada infrastruktur pemantauan dan telemetri.

Evolusi Menuju Arsitektur Hibrida dan Skalabilitas

Salah satu temuan paling signifikan adalah munculnya tren arsitektur hibrida yang menggabungkan efisiensi service mesh dengan ketangguhan kebijakan Zero Trust sebagai solusi yang menjembatani kesenjangan antara responsivitas dan akurasi keamanan. Sinergi ini menghasilkan distribusi beban keamanan yang lebih homogen, memungkinkan ekspansi arsitektur microservices berskala masif lintas-cloud dengan tetap menjaga rasio overhead komunikasi yang terkendali.

Implikasi terhadap Desain Lintas-Cloud

Diskusi ini juga mengungkap interdependensi kritis antara efisiensi keamanan dengan parameter kualitas layanan lainnya pada konteks multi-cloud. Mekanisme keamanan yang mengoptimalkan verifikasi identitas secara implisit memperbaiki manajemen trafik dan menekan risiko gangguan layanan akibat permintaan yang tidak sah. Namun, kompleksitas operasional ini membawa tantangan baru terkait desain lintas-platform, di mana setiap penyedia cloud memiliki model identitas dan kebijakan jaringan yang berbeda. Hal ini menuntut arah penelitian masa depan untuk bergerak menuju pengembangan kerangka kerja identitas terfederasi yang cerdas, aman, dan dapat diinteroperasikan guna mendukung heterogenitas platform dalam ekosistem multi-cloud yang semakin kompleks.

VI. KESIMPULAN

Penelitian ini menyimpulkan bahwa keamanan migrasi dan operasional arsitektur microservices pada lingkungan multi-cloud sangat bergantung pada pergeseran paradigma dari model keamanan berbasis perimeter menuju verifikasi identitas yang berkelanjutan pada setiap titik komunikasi. Melalui tinjauan literatur sistematis, ditemukan bahwa kerentanan utama tidak hanya terletak pada titik masuk sistem, melainkan pada asumsi kepercayaan implisit antar-layanan internal yang memungkinkan pergerakan lateral ketika satu komponen berhasil dikompromikan.

Berdasarkan perbandingan teknis, kombinasi hibrida antara service mesh berbasis mTLS untuk komunikasi internal dengan penegakan kebijakan Zero Trust pada titik-titik akses kritis teridentifikasi sebagai pendekatan paling efisien untuk skenario multi-cloud berskala besar. Pendekatan ini mampu memberikan tingkat proteksi yang setara dengan penerapan Zero Trust penuh, namun dengan beban operasional dan latensi yang jauh lebih terkendali.

Analisis ini juga menunjukkan bahwa meskipun API gateway berbasis token menawarkan kesederhanaan dan efisiensi komputasi yang tinggi untuk mengontrol akses eksternal, penerapannya secara tunggal tanpa pelengkap mekanisme keamanan internal masih menyisakan celah terhadap ancaman yang berasal dari dalam ekosistem layanan itu sendiri. Oleh karena itu, arsitektur berlapis yang mengombinasikan kontrol pada titik masuk dengan verifikasi berkelanjutan pada komunikasi internal muncul sebagai arah yang lebih menjanjikan.

Secara operasional, penguatan mekanisme keamanan semacam ini terbukti meningkatkan kelancaran proses migrasi itu sendiri, karena verifikasi identitas yang konsisten sejak awal fase transisi mencegah munculnya "lubang keamanan transisi" antara sistem legacy dan layanan microservices yang baru dibangun.

Sebagai penutup, tantangan utama di masa depan terletak pada pengembangan kerangka kerja identitas terfederasi yang mampu beroperasi secara konsisten lintas-penyedia cloud. Penelitian selanjutnya disarankan untuk mengeksplorasi integrasi deteksi anomali berbasis pembelajaran mesin pada lapisan service mesh guna mendeteksi indikasi pergerakan lateral secara real-time, demi menjamin keberlanjutan infrastruktur digital generasi mendatang.

Kontribusi Penulis: [Radhitya Dwi Akmal Purnomo]: Konseptualisasi, Metodologi, Penulisan Draf Awal, Penyuntingan, Supervisi. Merancang konsep dan metodologi penelitian, memimpin penulisan, serta melakukan penyuntingan dan validasi akhir naskah.
[Giovani Sapta Purnama A.]: Investigasi, Kurasi Data. Melakukan pengumpulan dan pengolahan data literatur serta penyusunan tabel hasil penelitian.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.
Ketersediaan Data: -
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.
Penulis Pertama: https: -
Penulis Kedua: https: -

REFERENCES

[1] A. D. Boursianis *et al*., "Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review," *Internet of Things (Netherlands)*, vol. 18, no. xxxx, p. 100187, 2022, doi: 10.1016/j.iot.2020.100187.

