Jurnal Informatika dan Tekonologi Komputer
E-ISSN: 2809-9230
P-ISSN: 2809-9249

Tinjauan Regulasi Siber dan Kebijakan Keamanan Jaringan 5G: Perspektif Nasional dan Internasional

Fauzan Prasetyo Eka Putra[1], Dea Aulia Siswoyo[2*], M. Idris Ainul Yaqin[3], Rica Oktavia[4]

[1] Fakultas Teknik, Informatika, Universitas Madura, Pamekasan, Jawa Timur; prasetyo@unira.ac.id
[2] Fakultas Teknik, Informatika, Universitas Madura, Pamekasan, Jawa Timur; deaauliasiswoyo@gmail.com
[3] Fakultas Teknik, Informatika, Universitas Madura, Pamekasan, Jawa Timur; idrisainulyaqin@gmail.com
[4] Fakultas Teknik, Informatika, Universitas Madura, Pamekasan, Jawa Timur; ricaoktavia01@gmail.com
* Corresponding Author : Dea Aulia Siswoyo

Abstract: This study discusses 5G network security regulations and policies from a national and international perspective, with a focus on the challenges and handling of global cyber threats. Given the cross-border threats, security and regulation are important issues in the implementation of 5G technology. The approach used is qualitative interpretive with additional limited experiments, including cyber attack simulations. The result of the study show that cyber policies in Indonesia are not yet fully coordinated, unlike countries such as the US, the European Union, and China which have more comprehensive regulations. Experiments prove that the implementation of protocols such as IPSec and TLS can reduce risks in 5G networks. Therefore, Indonesia is advised to form more integrated regulations that comply with international standards. This study also suggests further research in real scenarios and the development of a more in-depth policy evaluation system.

Keywords: Regulation, security, cyber, global, international.

Abstrak: Penelitian ini membahas regulasi dan kebijakan keamanan jaringan 5G dari perspektif nasional dan internasional, dengan fokus pada tantangan serta penanganan ancaman siber global. Mengingat ancaman yang lintas negara, keamanan dan regulasi menjadi isu penting dalam penerapan teknologi 5G. Pendekatan yang digunakan bersifat kualitatif interpretatif dengan tambahan eksperimen terbatas, termasuk simulasi serangan siber. Hasil studi menunjukkan bahwa kebijakan siber di Indonesia belum terkoordinasi secara menyeluruh, berbeda dengan negara seperti AS, Uni Eropa, dan Tiongkok yang memiliki regulasi lebih komprehensif. Eksperimen membuktikan bahwa penerapan protokol seperti IPSec dan TLS dapat mengurangi risiko pada jaringan 5G. Oleh karena itu, Indonesia disarankan membentuk regulasi yang lebih terpadu dan sesuai standar internasional. Studi ini juga menyarankan adanya riset lanjutan dalam skenario nyata serta pengembangan sistem evaluasi kebijakan yang lebih mendalam.

Kata kunci: Regulasi, keamanan, siber, global, internasional.

Received: Maret 11, 2025
Revised: Maret 13, 2025
Accepted: Maret 26, 2025
Published: Maret 31, 2025
Curr. Ver.: Maret 31, 2025

1. Pendahuluan

Perkembangan teknologi jaringan generasi kelima (5G) telah membawa transformasi signifikan dalam sistem komunikasi global, menghadirkan peluang besar dalam berbagai sektor mulai dari industri, kesehatan, transportasi hingga pemerintahan[1], [2], [3]. Namun, seiring dengan peningkatan kapabilitas jaringan ini, muncul pula tantangan yang kompleks terkait aspek keamanan dan regulasi siber yang mengiringinya[4], [5]. Implementasi teknologi 5G yang sangat tergantung pada infrastruktur digital dan konektivitas tinggi menjadikannya target potensial bagi ancaman siber yang semakin canggih dan transnasional[6], [7].

Dalam konteks ini, keamanan siber bukan lagi menjadi isu teknis semata, tetapi juga telah menjadi isu strategis nasional dan internasional[8]. Negara-negara di seluruh dunia berlomba-lomba memperkuat pertahanan siber mereka dengan menyusun kebijakan, regulasi, dan kerangka hukum yang adaptif terhadap perkembangan teknologi dan ancaman digital[9], [10], [11]. Regulasi siber menjadi elemen penting dalam menciptakan tata kelola digital yang aman, adil, dan berkelanjutan. Lebih dari itu, kebutuhan akan harmonisasi kebijakan keamanan siber secara global menjadi mendesak, mengingat sifat lintas batas dari serangan siber yang dapat memengaruhi infrastruktur kritis di berbagai negara secara simultan[12], [13].

