Journal of System & Technology
e-ISSN: XXXX-XXXX
Vol. 1, No. 1, Juni 2025

PENGARUH TEKNOLOGI 5G TERHADAP ARSITEKTUR DAN KEAMANAN JARINGAN

Rakhmadi Rahman[1], Reski Septiawan[1], Natasya Taslim[1]
[1]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare
rakhmadi.rahman@ith.ac.id, reskysptwn89@gmail.com, natasyataslim63@gmail.com
*Corresponding author: rakhmadi.rahman@ith.ac.id

Abstract: Teknologi jaringan seluler generasi kelima (5G) membawa perubahan fundamental terhadap arsitektur dan keamanan jaringan. Penelitian ini membahas transformasi arsitektur dari model monolitik menuju Service-Based Architecture (SBA) serta penerapan teknologi seperti Network Function Virtualization (NFV), Software-Defined Networking (SDN), dan Network Slicing dalam konteks jaringan 5G. Selain itu, kajian ini menyoroti tantangan keamanan baru yang muncul, termasuk kerentanan API, ancaman dari konektivitas masif perangkat IoT, dan perlunya sistem enkripsi yang adaptif. Metode yang digunakan adalah studi literatur dengan pendekatan deskriptif kualitatif, yang mengidentifikasi pola ancaman dan solusi mitigasi berdasarkan referensi ilmiah terkini. Hasil analisis menunjukkan bahwa penerapan arsitektur Zero Trust dan pemanfaatan kecerdasan buatan untuk deteksi ancaman dini menjadi kunci dalam menjaga integritas jaringan 5G yang bersifat terbuka dan modular.

Keywords—5G, Arsitektur Jaringan, Keamanan Jaringan, NFV, SDN

I. PENDAHULUAN

Transformasi teknologi komunikasi telah mengalami perkembangan pesat dari generasi pertama (1G) hingga generasi kelima (5G)[1][2]. Teknologi 5G menjadi puncak evolusi jaringan seluler yang menawarkan latensi rendah, kecepatan data tinggi, serta kemampuan konektivitas masif. Kemunculan 5G tidak hanya membawa peningkatan performa teknis, namun juga mendefinisikan ulang struktur dan arsitektur jaringan yang mendasarinya. Teknologi ini mengintegrasikan prinsip-prinsip modern seperti virtualisasi fungsi jaringan (NFV), jaringan yang dapat diprogram secara lunak (SDN), dan arsitektur berbasis layanan (SBA) yang memisahkan komponen fungsional menjadi entitas modular berbasis API[2][3][4].

Dengan kompleksitas tersebut, muncul tantangan baru yang berkaitan dengan keamanan jaringan. Arsitektur yang terbuka dan terdistribusi meningkatkan risiko terhadap serangan siber seperti Denial of Service (DoS), penyadapan (sniffing), pemalsuan identitas (spoofing), serta penyusupan (intrusion) melalui titik-titik rentan seperti interface API dan perangkat IoT[5][6]. Selain itu, keberadaan ribuan hingga jutaan perangkat yang terkoneksi secara bersamaan dalam ekosistem 5G memerlukan mekanisme manajemen identitas dan autentikasi yang jauh lebih kuat dibanding generasi sebelumnya[7][8][9].

Di Indonesia, penerapan jaringan 5G telah dimulai secara bertahap sejak tahun 2021. Namun, penyebaran infrastruktur masih terbatas di kota-kota besar dan belum menyentuh daerah terpencil secara merata. Di samping tantangan infrastruktur, aspek keamanan juga menjadi sorotan karena berbagai aktor ancaman mulai mengalihkan fokusnya ke jaringan generasi terbaru ini[10][11][12].

Oleh karena itu, penelitian ini bertujuan untuk mengkaji secara mendalam pengaruh teknologi 5G terhadap struktur arsitektur dan keamanan jaringan berdasarkan studi literatur. Hasil kajian ini diharapkan dapat memberikan kontribusi dalam pengembangan strategi keamanan dan arsitektur jaringan yang lebih tangguh dan adaptif dalam menghadapi era konektivitas cerdas yang ditawarkan oleh 5G.

