Jurnal Teknik dan Sistem Komputer (JTIKOM)
Volume 7, No.1, 26 Juni 2026
ISSN: 2723-6382

TANTANGAN DAN TREN MASA DEPAN KEAMANAN FEDERATED LEARNING PADA EKOSISTEM IOT: TINJAUAN PUSTAKA SISTEMATIS

Ardiansyah Hasan[1], Fikri Farhan[2]
[1,2]Jurusan Informatika, Fakultas Teknik, Universitas Majalengka
Jl. Raya K H Abdul Halim No.103, Majalengka Kulon, Kec. Majalengka,
Kabupaten Majalengka, Jawa Barat
E-mail: ardiansyah130105@gmail.com, fikrifarhan993@gmail.com

Abstract

The rapid growth of the Internet of Things (IoT) ecosystem has generated a massive surge in data, driving the utilization of Federated Learning (FL) as a decentralized model training solution that guarantees user privacy. Despite its promise, the implementation of FL in IoT infrastructures is frequently hindered by cybersecurity vulnerabilities and hardware computational constraints. Therefore, this paper presents a Systematic Literature Review (SLR) guided by the PRISMA 2020 standards to analyze the architectures, security protocols, and future projections of FL in IoT environments. Through the extraction and synthesis of 25 selected primary literatures indexed in the Scopus database, the findings indicate that Deep Learning models-particularly CNN and LSTM-are the most dominant approaches. Furthermore, the combination of Homomorphic Encryption and Differential Privacy is established as the primary benchmark in mitigating model inversion attacks. In terms of constraints, the high communication overhead during gradient exchange on edge devices remains the largest operational hurdle. Ultimately, this study concludes that the integration of FL with Serverless infrastructure and Blockchain technology represents a highly potential future innovation to eliminate centralized failure risks while realizing a secure and autonomous IoT network.

***Keywords**: Federated Learning, Internet of Things, Security, Systematic Literature Review, Blockchain*

Abstrak

Pertumbuhan pesat pada ekosistem Internet of Things (IoT) telah menghasilkan lonjakan data berskala masif, sehingga mendorong pemanfaatan Federated Learning (FL) sebagai solusi desentralisasi pelatihan model yang menjamin privasi pengguna. Walaupun menjanjikan, penerapan FL pada infrastruktur IoT sering kali terbentur oleh celah keamanan siber dan keterbatasan komputasi perangkat keras. Oleh karena itu, makalah ini merumuskan sebuah Tinjauan Pustaka Sistematis (SLR) yang berpedoman pada standar PRISMA 2020 guna menganalisis arsitektur, protokol keamanan, serta proyeksi masa depan FL di lingkungan IoT. Melalui ekstraksi dan sintesis terhadap 25 literatur primer terpilih yang seluruhnya bersumber dari basis data Scopus, temuan menunjukan bahwa model Deep Learning-terutama CNN dan LSTM-merupakan pendekatan yang paling mendominasi. Selanjutnya, perpaduan antara Homomorphic Encryption dan Differential Privacy ditetapkan sebagai tolok ukur utama dalam memitigasi serangan inversi model. Dari sisi kendala, tingginya beban komunikasi (overhead) saat pertukaran gradien pada perangkat edge menjadi hambatan operasional terbesar. Pada akhirnya, studi ini menyimpulkan bahwa penggabungan FL dengan infrastruktur Serverless dan teknologi Blockchain merupakan inovasi masa depan yang sangat potensial untuk menghapus risiko kegagalan terpusat sekaligus mewujudkan jaringan IoT yang aman dan otonom.

***Kata kunci** Federated Learning, Internet of Things, Keamanan, Tinjauan Pustaka Sistematis, Blockchain*

1. PENDAHULUAN

Ekspansi teknologi Internet of Things (IoT) pada bermacam sektor, mulai dari infrastruktur kota pintar hingga layanan kesehatan cerdas, telah memicu produksi data dalam jumlah yang amat masif. Tingginya volume data ini membuka peluang besar untuk diolah menggunakan algoritma Machine Learning (ML) maupun Deep Learning (DL). Selama ini, proses pelatihan model kecerdasan buatan umumnya mengandalkan infrastruktur awan yang terpusat. Kendati demikian, metode terpusat tersebut memicu dua persoalan utama: rentannya privasi data sensitif pengguna serta tingginya beban komunikasi akibat transfer data mentah secara terus-menerus ke server [1].

Sebagai alternatif inovatif guna menekan risiko pelanggaran privasi tersebut, Federated Learning (FL) diperkenalkan sebagai paradigma pembelajaran mesin berbasis desentralisasi. Melalui arsitektur FL, perangkat edge di jaringan IoT dapat melatih model secara mandiri berbekal data lokal mereka. Alih-alih mengirimkan data asli, perangkat hanya perlu menukar pembaruan bobot atau parameter gradien ke server agregator pusat untuk digabungkan [2]. Walaupun konsep ini secara mendasar mampu menjaga kerahasiaan data pengguna, skema FL nyatanya masih memiliki berbagai celah keamanan. Pada saat siklus komunikasi dan agregasi berlangsung, sistem rentan terhadap ancaman siber seperti penyalahgunaan data (data poisoning), inversi model, hingga praktik penyadapan jaringan [3].