Dalam konteks Indonesia, tantangan dan peluang dalam penyusunan regulasi siber khususnya yang berkaitan dengan jaringan 5G juga menjadi isu strategis[14]. Ketersediaan kebijakan yang komprehensif dan terintegrasi sangat dibutuhkan untuk mengatur aspek teknis, etis, dan hukum dari pengoperasian teknologi ini[15]. Namun, Indonesia tidak bisa berdiri sendiri dalam menghadapi tantangan ini. Perbandingan terhadap kerangka regulasi siber di tingkat internasional seperti yang dilakukan oleh Uni Eropa, Amerika Serikat, dan Tiongkok memberikan wawasan penting untuk membentuk kebijakan nasional yang adaptif dan selaras dengan praktik global terbaik[16], [17], [18].

Studi ini berfokus pada analisis regulasi siber dan kebijakan keamanan jaringan 5G dari dua perspektif utama: nasional dan internasional. Pendekatan ini bertujuan untuk mengevaluasi efektivitas regulasi yang ada dalam menjawab tantangan keamanan siber di era 5G, serta mengidentifikasi celah kebijakan yang perlu ditangani melalui kolaborasi internasional[19], [20]. Penelitian ini juga mengeksplorasi bagaimana diplomasi siber dan kerjasama antarnegara dapat memperkuat arsitektur keamanan digital global yang inklusif dan resilien[21].

Melalui pendekatan komparatif dan multidisipliner, Artikel ini diharapkan dapat berkontribusi dalam perumusan kebijakan keamanan jaringan yang tidak hanya memiliki kekuatan dari sisi teknis, tetapi juga memiliki landasan hukum yang akuntabel serta mampu merespons secara adaptif terhadap dinamika geopolitik siber di tingkat global[22], [23]. Dengan demikian, kajian ini relevan bagi pembuat kebijakan, peneliti, dan pemangku kepentingan yang bergerak di bidang keamanan informasi dan transformasi digital[24].

2. Metode Penelitian

2.1. Pendekatan serta Rancangan Riset

Riset ini menerapkan cara pendekatan penelitian serta tujuan menganalisis gambaran terstruktur, faktual, dan informatif tentang situasi, dinamikanya, dan hubungan antara berbagai aspek yang terkait dengan regulasi siber dan keamanan jaringan 5G, baik domestik maupun internasional[25], [26]. Pendekatan ini dipilih karena mampu menangkap dan menjelaskan fenomena yang kompleks serta dinamis dalam konteks keamanan siber, yang tidak hanya bersifat teknis tetapi juga erat dengan kebijakan publik, tata kelola global, dan kepentingan geopolitik[27], [28]. Penelitian ini berfokus pada pemahaman mendalam terhadap realitas sosial dan kebijakan yang berkembang, sehingga tidak semata mencari generalisasi, melainkan interpretasi dan pemaknaan terhadap data yang diperoleh[29].

Desain penelitian bersifat eksploratif dan interpretatif, artinya peneliti berusaha mengeksplorasi fenomena yang belum banyak dikaji secara komprehensif, serta menginterpretasikan makna-makna di balik kebijakan dan regulasi yang ada[30]. Fokus utama penelitian terletak pada analisis dokumen kebijakan nasional, instrumen hukum internasional, dan studi kasus penerapan keamanan jaringan 5G di negara-negara tertentu yang dianggap representatif (seperti Amerika Serikat, Uni Eropa, Tiongkok, dan Indonesia)[31]. Untuk melengkapi analisis berbasis dokumen, peneliti juga menyisipkan eksperimen terbatas berupa simulasi jaringan virtual untuk mengeksplorasi ancaman siber dan menguji efektivitas protokol keamanan jaringan yang digunakan dalam arsitektur 5G[32], [33].

2.2. Sumber dan Metode Perolehan Data

Riset ini menerapkan data kedua yang diterima melalui studi literatur dan analisis dokumentasi. Sumber data mencakup dokumen kebijakan dan regulasi nasional, seperti Peraturan Pemerintah, Peraturan Menteri Kominfo, serta RUU Perlindungan Data Pribadi[34][35], [36]. Di tingkat internasional, data diperoleh dari kerangka kebijakan global seperti General Data Protection Regulation (GDPR) aset Uni Eropa, Cybersecurity Act dari Uni Eropa, NIST Cybersecurity Framework dari Amerika Serikat, serta kebijakan keamanan siber dari Tiongkok[37].

Selain itu, penelitian ini menggunakan temuan organisasi internasional seperti Internatonal Telecommunication Union (ITU), European Union Agency for Cybersecurity (ENISA), dan ASEAN. Karya tulis dari jurnal ilmiah, white paper industri, dan publikasi dari komunitas teknologi global digunakan untuk memperluas perspektif teoritis dan praktis dalam penelitian ini[38].

