JURNAL UNGGUL TEKNOLOGI DAN INFORMATIKA (JUTIKA) ISSN: 3124-6591
Vol. 2, No. 1, Juni 2026, hlm. 18-27

Perkembangan Federated Learning dalam Menjaga Privasi Data: Kajian Literatur Sistematis

Abdul Rahman Yusup

Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
e-mail: aabcrd6@gmail.com

Diterima: 22 Mei 2026 | Direvisi: 30 Mei 2026 | Diterima: 25 Juni 2026

Abstrak

Perkembangan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) telah meningkatkan kebutuhan terhadap data dalam jumlah besar untuk menghasilkan model yang akurat. Pendekatan *centralized machine learning* yang selama ini banyak digunakan menghadapi berbagai tantangan, terutama terkait perlindungan privasi, keamanan data, dan kepatuhan terhadap regulasi perlindungan data pribadi. Sebagai alternatif, *Federated Learning* berkembang sebagai paradigma pembelajaran terdistribusi yang memungkinkan pelatihan model dilakukan pada perangkat lokal tanpa memindahkan data mentah ke server pusat. Penelitian ini bertujuan untuk menganalisis perkembangan Federated Learning, mengkaji perannya dalam menjaga privasi dan keamanan data, mengidentifikasi berbagai tantangan implementasi, serta merumuskan arah pengembangan penelitian di masa depan. Penelitian menggunakan metode *Systematic Literature Review* (SLR) dengan mengacu pada pedoman *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) 2020. Literatur diperoleh dari berbagai basis data ilmiah bereputasi dan dianalisis menggunakan *thematic analysis* melalui proses identifikasi, seleksi, sintesis, dan interpretasi temuan penelitian. Hasil kajian menunjukkan bahwa Federated Learning telah berkembang menjadi salah satu pendekatan utama dalam *privacy-preserving artificial intelligence* melalui mekanisme pelatihan terdistribusi, *secure aggregation*, *differential privacy*, dan *homomorphic encryption*. Meskipun demikian, implementasinya masih menghadapi tantangan berupa heterogenitas data, *communication overhead*, keterbatasan sumber daya perangkat, ancaman keamanan model, dan kebutuhan standarisasi tata kelola. Penelitian ini menegaskan bahwa Federated Learning memiliki prospek yang besar dalam mendukung pengembangan sistem AI yang aman, efisien, dan berorientasi pada perlindungan privasi data.

Kata Kunci: *Federated Learning; Data Privacy; Privacy-Preserving Machine Learning; Artificial Intelligence; Systematic Literature Review*

Abstract

The rapid advancement of Artificial Intelligence *(AI) and* Machine Learning *(ML) has significantly increased the demand for large-scale data to develop highly accurate predictive models. However, the conventional* centralized machine learning *approach raises critical concerns regarding data privacy, security, and compliance with personal data protection regulations. As an alternative,* Federated Learning *has emerged as a distributed learning paradigm that enables model training on local devices without transferring raw data to a central server. This study aims to analyze the development of Federated Learning, examine its role in preserving data privacy and security, identify its implementation challenges, and propose future research directions. The research employed a* Systematic Literature Review *(SLR) based on the* Preferred Reporting Items for Systematic Reviews and Meta-Analyses *(PRISMA) 2020 guidelines. Relevant literature was collected from reputable scientific databases and analyzed using thematic analysis through identification, selection, synthesis, and interpretation of research findings. The results indicate that Federated Learning has evolved into a key approach for* privacy-preserving artificial intelligence *by integrating distributed model training,* secure aggregation*,* differential privacy*, and* homomorphic encryption*. Nevertheless, its implementation continues to face challenges related to data heterogeneity, communication overhead, limited device resources, model security threats, and governance standardization. This study concludes that Federated Learning has substantial potential to support the development of secure, efficient, and privacy-preserving AI systems across various application domains.*

Keywords: *Federated Learning; Data Privacy; Privacy-Preserving Machine Learning; Artificial Intelligence; Systematic Literature Review*

1. PENDAHULUAN

Perkembangan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dalam beberapa tahun terakhir telah mendorong pemanfaatan data dalam skala yang semakin besar untuk mendukung proses pengambilan keputusan di berbagai sektor. Model pembelajaran mesin modern membutuhkan data dalam jumlah besar agar mampu menghasilkan

prediksi yang akurat dan berkinerja tinggi. Kondisi tersebut menyebabkan pendekatan *centralized machine learning*, yaitu pengumpulan seluruh data ke dalam satu pusat penyimpanan (*central server*), menjadi metode yang paling banyak digunakan dalam pengembangan AI. Pendekatan ini terbukti efektif dalam meningkatkan performa model, namun pada saat yang sama menimbulkan berbagai persoalan terkait privasi data, keamanan informasi, biaya komunikasi, serta kepatuhan terhadap regulasi perlindungan data pribadi. Meningkatnya kesadaran masyarakat terhadap keamanan data menjadikan perlindungan privasi sebagai salah satu isu utama dalam pengembangan teknologi AI modern (Nguyen et al., 2024).

Perkembangan teknologi digital semakin memperbesar tantangan tersebut. Berbagai perangkat yang terhubung melalui *Internet of Things* (IoT), telepon pintar, kendaraan cerdas, layanan kesehatan digital, maupun sistem keuangan menghasilkan data dalam jumlah yang sangat besar dan bersifat sensitif. Pengiriman seluruh data tersebut ke pusat pemrosesan meningkatkan risiko kebocoran data, penyalahgunaan informasi pribadi, serta serangan siber. Selain itu, berbagai regulasi perlindungan data di berbagai negara mendorong organisasi untuk membatasi perpindahan data pribadi dan memastikan bahwa proses pengolahan data dilakukan secara aman serta menghormati hak-hak pengguna. Kondisi ini mendorong munculnya paradigma baru dalam pengembangan *Machine Learning* yang mampu mempertahankan kualitas model tanpa harus memindahkan data dari perangkat pengguna (Lazaros et al., 2024).

Salah satu inovasi yang berkembang pesat untuk menjawab tantangan tersebut adalah *Federated Learning* (FL). Berbeda dengan pendekatan pembelajaran mesin terpusat, Federated Learning memungkinkan proses pelatihan model dilakukan secara lokal pada masing-masing perangkat atau institusi, sedangkan yang dikirim ke server pusat hanyalah parameter atau pembaruan model (*model updates*) tanpa memindahkan data asli. Dengan mekanisme tersebut, data pengguna tetap berada pada lokasi asal sehingga risiko pelanggaran privasi dapat diminimalkan. Pendekatan ini menjadikan Federated Learning sebagai salah satu teknologi yang banyak dikembangkan untuk mendukung implementasi AI yang berorientasi pada perlindungan data (*privacy-preserving artificial intelligence*) (Prasetyo & Ramadhani, 2025).

