Federated Learning untuk Deteksi dan Klasifikasi Serangan Jaringan Smart City: Tinjauan Literatur

[1]Rian Nur Ikhsan, [2]Fayruz Rahma, [3]Kurniawan Dwi Irianto
[1,2,3] Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta
email:[1]22523297@students.uii.ac.id, [2]fayruz.rahma@uii.ac.id, k.d.irianto@uii.ac.id

Abstract

The growth of smart cities and the Internet of Things (IoT) has generated massive volumes of sensitive data, creating significant cybersecurity challenges and limitations for centralized machine learning models. Federated Learning (FL) has emerged as a decentralized paradigm that preserves privacy by training models locally on devices. This systematic literature review aims to analyze current trends, challenges, and solutions in applying FL for cybersecurity in smart city environments based on recent publications. The analysis reveals that FL can be effectively implemented in Intrusion Detection Systems (IDS) to detect various types of network attacks. A major universal challenge is the presence of Non-Independent and Identically Distributed (Non-IID) data, which can degrade model performance. The key findings highlight that the most effective implementations of FL are not standalone, but rather hybrid approaches that integrate FL with complementary technologies—such as blockchain to enhance data integrity, adaptive algorithms to handle Non-IID data, and additional privacy-preserving techniques like Differential Privacy and encryption. Overall, the development of frameworks that combine FL with supporting technologies shows strong potential for enhancing the security of smart cities.

Keywords : Federated Learning; Intrusion Detection System (IDS); smart city; literature review

Abstrak

Pertumbuhan *smart city* dan Internet of Things (IoT) menghasilkan volume data sensitif yang masif, menciptakan tantangan keamanan siber yang signifikan sekaligus keterbatasan bagi model *machine learning* terpusat (*centralized*). Federated Learning
(FL) hadir sebagai paradigma desentralisasi yang menjaga privasi dengan melatih model secara lokal di perangkat. Tinjauan literatur sistematis ini bertujuan untuk menganalisis tren, tantangan, dan solusi dalam penerapan FL untuk keamanan siber di lingkungan *smart city* berdasarkan publikasi terkini. Hasil analisis menunjukkan bahwa FL dapat diterapkan pada Intrusion Detection System (IDS) untuk mendeteksi berbagai jenis serangan jaringan. Tantangan universal yang paling sering ditemui adalah data yang tidak identik dan terdistribusi secara independen (Non-Independent and Identically Distributed atau Non-IID), yang dapat menurunkan kinerja model. Temuan utama mengungkapkan bahwa implementasi FL yang optimal bukanlah yang berdiri sendiri, melainkan dengan pendekatan hibrida yang mengintegrasikan FL dengan teknologi pendukung, seperti *blockchain*
untuk menguatkan integritas, algoritma adaptif untuk mengatasi data Non-IID, serta teknik privasi tambahan seperti Differential Privacy
dan enkripsi. Pengembangan kerangka kerja yang mengintegrasikan FL dengan teknologi pendukung menunjukkan potensi dalam meningkatkan keamanan *smart city*.

Kata kunci: *Federated Learning*; Intrusion Detection System (IDS); kota cerdas; kajian literatur.

1. PENDAHULUAN

Dalam kehidupan modern, jumlah perangkat yang terhubung ke internet meningkat pesat, termasuk komponen-komponen penopang *smart city* dan Internet of Things (IoT) seperti layanan lalu lintas, *smart grid*, dan sistem kesehatan. Heterogenitas dan skala perangkat ini menghasilkan akumulasi data sensitif yang besar serta memperluas permukaan serangan (*attack surface*) jaringan sehingga lingkungan *smart city* menjadi rentan terhadap berbagai ancaman siber. Untuk mengatasi ancaman tersebut, teknik *machine learning* banyak diandalkan sebagai solusi deteksi dan klasifikasi intrusi jaringan karena kemampuannya mempelajari pola serangan dari data. Namun, pendekatan pembelajaran mesin yang bersifat terpusat (data lokal dikumpulkan ke server pusat untuk pelatihan) menghadapi keterbatasan terkait skalabilitas dan privasi karena memerlukan *bandwidth* besar untuk mengirim data. Selain itu, terdapat risiko terjadinya kebocoran informasi sensitif saat agregasi data ke pusat dilakukan (Bodagala & H, 2022).

