



Keamanan dan Privasi Data pada Teknologi 5G dalam Strategi Perlindungan untuk Ekosistem IoT

Ardelia Syifa¹, Septiani², Arizal Anshori³

^{1,2,3} Universitas Sigaperbangsa Karawang, Karawang

Email : 2210631160005@student.unsika.ac.id

Received: 22 Maret 2026; Received in revised form: 9 Agustus 2026; Accepted: 10 Agustus 2026

Abstract

The advent of 5G technology has revolutionized the telecommunications industry, promising faster speeds, lower latency, and greater network capacity. However, the proliferation of interconnected devices within the Internet of Things (IoT) ecosystem has introduced significant security and privacy challenges. This study explores the strategies for protecting data privacy and security within the 5G and IoT context. By analyzing existing literature, conducting case studies, and identifying key threats such as DDoS attacks and Man-in-the-Middle attacks, this research proposes a comprehensive framework for safeguarding data in this evolving landscape. The findings highlight the need for strong encryption, robust authentication, and effective network segmentation. Additionally, the study emphasizes the importance of raising public awareness about data privacy and the need for organizations to implement comprehensive data protection policies.

Keywords : 5G security; privacy; IoT (Internet of Things); data protection; cyber threats; network security

Abstrak

Kemunculan teknologi 5G telah merevolusi industri telekomunikasi, menjanjikan kecepatan yang lebih cepat, latensi yang lebih rendah, dan kapasitas jaringan yang lebih besar. Namun, berkembangnya perangkat yang saling terhubung dalam ekosistem Internet of Things (IoT) telah menimbulkan tantangan keamanan dan privasi yang signifikan. Penelitian ini mengeksplorasi strategi untuk melindungi privasi dan keamanan data dalam konteks 5G dan IoT. Dengan menganalisis literatur yang ada, melakukan studi kasus, dan mengidentifikasi ancaman utama seperti serangan DDoS dan serangan Man-in-the-Middle, penelitian ini mengusulkan kerangka kerja yang komprehensif untuk melindungi data dalam lanskap yang terus berkembang ini. Temuan-temuannya menyoroti perlunya enkripsi yang kuat, otentikasi yang kuat, dan segmentasi jaringan yang efektif. Selain itu, penelitian ini juga menekankan pentingnya meningkatkan kesadaran publik tentang privasi data dan perlunya organisasi menerapkan kebijakan perlindungan data yang komprehensif.

Kata kunci : keamanan 5G; privasi; IoT (Internet of Things); perlindungan data; ancaman siber; keamanan jaringan

1. PENDAHULUAN

Perkembangan teknologi 5G memberikan dampak signifikan dalam industri telekomunikasi global. Kecepatan internet yang jauh lebih cepat, latensi yang rendah, dan kapasitas jaringan yang lebih besar merupakan beberapa keunggulan utama yang ditawarkan oleh 5G. Dengan kemampuan ini, teknologi 5G diharapkan dapat mempercepat berbagai inisiatif digital dan memperluas akses teknologi, terutama di wilayah-wilayah yang selama ini masih terbatas jangkauannya. Diharapkan, implementasi 5G akan memberikan perubahan besar dalam berbagai sektor dan meningkatkan kualitas hidup masyarakat secara keseluruhan [1]. Dengan berkembangnya teknologi, jaringan 5G muncul sebagai generasi terbaru dari teknologi komunikasi seluler yang menawarkan kecepatan internet yang lebih tinggi dan latensi yang lebih rendah dibandingkan dengan pendahulunya. Namun, peningkatan konektivitas ini juga membawa tantangan baru dalam hal keamanan dan privasi data. Jaringan 5G tidak hanya mendukung komunikasi

antar perangkat, tetapi juga memfasilitasi pertumbuhan Internet of Things (IoT), di mana miliaran perangkat akan terhubung dan saling berkomunikasi [2].

Internet of Things atau IoT, merupakan sebuah konsep/gagasan yang tujuannya adalah untuk memperluas manfaat dari konektivitas jaringan internet yang terkoneksi secara penuh dan dapat dihubungkan pada perangkat, mesin, dan benda fisik lainnya dengan mempergunakan jaringan, sensor dan aktuator untuk mendapatkan data dan mengelolanya, sehingga mesin dapat berkolaborasi dan bertindak sesuai dengan informasi baru yang di dapat secara mandiri. Menurut IEEE (Institute of Electrical and Electronics Engineers) Internet of things (IoT) didefinisikan sebagai sebuah jaringan dengan masing-masing benda yang ternanam dengan sensor yang terhubung kedalam jaringan internet [8].