Implementasi Federated Learning telah berkembang pada berbagai bidang, seperti layanan kesehatan, sistem keuangan, pendidikan, *smart city*, kendaraan otonom, *Internet of Things* (IoT), serta *edge computing*. Pada sektor kesehatan, Federated Learning memungkinkan berbagai rumah sakit melatih model diagnosis berbasis AI secara kolaboratif tanpa harus saling membagikan data rekam medis pasien. Di sektor keuangan, teknologi ini dimanfaatkan untuk meningkatkan kemampuan deteksi penipuan (*fraud detection*) dengan tetap menjaga kerahasiaan data nasabah. Sementara itu, pada lingkungan IoT dan *edge computing*, Federated Learning memungkinkan perangkat cerdas melakukan proses pembelajaran secara terdistribusi sehingga mengurangi kebutuhan transfer data ke pusat komputasi dan meningkatkan efisiensi jaringan (Mahendra et al., 2025).

Meskipun menawarkan berbagai keunggulan, implementasi Federated Learning masih menghadapi sejumlah tantangan. Hasil berbagai penelitian menunjukkan bahwa heterogenitas data (*non-independent and identically distributed/non-IID data*), keterbatasan kapasitas perangkat, tingginya biaya komunikasi antarperangkat, keamanan model terhadap serangan *model poisoning*, serta kesulitan dalam menjaga konsistensi proses pelatihan menjadi permasalahan yang masih memerlukan solusi. Selain itu, perkembangan *Generative Artificial Intelligence*, *Large Language Models*, dan *Edge AI* juga membuka tantangan baru dalam penerapan Federated Learning pada sistem AI yang memiliki kompleksitas lebih tinggi. Oleh karena itu, penelitian mengenai Federated Learning tidak hanya berfokus pada peningkatan akurasi model, tetapi juga pada pengembangan metode yang mampu meningkatkan efisiensi, keamanan, skalabilitas, dan keandalan sistem.

Kajian literatur menunjukkan bahwa jumlah publikasi mengenai Federated Learning meningkat secara signifikan dalam lima tahun terakhir (Sukron & Rayyan, 2025). Namun, sebagian besar penelitian masih berfokus pada pengembangan algoritma, optimasi komunikasi, atau implementasi pada domain tertentu (Rabbani & Purnama, 2026), sedangkan kajian yang menyintesis perkembangan konsep Federated Learning, perannya dalam menjaga privasi data, tantangan implementasi, serta arah pengembangan teknologi di masa depan masih relatif terbatas (Barrotut & Ilyana, 2026). Padahal, sintesis yang komprehensif diperlukan untuk memberikan gambaran menyeluruh mengenai perkembangan penelitian sekaligus mengidentifikasi peluang pengembangan teknologi Federated Learning yang lebih efektif dan aman (Ismanto et al., 2026).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan Systematic Literature Review (SLR) mengenai perkembangan Federated Learning dalam menjaga privasi data. Secara khusus, penelitian ini bertujuan untuk menganalisis perkembangan konsep Federated Learning sebagai paradigma pembelajaran terdistribusi, mengidentifikasi perannya dalam meningkatkan privasi dan keamanan data, mengkaji berbagai tantangan implementasi pada berbagai sektor, serta merumuskan agenda penelitian masa depan. Hasil penelitian diharapkan dapat memberikan kontribusi

konseptual bagi pengembangan ilmu pengetahuan di bidang *Artificial Intelligence*, *Data Science*, dan *Cybersecurity*, sekaligus menjadi referensi bagi akademisi, peneliti, pengembang teknologi, dan pembuat kebijakan dalam mengembangkan sistem AI yang aman, efisien, dan berorientasi pada perlindungan privasi data.

2. METODE PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) untuk memperoleh sintesis ilmiah yang komprehensif mengenai perkembangan *Federated Learning* dalam menjaga privasi data. Proses penelitian mengacu pada pedoman Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020, yang meliputi tahapan identifikasi, penyaringan, penilaian kelayakan, dan inklusi artikel sesuai dengan tujuan penelitian. Penelusuran literatur dilakukan melalui basis data ilmiah bereputasi, yaitu Scopus, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, dan Google Scholar, menggunakan kata kunci *Federated Learning*, *Privacy-Preserving Machine Learning*, *Data Privacy*, *Distributed Machine Learning*, *Edge AI*, dan *Secure Federated Learning*. Kriteria inklusi meliputi artikel jurnal *peer-reviewed* berbahasa Inggris maupun Indonesia yang diterbitkan pada periode 2021–2026, tersedia dalam *full text*, dan membahas konsep, implementasi, tantangan, maupun pengembangan Federated Learning. Sementara itu, prosiding, editorial, artikel yang tidak melalui proses *peer review*, dan publikasi yang tidak relevan dengan fokus penelitian dikeluarkan dari proses seleksi. Seluruh artikel yang memenuhi kriteria dianalisis menggunakan thematic analysis melalui proses reduksi data, pengelompokan tema, sintesis temuan, dan interpretasi untuk mengidentifikasi perkembangan Federated Learning, perannya dalam menjaga privasi data, tantangan implementasi, serta arah pengembangan penelitian di masa depan.

3. HASIL DAN PEMBAHASAN

3.1 Perkembangan Federated Learning sebagai Paradigma Pembelajaran Terdistribusi

Perkembangan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) telah meningkatkan kebutuhan terhadap data dalam jumlah besar untuk menghasilkan model dengan tingkat akurasi yang tinggi. Selama bertahun-tahun, pendekatan *centralized machine learning* menjadi paradigma utama dalam pengembangan AI, yaitu dengan mengumpulkan seluruh data dari berbagai sumber ke dalam satu server pusat untuk diproses dan digunakan dalam pelatihan model. Pendekatan ini terbukti mampu menghasilkan performa model yang baik, namun juga menimbulkan berbagai persoalan, seperti meningkatnya risiko kebocoran data, tingginya biaya komunikasi, keterbatasan kepatuhan terhadap regulasi perlindungan data, serta ancaman terhadap privasi pengguna. Kondisi tersebut mendorong munculnya paradigma baru dalam pembelajaran mesin yang memungkinkan proses pelatihan dilakukan tanpa memindahkan data dari lokasi asalnya (Justam et al., n.d.).

Hasil sintesis literatur menunjukkan bahwa *Federated Learning* (FL) berkembang sebagai salah satu inovasi penting dalam bidang *privacy-preserving machine learning*. Konsep Federated Learning pertama kali diperkenalkan untuk mengatasi keterbatasan pembelajaran mesin terpusat melalui pendekatan pembelajaran terdistribusi (*distributed learning*). Pada Federated Learning, data tetap disimpan pada perangkat pengguna (*local devices*), sedangkan server pusat hanya menerima parameter atau pembaruan model (*model parameters* atau *model updates*) yang dihasilkan dari proses pelatihan lokal. Selanjutnya, server melakukan proses agregasi menggunakan algoritma tertentu, seperti *Federated Averaging (FedAvg)*, untuk menghasilkan model global yang kemudian didistribusikan kembali kepada seluruh klien. Mekanisme tersebut memungkinkan model AI terus berkembang tanpa harus mengumpulkan data mentah (*raw data*) dari setiap pengguna (Barrotut & Ilyana, 2026).

