PENGARUH IMPLEMENTASI 5G TERHADAP KEAMANAN SIBER : RISIKO DAN MITIGASI

Harry Pribadi Fitrian, Adilla Rezqy Yasiyroh, Fazar Rizwanul Ikhlas, Nur Anisa Fitri, Siti Fatimah
Informatika, Universitas Teknologi Digital
Jl. Raya Janti Karang Jambe No. 143, Yogyakarta
harrypribadi@digitechuniversity.ac.id

ABSTRAK

Perkembangan teknologi jaringan kini memasuki era 5G. Keunggulan teknologi 5G menawarkan kecepatan data tinggi, latensi rendah, dan kapasitas besar yang mendukung transformasi digital di berbagai sektor, termasuk pada perangkat *Internet of Things* (IoT). Namun, penerapan 5G juga menimbulkan tantangan keamanan, seperti risiko pencurian data dan serangan sistem akibat kompleksitas infrastruktur serta lonjakan perangkat IoT yang terhubung. Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan menganalisis 13 artikel ilmiah yang relevan untuk mengkaji risiko dan mitigasi keamanan jaringan 5G terhadap IoT. Hasil penelitian menekankan pentingnya pendekatan mitigasi *Intrusion Detection System* (IDS) sebagai langkah deteksi dini dan respons cepat terhadap serangan *Denial of Service* (DoS) yang dapat mengakibatkan terganggunya operasional perangkat IoT. Selain itu persyaratan keamanan juga dibutuhkan untuk meningkatkan keamanan sistem serta melindungi data perangkat IoT dari ancaman penyusupan, seperti serangan *Man-in-the-Middle* (MitM).

Kata kunci : *Jaringan 5G, IoT, Keamanan Siber, Intrusion Detection System,Persyaratan Keamanan.*

1. PENDAHULUAN

Perkembangan teknologi jaringan telekomunikasi telah mengalami kemajuan pesat dari generasi ke generasi, mulai dari 3G hingga 4G, dan kini memasuki era jaringan 5G. Transisi ini membuka peluang baru di berbagai sektor kehidupan, termasuk kesehatan, transportasi, manufaktur, pendidikan, hingga hiburan. Teknologi 5G menjanjikan kecepatan data yang jauh lebih tinggi, latensi rendah, dan kapasitas jaringan yang lebih besar dibandingkan pendahulunya, sehingga menjadi fondasi bagi transformasi digital yang semakin kompleks dan terpadu.

Kelebihan teknologi 5G mencakup kemampuan koneksi yang lebih stabil, kecepatan data yang memungkinkan *real-time communication*, serta dukungan penuh terhadap perkembangan *Internet of Things* (IoT). IoT yang ditingkatkan dengan 5G memberikan potensi luar biasa untuk menghubungkan miliaran perangkat pintar secara simultan, mempercepat otomatisasi, dan mendukung transformasi industri. Selain itu, 5G diyakini akan membawa dampak ekonomi yang signifikan dengan menciptakan peluang baru dalam berbagai sektor, meningkatkan produktivitas, dan memperluas adopsi teknologi canggih.

Namun, implementasi teknologi 5G juga menghadirkan sejumlah kekurangan dan tantangan. Penelitian ini berfokus pada tantangan keamanan dalam jaringan 5G, terutama terkait dengan keamanan IoT. Dengan meningkatnya jumlah perangkat IoT yang terhubung, risiko serangan siber seperti pencurian data, serangan Dos(*denial-of-service*) dan ancaman lainnya juga turut meningkat. Selain itu, kompleksitas infrastruktur 5G menimbulkan kekhawatiran terhadap privasi data, keamanan perangkat, dan potensi eksploitasi kerentanan jaringan.Tanpa mitigasi yang memadai, adopsi teknologi 5G dapat menciptakan celah keamanan yang berpotensi dimanfaatkan oleh penjahat siber.

Dengan fokus utama pada keamanan jaringan 5G terhadap IoT, diperlukan pendekatan yang komprehensif untuk mengatasi risiko yang muncul. Hal ini mencakup protokol *Intrusion Detection Systems* (IDS) dan persyaratan keamanan. Dua prosedur keamanan ini merupakan upaya yang memberikan manfaat optimal bagi masyarakat agar menciptakan ekosistem digital yang aman dan andal.

2. TINJAUAN PUSTAKA

2.1. Jaringan 5G

Jaringan 5G adalah teknologi jaringan telekomunikasi generasi kelima yang menawarkan kemampuan jauh lebih canggih dibandingkan generasi sebelumnya. Teknologi ini menghadirkan kecepatan unduh yang sangat tinggi, latensi yang rendah, dan kapasitas jaringan yang lebih besar, memungkinkan transformasi digital yang masif di berbagai sektor. Selain itu, 5G memiliki potensi signifikan dalam meningkatkan konektivitas yang lebih luas dan andal, sehingga sangat relevan untuk mendukung perkembangan aplikasi ilmiah dan *Internet of Things* (IoT), sekaligus membuka peluang inovasi baru dalam sains, teknologi, dan berbagai bidang lainnya.

