Perancangan *Federated Learning* Berbasis *Homomorphic Encryption* untuk Perangkat *Internet of Things*

Yuris Mulya Saputra[1], Ganjar Alfian[1,*], Muhammad Qois Huzyan Octava[1]
[1]Departemen Teknik Elektro dan Informatika, Sekolah Vokasi, Universitas Gadjah Mada;
ym.saputra@ugm.ac.id
qoisoctava@mail.ugm.ac.id
[*]Korespondensi: ganjar.alfian@ugm.ac.id;

Abstract – The growth of big data market for intelligence-based Internet-of-Things (IoT) users has attracted both industry and academia. Through using local data from various IoT devices, the service provider can produce valuable information for its users via maching learning (ML) such as centralized learning with a cloud server and local learning with the IoT devices. However, due to privacy leakage risk when the IoT users send the local data to the cloud server and limited computation resources of IoT devices, federated learning (FL) can be the efficient solution to solve the above problems. FL approach is a collaborative ML in which each IoT device can first conduct the individual training process and then share the local model only to the cloud server without data sharing. In this case, this approach can not only improve the training process performance, but also protect data privacy for the IoT users. This research focuses on FL system design with privacy-awareness for IoT users. Particularly, a homomorphic encryption based-encryption method is used to encrypt data from IoT devices during the local training process of the FL as the data privacy protection fom IoT malicious attackers. From this research, we can analyze the model accuracy performance between FL without and with the above encryption method.

Keywords – Federated Learning, Data Privacy, Encryption, IoT, Artificial Intelligence

Intisari – Semakin berkembangnya pasar *big data* yang digunakan oleh pengguna khususnya *Internet of Things* (IoT) berbasis kecerdasan buatan telah menarik banyak pihak baik dari industri maupun akademisi. Melalui penggunaan data lokal dari berbagai perangkat IoT, pemberi layanan aplikasi dapat menghasilkan informasi berguna melalui pendekatan *machine learning* (ML) seperti *centralized learning* dengan menggunakan *cloud server* dan *local learning* pada perangkat IoT langsung. Namun, dengan adanya risiko bocornya privasi pengguna ketika mengirim data lokal ke *cloud server* dan sumber daya komputasi yang terbatas pada IoT, penggunaan *federated learning* (FL) dapat menjadi solusi efisien. Pendekatan FL merupakan sebuah pendekatan ML kolaboratif di mana setiap perangkat IoT dapat melakukan proses *training* secara independen dan kemudian hanya mengirimkan model *local* kepada *cloud server* tanpa melakukan *data sharing*. Secara khusus, penggunaan FL untuk layanan aplikasi pada perangkat IoT tidak hanya memperbaiki kinerja untuk proses *training*, namun juga dapat melindungi privasi data bagi penggunanya. Penelitian ini berfokus pada perancangan sistem FL dengan *privacy-awareness* yang dapat digunakan oleh para pengguna perangkat IoT. Dalam hal ini, teknik enkripsi yang berbasis *homomorphic encryption* untuk mengenkripsi data dari perangkat IoT ketika proses *training* dari FL dapat diimplementasikan sebagai bentuk perlindungan privasi pengguna IoT dari *malicious attackers*. Dari penelitian ini, dapat dianalisis perbandingan tingkat akurasi model dari berbagai pendekatan baik tanpa dan dengan teknik enkripsi tersebut.

Kata kunci – *Federated Learning*, Keamanan Data, Enkripsi, IoT, Kecerdasan Buatan

I. PENDAHULUAN

Kebutuhan yang tinggi terhadap penggunaan *big data* untuk berbagai macam aplikasi yang berbasis kecerdasan buatan (misalnya untuk layanan kesehatan, *crowdsensing*, dan aplikasi jaringan yang menggunakan pendekatan *machine learning)* saat ini menjadi topik hangat untuk revolusi teknologi internet pada masa yang akan datang [1]. Hal ini didasari oleh adanya pandemi COVID-19 di mana masyarakat harus beradaptasi untuk bekerja dari rumah, sehingga menghasilkan data internet yang sangat besar untuk proses analisis khususnya ketika masyarakat secara umum menggunakan perangkat *mobile*. Dalam hal ini, informasi data yang disimpan dari perangkat *mobile* seperti *smartphone*, *smartwatch*, dan perangkat IoT selanjutnya dapat digunakan untuk membantu pemberi layanan dalam membuat layanan aplikasi dengan tingkat akurasi yang tinggi. Berdasarkan *Allied Market Research* dalam hal pasar *big data*, perkembangan layanan *big data* secara global pada Tahun 2030 akan meningkat lebih dari 3 kali lipat dari Tahun 2020 baik dalam hal perangkat lunak, perangkat keras, dan layanan data disebabkan kebutuhan tinggi pengguna terhadap kecerdasan buatan [2].

Adanya kebutuhan yang tinggi terhadap kecerdasan buatan memberikan motivasi terhadap pemberi layanan aplikasi untuk dapat mengumpulkan data dari berbagai perangkat pengguna khususnya perangkat IoT (*embedded sensors*) untuk keperluan ekstraksi informasi yang berguna melalui pemanfaatan *machine learning* (ML). Hal ini dapat dilakukan melalui *centralized learning* di mana semua data dari pengguna IoT akan diproses di *cloud server*, serta *local learning* di mana perangkat IoT pengguna akan memproses data lokal sendiri tanpa adanya *cloud server* [3, 4]. Namun, ada dua tantangan utama ketika dua hal tersebut dilakukan. Pertama, pengguna IoT mungkin tidak ingin melakukan *data sharing* yang disebabkan oleh risiko bocornya privasi pengguna ketika mengirim data lokal ke *cloud server*. Kedua, perangkat IoT biasanya memiliki data lokal yang tidak banyak dan sumber daya komputasi yang terbatas secara inheren,

sehingga penggunaan perangkat IoT untuk proses ML akan mengakibatkan kualitas *training* yang tidak efektif dan tingkat akurasi yang rendah.