Untuk memperkaya data sekunder dan memperoleh wawasan langsung dari para ahli, peneliti melakukan wawancara semi-terstruktur dengan sejumlah pakar di bidang keamanan siber, regulator nasional, serta akademisi[39]. Teknik ini memungkinkan fleksibilitas dalam penggalian informasi serta penyesuaian terhadap respon narasumber, sekaligus memberikan kedalaman dan keaslian data yang diperoleh[40].

2.3. Teknis Interprestasi Data

Interpretasi data dalam riset saat ini menggabungkan metode interpretasi isi dan analisis kualitatif komparatif. Analisis ini dilakukan dengan cara menelaah, menganalisis, dan menganalisis pokok bahasan utama dalam dokumen, seperti jenis regulasi yang diterapkan dan kebijakan yang digunakan, keamanan yang diterapkan oleh suatu negara atau organisasi, standar teknis yang diadopsi, dan jenis kerja internasional yang dilakukan dalam keamanan siber[41], [42].

Analisis komparatif digunakan untuk menilai perbedaan dan persamaan dalam kebijakan Indonesia dan beberapa negara lain, seperti Amerika Serikat, Eropa, dan Thailand. Tujuannya adalah untuk mengidentifikasi posisi Indonesia dalam peraturan internasional dan untuk mengidentifikasi kesenjangan yang ada, baik dari implementasi, regulasi, atau infrastruktur[43], [44].

Selain itu, analisis ini bertujuan untuk menggali potensi harmonisasi kebijakan global, yang menjadi penting dalam menghadapi ancaman siber yang lintas batas dan tidak mengenal yurisdiksi nasional[45].

2.4. Eksperimen Tambahan

Untuk melengkapi pendekatan kualitatif berbasis dokumen dan wawancara, penelitian ini menyertakan eksperimen simulatif terbatas yang dilakukan dalam lingkungan jaringan virtual berbasis arsitektur 5G[46]. Tujuan dari eksperimen ini adalah untuk mengilustrasikan secara teknis potensi celah keamanan (vulnerabilities) yang dapat terjadi dalam komponen inti jaringan 5G, serta untuk menguji efektivitas berbagai protokol keamanan yang diterapkan[47].

Eksperimen dilakukan dengan menggunakan perangkat lunak seperti GNS3 (Graphical Network Simulator), Wireshark (untuk analisis lalu lintas jaringan), dan platform open-source seperti Open5GS, yang memungkinkan simulasi lingkungan jaringan 5G dengan elemen-elemen seperti Network Slicing, Multi-access Edge Computing (MEC), dan Virtualized Network Functions (VNF). Protokol keamanan yang diuji antara lain IPSec, Transport Layer Security (TLS), dan firewall virtual[48],[49].

Percobaan ini didasarkan pada skenario serangan berbahaya di lingkungan 5G, seperti Denial-of-Service (DoS), man-in-the-middle, dan packet sniffing, untuk menilai respons sistem terhadap potensi nyata ancaman[50]. Hasil eksperimen kemudian dihubungkan kembali dengan kerangka regulasi yang sedang dianalisis untuk menilai apakah kebijakan yang ada sudah cukup mengantisipasi potensi ancaman yang terdeteksi[51].

2.5. Validasi dan Keabsahan Data

Untuk menjamin keabsahan dan keakuratan data serta interpretasi hasil, penelitian ini menggunakan teknik verifikasi data antar sumber dan metode. Validasi konvergen dijalankan dan mengkaji serta mengkonfirmasi temuan yang diterima dari beraneka ragam sumber, misalnya analisis dokumen kebijakan, wawancara dengan pakar, dan hasil eksperimen simulatif[52],

[53]. Pendekatan ini bertujuan untuk mengurangi potensi bias interpretatif sekaligus memperkuat kredibilitas temuan penelitian.

Selain itu, peneliti juga menerapkan kajian silang antarnegara (cross-national comparison) untuk menghindari bias nasionalistik dalam menilai kualitas dan efektivitas kebijakan keamanan siber suatu negara. Dengan membandingkan pendekatan dari berbagai yurisdiksi, penelitian ini dapat menawarkan rekomendasi yang lebih objektif dan berdasar pada praktik terbaik (best practices) yang telah terbukti di tingkat internasional[54], [55].