2.2. Keamanan Siber

Keamanan siber merupakan serangkaian langkah strategis yang dirancang untuk melindungi sistem, jaringan, perangkat, dan data digital dari berbagai ancaman atau serangan siber yang berpotensi mengakibatkan gangguan operasional, kerusakan infrastruktur, atau akses tidak sah terhadap informasi

yang sensitif. Langkah-langkah tersebut mencakup implementasi teknologi mutakhir, pengembangan kebijakan yang komprehensif, dan penerapan praktik terbaik yang bertujuan untuk mencegah ancaman, mendeteksi indikasi serangan, serta merespons insiden dengan efisiensi dan akurasi tinggi.

Komponen utama dalam keamanan siber meliputi perlindungan kerahasiaan data agar informasi hanya dapat diakses oleh pihak yang berwenang, pemeliharaan integritas data untuk memastikan keakuratan dan keterandalan informasi, serta jaminan ketersediaan sistem dan data agar dapat diakses secara konsisten sesuai kebutuhan. Lebih jauh, keamanan siber memainkan peran strategis dalam mendukung keberlanjutan operasional dalam ekosistem digital yang semakin kompleks, termasuk dalam menghadapi tantangan yang muncul akibat perkembangan teknologi canggih.

2.3. *Intrusion Detection Systems (IDS)*

Intrusion Detection Systems (IDS) adalah suatu sistem keamanan yang dirancang untuk memonitor, menganalisis, dan mendeteksi aktivitas yang mencurigakan atau tidak sah dalam jaringan atau sistem komputer. Tujuan utama IDS adalah untuk mengidentifikasi potensi ancaman atau serangan yang dapat merusak kerahasiaan, integritas, dan ketersediaan informasi dalam sistem tersebut. Sistem ini bekerja dengan memeriksa pola lalu lintas data, mencari anomali atau perilaku yang tidak biasa, serta membandingkan aktivitas yang terjadi dengan pola serangan yang telah diketahui sebelumnya.

2.4. Persyaratan Keamanan

Persyaratan keamanan merupakan sekumpulan prinsip dan prosedur yang dirumuskan untuk melindungi sistem, data, dan komunikasi dalam ekosistem 5G serta *Internet of Things* (IoT). Prinsip-prinsip ini mencakup berbagai aspek fundamental yang memastikan perlindungan terhadap kerahasiaan, integritas, autentikasi, keaslian data serta tindakan yang terjadi dalam sistem. Berikut adalah beberapa metode persyaratan keamanan:

a. Autentikasi : Prosedur verifikasi identitas perangkat dan entitas yang terlibat dalam komunikasi.
b. Integritas: Prosedur yang menjamin bahwa data yang diterima tetap asli dan tidak dimodifikasi tanpa izin.
c. Kerahasiaan: Prosedur untuk melindungi data agar hanya dapat diakses oleh pihak yang berwenang.
d. Non-repudiasi: Prosedur untuk mencegah entitas untuk menyangkal keabsahan pesan atau tindakan yang dilakukan.
e. Kesegaran data: Prosedur yang memastikan bahwa data yang digunakan adalah yang terbaru, mencegah penggunaan informasi yang usang.
f. Otorisasi: Prosedur yang mengatur hak akses perangkat atau pengguna terhadap sumber daya dalam sistem.
g. Ketersediaan: Prosedur yang menjamin bahwa informasi dan layanan dapat diakses oleh entitas yang berwenang, mengatasi serangan yang berupaya menggagalkan akses.

2.5. *Study Literature Review*

Systematic Literature Review (SLR) merupakan pendekatan metodologis yang diterapkan untuk secara sistematis mengidentifikasi, mengevaluasi, dan menganalisis literatur yang relevan dalam kaitannya dengan topik atau isu tertentu. Tujuan utama dari SLR adalah untuk menyajikan suatu sintesis yang komprehensif dan objektif mengenai evolusi pengetahuan dalam suatu bidang penelitian dengan mengintegrasikan temuan-temuan yang ada, serta mengidentifikasi kesenjangan dalam literatur yang ada dan mengusulkan area-area yang memerlukan eksplorasi lebih lanjut.

3. METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur atau biasa disebut *Systematic Literature Review* (SLR). Metode ini bertujuan untuk menggali pemahaman yang mendalam mengenai topik yang diteliti. Sebanyak 13 artikel ilmiah, yang diambil dari jurnal nasional dan internasional, menjadi sumber data utama dalam penelitian ini. Data tersebut dianalisis menggunakan model interaktif yang dikembangkan oleh Miles, Huberman, dan Saldana (2014), yang mencakup empat tahapan utama sebagai berikut.

