JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Kerangka Konseptual Keamanan Layanan Sistem dalam Ekosistem Platform Digital Multilapis

Fadli Dalimunthe[1*], Arif Maulana[2], Muhammad Partua Langka Situmeang[3], Muhammad Rasyya Alfarisi [4], Jakbar Ali Harahap[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]fadli.240170145@mhs.unimal.ac.id, [2]arif.240170147@mhs.unimal.ac.id, [3]muhammad.240170139@mhs.unimal.ac.id, [4]muhammad.240170151@mhs.unimal.ac.id, [5]jakbar.240170165@mhs.unimal.ac.id

ABSTRACT

The rapid growth of digital services and API utilization in multi-layered platform ecosystems has expanded attack surfaces, increasing systemic security risks. Traditional security approaches focusing on individual components are insufficient to address cross-layer vulnerabilities, especially in cloud-native, microservices-based architectures. This study aims to develop a holistic conceptual framework for system service security in multi-layered digital platforms by identifying key layers, analyzing interdependencies, and mapping risks and controls across infrastructure, platform/middleware, applications, and governance layers. Using a qualitative literature review of publications since 2020, thematic and conceptual analyses were conducted to synthesize existing technical and governance practices. The proposed framework integrates defense-in-depth mechanisms, including network segmentation, API hardening, service mesh with mutual TLS, secure software development lifecycle, identity and access management, and governance policies, highlighting cross-layer dependencies and systemic risk propagation. Additionally, it addresses the trade-off between security and system performance, proposing adaptive and contextual strategies such as lightweight cryptography, selective protection, and orchestrated controls. The results suggest that security must be designed end-to-end, considering technical, operational, and governance dimensions, to ensure resilience, service availability, and user trust in complex digital platform ecosystems. This framework provides a theoretical and practical reference for designing robust, adaptive, and measurable security architectures.

Keywords:
Multi-layered security, digital platforms, API security, governance, defense-in-depth

PENDAHULUAN

Pertumbuhan pesat layanan digital dan penggunaan API dalam ekosistem platform multilapis memperluas permukaan serangan dan meningkatkan ancaman terhadap keamanan sistem. Menurut laporan *State of the Internet* 2025 serangan terhadap aplikasi web mencapai 311 miliar insiden di 2024, meningkat 33 % dibandingkan tahun sebelumnya, dan serangan terhadap API mencapai 150 miliar antara Januari 2023 hingga Desember 2024, menunjukkan bahwa API telah menjadi target utama dalam lanskap serangan modern (Akamai, 2025). Laporan lain, *State of WAAP Report* 2024 dari CDNetworks melaporkan bahwa platformnya menghadang 887,4 miliar serangan web dan API pada 2024, bertambah 21,4 % dari 2023, sekaligus mencatat lonjakan tajam pada serangan DDoS di tingkat terabit yang berdampak pada ketersediaan layanan (Newswire, 2025). Tren ini mencerminkan bahwa dalam ekosistem platform digital multilapis yang melibatkan komponen infrastruktur, platform inti, layanan/aplikasi, data, dan pengguna kompleksitas sistem dan ketergantungan antarlapisan tidak hanya meningkat, tetapi juga menciptakan tantangan keamanan yang lebih besar karena gangguan pada satu lapisan mudah merembet ke lapisan lain, sehingga memperkuat urgensi pendekatan keamanan lintas-lapisan yang komprehensif.

Ekosistem platform digital modern memiliki karakteristik multilapis yang mencakup infrastruktur komputasi, platform inti, layanan atau aplikasi berbasis API, pengelolaan data, dan interaksi pengguna yang saling terhubung untuk menciptakan nilai dalam skala besar (Hein et al., 2020). Arsitektur berbasis *cloud* dan *microservices* meningkatkan fleksibilitas dan skalabilitas sistem, tetapi secara bersamaan memperbesar kompleksitas dan ketergantungan antarlapisan sehingga kegagalan atau kerentanan pada satu komponen dapat memengaruhi lapisan lain (Qazi, 2023). Kondisi ini berdampak langsung pada keamanan layanan sistem karena serangan siber semakin menargetkan titik integrasi seperti API dan rantai pasok perangkat lunak yang menyebabkan insiden keamanan bersifat lintas lapisan dan sulit ditangani dengan pendekatan keamanan parsial (Alenezi, 2023).

Keamanan layanan sistem memegang peran kunci dalam menjaga keandalan, ketersediaan, dan kepercayaan pengguna dalam ekosistem platform digital karena gangguan keamanan secara langsung berdampak pada kontinuitas layanan dan persepsi pengguna terhadap platform. Adopsi *cloud computing*, arsitektur *microservices*, API terbuka, dan integrasi pihak ketiga secara signifikan memperluas *attack surface* sehingga meningkatkan potensi eksploitasi melalui titik integrasi antarlayanan (Qazi, 2023). Kondisi ini menyebabkan keamanan tidak lagi dapat dipandang sebagai isu

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

teknis pada satu komponen karena kegagalan pada satu lapisan seperti kebocoran API atau kompromi layanan pihak ketiga dapat merambat ke lapisan lain dan mengganggu keseluruhan ekosistem platform, termasuk akses data, ketersediaan aplikasi, dan kepercayaan pengguna (Hein et al., 2020). Oleh karena itu, literatur keamanan sistem menekankan perlunya pendekatan keamanan layanan yang bersifat lintas lapisan dan terintegrasi untuk memastikan stabilitas dan keberlanjutan platform digital multilapis.