Keamanan dalam Internet of Things (IoT) merupakan hal yang sangat penting untuk memastikan bahwa sistem IoT tetap terlindungi dari berbagai ancaman yang dapat merusak fungsinya. Alat-alat keamanan yang diterapkan dalam IoT berfungsi untuk melindungi sistem dari potensi pelanggaran, mengidentifikasi risiko, dan mengintegrasikan langkah-langkah mitigasi untuk mengatasi kerentanannya. Keamanan IoT juga memainkan peran krusial dalam menjaga ketersediaan, kerahasiaan, dan integritas data dalam sistem tersebut. Selain itu, keamanan privasi dalam konteks IoT menjadi semakin penting, mengingat IoT menghubungkan berbagai perangkat dan data, sementara privasi berfungsi untuk melindungi informasi yang sensitif [6]. Dalam dunia yang semakin terhubung, baik pengembang, produsen, maupun konsumen harus bekerja sama untuk memastikan bahwa privasi tetap terjaga, terutama terkait dengan data pribadi yang dikumpulkan dan dipertukarkan dalam ekosistem IoT [7].

Peningkatan jumlah perangkat yang terhubung melalui jaringan 5G meningkatkan risiko terhadap serangan siber. Data yang ditransfer melalui jaringan ini dapat mencakup informasi sensitif, seperti lokasi pengguna, kebiasaan berinternet, dan data biometric [3]. Oleh karena itu, perlindungan terhadap data pribadi menjadi semakin penting untuk mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab [3]. Masyarakat Indonesia, saat ini mulai menyadari akan pentingnya perlindungan data pribadi, terutama dengan semakin banyaknya kasus kebocoran data yang merugikan individu dan organisasi. Pemerintah merespons dengan memperkenalkan berbagai regulasi, yang paling signifikan adalah Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022 [5]. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia telah memberikan kerangka hukum untuk perlindungan data, implementasinya masih menghadapi berbagai tantangan. Salah satu masalah utama adalah rendahnya kesadaran masyarakat mengenai hak-hak privasi mereka, yang berpotensi meningkatkan risiko penyalahgunaan data pribadi [3]. Penegakan hukum yang lemah terhadap pelanggaran data juga menjadi faktor yang mengkhawatirkan, mengingat sanksi yang ada belum cukup untuk memberikan efek jera [3].

Keamanan jaringan 5G juga dipengaruhi oleh infrastruktur keamanan siber yang ada. Saat ini, infrastruktur tersebut belum sepenuhnya siap untuk menghadapi kompleksitas yang dibawa oleh teknologi 5G dan IoT [3]. Dalam konteks ini, penting bagi semua pemangku kepentingan termasuk pemerintah, sektor swasta, dan Masyarakat untuk bekerja sama dalam menciptakan lingkungan digital yang aman [3]. Salah satu strategi untuk melindungi data di era 5G adalah dengan menerapkan enkripsi data secara menyeluruh. Enkripsi dapat membantu melindungi informasi dari serangan siber dan kebocoran data [2]. Selain itu, peningkatan kesadaran keamanan di kalangan pengguna juga menjadi kunci dalam menjaga privasi dan keamanan data mereka [3].

Perlunya regulasi yang ketat juga tidak bisa diabaikan. Pemerintah harus memastikan bahwa perangkat IoT yang dijual di pasaran memenuhi standar keamanan yang memadai dan bahwa ada kebijakan yang mendukung perlindungan data pengguna [4]. Dengan adanya regulasi yang jelas dan penegakan hukum yang tegas, diharapkan dapat mengurangi risiko pelanggaran privasi di era 5G. Di samping itu, pendekatan berbasis teknologi seperti penggunaan kecerdasan buatan (AI) untuk memantau dan menganalisis ancaman keamanan juga dapat menjadi langkah proaktif dalam melindungi data pribadi [4]. AI dapat membantu dalam mendeteksi pola perilaku mencurigakan dan memberikan peringatan dini sebelum serangan terjadi. Dalam rangka menghadapi tantangan ini, kolaborasi antara pemerintah, sektor swasta, dan masyarakat sangat diperlukan. Edukasi publik mengenai pentingnya perlindungan data pribadi harus ditingkatkan agar masyarakat lebih sadar akan risiko yang ada dan cara-cara untuk melindungi diri mereka sendiri [3]. Namun, penting untuk diingat bahwa penerapan kebijakan data privasi tidak hanya menjadi tanggung jawab pemerintah, tetapi juga membutuhkan partisipasi aktif dari seluruh lapisan masyarakat dan sektor swasta. Semua pihak harus berkolaborasi untuk menciptakan lingkungan digital yang aman, di mana privasi individu dihormati dan dilindungi. Dengan komitmen bersama,