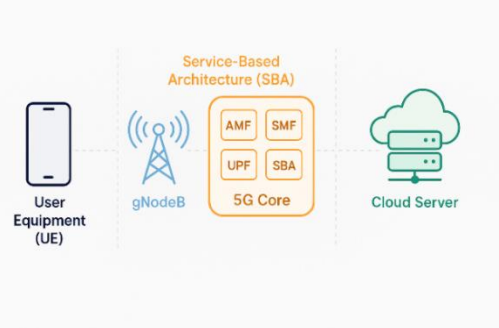
II. TINJAUAN PUSTAKA

A. *Teknologi 5G*

5G adalah teknologi komunikasi seluler generasi kelima yang mengedepankan tiga skenario utama: enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communication (URLLC), dan massive Machine Type Communication (mMTC). Teknologi ini mendukung penerapan millimeter wave, Massive MIMO, beamforming, dan spektrum frekuensi tinggi[13].

B. *Arsitektur Jaringan 5G*

Perubahan paling menonjol dari jaringan 5G adalah Service-Based Architecture (SBA) pada core network[4]. Fungsi seperti AMF, SMF, dan UPF dapat dijalankan secara terpisah dan diatur melalui API. Selain itu, teknologi seperti MEC (Multi-access Edge Computing) mempercepat pemrosesan data di dekat pengguna (gambar 1)[15].



Gambar 1. Diagram Arsitektur 5G

C. *Isu Keamanan 5G*

Arsitektur terbuka dan konektivitas masif memperbesar risiko terhadap berbagai serangan siber.

Identitas perangkat yang beragam dan trafik data yang dinamis memerlukan sistem autentikasi adaptif. Penelitian menunjukkan perlunya sistem enkripsi canggih, keamanan berbasis AI, dan segmentasi jaringan yang cermat[10][12].

III. METODOLOGI

Penelitian ini menggunakan metode studi pustaka dengan pendekatan deskriptif kualitatif (tabel 1). Data diperoleh dari jurnal ilmiah nasional dan internasional terakreditasi antara tahun 2020 hingga 2025. Analisis dilakukan dengan langkah-langkah reduksi data, klasifikasi tematik, dan sintesis konten untuk mengidentifikasi pola dan kesenjangan pada aspek arsitektur dan keamanan jaringan 5G [13][14].

Tabel 1. Metodologi Penelitian

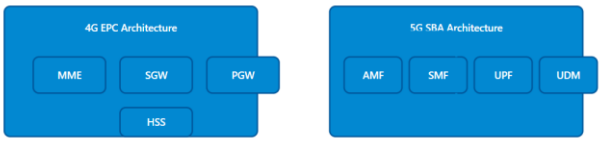
Komponen	Deskripsi
Desain Penelitian	Penelitian deskriptif kualitatif dengan studi literatur terkait keamanan jaringan 5G.
Sumber Data	Jurnal ilmiah, buku, artikel konferensi, laporan industri, publikasi resmi.
Proses Pengumpulan Data	- Identifikasi sumber terpercaya (IEEE Xplore, ScienceDirect, SpringerLink, dll.) - Kriteria inklusi: relevansi, peer-reviewed, publikasi ≤5 tahun terakhir - Pengunduhan artikel, pencatatan data penting untuk analisis.
Teknik Analisis Data	- Kategorisasi ancaman keamanan jaringan 5G - Analisis deskriptif untuk tren dan pola ancaman - Sintesis temuan dan rekomendasi mitigasi.
Validasi Data	Triangulasi sumber, evaluasi relevansi data, double-check referensi, dan validasi isi.
Tujuan Analisis	Memahami pola ancaman 5G dan menyusun strategi mitigasi keamanan yang relevan.