Penelitian sebelumnya dalam bidang keamanan sistem digital cenderung bersifat parsial dengan fokus pada komponen tertentu seperti keamanan cloud, keamanan microservices, atau API tanpa menggabungkannya dalam satu kerangka keamanan holistik. Misalnya, studi sistematis terhadap keamanan microservices menunjukkan bahwa meskipun ada banyak publikasi yang membahas ancaman dan solusi spesifik. Masih terdapat *gap* signifikan dalam model dan standar keamanan yang dirancang khusus untuk arsitektur microservices yang kompleks dan terdistribusi (Hutasuhut et al., 2024). Demikian pula, tinjauan terhadap layanan *cloud native* menegaskan bahwa fokus penelitian sering kali bertumpu pada aspek tertentu seperti keamanan container atau orkestrasi. Sementara interaksi antar-komponen cloud-native yang kompleks belum terintegrasi secara menyeluruh dalam literatur keamanan yang ada (Theodoropoulos et al., 2023). Pendekatan terpisah tersebut memperlihatkan keterbatasan dalam menangani ketergantungan antarlapisan pada ekosistem digital modern, karena model keamanan tradisional yang terfokus pada satu lapisan tidak memadai untuk mengantisipasi efek rantai (*ripple effects*) dari kerentanan pada platform multilapis. Akibatnya, masih minim penelitian yang menawarkan kerangka konseptual keamanan yang holistik dan lintas lapisan untuk platform digital multilapis, yang mampu mengintegrasikan kontrol keamanan mulai dari infrastruktur cloud hingga lapisan aplikasi dan integrasi pihak ketiga secara serentak.

Kompleksitas arsitektur platform digital multilapis menimbulkan tantangan dalam pengelolaan keamanan layanan sistem karena setiap lapisan memiliki risiko dan mekanisme pengamanan yang berbeda serta saling bergantung. Sementara pendekatan keamanan yang diterapkan selama ini masih cenderung parsial dan tidak terintegrasi. Kondisi tersebut memperbesar potensi celah keamanan khususnya pada titik interaksi antarlapisan sehingga keamanan layanan sistem tidak dapat dicapai secara efektif apabila hanya berfokus pada satu lapisan sistem. Penelitian ini berangkat dari asumsi bahwa pendekatan keamanan lintas lapisan diperlukan untuk mengelola risiko keamanan secara menyeluruh dalam ekosistem platform digital multilapis. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi lapisan dan komponen kunci yang memengaruhi keamanan layanan sistem, menganalisis pengaruh interaksi antarlapisan terhadap risiko dan kerentanan keamanan, serta menyusun kerangka konseptual keamanan layanan sistem yang holistik. Sejalan dengan tujuan tersebut, pertanyaan penelitian difokuskan pada lapisan apa saja yang berperan penting dalam keamanan layanan sistem platform digital multilapis, bagaimana interaksi antarlapisan memengaruhi risiko keamanan, dan elemen apa yang perlu dimasukkan dalam kerangka konseptual keamanan layanan sistem yang terintegrasi.

KAJIAN LITERATUR

Ekosistem Platform Digital Multilapis

Ekosistem platform digital multilapis merupakan struktur kompleks yang menggabungkan berbagai aktor dan komponen teknologi untuk menciptakan nilai melalui interaksi bersama, berbeda dengan model bisnis tradisional yang terbatas pada hubungan satu-arah yakni platform digital memfasilitasi co-creation antara penyedia, mitra, dan pengguna sehingga membentuk suatu *ecosystem of autonomous agents* yang saling bergantung dalam menciptakan layanan dan nilai tambah secara bersama-sama (Hein et al., 2020). Karakteristik ini terlihat dari sifat multilapisnya, di mana lapisan infrastruktur teknologi, platform inti, layanan/aplikasi, data, dan pengguna saling terhubung melalui interaksi digital yang intens, sehingga perubahan atau inovasi pada satu lapisan dapat memengaruhi capaian dan fungsi lapisan lainnya (Hein et al., 2020). Interaksi antarlapisan tersebut juga ditemukan dalam literatur yang menekankan pentingnya integrasi sumber daya dan kapabilitas pada berbagai tingkatan mikro, meso, dan makro untuk menghasilkan nilai yang lebih besar dan mendukung pertumbuhan performa keseluruhan dalam ekosistem digital, termasuk pada konteks penggabungan teknologi digital, kolaborasi rantai pasok, serta keterlibatan pengguna secara menyeluruh (Peng et al., 2023). Bukti empiris keterkaitan antarlapisan dan kompleksitas ekosistem ini juga diakui dalam kajian tata kelola platform digital, yang menunjukkan bahwa pemahaman komponen struktural seperti koordinasi antaraktor, peran fasilitator platform, serta hubungan teknis antara modul layanan menjadi kunci dalam desain dan pengelolaan ekosistem yang efektif (Costabile, 2024).

Keamanan Layanan Sistem pada Platform Digital

Keamanan layanan sistem pada platform digital mencakup tiga dimensi utama kerahasiaan, integritas, dan ketersediaan yang menjadi prasyarat agar layanan berjalan andal dan membangun kepercayaan pengguna; literatur menegaskan bahwa pelanggaran terhadap salah satu dimensi ini berdampak langsung pada kualitas layanan dan reputasi platform (Cremer et al., 2022a). Arsitektur modern berbasis microservices dan API menuntut kontrol keamanan terdistribusi karena setiap layanan kecil memproses data dan menyediakan fungsi yang saling bergantung; oleh karena

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

itu mekanisme otentikasi, otorisasi, dan proteksi komunikasi perlu diimplementasikan pada tingkat layanan untuk menjaga CIA secara end-to-end (Berardi et al., 2022). Bukti empiris menunjukkan bahwa insiden keamanan termasuk kebocoran data dan gangguan ketersediaan mengakibatkan penurunan kinerja bisnis dan nilai perusahaan serta downtime layanan yang signifikan; studi longitudinal menemukan efek negatif jangka panjang pada nilai perusahaan setelah pengumuman pelanggaran keamanan, yang mencerminkan konsekuensi ekonomi dan operasional dari kegagalan pengamanan layanan (S. E. A. Ali et al., 2021). Oleh karena itu, penelitian konsisten merekomendasikan pendekatan keamanan yang menggabungkan kontrol teknis di tingkat layanan dengan tata kelola risiko dan manajemen dependensi antar-layanan untuk mempertahankan keandalan dan kepercayaan pengguna pada platform digital multilapis (Cremer et al., 2022b).

