P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

Analisis Keamanan Jaringan 5G: Ancaman dan Upaya Mitigasi

[1]Sahrul Gunawan, [2]Atha Agdo Ramdi Santosa, [3]Essy Malays Sari Sakti
[1]Prodi Informatika, Fakultas Teknik, Universitas Persada Indonesia Y.A.I, Jakarta
[2]Prodi Informatika, Fakultas Teknik, Universitas Persada Indonesia Y.A.I

[1] atha.agdo.ramdi.s.2144190017@upi-yai.ac.id [2]sahrul.gunawan.2144190023@upi-yai.ac.id [3] essy..malays@upi-yai.ac.id

ABSTRAK

Jaringan 5G, sebagai generasi terbaru dari teknologi komunikasi seluler, menawarkan peningkatan signifikan dalam kecepatan, kapasitas, dan konektivitas. Namun, seiring dengan keuntungan yang dihadirkannya, jaringan ini juga membawa serangkaian tantangan baru terkait keamanan. Penelitian ini bertujuan untuk menganalisis ancaman keamanan yang dihadapi oleh jaringan 5G dan mengidentifikasi strategi mitigasi yang efektif. Melalui tinjauan literatur yang komprehensif dan studi kasus terkini, kami mengkategorikan ancaman utama yang meliputi serangan pada protokol komunikasi, risiko terhadap privasi pengguna, dan potensi eksploitasi oleh perangkat IoT yang terhubung. Selain itu, kami mengevaluasi berbagai pendekatan mitigasi, termasuk penerapan enkripsi end-to-end, penggunaan teknologi kecerdasan buatan untuk deteksi anomali, dan peningkatan kerjasama antara penyedia layanan dan regulator. Hasil dari penelitian ini menunjukkan bahwa meskipun jaringan 5G menghadirkan risiko keamanan yang signifikan, adopsi strategi mitigasi yang tepat dapat secara substansial mengurangi kerentanan dan meningkatkan ketahanan sistem. Penelitian ini memberikan wawasan bagi pengembang, penyedia layanan, dan pembuat kebijakan dalam upaya bersama untuk mengamankan infrastruktur komunikasi masa depan.

Kata kunci :*5G Network Security, Security Threats, Mitigation Strategies,Communication Protocols,IoT Vulnerabilities,Anomaly Detection*

ABSTRACT

The 5G network, as the latest generation of cellular communication technology, offers significant advancements in speed, capacity, and connectivity. However, alongside these benefits, it also introduces a range of new security challenges. This research aims to analyze the security threats faced by 5G networks and identify effective mitigation strategies. Through a comprehensive literature review and recent case studies, we categorize the primary threats, including attacks on communication protocols, risks to user privacy, and potential exploitation by connected IoT devices. Additionally, we evaluate various mitigation approaches, such as the implementation of end-to-end encryption, the use of artificial intelligence for anomaly detection, and enhanced collaboration between service providers and regulators. The findings of this research indicate that although 5G networks present significant security risks, the adoption of appropriate mitigation strategies can substantially reduce vulnerabilities and enhance system resilience. This study provides

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

insights for developers, service providers, and policymakers in their collective efforts to secure future communication infrastructure.

Keyword :*5G Network Security, Security Threats, Mitigation Strategies,Communication Protocols,IoT Vulnerabilities,Anomaly Detection*

1. PENDAHULUAN

Teknologi jaringan telekomunikasi telah mengalami perkembangan yang pesat dalam beberapa dekade terakhir. Mulai dari jaringan 2G yang memungkinkan komunikasi suara nirkabel hingga jaringan 4G yang memperkenalkan konektivitas data berkecepatan tinggi, setiap generasi baru telah membawa perubahan signifikan dalam cara kita berkomunikasi dan berinteraksi dengan dunia digital. Namun, saat ini kita berada di ambang sebuah revolusi baru dengan munculnya teknologi jaringan 5G yang menjanjikan kemampuan yang jauh lebih canggih dan transformatif.(Haidar Hari et al., 2023) Revolusi teknologi komunikasi nirkabel kini memasuki era baru dengan diperkenalkannya jaringan 5G. Jaringan ini menjanjikan kecepatan yang lebih tinggi, latensi yang lebih rendah, serta kapasitas koneksi yang jauh lebih besar dibandingkan pendahulunya, seperti 4G. Peningkatan ini diharapkan dapat mendukung perkembangan berbagai aplikasi inovatif, mulai dari kendaraan otonom hingga Internet of Things (IoT), serta mendorong transformasi digital di berbagai sektor industri.