Perkembangan Federated Learning mengalami peningkatan yang sangat pesat dalam lima tahun terakhir seiring meningkatnya perhatian terhadap perlindungan data pribadi dan berkembangnya teknologi komputasi terdistribusi. Literatur menunjukkan bahwa implementasi Federated Learning tidak lagi terbatas pada perangkat bergerak (*mobile devices*), tetapi telah berkembang ke berbagai lingkungan komputasi modern seperti *edge computing*, *cloud computing*, *Internet of Things* (IoT), kendaraan otonom (*autonomous vehicles*), jaringan 5G dan 6G, hingga *smart manufacturing*. Integrasi dengan teknologi tersebut memungkinkan proses pembelajaran dilakukan lebih dekat dengan sumber data (*edge intelligence*), sehingga mampu mengurangi latensi komunikasi, meningkatkan efisiensi penggunaan jaringan, serta mempercepat proses pembaruan model (Rachman et al., 2025).

Selain perkembangan pada sisi infrastruktur, hasil kajian juga menunjukkan bahwa penelitian Federated Learning telah mengalami diversifikasi berdasarkan karakteristik arsitektur dan mekanisme kolaborasi. Berdasarkan pendekatan implementasinya, Federated Learning umumnya dibedakan menjadi tiga kategori utama, yaitu *Horizontal Federated Learning*, *Vertical Federated Learning*, dan *Federated Transfer Learning*. *Horizontal Federated Learning* digunakan ketika berbagai klien memiliki fitur data yang sama namun berasal dari pengguna yang berbeda. Sebaliknya, *Vertical Federated Learning* diterapkan ketika organisasi memiliki data mengenai objek yang sama

tetapi dengan atribut yang berbeda. Adapun *Federated Transfer Learning* digunakan pada kondisi ketika baik fitur maupun pengguna berbeda sehingga diperlukan pendekatan *transfer learning* untuk memungkinkan kolaborasi antarorganisasi. Perkembangan ketiga pendekatan tersebut menunjukkan bahwa Federated Learning semakin fleksibel dalam mengakomodasi berbagai karakteristik data dan kebutuhan implementasi (Ardiansyah & Purnomo, 2025).

Peningkatan penelitian juga terlihat dari semakin banyaknya pengembangan algoritma optimasi Federated Learning. Jika pada tahap awal penelitian lebih banyak menggunakan algoritma *Federated Averaging (FedAvg)*, perkembangan terbaru menunjukkan munculnya berbagai algoritma baru yang dirancang untuk meningkatkan konvergensi model, mengurangi biaya komunikasi, serta mengatasi permasalahan data yang tidak homogen (*non-IID data*). Berbagai pendekatan optimasi tersebut berupaya meningkatkan efisiensi pelatihan model sekaligus mempertahankan tingkat akurasi pada lingkungan yang memiliki karakteristik data dan kapasitas perangkat yang berbeda-beda. Hal ini menunjukkan bahwa fokus penelitian Federated Learning telah bergeser dari pembuktian konsep menuju peningkatan performa dan skalabilitas implementasi (Prasetyo & Ramadhani, 2025).

Berdasarkan hasil sintesis literatur, perkembangan Federated Learning sebagai paradigma pembelajaran terdistribusi dapat dirangkum sebagaimana disajikan pada Tabel 1.

Tabel 1. Perkembangan Federated Learning sebagai Paradigma Pembelajaran Terdistribusi

Aspek Perkembangan	Deskripsi	Kontribusi
Paradigma Pembelajaran	Peralihan dari centralized learning menuju distributed learning	Mengurangi kebutuhan pengiriman data ke server pusat
Mekanisme Pelatihan	Pelatihan model dilakukan pada perangkat lokal	Menjaga privasi data pengguna
Agregasi Model	Penggabungan parameter model menggunakan algoritma agregasi	Menghasilkan model global yang lebih efisien
Infrastruktur	Integrasi dengan Cloud Computing, Edge Computing, IoT, dan jaringan 5G	Mendukung implementasi AI terdistribusi
Arsitektur Federated Learning	Horizontal FL, Vertical FL, dan Federated Transfer Learning	Fleksibilitas implementasi pada berbagai jenis data
Pengembangan Algoritma	Optimasi FedAvg dan algoritma Federated Learning lainnya	Meningkatkan akurasi, efisiensi, dan skalabilitas model

Hasil kajian menunjukkan bahwa Federated Learning telah berkembang dari sekadar alternatif terhadap pembelajaran mesin terpusat menjadi paradigma baru dalam pengembangan AI yang berorientasi pada perlindungan privasi. Integrasi Federated Learning dengan *edge computing*, *cloud computing*, dan berbagai perangkat cerdas menunjukkan bahwa teknologi ini memiliki potensi besar dalam mendukung implementasi AI yang lebih aman, efisien, dan terdistribusi. Perkembangan tersebut sekaligus menandai perubahan orientasi penelitian AI modern, yaitu dari pendekatan yang berpusat pada pengumpulan data menuju pendekatan yang menempatkan privasi pengguna sebagai bagian integral dari proses pembelajaran mesin. Dengan demikian, Federated Learning menjadi fondasi penting dalam pengembangan sistem AI yang tidak hanya memiliki performa tinggi, tetapi juga memenuhi tuntutan keamanan data dan kepatuhan terhadap regulasi perlindungan privasi.

3.2 Peran Federated Learning dalam Menjaga Privasi dan Keamanan Data

Hasil sintesis literatur menunjukkan bahwa *Federated Learning* (FL) berkembang sebagai salah satu pendekatan yang paling menjanjikan dalam mewujudkan *privacy-preserving artificial intelligence*. Berbeda dengan pendekatan *centralized machine learning* yang mengharuskan seluruh data dikumpulkan pada server pusat, Federated Learning mempertahankan data tetap berada pada perangkat atau institusi asal (*data locality*). Dalam mekanisme ini, proses pelatihan model dilakukan secara lokal pada masing-masing klien, sedangkan server pusat hanya menerima parameter model atau hasil pembaruan (*model updates*) untuk selanjutnya dilakukan proses agregasi. Dengan demikian, data mentah (*raw data*) tidak pernah berpindah dari lokasi penyimpanannya sehingga risiko kebocoran data selama proses transmisi dapat diminimalkan. Pendekatan ini menjadi solusi yang semakin relevan di tengah meningkatnya tuntutan perlindungan data pribadi dan kepatuhan terhadap berbagai regulasi privasi (Pratama et al., 2025).