[2] Fauzan Prasetyo Eka Putra, Maktsuful Ghummah, Moh. Amrullah, and Rafli Hidayatullah, "Studi Kinerja Mesh Network untuk Penerapan Internet of Things (IoT) di Lingkungan Perkotaan," *J. Inform. Dan Tekonologi Komput.*, vol. 5, no. 1, pp. 63–73, 2025, doi: 10.55606/jitek.v5i1.5895.

[3] K. L. G. Snider, R. Shandler, S. Zandani, and D. Canetti, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," *J. Cybersecurity*, vol. 7, no. 1, pp. 1–11, 2021, doi: 10.1093/cybsec/tyab019.

[4] A. Bagus Prakoso, M. Anugrah Putra, M. Hanif Hilmi, S. Yoma Patria Risky, and J. Maulindar, "Penerapan Algoritma Regresi Random Forest Untuk Prediksi Produksi Jagung Menggunakan Data Statistik Sistem Pertanian Cerdas Smart City," *Pros. Semin. Nas. Teknol. Inf. dan Bisnis*, pp. 28–33, 2025, doi: 10.47701/19h5ny78.

[5] S. R. Jena, R. Shanmugam, K. Saini, and S. Kumar, "Cloud Computing Tools: Inside Views and Analysis," *Procedia Comput. Sci.*, vol. 173, no. 2019, pp. 382–391, 2020, doi: 10.1016/j.procs.2020.06.045.

[6] A. F. Rachman, F. P. E. Putra, S. Syirofi, and D. Wahid, "Case Study of Computer Network Development for the Internet Of Things (IoT) Industry in an Urban Environment," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 399–407, 2024, doi: 10.47709/brilliance.v4i1.4302.

[7] M. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian J. CyberSecurity*, vol. 2023, no. 1, pp. 57–63, 2023, doi: 10.58496/MJCS/2023/010.

[8] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Increasing cybersecurity investments in private sector firms," *J. Cybersecurity*, vol. 1, no. 1, pp. 3–17, 2015, doi: 10.1093/cybsec/tyv011.

[9] R. D. Gunawan, F. Ariany, and N. Novriyadi, "Implementasi Metode SAW Dalam Sistem Pendukung Keputusan Pemilihan Plano Kertas," *J. Artif. Intell. Technol. Inf.*, vol. 1, no. 1, pp. 29–38, 2023, doi: 10.58602/jaiti.v1i1.23.

[10] R. A. Prasetyo, "Mengoptimalkan Irigasi Pertanian Cerdas Melalui Internet of Multimedia Things (IoMT) dengan Deteksi Kebutuhan Air Tanaman Berbasis Deep Learning," *J. Inform.*, vol. 11, no. 1, pp. 1–10, 2020, [Online]. Available: https://www.researchgate.net/publication/376415558

[11] F. P. E. Putra, U. Ubaidi, R. N. Saputra, F. M. Haris, and S. N. R. Barokah, "Application of Internet of Things Technology in Monitoring Water Quality in Fishponds," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 356–361, 2024, doi: 10.47709/brilliance.v4i1.4231.

[12] B. Nofrianti, R. S. Hadikusuma, and L. Nurpulaela, "Implementasi Antena Wajanbolic Sebagai Penguat Sinyal Untuk Konsep Pertanian Cerdas Di Pasaman Sumatera Barat Implementation of Wokbolic Antenna As Signal Amplifier for Smart Agriculture Concept in Pasaman, West Sumatera," *Univ. Bunda Mulia*, vol. 6, no. 2, pp. 1049–1059, 2021, [Online]. Available: https://doi.org/10.25124/jett.v8i2.4210

[13] P. Asnur, R. Apriyanti, D. Hertinsyana, V. Widi Prabawasari, T. Yuni Gunarto, and B. Haryadi, "Implementasi Pertanian Cerdas Berbasis Internet of Things Di Desa Wisata Mucila-Munjul, Jakarta Timur Implementation of a Smart Farm Based on the Internet of Things in the Village of Wisata Mucila-Munjul, East Jakarta," *J. Pengabdi. Kpd. Masy.*, vol. 4, pp. 1–7, 2024.

[14] M. F. P. Nugraha, M. Sudiarsa, and E. Y. Setyono, "Analisis Optimasi Waktu Dan Biaya Proyek DenganPenambahan Sumber Daya Menggunakan Metode Time Cost Trade Off," *Jur. Tek. Sipil-PNB*, vol. 2, pp. 235–244, 2023.