Namun, seiring dengan berbagai keuntungan yang ditawarkan, jaringan 5G juga menghadirkan tantangan baru dalam hal keamanan. Karakteristik unik dari teknologi 5G, seperti penggunaan spektrum frekuensi yang lebih tinggi dan arsitektur jaringan yang lebih kompleks, membuka celah baru bagi potensi serangan siber. Keamanan jaringan 5G menjadi perhatian utama, terutama mengingat dampak potensial dari serangan yang berhasil dapat meluas ke berbagai sektor kehidupan, termasuk infrastruktur kritis, komunikasi pribadi, dan layanan penting lainnya. Serangan terhadap jaringan 5G dapat memiliki konsekuensi yang sangat serius, termasuk gangguan layanan, pencurian data sensitif, dan bahkan ancaman terhadap keamanan nasional. (Ira Safira, 2024) Ancaman terhadap keamanan jaringan ini mencakup serangan pada protokol komunikasi, risiko pelanggaran privasi, serta eksploitasi terhadap perangkat IoT yang terhubung ke jaringan.

Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis ancaman-ancaman keamanan yang spesifik terhadap jaringan 5G serta mengusulkan upaya-upaya mitigasi yang efektif. Dengan melakukan tinjauan literatur yang mendalam dan mengevaluasi studi kasus terkini, penelitian ini diharapkan dapat memberikan wawasan yang komprehensif tentang langkah-langkah yang perlu diambil untuk melindungi infrastruktur jaringan 5G dari berbagai ancaman siber.

Melalui penelitian ini, kami berupaya untuk memberikan panduan bagi pengembang, penyedia layanan, serta pembuat kebijakan dalam merancang dan mengimplementasikan strategi keamanan yang kokoh. Dengan demikian, diharapkan bahwa manfaat dari teknologi 5G dapat dioptimalkan tanpa mengorbankan aspek keamanan dan privasi pengguna.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

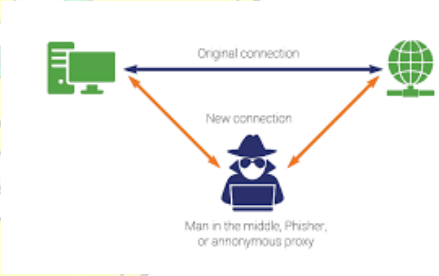
2. LANDASAN TEORI

Jaringan 5G (fifth-generation) merupakan evolusi dari teknologi komunikasi nirkabel yang menjanjikan peningkatan signifikan dalam kecepatan, kapasitas, latensi rendah, dan efisiensi spektrum dibandingkan pendahulunya. Setiap 10 tahun, migrasi teknologi jaringan seluler selalu terjadi. Pada tahun 2020 penggunaan teknologi Generasi ke-4 (4G) hampir secara menyeluruh dapat dinikmati di Indonesia. Teknologi komunikasi yang tak pernah berhenti, kini sudah mulai mempersiapkan negara ini untuk memasuki tahap selanjutnya, yaitu konektivitas komunikasi berbasis 5G. (Masa et al., 2023) Munculnya teknologi 5G telah membawa janji akan kecepatan tinggi, latensi rendah, dan kapasitas yang besar untuk melayani kebutuhan yang semakin kompleks. (Mahmudi, 2023) Namun, dengan kemajuan ini juga datang tantangan baru dalam hal keamanan. Analisis keamanan jaringan 5G menjadi krusial untuk memahami ancaman yang mungkin muncul dan mengembangkan upaya mitigasi yang efektif.

