KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.3 Juni 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 289-305
DOI : https://doi.org/10.61722/jipm.v4i3.2371

Systematic Literature Review terhadap Keamanan dan Otomatisasi pada Intent-Based Networking

Wisra Yandi[1], Yulindon[2]
[1]Program Studi Sarjana Terapan Teknik Telekomunikasi, Politeknik Negeri Padang, Padang, Sumatera Barat, Indonesia.
*Penulis Korespondensi: wisrayandi2@gmail.com

Abstract.. *The increasing complexity of modern computer networks requires network management systems that are more automated, flexible, secure, and adaptive.* Intent-Based Networking *(IBN) has emerged as a network management approach that enables user requirements to be translated into automated network configurations based on high-level intents. This study aims to analyze research developments related to security and automation in* Intent-Based Networking *using the* Systematic Literature Review *(SLR) method. The research methodology follows the PRISMA 2020 framework to ensure a systematic and transparent literature selection process. Relevant studies were collected from several international scientific databases, including IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, and ACM Digital Library during the 2021–2026 period. The results show that IBN implementation improves network management efficiency through automated configuration,* real-time *network monitoring, and network service optimization based on* Artificial Intelligence *(AI). The integration of* Software Defined Networking *(SDN),* Machine Learning*, and* security orchestration *also supports the development of more adaptive and intelligent networks. However, IBN implementation still faces several challenges, such as* intent *manipulation, policy translation errors, increased* attack surface*, and the complexity of integrating network automation systems. This study provides a comprehensive synthesis of security and automation developments in* Intent-Based Networking *and can serve as a reference for developing more secure, flexible, and adaptive automated networks in the future.*

Keywords: *Artificial Intelligence*; *Intent-Based Networking*; Network Automation; Network Security; *Systematic Literature Review*

Abstrak. Perkembangan jaringan komputer modern yang semakin kompleks menuntut sistem pengelolaan jaringan yang lebih otomatis, fleksibel, aman, dan adaptif. *Intent-Based Networking* (IBN) hadir sebagai pendekatan manajemen jaringan yang memungkinkan kebutuhan pengguna diterjemahkan menjadi konfigurasi jaringan otomatis berbasis *intent*. Penelitian ini bertujuan untuk menganalisis perkembangan penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking* menggunakan metode *Systematic Literature Review* (SLR). Metode penelitian mengacu pada kerangka PRISMA 2020 untuk memastikan proses seleksi literatur dilakukan secara sistematis dan transparan. Literatur diperoleh dari berbagai database ilmiah internasional seperti IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, dan ACM Digital Library pada periode 2021–2026. Hasil kajian menunjukkan bahwa implementasi IBN mampu meningkatkan efisiensi pengelolaan jaringan melalui otomatisasi konfigurasi, monitoring jaringan secara *real-time*, dan optimasi layanan jaringan berbasis *Artificial Intelligence* (AI). Integrasi teknologi *Software Defined Networking* (SDN), *Machine Learning*, dan *security orchestration* juga mendukung pengembangan jaringan yang lebih adaptif dan cerdas. Namun demikian, implementasi IBN masih menghadapi berbagai tantangan seperti manipulasi *intent*, kesalahan translasi kebijakan jaringan, peningkatan *attack surface*, serta kompleksitas integrasi sistem otomatisasi jaringan. Penelitian ini memberikan sintesis komprehensif mengenai perkembangan keamanan dan otomatisasi pada *Intent-Based Networking* serta dapat menjadi referensi dalam pengembangan jaringan otomatis yang lebih aman, fleksibel, dan adaptif pada masa mendatang.

Kata kunci: Artificial Intelligence*;* Intent-Based Networking*; Keamanan Jaringan; Otomatisasi Jaringan;* Systematic Literature Review

Naskah Masuk: 01 Mei 2026; Revisi: 05 Mei 2026; Diterima: 14 Mei 2026; Terbit: 15 Mei 2026

1. LATAR BELAKANG

Perkembangan teknologi jaringan komputer pada era transformasi digital mengalami peningkatan yang sangat pesat seiring berkembangnya *cloud computing*, *Internet of Things* (IoT), *big data, artificial intelligence* (AI), *edge computing*, serta jaringan generasi kelima (5G). Peningkatan penggunaan layanan digital menyebabkan trafik jaringan global terus bertambah dan mendorong kompleksitas pengelolaan jaringan menjadi semakin tinggi. Perkembangan *cloud computing, Internet of Things,* dan jaringan 5G meningkatkan kebutuhan terhadap sistem pengelolaan jaringan yang otomatis, fleksibel, aman, dan adaptif pada infrastruktur jaringan *modern* (Mehmood et al., 2023; Trantzas et al., 2025). Infrastruktur jaringan modern dituntut mampu menyediakan layanan yang cepat, aman, fleksibel, serta mampu menyesuaikan kondisi jaringan secara dinamis.

Namun, pengelolaan jaringan secara konvensional yang masih bergantung pada konfigurasi manual dinilai kurang efektif karena memerlukan waktu yang lama, sulit melakukan skalabilitas layanan, serta rentan terhadap *human error*. Selain itu, peningkatan jumlah perangkat yang terhubung ke jaringan menyebabkan kebutuhan terhadap otomatisasi dan pengelolaan jaringan cerdas menjadi semakin penting (Sunaryo et al., 2023). Di sisi lain, perkembangan sistem cloud dan otomatisasi jaringan juga meningkatkan potensi ancaman keamanan siber pada infrastruktur jaringan modern (Ahmad et al., 2023). Oleh karena itu, diperlukan pendekatan manajemen jaringan yang lebih cerdas, adaptif, aman, dan otomatis untuk mendukung kebutuhan infrastruktur jaringan generasi masa depan.

Salah satu teknologi yang berkembang dalam pengelolaan jaringan modern adalah Intent-Based Networking (IBN). Menurut Mehmood et al. (2023), Intent-Based Networking merupakan pendekatan manajemen jaringan yang memungkinkan kebutuhan pengguna diterjemahkan menjadi konfigurasi jaringan otomatis berbasis intent atau tujuan layanan tingkat tinggi. Pada pendekatan ini, administrator tidak perlu melakukan konfigurasi perangkat jaringan secara manual karena sistem akan menerjemahkan intent menjadi konfigurasi jaringan melalui proses orchestration, policy translation, verification, monitoring, dan closed-loop automation. Pendekatan tersebut dinilai mampu meningkatkan efisiensi pengelolaan jaringan dan mempercepat deployment layanan jaringan (Manias et al., 2024). Selain itu, penerapan IBN memungkinkan jaringan melakukan pengelolaan layanan secara lebih fleksibel dan adaptif berdasarkan kebutuhan pengguna serta kondisi jaringan secara dinamis (AlSamarneh et al., 2025).

Penerapan Intent-Based Networking banyak didukung oleh teknologi Software Defined Networking (SDN), Network Function Virtualization (NFV), machine learning, dan artificial intelligence. Integrasi teknologi tersebut memungkinkan jaringan melakukan pengambilan keputusan secara otomatis berdasarkan kondisi jaringan secara real-time. Oleh sebab itu, IBN menjadi salah satu solusi penting dalam pengembangan autonomous network dan smart network management pada lingkungan cloud computing, data center, edge computing, dan jaringan 5G (Sadouki & Kornyshova, 2025).