[15] F. P. E. Putra, M. A. Mahmud, and I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 996–1001, 2024, doi: 10.47709/digitech.v3i2.3457.
[16] N. Rahmansyah and S. A. Lusinia, *Buku Ajar Sistem Pendukung Keputusan*. 2016. doi: 10.1063/1.1935433.
[17] S. Savaş and S. Karataş, "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance," *Int. Cybersecurity Law Rev.*, vol. 3, no. 1, pp. 7–34, 2022, doi: 10.1365/s43439-021-00045-4.
[18] M. Bravetti *et al.*, "A Formal Approach to Microservice Architecture Deployment * To cite this version : HAL Id : hal-03077047 A Formal Approach to Microservice Architecture Deployment ∗ ," 2020.
[19] G. De Palma, S. Giallorenzo, M. Trentin, and · Gejsi Vjerdha, "A Framework for Bridging the Gap between Monolithic and Serverless Programming," 2023, [Online]. Available: https://www.github.com/Gejsi/fenrir.
[20] E. Bobrov *et al.*, "DevOps and its philosophy: Education matters!," *Microservices Sci. Eng.*, pp. 349–361, 2019, doi: 10.1007/978-3-030-31646-4_14.
[21] H. Song, F. Chauvel, and P. H. Nguyen, "Using microservices to customize multi-tenant software-as-a-service," *Microservices Sci. Eng.*, no. 1, pp. 299–331, 2019, doi: 10.1007/978-3-030-31646-4_12.
[22] L. Wang and J. Zhao, *Architecture of advanced numerical analysis systems: Designing a scientific computing system using OCaml*. 2022. doi: 10.1007/978-1-4842-8853-5.
[23] B. Benson and G. Dorai, "Grey Areas of Digital Forensic Tools and a Framework to Solve the IoT Data Forensic Analysis Problems," pp. 1–4.
[24] D. Taibi, V. Lenarduzzi, and C. Pahl, "Microservices Anti-Patterns : A Taxonomy".
[25] M. Mazzara, A. Bucchiarone, N. Dragoni, and V. Rivera, "Size matters: Microservices research and applications," *Microservices Sci. Eng.*, pp. 29–42, 2019, doi: 10.1007/978-3-030-31646-4_2.
[26] H. Monfleur *et al.*, "Towards Concern-Oriented Microservice Architecture To cite this version : HAL Id : hal-04201189 Towards Concern-Oriented Microservice Architecture," 2023.
[27] F. Jrad, J. Tao, and A. Streit, "A broker-based framework for multi-cloud workflows," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 61–68, 2013, doi: 10.1145/2462326.2462339.
[28] S. S. Gill, "A Manifesto for Modern Fog and Edge Computing: Vision, New Paradigms, Opportunities, and Future Directions," *EAI/Springer Innov. Commun. Comput.*, no. 2022, pp. 237–253, 2022, doi: 10.1007/978-3-030-74402-1_13.
[29] K. Jeffery, G. Horn, and L. Schubert, "A vision for better cloud applications," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, no. 3, pp. 7–12, 2013, doi: 10.1145/2462326.2462329.
[30] C. Canali and R. Lancellotti, "Automatic Virtual Machine Clustering based on Bhattacharyya Distance for Multi-Cloud Systems," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 45–52, 2013, doi: 10.1145/2462326.2462337.
[31] G. Baryannis *et al.*, "Lifecycle management of service-based applications on multi-clouds: A research roadmap," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 13–20, 2013, doi: 10.1145/2462326.2462331.
[32] A. kumar Polinati, "Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments," *Cornell Univ.*, pp. 1–24, 2025.
[33] F. Paraiso, P. Merle, and L. Seinturier, "Managing elasticity across multiple cloud providers," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 53–60, 2013, doi: 10.1145/2462326.2462338.
[34] A. Gunka, S. Seycek, and H. Kühn, "Moving an application to the cloud - An evolutionary approach," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 35–42, 2013, doi: 10.1145/2462326.2462334.
[35] D. Petcu, "Multi-cloud: Expectations and current approaches," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 1–6, 2013, doi: 10.1145/2462326.2462328.
[36] D. Franceschelli, D. Ardagna, M. Ciavotta, and E. Di Nitto, "SPACE4CLOUD: A tool for system performance and cost evaluation of CLOUD systems," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 27–34, 2013, doi: 10.1145/2462326.2462333.
[37] P. Bar *et al.*, "Towards a monitoring feedback loop for cloud applications," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 43–44, 2013, doi: 10.1145/2462326.2462336.
[38] C. Quinton, N. Haderer, R. Rouvoy, and L. Duchien, "Towards multi-cloud configurations using feature models and ontologies," *MultiCloud 2013 - Proc. Int. Work. Multi-Cloud Appl. Fed. Clouds*, pp. 21–26, 2013, doi: 10.1145/2462326.2462332.
[39] K. Delbene, M. Medin, and R. Murray, "The Road to Zero Trust (Security)," *Def. Innov. Board*, pp. 1–10, 2019, [Online]. Available: https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF
[40] S. Rose, "Planning for a Zero Trust Architecture," no. December, 2022, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf
[41] J. Uddoh, D. Ajiga, B. Okare, T. A.-J. Z. T. Bank, and undefined 2022, "Zero trust architecture models for preventing insider attacks and enhancing digital resilience in banking systems," *Gisrrj.Com*, vol. 5, no. 4, pp. 213–230, 2022, [Online]. Available: https://gisrrj.com/paper/GISRRJ225417.pdf
[42] M. M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 18–21, 2023, doi: 10.58496/MJCS/2023/004.