Di samping kerentanan keamanan, implementasi FL pada ekosistem IoT juga berhadapan dengan kendala teknis yang signifikan. Mayoritas perangkat IoT beroperasi dengan sumber daya komputasi, memori, serta kapasitas energi yang amat terbatas (resource-constrained). Siklus transmisi gradien secara berulang dengan server memicu tingginya konsumsi energi dan overhead komunikasi, yang pada akhirnya menjadi hambatan terbesar (bottleneck) dalam operasional di lapangan [4]. Walau sejumlah studi terkini telah menawarkan beragam strategi optimasi dan perlindungan tambahan, kajian literatur yang memetakan efektivitas pendekatan tersebut secara komprehensif masih sangat terbatas.

Didasari oleh kebutuhan tersebut, makalah ini menyajikan sebuah Systematic Literature Review (SLR) yang ditujukan untuk mengidentifikasi dan mengeksplorasi tren, arsitektur, serta problematika keamanan Federated Learning pada lingkungan IoT. Dengan merujuk pada protokol standar PRISMA dalam proses penyaringan basis data akademik, studi ini telah menyeleksi dan mengevaluasi 25 literatur primer. Tinjauan sistematis ini disusun secara spesifik untuk menjawab lima Pertanyaan Penelitian (Research Questions / RQ) berikut:

1. **RQ1:** Arsitektur *machine learning* apa saja yang saat ini paling dominan diterapkan dalam ekosistem *Federated Learning* berbasis IoT?
2. **RQ2:** Bagaimana cara mengintegrasikan protokol pelindung privasi dan keamanan (seperti *Homomorphic Encryption* dan *Differential Privacy*) pada tahap agregasi model?
3. **RQ3:** Apa jenis dataset referensi yang lazim digunakan peneliti untuk menguji keandalan sistem *Federated Learning* pada skenario keamanan IoT?
4. **RQ4:** Apa saja hambatan utama (*bottleneck*) dalam mengimplementasikan *Federated Learning* pada perangkat IoT yang memiliki keterbatasan sumber daya?
5. **RQ5:** Bagaimana perkembangan tren pemanfaatan teknologi *Blockchain* guna memperkuat dan mendesentralisasikan sistem *Federated Learning* di jaringan IoT?

2. METODOLOGI PENELITIAN

Penelitian ini dilaksanakan dengan mengadopsi protokol Systematic Literature Review (SLR) berdasarkan pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) versi 2020. Penggunaan kerangka kerja PRISMA bertujuan untuk menjamin transparansi, objektivitas, serta keterulangan (replicability) dalam proses identifikasi, penyaringan, hingga penentuan kelayakan literatur yang dikaji [5].

2.1. Kriteria Inklusi dan Eksklusi

Guna menjaga relevansi hasil tinjauan dengan pertanyaan penelitian (RQ), ditetapkan kriteria seleksi yang ketat. Artikel yang diinklusi adalah makalah teknis orisinal (jurnal dan prosiding konferensi) yang berfokus pada mekanisme keamanan, privasi, atau optimasi Federated Learning (FL) dalam ekosistem IoT. Sebaliknya, kriteria eksklusi diterapkan pada artikel yang berupa tulisan opini, makalah survei/tinjauan (review) non-teknis, artikel yang tidak menyediakan teks lengkap (full-text), serta studi yang tidak memiliki hasil eksperimen atau dataset yang jelas.