Indonesia dapat memanfaatkan potensi besar dari teknologi 5G sambil memastikan bahwa hak-hak privasi warganya tetap terjaga di era digital yang terus berkembang ini. Dukungan yang berkelanjutan dan kesadaran kolektif menjadi kunci dalam menghadapi tantangan privasi data di masa depan [3]. Dengan komitmen bersama dari semua pihak, Indonesia dapat memanfaatkan potensi besar dari teknologi 5G sambil memastikan bahwa hak-hak privasi warganya tetap terjaga.

Penelitian ini bertujuan untuk mengeksplorasi strategi perlindungan untuk ekosistem IoT dalam konteks keamanan dan privasi data pada teknologi 5G. Dengan memahami tantangan dan peluang yang ada, diharapkan dapat memberikan rekomendasi bagi pembuat kebijakan dan praktisi dalam meningkatkan perlindungan data pribadi di era digital ini.

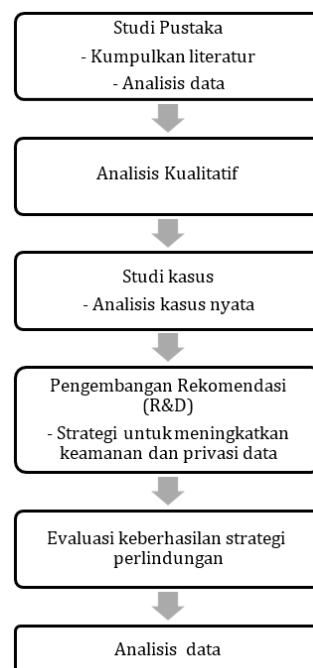
2. METODE PENELITIAN

Dalam penelitian ini, metode yang digunakan untuk mengeksplorasi isu keamanan dan privasi data pada teknologi 5G serta strategi perlindungan untuk ekosistem IoT terdiri dari beberapa langkah sistematis. Metode ini dirancang untuk memberikan pemahaman yang mendalam tentang tantangan yang dihadapi dan solusi yang dapat diterapkan untuk meningkatkan keamanan data. Studi pustaka adalah istilah lain dari kajian pustaka, tinjauan pustaka, kajian teoritis, landasan teori, telaah pustaka (literature review), dan tinjauan teoritis [9]. Yang dimaksud penelitian kepustakaan adalah penelitian yang dilakukan hanya berdasarkan atas karya tertulis, termasuk hasil penelitian baik yang telah maupun yang belum dipublikasikan [10].

Metode analisis data kualitatif adalah metode pengolahan data secara mendalam dengan data dari hasil pengamatan, wawancara, dan literatur. Teknik menganalisis data kualitatif dengan cara meringkas, mengkategorikan dan menafsirkan [11]. Analisis kualitatif bertujuan memperoleh gambaran seutuhnya mengenai suatu hal menurut pandangan manusia yang diteliti [12]. Studi kasus merupakan penelitian dimana peneliti menggali suatu fenomena tertentu (kasus) dalam suatu waktu dan kegiatan (program, even, proses, institusi atau kelompok sosial) serta mengumpulkan informasi secara terinci dan mendalam dengan menggunakan berbagai prosedur pengumpulan data selama periode tertentu [13].

Penelitian dan pengembangan dalam Bahasa Inggris diterjemahkan sebagai research and development (R & D) merupakan metode penelitian yang banyak diadopsi oleh dunia akademik dewasa ini untuk merancang dan menguji efektifitas produk. Metode ini bertujuan untuk menghasilkan produk melalui proses penemuan potensi masalah, mendesain dan mengembangkan suatu produk sebagai Solusi terbaik [14].