IV. HASIL DAN PEMBAHASAN

A. *Perubahan Arsitektur Jaringan*

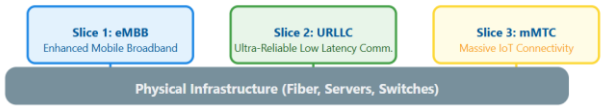
Teknologi 5G menggantikan model EPC (Evolved Packet Core) dengan arsitektur SBA. Komponen inti seperti AMF dan UPF dapat berjalan dalam lingkungan virtual yang scalable. Network Slicing memungkinkan pemisahan logis jaringan sesuai kebutuhan layanan[15][16].

Gambar 2 menunjukkan perbandingan antara arsitektur 4G dan 5G. Dalam gambar tersebut, terlihat bahwa fungsi inti seperti Mobility Management Entity (MME), Serving Gateway (SGW), dan Packet Gateway (PGW) pada 4G digantikan oleh fungsi-fungsi baru dalam SBA, yaitu Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), dan Unified Data Management (UDM). Fungsi-fungsi ini dapat berjalan secara terpisah dan berinteraksi melalui Application Programming Interface (API), yang memungkinkan pengelolaan sumber daya yang lebih efisien dan penerapan layanan yang lebih dinamis.



Gambar 2. Perbandingan general antara 4G EPC dengan 5G Service-Based Architecture, menampilkan komponen inti dan interaksi layanan

Selain itu, teknologi Network Slicing memungkinkan infrastruktur fisik jaringan dibagi menjadi beberapa jaringan virtual yang independen sesuai dengan kebutuhan layanan.

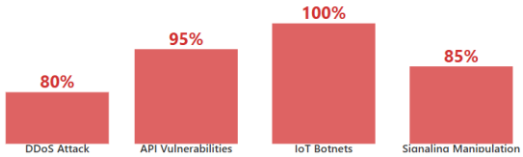


Gambar 3. Konsep Network Slicing pada Jaringan 5G

Gambar 3 menggambarkan konsep ini, di mana satu slice dapat difokuskan untuk enhanced Mobile Broadband (eMBB), slice lain untuk Ultra Reliable Low Latency Communication (URLLC), dan slice lain untuk massive Machine Type Communication (mMTC). Dengan pemisahan ini, setiap layanan mendapatkan sumber daya dan konfigurasi jaringan yang spesifik, memastikan performa optimal.

B. *Ancaman Keamanan dalam 5G*

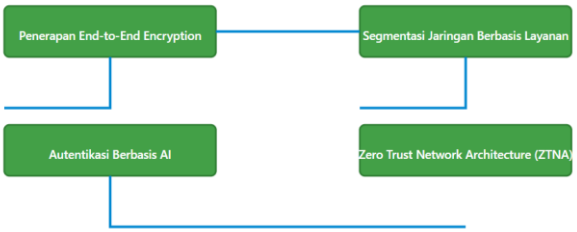
Penggunaan API antar layanan menimbulkan tantangan baru seperti manipulasi signaling dan penyusupan fungsi jaringan[17][18]. Koneksi perangkat IoT menambah permukaan serangan yang harus dilindungi.



Gambar 4. Jenis Ancaman Keamanan dalam Jaringan 5G

Gambar 4 menggambarkan jenis-jenis ancaman keamanan utama pada jaringan 5G serta tingkat risiko relatifnya. Dalam gambar tersebut, terlihat bahwa ancaman seperti Distributed Denial of Service (DDoS), kerentanan API, botnet IoT, dan manipulasi signaling memiliki tingkat risiko yang bervariasi. Kerentanan-kerentanan ini membutuhkan perhatian khusus agar jaringan tetap aman dan andal. Penelitian menunjukkan bahwa ancaman ini dapat dieksploitasi dengan lebih mudah jika mekanisme keamanan tidak dirancang secara menyeluruh.