Federated Learning (FL) hadir sebagai pendekatan desentralisasi yang memungkinkan pelatihan model global secara kolaboratif di berbagai perangkat tanpa memindahkan data lokal ke server pusat. Pendekatan ini sejalan dengan prinsip *privacy by design*, karena data sensitif tetap berada pada perangkat masing-masing dan hanya parameter atau pembaruan model yang dikirimkan untuk agregasi. Selain itu, FL dapat mengurangi beban komunikasi dan konsumsi *bandwidth* dibandingkan pelatihan terpusat, mengurangi *overhead* komunikasi, serta memungkinkan perangkat yang heterogen untuk berkolaborasi membangun model deteksi yang lebih tangguh tanpa harus berbagi data milik pihak terkait (Al-Huthaifi, Li, Huang, Gu, & Li, 2023).

Tinjauan literatur ini bertujuan untuk menganalisis tren, tantangan, dan solusi dalam penerapan FL untuk Intrusion Detection System (IDS) pada lingkungan *smart city*. Tinjauan ini penting karena *smart city* mengelola infrastruktur kritikal dan data sensitif warga sehingga solusi deteksi intrusi harus memenuhi kebutuhan keamanan, privasi, dan skalabilitas secara simultan. Selain itu, heterogenitas perangkat dan sifat data yang Non-Independent and Identically Distributed (Non-IID) menimbulkan tantangan teknis yang memerlukan evaluasi menyeluruh terhadap metode FL yang ada. Dengan merangkum perkembangan penelitian, tinjauan ini diharapkan dapat menjadi acuan bagi peneliti dan praktisi dalam merancang sistem IDS berbasis FL yang lebih aman, efisien, dan layak diterapkan di konteks *smart city*.

2. KERANGKA TEORI

2.1. Konsep Dasar Federated Learning

Federated Learning (FL) merupakan paradigma pembelajaran mesin yang berbeda dari pendekatan tradisional. Pada metode konvensional, data dari semua sumber dikumpulkan dan dipusatkan di satu server untuk proses pelatihan model. Sebaliknya, dalam FL, yang didistribusikan ke klien-klien lokal (seperti perangkat seluler atau sensor) adalah model global itu sendiri, bukan datanya. Data tetap berada di perangkat asal sehingga privasi tetap terjaga.

2.2. Tahapan Utama Federated Learning

Proses inti FL terdiri dari tiga tahapan utama:

1. **Inisiasi & Distribusi**. Pada tahap inisiasi, server pusat membangun model global, yang berupa *neural network* (jaringan syaraf), sebagai kerangka dasar untuk *learning model*. Seluruh parameter atau bobot model diinisialisasi dengan nilai acak atau strategi tertentu, menyediakan titik awal yang konsisten untuk seluruh proses. Inisialisasi yang tepat sangat krusial untuk memastikan stabilitas konvergensi model dan menghindari masalah selama *training*.
   Selanjutnya, server mendistribusikan model beserta *initial parameter* ini ke subset klien yang terpilih. Distribusi ini menempatkan semua perangkat pada kondisi awal yang identik. Ini merupakan prasyarat fundamental agar *training* mandiri yang dihasilkan nanti dapat digabungkan secara efektif oleh server untuk membentuk iterasi model global yang akan datang.

2. **Pelatihan Lokal**. Setiap klien yang terpilih akan melakukan proses pelatihan lokal secara independen menggunakan dataset ataupun log pribadi yang tersimpan di perangkat masing-masing. Pada fase ini, data mentah, seperti log perangkat, sama sekali tidak meninggalkan lingkungan lokal klien sehingga privasi dan keamanan data dapat terjaga secara inheren.
   Hasil dari pelatihan berupa *updates model* (model pembaruan) yang merepresentasikan pengetahuan yang telah dipelajari. Pembaruan ini dapat berupa himpunan gradien yang dihitung selama pelatihan ataupun langsung berupa set parameter baru yang telah diperbarui. Kumpulan vektor ini yang kemudian akan dikirim kembali ke server pusat sehingga data pelatihan tetap ada di lokal dan tidak terekspos selama komunikasi.