Gambar 1 adalah rincian dari metode penelitian.



Gambar 1. Flowchart Tahapan Penelitian

Studi pustaka dilakukan dengan mengumpulkan dan menganalisis literature terkait keamanan dan privasi data dalam konteks 5G dan IoT. Sumber-sumber yang digunakan mencakup jurnal ilmiah, laporan industri, dan publikasi pemerintah yang relevan. Penelitian sebelumnya mengenai ancaman keamanan siber, kerentanan perangkat IoT, serta praktik terbaik dalam perlindungan data menjadi dasar untuk memahami konteks dan tantangan yang ada.

Analisis kualitatif dilakukan untuk mengidentifikasi dan mengevaluasi tantangan serta strategi perlindungan yang ada dalam ekosistem IoT di era 5G. Data dikumpulkan melalui analisis dokumen dan laporan dari berbagai sumber yang membahas isu-isu keamanan dan privasi dalam teknologi IoT. Pendekatan ini bertujuan untuk mendapatkan perspektif mendalam mengenai isu-isu yang dihadapi serta solusi yang dianggap efektif dalam meningkatkan keamanan dan privasi data. Studi kasus dilakukan pada beberapa organisasi yang telah menerapkan strategi perlindungan data dalam lingkungan 5G dan IoT. Analisis terhadap kebijakan keamanan siber yang diterapkan oleh organisasi- organisasi ini memberikan wawasan praktis tentang efektivitas berbagai pendekatan dalam melindungi data pengguna.

Pengembangan rekomendasi, berdasarkan hasil analisis kualitatif dan studi kasus, penelitian ini mengembangkan rekomendasi strategis untuk meningkatkan keamanan dan privasi data dalam ekosistem IoT di era 5G. Rekomendasi tersebut mencakup langkah- langkah teknis seperti enkripsi data, penggunaan autentikasi multi-faktor, serta kebijakan privasi yang ketat. Evaluasi keberhasilan strategi perlindungan, sebagai bagian dari metode penelitian, evaluasi dilakukan terhadap keberhasilan strategi perlindungan yang telah diterapkan oleh organisasi atau individu dalam menjaga keamanan data mereka. Evaluasi ini melibatkan pengukuran efektivitas langkah- langkah mitigasi terhadap ancaman yang teridentifikasi sebelumnya.

Analisis data yang dikumpulkan dari studi kasus dianalisis menggunakan metode statistik deskriptif untuk mengidentifikasi pola-pola perilaku dan sikap pengguna terhadap keamanan data. Hasil analisis ini akan disajikan dalam bentuk tabel untuk memudahkan pemahaman serta interpretasi oleh pembaca.

3. HASIL DAN PEMBAHASAN

3.1 Alur Proses Keamanan dan Privasi Data pada Teknologi 5G

Berdasarkan hasil observasi terhadap penerapan teknologi 5G dalam ekosistem IoT di PT XYZ, ditemukan bahwa alur proses produksi terdiri dari beberapa tahapan utama yang saling berkaitan: enkripsi data, autentikasi, dan segmentasi jaringan. Setiap tahapan memiliki peran penting dalam memastikan keamanan dan privasi data yang dikirimkan antar perangkat dalam jaringan 5G. Ketidakterhasilan dalam satu tahapan, misalnya dalam segmentasi jaringan, dapat berdampak langsung pada potensi serangan siber yang bisa mengancam keamanan data pengguna.

Temuan yang signifikan dalam alur proses adalah bahwa meskipun enkripsi data sudah diterapkan pada sebagian besar sistem, masih terdapat kesenjangan dalam pelaksanaannya pada tahap transmisi data di beberapa perangkat IoT. Selain itu, otentikasi yang diterapkan tidak selalu konsisten, terutama pada perangkat yang lebih lama atau yang tidak memiliki pembaruan perangkat keras terbaru.

3.2 Ancaman Keamanan pada Infrastruktur 5G dan Dampaknya

Dua ancaman utama yang diidentifikasi dalam penelitian ini adalah serangan DDoS dan MitM, yang berpotensi mengganggu ketersediaan dan kerahasiaan data dalam jaringan 5G.