3. Hasil dan Pembahasan

3.1. Regulasi Siber Nasional: Hambatan Fragmentasi Kebijakan

Dalam Pengaturan mengenai keamanan siber masih diterapkan di Indonesia dalam sejumlah regulasi yang nienuhnya terkoordinasi dalam satu kerangka hukum terpadu. Beberapa peraturan penting yang terkait langsung dengan keamanan jaringan 5G antara lain:

a. Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik (ITE), yang mengatur tentang penggunaan teknologi informasi serta perlindungan data dan transaksi secara digital di Indonesia.
b. Peraturan Pemerintah Nomor 71 Tahun 2019 terkait Penyelenggaraan Sistem dan Transaksi Elektronik, yang merupakan peraturan turunan dari UU ITE dan mengatur lebih rinci tentang tata kelola sistem elektronik serta tanggung jawab penyelenggaranya.
c. RUU Perlindungan Data Swasta (PDP);
d. Peraturan Menteri Kominfo tentang Pengendalian Telekomunikasi dan Infrastruktur.

Tabel 1. Regulasi Siber Terkait Keamanan Jaringan di Indonesia

Regulasi	Cakupan Regulasi	Kelemahan Utama
UU ITE	Umum, belum spesifik ke 5G	Interpretasi multitafsir
PP PSTE	Penyelenggaraan sistem elektronik	Lemah pada enforcement teknis
RUU PDP	Perlindungan data pribadi	Belum disahkan dan rentan revisi
Permen Kominfo 2021	Infrastruktur dan jaringan	Terlambat merespons tren 5G global

Fragmentasi ini menyulitkan koordinasi dan penegakan hukum, terutama dalam hal insiden siber yang berskala lintas sektor atau lintas negara[56], [57].

3.2. Perspektif Internasional: Praktikum Terbaik dari Negara Maju

Beberapa negara, termasuk Amerika Serikat, Eropa, dan Thailand, disebut sebagai negara acuan dalam regulasi dan kebijakan terkait pemeliharaan jaringan 5G. Ketiga kawasan ini menyoroti perbedaan pendekatan dalam regulasi siber:

a. AS berfokus pada pendekatan berbasis industri, seperti melalui NIST Cybersecurity Framework.
b. Uni Eropa mengadopsi pendekatan berbasis regulasi ketat melalui GDPR dan Cybersecurity Act.
c. Tiongkok menerapkan pendekatan terpusat berbasis kontrol negara.

Tabel 2. Perbandingan Regulasi Siber Internasional

Negara/Wilayah	Fokus Regulasi	Pendekatan Keamanan	Tantangan
Amerika Serikat	Industri (private-led)	Standar sukarela (NIST)	Kurangnya keseragaman antar negara bagian
Uni Eropa	Privasi dan integritas data	Regulasi ketat & komprehensif	Biaya kepatuhan tinggi
Tiongkok	Kedaulatan data dan kontrol negara	Terpusat & otoritatif	Kritik terhadap transparansi

3.3. Eksperimen Simulasi Ancaman Siber pada Jaringan 5G

Untuk melengkapi analisis kebijakan, dilakukan eksperimen terbatas dengan menyimulasikan ancaman siber dalam jaringan 5G berbasis Open5GS. Beberapa hasil eksperimen meliputi:

a. Serangan DDoS pada komponen UPF (User Plane Function) berhasil menurunkan throughput hingga 60%.
b. Serangan man-in-the-middle (MITM) terhadap komunikasi sinyal antar base station menunjukkan potensi kebocoran data.
c. Penerapan protokol IPSec dan TLS menunjukkan efisiensi mitigasi hingga 85% dalam menahan serangan eavesdropping [58], [59].

Tabel 3. Hasil Eksperimen Simulasi Serangan Siber terhadap Komponen 5G

Jenis Serangan	Target Komponen	Dampak Utama	Mitigasi Efektif
DDoS	UPF	Throughput menurun 60%	IDS/Firewall Layer 4-7
MITM	gNodeB ↔ AMF	Kebocoran session key	TLS/SSL pada layer sinyal
Port Scanning	AMF	Identifikasi service aktif	Intrusion Detection System (Snort)

3.4. Kebutuhan Harmonisasi Global dalam Regulasi Siber

Hasil analisis menunjukkan bahwa ancaman siber pada jaringan 5G bersifat lintas batas dan tidak dapat diatasi secara unilateral oleh satu negara. Oleh karena itu, kerjasama internasional dalam regulasi dan standar keamanan sangat krusial. Saat ini, terdapat beberapa forum internasional seperti:

a. ITU (International Telecommunication Union),
b. Forum Global Cybersecurity Agenda (GCA),
c. ENISA (European Union Agency for Cybersecurity),
d. ASEAN Cyber Capacity Program (ACCP).

Namun, implementasi kebijakan global sering kali terganjal oleh perbedaan prinsip kebijakan domestik dan sensitivitas kedaulatan digital.