3. **Agregasi**. Setelah menyelesaikan pelatihan lokal, setiap klien mengirimkan hasil *updates model* (model pembaruan) yang berupa vektor parameter ataupun gradien ke server pusat. Penting untuk ditekankan bahwa yang ditransfer hanyalah hasil komputasi dari *local learning*, bukan data mentah yang digunakan selama pelatihan sehingga dapat mempertahankan privasi data pada sumber lokal.
   Di sisi server, semua pembaruan yang diterima dari berbagai klien kemudian dikumpulkan dan digabungkan melalui sebuah proses agregasi. Algoritma yang paling umum digunakan untuk tujuan ini adalah Federated Averaging (FedAvg), yang pada dasarnya melakukan rata-rata tertimbang (*weighted average*) dari parameter-parameter model yang dikirim oleh klien, dengan bobot yang sering kali proporsional terhadap jumlah data pelatihan masing-masing klien. Hasil dari agregasi ini adalah sebuah model global baru yang telah menginkorporasikan pengetahuan yang dipelajari secara kolektif dari semua klien.

Siklus yang terdiri dari distribusi model, pelatihan lokal, dan agregasi ini kemudian diulang secara iteratif dalam banyak putaran (*rounds*). Dengan setiap iterasi, model global secara bertahap meningkat keakuratannya dan keandalannya. Model global belajar dari kumpulan data yang terdistribusi dan heterogen tanpa pernah memusatkan atau memindahkan data mentah itu sendiri. Dengan demikian, proses ini mengatasi tantangan privasi dan *bandwidth* yang melekat pada pendekatan terpusat tradisional.

3. METODOLOGI

Metode yang digunakan dalam penelitian ini adalah tinjauan literatur sistematis. Tujuannya adalah untuk mengidentifikasi tren, tantangan, dan solusi utama dalam penerapan FL untuk keamanan *smart city* berdasarkan publikasi empat tahun terakhir (2022-2025). Prosedur tinjauan literatur sistematis ini dibagi menjadi dua tahapan utama untuk memastikan kelengkapan dan akurasi analisis.

3.1. Pengumpulan Studi

Tahap pertama adalah pengumpulan literatur yang relevan dari database terkemuka, seperti IEEE Xplore dan ScienceDirect (Elsevier). Terdapat beberapa kriteria pemilihan, yaitu:

1. Topik tentang keamanan jaringan, seperti IDS, deteksi DDoS, atau deteksi anomali.
2. Artikel fokus pada penerapan FL.
3. Konteks aplikasi dalam lingkungan IoT atau *smart city*.
4. Dipublikasikan dalam kurun waktu empat tahun terakhir (2022-2025).

3.2. Sintesis dan Analisis Materi

Setelah literatur terkumpul, setiap studi dianalisis secara mendalam. Data yang telah diekstrak dari literatur dimasukkan ke dalam sebuah matriks tinjauan terperinci dalam bentuk tabel-tabel. Dari matriks inilah dilakukan sintesis untuk menemukan pola-pola yang muncul, seperti:

1. Area fokus riset dalam penerapan FL untuk keamanan *smart city*
2. Metode FL yang digunakan
3. *Machine learning* yang digunakan pada penerapan FL
4. Tren teknologi pendamping FL
5. Tantangan dan solusi dalam penerapan FL

4. HASIL DAN PEMBAHASAN

Analisis terhadap kumpulan studi literatur yang telah dikaji menunjukkan beberapa tren dalam penerapan FL untuk keamanan *smart city*.

4.1. Area Fokus Riset

Berdasarkan makalah-makalah yang dikaji, fokus riset FL dalam area keamanan jaringan pada *smart city* dapat dikelompokkan ke dalam empat bidang utama (Tabel 1). Pertama, penelitian yang mengarah pada penerapan FL untuk deteksi intrusi dan anomali, termasuk deteksi serangan jaringan seperti Intrusion Detection System (IDS). Pendekatan ini memanfaatkan kemampuan FL untuk melatih model deteksi secara terdistribusi dari beragam perangkat jaringan tanpa perlu memusatkan data sensitif. Fokus penelitian kedua adalah penggunaan FL dalam manajemen aplikasi *smart city*, seperti sistem transportasi, pengelolaan energi, layanan kesehatan, dan berbagai layanan publik lainnya. Fokus ketiga berkaitan dengan pengembangan pendekatan yang bertujuan meningkatkan keamanan dan privasi dalam implementasi FL. Tantangan seperti serangan terhadap parameter model ketika transmisi, ketidakpercayaan antar *node*, serta sifat data yang non-IID mendorong penelitian pada dukungan teknologi seperti *blockchain* untuk mekanisme konsensus, enkripsi untuk melindungi parameter model selama komunikasi, dan skema *trusted execution.* Fokus terakhir adalah penelitian berupa *framework* umum atau survei mengenai penerapan FL itu sendiri.