Serangan DDoS:

DDoS merupakan ancaman yang cukup serius bagi jaringan 5G, yang dapat mengakibatkan gangguan besar terhadap ketersediaan layanan. Penelitian menunjukkan bahwa dengan meningkatnya konektivitas perangkat IoT, serangan DDoS dapat melumpuhkan infrastruktur dengan cara membanjiri server dengan permintaan palsu. Penurunan kecepatan layanan dan bahkan kerusakan pada server dapat terjadi dalam waktu yang sangat singkat jika serangan ini tidak ditanggulangi dengan cepat.

Serangan MitM:

Serangan ini lebih berfokus pada penyusupan komunikasi antar perangkat yang sedang berinteraksi dalam jaringan. Dalam konteks IoT, serangan ini bisa sangat merusak karena penyerang dapat mengakses informasi sensitif seperti data pribadi pengguna, identitas, dan lokasi perangkat. Tanpa adanya

sistem enkripsi yang kuat dan autentikasi yang memadai, data yang ditransmisikan antar perangkat IoT dapat dengan mudah disadap dan dimodifikasi oleh pihak yang tidak berwenang.

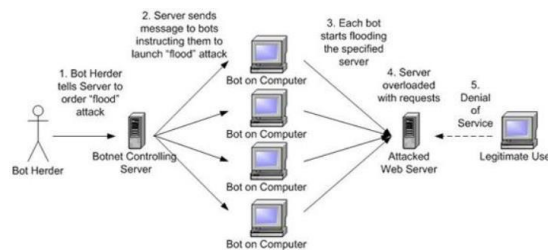
Tabel 1. Rekapitulasi Ancaman Keamanan pada Infrastruktur 5G

Jenis Ancaman	Dampak	Frekuensi Serangan	Mitigasi yang Diterapkan
DDoS	Gangguan Ketersediaan Layanan	Tinggi	Pembatasan Lalu Lintas Jaringan, Firewall
MitM	Pencurian Data Sensitif	Menengah	Enkripsi, Autentikasi Multi-Faktor

3.3 Perlindungan Data pada Teknologi 5G

Melihat ancaman yang ada, perlindungan data pada jaringan 5G perlu diterapkan secara menyeluruh di setiap tahapan proses. Penelitian ini menunjukkan bahwa enkripsi data memainkan peran penting dalam menjaga keamanan data yang dikirimkan antar perangkat dalam ekosistem IoT.

Namun, meskipun protokol enkripsi seperti AES (Advanced Encryption Standard) sudah diterapkan, implementasinya masih kurang pada perangkat IoT tertentu. Banyak perangkat yang tidak diperbarui secara rutin, sehingga tidak dapat mengikuti protokol enkripsi yang lebih canggih. Hal ini memperbesar risiko kebocoran data. Selain enkripsi, autentikasi multi-faktor juga perlu diterapkan untuk meningkatkan lapisan keamanan. Sayangnya, banyak perangkat yang masih menggunakan metode autentikasi yang lemah, seperti hanya mengandalkan kata sandi atau PIN yang mudah ditebak.



Gambar 2. Serangan DDoS dalam Jaringan 5G

3.4 Rekomendasi untuk Penguatan Keamanan Data dalam Teknologi 5G

Berdasarkan hasil penelitian ini, beberapa langkah untuk meningkatkan keamanan dan privasi data dalam ekosistem 5G yang mendukung IoT adalah sebagai berikut:

1. Peningkatan Standarisasi Keamanan
Penguatan standar enkripsi dan autentikasi adalah langkah utama yang perlu diterapkan di seluruh perangkat IoT yang terhubung ke jaringan 5G. Penggunaan AES untuk enkripsi data dan penerapan autentikasi dua faktor dapat membantu mengurangi risiko serangan MitM.
2. Segmentasi Jaringan dan Penggunaan Firewall
Dengan menggunakan network slicing dalam teknologi 5G, kita bisa memisahkan berbagai kategori perangkat IoT berdasarkan tingkat sensitivitas data yang mereka kirimkan. Dengan cara ini, risiko serangan DDoS dapat dikurangi dengan membatasi dampaknya hanya pada segmen-segmen tertentu dari jaringan.
3. Pembaruan Perangkat IoT secara Berkala
Pengelolaan perangkat IoT sangat penting untuk memastikan perangkat tersebut tetap aman dari ancaman yang terus berkembang. Pembaruan perangkat lunak dan firmware secara teratur akan memastikan bahwa perangkat tetap terlindungi dari kerentanannya.
4. Peningkatan Kesadaran Pengguna
Selain penguatan teknis, pendidikan dan kesadaran pengguna mengenai pentingnya perlindungan data pribadi dan langkah-langkah keamanan seperti enkripsi dan autentikasi harus dilakukan. Pengguna yang lebih sadar akan pentingnya menjaga data pribadi mereka akan lebih berhati-hati dalam menggunakan perangkat IoT.