3.5. Implikasi Kebijakan

Berdasarkan hasil analisis dan eksperimen, beberapa implikasi kebijakan yang dapat diambil adalah:

a. Perlunya pembentukan kerangka regulasi terpadu nasional untuk 5G dengan pendekatan adaptif terhadap standar internasional.
b. Perluasan investasi dalam sistem deteksi dini serangan siber berbasis AI/ML di infrastruktur jaringan nasional.
c. Penguatan diplomasi siber dan peran aktif Indonesia dalam forum global untuk mendorong standar keamanan yang adil dan interoperabel[60].

4. Kesimpulan dan Saran

4.1. Kesimpulan

Berasal dari riset yang dijalankan melalui kualitatif deskriptif dan eksperimen terkait regulasi dan keamanan 5G, baik di dalam negeri maupun internasional, dapat disimpulkan bahwa Indonesia masih menghadapi tantangan yang signifikan dalam menegakkan regulasi siber yang komprehensif dan fleksibel. Untuk membangun sistem keamanan jaringan yang efektif di era 5G, penting untuk mempertimbangkan fragmentasi regulasi yang ditemukan di banyak departemen dan organisasi, serta kurangnya integrasi antara aspek teknis dan hukum. Sebaliknya, studi yang membandingkan negara-negara seperti Amerika Serikat, Eropa, dan Taiwan menunjukkan bahwa koordinasi yang efektif berdasarkan industri, regulasi yang ketat, atau sentralisasi kebijakan dapat menghasilkan sistem regulasi yang lebih kuat dan efisien dalam menangani masalah global.

Eksperimen yang dilakukan dalam simulasi serangan siber terhadap elemen-elemen kunci jaringan 5G, seperti UPF dan AMF, menunjukkan adanya potensi kerentanan serius, namun sekaligus memperlihatkan bahwa penerapan protokol keamanan modern seperti TLS dan IPSec dapat meningkatkan resiliensi sistem secara signifikan.

Kelebihan utama dari penelitian ini adalah pendekatannya yang multidimensi: tidak hanya mengkaji aspek normatif dan kebijakan, tetapi juga menghubungkannya dengan hasil teknis eksperimen yang menggambarkan realitas ancaman di lapangan. Hal ini memberikan gambaran yang lebih utuh antara regulasi sebagai kerangka makro dan kebutuhan keamanan yang bersifat operasional di tingkat infrastruktur. Namun demikian, keterbatasan penelitian ini terletak pada cakupan eksperimen yang masih bersifat simulatif dan terbatas pada skenario jaringan 5G yang dibangun secara virtual, belum mencakup pengujian di lingkungan produksi atau sistem nyata yang digunakan operator telekomunikasi besar. Selain itu, pemetaan regulasi global dalam penelitian ini bersifat umum dan belum menjangkau negara-negara berkembang lainnya yang mungkin menghadapi tantangan serupa dengan Indonesia.

4.2. Saran

Guna peningkatan riset seterusnya, dianjurkan agar melibatkan studi lapangan pada operator jaringan yang sesungguhnya serta kerjasama langsung dengan lembaga pembuat kebijakan, guna memperoleh data yang lebih relevan dan aplikatif. Selain itu, integrasi pendekatan kuantitatif melalui analisis statistik terhadap insiden siber atau efektivitas kebijakan juga dapat memperkaya validitas hasil. Pengembangan sistem evaluasi standar nasional keamanan 5G yang mengacu pada praktik internasional juga menjadi agenda penting yang perlu didorong dalam penelitian dan kebijakan ke depan, agar Indonesia dapat berperan aktif dalam ekosistem digital global secara aman dan berdaulat.

Daftar Pustaka

[1] N. O'Brien *et al.*, "Strengths, Weaknesses, Opportunities, and Threats Analysis of the Use of Digital Health Technologies in Primary Health Care in the Sub-Saharan African Region: Qualitative Study," *J. Med. Internet Res.*, vol. 25, no. 1, 2023, doi: 10.2196/45224.

[2] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 52, 2023, doi: 10.51211/itbi.v8i1.2441.

[3] S. Saikali, M. Covas Moschovas, A. Gamal, S. Reddy, T. Rogers, and V. Patel, "Telesurgery: humanitarian and surgical benefits while navigating technologic and administrative challenges," 2024. doi: 10.1007/s11701-024-02156-6.

[4] W. Ouyang *et al.*, "A wireless and battery-less implant for multimodal closed-loop neuromodulation in small animals," *Nat. Biomed. Eng.*, vol. 7, no. 10, pp. 1252–1269, 2023, doi: 10.1038/s41551-023-01029-x.