Salah satu keunggulan utama Federated Learning adalah kemampuannya menjaga kerahasiaan data pengguna tanpa mengurangi manfaat kolaborasi dalam pelatihan model AI. Pada pendekatan pembelajaran terpusat, organisasi harus menggabungkan data dari berbagai sumber untuk memperoleh model yang memiliki tingkat akurasi tinggi. Namun, proses tersebut meningkatkan risiko penyalahgunaan data, akses tidak sah, maupun pelanggaran terhadap kebijakan perlindungan data.

Federated Learning mengubah paradigma tersebut dengan memungkinkan berbagai perangkat atau organisasi membangun model AI secara bersama-sama tanpa harus saling membagikan data asli. Dengan mekanisme tersebut, setiap peserta tetap memiliki kendali penuh terhadap data yang dimiliki sehingga prinsip *data sovereignty* dan *data ownership* dapat dipertahankan (Maruanaya et al., 2026).

Literatur juga menunjukkan bahwa Federated Learning semakin banyak dikombinasikan dengan berbagai teknik perlindungan privasi untuk meningkatkan keamanan sistem. Salah satu teknik yang paling banyak digunakan adalah Secure Aggregation, yaitu metode yang memungkinkan server melakukan agregasi parameter model tanpa dapat mengetahui isi parameter yang dikirim oleh masing-masing klien. Melalui teknik ini, pembaruan model yang dikirimkan telah dienkripsi sehingga hanya hasil agregasi yang dapat diproses oleh server. Pendekatan tersebut mampu mengurangi risiko penyadapan selama proses komunikasi sekaligus meningkatkan kerahasiaan informasi yang berasal dari setiap peserta pelatihan (Ardiansyah & Purnomo, 2025).

Selain *Secure Aggregation*, berbagai penelitian juga mengembangkan integrasi Federated Learning dengan Differential Privacy. Teknik ini bekerja dengan menambahkan gangguan (*noise*) secara terkontrol pada parameter model sebelum dikirim ke server sehingga identitas maupun informasi spesifik mengenai data pengguna tidak dapat direkonstruksi kembali. Penerapan *Differential Privacy* memberikan jaminan matematis terhadap perlindungan privasi karena mampu membatasi kemungkinan identifikasi individu dari hasil analisis model. Kombinasi Federated Learning dan *Differential Privacy* menjadi salah satu pendekatan yang banyak direkomendasikan untuk implementasi AI pada sektor yang mengelola data sensitif, seperti layanan kesehatan, keuangan, dan pemerintahan (Yuliyanto & Wijaya, 2025).

Penguatan keamanan Federated Learning juga dilakukan melalui penerapan Homomorphic Encryption, yaitu teknik enkripsi yang memungkinkan proses komputasi dilakukan terhadap data yang masih berada dalam keadaan terenkripsi. Dengan pendekatan ini, server dapat melakukan agregasi parameter model tanpa harus mendekripsi informasi yang diterima dari setiap klien. Meskipun teknik ini meningkatkan kebutuhan komputasi, berbagai penelitian menunjukkan bahwa integrasi *Homomorphic Encryption* mampu memperkuat perlindungan data pada lingkungan yang memiliki tingkat sensitivitas tinggi. Selain itu, beberapa penelitian mulai mengombinasikan Federated Learning dengan teknologi *blockchain* untuk meningkatkan integritas data, transparansi proses pelatihan, serta ketertelusuran (*traceability*) setiap pembaruan model yang dilakukan oleh peserta (Andrian & Wijaya, 2026).

Implementasi Federated Learning dalam menjaga privasi telah diterapkan pada berbagai sektor strategis. Pada sektor kesehatan, teknologi ini memungkinkan beberapa rumah sakit atau institusi medis mengembangkan model diagnosis berbasis AI secara kolaboratif tanpa perlu bertukar data rekam medis pasien. Pada sektor keuangan, Federated Learning dimanfaatkan untuk mendukung deteksi penipuan (*fraud detection*), penilaian risiko kredit, dan analisis transaksi tanpa membuka informasi nasabah kepada pihak lain. Di bidang *Internet of Things* (IoT) dan *edge computing*, Federated Learning memungkinkan perangkat cerdas melakukan pembelajaran secara lokal sehingga mengurangi kebutuhan pengiriman data ke pusat komputasi, menekan latensi komunikasi, serta meningkatkan efisiensi penggunaan jaringan. Temuan-temuan tersebut menunjukkan bahwa Federated Learning mampu memberikan keseimbangan antara kebutuhan analisis data dan perlindungan privasi pengguna (Kusumastuti et al., 2025).

Berdasarkan hasil sintesis literatur, peran Federated Learning dalam menjaga privasi dan keamanan data dapat dirangkum sebagaimana disajikan pada Tabel 2.

Tabel 2. Peran Federated Learning dalam Menjaga Privasi dan Keamanan Data

Aspek	Mekanisme	Manfaat
Data Locality	Data tetap berada pada perangkat lokal	Mengurangi risiko kebocoran data
Secure Aggregation	Agregasi parameter model secara terenkripsi	Meningkatkan kerahasiaan komunikasi
Differential Privacy	Penambahan noise pada parameter model	Melindungi identitas dan data individu
Homomorphic Encryption	Komputasi dilakukan pada data terenkripsi	Memperkuat keamanan proses agregasi
Blockchain Integration	Pencatatan proses pelatihan secara terdistribusi	Meningkatkan integritas dan transparansi
Edge Computing	Pelatihan model dilakukan dekat dengan sumber data	Mengurangi latensi dan biaya komunikasi

Hasil kajian menunjukkan bahwa Federated Learning telah menjadi salah satu fondasi utama dalam pengembangan AI yang berorientasi pada perlindungan privasi (*privacy-preserving AI*). Keunggulan teknologi ini tidak hanya terletak pada kemampuannya mempertahankan data di lokasi asal,

tetapi juga pada fleksibilitasnya untuk dikombinasikan dengan berbagai mekanisme keamanan modern, seperti *Secure Aggregation*, *Differential Privacy*, *Homomorphic Encryption*, dan *blockchain*. Integrasi berbagai teknologi tersebut menjadikan Federated Learning semakin relevan dalam mendukung implementasi AI pada lingkungan yang membutuhkan tingkat keamanan dan kerahasiaan data yang tinggi. Dengan demikian, Federated Learning tidak hanya menawarkan solusi teknis terhadap perlindungan privasi, tetapi juga menjadi pendekatan strategis dalam membangun sistem AI yang aman, terpercaya, dan sesuai dengan tuntutan regulasi perlindungan data di era transformasi digital.