3.5 Evaluasi Keberhasilan Perlindungan Data dalam Infrastruktur 5G

Evaluasi terhadap penerapan kebijakan perlindungan data di PT XYZ menunjukkan adanya peningkatan dalam pengendalian ancaman siber setelah penerapan enkripsi data yang lebih kuat dan autentikasi multi-faktor. Namun, beberapa perangkat IoT yang lebih lama masih menjadi celah bagi serangan, yang menunjukkan perlunya pembaruan dan pengawasan yang lebih ketat.

4. SIMPULAN

Berdasarkan hasil analisis proses produksi pressure plate di PT xyz, dapat disimpulkan bahwa alur produksi yang meliputi tahap pengecoran, pengujian material, proses machining, dan inspeksi kualitas akhir membentuk satu sistem yang saling bergantung dalam menentukan mutu produk. Kualitas pada tahap awal terbukti berpengaruh signifikan terhadap keberhasilan proses lanjutan dan mutu produk akhir. Perkembangan teknologi 5G telah menunjukkan dampak signifikan yang ditawarkannya dalam industri telekomunikasi global. Keunggulan utamanya yaitu kecepatan internet yang jauh lebih cepat, latensi yang rendah, dan kapasitas jaringan yang lebih besar menunjukkan potensi besar dari teknologi ini. Implementasi 5G diharapkan dapat mempercepat berbagai inisiatif digital dan memperluas akses teknologi, terutama di wilayah-wilayah yang sebelumnya terbatas jangkauannya. Dengan demikian, diharapkan implementasi 5G akan memberikan perubahan besar dalam berbagai sektor dan meningkatkan kualitas hidup masyarakat secara keseluruhan. Selain itu, penelitian lebih lanjut diperlukan untuk memahami lebih dalam tentang bagaimana teknologi 5G dapat diterapkan secara efektif dan aman. Penelitian ini harus mencakup aspek-aspek seperti keamanan jaringan, privasi data, dan infrastruktur yang mendukung. Dengan demikian, kita dapat memastikan bahwa implementasi 5G tidak hanya memberikan manfaat teknis, tetapi juga mempertimbangkan aspek-aspek penting lainnya yang berkaitan dengan privasi dan keamanan data. Rekomendasi untuk penelitian selanjutnya mencakup penelitian yang lebih mendalam mengenai tantangan implementasi 5G, studi tentang bagaimana organisasi dapat mempersiapkan diri untuk menghadapi tantangan ini, dan penelitian yang berfokus pada pengembangan teknologi keamanan yang lebih lanjut. Dengan demikian, kita dapat memastikan bahwa perkembangan teknologi 5G memberikan manfaat yang optimal dan aman bagi masyarakat.