Ancaman dan Risiko Keamanan dalam Arsitektur Multilapis

Ancaman dan risiko keamanan dalam arsitektur multilapis platform digital meningkat seiring adopsi *cloud computing, microservices*, API, dan integrasi pihak ketiga karena karakteristik distribusi dan dependensi layanan menciptakan perluasan *attack surface* yang lebih besar dibandingkan arsitektur monolitik. Hal ini terjadi karena setiap layanan microservice berkomunikasi melalui API dan bergantung pada komponen jaringan, autentikasi, serta orchestrator cloud, sehingga setiap celah atau kesalahan konfigurasi dapat dimanfaatkan oleh aktor ancaman untuk menembus sistem yang lebih luas (Oluwatobiloba, 2025). Pendekatan empiris terhadap praktik keamanan microservices menunjukkan bahwa rangkaian tantangan keamanan tidak terbatas pada satu lapisan saja, melainkan terkait dengan komunikasi antar-service, otorisasi dan autentikasi, token management, serta keamanan lingkungan runtime yang rentan terhadap kesalahan desain dan implementasi, yang jika tidak ditangani dapat menghasilkan kerentanan signifikan dalam konteks keamanan keseluruhan sistem multilapis (R. N. Ali et al., 2022. *Attack surface* yang diperluas ini meningkatkan risiko kegagalan keamanan lintas lapisan, di mana eksposur API yang tidak aman dan interaksi antar layanan yang tidak terlindungi merupakan vektor utama bagi eksploitasi seperti *insecure inter-service communications* dan ancaman terhadap container atau orkestrasi microservices, yang berdampak pada integritas dan ketersediaan layanan dalam seluruh ekosistem platform digital modern.

Pendekatan Keamanan dan Keterbatasan Penelitian Terdahulu

Penelitian keamanan pada platform digital sering bersifat parsial, berfokus pada aspek tertentu seperti keamanan microservices, proteksi API, atau keamanan rantai pasok perangkat lunak sehingga sedikit yang mengusulkan model yang mengintegrasikan kontrol di semua lapisan ekosistem multilapis. Studi empiris terhadap praktik keamanan microservices menyoroti banyak isu implementasi dan praktik yang belum matang, survei tentang keamanan layanan *cloud-native* menunjukkan fokus terfragmentasi pada komponen seperti container, orkestrator, dan jaringan tanpa kerangka lintas-lapisan yang komprehensif dan kajian tentang serangan rantai pasok mengilustrasikan bagaimana vektor-vektor yang mengeksploitasi dependensi pihak ketiga dapat memicu dampak berantai di banyak lapisan sekaligus (Ohm & Stuke, 2023). Kondisi ini menandai gap penelitian yang jelas: perlu pengembangan kerangka konseptual keamanan holistik yang memetakan risiko, titik kontrol, dan mekanisme mitigasi secara terkoordinasi antar-lapisan dalam ekosistem platform digital multilapis.

Kerangka Konseptual Keamanan Layanan Sistem

Kerangka konseptual berperan penting dalam penelitian keamanan layanan sistem karena membantu memetakan hubungan antar komponen dan mengidentifikasi risiko keamanan secara sistematis pada arsitektur platform digital yang kompleks. Dalam ekosistem platform digital multilapis, kerangka konseptual mengintegrasikan lapisan infrastruktur, layanan berbasis microservices dan API, serta aliran data sebagai satu kesatuan yang saling bergantung, sehingga kegagalan keamanan pada satu lapisan dapat dipahami dampaknya terhadap lapisan lain. Literatur menunjukkan bahwa sebagian besar penelitian sebelumnya masih memfokuskan keamanan pada komponen tertentu, seperti container atau microservices secara terpisah, tanpa pendekatan lintas lapisan yang holistik, sehingga diperlukan kerangka konseptual yang mampu menjembatani keterbatasan tersebut dan memberikan pandangan menyeluruh terhadap keamanan layanan sistem (Theodoropoulos et al., 2023).

METODE PENELITIAN

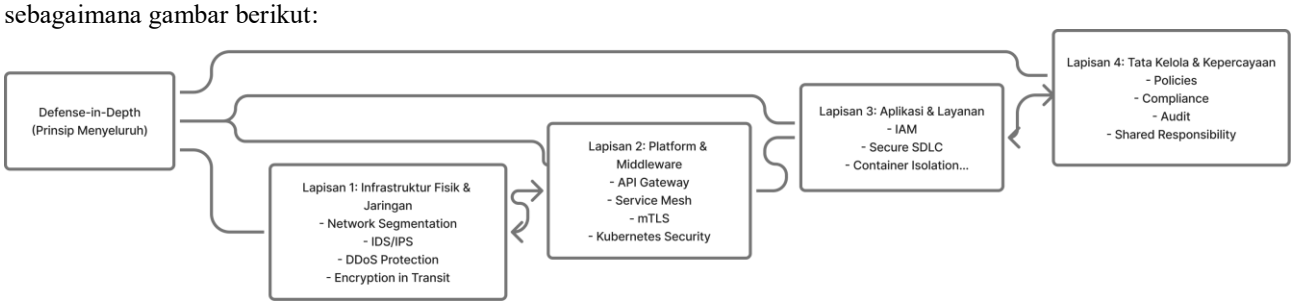
Penelitian ini menggunakan pendekatan kualitatif dengan desain studi literatur untuk menyusun kerangka konseptual keamanan layanan sistem dalam ekosistem platform digital multilapis. Ruang lingkup penelitian difokuskan pada kajian konsep dan temuan empiris terkait keamanan layanan sistem, platform digital, dan arsitektur multilapis yang dipublikasikan dalam jurnal nasional dan internasional. Objek penelitian berupa artikel ilmiah yang diperoleh dari basis data akademik bereputasi dengan teknik pengumpulan data melalui penelusuran dan seleksi literatur berdasarkan kriteria relevansi. Keamanan layanan sistem didefinisikan secara operasional melalui dimensi kerahasiaan, integritas,

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

dan ketersediaan, sedangkan ekosistem platform digital multilapis mencakup lapisan infrastruktur, platform inti, layanan/aplikasi, data, dan pengguna. Analisis data dilakukan melalui analisis tematik dan sintesis konseptual untuk mengidentifikasi hubungan antarlapisan, risiko keamanan, serta mekanisme pengendalian yang selanjutnya dirumuskan dalam kerangka konseptual penelitian.