Di sisi lain, implementasi otomatisasi jaringan melalui Intent-Based Networking juga menghadirkan berbagai tantangan baru dalam aspek keamanan jaringan. Integrasi antara AI, orchestration system, automation engine, dan SDN membuka peluang munculnya ancaman keamanan seperti manipulasi intent, kesalahan translasi kebijakan jaringan, privilege escalation, serangan terhadap orchestrator, serta eksploitasi sistem

otomatisasi jaringan (Ahmad et al., 2023). Risiko tersebut dapat memengaruhi stabilitas dan keamanan infrastruktur jaringan apabila tidak dikelola dengan baik. Kim et al. (2024) menjelaskan bahwa penggunaan sistem otomatisasi berbasis intent dapat meningkatkan attack surface karena adanya integrasi berbagai komponen jaringan cerdas dan otomatis yang saling terhubung.

Keamanan dan otomatisasi merupakan dua aspek yang saling berkaitan dalam implementasi Intent-Based Networking. Proses otomatisasi jaringan yang tidak didukung oleh mekanisme keamanan yang baik dapat meningkatkan risiko serangan siber dan kesalahan konfigurasi otomatis. Sebaliknya, penerapan sistem keamanan yang efektif juga membutuhkan dukungan otomatisasi agar jaringan mampu melakukan monitoring, deteksi ancaman, dan respons keamanan secara cepat serta adaptif. Oleh karena itu, integrasi keamanan dan otomatisasi menjadi faktor penting dalam pengembangan jaringan cerdas berbasis Intent-Based Networking.

Beberapa penelitian sebelumnya telah membahas perkembangan dan implementasi Intent-Based Networking pada berbagai lingkungan jaringan modern. Mehmood et al. (2023) melakukan structured literature review mengenai intent-driven autonomous network management pada jaringan seluler masa depan dan menunjukkan bahwa IBN mampu meningkatkan efisiensi pengelolaan jaringan secara signifikan. Penelitian lain oleh Manias et al. (2024) membahas penggunaan large language model untuk intent extraction pada jaringan 5G core network guna meningkatkan otomatisasi sistem jaringan berbasis AI. Selain itu, Trantzas et al. (2025) mengembangkan pendekatan intent-driven network automation berbasis sustainable artificial intelligence untuk meningkatkan efisiensi pengelolaan jaringan modern.

Penelitian lain oleh AlSamarneh et al. (2025) meneliti proses penerjemahan intent pengguna menjadi kebijakan jaringan otomatis menggunakan pendekatan machine learning dan neural computing. Huang et al. (2026) juga mengembangkan intent-based security orchestration untuk mendukung respons keamanan otomatis pada lingkungan keamanan siber modern. Selain itu, penelitian mengenai implementasi Intent-Based Networking pada lingkungan edge computing menunjukkan bahwa pendekatan intent-based mampu meningkatkan efisiensi pengelolaan sumber daya jaringan dan layanan secara dinamis pada infrastruktur jaringan modern (He et al., 2023). Kajian systematic literature review mengenai automation quality of service pada jaringan komputer juga menunjukkan adanya peningkatan tren penelitian terkait otomatisasi jaringan berbasis AI dan SDN dalam lima tahun terakhir (Sunaryo et al., 2023).

Namun, sebagian besar penelitian terdahulu masih berfokus pada implementasi teknis, arsitektur sistem, dan otomatisasi jaringan secara umum. Penelitian sebelumnya juga cenderung membahas aspek keamanan dan otomatisasi secara terpisah sehingga belum terdapat kajian literatur sistematis yang secara khusus mengintegrasikan aspek keamanan, otomatisasi, dan teknologi pendukung Intent-Based Networking dalam satu analisis komprehensif pada konteks jaringan modern berbasis AI, SDN, cloud computing, edge computing, dan 5G. Selain itu, masih terbatas penelitian yang melakukan sintesis menyeluruh terhadap tren penelitian, tantangan implementasi, mekanisme keamanan, serta perkembangan teknologi otomatisasi IBN pada periode 2021–2026. Rentang tahun tersebut dipilih karena menunjukkan perkembangan penelitian terbaru mengenai keamanan, otomatisasi jaringan, serta penerapan artificial intelligence pada Intent-Based Networking.

Berdasarkan kondisi tersebut, diperlukan kajian literatur sistematis yang mampu menganalisis secara komprehensif perkembangan penelitian mengenai keamanan dan otomatisasi pada Intent-Based Networking. Kajian ini penting untuk memahami tren penelitian, teknologi pendukung, tantangan implementasi, mekanisme keamanan, serta peluang pengembangan IBN pada jaringan generasi masa depan. Selain itu, penelitian ini juga diperlukan untuk memberikan gambaran mengenai bagaimana keamanan dan otomatisasi diterapkan secara terintegrasi pada sistem jaringan modern berbasis AI dan SDN.

Penelitian ini melakukan kajian literatur sistematis mengenai keamanan dan otomatisasi pada Intent-Based Networking berdasarkan artikel internasional bereputasi periode 2021–2026. Kajian dilakukan untuk mengidentifikasi perkembangan teknologi, tren penelitian, tantangan keamanan, mekanisme otomatisasi, serta peluang pengembangan Intent-Based Networking pada jaringan modern. Penelitian ini juga menghasilkan pemetaan penelitian terkait keamanan dan otomatisasi pada Intent-Based Networking berdasarkan tren, metode, dan teknologi yang digunakan. Hasil penelitian diharapkan dapat membantu peneliti, administrator jaringan, dan pengembang sistem jaringan dalam memahami arah perkembangan penelitian IBN serta menjadi referensi akademik dalam pengembangan sistem jaringan otomatis yang lebih aman, adaptif, dan cerdas pada masa mendatang.

Metode Systematic Literature Review (SLR) dipilih karena mampu memberikan analisis yang sistematis, terstruktur, dan komprehensif terhadap perkembangan penelitian terkait keamanan dan otomatisasi pada Intent-Based Networking berdasarkan literatur ilmiah yang relevan dan bereputasi internasional. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem jaringan otomatis yang aman, adaptif, dan cerdas pada era transformasi digital.

2. KAJIAN TEORITIS

A. *Intent-Based Networking* (IBN)

Intent-Based Networking (IBN) merupakan paradigma baru dalam manajemen jaringan yang memungkinkan administrator jaringan menyampaikan kebutuhan layanan dalam bentuk *intent* atau tujuan tingkat tinggi tanpa harus melakukan konfigurasi perangkat jaringan secara manual (Manias et al., 2024; Mehmood et al., 2023). Pada pendekatan ini, sistem akan menerjemahkan kebutuhan pengguna menjadi konfigurasi jaringan otomatis melalui proses *orchestration*, *policy translation*, *verification*, *monitoring*, dan *closed-loop automation*.

Menurut (Mehmood et al., 2023), IBN memungkinkan sistem jaringan melakukan pengelolaan layanan secara otomatis dan adaptif berdasarkan kondisi jaringan secara *real-time*. Teknologi ini dikembangkan untuk meningkatkan efisiensi pengelolaan jaringan modern yang semakin kompleks akibat perkembangan *cloud computing*, *Internet of Things* (IoT), dan jaringan 5G.

