JIKUM
JURNAL ILMU KOMPUTER

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

Strategi Layanan Keamanan Siber pada Ekosistem Multi-Platform: Tinjauan Literatur

Khairudiah[1], Reifan[2], Alam Al Hasbi[3], Nasywa Az zahra[4], Farid Deza Amin[5*]
Universitas Malikussaleh, Indonesia
[5]farid240170231@mhs.unimal.ac.id

ABSTRACT

The rapid escalation of digital technology adoption has compelled modern organizations to operate within complex multi-platform ecosystems, integrating diverse operating systems, mobile devices, web applications, and cloud services. While this convergence enhances operational agility, it significantly expands the potential attack surface, exposing critical assets to sophisticated cyber threats. This study employs a Systematic Literature Review (SLR) methodology to evaluate and compare contemporary cybersecurity strategies. Analyzing 15 primary studies selected from reputable databases between 2018 and 2024, this research contrasts the efficacy of Perimeter-based models, Defense-in-Depth, and Zero Trust Architecture (ZTA). The findings demonstrate that traditional static security perimeters are obsolete in decentralized environments. Conversely, a hybrid approach combining Zero Trust with AI-driven threat detection offers superior resilience, reducing incident response latency and preventing lateral movement. The study concludes by proposing an integrated security framework that positions cybersecurity as a strategic business enabler rather than a technical support function.

Keywords: *cybersecurity, multi-platform, systematic literature review, zero trust, defense in depth*

PENDAHULUAN

Transformasi digital telah mengubah lanskap operasional organisasi secara fundamental. Adopsi ekosistem multi-platform—yang mencakup integrasi antara sistem operasi *on-premise*, perangkat seluler (BYOD), dan infrastruktur *cloud*—telah menjadi standar baru untuk meningkatkan produktivitas dan kolaborasi. Namun, keuntungan operasional ini berbanding lurus dengan peningkatan risiko keamanan. Laporan industri terbaru mencatat lonjakan serangan *ransomware* dan pencurian identitas yang menargetkan celah integrasi antar-platform yang berbeda protokol keamanannya.

Tantangan utama yang dihadapi saat ini adalah ketidakefektifan model keamanan tradisional (berbasis perimeter) dalam melindungi aset yang tersebar. Dalam model lama, keamanan difokuskan pada "benteng" jaringan kantor, padahal data kini bergerak bebas di luar dinding tersebut. Hipotesis penelitian ini adalah bahwa organisasi memerlukan pergeseran paradigma dari keamanan berbasis lokasi menjadi keamanan berbasis identitas dan data.

Penelitian ini bertujuan untuk: (1) Mengidentifikasi tantangan keamanan spesifik pada lingkungan multi-platform, dan (2) Mengevaluasi efektivitas strategi keamanan modern melalui pendekatan *Systematic Literature Review* (SLR). Hasil kajian ini diharapkan memberikan panduan strategis bagi organisasi dalam merancang arsitektur keamanan yang adaptif.

TINJAUAN PUSTAKA

Bagian ini meninjau literatur terkait keamanan siber dalam konteks multi-platform. Keamanan siber bertujuan melindungi kerahasiaan, keutuhan, dan ketersediaan informasi melalui pendekatan manajemen risiko yang terstruktur. Dalam ekosistem multi-platform, keberagaman perangkat dan sistem menimbulkan tantangan dalam penerapan kontrol keamanan yang konsisten. Ancaman siber kini tidak lagi bersifat statis, melainkan dinamis dan menargetkan titik terlemah dalam integrasi antar platform.

Strategi layanan keamanan siber memandang keamanan sebagai proses berkelanjutan yang mencakup pencegahan, deteksi, respons, dan pemulihan insiden. Pendekatan ini mengintegrasikan teknologi, sumber daya manusia, dan proses organisasi guna mencapai ketahanan siber. Laporan lanskap ancaman terbaru menunjukkan pergeseran dari serangan infrastruktur murni ke serangan berbasis identitas dan aplikasi.

Terkait konsep pertahanan, Defense in Depth menerapkan mekanisme perlindungan berlapis pada setiap level sistem. Sementara itu, arsitektur Zero Trust menekankan prinsip verifikasi berkelanjutan tanpa asumsi kepercayaan, terlepas dari lokasi atau platform pengguna. Konsep ini relevan dengan temuan mengenai pentingnya menyembunyikan dan mengamankan data, meskipun konteks awalnya adalah steganografi, prinsip perlindungan datanya tetap valid dalam arsitektur modern.

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

METODE PENELITIAN

Penelitian ini menggunakan metode Tinjauan Literatur Sistematis (*Systematic Literature Review*) dengan mengikuti protokol standar PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Pendekatan ini dipilih untuk memastikan proses seleksi data yang objektif dan terukur, setara dengan ketatnya metode eksperimental.

Strategi Pencarian Data

Pencarian literatur dilakukan pada *database* akademis utama yaitu IEEE Xplore, ScienceDirect, dan Google Scholar. Kata kunci (*search strings*) yang digunakan adalah kombinasi boolean: *("Cybersecurity Strategy" OR "Network Security") AND ("Multi-platform" OR "Cloud Ecosystem" OR "Cross-platform")* **Kriteria Seleksi** Untuk menjamin kualitas analisis, diterapkan kriteria inklusi dan eksklusi yang ketat sebagaimana dirincikan pada **Tabel 1**.