HASIL DAN PEMBAHASAN

Keamanan platform digital tidak dapat dipahami secara parsial melainkan harus dianalisis melalui pendekatan berlapis yang mencakup aspek teknis, operasional, dan tata kelola. Pendekatan keamanan multilapis (*multi-layered security/defense-in-depth*) diakui secara luas dalam literatur keamanan siber sebagai strategi fundamental untuk menghadapi ancaman kompleks di platform digital. Model ini menempatkan serangkaian kontrol dan mekanisme di berbagai titik arsitektur sistem daripada bergantung pada satu titik tunggal saja. Pendekatan ini penting karena setiap lapisan memiliki vektor risiko yang unik dan hanya kombinasi kontrol berlapis yang dapat memberikan perlindungan menyeluruh terhadap ancaman mutakhir. Kerangka konseptual yang diusulkan terdiri atas empat lapisan utama sebagaimana gambar berikut:



Gambar 1. Kerangka Konseptual Keamanan Multilapis pada Ekosistem Platform Digital

Diagram ini memvisualisasikan pendekatan keamanan end-to-end berbasis prinsip *defense-in-depth* yang mencakup lapisan infrastruktur, platform, aplikasi, dan tata kelola. Panah dua arah menunjukkan interdependensi antar-lapisan, di mana kelemahan pada satu lapisan dapat berdampak sistemik terhadap lapisan lainnya. Berikut adalah rincian dari lapisan tersebut:

1. lapisan infrastruktur fisik dan jaringan

Pada tingkat tersebut, ancaman meliputi serangan DoS/DDoS, eksploitasi jaringan, dan insiden pada perangkat fisik atau host. Penerapan segmen jaringan, protokol proteksi, serta sistem deteksi intrusi adalah elemen penting. Implementasi mekanisme seperti segmentasi jaringan, enkripsi trafik, dan proteksi terhadap serangan terdistribusi adalah contoh kontrol di lapisan ini. Analisis keamanan pada infrastruktur menunjukkan bahwa kerentanan di bagian ini dapat menyebabkan dampak sistemik yang luas, termasuk pelanggaran layanan atau penyalahgunaan sumber daya komputasi. Oleh karena itu, kontrol teknis di lapisan ini menjadi fondasi dari keseluruhan model keamanan multilapis.

2. lapisan platform dan middleware

Middleware dan komponen platform digital seperti API gateway dan orkestrator layanan termasuk Kubernetes atau service mesh memiliki peran krusial dalam pertukaran antar komponen aplikasi serta manajemen sumber daya. Penelitian di lingkungan microservices dan middleware menegaskan bahwa risiko pada lapisan ini terkait dengan pengelolaan API, autentikasi dan otorisasi antar-layanan, dan orkestrasi container yang rentan jika tidak dilindungi dengan baik . Kontrol seperti penggunaan Service Mesh dengan mTLS, API Gateway yang di-hardening, dan DevSecOps pipeline direkomendasikan untuk meningkatkan dasar keamanan.

3. lapisan aplikasi dan layanan

Lapisan aplikasi merupakan tempat fungsi bisnis dieksekusi di mana risiko terhadap data sensitif, sesi pengguna, atau integrasi pihak ketiga menjadi sangat nyata. Literatur keamanan aplikasi modern menyoroti peran autentikasi kuat, pengelolaan identitas, serta pipeline keamanan selama Siklus Hidup Pengembangan Perangkat Lunak (Secure SDLC) untuk meminimalkan celah di level ini. Contoh kontrol teknis pada lapisan ini adalah penggunaan microservices yang terisolasi melalui kontainer, implementasi mutual TLS (mTLS), serta layanan manajemen identitas dan akses terpusat. Studi keamanan cloud-native menggarisbawahi bahwa otomatisasi keamanan pada level aplikasi seperti pengujian kontinyu dan monitoring runtime mengurangi kemungkinan eksploitasi kesalahan konfigurasional atau kerentanan aplikasi .

4. lapisan tata kelola dan kepercayaan.

Pendekatan multilapis tidak hanya melibatkan kontrol teknis, tetapi juga elemen governance seperti kebijakan, kepatuhan, audit, serta model tanggung jawab bersama (shared responsibility). Penelitian nasional menunjukkan bahwa model tata kelola keamanan yang terintegrasi membantu organisasi membangun sistem keamanan yang tangguh,

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

adaptif, dan berkelanjutan, yang mampu memenuhi kebutuhan aspek operasional sekaligus menjaga kepercayaan pemangku kepentingan (Lestari et al., 2025). Model governance mencakup standar, prosedur operasional, dan struktur organisasi yang jelas untuk mengatasi ancaman, dan audit berkala untuk memastikan efektivitas pengendalian keamanan yang telah diterapkan di berbagai lapisan.

Setiap lapisan memiliki karakteristik risiko, ancaman, dan mekanisme pengendalian keamanan yang berbeda, tetapi saling bergantung satu sama lain. Tabel pemetaan lapisan keamanan, risiko, dan mekanisme pengendalian dapata dilihat pada tabel berikut:

Tabel 1. Pemetaan Lapisan Keamanan, Risiko, dan Mekanisme Pengendalian

Lapisan	Ancaman Utama	Risiko Dominan	Kontrol Keamanan Kunci
Infrastruktur	DDoS, sniffing, host compromise	Service outage, data leakage	Network segmentation, IDS/IPS, TLS
Platform and Middleware	API abuse, misconfiguration	Privilege escalation	API gateway, mTLS, service mesh
Aplikasi and Layanan	Injection, identity theft	Data breach	IAM, Secure SDLC, container isolation
Tata Kelola	Ambiguous responsibility	Compliance failure	Policies, audit, shared responsibility

Kelemahan pada satu lapisan berpotensi menimbulkan dampak sistemik terhadap lapisan lainnya sehingga diperlukan pendekatan keamanan yang terintegrasi. Pada lapisan infrastruktur, isu utama yang teridentifikasi meliputi keamanan jaringan, proteksi terhadap serangan terdistribusi, serta perlindungan data dalam transmisi. Lapisan platform dan middleware menyoroti risiko pada pengelolaan API, orkestrasi layanan, serta autentikasi dan otorisasi antar-layanan. Sementara itu, pada lapisan aplikasi dan layanan, tantangan utama berkaitan dengan pengelolaan identitas pengguna, keamanan siklus pengembangan perangkat lunak, serta integrasi layanan pihak ketiga. Lapisan tata kelola berfungsi sebagai pengikat seluruh lapisan teknis melalui kebijakan, standar, mekanisme audit, dan model tanggung jawab bersama. Pendekatan yang hanya memfokuskan satu lapisan saja cenderung mengabaikan hubungan kompleks antar komponen sistem dan berpotensi menyebabkan "siloed security" yang tidak mampu menghadapi ancaman lintas-lapisan. Literatur multilapis menggarisbawahi bahwa strategi seperti *Defense-in-Depth* (DiD) mensyaratkan adanya koordinasi kontrol teknis, proses operasional, dan kebijakan tata kelola secara bersamaan untuk mencapai ketahanan sistem yang optimal.