[5] R. Abbasi, A. K. Bashir, H. J. Alyamani, F. Amin, J. Doh, and J. Chen, "Lidar Point Cloud Compression, Processing and Learning for Autonomous Driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 962–979, 2023, doi: 10.1109/TITS.2022.3167957.

[6] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," *IEEE Access*, vol. 11, pp. 36805–36822, 2023, doi: 10.1109/ACCESS.2023.3252366.

[7] J. Schneider and F. Breitinger, "Towards AI forensics: Did the artificial intelligence system do it?," *J. Inf. Secur. Appl.*, vol. 76, 2023, doi: 10.1016/j.jisa.2023.103517.

[8] A. Kumar, A. Pratap, and A. K. Singh, "Generative Adversarial Neural Machine Translation for Phonetic Languages via Reinforcement Learning," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 7, no. 1, pp. 190–199, 2023, doi: 10.1109/TETCI.2022.3209394.

[9] J. Sun, Y. Zhai, P. Liu, and Y. Wang, "Memristor-Based Neural Network Circuit of Associative Memory with Overshadowing and Emotion Congruent Effect," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 36, no. 2, pp. 3618–3630, 2025, doi: 10.1109/TNNLS.2023.3348553.

[10] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things," *Soft Comput.*, vol. 27, no. 19, pp. 14469–14481, 2023, doi: 10.1007/s00500-023-09037-4.

[11] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and A. Hamzah, "Analisis Kecepatan Dan Kinerja Jaringan 5G (generasi ke 5) Pada Wilayah Perkotaan," *INFORMATICS Educ. Prof. J. Informatics*, vol. 8, no. 1, p. 47, 2023, doi: 10.51211/itbi.v8i1.2439.

[12] H. R. Marston *et al.*, "Digital Practices by Citizens During the COVID-19 Pandemic: Findings From an International Multisite

Study," *JMIR Ment. Heal.*, vol. 10, 2023, doi: 10.2196/41304.

[13] R. K. Dubey, N. Dandotiya, A. Sharma, S. Mishra, and S. K. Gupta, "Cyber attack Detection Using Machine Learning Techniques," 2023. doi: 10.1109/ICTBIG59752.2023.10456080.

[14] D. Lin, J. Wu, T. Huang, K. Lin, and Z. Zheng, "Who is Who on Ethereum? Account Labeling Using Heterophilic Graph Convolutional Network," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 54, no. 3, pp. 1541–1553, 2024, doi: 10.1109/TSMC.2023.3329520.

[15] J. R. Saura, S. Ribeiro-Navarrete, D. Palacios-Marqués, and A. Mardani, "Impact of extreme weather in production economics: Extracting evidence from user-generated content," *Int. J. Prod. Econ.*, vol. 260, 2023, doi: 10.1016/j.ijpe.2023.108861.

[16] R. V. Manjunath and N. Yashaswini Gowda, "Automated approach for skin lesion segmentation utilizing a hybrid deep learning algorithm," *Multimed. Tools Appl.*, vol. 83, no. 15, pp. 46017–46035, 2024, doi: 10.1007/s11042-023-16934-1.

[17] T. Li, W. Bai, Q. Liu, Y. Long, and C. L. P. Chen, "Distributed Fault-Tolerant Containment Control Protocols for the Discrete-Time Multiagent Systems via Reinforcement Learning Method," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 34, no. 8, pp. 3979–3991, 2023, doi: 10.1109/TNNLS.2021.3121403.

[18] A. Paya, S. Arroni, V. García-Díaz, and A. Gómez, "Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems," *Comput. Secur.*, vol. 136, 2024, doi: 10.1016/j.cose.2023.103546.

[19] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: deep learning model for IoT intrusion detection systems," *J. Supercomput.*, vol. 79, no. 12, pp. 13241–13261, 2023, doi: 10.1007/s11227-023-05197-0.

[20] P. Joshi, M. Hasanuzzaman, C. Thapa, H. Afli, and T. Scully, "Enabling All In-Edge Deep Learning: A Literature Review," *IEEE Access*, vol. 11, pp. 3431–3460, 2023, doi: 10.1109/ACCESS.2023.3234761.

[21] A. Algarni, T. Acarer, and Z. Ahmad, "An Edge Computing-Based Preventive Framework With Machine Learning- Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications," *IEEE Access*, vol. 12, pp. 53646–53663, 2024, doi: 10.1109/ACCESS.2024.3387529.

[22] M. Ehteshamuddin, K. Sheelvardhan, A. Kumar, S. Guglani, S. Roy, and A. Dasgupta, "Machine Learning-Assisted Multiobjective Optimization of Advanced Node Gate-All-Around Transistor for Logic and RF Applications," *IEEE Trans. Electron Devices*, vol. 71, no. 2, pp. 976–982, 2024, doi: 10.1109/TED.2023.3345288.