Tabel 1. Klasifikasi Studi Berdasarkan Fokus Aplikasi dan Teknologi

No.	Fokus Riset	Referensi
1	Deteksi Intrusi & Anomali (IDS)	(Bodagala & H, 2022), (Ahmadi & Javidan, 2023), (Aborokbah, 2024), (Thantharate & T, 2024), (Olanrewaju-George & Pranggono, 2025), (Djenouri & Belbachir, 2023), (Thakur, et al., 2024), (Bhardwaj, Shekhar, & Saini, 2023), (Hamid & Bawany, 2024)
2	Manajemen Aplikasi Smart City (Lalu Lintas, Energi, Healthcare, dll.)	(Samantray & Reddy, 2025), (Al-Huthaifi, et al., 2024), (Sharma, Seetharaman, BD, & Khangaonkar, 2023), (Khan, et al., 2025), (Akbar, Ullah, Malik, & Qaisar, 2025), (Khatua, De, Maji, Maity, & Nielsen, 2024)
3	Peningkatan Privasi & Keamanan FL (Blockchain, Enkripsi, Trust, Solusi Non-IID)	(Sumitra, Sharma, & Shenoy, 2024), (Wang, Chen, Han, & Zhu, 2024), (Hijazi, Aloqaily, Guizani, Ouni, & Karray, 2024), (Wang, et al., 2025), (Rasti-Meymandi, Sajedi, & Plataniotis, 2025), (Abdel-Basset, Hawash, Moustafa, Razzak, & Elfattah, 2024), (Wehbi, et al., 2025)
4	Framework Umum	(Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Diba, et al., 2025), (Ramu, et al., 2022)

4.2. Metode FL

Berdasarkan makalah-makalah yang dikaji, metode FL dapat diklasifikasikan ke dalam empat kelompok utama (Tabel 2). Kategori pertama mencakup algoritma dasar dan umum yang menjadi fondasi pelatihan kolaboratif pada FL. Pendekatan dalam kelompok ini umumnya berfokus pada mekanisme agregasi standar, seperti Federated Averaging (FedAvg), yang menggabungkan pembaruan model dari berbagai klien menjadi model global secara iteratif. Kategori kedua adalah metode FL yang dikombinasikan dengan mekanisme privasi dan keamanan. Pendekatan ini dirancang untuk mengatasi risiko serangan terhadap parameter model maupun potensi kebocoran informasi selama proses komunikasi. Kategori ketiga adalah algoritma lanjutan yang ditujukan untuk mengatasi tantangan sifat data non-IID serta kebutuhan personalisasi model bagi masing-masing klien. Kategori keempat mencakup arsitektur hibrida dan pendekatan lainnya yang memperluas fleksibilitas penerapan FL.

Tabel 2. Klasifikasi Studi Berdasarkan Metode Federated Learning

No.	Metode *Federated Learning*	Referensi
1	Algoritma Dasar & Umum	(Bodagala & H, 2022), (Thantharate & T, 2024), (Thakur, et al., 2024), (Diba, et al., 2025), (Hamid & Bawany, 2024)
2	Kombinasi dengan Privasi/Keamanan	(Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Sumitra, Sharma, & Shenoy, 2024), (Wang, Chen, Han, & Zhu, 2024), (Samantray & Reddy, 2025), (Djenouri & Belbachir, 2023), (Hijazi, Aloqaily, Guizani, Ouni, & Karray, 2024), (Abdel-Basset, Hawash, Moustafa, Razzak, & Elfattah, 2024), (Wehbi, et al., 2025), (Al-Huthaifi, et al., 2024), (Sharma, Seetharaman, BD, & Khangaonkar, 2023), (Akbar, Ullah, Malik, & Qaisar, 2025)
3	Algoritma Lanjutan (Non-IID & Personalisasi)	(Olanrewaju-George & Pranggono, 2025), (Wang, et al., 2025), (Rasti-Meymandi, Sajedi, & Plataniotis, 2025)
4	Arsitektur Hibrida & Lainnya	(Ahmadi & Javidan, 2023), (Aborokbah, 2024), (Ramu, et al., 2022), (Khan, et al., 2025), (Bhardwaj, Shekhar, & Saini, 2023), (Khatua, De, Maji, Maity, & Nielsen, 2024)