Keamanan sebagai Sistem Multilapis dalam Ekosistem Platform Digital

Kerangka konseptual yang diusulkan dalam penelitian ini berangkat dari integrasi dua arus utama literatur, yakni teori platform dan ekosistem digital serta literatur teknis keamanan sistem multilapis. Dalam perspektif teori platform, platform digital dipahami bukan sekadar artefak teknologi, melainkan sebagai sistem berlapis yang mencakup abstraksi teknis, tata kelola, serta interaksi dan keterlibatan aktor (Hund et al., 2021). Pandangan ini menempatkan platform sebagai struktur hierarkis di mana setiap lapisan memiliki fungsi, kepentingan, dan mekanisme koordinasi yang berbeda, namun saling memengaruhi. Sejalan dengan temuan, (Autio et al., 2017) dan (Jovanovic et al., 2022) menegaskan bahwa keberhasilan dan keberlanjutan platform sangat ditentukan oleh keselarasan antara arsitektur teknologi, desain layanan, dan mekanisme tata kelola. Temuan tersebut memperkuat argumentasi bahwa keamanan platform tidak dapat direduksi menjadi persoalan teknis semata, melainkan harus diposisikan sebagai isu sistemik yang melibatkan keputusan arsitektural, pengelolaan relasi antar-aktor, serta aturan dan tanggung jawab yang mengikat seluruh ekosistem. Oleh karena itu, elemen tata kelola dalam kerangka ini tidak bersifat pelengkap, tetapi menjadi fondasi yang menentukan efektivitas kontrol keamanan di lapisan teknis.

Dari sisi literatur teknis, pendekatan keamanan multilapis telah lama dikembangkan dalam konteks arsitektur cloud, edge, dan IoT melalui mekanisme seperti enkripsi *end-to-end, mutual Transport Layer Security* (mTLS), *service mesh*, dan pengamanan API. Namun, literatur teknis tersebut sering kali berdiri terpisah dari diskursus platform dan governance. Artikel ini menjembatani kesenjangan tersebut dengan mengintegrasikan mekanisme teknis spesifik keamanan ke dalam kerangka platform multilapis, sehingga menghasilkan model yang tidak hanya konseptual, tetapi juga implementable bagi perancang dan pengelola platform digital. Dengan demikian, kontribusi utama kerangka ini terletak pada kemampuannya menunjukkan bahwa keamanan layanan sistem harus dirancang secara end-to-end, mulai dari lapisan infrastruktur hingga lapisan tata kelola. Pendekatan ini berbeda secara fundamental dari model keamanan tradisional yang berfokus pada perimeter jaringan atau aplikasi secara terisolasi. Dalam ekosistem platform digital multilapis, ancaman bersifat lintas-lapisan dan melibatkan banyak aktor, sehingga hanya pendekatan terintegrasi yang mampu memberikan ketahanan sistem secara menyeluruh. Kerangka ini, oleh karena itu, memperkuat argumen bahwa keamanan dalam platform digital modern merupakan hasil dari koordinasi lintas lapisan, bukan sekadar akumulasi

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

kontrol teknis yang berdiri sendiri. Oleh karena itu, kerangka empat lapisan yakni infrastruktur, platform, aplikasi, dan tata kelola merupakan operasionalisasi dari pandangan platform sebagai socio-technical system, di mana lapisan tata kelola merefleksikan 'aturan' dan lapisan teknis merefleksikan 'arsitektur' dalam teori platform.

Interdependensi Antar-Lapisan dan Implikasinya terhadap Keamanan

Ekosistem platform digital bersifat interdependen lintas lapisan, sehingga kegagalan atau kelemahan pada satu lapisan berpotensi memicu risiko sistemik pada lapisan lainnya. Berikut ini ialah tabel rincian interdependensi antar-lapisan dan implikasinya terhadap keamanan:

Tabel 2. Interdependensi Risiko Keamanan Antar-Lapisan Platform Digital

Lapisan	Kontrol Keamanan Utama	Ketergantungan Lintas Lapisan	Dampak Kelemahan
Tata Kelola	Kebijakan, kepatuhan, audit, shared responsibility	Implementasi kontrol teknis pada aplikasi dan platform	Risiko kepatuhan, eskalasi insiden, hilangnya kepercayaan
Aplikasi dam Layanan	IAM, Secure SDLC, isolasi kontainer, runtime monitoring	Autentikasi, API, dan orkestrasi dari middleware	Kebocoran data, eksploitasi logika aplikasi
Platform dam Middleware	API Gateway, mTLS, service mesh, keamanan orkestrator	Stabilitas jaringan dan kebijakan akses	Pergerakan lateral, perluasan permukaan serangan
Infrastruktur dan Jaringan	Segmentasi jaringan, IDS/IPS, proteksi DDoS	Fondasi seluruh lapisan di atasnya	Gangguan layanan, kegagalan sistemik