Ancaman terhadap Keamanan Jaringan 5G :

1. Serangan DDoS (Distributed Denial of Service) adalah jenis serangan siber di mana penyerang berusaha membuat layanan, jaringan, atau situs web tidak dapat diakses oleh pengguna yang sah dengan membanjiri target dengan sejumlah besar lalu lintas internet yang jahat. DDoS telah dikenal untuk komunitas jaringan sejak awal 1980. Target serangan DDoS bisa ditujukan ke berbagai jaringan, bisa ke *routing device, web, electronic mail,* atau *server domain name system*.(- et al., 2022) Serangan ini bertujuan membuat server shutdown, reboot, crash, atau "not responding". Jaringan 5G, dengan perangkat yang saling terhubung dalam jumlah besar (Internet of Things, IoT), menjadi target yang menarik untuk serangan DDoS. Serangan ini dapat melumpuhkan infrastruktur jaringan dengan mengirimkan lalu lintas yang sangat besar sehingga menyebabkan gangguan layanan.

2. Serangan Man-in-the-Middle (MitM), Serangan ini merupakan salah satu jenis serangan yang berbahaya karena serangan ini dapat terjadi pada berbagai media informasi seperti website, smartphone, dan bahkan surat. (Gede E A Kamajaya, 2020) Serangan ini juga terjadi ketika penyerang menyusup dan mengubah komunikasi antara dua pihak tanpa diketahui. Dalam konteks 5G, ini dapat mencakup penyadapan data pribadi atau informasi sensitif yang dikirimkan melalui jaringan.



Gambar 1 .Ilustrasi serangan Man In The Middle

3. Menurut (Adhistian, 2020) Meningkatkan IOT akan menjadi fitur kunci dalam menyebarkan jaringan 5G. 4G COMP saat ini (koordinasi multi-point) akan menjadi terobosan awal seperti dalam jaringan kognitif. Setiap NE akan memerlukan koordinasi untuk parameter yang diperlukan seperti gangguan, alokasi sumber

daya dan jabat tangan antara terminal nirkable. juga menimbulkan dampak yaitu Perangkat IoT yang Tidak Aman, Banyak perangkat IoT yang dihubungkan ke jaringan 5G memiliki tingkat keamanan yang rendah, sehingga mudah menjadi pintu masuk bagi penyerang. Ancaman ini mencakup pengambilalihan perangkat untuk digunakan dalam serangan yang lebih luas atau eksploitasi data yang tersimpan pada perangkat.

4. Serangan pada Infrastruktur Jaringan, Elemen-elemen kritis dari infrastruktur jaringan 5G, seperti base stations dan network slicing, menjadi target potensial untuk serangan yang bertujuan mengganggu operasi jaringan secara keseluruhan.

Upaya Mitigasi

1. Enkripsi Data,

   Salah satu cara untuk mengamankan data komputer adalah melakukan enkripsi pada sebuah data atau file yang kita anggap penting. Teknik enkripsi ini adalah teknik untuk merubah bentuk data, sehingga orang lain tidak mengetahui bentuk asli dari data tersebut,(H. Kridalaksana et al., 2017) Mengimplementasikan enkripsi yang kuat untuk data yang dikirimkan melalui jaringan 5G juga sangat penting untuk mencegah akses tidak sah dan melindungi privasi pengguna. Protokol enkripsi harus diperbarui secara berkala untuk melawan teknik dekripsi yang baru.

2. Autentikasi dan Otorisasi yang Kuat, Otentikasi dalam Cloud Computing untuk memastikan bahwa orang yang tepat mendapatkan akses ke data yang tersedia dari penyedia teknologi cloud.(Munirul Ula, 2019) Penggunaan metode autentikasi multifaktor (MFA) dan otorisasi yang ketat juga dapat membantu memastikan bahwa hanya pengguna dan perangkat yang sah yang dapat mengakses jaringan. Ini juga mencakup penggunaan sertifikat digital dan sistem manajemen identitas yang canggih.