3.3 Tantangan Implementasi Federated Learning

Hasil sintesis literatur menunjukkan bahwa meskipun *Federated Learning* (FL) menawarkan solusi yang efektif dalam menjaga privasi data, implementasinya masih menghadapi berbagai tantangan teknis maupun operasional. Berbeda dengan pendekatan *centralized machine learning* yang mengelola seluruh data pada satu pusat komputasi, Federated Learning melibatkan banyak perangkat atau organisasi yang memiliki karakteristik data, kapasitas komputasi, dan kondisi jaringan yang berbeda-beda. Keragaman tersebut menyebabkan proses pelatihan model menjadi lebih kompleks sehingga diperlukan berbagai strategi optimasi agar model global tetap memiliki tingkat akurasi, efisiensi, dan keamanan yang tinggi. Oleh karena itu, penelitian mengenai Federated Learning saat ini tidak hanya berfokus pada peningkatan performa model, tetapi juga pada pengembangan mekanisme yang mampu mengatasi berbagai tantangan implementasi di lingkungan nyata (Rusdha et al., 2026).

Salah satu tantangan yang paling banyak dibahas dalam literatur adalah heterogenitas data atau *non-independent and identically distributed* (*non-IID data*). Dalam implementasi nyata, setiap perangkat atau organisasi umumnya memiliki karakteristik data yang berbeda, baik dari segi jumlah, distribusi, maupun kualitas data. Sebagai contoh, data pasien pada satu rumah sakit dapat memiliki karakteristik yang berbeda dengan rumah sakit lainnya, demikian pula pola transaksi pada satu lembaga keuangan dapat berbeda dengan lembaga keuangan lainnya. Perbedaan tersebut menyebabkan model lokal berkembang dengan arah yang tidak seragam sehingga proses agregasi model global menjadi lebih sulit. Akibatnya, tingkat konvergensi model menurun dan akurasi sistem dapat berkurang dibandingkan dengan pendekatan pembelajaran terpusat.

Tantangan berikutnya berkaitan dengan beban komunikasi (*communication overhead*). Federated Learning memerlukan pertukaran parameter model secara berulang antara server pusat dan seluruh klien selama proses pelatihan berlangsung. Pada model AI modern yang memiliki jutaan hingga miliaran parameter, ukuran pembaruan model menjadi sangat besar sehingga meningkatkan kebutuhan bandwidth jaringan serta memperpanjang waktu pelatihan. Permasalahan ini semakin terasa pada lingkungan yang memiliki koneksi internet terbatas atau jumlah klien yang sangat banyak, seperti implementasi pada *Internet of Things* (IoT) dan *edge computing*. Oleh karena itu, berbagai penelitian mengembangkan teknik kompresi parameter, *model pruning*, *gradient compression*, serta mekanisme pembaruan adaptif untuk mengurangi biaya komunikasi tanpa mengorbankan kualitas model (Abdurrohman & Juniarrochman, 2026).

Selain komunikasi, heterogenitas perangkat (*client heterogeneity*) juga menjadi tantangan penting dalam Federated Learning. Setiap perangkat yang berpartisipasi dalam pelatihan model memiliki kemampuan komputasi, kapasitas memori, daya baterai, dan kualitas koneksi jaringan yang berbeda. Sebagian perangkat mampu menyelesaikan proses pelatihan dengan cepat, sementara perangkat lain membutuhkan waktu yang lebih lama atau bahkan gagal mengirimkan pembaruan model akibat keterbatasan sumber daya. Kondisi tersebut menyebabkan ketidakseimbangan proses pelatihan (*straggler problem*) yang dapat memperlambat konvergensi model global. Untuk mengatasi permasalahan tersebut, berbagai penelitian mengembangkan algoritma pemilihan klien (*client selection*), pelatihan asinkron (*asynchronous federated learning*), dan mekanisme penjadwalan adaptif agar proses pelatihan menjadi lebih efisien (Prasetyo & Ramadhani, 2025).

Dari aspek keamanan, Federated Learning juga menghadapi ancaman berupa serangan terhadap model (*model poisoning attack*) dan serangan inferensi (*inference attack*). Pada *model poisoning*, pihak yang tidak bertanggung jawab mengirimkan parameter model yang telah dimanipulasi sehingga dapat menurunkan performa model global atau bahkan menghasilkan keputusan yang salah. Sementara itu, *inference attack* memungkinkan penyerang memperoleh informasi mengenai data lokal hanya berdasarkan parameter model yang dikirimkan ke server. Meskipun data mentah tidak pernah dipindahkan, berbagai penelitian menunjukkan bahwa parameter model tetap berpotensi mengungkap informasi sensitif apabila tidak dilindungi dengan mekanisme keamanan tambahan. Oleh karena itu, pengembangan metode deteksi anomali, *robust aggregation*, *secure aggregation*, serta integrasi dengan *differential privacy* dan *homomorphic encryption* menjadi fokus utama penelitian terkini (Yanti et al., 2025).

Tantangan lainnya adalah skalabilitas sistem. Seiring meningkatnya jumlah perangkat yang berpartisipasi dalam Federated Learning, proses

koordinasi, sinkronisasi, dan agregasi model menjadi semakin kompleks. Lingkungan yang melibatkan ribuan hingga jutaan perangkat memerlukan mekanisme manajemen sumber daya yang efisien agar sistem tetap mampu beroperasi secara stabil. Selain itu, perkembangan *Foundation Models* dan *Large Language Models* (LLMs) menghadirkan tantangan baru karena ukuran model yang sangat besar meningkatkan kebutuhan komputasi, memori, dan komunikasi selama proses pelatihan. Oleh sebab itu, penelitian terbaru mulai mengembangkan pendekatan *hierarchical federated learning*, *clustered federated learning*, serta integrasi dengan *edge computing* dan *cloud computing* untuk meningkatkan skalabilitas sistem (Fitriansyah & Nugroho, 2026).

Hasil sintesis literatur juga menunjukkan bahwa tantangan implementasi Federated Learning tidak hanya bersifat teknis, tetapi juga berkaitan dengan aspek tata kelola dan regulasi. Kolaborasi antarorganisasi dalam Federated Learning memerlukan kesepakatan mengenai kepemilikan model, mekanisme berbagi manfaat, standar interoperabilitas, serta kepatuhan terhadap regulasi perlindungan data yang berlaku di masing-masing yurisdiksi. Perbedaan kebijakan dan standar keamanan dapat menjadi hambatan dalam membangun ekosistem Federated Learning yang bersifat lintas institusi maupun lintas negara. Oleh karena itu, pengembangan Federated Learning pada masa depan memerlukan pendekatan multidisipliner yang mengintegrasikan aspek teknologi, keamanan siber, tata kelola data, hukum, dan kebijakan publik (Agustina et al., 2025).