[23] J. Chen and J. Zhang, "Crude oil price shocks, volatility spillovers, and global systemic financial risk transmission mechanisms: Evidence from the stock and foreign exchange markets," *Resour. Policy*, vol. 85, 2023, doi: 10.1016/j.resourpol.2023.103875.

[24] Y. Nie, P. Sommella, M. Carratù, M. O'Nils, and J. Lundgren, "A Deep CNN Transformer Hybrid Model for Skin Lesion Classification of Dermoscopic Images Using Focal Loss," *Diagnostics*, vol. 13, no. 1, 2023, doi: 10.3390/diagnostics13010072.

[25] M. H. Javid, W. Jadoon, H. Ali, and M. D. Ali, "Design and Analysis of an Improved Deep Ensemble Learning Model for Melanoma Skin Cancer Classification," 2023. doi: 10.1109/ICACS55311.2023.10089716.

[26] C. Chen, C. Wang, B. Liu, C. He, L. Cong, and S. Wan, "Edge Intelligence Empowered Vehicle Detection and Image Segmentation for Autonomous Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 13023–13034, 2023, doi: 10.1109/TITS.2022.3232153.

[27] Z. Liu *et al.*, "PPRU: A Privacy-Preserving Reputation Updating Scheme for Cloud-Assisted Vehicular Networks," *IEEE Trans. Veh. Technol.*, vol. 74, no. 2, pp. 1877–1892, 2025, doi: 10.1109/TVT.2023.3340723.

[28] N. Tong, Y. Xu, J. Zhang, S. Gou, and M. Li, "Robust and efficient abdominal CT segmentation using shape constrained multi-scale attention network," *Phys. Medica*, vol. 110, 2023, doi: 10.1016/j.ejmp.2023.102595.

[29] I. Tomar, I. Sreedevi, and N. Pandey, "PLC and SCADA based Real Time Monitoring and Train Control System for the Metro Railways Infrastructure," *Wirel. Pers. Commun.*, vol. 129, no. 1, pp. 521–548, 2023, doi: 10.1007/s11277-022-10109-1.

[30] L. Adreani, P. Bellini, M. Fanfani, P. Nesi, and G. Pantaleo, "Smart City Digital Twin Framework for Real-Time Multi-Data Integration and Wide Public Distribution," *IEEE Access*, vol. 12, pp. 76277–76303, 2024, doi: 10.1109/ACCESS.2024.3406795.

[31] Y. Sugimura, H. Wakashima, Z. Liang, and R. Shibasaki, "Logistics strategy simulation of second-ranked ports on the basis of Japan's port reforms: a case study of Hakata Port," *Marit. Policy Manag.*, vol. 50, no. 6, pp. 707–723, 2023, doi: 10.1080/03088839.2022.2057610.

[32] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[33] E. Konstantopoulou, N. Sklavos, and I. Ognjanovic, "Securing Public Safety Mission-Critical 5G Communications of Smart Cities," 2024. doi: 10.1007/978-3-031-34601-9_4.

[34] C. Zhao, C. Wang, G. Hu, H. Chen, C. Liu, and J. Tang, "ISTVT: Interpretable Spatial-Temporal Video Transformer for Deepfake Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1335–1348, 2023, doi: 10.1109/TIFS.2023.3239223.

[35] J. Kaur, U. Garg, and G. Bathla, "Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review," *Artif. Intell. Rev.*, vol. 56, no. 11, pp. 12725–12769, 2023, doi: 10.1007/s10462-023-10433-3.

[36] P. Yan, W. Sun, X. Li, M. Li, Y. Jiang, and H. Luo, "PKDN: Prior Knowledge Distillation Network for bronchoscopy diagnosis," *Comput. Biol. Med.*, vol. 166, 2023, doi: 10.1016/j.compbiomed.2023.107486.

[37] M. Tian *et al.*, "Delineation of clinical target volume and organs at risk in cervical cancer radiotherapy by deep learning networks," *Med. Phys.*, vol. 50, no. 10, pp. 6354–6365, 2023, doi: 10.1002/mp.16468.

[38] A. Ali, B. A. S. Al-rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," *Sensors*, vol. 23, no. 15, 2023, doi: 10.3390/s23156762.

[39] N. Zad *et al.*, "Development of machine learning algorithms to estimate maximum residue limits for veterinary medicines," *Food Chem. Toxicol.*, vol. 179, 2023, doi: 10.1016/j.fct.2023.113920.

[40] H. Wu, H. Li, X. Luo, and S. Jiang, "Blockchain-Based Onsite Activity Management for Smart Construction Process Quality Traceability," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21554–21565, 2023, doi: 10.1109/JIOT.2023.3300076.