C. *Strategi Mitigasi dan Solusi*



Gambar 5. Strategi Mitigasi Keamanan 5G

Untuk mengatasi kerentanan dan risiko yang dihadapi oleh jaringan 5G, diperlukan serangkaian strategi mitigasi yang efektif. Gambar 5 menunjukkan flowchart alur strategi mitigasi keamanan yang direkomendasikan. Langkah-langkah yang diusulkan meliputi:

1) Penerapan Enkripsi End-to-End: Mengamankan data yang ditransmisikan antara perangkat dan jaringan untuk mencegah penyadapan[16].
2) Segmentasi Jaringan Berbasis Layanan: Memisahkan jaringan berdasarkan jenis layanan untuk membatasi akses dan mengurangi risiko.
3) Autentikasi Berbasis AI: Menggunakan kecerdasan buatan untuk meningkatkan keamanan identitas perangkat dan mendeteksi perilaku mencurigakan[17].
4) Zero Trust Network Architecture (ZTNA): Mengadopsi pendekatan di mana tidak ada perangkat atau pengguna yang dipercaya secara otomatis, sehingga semua akses harus divalidasi[18].

Pendekatan ini menyelaraskan keamanan dengan fleksibilitas arsitektur 5G, memastikan bahwa meskipun jaringan bersifat terbuka dan modular, mekanisme proteksi tetap berjalan dengan kuat dan adaptif terhadap serangan.

D. *Integrasi Deteksi Dini dan Pembelajaran Mesin*



Gambar 6. Diagram Alur Data

Gambar 6 memperlihatkan integrasi sistem deteksi dini yang memanfaatkan pembelajaran mesin (machine learning) dalam arsitektur keamanan 5G. Data aktivitas host dan jaringan dikumpulkan dan dianalisis oleh sistem AI untuk mendeteksi pola anomali dan perilaku berbahaya yang tidak selalu teridentifikasi oleh metode berbasis signature. Sistem ini mampu memberikan tanggapan otomatis berupa alarm atau mitigasi untuk mencegah serangan berlapis yang kompleks[19].

Dengan menggabungkan berbagai parameter aktivitas, seperti beban CPU, durasi login, aktivitas file, dan pola lalu lintas jaringan, sistem pembelajaran mesin menciptakan profil keamanan adaptif yang kontekstual[13]. Pendekatan ini sangat penting mengingat besarnya skala dan dinamika jaringan 5G yang tidak bisa dikontrol secara manual sepenuhnya[20].

V. KESIMPULAN

Teknologi 5G membawa reformasi besar pada sistem komunikasi dan arsitektur jaringan. Namun, kemajuan ini dibarengi risiko keamanan yang lebih luas dan kompleks. Oleh karena itu, perancangan dan implementasi 5G harus memasukkan prinsip keamanan sejak tahap awal desain, serta memanfaatkan teknologi mutakhir seperti kecerdasan buatan dan kriptografi lanjutan untuk memastikan keandalan dan perlindungan jaringan.

VI. SARAN

Sebagai tindak lanjut dari penelitian ini, disarankan untuk melakukan penelitian lebih lanjut guna mengembangkan metode keamanan yang semakin canggih, khususnya dalam menerapkan algoritma pembelajaran mesin untuk deteksi dini ancaman di jaringan 5G. Selain itu, organisasi perlu mempertimbangkan penerapan Zero Trust Network Architecture agar akses terhadap sumber daya jaringan dapat dikontrol secara ketat dan aman. Pendidikan dan pelatihan mengenai keamanan siber juga penting diberikan kepada masyarakat, terutama bagi pengguna perangkat IoT yang terhubung ke jaringan 5G. Terakhir, evaluasi dan pengujian keamanan secara berkala perlu dilakukan untuk mengidentifikasi dan mengatasi kerentanan yang mungkin muncul dalam infrastruktur jaringan 5G, sehingga keandalan dan keamanan jaringan dapat terus terjaga.