4.3. Algoritma Model Machine Learning

Berdasarkan makalah-makalah yang dianalisis, FL diimplementasikan menggunakan beragam algoritma model *machine learning* (Tabel 3), tergantung pada karakteristik data, tujuan analisis, dan skenario penerapannya. Mayoritas penelitian memanfaatkan model berbasis Deep Neural Network (DNN), termasuk arsitektur Convolutional Neural Network (CNN) dan Recurrent Neural Network (RNN), karena kemampuannya dalam mempelajari representasi fitur kompleks dan menangani data berskala besar secara efektif. Selain itu, beberapa studi memanfaatkan pendekatan berbasis graf seperti Graph Neural Network (GNN) maupun Graph Ordinary Differential Equation (GODE) untuk memodelkan hubungan antarentitas dalam struktur data. Pendekatan *unsupervised* seperti *autoencoder* juga digunakan, terutama dalam deteksi anomali, karena mampu mengekstraksi pola dari data tanpa memerlukan label eksplisit. Pada sisi lain, metode *machine learning* klasik, seperti algoritma berbasis pohon keputusan dan variannya, tetap digunakan pada beberapa studi lainnya. Selain itu, sebagian kecil studi menerapkan *reinforcement learning*.

Tabel 3. Klasifikasi Studi Berdasarkan Algoritma Model Machine Learning yang Dipakai dalam Implementasi FL

No.	Algoritma Model *Machine Learning*	Referensi
1	DNN/CNN/RNN	(Bodagala & H, 2022), (Sumitra, Sharma, & Shenoy, 2024), (Wang, Chen, Han, & Zhu, 2024), (Samantray & Reddy, 2025), (Ahmadi & Javidan, 2023), (Thantharate & T, 2024), (Olanrewaju-George & Pranggono, 2025), (Djenouri & Belbachir, 2023), (Hijazi, Aloqaily, Guizani, Ouni, & Karray, 2024), (Thakur, et al., 2024), (Wang, et al., 2025), (Rasti-Meymandi, Sajedi, & Plataniotis, 2025), (Abdel-Basset, Hawash, Moustafa, Razzak, & Elfattah, 2024), (Sharma, Seetharaman, BD, & Khangaonkar, 2023), (Bhardwaj, Shekhar, & Saini, 2023)
2	*Graph-based* (GNN, GODE)	(Aborokbah, 2024), (Al-Huthaifi, et al., 2024)
3	*Unsupervised* (Autoencoder)	(Olanrewaju-George & Pranggono, 2025)
4	*Machine Learning* Klasik (t*ree-based*, dll.)	(Thakur, et al., 2024), (Wehbi, et al., 2025), (Khan, et al., 2025), (Bhardwaj, Shekhar, & Saini, 2023)
5	*Reinforcement Learning*	(Wang, et al., 2025), (Akbar, Ullah, Malik, & Qaisar, 2025)

4.4. Tren Teknologi Pendamping Federated Learning

Beberapa studi mengintegrasikan FL dengan teknologi lain untuk membentuk sistem yang lebih komprehensif. Kombinasi teknologi yang telah ditemukan antara lain:

- **FL + Blockchain**. Kombinasi ini sangat populer untuk meningkatkan keamanan. FL menangani privasi data, sementara Blockchain menjamin integritas, auditabilitas, dan desentralisasi proses agregasi (Wang, Chen, Han, & Zhu, 2024), (Samantray & Reddy, 2025), (Sharma, Seetharaman, BD, & Khangaonkar, 2023).
- **FL + Edge/Fog Computing**. Perangkat IoT seringkali memiliki kemampuan komputasi yang terbatas sehingga data diproses di *edge node* terdekat. *Edge node* inilah yang kemudian bertindak sebagai klien dalam arsitektur FL (Abdel-Basset, Hawash, Moustafa, Razzak, & Elfattah, 2024), (Ramu, et al., 2022).
- **FL + XAI (Explainable AI)**. Teknologi FL dapat menjaga privasi, tetapi model *machine learning* seringkali dianggap sebagai "kotak hitam" (*blackbox*). XAI (dengan teknik seperti LIME dan SHAP) digunakan untuk membuat keputusan model menjadi transparan dan dapat dipercaya oleh pengguna (Khan, et al., 2025).
- **FL + Reinforcement Learning (RL)**. Pendekatan ini digunakan dalam skenario kontrol yang dinamis. Contohnya adalah Federated Multi-Agent RL (FMARL) untuk optimasi sinyal lalu lintas (Akbar, Ullah, Malik, & Qaisar, 2025) atau penggunaan *proximal policy optimization* (PPO) untuk seleksi *node* FL (Wang, et al., 2025).