[41] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," 2023. doi: 10.47709/digitech.v3i2.3379.

[42] F. A. Proudlock *et al.*, "Extended optical treatment versus early patching with an intensive patching regimen in children with amblyopia in Europe (EuPatch): a multicentre, randomised controlled trial," *Lancet*, vol. 403, no. 10438, pp. 1766–1778, 2024, doi: 10.1016/S0140-6736(23)02893-3.

[43] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 280–308, 2023, doi: 10.1016/j.iotcps.2023.04.002.

[44] K. Kuru, "MetaOmniCity: Toward Immersive Urban Metaverse Cyberspaces Using Smart City Digital Twins," *IEEE Access*, vol. 11, pp. 43844–43868, 2023, doi: 10.1109/ACCESS.2023.3272890.

[45] X. Guo, D. Wang, J. Li, and H. Zhang, "Global research status and trends in orthopaedic surgical robotics: a bibliometric and visualisation analysis study," *J. Robot. Surg.*, vol. 17, no. 4, pp. 1743–1756, 2023, doi: 10.1007/s11701-023-01579-x.

[46] M. A. Habibi *et al.*, "Toward an Open, Intelligent, and End-to-End Architectural Framework for Network Slicing in 6G Communication Systems," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1615–1658, 2023, doi: 10.1109/OJCOMS.2023.3294445.

[47] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6695–6709, 2023, doi: 10.1109/JSYST.2023.3305757.

[48] H. Badihi, S. Jadidi, Z. Yu, Y. Zhang, and N. Lu, "Smart Cyber-Attack Diagnosis and Mitigation in a Wind Farm Network Operator," *IEEE Trans. Ind. Informatics*, vol. 19, no. 9, pp. 9468–9478, 2023, doi: 10.1109/TII.2022.3228686.

[49] M. Vijayan and V. S, "A Regression-Based Approach to Diabetic Retinopathy Diagnosis Using Efficientnet," *Diagnostics*, vol. 13, no. 4, 2023, doi: 10.3390/diagnostics13040774.

[50] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020713.

[51] M. A. Putratama, R. Rigo-Mariani, A. D. Mustika, V. Debusschere, A. Pachurka, and Y. Besanger, "A Three-Stage Strategy With Settlement for an Energy Community Management Under Grid Constraints," *IEEE Trans. Smart Grid*, vol. 14, no. 2, pp. 1505–1514, 2023, doi: 10.1109/TSG.2022.3167862.

[52] L. Zhu, C. Shen, X. Wang, H. Liang, H. Wang, and T. Tang, "A Learning Based Intelligent Train Regulation Method With Dynamic Prediction for the Metro Passenger Flow," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 4, pp. 3935–3948, 2023, doi: 10.1109/TITS.2022.3231838.

[53] J. Cai, W. Liang, X. Li, K. Li, Z. Gui, and M. K. Khan, "GTxChain: A Secure IoT Smart Blockchain Architecture Based on Graph Neural Network," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21502–21514, 2023, doi: 10.1109/JIOT.2023.3296469.

[54] E. Khodayari Moez *et al.*, "Circulating proteome for pulmonary nodule malignancy," *JNCI J. Natl. Cancer Inst.*, vol. 115, no. 9, pp. 1060–1070, 2023, doi: 10.1093/jnci/djad122.

[55] O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, and D. Z. Rodriguez, "Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN," *IEEE Access*, vol. 11, pp. 1023–1038, 2023, doi: 10.1109/ACCESS.2022.3233775.

[56] M. I. B. Ahmed *et al.*, "Personal Protective Equipment Detection: A Deep-Learning-Based Sustainable Approach," *Sustain.*, vol. 15, no. 18, 2023, doi: 10.3390/su151813990.

[57] F. Jiao *et al.*, "What can we learn when fitting a simple telegraph model to a complex gene expression model?," *PLoS Comput. Biol.*, vol. 20, no. 5, 2024, doi: 10.1371/journal.pcbi.1012118.

[58] W. J. Neumann, R. Gilron, S. Little, and G. Tinkhauser, "Adaptive Deep Brain Stimulation: From Experimental Evidence Toward Practical Implementation," 2023. doi: 10.1002/mds.29415.

[59] G. López-Millán, R. Marín-López, F. Pereñíguez-García, O. Canovas, and J. A. Parra Espín, "Analysis and practical validation of a standard SDN-based framework for IPsec management," *Comput. Stand. Interfaces*, vol. 83, 2023, doi: 10.1016/j.csi.2022.103665.

[60] A. Oseni *et al.*, "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 1000–1014, 2023, doi: 10.1109/TITS.2022.3188671.