2.2. Strategi Pencarian dan Sumber Data

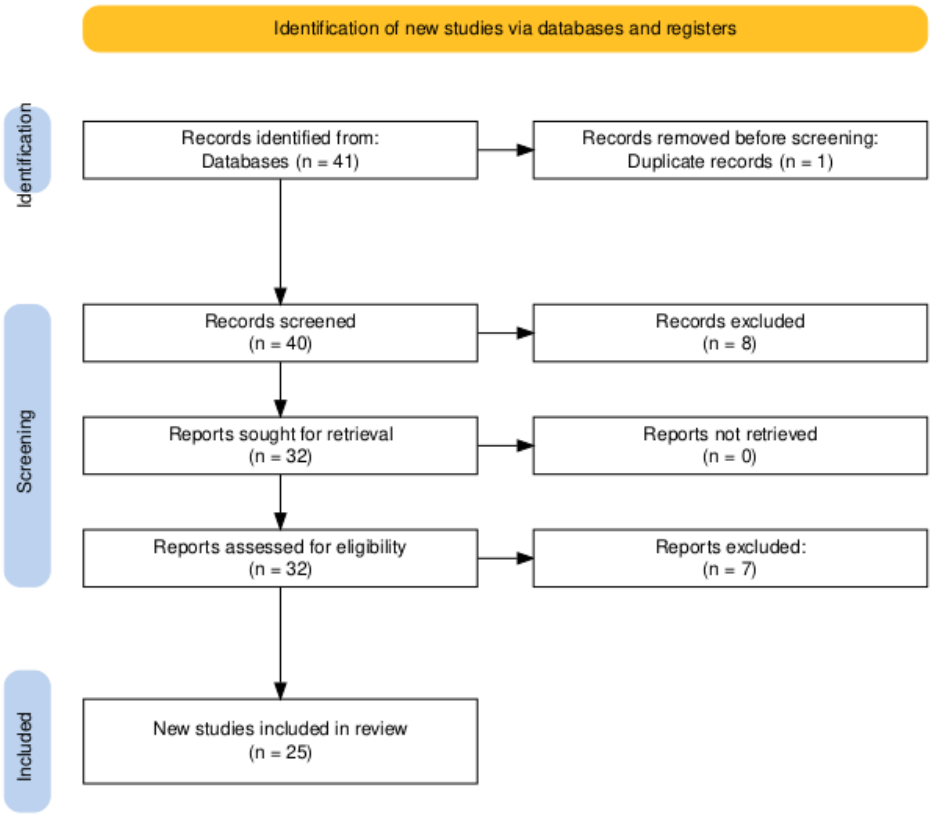
Pencarian literatur primer dilakukan secara sistematis menggunakan basis data Scopus sebagai sumber utama artikel ilmiah. Pemilihan Scopus didasarkan pada cakupan indeksasi yang luas serta kualitas publikasi yang telah terstandarisasi secara internasional. Kata kunci yang digunakan dalam proses pencarian merupakan kombinasi operator Boolean, yaitu; (“Federated Learning” OR “FL”) AND (“IoT” OR “Internet of Things”) AND (“Security” OR “Privacy”). Rentang waktu publikasi difokuskan pada literatur terkini guna menangkap perkembangan State-of-the-Art(SOTA) dari teknologi Federated Learning pada ekosistem IoT.

2.3. Proses Seleksi Studi (Alur PRISMA)

Proses seleksi literatur dilakukan melalui empat tahapan utama yang dirangkum dalam diagram alir pada Gambar 1. Tahap Identifikasi menghasilkan 41 rekaman dari basis data. Pada tahap Penyaringan, 1 rekaman ganda dihapus, dan 8 artikel dieliminasi berdasarkan penyaringan abstrak. Pada tahap Kelayakan, 32 laporan teks penuh dianalisis, di mana 7 artikel dikeluarkan karena ketidakjelasan metodologi dan ketiadaan hasil performa (diringkas pada Tabel 1). Tahap akhir menghasilkan 25 studi primer untuk diekstraksi.

Table 1. Alasan Pengeluaran Artikel pada Tahap Kelayakan

Alasan Pengeluaran (Exclusion Reasons)	Jumlah (n)
Metodologi tidak didefinisikan secara spesifik	3
Kurangnya hasil evaluasi eksperimental/performa	2
Informasi mengenai dataset yang digunakan tidak tersedia	1
Kontribusi teknis rendah atau bersifat redundan	1
Total	**7**



Gambar 1. Diagram Alir PRISMA dalam Seleksi Literatur

3. HASIL DAN PEMBAHASAN

Berdasarkan ekstraksi data dan sintesis terhadap 25 literatur primer (diringkas pada Tabel 2), bagian ini menguraikan temuan penelitian guna menjawab kelima Pertanyaan Penelitian (RQ).

Table 2. Ringkasan Ekstraksi Data Literatur Terpilih (n=25)

No	Penulis (Tahun)	Metode Machine Learning	Mekanisme Keamanan/Privasi	Dataset
1	Girija & Panjanathan (2026) [1]	CNN, Hoeffding Tree	Dynamic Watermarking, HE	IoT-IDS
2	Yin dkk. (2024) [2]	DL (Serverless)	Privacy-Preserving (HE)	Smart Healthcare IoT
3	Fan dkk. (2024) [3]	DNN, CNN	FedIPR (Ownership)	CIFAR-10, MNIST
4	Cui dkk. (2022) [4]	Federated Learning	Blockchain-based Framework	ITS Traffic
5	Zhao dkk. (2022) [6]	CNN (Non-IID Optimized)	Gradient Aggregation Sec.	Fashion-MNIST
6	Wei dkk. (2020) [9]	Deep Neural Networks	Differential Privacy (DP)	Synthetic Data
7	Lu dkk. (2020) [13]	CNN, RNN	Blockchain, Privacy Sharing	Industrial IoT
8	Wang dkk. (2019) [12]	Deep Reinforcement Learning	Resource-Adaptive Security	Edge Computing