Komponen utama pada *Intent-Based Networking* terdiri atas *intent input*, *intent translation*, *policy verification*, *network automation*, serta *monitoring and assurance*. *Intent input* merupakan proses memasukkan kebutuhan layanan jaringan dalam bentuk tujuan tingkat tinggi yang diinginkan pengguna. Selanjutnya, sistem akan melakukan *intent translation* untuk menerjemahkan kebutuhan tersebut menjadi konfigurasi jaringan yang dapat dipahami oleh perangkat jaringan. Setelah proses translasi dilakukan, sistem melakukan *policy verification* untuk memastikan bahwa konfigurasi

jaringan telah sesuai dengan kebijakan dan kebutuhan layanan pengguna. Tahapan berikutnya adalah *network automation*, yaitu proses implementasi konfigurasi jaringan secara otomatis pada infrastruktur jaringan. Selain itu, sistem juga melakukan *monitoring and assurance* secara berkelanjutan untuk memastikan layanan jaringan berjalan sesuai dengan *intent* yang telah ditentukan. Penerapan IBN mampu meningkatkan fleksibilitas jaringan, mempercepat *deployment* layanan, mengurangi *human error*, serta mendukung pengembangan *autonomous network* pada infrastruktur jaringan modern.

B. *Software Defined Networking* (SDN)

Software Defined Networking (SDN) merupakan arsitektur jaringan yang memisahkan *control plane* dan *data plane* sehingga pengelolaan jaringan dapat dilakukan secara terpusat melalui *controller* (Sunaryo et al., 2023; Trantzas et al., 2025). SDN memungkinkan administrator jaringan melakukan konfigurasi dan pengelolaan jaringan secara lebih fleksibel dan dinamis.

Dalam implementasi IBN, SDN berperan penting karena mendukung proses otomatisasi konfigurasi jaringan berdasarkan *intent* pengguna. Integrasi antara IBN dan SDN memungkinkan sistem jaringan melakukan pengambilan keputusan secara otomatis berdasarkan kondisi jaringan secara *real-time*.Karakteristik utama SDN meliputi kemampuan *programmability*, yaitu jaringan dapat diprogram sesuai kebutuhan , serta *centralized control* yang memungkinkan pengelolaan jaringan dilakukan melalui *controller* terpusat. Selain itu, SDN juga mendukung *network abstraction* sehingga infrastruktur jaringan dapat dikelola secara lebih fleksibel tanpa bergantung pada perangkat tertentu. Teknologi ini juga mendukung proses *automation* dalam konfigurasi dan pengelolaan jaringan secara otomatis. Oleh karena itu, SDN banyak diterapkan pada *data center*, jaringan 5G, *cloud computing*, dan *edge computing* karena mampu meningkatkan efisiensi pengelolaan jaringan modern.

C. *Network Automation*

Network Automation merupakan proses otomatisasi konfigurasi, pengelolaan, pemantauan, dan optimasi jaringan menggunakan perangkat lunak atau sistem cerdas (Sunaryo et al., 2023; Trantzas et al., 2025). Teknologi ini dikembangkan untuk mengurangi ketergantungan terhadap konfigurasi manual yang berpotensi menimbulkan *human error*.

Dalam implementasi IBN, *network automation* menjadi komponen penting karena memungkinkan sistem melakukan konfigurasi jaringan secara otomatis berdasarkan *intent* yang diberikan pengguna. Selain itu, otomatisasi jaringan juga mendukung proses *monitoring*, deteksi gangguan, serta optimasi layanan jaringan secara berkelanjutan.

Penerapan *network automation* memberikan berbagai manfaat dalam pengelolaan jaringan modern, seperti meningkatkan efisiensi pengelolaan jaringan, mengurangi waktu konfigurasi layanan, meminimalkan kesalahan konfigurasi, serta mendukung pengelolaan jaringan secara lebih adaptif dan dinamis. Selain itu, otomatisasi jaringan juga mampu meningkatkan kualitas layanan jaringan karena sistem dapat melakukan pemantauan dan optimasi layanan secara berkelanjutan. Penerapan *network automation* saat ini banyak didukung oleh teknologi *machine learning*, *artificial intelligence*, dan SDN untuk menciptakan sistem jaringan yang lebih cerdas dan otomatis.

D. Keamanan Jaringan

Keamanan jaringan merupakan aspek penting dalam pengelolaan infrastruktur jaringan modern (Ahmad et al., 2023; Kim et al., 2024). Tujuan utama keamanan jaringan adalah melindungi data, layanan, dan infrastruktur jaringan dari ancaman keamanan siber seperti serangan *malware*, manipulasi data, *unauthorized access*, dan serangan *distributed denial of service* (DDoS).

Pada implementasi IBN, aspek keamanan menjadi semakin penting karena sistem jaringan melakukan proses otomatisasi dan pengambilan keputusan secara otomatis. Integrasi antara *automation engine*, SDN, dan *artificial intelligence* dapat meningkatkan *attack surface* apabila tidak dilengkapi mekanisme keamanan yang baik.

Beberapa tantangan keamanan pada implementasi IBN meliputi manipulasi *intent* jaringan, kesalahan translasi kebijakan jaringan, serangan terhadap *orchestrator*, *privilege escalation*, serta eksploitasi sistem otomatisasi jaringan. Ancaman tersebut dapat memengaruhi stabilitas dan keamanan infrastruktur jaringan apabila tidak dikelola dengan baik. Oleh karena itu, diperlukan mekanisme keamanan seperti *authentication*, *authorization*, *policy verification*, dan *security orchestration* untuk meningkatkan keamanan pada implementasi IBN.

E. *Artificial Intelligence* pada Jaringan

Artificial Intelligence (AI) merupakan teknologi yang memungkinkan sistem komputer melakukan proses analisis, pembelajaran, dan pengambilan keputusan secara otomatis (AlSamarneh et al., 2025; Manias et al., 2024). Pada jaringan komputer modern, AI banyak digunakan untuk mendukung otomatisasi pengelolaan jaringan, analisis trafik, deteksi ancaman keamanan, dan optimasi layanan jaringan.

Dalam implementasi IBN, AI berperan penting dalam proses analisis kebutuhan layanan pengguna, *intent translation*, prediksi kondisi jaringan, deteksi ancaman keamanan, serta optimasi layanan jaringan. Teknologi AI yang banyak diterapkan pada jaringan modern meliputi *machine learning*, *deep learning*, dan *large language model* (LLM). Integrasi AI dengan IBN memungkinkan jaringan melakukan pengambilan keputusan secara lebih adaptif dan cerdas berdasarkan kondisi jaringan secara *real-time*.

F. *Systematic Literature Review* (SLR)

Systematic Literature Review (SLR) merupakan metode penelitian yang digunakan untuk mengidentifikasi, mengevaluasi, dan menganalisis berbagai penelitian sebelumnya secara sistematis dan terstruktur (Mehmood et al., 2023; Sunaryo et al., 2023). Metode ini bertujuan untuk memperoleh pemahaman komprehensif terhadap perkembangan penelitian pada suatu bidang tertentu.