Tabel 1. Kriteria Inklusi dan Eksklusi Penelitian

Parameter	Kriteria Inklusi (Data Diterima)	Kriteria Eksklusi (Data Ditolak)
Rentang Waktu	2018 – 2024 (5 tahun terakhir)	Publikasi sebelum tahun 2018
Jenis Sumber	Jurnal Terakreditasi, Prosiding, Standar (NIST/ISO)	Artikel Blog, Opini Pribadi, *Whitepaper* Komersial
Bahasa	Bahasa Inggris dan Indonesia	Bahasa selain Inggris/Indonesia
Relevansi	Membahas strategi & arsitektur multi-platform	Membahas *coding* dasar tanpa konteks strategi

HASIL DAN PEMBAHASAN

Dari total 120 artikel awal yang teridentifikasi, proses penyaringan (*screening*) menghasilkan 15 literatur inti yang paling relevan untuk dianalisis secara mendalam. Hasil ekstraksi data menunjukkan adanya korelasi positif antara adopsi kerja hibrida (pasca-pandemi) dengan peningkatan riset keamanan multi-platform, dengan lonjakan signifikan penelitian terjadi pada rentang tahun 2021 hingga 2022.

Komparisasi Strategi Keamanan

Bagian ini menyajikan analisis komparatif antara tiga pendekatan dominan yang ditemukan dalam literatur: (1) Keamanan Tradisional Berbasis Perimeter, (2) *Defense in Depth* (Pertahanan Berlapis), dan (3) *Zero Trust Architecture* (ZTA). Perbandingan teknis dan operasional disajikan secara rinci pada Tabel 2.

Tabel 2. Matriks Perbandingan Efektivitas Strategi Keamanan

Fitur / Dimensi	Traditional (Perimeter-Based)	Defense in Depth (DiD)	Zero Trust Architecture (ZTA)
Konsep Dasar	*Trust but Verify* (Percaya jaringan internal)	Perlindungan berlapis (*Layered*)	*Never Trust, Always Verify*
Fokus Kontrol	*Firewall* & VPN Jaringan	*Endpoint*, Jaringan, & Aplikasi	Identitas Pengguna & Perangkat
Fleksibilitas Multi-Platform	**Rendah** (Sulit untuk *remote/cloud*)	**Sedang** (Manajemen kompleks)	**Tinggi** (Agnostik terhadap lokasi)
Resistensi Lateral Movement	**Rendah** (Penyerang bebas jika masuk)	**Sedang** (Terhambat lapisan lain)	**Tinggi** (Segmentasi mikro membatasi)
Ketergantungan Infrastruktur	Terpusat di kantor (*On-premise*)	Hibrida	Terdesentralisasi (*Cloud-native*)
Beban Kinerja (Overhead)	Rendah	Tinggi (Banyak agen keamanan)	Sedang (Verifikasi berulang)

Berdasarkan **Tabel 2**, strategi tradisional terbukti memiliki kelemahan fatal dalam mencegah pergerakan lateral (*lateral movement*) penyerang di lingkungan multi-platform. Sebaliknya, **Zero Trust** menawarkan keamanan tertinggi namun membutuhkan kematangan infrastruktur identitas.

Kerangka Kerja Usulan (Proposed Framework)

Berdasarkan sintesis temuan, penelitian ini mengusulkan kerangka kerja keamanan integratif. Kerangka kerja ini menempatkan **Manajemen Identitas (IAM)** sebagai gerbang pertahanan utama, didukung oleh analisis perilaku berbasis AI. Model ini memastikan bahwa setiap permintaan akses diverifikasi konteksnya sebelum diizinkan menyentuh data atau aplikasi perusahaan.

JIKUM
JURNAL ILMU KOMPUTER

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

KESIMPULAN

Penelitian ini menyimpulkan bahwa kompleksitas ekosistem multi-platform menuntut evolusi strategi keamanan siber. Berdasarkan analisis SLR terhadap 15 studi utama, ditemukan bahwa:

1. Model keamanan berbasis perimeter sudah tidak relevan dan harus digantikan atau dilengkapi dengan model yang lebih dinamis.
2. **Zero Trust Architecture (ZTA)** adalah pendekatan yang paling efektif secara teoritis dan praktis untuk mengamankan aset yang tersebar, karena memverifikasi setiap permintaan akses tanpa asumsi kepercayaan.
3. Implementasi yang sukses memerlukan kombinasi antara teknologi (enkripsi, AI) dan kebijakan tata kelola yang ketat.

Implikasi praktis dari studi ini adalah organisasi disarankan untuk segera mengadopsi prinsip *Least Privilege* dan segmentasi mikro. Untuk penelitian selanjutnya, direkomendasikan melakukan uji performa (*stress test*) guna mengukur dampak latensi dari implementasi enkripsi penuh pada arsitektur Zero Trust.

REFERENSI

Alasmary, W., et al. (2021). Cybersecurity challenges in multi-platform environments. Journal of Information Security, 12(3), 145–158.

Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security. Oxford University Press.

ENISA. (2021). Threat landscape report 2021. European Union Agency for Cybersecurity.

ISO/IEC. (2018). ISO/IEC 27001: Information security management systems. International Organization for Standardization.

Microsoft. (2022). Zero trust security guidance. Microsoft Security Documentation.

Munir, R. (2019). Kriptografi. Informatika Bandung.

NIST. (2020). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology.

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32–44.

Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Pearson.

Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education.