3.1. Pengumpulan data

Pengumpulan data adalah proses sistematis untuk mengumpulkan informasi yang relevan dari berbagai sumber guna menjawab pertanyaan penelitian. Tahap ini melibatkan berbagai jenis sumber data, seperti dokumen tertulis (jurnal ilmiah, laporan, buku), wawancara, observasi langsung, serta artefak atau media, yang semuanya bertujuan untuk menyediakan informasi yang diperlukan untuk analisis secara mendalam.

3.2. Kondensasi data

Kondensasi data merupakan suatu proses sistematis yang melibatkan pemilihan, penyederhanaan, peringkasan, atau transformasi data mentah yang diperoleh selama tahap pengumpulan data. Proses ini bertujuan untuk memusatkan analisis pada data yang paling relevan dan signifikan bagi tujuan penelitian, sekaligus mengeliminasi informasi yang tidak relevan atau redundan.

3.3. Penyajian data

Penyajian data merupakan proses pengorganisasian dan peringkasan data dalam bentuk yang terstruktur dan sistematis, dengan tujuan mempermudah peneliti dalam memahami informasi

yang kompleks serta mengidentifikasi pola, hubungan, atau tren yang relevan. Sehingga data yang disajikan dapat mendukung peneliti dalam proses penarikan kesimpulan secara efektif dan valid.

3.4. Verifikasi data (kesimpulan)

Verifikasi data merupakan tahapan penting yang bertujuan untuk memastikan bahwa kesimpulan yang dihasilkan didasarkan pada data yang valid, relevan, dan dapat dipertanggungjawabkan secara ilmiah. Tahapan ini melibatkan evaluasi ulang terhadap data dan temuan guna menjamin keakuratan serta konsistensi dalam interpretasi yang dilakukan.

4. HASIL DAN PEMBAHASAN

4.1. Resiko Serangan Siber pada Perangkat IoT berbasis Jaringan 5G

Tidak dapat disangkal bahwa jaringan 5G menawarkan beberapa keunggulan seperti kecepatan tinggi, latency rendah, dan konektivitas masif, yang ideal untuk mendukung IoT. Namun, teknologi ini juga menghadirkan tantangan, terutama dalam keamanan, dengan meningkatnya risiko serangan siber dan privasi data akibat banyaknya perangkat terhubung dan kompleksitas jaringan.

Bentuk serangan yang sering ditemui adalah serangan *Denial of Service* atau biasa disebut DoS. DoS merupakan serangan yang dilakukan dengan cara membebani sumber daya sistem, seperti bandwidth atau kapasitas pemrosesan, melalui pengiriman permintaan palsu atau aktivitas yang berlebihan. Akibatnya, layanan jaringan atau perangkat menjadi tidak dapat diakses oleh pengguna yang sah, sehingga mengakibatkan terganggunya operasional serta fungsi normal perangkat IoT.

Selain serangan DoS, ancaman lain yang tak kalah serius adalah pencurian data. Serangan ini bertujuan untuk memperoleh akses tidak sah terhadap informasi sensitif yang disimpan atau ditransmisikan dalam jaringan, sehingga berpotensi menimbulkan dampak signifikan terhadap privasi, keamanan, serta keberlanjutan operasional sistem. Salah satu bentuk pencurian data yang sering terjadi adalah serangan *Man-in-the-Middle* (MitM), di mana penyerang menyadap komunikasi antara dua pihak untuk mencuri data yang dikirimkan, seperti kredensial login atau informasi pembayaran.

4.2. Mitigasi Serangan Siber pada Perangkat IoT berbasis Jaringan 5G

Mitigasi serangan siber pada perangkat IoT berbasis jaringan 5G menjadi hal yang esensial untuk menjaga keberlanjutan operasional dan privasi pengguna. Untuk mencapai hal tersebut, diperlukan penerapan berbagai strategi dan teknologi keamanan yang dapat mendeteksi, mencegah, dan merespons serangan siber secara efektif. Mitigasi serangan siber memerlukan berbagai langkah yang disesuaikan dengan jenis ancaman yang dihadapi.

Salah satu prosedur yang sangat penting dalam mencegah serangan siber secara efektif adalah prosedur *Intrusion Detection System* (IDS). IDS memiliki kemampuan untuk memberikan peringatan awal mengenai aktivitas yang mencurigakan, yang selanjutnya dapat diteruskan kepada sistem respons otomatis atau operator jaringan untuk melaksanakan tindakan mitigasi yang sesuai. Beberapa bentuk tindakan berupa pemblokiran alamat IP atau pengurangan prioritas terhadap lalu lintas yang berpotensi merugikan. Dengan demikian, implementasi IDS memungkinkan deteksi yang cepat serta respon yang akurat terhadap ancaman serangan *Denial of Service* (DoS).