4.5. Tantangan dan Solusi dalam Implementasi FL

Analisis literatur mengidentifikasi dua kategori tantangan utama dalam implementasi FL untuk keamanan *smart city*, yaitu heterogenitas data (Non-IID) dan kerentanan keamanan model FL itu sendiri.

1. **Data Non-IID.** Tantangan terbesar dan paling sering disebutkan dalam literatur adalah masalah data Non-Independent and Identically Distributed (Non-IID) (Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Sumitra, Sharma, & Shenoy, 2024), (Wang, et al., 2025), (Diba, et al., 2025), (Rasti-Meymandi, Sajedi, & Plataniotis, 2025), (Abdel-Basset, Hawash, Moustafa, Razzak, & Elfattah, 2024). Data pada setiap perangkat IoT atau node *smart city* bersifat unik. Misalnya, data dari kamera lalu lintas sangat berbeda dengan data dari *smart meter*. Algoritma FL standar, seperti FedAvg, kinerjanya menurun dalam skenario ini (Olanrewaju-George & Pranggono, 2025). Beberapa solusi yang diusulkan untuk mengatasi hal ini antara lain:
    a. Menggunakan algoritma FL yang secara spesifik dirancang untuk data Non-IID, seperti FedProx (Wang, et al., 2025).
    b. Mengoptimasi proses agregasi; tidak dengan rata-rata sederhana, tetapi menggunakan bobot berdasarkan reputasi klien (Wehbi, et al., 2025).
    c. Menerapkan seleksi klien yang cerdas, misalnya dengan *reinforcement learning* (Wang, et al., 2025).
    d. Menggunakan Personalized FL (PFL) (Rasti-Meymandi, Sajedi, & Plataniotis, 2025), di mana setiap klien mendapatkan model yang disesuaikan dengan karakteristik data lokalnya.

2. **Ancaman Privasi**. Meskipun dirancang dengan prinsip *privacy by design*, FL tidak sepenuhnya kebal terhadap ancaman. Model FL masih rentan terhadap serangan baru, seperti:
    a. *Gradient Leakage Attacks* (GLA). Pihak penyerang dapat mencoba merekayasa balik data mentah dari gradien model yang dikirimkan oleh klien (Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Sumitra, Sharma, & Shenoy, 2024).
    b. *Poisoning Attacks*. Klien jahat dapat mengirimkan pembaruan model palsu (*poisoned*) untuk merusak akurasi model global (Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Wehbi, et al., 2025).

    Untuk menanggulangi ancaman ini, beberapa solusi "pelapis" telah dikembangkan. Yang paling umum adalah:
    - **Enkripsi**; dapat dilakukan menggunakan Fully Homomorphic Encryption (FHE) agar server dapat mengagregasi model tanpa dekripsi (Hijazi, Aloqaily, Guizani, Ouni, & Karray, 2024), atau bahkan Quantum-Key-Encryption (Samantray & Reddy, 2025).
    - **Differential Privacy**; yaitu dengan menambahkan "*noise*" statistik pada pembaruan gradien agar kontribusi satu klien tidak dapat dibedakan (Al-Huthaifi, Li, Huang, Gu, & Li, 2023), (Sumitra, Sharma, & Shenoy, 2024), (Al-Huthaifi, et al., 2024).
    - **Blockchain**; berfungsi sebagai buku besar terdesentralisasi untuk mencatat pembaruan model dan mengelola reputasi klien, sangat efektif untuk melawan serangan *poisoning* (Wang, Chen, Han, & Zhu, 2024), (Samantray & Reddy, 2025), (Sharma, Seetharaman, BD, & Khangaonkar, 2023).