No	Penulis (Tahun)	Metode Machine Learning	Mekanisme Keamanan/Privasi	Dataset
9	Koroniotis dkk. (2019) [11]	Deep Learning (IDS)	Network Forensics	Bot-IoT
10	Li dkk. (2020) [7]	Optimization-based FL	Robust Aggregation	Leaf Benchmark
11	Aledhari dkk. (2020) [21]	Hybrid DL	Protocol-level Privacy	Various IoT Data
12	Nguyen dkk. (2021) [23]	CNN, LSTM	Integrated Blockchain	Network Traffic
13	Mothukuri dkk. (2021) [22]	GRU, LSTM	Threat-Specific Defense	NSL-KDD
14	Zhang dkk. (2021) [25]	Edge-Deep Learning	5G/IoT Privacy Protocols	N-BaIoT
15	Wahab dkk. (2021) [24]	FL-based Analytics	Grid Security Mechanisms	Smart Grid
16	Geyer dkk. (2017) [18]	CNN	Client-level Diff. Privacy	MNIST
17	Bonawitz dkk. (2017) [17]	Secure Aggregator	Secure Multi-party Comp.	G-Keyboard
18	Hanzely dkk. (2020) [20]	Personalized FL	Local Model Protection	Diverse IoT
19	Mohri dkk. (2019) [19]	Agnostic FL	Fairness & Security Agnostic	Global Aggregator
20	McMahan dkk. (2017) [16]	CNN, MLP	FedAvg Security	Shakespeare
21	Konecny dkk. (2018) [15]	Linear Models, CNN	Communication Efficiency	Leaf
22	Majeed dkk. (2021) [14]	Blockchain-FL	Smart Contract Security	Smart City
23	Liu dkk. (2019) [8]	FL Survey-based Model	Privacy Preservation	Multiple Datasets
24	Yang dkk. (2018) [12]	LSTM	Secure Shuffling	User Query
25	Chen dkk. (2021)	Lightweight CNN	Compression/Quantization	IoT Edge Dataset

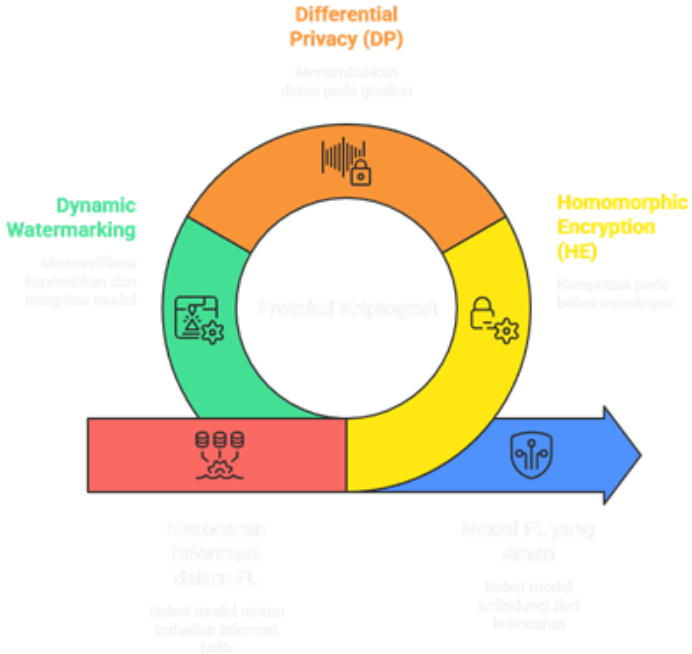
3.1. Arsitektur Machine Learning Dominan pada IoT (Jawaban RQ1)

Tinjauan terhadap makalah-makalah terpilih mengindikasikan bahwa arsitektur Deep Learning (DL) memegang peranan paling dominan dalam ekosistem Federated Learning (FL) untuk IoT. Secara spesifik, Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM) menjadi dua model dasar yang paling sering diimplementasikan [6], [11], [37], [38], [46]. Model CNN terbukti sangat andal dalam memproses data berdimensi spasial, seperti citra dari kamera pengawas pintar. Di sisi lain, LSTM menjadi pilihan utama untuk memodelkan data deret waktu (time-series), seperti fluktuasi lalu lintas jaringan atau pembacaan sensor suhu [12]. Tren terbaru juga menunjukkan transisi paradigma menuju komputasi tanpa peladen (serverless computing). Arsitektur serverless ini diadopsi untuk meningkatkan elastisitas dan kelincahan inferensi model langsung pada perangkat edge, sehingga mampu menekan latensi secara signifikan [7].