Secara keseluruhan, hasil kajian menunjukkan bahwa keberhasilan implementasi Federated Learning bergantung pada kemampuan mengatasi berbagai tantangan tersebut secara terpadu. Pengembangan algoritma yang lebih adaptif, peningkatan efisiensi komunikasi, penguatan mekanisme keamanan, optimalisasi pengelolaan sumber daya, serta harmonisasi tata kelola menjadi faktor penting dalam mewujudkan Federated Learning sebagai paradigma pembelajaran mesin yang tidak hanya menjaga privasi data, tetapi juga mampu memberikan performa yang tinggi, aman, dan berkelanjutan pada berbagai lingkungan komputasi modern (Tosida et al., 2026).

3.4 Arah Pengembangan Federated Learning di Masa Depan

Hasil sintesis literatur menunjukkan bahwa arah pengembangan *Federated Learning* (FL) pada masa depan tidak lagi hanya berfokus pada peningkatan akurasi model, tetapi juga diarahkan pada pengembangan sistem pembelajaran mesin yang lebih adaptif, aman, efisien, dan mampu beroperasi pada lingkungan komputasi yang semakin kompleks. Pesatnya perkembangan *Artificial Intelligence*, khususnya *Generative Artificial Intelligence*, *Large Language Models* (LLMs), *Edge AI*, serta meningkatnya kebutuhan terhadap perlindungan data pribadi, mendorong Federated Learning menjadi salah satu teknologi strategis dalam membangun ekosistem AI yang berorientasi pada privasi (*privacy-preserving AI*). Oleh karena itu, berbagai penelitian mulai mengembangkan pendekatan baru yang mampu meningkatkan skalabilitas, keamanan, interoperabilitas, dan efisiensi Federated Learning agar dapat diimplementasikan pada berbagai sektor secara lebih luas (Rahmeisi et al., 2025).

Salah satu arah pengembangan yang memperoleh perhatian besar adalah integrasi Federated Learning dengan Foundation Models dan Large Language Models (LLMs). Perkembangan model AI berukuran besar telah menghasilkan kemampuan yang sangat baik dalam memahami bahasa, gambar, maupun data multimodal. Namun, proses pelatihan model tersebut membutuhkan data dalam jumlah besar yang sering kali mengandung informasi sensitif. Federated Learning menawarkan solusi melalui mekanisme pelatihan terdistribusi yang memungkinkan organisasi mengembangkan model AI secara kolaboratif tanpa harus memindahkan data asli ke pusat komputasi. Berbagai penelitian terbaru menunjukkan bahwa integrasi Federated Learning dengan *Foundation Models* berpotensi memperluas penerapan AI pada sektor kesehatan, pendidikan, pemerintahan, dan industri dengan tetap menjaga kerahasiaan data pengguna (Ashari et al., 2025).

Perkembangan berikutnya mengarah pada penguatan Federated Edge Learning, yaitu integrasi Federated Learning dengan *edge computing*. Pendekatan ini memungkinkan proses pelatihan model dilakukan secara langsung pada perangkat yang berada di dekat sumber data, seperti telepon pintar, kamera pintar, kendaraan otonom, sensor industri, maupun perangkat *Internet of Things* (IoT). Dengan memanfaatkan komputasi di sisi *edge*, kebutuhan pengiriman data ke pusat dapat dikurangi secara signifikan sehingga latensi komunikasi menjadi lebih rendah dan penggunaan bandwidth lebih efisien. Selain meningkatkan respons sistem secara real-time, Federated Edge Learning juga memperkuat perlindungan privasi karena sebagian besar proses komputasi dilakukan pada perangkat lokal (Mahendra et al., 2025).

Literatur juga menunjukkan bahwa penelitian masa depan akan semakin berfokus pada pengembangan Federated Learning yang aman dan terpercaya (*Trustworthy Federated Learning*). Meskipun Federated Learning telah mampu menjaga kerahasiaan data mentah, ancaman terhadap parameter model, serangan *model poisoning*, *backdoor attack*, dan *model inversion attack* masih menjadi tantangan serius. Oleh karena itu, berbagai penelitian mulai mengembangkan algoritma agregasi

yang lebih tangguh (*robust aggregation*), sistem deteksi anomali berbasis AI, mekanisme autentikasi klien, serta integrasi dengan teknologi *blockchain* untuk meningkatkan integritas proses pelatihan. Pengembangan tersebut bertujuan membangun ekosistem Federated Learning yang tidak hanya melindungi data, tetapi juga mampu menjamin kepercayaan terhadap keseluruhan proses pembelajaran model (Yuliyanto & Wijaya, 2025).

Arah penelitian lainnya adalah integrasi Federated Learning dengan berbagai teknik Privacy-Enhancing Technologies (PETs). Hasil sintesis menunjukkan bahwa kombinasi Federated Learning dengan *Differential Privacy*, *Homomorphic Encryption*, *Secure Multi-Party Computation* (SMPC), dan *Trusted Execution Environment* (TEE) menjadi fokus utama dalam pengembangan AI yang berorientasi pada perlindungan privasi. Integrasi berbagai teknologi tersebut diharapkan mampu memperkuat keamanan parameter model sekaligus meminimalkan risiko rekonstruksi data oleh pihak yang tidak berwenang. Penelitian pada masa mendatang juga diperkirakan akan mengembangkan pendekatan adaptif yang mampu memilih mekanisme perlindungan privasi sesuai dengan tingkat sensitivitas data dan kebutuhan komputasi.

Selain aspek teknis, hasil kajian memperlihatkan bahwa pengembangan Federated Learning juga akan dipengaruhi oleh meningkatnya kebutuhan terhadap standarisasi dan tata kelola. Implementasi Federated Learning yang melibatkan berbagai organisasi memerlukan standar interoperabilitas, mekanisme audit, tata kelola data, serta pembagian tanggung jawab yang jelas di antara seluruh peserta. Oleh karena itu, penelitian masa depan tidak hanya berfokus pada algoritma, tetapi juga pada pengembangan kerangka *Federated Learning Governance* yang mengatur proses kolaborasi, keamanan data, kepatuhan terhadap regulasi perlindungan data, serta mekanisme evaluasi terhadap kualitas model yang dihasilkan. Pendekatan tersebut menjadi semakin penting mengingat implementasi Federated Learning akan semakin banyak digunakan dalam sektor yang memiliki tingkat sensitivitas data tinggi (Tosida et al., 2026).