5. KESIMPULAN

Tinjauan literatur ini menunjukkan bahwa pendekatan FL memiliki potensi dalam pengamanan jaringan *smart city* karena memungkinkan deteksi ancaman secara kolaboratif tanpa memindahkan data dari sumbernya sehingga privasi tetap terjaga. Tantangan utama yang dihadapi terutama terkait heterogenitas data (Non-IID) dan efisiensi komunikasi, yang kini mulai diatasi melalui algoritma-algoritma baru, seperti seleksi klien adaptif dan pendekatan PFL. Tren terbaru juga menegaskan bahwa FL lebih efektif ketika diterapkan dalam arsitektur hibrida, misalnya dikombinasikan dengan *blockchain* untuk menjamin kepercayaan dan integritas proses, Differential Privacy untuk perlindungan data tambahan, serta *edge computing* untuk menurunkan latensi. Ke depannya, penelitian dapat diarahkan pada optimalisasi integrasi berbagai teknologi pendukung tersebut, peningkatan aspek Explainability (XAI), serta pengembangan kemampuan FL yang tertanam secara *native* dalam ekosistem komputasi masa depan seperti 6G dan *edge computing*.

UCAPAN TERIMA KASIH

Terima kasih kepada Jurusan Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, atas dukungannya dalam publikasi makalah ilmiah ini.

DAFTAR PUSTAKA

Abdel-Basset, M., Hawash, H., Moustafa, N., Razzak, I., & Elfattah, M. A. (2024). Privacy-preserved learning from non-i.i.d data in fog-assisted IoT: A federated learning approach. *Digital Communications and Networks*, 404-415. doi:https://doi.org/10.1016/j.dcan.2022.12.013

Aborokbah, M. M. (2024). A Novel Intrusion Detection Model for Enhancing Security in Smart City. *IEEE Access*, 107431-107444. doi:https://doi.org/10.1109/ACCESS.2024.3438619

Ahmadi, K., & Javidan, R. (2023). DDoS Attack Detection in a Real Urban IoT Environment Using Federated Deep Learning. *2023 IEEE International Conference on Cyber Security and Resilience (CSR).* Venice, Italy: IEEE Xplore. doi:https://doi.org/10.1109/CSR57506.2023.10224916

Akbar, A., Ullah, S. S., Malik, A., & Qaisar, S. M. (2025). RT-FedFlow: An efficient framework for real-time traffic signal optimization using federated multi-agent reinforcement learning. *Engineering Applications of Artificial Intelligence*. doi:https://doi.org/10.1016/j.engappai.2025.112147

Al-Huthaifi, R., Li, T., Al-Huda, Z., Huang, W., Luo, Z., & Xie, P. (2024). FedGODE: Secure traffic flow prediction based on federated learning and graph ordinary differential equation networks. *Knowledge-Based Systems*. doi:https://doi.org/10.1016/j.knosys.2024.112029

Al-Huthaifi, R., Li, T., Huang, W., Gu, J., & Li, C. (2023). Federated learning in smart cities: Privacy and security survey. *Information Sciences*, 833-857. doi:https://doi.org/10.1016/j.ins.2023.03.033

Bhardwaj, V., Shekhar, & Saini, R. K. (2023). Federated Learning for Getting the IoT Arrangement of Smart City Against Digital Threats. *2023 11th International Conference on Intelligent Systems and Embedded Design (ISED).* Dehradun, India: IEEE Xplore. doi:https://doi.org/10.1109/ISED59382.2023.10444590

Bodagala, H., & H, P. (2022). Security for IoT using Federated Learning. *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC).* Hyderabad, India: IEEE Xplore. doi:https://doi.org/10.1109/ICMACC54824.2022.10093557

Diba, B. S., Plabon, J. D., Mowla, T. J., Nahar, N., Mistry, D., Sarker, S., . . . Shin, J. (2025). Open problems and challenges in federated learning for IoT: A comprehensive review and strategic guide. *Computers and Electrical Engineering*. doi:https://doi.org/10.1016/j.compeleceng.2025.110515

Djenouri, Y., & Belbachir, A. N. (2023). Empowering Urban Connectivity in Smart Cities using Federated Intrusion Detection. *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA).* Thessaloniki, Greece: IEEE Xplore. doi:https://doi.org/10.1109/DSAA60987.2023.10302528