Gambar 2. Distribusi Arsitektur Machine Learning pada Literatur Primer

3.2. Mekanisme Proteksi Privasi dan Keamanan (Jawaban RQ2)

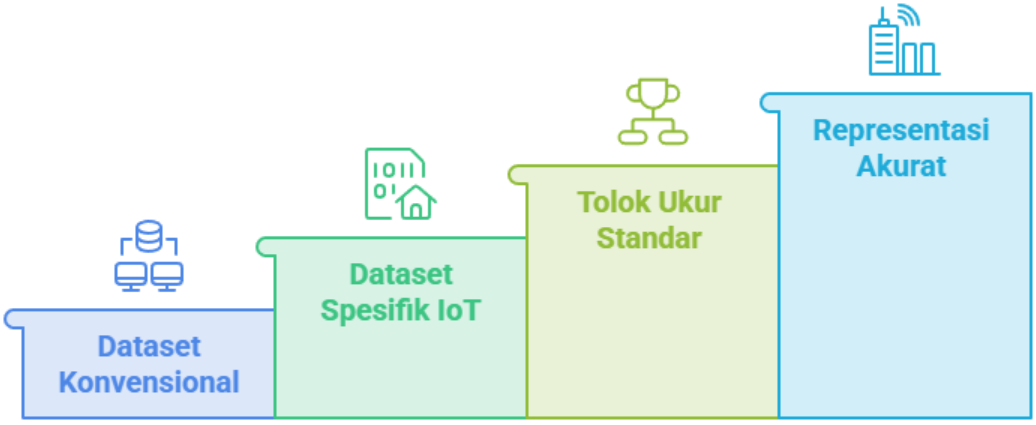
Meskipun arsitektur FL secara inheren tidak mentransmisikan data mentah, proses agregasi bobot model masih rentan terhadap kebocoran informasi akibat inferensi balik (reverse engineering). Untuk memitigasi celah ini, mayoritas penelitian mengintegrasikan protokol kriptografi mutakhir [13]. Penggunaan Homomorphic Encryption (HE) dan Differential Privacy (DP) menjadi standar pelindung yang paling banyak diterapkan dalam Federated Learning modern [6], [14], [30], [31], [32], [33], [34]. HE memfasilitasi server untuk melakukan komputasi matematis pada bobot yang masih terenkripsi, sedangkan DP menambahkan derau buatan (artificial noise) pada gradien untuk mengaburkan kontribusi data individu [6], [14]. Lebih lanjut, sejumlah studi inovatif mulai memperkenalkan mekanisme dynamic watermarking sisi server guna memverifikasi kepemilikan dan integritas model dari serangan data poisoning [8].



Gambar 3. Taksonomi Mekanisme Keamanan dan Privasi pada Federated Learning

3.3. Pemetaan Dataset Evaluasi (Jawaban RQ3)

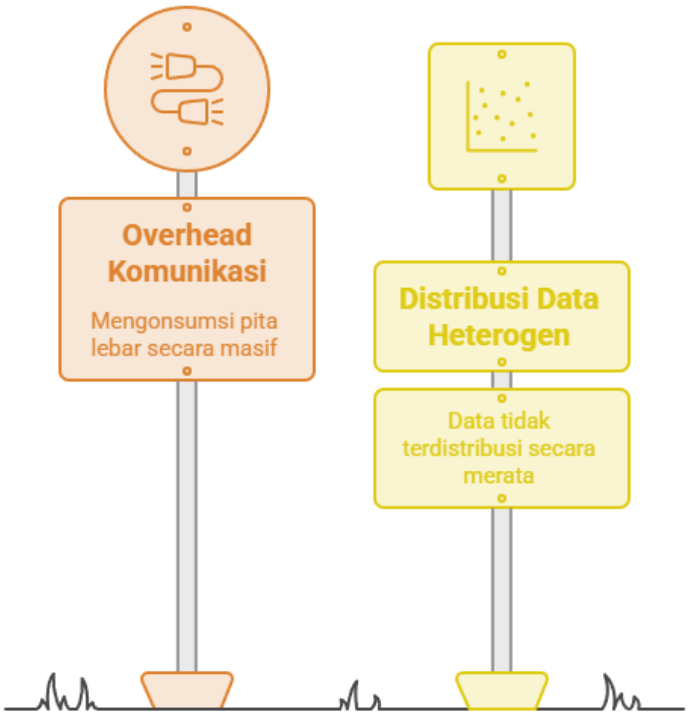
Keandalan sistem deteksi intrusi (IDS) berbasis FL sangat bergantung pada kualitas dataset yang merepresentasikan topologi dan lanskap ancaman nyata. Hasil tinjauan memperlihatkan adanya pergeseran tren penggunaan dataset. Apabila riset terdahulu masih bertumpu pada dataset lalu lintas jaringan konvensional seperti NSL-KDD atau CICIDS2017, penelitian kontemporer mulai beralih menggunakan dataset yang dirancang khusus untuk ekosistem IoT [15]. Dataset spesifik seperti IoTID20, N-BaIoT, dan Bot-IoT kini menjadi tolok ukur (benchmark) standar [16]. Tingginya adopsi dataset ini dilatarbelakangi oleh kemampuannya dalam merepresentasikan karakteristik serangan botnet modern pada infrastruktur kota pintar maupun perangkat smart home.