Pada penelitian ini, metode SLR digunakan untuk menganalisis perkembangan penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking* berdasarkan artikel internasional bereputasi periode 2021–2026. Tahapan dalam metode SLR meliputi identifikasi topik penelitian, penentuan kata kunci pencarian, pengumpulan artikel dari database ilmiah, seleksi artikel berdasarkan kriteria inklusi dan eksklusi, serta analisis dan sintesis literatur. Melalui tahapan tersebut, penelitian dapat dilakukan secara sistematis dan terstruktur sehingga menghasilkan analisis yang lebih objektif dan komprehensif terhadap perkembangan penelitian terkait keamanan dan otomatisasi pada IBN.

G. Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai dasar dalam memahami perkembangan teknologi dan penelitian terkait keamanan serta otomatisasi pada *Intent-Based*

Networking (IBN). Beberapa penelitian sebelumnya telah membahas implementasi IBN pada berbagai lingkungan jaringan modern dengan fokus penelitian yang berbeda.

Mehmood et al. (2023) melakukan *structured literature review* mengenai *intent-driven autonomous network management* pada jaringan seluler masa depan dan menunjukkan bahwa IBN mampu meningkatkan efisiensi pengelolaan jaringan secara signifikan. Penelitian tersebut menjelaskan bahwa penerapan otomatisasi berbasis *intent* mampu mendukung pengembangan jaringan yang lebih adaptif dan cerdas.

Selanjutnya, Manias et al. (2024) membahas penggunaan *large language model* dalam proses *intent extraction* pada jaringan 5G *core network*. Penelitian tersebut menunjukkan bahwa integrasi *artificial intelligence* mampu meningkatkan otomatisasi jaringan serta mendukung pengambilan keputusan jaringan secara lebih efisien.

Trantzas et al. (2025) mengembangkan pendekatan *intent-driven network automation* berbasis *sustainable artificial intelligence* untuk meningkatkan efisiensi pengelolaan jaringan modern. Penelitian tersebut menunjukkan bahwa penerapan AI pada otomatisasi jaringan mampu meningkatkan fleksibilitas layanan dan efisiensi operasional jaringan.

Penelitian lain oleh AlSamarneh et al. (2025) meneliti proses penerjemahan *intent* pengguna menjadi kebijakan jaringan otomatis menggunakan pendekatan *machine learning* dan *neural computing*. Hasil penelitian menunjukkan bahwa teknologi *machine learning* mampu meningkatkan akurasi translasi kebijakan jaringan secara otomatis.

Dalam aspek keamanan jaringan, Ahmad et al. (2023) mengidentifikasi berbagai tantangan keamanan pada implementasi IBN, seperti manipulasi *intent*, kesalahan translasi kebijakan, serta serangan terhadap *orchestrator*. Selain itu, Huang et al. (2026) mengembangkan *intent-based security orchestration* untuk mendukung respons keamanan otomatis pada lingkungan keamanan siber modern.

Penelitian oleh He et al. (2023) juga menunjukkan bahwa implementasi IBN pada lingkungan *edge computing* mampu meningkatkan efisiensi pengelolaan sumber daya jaringan dan layanan secara dinamis. Sementara itu, Sunaryo et al. (2023) melalui kajian *systematic literature review* menunjukkan adanya peningkatan tren penelitian terkait otomatisasi jaringan berbasis AI dan SDN dalam beberapa tahun terakhir.

Berdasarkan penelitian terdahulu tersebut, dapat diketahui bahwa keamanan dan otomatisasi merupakan aspek penting dalam pengembangan *Intent-Based Networking*. Ringkasan penelitian terdahulu dapat dilihat pada Tabel 1.

Tabel 1. Penelitian Terdahulu Terkait Keamanan dan Otomatisasi pada *Intent-Based Networking*

Penulis	Tahun	Metode	Fokus Penelitian	Hasil Penelitian
Mehmood et al.	2021	Structured Literature Review	Intent-driven autonomous network management	IBN mampu meningkatkan efisiensi pengelolaan jaringan otomatis
Manias et al.	2024	Artificial Intelligence	Intent extraction berbasis large language model	AI mampu meningkatkan otomatisasi pada jaringan 5G

Penulis	Tahun	Metode	Fokus Penelitian	Hasil Penelitian
Ahmad et al.	2023	Analisis Keamanan	Keamanan pada IBN	Mengidentifikasi tantangan keamanan pada sistem IBN
Trantzas et al.	2025	Network Automation	Intent-driven network automation	AI mendukung otomatisasi jaringan modern
AlSamarneh et al.	2025	Machine Learning	Translasi intent pengguna	Machine learning meningkatkan otomatisasi kebijakan jaringan
Huang et al.	2025	Security Orchestration	Security orchestration	Mendukung respons keamanan otomatis
He et al.	2023	Edge Computing	IBN pada edge computing	Meningkatkan efisiensi pengelolaan sumber daya jaringan
Sunaryo et al.	2023	Systematic Literature Review	Otomatisasi jaringan berbasis AI dan SDN	Menunjukkan peningkatan tren penelitian otomatisasi jaringan

Berdasarkan Tabel 1, dapat diketahui bahwa penelitian mengenai *Intent-Based Networking* sebagian besar berfokus pada otomatisasi jaringan, penerapan *artificial intelligence*, dan keamanan jaringan modern. Namun, penelitian yang secara khusus mengintegrasikan aspek keamanan dan otomatisasi pada IBN dalam satu kajian literatur sistematis masih terbatas. Oleh karena itu, penelitian ini dilakukan untuk memberikan analisis yang lebih komprehensif terkait keamanan dan otomatisasi pada *Intent-Based Networking*.

3. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan pendekatan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) 2020. Metode SLR merupakan pendekatan penelitian yang dilakukan secara sistematis, terstruktur, dan komprehensif untuk mengidentifikasi, mengevaluasi, serta menganalisis berbagai penelitian terdahulu yang relevan dengan topik penelitian (Page et al., 2021).

Pada penelitian ini, metode SLR digunakan untuk menganalisis perkembangan penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking* (IBN). Metode ini dipilih karena mampu memberikan analisis yang objektif terhadap perkembangan penelitian berdasarkan artikel ilmiah bereputasi internasional. Selain itu, metode SLR juga memungkinkan peneliti memperoleh gambaran mengenai tren penelitian, tantangan implementasi, teknologi pendukung, serta peluang pengembangan keamanan dan otomatisasi pada IBN.

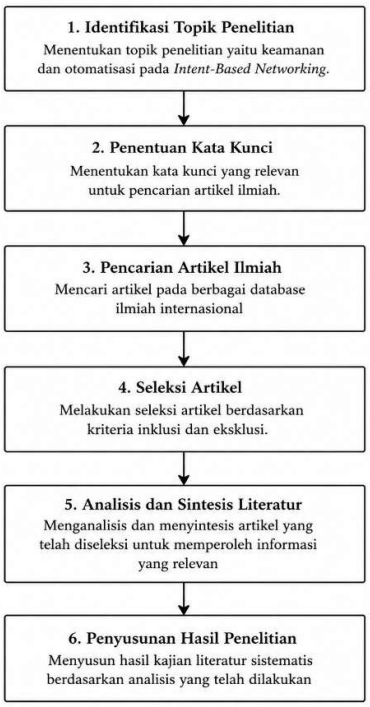
B. Tahap Penelitian

Penelitian dilakukan melalui beberapa tahapan yang disusun secara sistematis agar proses pengumpulan dan analisis literatur dapat dilakukan secara terstruktur. Tahapan penelitian mengikuti pendekatan PRISMA 2020 yang meliputi proses identifikasi, seleksi, evaluasi, dan sintesis literatur secara sistematis (Page et al., 2021).