Hamid, S., & Bawany, N. Z. (2024). Federated Learning for Enhanced Intrusion Detection in Smart City Environments. *2024 18th International Conference on Open Source Systems and Technologies (ICOSST).* Lahore, Pakistan: IEEE Xplore. doi:https://doi.org/10.1109/ICOSST64562.2024.10871154

Hijazi, N. M., Aloqaily, M., Guizani, M., Ouni, B., & Karray, F. (2024). Secure Federated Learning With Fully Homomorphic Encryption for IoT Communications. *IEEE Internet of Things Journal*, 4289-4300. doi:https://doi.org/10.1109/JIOT.2023.3302065

Khan, M. A., Farooq, M. S., Saleem, M., Shahzad, T., Ahmad, M., Abbas, S., & Abu-Mahfouz, A. M. (2025). Smart buildings: Federated learning-driven secure, transparent and smart energy management system using XAI. *Energy Reports*, 2066-2081. doi:https://doi.org/10.1016/j.egyr.2025.01.063

Khatua, S., De, D., Maji, S., Maity, S., & Nielsen, I. E. (2024). A federated learning model for integrating sustainable routing with the Internet of Vehicular Things using genetic algorithm. *Decision Analytics Journal*. doi:https://doi.org/10.1016/j.dajour.2024.100486

Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. *Cyber Security and Applications*. doi:https://doi.org/10.1016/j.csa.2024.100068

Ramu, S. P., Boopalan, P., Pham, Q.-V., Maddikunta, P. K., Huynh-The, T., Alazab, M., . . . Gadekallu, T. R. (2022). Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustainable Cities and Society*. doi:https://doi.org/10.1016/j.scs.2021.103663

Rasti-Meymandi, A., Sajedi, A., & Plataniotis, K. N. (2025). FedPnP: Personalized graph-structured federated learning. *Pattern Recognition*. doi:https://doi.org/10.1016/j.patcog.2025.111455

Samantray, B. S., & Reddy, K. H. (2025). A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities. *Blockchain: Research and Applications*. doi:https://doi.org/10.1016/j.bcra.2025.100385

Sharma, V., Seetharaman, T., BD, V., & Khangaonkar, A. M. (2023). Blockchain and Federated Learning Enabled Smart Traffic Management System for Smart Cities. *2023 4th International Conference on Intelligent Engineering and Management (ICIEM).* London, United Kingdom: IEEE Xplore. doi:https://doi.org/10.1109/ICIEM59379.2023.10167236

Sumitra, Sharma, J., & Shenoy, M. V. (2024). HAFedL: A Hessian-Aware Adaptive Privacy Preserving Horizontal Federated Learning Scheme for IoT Applications. *IEEE Access*, 126738-126753. doi:https://doi.org/10.1109/ACCESS.2024.3454074

Thakur, A., Tyagi, R., Tripathy, H. K., Yang, T., Rathore, R. S., Mo, D., & Wang, L. (2024). Detecting Network Attack using Federated Learning for IoT Devices. *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS).* Hassan, India: IEEE Xplore. doi:https://doi.org/10.1109/IACIS61494.2024.10721980

Thantharate, P., & T, A. (2024). CYBRIA - Pioneering Federated Learning for Privacy-Aware Cybersecurity with Brilliance. *2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET).* Boca Raton, FL, USA: IEEE Xplore. doi:https://doi.org/10.1109/HONET59747.2023.10374608

Wang, S., Chen, C., Han, B., & Zhu, J. (2024). A Trusted and Decentralized Federated Learning Framework for IoT devices in Smart City. *2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics.* Copenhagen, Denmark: IEEE Xplore. doi:https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics62450.2024.00029

Wang, W., Li, P., Li, S., Zhang, J., Zhou, Z., Wu, D. O., . . . Gong, P. (2025). Optimizing Proximity Strategy for Federated Learning Node Selection in the Space-Air–Ground Information Network for Smart Cities. *IEEE Internet of Things Journal*, 6418-6430. doi:https://doi.org/10.1109/JIOT.2024.3416943

Wehbi, O., Arisdakessian, S., Guizani, M., Wahab, O. A., Mourad, A., Otrok, H., . . . Ouni, B. (2025). Enhancing Mutual Trustworthiness in Federated Learning for Data-Rich Smart Cities. *IEEE Internet of Things Journal*, 3105-3117. doi:https://doi.org/10.1109/JIOT.2024.3476950