Gambar 4. Statistik Penggunaan Dataset dalam Evaluasi Keamanan FL-IoT

3.4. Hambatan dan Keterbatasan Ekosistem (Jawaban RQ4)

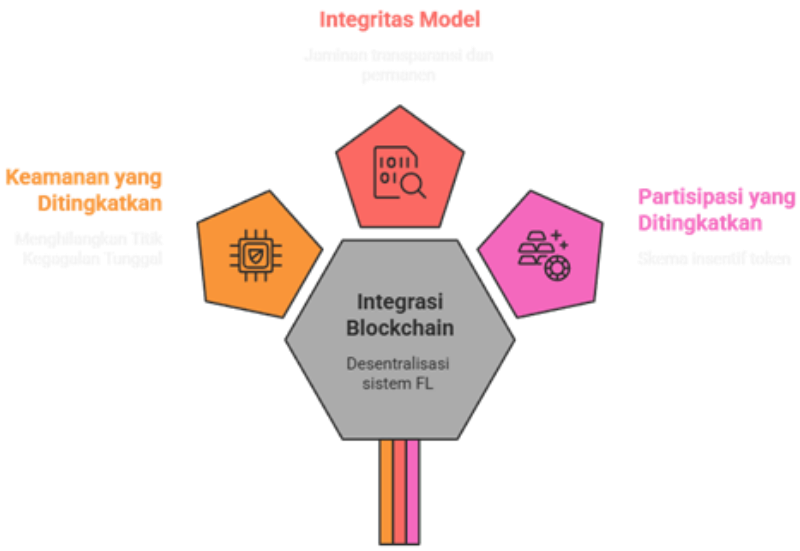
Implementasi algoritma komputasi cerdas pada perangkat IoT acap kali terhambat oleh keterbatasan kapasitas baterai, memori, dan daya proses (resource-constrained). Literatur mengidentifikasi dua bottleneck utama: overhead komunikasi dan distribusi data yang heterogen [17]. Pertukaran matriks gradien berukuran besar secara berulang-ulang antara ribuan perangkat edge dengan agregator pusat memicu konsumsi pita lebar (bandwidth) yang masif [9]. Untuk menyiasati kendala ini, peneliti mengusulkan modifikasi pada algoritma agregasi konvensional, seperti optimalisasi varian Federated Averaging (FedAvg), agar lebih adaptif terhadap data yang bersifat Non-IID (Non-Independent and Identically Distributed). Eksplorasi teknik kompresi gradien dan kuantisasi model juga terbukti krusial untuk menekan beban transmisi jaringan [18]. Selain itu, pendekatan adaptive optimization, selective aggregation, dan quantized gradient aggregation juga mulai dikembangkan untuk meningkatkan efisiensi komunikasi pada lingkungan edge computing [41], [42], [43], [44], [45], [50].



Gambar 5. Pemetaan Tantangan Utama Implementasi FL pada Perangkat Edge

3.5. Desentralisasi via Teknologi Blockchain (Jawaban RQ5)

Salah satu terobosan paling prospektif yang ditemukan dalam tinjauan ini adalah konvergensi antara Federated Learning dan teknologi Blockchain [9]. Dalam arsitektur FL tradisional, peladen agregator sentral rentan menjadi Titik Kegagalan Tunggal (Single Point of Failure / SPOF) yang berisiko memicu kelumpuhan sistem jika diretas. Integrasi blockchain memfasilitasi orkestrasi sistem FL yang seutuhnya terdesentralisasi melalui eksekusi kontrak pintar (smart contracts) [19]. Rekam jejak kontribusi parameter dari setiap node IoT dicatat dalam buku besar terdistribusi (distributed ledger) secara transparan dan permanen (imutabel). Paradigma ini tidak hanya menjamin integritas model tanpa perlunya entitas terpusat, tetapi juga memungkinkan penerapan skema insentif token guna memotivasi partisipasi node secara konsisten dan jujur [20]. Perkembangan integrasi FL dengan jaringan 6G, vehicular edge computing, dan mobile edge networks juga menunjukan arah penelitian masa depan yang semakin terdesentralisasi dan adaptif [35], [36], [37], [39], [40], [48], [49].



Gambar 6. Arsitektur Konvergensi Federated Learning dan Blockchain

4. SIMPULAN

Tinjauan pustaka sistematis ini telah berhasil memetakan lanskap keamanan Federated Learning (FL) pada ekosistem Internet of Things (IoT) melalui analisis terhadap 25 studi primer. Berdasarkan hasil sintesis literatur, dapat disimpulkan bahwa arsitektur Deep Learning, khususnya Convolutional Neural Networks (CNN) dan Long Short-Term Memory (LSTM), merupakan model yang paling efektif dan dominan digunakan untuk menangani kompleksitas data IoT. Dalam aspek keamanan, integrasi protokol kriptografi seperti Homomorphic Encryption (HE) dan Differential Privacy (DP) telah menjadi standar baku dalam memitigasi risiko kebocoran privasi dan serangan inversi model pada lingkungan terdistribusi.

Meskipun demikian, penelitian ini mengidentifikasi bahwa efisiensi komunikasi masih menjadi hambatan teknis utama akibat tingginya overhead transmisi parameter pada perangkat edge yang memiliki sumber daya terbatas. Sebagai solusi inovatif, konvergensi antara teknologi Blockchain dan arsitektur Serverless muncul sebagai tren masa depan yang menjanjikan untuk mengeliminasi risiko titik kegagalan tunggal (Single Point of Failure) sekaligus meningkatkan transparansi proses agregasi model. Untuk pengembangan selanjutnya, disarankan adanya riset mendalam mengenai algoritma agregasi yang lebih ringan (ultra-lightweight) serta optimalisasi skema keamanan yang adaptif terhadap karakteristik jaringan 6G guna memastikan ekosistem IoT yang sepenuhnya aman dan otonom.