Tahapan penelitian dapat dijelaskan sebagai berikut:

1. Identifikasi topik penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking*.
2. Penentuan kata kunci pencarian artikel ilmiah.
3. Pengumpulan artikel dari berbagai database ilmiah internasional.
4. Seleksi artikel berdasarkan kriteria inklusi dan eksklusi.
5. Analisis dan sintesis hasil penelitian terdahulu.
6. Penyusunan hasil kajian literatur sistematis.

Diagram alur penelitian digunakan untuk menggambarkan tahapan penelitian yang dilakukan pada metode *Systematic Literature Review*. Diagram alur penelitian dapat dilihat pada Gambar 1.



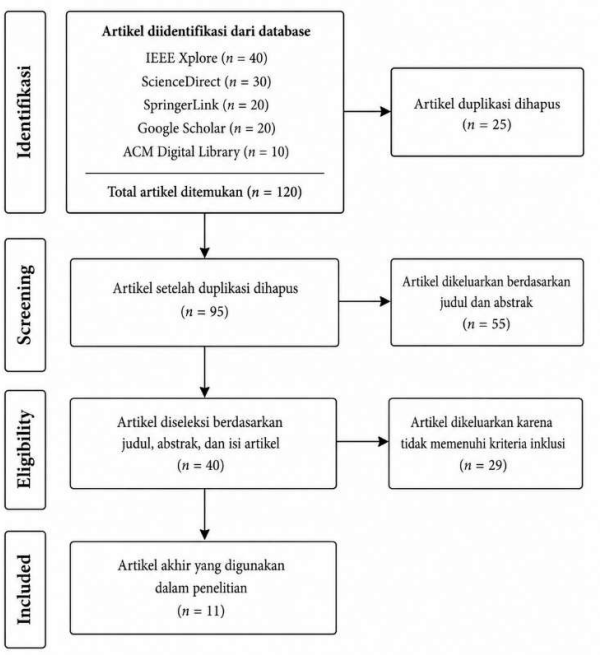
Gambar 1. Diagram Alur Penelitian

Berdasarkan Gambar 1, penelitian diawali dengan identifikasi topik penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking*. Selanjutnya dilakukan penentuan kata kunci pencarian artikel ilmiah yang relevan dengan topik penelitian. Artikel ilmiah kemudian dikumpulkan dari berbagai database internasional seperti IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, dan ACM Digital Library.

Artikel yang diperoleh selanjutnya diseleksi berdasarkan kriteria inklusi dan eksklusi untuk memastikan kesesuaian dengan fokus penelitian. Setelah proses seleksi dilakukan, artikel dianalisis dan disintesis untuk memperoleh informasi mengenai

perkembangan penelitian keamanan dan otomatisasi pada *Intent-Based Networking*. Tahapan terakhir adalah penyusunan hasil kajian literatur sistematis berdasarkan hasil analisis yang telah dilakukan.

Proses seleksi artikel pada penelitian ini mengikuti pendekatan PRISMA 2020 untuk memastikan proses kajian literatur dilakukan secara sistematis dan transparan (Page et al., 2021). Diagram PRISMA 2020 dapat dilihat pada Gambar 2.



Gambar 2. Diagram Prisma

Berdasarkan Gambar 2, proses penelitian dimulai dengan identifikasi artikel dari berbagai database ilmiah internasional, yaitu IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, dan ACM Digital Library dengan total artikel sebanyak 120 artikel. Selanjutnya dilakukan proses penghapusan artikel duplikasi sehingga diperoleh 95 artikel yang dapat digunakan pada tahap berikutnya.

Pada tahap *screening*, artikel diseleksi berdasarkan judul dan abstrak sehingga diperoleh 40 artikel yang relevan dengan topik penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking*. Selanjutnya dilakukan tahap *eligibility* dengan menyeleksi artikel berdasarkan kesesuaian isi dan kriteria inklusi penelitian. Hasil akhir proses seleksi diperoleh 11 artikel yang digunakan sebagai sumber utama dalam penelitian ini.

C. Sumber Data Penelitian

Sumber data pada penelitian ini berasal dari artikel ilmiah internasional yang diperoleh melalui berbagai database ilmiah bereputasi. Database yang digunakan meliputi IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, dan ACM Digital Library. Pemilihan database tersebut dilakukan karena menyediakan artikel ilmiah yang relevan dengan topik keamanan dan otomatisasi pada *Intent-Based Networking*.

Artikel yang digunakan merupakan artikel ilmiah yang diterbitkan pada periode 2021–2026 dan memiliki keterkaitan dengan teknologi *Software Defined Networking*

(SDN), *Artificial Intelligence* (AI), *Network Automation*, serta keamanan jaringan. Selain itu, artikel yang dipilih harus tersedia dalam teks lengkap (*full text*) dan berasal dari jurnal atau prosiding internasional bereputasi.

D. Kata Kunci Pencarian

Proses pencarian artikel dilakukan menggunakan beberapa kata kunci yang berkaitan dengan topik penelitian. Kata kunci tersebut digunakan untuk memperoleh artikel ilmiah yang relevan dengan keamanan dan otomatisasi pada *Intent-Based Networking*.

Adapun kata kunci yang digunakan pada penelitian ini meliputi:

1. *Intent-Based Networking*
2. *Network Automation*
3. *Network Security*
4. *Software Defined Networking*
5. *Artificial Intelligence in Networking*
6. *Intent-driven Network Management*
7. *Autonomous Network*
8. *Security Orchestration*

Kata kunci tersebut digunakan secara terpisah maupun dikombinasikan menggunakan operator Boolean seperti *AND* dan *OR* untuk memperoleh hasil pencarian artikel yang lebih spesifik dan relevan dengan topik penelitian.

E. Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi digunakan untuk menentukan artikel yang layak digunakan dalam penelitian. Proses ini bertujuan agar artikel yang dianalisis sesuai dengan fokus penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking*.

Kriteria inklusi pada penelitian ini meliputi:

1. Artikel ilmiah internasional yang membahas keamanan dan otomatisasi pada *Intent-Based Networking*.
2. Artikel diterbitkan pada periode 2021–2026.
3. Artikel berasal dari jurnal atau prosiding internasional bereputasi.
4. Artikel memiliki keterkaitan dengan teknologi *Software Defined Networking* (SDN), *Artificial Intelligence* (AI), *Network Automation*, dan keamanan jaringan.
5. Artikel tersedia dalam bahasa Inggris dan dapat diakses dalam bentuk *full text*.

Sementara itu, kriteria eksklusi pada penelitian ini meliputi:

1. Artikel yang tidak membahas keamanan atau otomatisasi pada *Intent-Based Networking*.
2. Artikel dengan tahun publikasi di luar periode 2021–2026.
3. Artikel yang tidak tersedia dalam bentuk teks lengkap (*full text*).
4. Artikel yang bersifat duplikasi dari database lain.
5. Artikel yang tidak memiliki keterkaitan dengan fokus penelitian.