Tabel ini menunjukkan bahwa kelemahan pada satu lapisan dapat memicu risiko sistemik lintas lapisan, sehingga keamanan harus dirancang secara terintegrasi. Dalam konteks tata kelola, ketidakjelasan pembagian tanggung jawab keamanan antara pemilik platform dan penyedia layanan pihak ketiga dapat melemahkan efektivitas kontrol teknis pada lapisan aplikasi, khususnya terkait pengelolaan identitas, perlindungan data, dan keamanan integrasi layanan. Literatur platform menunjukkan bahwa ekosistem digital ditandai oleh keterlibatan aktor yang beragam dengan tingkat kontrol dan kepentingan yang berbeda, sehingga tanpa kerangka tata kelola yang jelas, kontrol teknis cenderung diterapkan secara tidak konsisten (Autio et al., 2017). Sebaliknya, kegagalan teknis pada lapisan platform dan middleware seperti kesalahan konfigurasi API, orkestrator layanan, atau mekanisme autentikasi antar-layanan tidak hanya berdampak pada kinerja sistem, tetapi juga dapat menimbulkan implikasi hukum, reputasi, dan kepatuhan. Penelitian keamanan platform menegaskan bahwa insiden teknis sering kali bereskalasi menjadi isu tata kelola, misalnya pelanggaran perjanjian layanan (SLA) atau ketidakpatuhan terhadap regulasi perlindungan data, yang pada akhirnya mempengaruhi tingkat kepercayaan pengguna dan mitra ekosistem (Poniatowski et al., 2022). Literatur mengenai evolusi platform secara konsisten menekankan bahwa arsitektur teknologi, desain layanan, dan tata kelola berkembang secara simultan (co-evolution) dan saling membentuk satu sama lain. Oleh karena itu, penelitian ini memposisikan lapisan tata kelola sebagai komponen inti dalam kerangka keamanan multilapis, bukan sekadar elemen pendukung. Tata kelola berperan dalam menetapkan standar, kebijakan, serta mekanisme akuntabilitas yang menentukan bagaimana kontrol teknis dirancang, diimplementasikan, dan diawasi pada seluruh lapisan sistem. Dengan demikian, efektivitas keamanan teknis sangat ditentukan oleh kualitas koordinasi dan integrasi antar-lapisan, yang hanya dapat dicapai melalui pendekatan keamanan yang terintegrasi dan berorientasi sistem.

Tantangan Trade-off antara Keamanan dan Kinerja Sistem

Implementasi kontrol keamanan yang kuat termasuk enkripsi end-to-end, autentikasi berlapis, dan enkripsi saluran menyebabkan biaya performa yang nyata pada sistem terdistribusi. Pengukuran empiris dan kajian literatur menunjukkan bahwa mekanisme kriptografi dan protokol keamanan menambah latensi, overhead CPU, dan konsumsi energi, sehingga berdampak pada *quality of service* khususnya untuk aplikasi real. Hal ini terbukti pada studi yang membahas atribut kualitas pada edge computing dan konsekuensi keamanan terhadap latensi dan konsumsi energi (Ashouri et al., 2021). Oleh karena itu, arsitektur cloud–edge memunculkan keputusan desain yang bersifat trade-off yakni memindahkan pemrosesan ke edge mengurangi latensi, tetapi membatasi kapasitas kriptografi (*resource-constrained devices*), sementara menempatkan enkripsi penuh dan pemeriksaan keamanan di cloud meningkatkan keamanan, tetapi memperbesar waktu respons dan lalu lintas jaringan. Beberapa studi eksperimen dan tinjauan sistematis mengilustrasikan skenario ini. Edge memberikan keunggulan latensi, tetapi menuntut mekanisme keamanan yang ringan dan selektif agar tidak mengorbankan real-time performance (Soni et al., 2025).

Rekomendasi pendekatan keamanan adaptif dan kontekstual sebagai kompromi praktis. Pendekatan ini meliputi: (1) penggunaan algoritma kriptografi *lightweight* yang memenuhi standar keamanan minimal pada perangkat edge

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

(*authenticated lightweight ciphers, AEAD schemes*), (2) selektifasi enkripsi/validasi berdasarkan sensitivitas data dan tingkat risiko (data classification ke different security profiles), serta (3) offloading operasi kriptografi berat ke node edge yang lebih kapabel atau ke cloud hanya saat diperlukan. Empiris menunjukkan bahwa kombinasi *lightweight crypto* dan *selective full-path protection* mengurangi overhead latensi sambil mempertahankan jaminan kerahasiaan dan integritas untuk data kritis (Al-Shatari et al., 2023). Selain itu, teknik arsitektural seperti service mesh (mTLS di tingkat internal) dan *zero-trust microservices* dapat mengamankan komunikasi antar-layanan dengan overhead yang relatif terukur bila dikelola dengan baik misalkan off-line certificate provisioning, hardware acceleration, dan pengelolaan lifecycle sertifikat otomatis. Studi perbandingan menunjukkan bahwa desain yang memadukan API Gateway (pengamanan di perimeter layanan) dengan mTLS internal (pengamanan antar-layanan) dapat memberikan keseimbangan antara keamanan dan performa apabila konfigurasi dan manajemen sertifikat dioptimalkan (Reed et al., 2021). Dengan demikian, kerangka konseptual yang diusulkan tetap normatif, tetapi implementable karena memasukkan prinsip-prinsip adaptif yaitu menetapkan kebijakan keamanan yang kontekstual per-lapisan dan mekanisme orkestrasi yang dapat menyeimbangkan kebutuhan keamanan dan kinerja berdasarkan profil layanan. Pengujian kinerja terukur (latensi, throughput, resource use) tetap diperlukan sebagai bagian dari validasi implementasi untuk menentukan konfigurasi optimal pada setiap kasus aplikasi real-time. Berikut ini ialah tabel trade-off mekanisme keamanan terhadap kinerja sistem terdistribusi:

Tabel 3. Trade-off Mekanisme Keamanan terhadap Kinerja Sistem Terdistribusi

Mekanisme Keamanan	Tujuan Keamanan	Dampak terhadap Kinerja	Implikasi Desain Sistem
Enkripsi end-to-end	Kerahasiaan dan integritas data	Peningkatan latensi dan overhead CPU	Cocok untuk data sensitif; perlu optimasi atau offloading
Autentikasi berlapis	Pencegahan akses tidak sah	Waktu respons bertambah	Perlu caching atau token berbasis sesi
mTLS antar-layanan	Keamanan komunikasi internal	Overhead handshake dan manajemen sertifikat	Efektif pada service mesh dengan otomasi
Keamanan di edge (lightweight crypto)	Proteksi data real-time	Overhead rendah, tingkat proteksi terbatas	Sesuai untuk aplikasi latensi rendah
Inspeksi keamanan terpusat (cloud)	Deteksi ancaman menyeluruh	Penambahan latensi jaringan	Digunakan selektif untuk trafik kritis

Sebagaimana ditunjukkan pada Tabel 3, implementasi kontrol keamanan tingkat lanjut seperti mutual TLS (mTLS) antar-layanan yang penting untuk memastikan keaslian dan kerahasiaan komunikasi internal membawa konsekuensi langsung berupa overhead handshake kriptografi dan kompleksitas manajemen siklus hidup sertifikat. Dampak ini dapat termanifestasi sebagai peningkatan latensi pada transaksi yang melibatkan banyak percakapan antar-mikrolayanan (chatty microservices) dan konsumsi sumber daya CPU yang lebih tinggi. Oleh karena itu, desain sistem platform digital multilapis tidak boleh mengadopsi kontrol keamanan secara seragam, tetapi harus mempertimbangkan pendekatan strategis yang kontekstual dan terukur.