3. Segmentasi Jaringan

   Keamanan data dan perangkat jaringan merupakan hal esensial dalam pengembangan suatu jaringan komputer. Tidak terkecuali dalam pembuatan jaringan komputer baru, maupun pengembangan dari jaringan komputer yang telah ada.(Riyan Almakhia, 2023) Menggunakan teknik segmentasi jaringan, seperti network slicing, untuk memisahkan lalu lintas yang berbeda dapat mengurangi risiko bahwa serangan pada satu segmen akan mempengaruhi seluruh jaringan. Setiap segmen dapat diperlakukan dengan kebijakan keamanan yang spesifik sesuai dengan tingkat risiko yang berbeda.

4. Pemantauan dan Deteksi Intrusi,

   Sistem Deteksi Intrusi (IDS) adalah proses pemantauan lalu lintas jaringan dalam sistem untuk mendeteksi pola dan aktivitas yang mencurigakan yang memungkinkan ada serangan dalam sistem itu. beberapa jenisserangan,yaitu Botnet, UDP, SYN, broadcast, sleep deprivation, dan serangan bertubi-tubi.(Gunawan et al., 2022)

   Desain Arsitektur teknologi berhubungan dengan aplikasi-

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

aplikasi yang digunakan perusahaan. Sistem Informasi Penjualan akan menggunakan Client/Server Architecture Pattern, sedangkan aplikasi-aplikasi lainnya akan menggunakan Service Oriented. Desain jaringan untuk kantor cabang menggunakan jaringan lokal (LAN) dan untuk jaringan entreprise menggunakan TCP/IP untuk koneksi ke pusat data menggunakan VPN IP. (Essy Malays Sari Sakti, 2018)Implementasi sistem pemantauan yang real-time dan deteksi intrusi yang canggih dapat membantu mengidentifikasi dan merespon ancaman sebelum mereka menyebabkan kerusakan yang signifikan. Teknik ini meliputi analisis perilaku jaringan dan penggunaan kecerdasan buatan untuk mendeteksi anomali.

5. Pembaruan dan Patch Secara Teratur, Memastikan bahwa semua perangkat dan infrastruktur jaringan selalu diperbarui dengan patch keamanan terbaru adalah kunci untuk menutup kerentanan yang dapat dieksploitasi oleh penyerang. Ini membutuhkan kerjasama yang erat antara produsen perangkat dan operator jaringan.

3. METODOLOGI

Penelitian ini bertujuan untuk menganalisis keamanan jaringan 5G dengan fokus pada ancaman yang dihadapi dan upaya mitigasi yang diterapkan. Metode penelitian yang digunakan adalah pendekatan kualitatif melalui studi literatur. Pendekatan ini memungkinkan peneliti untuk mengumpulkan dan menganalisis data dari berbagai sumber yang telah dipublikasikan, sehingga dapat memberikan gambaran yang komprehensif mengenai topik yang diteliti.

Metode Penelitian

1. Desain Penelitian

Penelitian ini menggunakan desain penelitian deskriptif kualitatif, di mana data yang dikumpulkan dari berbagai literatur dianalisis secara statistik untuk mengidentifikasi tren dan pola yang ada dalam keamanan jaringan 5G. Penelitian deskriptif kualitatif cocok untuk memberikan pemahaman mendalam tentang fenomena berdasarkan data yang ada.

2. Pengumpulan Data

Data yang digunakan dalam penelitian ini berasal dari sumber sekunder berupa jurnal ilmiah, buku, artikel konferensi, laporan industri, dan publikasi lain yang relevan dengan topik keamanan jaringan 5G. Proses pengumpulan data melibatkan beberapa langkah berikut:

Identifikasi Sumber: Mengidentifikasi sumber-sumber terpercaya seperti database akademik (IEEE Xplore, ScienceDirect, SpringerLink), perpustakaan digital, dan situs web resmi organisasi terkait.

Kriteria Seleksi: Menentukan kriteria inklusi untuk memastikan hanya literatur yang relevan dan berkualitas yang diikutsertakan dalam analisis. Kriteria inklusi dapat mencakup publikasi dalam lima tahun terakhir, relevansi topik, dan peer-reviewed.