DAFTAR PUSTAKA

- [1] Hamzah, U. M., Montolalu, B., & Hafidz, I. (2021). "5G Network as a Technology to Fight Covid-19 Pandemic in Indonesia: A Review". *Journal of Computer, Electronic, and Telecommunication*, vol. 2, no. 2, pp. 165-180, 2021. [Online]. Available: <https://doi.org/10.52435/complete.v2i2.165>
- [2] Archa Anugerah. (2023, Maret 07). Privasi dan Keamanan Data di Era 5G, *bidiknews24.com*. [Online]. Available: <https://bidiknews24.com/privasi-dan-keamanan-data-di-era-5g>
- [3] Y. Fatmawati and A. Firdonsyah, "Penerapan kebijakan data privacy di era teknologi 5G di Indonesia," *Pencerah Publik*, vol. 11, no. 1, 2024.
- [4] Laras. (2023, Januari 13). Waspada! Data Pribadi Bisa Dicuri Lewat Jaringan 5G, *Bisnis Tekni*. [Online]. Available: <https://teknologi.bisnis.com/read/20230113/84/1617987/waspada-data-pribadi-bisa-dicuri-lewat-jaringan-5g>
- [5] V. W. S. Soemarwi and W. Susanto, "Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right," *Proc. Int. Conf. Econ. Business, Soc. Humanit. (ICEBSH 2021)*, vol. 570, no. Icebsh, pp. 561–566, 2021, doi: 10.2991/assehr.k.210805.088.
- [6] F. Prasetyo Eka Putra, S. Mellyana Dewi, and A. Hamzah, "Jurnal Sistim Informasi dan Teknologi <https://jsisfotek.org/index.php> Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi," vol. 5, no. 2, pp. 26–32, 2023, doi: 10.37034/jsisfotek.v5i1.232.
- [7] F. Nahdi and H. Dhika, "Analisis Dampak Internet of Things (IoT) Pada Perkembangan Teknologi di Masa Yang Akan Datang," pp. 33–40.
- [8] D. Setiadi and M. N. Abdul Muhaemin, "Penerapan Internet Of Things (IoT) Pada Sistem Monitoring Irigasi (Smart Irigasi)," *Infotronik: Jurnal Teknologi Informasi Dan Elektronika*, vol. 3, no. 2, p. 95, 2018.
- [9] Melfianora, "PENULISAN KARYA TULIS ILMIAH DENGAN STUDI LITERATUR," *UPT Balai Pelatih. Penyuluh Pertanian.*, pp. 1– 3, [Online]. Available: <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://osf.io/gfe9w/download&ved=2ahUKEwiBiKG100-JAXXLoGMGHQXKGzIQFnoECBYQAQ>

-
- &usg=AOvVaw2htNSHllJpCc6K7MtEbk G
- [10] B. Embun, "Banjir Embun," *Penelitian Kepustakaan*, Apr. 17, 2012. [Online]. Available: <http://banjirembun.blogspot.co.id/2012/04/penelitian-kepustakaan.html>. [Accessed: Nov. 21, 2024].
 - [11] B. A. B. Iii and M. Penelitian, "No Title," pp. 27–42, 2009, [Online]. Available: http://eprints.undip.ac.id/40650/3/BAB_III.pdf
 - [12] BINUS, "MEMAHAMI PERBEDAAN ANALISIS KUALITATIF DAN ANALISIS KUANTITATIF DALAM PENELITIAN ILMIAH," [binus.ac.id](https://accounting.binus.ac.id/2021/08/12/memahami-perbedaan-analisis-kualitatif-dan-analisis-kuantitatif-dalam-penelitian-ilmiah/). [Online]. Available: <https://accounting.binus.ac.id/2021/08/12/memahami-perbedaan-analisis-kualitatif-dan-analisis-kuantitatif-dalam-penelitian-ilmiah/>
 - [13] D. Assyakurrohim, D. Ikham, R. A. Sirodj, and M. W. Afgani, "Jurnal Pendidikan Sains dan Komputer Metode Studi Kasus dalam Penelitian Kualitatif Jurnal Pendidikan Sains dan Komputer," vol. 3, no. 1, pp. 1–9, 2023.
 - [14] M. Waruw, "Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan," *J. Ilm. Profesi Pendidik.*, vol. 9, pp. 1220–1230.
 - [15] E. M. S. S. Sahrul Gunawan, Atha Agdo Ramdi Santosa, "Analisis Keamanan Jaringan 5G : Ancaman dan Upaya Mitigasi," *Inform. Prodi Tek. Fak. I, Univ. Persada Indones. YA*, vol. 22, no. 2, pp. 54– 62, 2024.
 - [16] M. A. Masa, T. S. D. Abdurrahman, A. Basalamah, M. N. Rahman, H. Lahmado, and A. Afdhal, "Analisis Potensi Teknologi Jaringan 5G Area Sulawesi Selatan," *Jambura J. Electr. Electron. Eng.*, vol. 5, no. 1, pp. 41–47, 2023, doi: 10.37905/jjee.v5i1.16870.
 - [17] A. Maulana, H. Tiftazani, M. N. Mahmudi, R. Septiawan, and R. A. R. Qori, "Analisis Quality of Services Jaringan 5G Provider X dan Y untuk Aplikasi Vidio Streaming Resolusi 4K (Studi Kasus di Kota Pekanbaru) Network Quality of Services Analysis of 5G Provider X and Y for 4K Video Streaming Application (a Case Study in Pekanba," vol. 11, no. 1, 2023, [Online].