Dengan demikian, untuk mengelola trade-off antara keamanan dan kinerja secara efektif, desain sistem harus mengadopsi strategi orkestrasi keamanan yang cerdas seperti penerapan *offline certificate provisioning*, *caching session ticket*, dan pemanfaatan akselerasi perangkat keras kriptografi untuk mengurangi overhead teknis; menerapkan pendekatan keamanan yang selektif dan berbasis risiko dengan mengklasifikasikan data dan menegaskan kebijakan perlindungan secara otomatis melalui *service mesh* atau *API gateway*; serta mengintegrasikan pengujian kinerja dan keamanan yang berkelanjutan (*continuous performance and security testing*) ke dalam siklus DevOps guna memvalidasi dampak setiap perubahan kebijakan secara empiris. Dengan mengoperasionalkan ketiga prinsip ini, kerangka konseptual yang diusulkan memfasilitasi peralihan dari paradigma "keamanan versus kinerja" yang antagonistik menuju paradigma "keamanan dan kinerja" yang simbiosis sehingga menghasilkan arsitektur platform digital yang tangguh dan efisien secara operasional.

Kontribusi Kerangka Konseptual terhadap Pengembangan Keamanan Platform

Secara teoretis, penelitian ini memperluas pemahaman literatur keamanan sistem informasi dengan menggabungkan dua domain studi yang selama ini berkembang relatif terpisah yakni keamanan multilapis dan ekosistem platform digital. Pendekatan ini menyatukan aspek arsitektural, teknologi, dan governance ke dalam satu

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

kerangka yang komprehensif, sehingga memungkinkan analisis risiko tidak hanya pada level komponen teknis, tetapi juga pada dinamika interaksi aktor serta aturan tata kelola dalam ekosistem. Literatur terbaru menekankan bahwa platform digital modern karena sifatnya sebagai *socio-technical system* memerlukan model keamanan yang mencakup dimensi teknis dan non-teknis secara simultan; keterbatasan pendekatan parsial telah diidentifikasi sebagai salah satu penyebab kegagalan mitigasi risiko dalam konteks sistem kompleks (Autio et al., 2017).

Secara praktis, kerangka konseptual ini memberikan alat analitis yang sistematis bagi perancang platform, pengelola sistem, dan auditor keamanan untuk memetakan ancaman dan kontrol keamanan pada masing-masing lapisan. Hal ini sejalan dengan tuntutan praktik keamanan modern yang memerlukan pendekatan berbasis risiko yang terukur, serta panduan operasional yang dapat diterjemahkan ke dalam kebijakan, prosedur, dan desain teknis (*security by design*). Studi pada *cloud-native security* menunjukkan bahwa pemetaan kontrol berdasarkan lapisan arsitektural membantu organisasi menetapkan prioritas mitigasi yang lebih efektif dibandingkan pendekatan reaktif atau titik fokus tunggal (kecuali perimeter) yang umum ditemukan dalam praktik tradisional. Dengan demikian, kerangka ini tidak hanya berkontribusi secara konseptual, tetapi juga memiliki nilai aplikasi yang tinggi dalam konteks tata kelola risiko keamanan platform digital yang dinamis dan heterogen.

Keterbatasan dan Arah Penelitian Selanjutnya

Kerangka konseptual yang diusulkan dalam penelitian ini dikembangkan melalui sintesis literatur dan analisis konseptual sehingga validasinya masih terbatas pada tataran teoretis. Penelitian ini belum melibatkan pengujian empiris melalui implementasi langsung pada platform digital berskala besar, baik dalam bentuk eksperimen terkontrol, simulasi sistem, maupun pengukuran kuantitatif terhadap metrik keamanan dan kinerja. Akibatnya, efektivitas kerangka dalam meningkatkan ketahanan sistem, menurunkan tingkat risiko, dan dampaknya terhadap latensi dan penggunaan sumber daya belum dapat dievaluasi secara objektif. Penelitian selanjutnya disarankan untuk menerapkan kerangka ini pada studi kasus platform digital nyata dengan pendekatan eksperimental atau *benchmarking*, menggunakan indikator kuantitatif seperti tingkat insiden keamanan, waktu deteksi dan respons, dan overhead kinerja seperti penerapan dalam bentuk *security checklist* dan diujikan melalui wawancara dengan praktisi DevOps, validasi melalui *simulasi threat modeling* (misal dengan metode STRIDE) pada studi kasus platform e-commerce, dan lain-lain. Selain itu, pengujian komparatif terhadap arsitektur keamanan eksisting diperlukan untuk menilai keunggulan relatif kerangka ini. Pendekatan longitudinal juga direkomendasikan guna mengamati adaptabilitas kerangka terhadap perubahan arsitektur platform dan dinamika ancaman keamanan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa keamanan layanan sistem pada platform digital modern harus dirancang dan dianalisis sebagai arsitektur multilapis yang terintegrasi, bukan sebagai kumpulan kontrol keamanan yang berdiri sendiri. Kerangka konseptual yang diusulkan memformalkan empat lapisan keamanan yakni infrastruktur fisik dan jaringan, platform dan middleware, aplikasi dan layanan, serta tata kelola dan kepercayaan yang masing-masing memiliki vektor ancaman, kontrol keamanan, dan dependensi teknis yang berbeda. Hasil analisis menunjukkan bahwa kerentanan pada satu lapisan, seperti kesalahan konfigurasi jaringan atau pengelolaan API, dapat bereskalasi menjadi kegagalan sistemik yang mempengaruhi ketersediaan layanan, integritas data, dan kepatuhan keamanan secara keseluruhan. Dari perspektif arsitektural, penelitian ini menegaskan bahwa mekanisme keamanan cloud-native seperti segmentasi jaringan, enkripsi end-to-end, service mesh dengan mutual TLS, serta pipeline DevSecOps harus diimplementasikan secara konsisten lintas lapisan untuk mencapai ketahanan sistem. Selain itu, temuan menunjukkan adanya trade-off inheren antara penguatan kontrol keamanan dan kinerja sistem, khususnya pada arsitektur terdistribusi berbasis cloud–edge. Oleh karena itu, pendekatan keamanan adaptif dan kontekstual melalui pemilihan algoritma kriptografi ringan, pengamanan selektif berdasarkan sensitivitas data, dan orkestrasi kontrol keamanan menjadi strategi teknis yang relevan untuk menjaga keseimbangan antara keamanan dan kualitas layanan. Secara keseluruhan, kerangka konseptual ini memberikan dasar teknis yang sistematis bagi perancang dan pengelola platform digital untuk memetakan risiko, memilih kontrol keamanan yang tepat pada setiap lapisan arsitektur, serta mengevaluasi dampak keamanan terhadap kinerja sistem. Dengan demikian, kerangka ini berpotensi menjadi referensi teknis dalam perancangan arsitektur keamanan platform digital multilapis yang tangguh, adaptif, dan terukur.