Perkembangan Federated Learning juga diprediksi akan semakin luas pada berbagai sektor strategis. Di bidang kesehatan, teknologi ini akan mendukung kolaborasi penelitian medis lintas rumah sakit tanpa harus memindahkan data pasien. Pada sektor keuangan, Federated Learning akan meningkatkan kemampuan deteksi penipuan dan analisis risiko dengan tetap menjaga kerahasiaan informasi nasabah. Di bidang industri, teknologi ini berpotensi memperkuat sistem *predictive maintenance* dan otomatisasi manufaktur berbasis AI. Sementara itu, pada sektor pemerintahan dan *smart city*, Federated Learning dapat dimanfaatkan untuk meningkatkan kualitas pelayanan publik melalui analisis data yang aman dan terdesentralisasi. Perluasan implementasi tersebut menunjukkan bahwa Federated Learning memiliki peran strategis dalam mendukung transformasi digital yang berorientasi pada keamanan dan privasi data (Kusumastuti et al., 2025).

Berdasarkan hasil sintesis literatur, dapat dipahami bahwa arah pengembangan Federated Learning pada masa depan akan bergerak menuju pembentukan ekosistem AI yang lebih cerdas, aman, kolaboratif, dan berkelanjutan. Pengembangan algoritma yang lebih efisien, integrasi dengan *Foundation Models*, pemanfaatan *Edge AI*, penerapan teknologi peningkatan privasi, penguatan keamanan siber, serta penyusunan tata kelola Federated Learning menjadi agenda penelitian yang memiliki prospek besar. Dengan demikian, Federated Learning tidak hanya diposisikan sebagai metode pembelajaran mesin terdistribusi, tetapi juga sebagai fondasi utama dalam membangun sistem *Artificial Intelligence* yang mampu menyeimbangkan kebutuhan inovasi teknologi dengan perlindungan privasi dan keamanan data pada era transformasi digital.

4. KESIMPULAN

Berdasarkan hasil *Systematic Literature Review* mengenai perkembangan *Federated Learning* dalam menjaga privasi data, dapat disimpulkan bahwa Federated Learning telah berkembang menjadi paradigma baru dalam pembelajaran mesin terdistribusi yang mampu menjawab berbagai keterbatasan pendekatan *centralized machine learning*. Berbeda dengan model pembelajaran terpusat, Federated Learning memungkinkan proses pelatihan dilakukan pada perangkat atau institusi tempat data berada, sedangkan server pusat hanya menerima parameter model untuk proses agregasi. Pendekatan ini menjadikan Federated Learning sebagai salah satu teknologi utama dalam pengembangan *privacy-preserving artificial intelligence* karena mampu mempertahankan kerahasiaan data tanpa mengurangi efektivitas proses pembelajaran model.

Hasil penelitian juga menunjukkan bahwa Federated Learning memiliki peran yang signifikan dalam menjaga privasi dan keamanan data melalui mekanisme pelatihan lokal, *secure aggregation*, *differential privacy*, *homomorphic encryption*, serta integrasi dengan teknologi pendukung lainnya. Implementasi teknologi ini telah berkembang pada berbagai sektor, seperti layanan kesehatan, keuangan, *Internet of Things*, *edge computing*, dan *smart city*, yang memerlukan pengelolaan data sensitif secara aman. Namun demikian, penerapan Federated Learning masih menghadapi berbagai tantangan, antara lain heterogenitas data (*non-IID data*), tingginya biaya komunikasi, keterbatasan kapasitas

perangkat, ancaman *model poisoning*, skalabilitas sistem, serta kebutuhan terhadap tata kelola dan standarisasi implementasi. Berbagai tantangan tersebut menunjukkan bahwa pengembangan Federated Learning memerlukan pendekatan yang tidak hanya berorientasi pada peningkatan performa algoritma, tetapi juga pada penguatan keamanan, efisiensi, dan interoperabilitas sistem.

Selain itu, hasil sintesis literatur mengidentifikasi bahwa arah pengembangan Federated Learning pada masa depan akan difokuskan pada integrasi dengan *Foundation Models*, *Large Language Models*, *Edge AI*, serta berbagai *Privacy-Enhancing Technologies* untuk memperkuat keamanan dan perlindungan data. Pengembangan *Trustworthy Federated Learning*, penguatan tata kelola Federated Learning, serta harmonisasi standar implementasi juga menjadi agenda penelitian yang penting dalam mendukung penerapan AI yang bertanggung jawab. Dengan demikian, penelitian ini memberikan kontribusi konseptual berupa pemetaan perkembangan Federated Learning, identifikasi perannya dalam menjaga privasi data, analisis tantangan implementasi, serta perumusan arah penelitian yang dapat menjadi referensi bagi akademisi, peneliti, pengembang teknologi, dan pembuat kebijakan dalam mengembangkan sistem AI yang aman, efisien, dan berkelanjutan.

5. SARAN

Berdasarkan hasil penelitian, organisasi dan pengembang teknologi disarankan untuk mengintegrasikan Federated Learning sebagai bagian dari strategi pengembangan *Artificial Intelligence* yang berorientasi pada perlindungan privasi data. Implementasi Federated Learning perlu didukung oleh penguatan mekanisme keamanan, seperti *secure aggregation*, *differential privacy*, dan *homomorphic encryption*, serta tata kelola data yang sesuai dengan regulasi perlindungan data pribadi. Selain itu, pengembangan infrastruktur komputasi yang mendukung *edge computing* dan peningkatan kapasitas sumber daya manusia di bidang AI dan keamanan siber menjadi faktor penting dalam mengoptimalkan penerapan Federated Learning pada berbagai sektor.

Bagi peneliti selanjutnya, disarankan untuk mengembangkan penelitian empiris mengenai efektivitas Federated Learning pada lingkungan nyata, khususnya pada sektor kesehatan, keuangan, industri, dan *Internet of Things*. Penelitian lanjutan juga dapat diarahkan pada pengembangan algoritma yang mampu mengatasi permasalahan *non-IID data*, mengurangi *communication overhead*, meningkatkan ketahanan terhadap serangan siber, serta mengintegrasikan Federated Learning dengan *Foundation Models*, *Large Language Models*, *blockchain*, dan teknologi peningkatan privasi lainnya. Selain itu, kajian mengenai tata kelola, standarisasi, dan evaluasi implementasi Federated Learning perlu terus dikembangkan untuk mendukung terciptanya sistem AI yang aman, terpercaya, adaptif, dan berkelanjutan.

6. UCAPAN TERIMAKASIH

Penulis menyampaikan penghargaan dan terima kasih kepada seluruh peneliti yang telah menghasilkan berbagai publikasi ilmiah mengenai *Federated Learning*, *Machine Learning*, keamanan data, dan perlindungan privasi yang menjadi sumber utama dalam penyusunan artikel ini. Apresiasi juga disampaikan kepada pengelola berbagai basis data ilmiah bereputasi yang telah menyediakan akses terhadap literatur berkualitas sehingga mendukung proses penelusuran, seleksi, dan sintesis artikel secara sistematis.

Penulis juga mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, masukan, dan motivasi selama proses penyusunan artikel ini. Semoga hasil penelitian ini dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang *Artificial Intelligence*, khususnya mengenai Federated Learning sebagai paradigma pembelajaran mesin yang mampu menjaga privasi data, meningkatkan keamanan informasi, serta mendukung transformasi digital yang inovatif, aman, dan berkelanjutan.