REFERENCES

[1] R. W. Coêlho, R. A. Silva, L. A. F. Martimiano, and E. J. Leonardo, "IoT and 5G Networks: A Discussion of SDN, NFV and Information Security," J. Braz. Comput. Soc., vol. 30, no. 1, pp. 212–227, 2024.
[2] H. Hawilo, M. Jammal, A. Shami, and R. Asal, "Exploring microservices as the architecture of choice for NFV platforms," IEEE Netw., vol. 33, no. 2, pp. 184–191, 2019.
[3] F. B. Wala and M. Kiran, "5G Network Security Practices: An Overview and Survey," arXiv preprint arXiv:2401.14350, 2024.
[4] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Wang, "A Survey on Security Aspects for 3GPP 5G Networks," IEEE Commun. Surv. Tutor., vol. 22, no. 1, pp. 170–195, 2020.
[5] 3GPP, "System Architecture for the 5G System," 3GPP TS 23.501, Release 16, Dec. 2020.
[6] G. Nencioni, R. G. Garroppo, S. Giordano, and R. F. Olimid, "5G Multi-access Edge Computing: A Survey on Security, Dependability, and Performance," arXiv preprint arXiv:2107.13374, 2021.
[7] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, and J. J. Ramos-Munoz, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 80–87, May 2017.
[8] P. Esteves-Verissimo, R. Nejabati, and D. Simeonidou, "Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security," Int. J. Inf. Secur., vol. 23, 2024.
[9] H. N. Fakhouri, M. A. Khan, and M. A. Jan, "Machine Learning in 5G Security: A Comprehensive Survey," Electronics, vol. 12, no. 22, p. 4604, 2023.
[10] S. Gunawan and A. A. R. Santosa, "Analisis Keamanan Jaringan 5G: Ancaman dan Upaya Mitigasi," J. Ilm. Tek. Inform., vol. 9, no. 1, pp. 45–52, 2024.

[11] A. B. Maulana et al., “Analisis Serangan Denial of Service pada Jaringan Privat 5G,” Tech. Rep., Telkom University, 2022.
[12] Febriyani, “Keamanan Sistem Informasi Jaringan 5G di Indonesia,” ResearchGate, [Online]. Available: https://www.researchgate.net/publication/xxxx. [Accessed: May 29, 2025].
[13] H. P. Fitrian, A. S. Nugroho, and T. R. Naufal, “Implikasi 5G terhadap Performa dan Keamanan,” JATI ITN Malang, vol. 7, no. 2, pp. 101–110, 2025.
[14] A. Yani, D. Fitria, and M. A. Lubis, “Keamanan dan Kecepatan 5G dalam Implementasi IoT,” J. Appl. Technol., vol. 3, no. 1, pp. 55–63, 2024.
[15] R. Rahman, A. Arthanty, and A. N. Putri, “Pengembangan Sistem Deteksi Dini Serangan APT (Advanced Persistent Threat),” J. Syst. Technol., vol. 5, no. 1, pp. 12–22, 2025.
[16] N. Haider, M. Z. Shafiq, and A. X. Liu, “Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, Advantages, and Future Research Trends,” IEEE Access, vol. 8, pp. 219–235, 2020.
[17] K. Ramezanpour and J. Jagannath, “Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN,” arXiv preprint arXiv:2105.01478, 2021.
[18] T. Sachdeva, A. Sharma, and R. Khanna, “Comparative Analysis of 5G Security Mechanisms,” in Proc. 6th Int. Conf. Inf. Syst. Comput. Netw. (ISCON), Mathura, India, 2023, pp. 1–4.
[19] P. Scalise, A. Cicchetti, D. Gallo, and A. Petitti, “A Systematic Survey on 5G and 6G Security: Considerations, Challenges, Trends, and Research Areas,” Future Internet, vol. 16, no. 3, p. 67, 2024.
[20] M. Vomvas, N. Ludant, and G. Noubir, “Establishing Trust in the Beyond-5G Core Network using Trusted Execution Environments,” arXiv preprint arXiv:2405.12177, 2024.