Penting juga untuk memastikan bahwa perangkat lunak menerapkan persyaratan keamanan yang ketat di setiap lapisan jaringan dan sistem. Penggunaan metode autentikasi seperti *Public Key Infrastructure* (PKI) dapat meningkatkan keamanan sistem dengan memastikan identitas pengguna melalui penerapan pasangan kunci publik dan privat. PKI juga memungkinkan terwujudnya komunikasi yang aman serta perlindungan data dari potensi penyusupan. Pendekatan ini sangat krusial dalam mencegah terjadinya serangan Man-in-the-Middle (MitM), di mana pihak yang tidak berwenang dapat menyusup ke dalam saluran komunikasi dan mengakses atau memodifikasi data yang sedang ditransmisikan. Melalui implementasi PKI, setiap pihak yang terlibat dalam komunikasi dapat memverifikasi identitas satu sama lain.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian melalui pendekatan *Studi Literature Review* (SLR) dapat disimpulkan bahwa mitigasi serangan siber pada perangkat IoT berbasis jaringan 5G sangat penting untuk menjaga operasional dan privasi data. Penerapan *Intrusion Detection System* (IDS) memungkinkan deteksi dini dan respons cepat terhadap serangan *Denial of Service* (DoS). Selain itu persyaratan keamanan yang ketat dengan metode autentikasi seperti *Public Key Infrastructure* (PKI) dapat meningkatkan keamanan sistem serta melindungi data dari ancaman penyusupan, seperti serangan *Man-in-the-Middle* (MitM)

DAFTAR PUSTAKA

[1] Sugiyatno, P. Sidiq, and I. Fikma Edrisy, “Pengaruh Teknologi 5G pada Evolusi Komunikasi: Sebuah Kajian Terhadap Perkembangan dan Implikasinya di Bidang Sains,” *Nucleus*, vol. 4, no. 2, pp. 115–120, Feb. 2024.

[2] Y. Fatmawati and A. Firdonsyah, “Penerapan Kebijakan Data Privacy di Era Teknologi 5G di Indonesia,” *Pencerah Publik*, vol. 11, no. 1, pp. 42–49, Apr. 2024.

[3] F. P. E. Putra, M. Riski, M. S. Yahya, dan M. H. Ramadhan, "Mengenal Teknologi Jaringan

Nirkabel Terbaru Teknologi 5G," *Jurnal Sistem Informasi dan Teknologi*, vol. 5, no. 2, pp. 167–174, Jul. 2023.

[4] C. Vincha and J. Satrio, "Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia," *Jurnal Ketahanan Nasional*, vol. 30, no. 2, pp. 222–242, Aug. 2024.

[5] N. Febriyani, "Keamanan Sistem Informasi Jaringan 5G Di Indonesia Masa Kini Dan Masa Depan," Apr. 2023.

[6] N. H. Hari, F. P. E. Putra, U. Hasanah, S. R. Sutarsih, and Riyan, "Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi," *Jurnal Informasi Dan Teknologi*, vol. 5, no. 2, Jul. 2023.

[7] Trikolas, A. Sungkowo, R. R. A. Hakim, and A. Jaenul, "Kelebihan, Kekurangan, Peluang Teknologi 5G di Indonesia," *INSOLOGI: Jurnal Sains dan Teknologi*, vol. 1, no. 1, pp. 43–49, Feb. 2022.

[8] S. Srinivasan and H. M. Shanmugam, "A Review on Future Security Challenges in 5G," *Asia-Pacific Journal of Management and Technology*, vol. 1, no. 2, Malaysia, Oct. 2020. pp. 8–12.

[9] J. Cook, S. U. Rehman and M. A. Khan, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," in *IEEE Access*, vol. 11, pp. 39295-39317,

[10] M. Wazid, A. K. Das, S. Shetty, P. Gope and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," *in IEEE Access*, vol. 9, Malaysia, 2021. pp. 4466-4489

[11] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the Internet of Things era: an Overview on Security and Privacy Challenges," *Computer Networks*, Italy, Oct. 2020. vol. 179, pp. 107345.

[12] U. Y. Oktiawati, E. Ernawita, S. Anwar, A. Ramatni, J. W. Kuswinardi, and J. W. Sitopu, "Kemajuan Teknologi 5G Mempercepat Adopsi dan Inovasi IoT Terhadap Pendidikan di Perguruan Tinggi," *Jurnal Edu Research*, vol. 5, no. 2, pp. 193-202, Jun. 2024.

[13] A. K. Ahmed and A. A. Khorsheed, "Open Network Structure and Smart Network to Sharing Cybersecurity within the 5G Network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, p. 573, Jul. 2022