7. DAFTAR PUSTAKA

Abdurrohman, A., & Juniarrochman, W. (2026). Pengembangan Arsitektur Federated Learning untuk Privacy-Preserving Analytics pada Sistem IoT Skala Besar. *Asian Journal of Multidisciplinary Research*, *3*(1), 41–57.

Agustina, F., Syarif, A. M., Mulyanto, E., & Dolphina, E. (2025). BLOCKCHAIN UNTUK PEMERINTAHAN DIGITAL: SUATU KAJIAN LITERATUR SISTEMATIS. *INTEGRATIVE RESEARCH IN COMPUTER SCIENCE*, *1*(01), 77–107.

Andrian, D., & Wijaya, N. (2026). SYSTEMATIC LITERATURE REVIEW: TANTANGAN KEAMANAN CLOUD COMPUTING DALAM IMPLEMENTASI ARTIFICIAL INTELLIGENCE (AI). *Jurnal Media Akademik (JMA)*, *4*(6).

Ardiansyah, R., & Purnomo, R. (2025). Security and Privacy Challenges in Wireless Sensor Networks: A Systematic Literature Review of Threat Mitigation Strategies. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network*, *1*(01).

Ashari, I. F., Afriansyah, A., & Praseptiawan, M. (2025). *Kapita Selekta Informatika: Tren,*

Teknologi, dan Implementasi. ITERA Press.

Barrotut, B., & Ilyana, I. (2026). Tren Masa Depan Wireless Sensor Networks: Integrasi Artificial Intelligence untuk Jaringan Sensor yang Otonom dan Adaptif. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network*, *2*(01).

Fitriansyah, A., & Nugroho, R. A. (2026). *Internet of Things dan Machine Learning*. Minhaj Pustaka.

Ismanto, E., Meidelfi, D., Sukma, F., Lubis, H., Inayah, I., Salma, T. D., Santoso, K. I., Arsyah, U. I., Natsir, F., & Izzatillah, M. (2026). *DEEP LEARNING DI DUNIA NYATA: DARI TEORI KE INOVASI*. Penerbit Widina.

Justam, A. S., Sartika, H. M., Lukman Fanani, M. Z., Nurdzakirah Amir, A. A., Joshua Reska, F., Fitriani, C. D., Alya Rohalia, S., Mawaddah, R., Faturachman, I., & Fadilah, N. (n.d.). *BUKU KECERDASAN ARTIFISIAL (AI) DAN MACHINE LEARNING (ML)*.

Kusumastuti, S. Y., Resty, A., Sari, I. K., Nalurita, F., & Judijanto, L. (2025). *Big Data: Teori dan Penerapan Teknologi Big Data dalam Berbagai Bidang*. PT. Sonpedia Publishing Indonesia.

Lazaros, K., Koumadorakis, D., Vrahatis, A., & Kotsiantis, S. (2024). Federated Learning: Navigating the Landscape of Collaborative Intelligence. *Electronics*. https://doi.org/10.3390/electronics13234744

Mahendra, G. S., Jailani, A. K., Agus, M., Kelvin, K., Sari, P. A. P., Wardani, D. K., & Judijanto, L. (2025). *Smart Computing IoT & Machine Learning*. PT. Sonpedia Publishing Indonesia.

Maruanaya, R. F., Tuhumena, W. A., Kurniawan, E. D. A., Ramli, R. B., Fahmi, N. M., Septian, F. I., Patty, H. W. M., & Dirga, M. F. (2026). *Artificial Intelligence dalam pendidikan: Peluang, etika, dan implikasi pedagogis*. CV. Edu Akademi.

Nguyen, G., Díaz, J. S.-P., Calatrava, A., Berberi, L., Lytvyn, O., Kozlov, V., Tran, V., Moltó, G., & López García, Á. (2024). Landscape of machine learning evolution: privacy-preserving federated learning frameworks and tools. *Artificial Intelligence Review*, *58*. https://doi.org/10.1007/s10462-024-11036-2

Prasetyo, P. C., & Ramadhani, W. (2025). Implementasi Federated Learning Pada Wireless Sensor Network Untuk Deteksi Anomali Terdistribusi. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network*, *1*(01).

Pratama, M. F., Efendi, B., & Nasution, L. N. (2025). Transformasi Digital Ekonomi dalam Mendukung Inklusi Keuangan di Indonesia. *MUQADDIMAH: Jurnal Ekonomi, Manajemen, Akuntansi Dan Bisnis*, *3*(1), 65–85.

Rabbani, Y. I., & Purnama, G. S. (2026). Analisis Literatur Sistematis tentang Algoritma Klasterisasi Dinamis untuk Perpanjangan Masa Pakai WSN. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network*, *2*(01).

Rachman, A., Mumpuni, I. D., Dewa, W. A., Widarti, D. W., Islamiah, F., Kurniawan, E., Paenrongi, A. K. D. I., Mayangsari, M. K., Victory, T., & Wazaumi, D. D. (2025). Big Data dan Manajemen Basis Data Terdistribusi. *Penerbit Mifandi Mandiri Digital*, *1*(02).

Rahmeisi, N., Gani, E., & Arfriandi, A. (2025). Tinjauan Literatur: Pendekatan Machine Learning dalam Deteksi Serangan Web. *Jurnal Ilmiah Sistem Informasi*, *4*(3), 772–791.

Rusdha, S. N., Rahman, F. A., Zam, Z. S. R., Mizan, V. P., Yusuf, F., & Oktarina, R. (2026). Implementasi blockchain dalam keamanan data medis: tinjauan sistematis publish or perish. *Jurnal CoSciTech (Computer Science and Information Technology)*, *7*(1), 112–120.

Sukron, H. S. H., & Rayyan, R. (2025). Kajian Literatur: Isu Keamanan, Energi, dan Skalabilitas pada Wireless Sensor Network. *Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network*, *1*(01).

Tosida, E. T., Harsani, P., & Andria, F. (2026). *Kecerdasan Buatan dalam Bisnis dan Pemerintahan Teori dan Praktik*. PT KIMHSAFI ALUNG CIPTA.

Yanti, H. A., Aulia, I., Fathiyana, R. Z., Sularso, A. N., Ilmi, N., Muttaqin, W., Adidrana, D., Yutia, S. N., Putro, Z. P., & Yafie, H. A. (2025). *ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: FOUNDATIONS, APPLICATIONS, AND FUTURE PERSPECTIVES*. Penerbit Widina.

Yuliyanto, A., & Wijaya, F. (2025). Model Integratif Keamanan dan Privasi pada Sistem AI Generatif di Era Big Data. *JIMU: Jurnal Ilmiah Multidisipliner*, *3*(04).