Pengumpulan Data: Mengunduh dan mengumpulkan artikel yang memenuhi kriteria seleksi untuk dianalisis lebih lanjut.

3. Analisis Data

Setelah data dikumpulkan, langkah selanjutnya adalah analisis data secara kuantitatif. Teknik analisis yang digunakan meliputi:

Kategorisasi: Mengkategorikan data berdasarkan jenis ancaman dan upaya mitigasi yang diidentifikasi dalam literatur.

Statistik Deskriptif: Menggunakan statistik deskriptif untuk menganalisis frekuensi dan distribusi jenis ancaman serta upaya mitigasi yang dibahas dalam literatur. Ini termasuk menghitung

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

persentase dan rata-rata kejadian ancaman dan metode mitigasi yang disebutkan.
Analisis Tren: Mengidentifikasi tren dalam ancaman dan upaya mitigasi dari waktu ke waktu untuk melihat bagaimana perkembangan teknologi 5G mempengaruhi lanskap keamanan.
4. Validitas dan Reliabilitas
Untuk memastikan validitas dan reliabilitas penelitian:
Triangulasi Sumber: Menggunakan berbagai sumber data untuk mengurangi bias dan meningkatkan validitas temuan.
Peer Review: Melibatkan ahli dalam bidang keamanan jaringan untuk meninjau dan memvalidasi temuan penelitian.

Tabel 1. Metodologi Penelitian

Komponen	Deskripsi
1. Desain Penelitian	Pendekatan: Kualitatif Jenis Penelitian: Studi literatur Sumber Data: 12 jurnal ilmiah yang relevan dengan topik keamanan jaringan 5G
2. Pengumpulan Data	Proses Pengumpulan: 1.Mengidentifikasi jurnal yang relevan menggunakan database akademik seperti IEEE, Springer, dan Elsevier 2. Memilih jurnal yang memenuhi kriteria inklusi: diterbitkan dalam 5 tahun terakhir, peer-reviewed, dan membahas keamanan jaringan 5G 3. Membaca dan mencatat informasi penting dari setiap jurnal Alat Pengumpulan Data: software manajemen referensi (misalnya, Mendeley, EndNote)
3. Analisis Data	Teknik Analisis: 1.Mengidentifikasi tema dan kategori utama dari setiap jurnal 2. Analisis deskriptif: Menghitung frekuensi tema tertentu 3. Analisis komparatif: Membandingkan hasil dari berbagai jurnal untuk menemukan pola dan perbedaan Alat Analisis Data: Software analisis data seperti Excel
4.Validitas dan Reliabilitas	Validitas 1. Validitas isi: Memastikan jurnal yang dipilih benar-benar relevan dengan topik penelitian 2. Validitas konstruk: Menggunakan kerangka teori yang kuat untuk analisis Reliabilitas: 1. Reliabilitas antar peneliti: Jika melibatkan lebih dari satu peneliti, memastikan konsistensi dalam proses pengumpulan dan analisis data 2. Reliabilitas data: Melakukan double-check terhadap data yang