F. Teknik Analasis Data

Teknik analisis data pada penelitian ini dilakukan menggunakan metode analisis deskriptif. Analisis deskriptif digunakan untuk menggambarkan perkembangan penelitian berdasarkan fokus penelitian, metode penelitian, teknologi yang digunakan, serta tantangan keamanan dan otomatisasi pada *Intent-Based Networking* (Page et al., 2021; Sunaryo et al., 2023).

Artikel yang telah diseleksi kemudian dianalisis berdasarkan beberapa aspek, seperti teknologi yang digunakan, metode otomatisasi jaringan, mekanisme keamanan, serta implementasi *Intent-Based Networking* pada berbagai lingkungan jaringan modern. Selain itu, penelitian juga menganalisis perkembangan penggunaan teknologi *Software Defined Networking* (SDN), *Artificial Intelligence* (AI), *Machine Learning*, dan *Network Automation* dalam mendukung implementasi IBN.

Selanjutnya, hasil analisis literatur disintesis untuk memperoleh gambaran mengenai tren penelitian, tantangan implementasi, mekanisme keamanan, serta peluang pengembangan keamanan dan otomatisasi pada *Intent-Based Networking*. Hasil sintesis tersebut digunakan sebagai dasar dalam menyusun pembahasan dan kesimpulan penelitian.

4. HASIL DAN PEMBAHASAN

A. Hasil Analisis Literatur

Berdasarkan proses seleksi literatur menggunakan pendekatan *Systematic Literature Review* (SLR) berbasis PRISMA 2020, diperoleh 11 artikel internasional bereputasi yang relevan dengan topik keamanan dan otomatisasi pada *Intent-Based Networking* (IBN). Distribusi penelitian menunjukkan bahwa kajian mengenai IBN mengalami peningkatan signifikan pada periode 2021–2026 seiring berkembangnya teknologi *Software Defined Networking* (SDN), *Artificial Intelligence* (AI), *Internet of Things* (IoT), dan jaringan 5G.

Sebagian besar penelitian berfokus pada implementasi otomatisasi jaringan, keamanan jaringan, translasi *intent*, *security orchestration*, serta integrasi teknologi AI dan *Machine Learning* dalam pengelolaan jaringan modern. Selain itu, hasil kajian menunjukkan bahwa implementasi IBN mampu meningkatkan efisiensi pengelolaan jaringan melalui otomatisasi konfigurasi jaringan, optimasi trafik, dan pengambilan keputusan secara adaptif berdasarkan kondisi jaringan secara *real-time*.

Namun demikian, implementasi IBN juga menghadapi berbagai tantangan seperti manipulasi *intent*, kesalahan translasi kebijakan jaringan, peningkatan *attack surface*, serta kompleksitas integrasi antar sistem otomatisasi jaringan. Selain itu, sebagian besar penelitian masih dilakukan pada lingkungan simulasi sehingga validasi pada kondisi jaringan nyata masih perlu dikembangkan lebih lanjut.

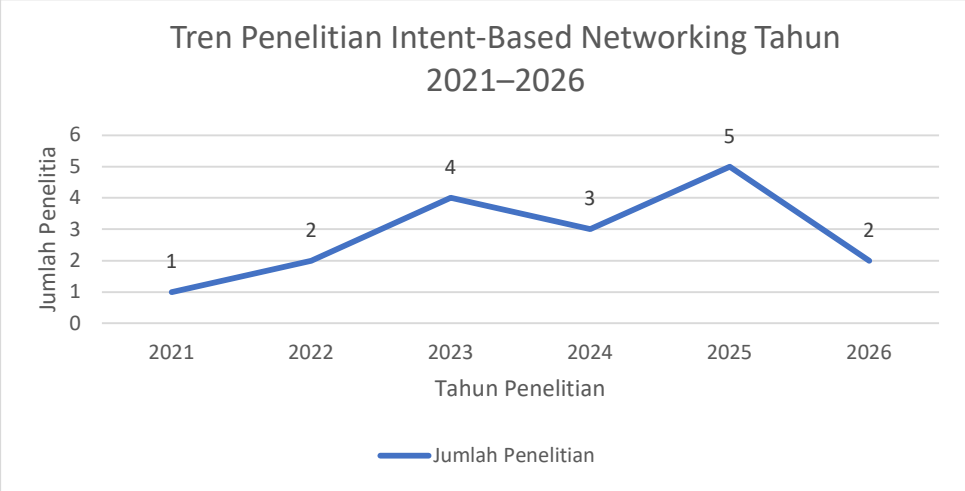
Ringkasan parameter hasil analisis literatur disajikan pada Tabel 2.

Tabel 2. Ringkasan Hasil Analisis Literatur *Intent-Based Networking*

Parameter	Temuan Utama	Dampak
Otomatisasi Jaringan	Konfigurasi jaringan dilakukan otomatis	Mengurangi *human error*
Keamanan Jaringan	Peningkatan penggunaan *security orchestration*	Respons keamanan lebih adaptif
Translasi *Intent*	AI dan *Machine Learning* meningkatkan akurasi translasi	Pengelolaan jaringan lebih efisien
Integrasi SDN	SDN mendukung kontrol jaringan terpusat	Jaringan lebih fleksibel
Network Monitoring	Monitoring dilakukan secara *real-time*	Optimasi trafik lebih cepat

Parameter	Temuan Utama	Dampak
Tantangan Implementasi	Kompleksitas integrasi dan keamanan	Membutuhkan mekanisme proteksi tambahan

Berdasarkan Tabel 2, penelitian mengenai *Intent-Based Networking* sebagian besar berfokus pada pengembangan otomatisasi jaringan dan keamanan jaringan berbasis AI serta SDN. Selain itu, integrasi *Machine Learning* dan *security orchestration* menunjukkan peningkatan signifikan dalam mendukung pengelolaan jaringan modern yang lebih adaptif dan cerdas. Untuk memberikan gambaran mengenai perkembangan penelitian *Intent-Based Networking* pada periode 2021–2026, dilakukan analisis distribusi publikasi penelitian berdasarkan tahun publikasi. Tren penelitian tersebut dapat dilihat pada Gambar 3.



Gambar 3. Tren Penelitian Intent-Based Networking Tahun 2021–2026

B. Klasifikasi Pendekatan Penelitian

Berdasarkan hasil analisis literatur, pendekatan penelitian mengenai keamanan dan otomatisasi pada *Intent-Based Networking* dapat diklasifikasikan menjadi beberapa kategori utama, yaitu pendekatan berbasis keamanan jaringan, otomatisasi jaringan, *Artificial Intelligence* (AI), *Machine Learning*, dan *security orchestration*.

Pendekatan berbasis keamanan jaringan berfokus pada pengembangan mekanisme proteksi jaringan seperti *authentication*, *policy verification*, dan *security orchestration* untuk mengatasi ancaman keamanan pada implementasi IBN. Penelitian Ahmad et al. (2023) menunjukkan bahwa tantangan keamanan pada IBN meliputi manipulasi *intent*, kesalahan translasi kebijakan, dan serangan terhadap *orchestrator*.