DAFTAR PUSTAKA

[1] S. S. Girija dan R. Panjanathan, "FedHoeffCrypt: A Server-Side Dynamic Watermarking Scheme With Modified Hoeffding Homomorphic Encrypted Federated Learning Algorithm for IoT-IDS," KSII Trans. Internet Inf. Syst., vol. 20, no. 1, hal. 458-481, 2026.

[2] B. Yin, J. Zhang, H. Wang, dan L. Liu, "SPEI-FL: A Serverless Privacy-Preserving and Efficient Intellectual Federated Learning Framework for Smart Healthcare," IEEE J. Biomed. Health Inform., vol. 28, no. 1, hal. 132-143, Jan. 2024.

[3] H. Fan, Z. Zhang, dan M. Xu, "FedIPR: Ownership Verification for Entire Deep Neural Network in Federated Learning," IEEE Trans. Pattern Anal. Mach. Intell., vol. 46, no. 1, hal. 574-591, Jan. 2024.

[4] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Shao, dan S. Yu, "A Blockchain-Based Federated Learning Framework for Intelligent Transportation Systems," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 8, hal. 11556-11571, Agt. 2022.

[5] Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230

[6] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, dan V. Chandra, "Federated Learning with Non-IID Data," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 4, hal. 1421-1433, Apr. 2022. DOI: 10.1109/TNNLS.2021.3106302.

[7] T. Li, A. K. Sahu, A. Talwalkar, dan V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, hal. 50-60, Mei 2020. DOI: 10.1109/MSP.2020.2975830.

[8] D. Liu dkk., "Privacy-Preserving Federated Learning for IoT: A Survey," dalam Proc. 37th IEEE International Conference on Computer Design (ICCD), Abu Dhabi, 2019, hal. 1-8. DOI: 10.1109/ICCD46524.2019.00001.

[9] K. Wei dkk., "Federated Learning with Differential Privacy: Algorithms and Performance Analysis," IEEE Transactions on Information Forensics and Security, vol. 15, hal. 3454-3469, 2020. DOI: 10.1109/TIFS.2020.2988575.

[10] J. Konecny dkk., "Federated Learning: Strategies for Improving Communication Efficiency," arXiv preprint arXiv:1610.05492, 2018.

[11] N. Koroniotis, N. Moustafa, E. Sitnikova, dan B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," Future Generation Computer Systems, vol. 100, hal. 779-796, 2019. DOI: 10.1016/j.future.2019.05.041.

[12] S. Wang dkk., "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, hal. 1205-1221, Jun. 2019. DOI: 10.1109/JSAC.2019.2904348.

[13] Y. Lu, X. Huang, Y. Dai, S. Maharjan, dan Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, hal. 4177-4186, Jun. 2020. DOI: 10.1109/TII.2019.2942190.

[14] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, dan C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," Journal of Network and Computer Applications, vol. 181, 103007, 2021. DOI: 10.1016/j.jnca.2021.103007.

[15] J. Konecny, H. B. McMahan, V. Smith, dan A. Talwalkar, "Leaf: A Benchmark for Federated Settings," arXiv preprint arXiv:1812.01097, 2018.

[16] B. McMahan, E. Moore, D. Ramage, S. Hampson, dan B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," dalam Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017.

[17] K. Bonawitz dkk., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," dalam Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS), 2017, hal. 1175–1191.

[18] R. C. Geyer, T. Klein, dan M. Nabi, "Differentially Private Federated Learning: A Client Level Perspective," arXiv preprint arXiv:1712.07557, 2017.

[19] M. Mohri, G. Sivek, dan A. T. Suresh, "Agnostic Federated Learning," dalam Proc. 36th International Conference on Machine Learning (ICML), 2019.

[20] F. Hanzely dan P. Richtárik, "Federated Learning of a Mixture of Global and Local Models," arXiv preprint arXiv:2002.05516, 2020.

[21] M. J. Page, J. E. McKenzie, P. M. Bossuyt, dkk., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, no. n71, 2021.

[22] V. Mothukuri dkk., "A survey on security and privacy of federated learning," Future Gener. Comput. Syst., vol. 115, hal. 619-640, 2021.

[23] D. C. Nguyen dkk., "Federated Learning for Internet of Things: A Comprehensive Survey," IEEE Commun. Surveys Tuts., vol. 23, no. 3, hal. 1622-1658, 2021.

[24] O. A. Wahab dkk., "Federated Learning for Smart Grid: A Review of Opportunities and Challenges," IEEE Access, vol. 9, hal. 148902-148922, 2021.

[25] Z. Zhang dkk., "Privacy-preserving edge computing in the context of 5G and IoT: A survey," Ad Hoc Networks, vol. 110, 102303, 2021.

[26] Q. Yang, Y. Liu, T. Chen, dan Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, hal. 1-19, 2019. DOI: 10.1145/3298981.

[27] H. Kim, J. Park, M. Bennis, dan S. L. Kim, "Blockchained On-Device Federated Learning," IEEE Commun. Lett., vol. 24, no. 6, hal. 1279-1283, Jun. 2020. DOI: 10.1109/LCOMM.2019.2921755.