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

	dikumpulkan untuk menghindari kesalahan interpretasi atau pencatatan

4. HASIL DAN PEMBAHASAN

1. Hasil Analisis

Identifikasi Ancaman Keamanan
Serangan DDoS (Distributed Denial of Service): Jaringan 5G berpotensi lebih rentan terhadap serangan DDoS karena banyaknya perangkat yang terhubung.
Pemalsuan Identitas dan Penipuan: Ancaman berupa spoofing dan phishing semakin canggih, memanfaatkan konektivitas tinggi dan kecepatan jaringan 5G.
Serangan Terhadap Infrastruktur: Menargetkan elemen-elemen kritis seperti jaringan inti dan akses radio, yang dapat mengakibatkan gangguan layanan besar-besaran.
Kelemahan dalam Protokol Komunikasi: Potensi eksploitasi kelemahan dalam protokol 5G .
Ancaman Privasi: Peningkatan jumlah data yang ditransmisikan dan disimpan meningkatkan risiko pelanggaran privasi dan penyadapan.
Upaya Mitigasi
Penerapan Enkripsi End-to-End: Melindungi data yang ditransmisikan di jaringan 5G dari penyadapan dan manipulasi.
Otentikasi dan Autentikasi Multi-Faktor: Memastikan hanya pengguna yang sah dapat mengakses layanan dan data, mengurangi risiko penipuan identitas.
Segmentasi Jaringan: Meminimalkan dampak serangan dengan memisahkan jaringan menjadi beberapa segmen yang lebih kecil dan lebih aman.
Keamanan Berbasis AI dan Pembelajaran Mesin: Mendeteksi dan merespons ancaman secara real-time dengan menganalisis pola lalu lintas dan aktivitas anomali.
Pembaruan dan Patch Berkala: Memastikan semua perangkat dan sistem dalam jaringan 5G selalu diperbarui dengan patch keamanan terbaru.

2. Pembahasan

Penyerangan DDoS
Jaringan 5G, dengan latensi rendah dan kapasitas tinggi, menawarkan lebih banyak titik masuk bagi penyerang untuk melancarkan serangan DDoS. Serangan semacam ini dapat melumpuhkan layanan dengan mengirimkan lalu lintas berlebih ke server atau perangkat tertentu. Untuk mitigasinya, diperlukan mekanisme deteksi dini dan respons cepat seperti firewalls dan sistem mitigasi DDoS yang canggih.
Pemalsuan Identitas dan Penipuan
Dengan meningkatnya jumlah perangkat dan pengguna dalam ekosistem 5G, ancaman pemalsuan identitas dan penipuan juga meningkat. Penggunaan metode otentikasi yang lebih kuat seperti biometrik, token fisik, dan otentikasi multi-faktor dapat mengurangi risiko ini secara signifikan.
Serangan Terhadap Infrastruktur
Infrastruktur 5G yang kompleks mencakup berbagai elemen seperti menara seluler, jaringan inti, dan perangkat endpoint. Setiap elemen ini dapat menjadi target serangan. Pendekatan segmentasi jaringan dan isolasi fungsi kritis dapat membantu membatasi dampak serangan terhadap infrastruktur.
Kelemahan dalam Protokol Komunikasi
Protokol komunikasi yang digunakan dalam jaringan 5G perlu terus dievaluasi dan diperbarui untuk menghindari eksploitasi kelemahan yang ada. Penggunaan enkripsi yang kuat dan mekanisme otentikasi yang ketat dalam protokol ini sangat penting untuk menjaga integritas dan keamanan komunikasi.
Ancaman Privasi
Dalam era 5G, data pengguna semakin banyak dan lebih sensitif, sehingga ancaman terhadap privasi menjadi perhatian utama. Penggunaan enkripsi end-to-end dan kebijakan privasi yang ketat, serta kepatuhan terhadap regulasi seperti GDPR, sangat penting untuk melindungi data pribadi pengguna dari akses dan penyalahgunaan yang tidak sah.

5. KESIMPULAN

Dalam analisis keamanan jaringan 5G, sejumlah ancaman utama telah diidentifikasi, termasuk serangan DDoS, pemalsuan identitas, serangan terhadap infrastruktur, kelemahan dalam protokol komunikasi, dan ancaman privasi. Ancaman-ancaman ini dapat mengganggu kinerja dan integritas jaringan 5G, serta membahayakan data pribadi pengguna.

Upaya mitigasi yang efektif memerlukan pendekatan berlapis yang melibatkan penerapan enkripsi end-to-end untuk melindungi data dalam transmisi, otentikasi multi-faktor untuk mengamankan akses, segmentasi jaringan untuk membatasi dampak serangan, serta penggunaan kecerdasan buatan dan pembelajaran mesin untuk deteksi dan respons ancaman secara real-time. Selain itu, pembaruan dan patch berkala sangat penting untuk mengatasi kerentanan keamanan yang baru muncul.