Pendekatan berbasis otomatisasi jaringan bertujuan meningkatkan efisiensi pengelolaan jaringan melalui konfigurasi otomatis, monitoring jaringan secara *real-time*, dan optimasi trafik jaringan. Selain itu, pendekatan berbasis AI dan *Machine Learning* digunakan untuk meningkatkan akurasi translasi *intent* pengguna menjadi kebijakan jaringan otomatis.

Sementara itu, pendekatan berbasis *security orchestration* digunakan untuk meningkatkan kemampuan jaringan dalam mendeteksi dan merespons ancaman keamanan secara otomatis dan adaptif. Integrasi berbagai pendekatan tersebut menunjukkan bahwa implementasi IBN semakin berkembang menuju jaringan cerdas

(*autonomous network*) yang mampu melakukan pengelolaan jaringan secara otomatis dan aman.

C. Tabel Perbandingan Penelitian

Untuk memberikan gambaran komprehensif mengenai penelitian terdahulu, dilakukan perbandingan beberapa penelitian berdasarkan fokus penelitian, teknologi yang digunakan, hasil penelitian, kelebihan, dan keterbatasan masing-masing penelitian. Perbandingan tersebut disajikan pada Tabel 3.

Tabel 3. Perbandingan Penelitian Keamanan dan Otomatisasi pada *Intent-Based Networking*

Peneliti	Fokus Penelitian	Teknologi	Hasil Utama	Kelebihan	Keterbatasan
Ahmad et al. (2023)	Keamanan IBN	Security Orchestration	Mengidentifikasi ancaman keamanan IBN	Fokus keamanan jaringan	Tidak membahas otomatisasi
Mehmood et al. (2023)	*Autonomous Network*	AI, IBN	Pengelolaan jaringan lebih otomatis	Mendukung jaringan cerdas	Kompleksitas implementasi
Sunaryo et al. (2023)	Otomatisasi jaringan	AI, SDN	Otomatisasi jaringan meningkat	Analisis tren otomatisasi	Fokus QoS
Manias et al. (2024)	*Intent Extraction*	LLM, AI	Translasi *intent* lebih akurat	Mendukung otomatisasi AI	Belum fokus keamanan
Kim et al. (2024)	Tantangan keamanan IBN	Security	Peningkatan *attack surface*	Analisis ancaman jaringan	Tidak membahas AI
Trantzas et al. (2025)	*Network Automation*	Generative AI	Otomatisasi jaringan lebih adaptif	Integrasi AI modern	Kompleksitas tinggi
AlSamarneh et al. (2025)	Translasi *Intent*	Machine Learning	Akurasi translasi meningkat	Efisiensi konfigurasi jaringan	Membutuhkan data besar
Sadouki & Kornyshova (2025)	IBN pada *Industry 4.0*	IoT, IBN	Mendukung jaringan industri	Mendukung otomatisasi industri	Integrasi sistem kompleks
Huang et al. (2026)	*Security Orchestration*	AI Security	Respons keamanan otomatis	Integrasi keamanan dan AI	Implementasi kompleks
Penelitian ini	Kajian Literatur Sistematis	IBN, SDN, AI	Analisis keamanan dan otomatisasi IBN	Sintesis komprehensif	Tidak melakukan eksperimen langsung

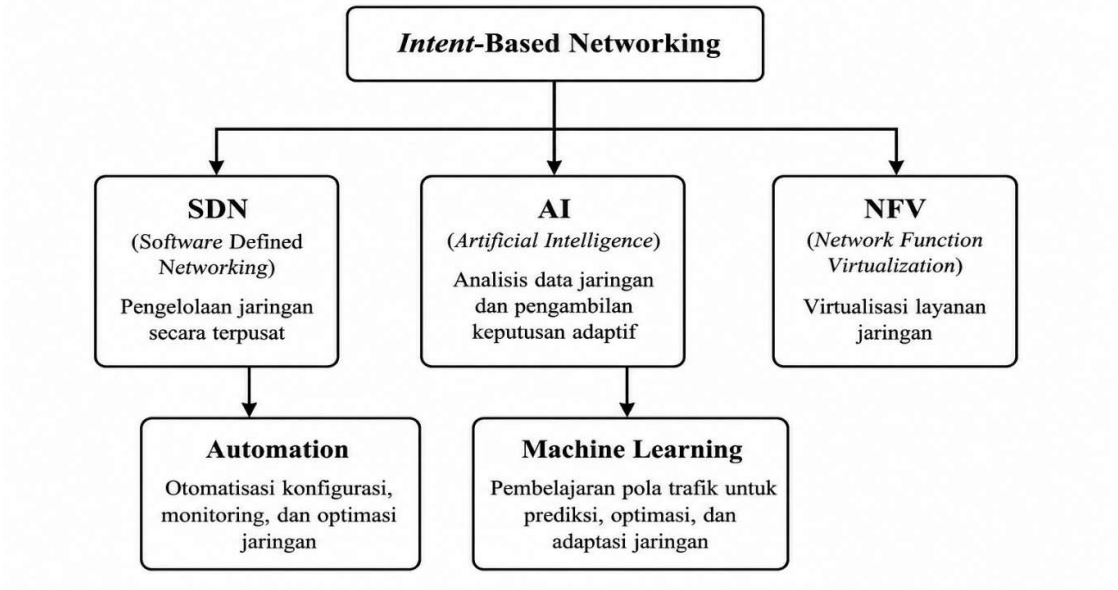
Berdasarkan Tabel 3, sebagian besar penelitian terdahulu masih berfokus pada aspek keamanan atau otomatisasi secara terpisah. Penelitian terbaru mulai mengintegrasikan AI, *Machine Learning*, dan *security orchestration* untuk mendukung implementasi jaringan otomatis yang lebih aman dan adaptif. Namun demikian, masih terdapat tantangan terkait kompleksitas integrasi sistem dan keamanan jaringan pada implementasi IBN modern.

D. Analisis Keamanan dan Otomatisasi pada *Intent-Based Networking*

Keamanan dan otomatisasi merupakan dua komponen utama dalam implementasi *Intent-Based Networking*. Berdasarkan hasil kajian literatur, otomatisasi jaringan mampu meningkatkan efisiensi pengelolaan jaringan melalui konfigurasi otomatis, monitoring jaringan secara *real-time*, serta optimasi layanan jaringan berdasarkan kondisi trafik jaringan.

Implementasi otomatisasi jaringan pada IBN umumnya didukung oleh teknologi SDN, AI, *Machine Learning*, dan *Network Function Virtualization* (NFV). Integrasi teknologi tersebut memungkinkan jaringan melakukan pengelolaan layanan secara otomatis, fleksibel, dan adaptif.

Di sisi lain, implementasi otomatisasi jaringan juga meningkatkan risiko ancaman keamanan akibat integrasi berbagai sistem jaringan cerdas yang saling terhubung. Tantangan keamanan pada IBN meliputi manipulasi *intent*, kesalahan translasi kebijakan jaringan, serangan terhadap *orchestrator*, dan peningkatan *attack surface*. Oleh karena itu, mekanisme keamanan seperti *security orchestration*, *authentication*, dan *policy verification* menjadi aspek penting dalam implementasi IBN modern. Implementasi *Intent-Based Networking* didukung oleh integrasi berbagai teknologi modern yang memungkinkan pengelolaan jaringan dilakukan secara otomatis, fleksibel, dan adaptif. Hubungan antar teknologi pendukung tersebut dapat dilihat pada Gambar 4.