REFERENSI

Akamai. (2025, April 22). *Akamai Research: Web Attacks Up 33%, APIs Emerge as Primary Targets*. Akamai Technologies, Inc.

Alenezi, A. M. (2023). *Digital and Cloud Forensic Challenges*. http://arxiv.org/abs/2305.03059

Ali, R. N., Mojtaba, S., Raviz, H., Ali, S., Peng, L., Amir, M., & Valentina, L. (2022). An Empirical Study of Security

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Practices for Microservices Systems. *Journal of Systems and Software*. https://kubernetes.io

Ali, S. E. A., Lai, F. W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: the context of efficient market hypothesis. *Sustainability (Switzerland)*, *13*(3), 1–27. https://doi.org/10.3390/su13031066

Al-Shatari, M., Hussin, F. A., Aziz, A. A., Eisa, T. A. E., Tran, X. T., & Dalam, M. E. E. (2023). IoT Edge Device Security: An Efficient Lightweight Authenticated Encryption Scheme Based on LED and PHOTON. *Applied Sciences (Switzerland)*, *13*(18). https://doi.org/10.3390/app131810345

Ashouri, M., Davidsson, P., & Spalazzese, R. (2021). Quality attributes in edge computing for the Internet of Things: A systematic mapping study. In *Internet of Things (Netherlands)* (Vol. 13). Elsevier B.V. https://doi.org/10.1016/j.iot.2020.100346

Autio, E., Nambisan, S., Thomas, L. D. W., & Wright, M. (2017). *DIGITAL AFFORDANCES, SPATIAL AFFORDANCES, AND THE GENESIS OF ENTREPRENEURIAL ECOSYSTEMS*.

Berardi, D., Giallorenzo, S., Melis, A., Prandini, M., Mauro, J., & Montesi, F. (2022). Microservice security: a systematic literature review. *PeerJ Computer Science*, *7*. https://doi.org/10.7717/PEERJ-CS.779

Costabile, C. (2024). Digital platform ecosystem governance of private companies: Building blocks and a research agenda based on a multidisciplinary, systematic literature review. *Data and Information Management*, *8*(1). https://doi.org/10.1016/j.dim.2023.100053

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022a). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022b). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets*, *30*(1), 87–98. https://doi.org/10.1007/s12525-019-00377-4

Hund, A., Wagner, H. T., Beimborn, D., & Weitzel, T. (2021). Digital innovation: Review and novel perspective. In *Journal of Strategic Information Systems* (Vol. 30, Issue 4). Elsevier B.V. https://doi.org/10.1016/j.jsis.2021.101695

Hutasuhut, N. R. P., Amri, M. G., & Aji, R. F. (2024). Security Gap in Microservices: A Systematic Literature Review. *International Journal of Advanced Computer Science and Applications*, *15*.

Jovanovic, M., Sjödin, D., & Parida, V. (2022). Co-evolution of platform architecture, platform services, and platform governance: Expanding the platform value of industrial digital platforms. *Technovation*, *118*. https://doi.org/10.1016/j.technovation.2020.102218

Lestari, M., Entina Puspita, M., & Fritz Wijaya, A. (2025). Model Tata Kelola TI Terintegrasi untuk Keamanan Informasi di Sektor Fintech. *Jurnal Teknologi Dan Manajemen Industri Terapan (JTMIT)*, *4*(3), 766–776.

Newswire. (2025, May 28). *CDNetworks' State of WAAP Report Reveals 887.4 Billion Web App and API Attacks in 2024, a 21.4% YoY increase*. CDNetworks .

Ohm, M., & Stuke, C. (2023, August 29). SoK: Practical Detection of Software Supply Chain Attacks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3600160.3600162

Oluwatobiloba, A. (2025). *Security Challenges in Cloud-Native Microservices: A Risk Assessment and Mitigation Framework*.

Peng, H., Lu, Y., & Gupta, S. (2023). Promoting value emergence through digital platform ecosystems: Perspectives on resource integration in China. *Technological Forecasting and Social Change*.

Poniatowski, M., Lüttenberg, H., Beverungen, D., & Kundisch, D. (2022). Three layers of abstraction: a conceptual framework for theorizing digital multi-sided platforms. *Information Systems and E-Business Management*, *20*(2), 257–283. https://doi.org/10.1007/s10257-021-00513-8

Qazi, F. (2023). Application Programming Interface (API) Security in Cloud Applications. *EAI Endorsed Transactions on Cloud Systems*, *7*(23), e1. https://doi.org/10.4108/eetcs.v7i23.3011

Reed, J., Martinez, A., Thompson, D., Chen, E., & Esther, D. (2021). *Comparative Study of mTLS vs. API Gateway-Based Security in Kubernetes Microservices*.

Soni, A. A., Dhenia, R. N. K., & Parikh, M. (2025). Edge Vs Cloud Computing Performance Trade-Offs for Real-Time Analytics. *International Journal of Science and Engineering Applications*. https://doi.org/10.7753/ijsea1406.1007

Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Girolamo, M. Di, Barone, P., Taleb, T., & Tserpes, K. (2023). Security in Cloud-Native Services: A Survey. In *Journal of Cybersecurity and Privacy* (Vol. 3, Issue 4, pp. 758–793). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/jcp3040034