Secara keseluruhan, meskipun jaringan 5G membawa banyak manfaat seperti kecepatan tinggi dan latensi rendah, tantangan keamanan yang dihadapinya juga signifikan. Dengan mengimplementasikan strategi mitigasi yang komprehensif, risiko-risiko ini dapat diminimalisir, sehingga keamanan dan privasi pengguna jaringan 5G dapat lebih terjamin.

DAFTAR PUSTAKA

-, M. A., Alwi, E. I., & As'ad, I. (2022). ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER. *Cyber Security Dan Forensik Digital*, *5*(1). https://doi.org/10.14421/csecurity.2022.5.1.3423

Adhistian, P. (2020). TEKNOLOGI JARINGAN 5G UNTUK JARINGAN MASA DEPAN MENJADI KEBUTUHAN MANUSIA. *Teknologi : Jurnal Ilmiah Dan Teknologi*, *2*(2). https://doi.org/10.32493/teknologi.v2i2.7901

Essy Malays Sari Sakti, A. B. (2018). Perancangan Arsitektur Sistem Informasi PT. ASMI PUTRI BUMI. *Teknik Informatika, 2Sistem Informasi , Universitas Persada Indonesai Y.A.I Jl. Salemba Raya No. 7-9 Jakarta Pusat 10340. Indonesia*.

Gede E A Kamajaya, I. R. Y. P. (2020). ANALISA INVESTIGASI STATIC FORENSICS SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING. *Program Studi Magister Teknik Informatika – Universitas Islam Indonesia1, 3 Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia2*.

Gunawan, R. G., Erik Suanda Handika, & Edi Ismanto. (2022). Pendekatan Machine Learning Dengan Menggunakan Algoritma Xgboost (Extreme Gradient Boosting) Untuk Peningkatan Kinerja Klasifikasi Serangan Syn. *Jurnal CoSciTech (Computer Science and Information Technology)*, *3*(3). https://doi.org/10.37859/coscitech.v3i3.4356

H. Kridalaksana, A., Rangan, A. Y., & Ansharie, A. (2017). ENKRIPSI DATA AUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA. *Sebatik*, *17*(1). https://doi.org/10.46984/sebatik.v17i1.79

Haidar Hari, N., Eka Putra, F. P., Hasanah, U., Sutarsih, S. R., & Riyan. (2023). Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi. *Jurnal Informasi Dan Teknologi*. https://doi.org/10.37034/jidt.v5i2.357

Ira Safira. (2024). ANALISIS KEAMANAN JARINGAN 5G: TANTANGAN DAN SOLUSI DALAM ERA INTERNET TERHUBUNG. *Fakultas Teknik , Universitas Medan Area, Indonesia*.

Mahmudi, M. N. (2023). Analisa QoS Jaringan 5G Analisa QoS Jaringan 5G Provider X Dan Y Untuk Aplikasi Vidio Streaming Resolusi 4K (Studi Kasus Di Kota Pekanbaru). *Telekontran : Jurnal Ilmiah Telekomunikasi, Kendali Dan Elektronika Terapan*, *11*(1). https://doi.org/10.34010/telekontran.v11i1.9868

Masa, M. A., Abdurrahman, T. S. D., Basalamah, A., Rahman, M. N., Lahmado, H., & Afdhal, A. (2023). Analisis Potensi Teknologi Jaringan 5G Area Sulawesi Selatan. *Jambura*

Journal of Electrical and Electronics Engineering, *5*(1). https://doi.org/10.37905/jjeee.v5i1.16870

Munirul Ula. (2019). ANALISIS METODE PENGAMANAN DATA PADALAYANAN CLOUD COMPUTING. *Program Studi Sistem Informasi Fakultas Teknik Universitas Malikussaleh*.

Riyan Almakhia, A. S. B. R. D. A. (2023). Implementasi Protokol Keamanan Dan Segmentasi Jaringan Dalam Project Pembangunan WLAN Untuk PT Pan Pacific Insurance . *Program Studi Teknologi Komputer, Universitas Bina Sarana Informatika Jl. Kramat Raya No. 98, Jakarta Pusat, DKI Jakarta*.