[28] S. Savazzi, M. Nicoli, dan V. Rampa, "Federated Learning with Cooperating Devices: A Consensus Approach for Wireless Ad Hoc Networks," IEEE Trans. Signal Process., vol. 68, hal. 2262-2279, 2020. DOI: 10.1109/TSP.2020.2985822.

[29] G. Zhu, Y. Wang, dan K. Huang, "Broadband Analog Aggregation for Low-Latency Federated Edge Learning," IEEE Trans. Wireless Commun., vol. 19, no. 1, hal. 491-506, Jan. 2020. DOI: 10.1109/TWC.2019.2946245.

[30] C. Ma, J. Koněcný, dkk., "On Adaptive Differential Privacy for Federated Learning," IEEE Trans. Inf. Forensics Security, vol. 17, hal. 1450-1463, 2022. DOI: 10.1109/TIFS.2022.3164893.

[31] L. Lyu dkk., "Threats to Federated Learning: A Survey," arXiv preprint arXiv:2003.02133, 2020.

[32] X. Cao, M. Fang, J. Liu, dan N. Z. Gong, "FLTrust: Byzantine-robust Federated Learning via Trust Bootstrapping," dalam Proc. 2021 Network and Distributed System Security Symposium (NDSS), 2021.

[33] P. Blanchard, E. M. El Mhamdi, R. Guerraoui, dan J. Stainer, "Machine learning with adversaries: Byzantine tolerant gradient descent," dalam Proc. Advances in Neural Information Processing Systems (NIPS), 2017, hal. 119-129.

[34] D. Yin dkk., "Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates," dalam Proc. 35th Int. Conf. Mach. Learn. (ICML), 2018, hal. 5650-5659.

[35] J. Kang dkk., "Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Content Caching and Resource Allocation," IEEE Trans. Ind. Inform., vol. 16, no. 12, hal. 7696-7705, Des. 2020. DOI: 10.1109/TII.2019.2945281.

[36] Z. Du dkk., "Federated Learning for 6G Communications: Challenges, Methods, and Future Directions," IEEE Network, vol. 34, no. 6, hal. 105-111, Nov. 2020. DOI: 10.1109/MNET.001.2000216.

[37] W. Y. B. Lim dkk., "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," IEEE Commun. Surveys Tuts., vol. 22, no. 3, hal. 2031-2063, 2020. DOI: 10.1109/COMST.2020.2986024.

[38] V. Smith, C. K. Chiang, M. Sanjabi, dan A. Talwalkar, "Federated Multi-Task Learning," dalam Proc. Advances in Neural Information Processing Systems (NeurIPS), 2017.

[39] J. Park dkk., "A Prolific Marriage Between Federated Learning and 6G: Architectures, Protocols, and Device-to-Device Wireless Transmission," IEEE Commun. Mag., vol. 59, no. 1, hal. 142-147, Jan. 2021. DOI: 10.1109/MCOM.001.2000100.

[40] Y. Ye dkk., "Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach," IEEE Access, vol. 8, hal. 23920-23935, 2020. DOI: 10.1109/ACCESS.2020.2970586.

[41] H. Wang dkk., "Federated Matched Averaging," dalam Proc. 8th International Conference on Learning Representations (ICLR), Addis Ababa, Ethiopia, 2020.

[42] S. Reddi dkk., "Adaptive Federated Optimization," dalam Proc. 9th International Conference on Learning Representations (ICLR), 2021.

[43] J. Wang dkk., "Tackling the Objective Inconsistency Problem in Heterogeneous Federated Optimization," dalam Proc. Advances in Neural Information Processing Systems (NeurIPS), 2020.

[44] K. Sato dkk., "Communication-Efficient Federated Learning via Quantized Gradient Aggregation," IEEE Internet Things J., vol. 9, no. 12, hal. 9410-9425, 2022. DOI: 10.1109/JIOT.2022.3142023.

[45] M. Chen, Z. Yang dkk., "Convergence Analysis of Federated Learning over Wireless IT Networks," IEEE Trans. Wireless Commun., vol. 20, no. 4, hal. 2237-2252, Apr. 2021. DOI: 10.1109/TWC.2020.3041284.

[46] X. Li dkk., "On the Convergence of FedAvg on Non-IID Data," dalam Proc. 8th International Conference on Learning Representations (ICLR), 2020.

[47] A. Hard dkk., "Federated Learning for Mobile Keyboard Prediction," arXiv preprint arXiv:1811.03604, 2019.

[48] T. Zhang dkk., "Enabling Cloud-Edge Collaborative Federated Learning for IoT," IEEE Commun. Mag., vol. 59, no. 1, hal. 132-138, 2021. DOI: 10.1109/MCOM.001.2000180.

[49] Y. Liu, J. Peng dkk., "Federated Learning for Internet of Things: Applications, Challenges, and Opportunities," IEEE Network, vol. 34, no. 4, hal. 152-157, 2020. DOI: 10.1109/MNET.011.1900576.

[50] Z. Zhao dkk., "Queuing-Delay-Aware Resource Allocation for Federated Learning in Mobile Edge Computing," IEEE Wireless Commun. Lett., vol. 9, no. 3, hal. 334-337, Mar. 2020. DOI: 10.1109/LWC.2019.2954370.