Gambar 4. Teknologi Pendukung *Intent-Based Networking*

Berdasarkan Gambar 4, implementasi *Intent-Based Networking* didukung oleh teknologi SDN, AI, NFV, dan *Machine Learning*. Teknologi SDN berperan dalam pengelolaan jaringan secara terpusat, sedangkan AI dan *Machine Learning* digunakan untuk mendukung otomatisasi dan pengambilan keputusan jaringan secara adaptif. Selain itu, NFV memungkinkan virtualisasi layanan jaringan sehingga implementasi jaringan menjadi lebih fleksibel dan efisien.

E. Pembahasan

Secara keseluruhan, hasil kajian menunjukkan bahwa implementasi *Intent-Based Networking* mampu meningkatkan efisiensi pengelolaan jaringan modern melalui otomatisasi konfigurasi jaringan, monitoring jaringan secara otomatis, dan optimasi trafik berbasis AI. Integrasi teknologi SDN, AI, dan *Machine Learning* memungkinkan jaringan melakukan pengambilan keputusan secara otomatis berdasarkan kondisi jaringan secara *real-time*.

Namun demikian, implementasi IBN masih menghadapi berbagai tantangan seperti keamanan jaringan, kompleksitas integrasi sistem, interoperabilitas perangkat jaringan, serta kebutuhan sumber daya komputasi yang tinggi. Selain itu, sebagian besar penelitian masih dilakukan pada lingkungan simulasi sehingga implementasi pada kondisi jaringan nyata masih memerlukan penelitian lebih lanjut.

Perkembangan teknologi AI, *Large Language Model* (LLM), *Machine Learning*, dan *security orchestration* menunjukkan peluang besar dalam pengembangan jaringan otomatis yang lebih aman, adaptif, dan cerdas pada masa mendatang.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil *Systematic Literature Review* (SLR) terhadap keamanan dan otomatisasi pada *Intent-Based Networking* (IBN), dapat disimpulkan bahwa implementasi IBN mampu meningkatkan efisiensi pengelolaan jaringan melalui otomatisasi konfigurasi, monitoring jaringan secara *real-time*, serta optimasi layanan jaringan secara adaptif. Integrasi teknologi *Software Defined Networking* (SDN), *Artificial Intelligence* (AI), *Machine Learning*, dan *Network Function Virtualization* (NFV) memberikan kontribusi besar dalam mendukung pengembangan jaringan modern yang lebih fleksibel, cerdas, dan terpusat.

Hasil kajian menunjukkan bahwa otomatisasi jaringan pada IBN mampu mengurangi *human error*, meningkatkan efisiensi pengelolaan jaringan, serta mempercepat proses pengambilan keputusan jaringan berdasarkan kondisi trafik secara dinamis. Selain itu, penerapan *security orchestration* dan AI juga meningkatkan kemampuan jaringan dalam mendeteksi serta merespons ancaman keamanan secara otomatis dan adaptif.

Namun demikian, implementasi IBN masih menghadapi berbagai tantangan, seperti manipulasi *intent*, kesalahan translasi kebijakan jaringan, peningkatan *attack surface*, kompleksitas integrasi sistem, serta kebutuhan sumber daya komputasi yang tinggi. Selain itu, sebagian besar penelitian yang dianalisis masih dilakukan pada lingkungan simulasi sehingga validasi implementasi pada kondisi jaringan nyata masih perlu dikembangkan lebih lanjut.

Berdasarkan hasil penelitian tersebut, penelitian selanjutnya disarankan untuk lebih banyak melakukan implementasi dan pengujian IBN pada lingkungan jaringan nyata (*real-world environment*) dengan skenario jaringan yang lebih kompleks. Selain itu, pengembangan integrasi AI, *Large Language Model* (LLM), *Machine Learning*, dan

security orchestration juga perlu ditingkatkan untuk mendukung implementasi jaringan otomatis yang lebih aman, adaptif, dan efisien pada masa mendatang.

DAFTAR REFERENSI

Ahmad, I., Malinen, J., Christou, F., Porambage, P., Kirstadter, A., & Suomalainen, J. (2023). Security in Intent-Based Networking: Challenges and Solutions. *2023 IEEE Conference on Standards for Communications and Networking, CSCN 2023*, 296–301. https://doi.org/10.1109/CSCN60443.2023.10453125

AlSamarneh, A. A., Al-Hammouri, A. T., & Al-Jarrah, O. Y. (2025). Navigating intent-based networking: from user descriptions to deployable configurations. *Neural Computing and Applications*, *37*(22), 17723–17758. https://doi.org/10.1007/s00521-025-11193-7

He, T., Toosi, A. N., Akbari, N., Islam, M. T., & Cheema, M. A. (2023). An Intent-based Framework for Vehicular Edge Computing. *2023 IEEE International Conference on Pervasive Computing and Communications, PerCom 2023*, 121–130. https://doi.org/10.1109/PERCOM56429.2023.10099081

Huang, Z., Robin, J., Herbaut, N., Ben Rabah, N., & Le Grand, B. (2026). Toward an Intent-Based and Ontology-Driven Autonomic Security Response in Security Orchestration Automation and Response. *Lecture Notes in Computer Science*, *16213 LNCS*(c), 266–283. https://doi.org/10.1007/978-3-032-15140-7_15

Kim, J., Okhravi, H., Tian, D. J., & Ujcich, B. E. (2024). Security Challenges of Intent-Based Networking. *Communications of the ACM*, *67*(7), 56–65. https://doi.org/10.1145/3639702

Manias, D. M., Chouman, A., & Shami, A. (2024). Towards Intent-Based Network Management: Large Language Models for Intent Extraction in 5G Core Networks. *20th International Conference on the Design of Reliable Communication Networks, DRCN 2024*, 1–7. https://doi.org/10.1109/DRCN60692.2024.10539172

Mehmood, K., Kralevska, K., & Palma, D. (2023). Intent-driven autonomous network and service management in future cellular networks: A structured literature review. *Computer Networks*, *220*(November 2022), 109477. https://doi.org/10.1016/j.comnet.2022.109477

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

Sadouki, K., & Kornyshova, E. (2025). Intent-based approaches for industry 4.0 applications: A systematic mapping study. *Internet of Things (The Netherlands)*, *32*. https://doi.org/10.1016/j.iot.2025.101629

Sunaryo, B., Rusydi, M. I., Hazmi, A., & Sasaki, M. (2023). A Systematic Literature Review of Automation Quality of Service in Computer Networks: Research Trends, Datasets, and Methods. *Jurnal RESTI*, *7*(2), 353–366. https://doi.org/10.29207/resti.v7i2.4810

Trantzas, K., Brodimas, D., Agko, B., Tziavas, G. C., Tranoris, C., Denazis, S., & Birbas, A. (2025). Intent-driven network automation through sustainable multimodal generative AI. *Eurasip Journal on Wireless Communications and Networking*, *2025*(1). https://doi.org/10.1186/s13638-025-02472-x