Federated learning telah dianggap sebagai pendekatan yang sangat efektif untuk mengatasi dua tantangan tersebut seperti yang ditampilkan. Dengan menggunakan FL, proses *training* dapat dilakukan oleh banyak perangkat IoT tanpa adanya *data sharing* yang mungkin mengandung informasi pribadi pengguna [5, 6]. Secara spesifik, setiap perangkat IoT dapat melakukan proses *training* dengan menggunakan data lokal serta sumber daya komputasinya untuk menghasilkan sebuah model *training* lokal secara independen. Kemudian, pemberi layanan aplikasi atau *cloud server* dapat meminta setiap perangkat IoT yang berpartisipasi untuk mengirimkan model lokal tersebut untuk memperbarui model global yang nantinya dapat digunakan untuk ekstraksi informasi berguna bagi seluruh pengguna IoT.

Akan tetapi penggunaan FL secara konvensional masih dapat membuat data pribadi pengguna IoT bocor (walaupun proses *training* dilakukan secara lokal) ketika model lokal dikirimkan ke *cloud server*. Untuk mengatasi hal tersebut sebelum proses *training* dilakukan, sebuah teknik enkripsi tanpa harus melakukan deskripsi terhadap data dan model lokal serta dapat melakukan operasi matematis seperti perkalian dapat diimplementasikan.

Tujuan dan kontribusi yang ingin dicapai melalui penelitian ini yaitu 1) membuat rancangan bangun sistem keamanan *big data* berbasis kecerdasan buatan melalui pendekatan *federated learning* (FL) yang sederhana dengan menggunakan perangkat IoT dari pengguna; dan 2) memberikan nilai kemudahan dalam melindungi data pengguna IoT dengan menggunakan teknik enkripsi tingkat lanjut berupa *fully homomorphic encryption* (FHE) ketika terjadi komunikasi antar perangkat IoT pada proses *training* untuk menghasilkan informasi yang berguna. Batasan masalah yang terdapat dalam penelitian ini yaitu rancang bangun FL dibatasi pada metode *logistic regression* dengan klasifikasi biner pada dataset yang digunakan.

II. DASAR TEORI

Adanya kebutuhan yang tinggi terhadap kecerdasan buatan memberikan motivasi terhadap pemberi layanan aplikasi untuk dapat mengumpulkan data dari berbagai perangkat IoT (*embedded sensors*) untuk keperluan ekstraksi informasi yang berguna melalui pemanfaatan *machine learning* (ML). Pada umumnya, hal ini dapat dilakukan melalui *centralized learning (CL)* di mana semua data dari pengguna IoT akan diproses di *cloud server* [3, 7, 8, 9, 10]. Namun, melalui metode di atas, pengguna IoT mungkin tidak ingin melakukan *data sharing* yang disebabkan oleh risiko bocornya privasi pengguna ketika mengirim data lokal ke *cloud server*. Selain itu, perangkat IoT biasanya memiliki data lokal yang tidak banyak dan sumber daya komputasi yang terbatas secara inheren jika *local training* [4] tanpa adanya kolaborasi antar perangkat IoT dilakukan. Hal ini menyebabkan penggunaan perangkat IoT untuk proses ML akan mengakibatkan kualitas *training* yang tidak efektif dan tingkat akurasi yang rendah.

Untuk mengatasi dua masalah di atas, *federated learning* (FL) [5, 6] menjadi solusi yang sangat efektif yang tidak hanya melindungi data pengguna perangkat IoT, namun juga memungkinkan antar perangkat IoT untuk melakukan kolaborasi proses *training* dengan adanya keterbatasan sumber daya komputasi. Pada akhirnya, model global yang digunakan untuk ekstraksi informasi penting bagi pemberi layanan aplikasi dapat mencapai tingkat akurasi yang tinggi. Penelitian terkait FL banyak dilakukan untuk optimisasi jumlah perangkat pengguna yang digunakan untuk proses *training*. Pada penelitian [11], sebuah sistem bernama *FedCS* dibuat untuk memilih partisipan yang akan berkontribusi dalam proses *training* yang sesuai dengan kemampuan komputasinya. Pada penelitian [12], sebuah sistem gabungan berbasis FL untuk memilih perangkat pengguna sebagai partisipan *training* berdasarkan data yang disimpan oleh perangkat yang bersifat *independently and identically distributed* (i.i.d) dikembangkan. Penelitian terkait dengan FL berlanjut untuk melakukan optimisasi jaringan *mobile edge* termasuk untuk aplikasi perangkat IoT. Pada penelitian [13], penggunaan FL yang digabungkan dengan *deep reinforcement learning* (DRL) dirancang untuk optimisasi *caching* dan *computation offloading* pada sebuah sistem *mobile edge computing* (MEC). Pada penelitian [14], sistem FL dengan DRL juga dikembangkan untuk *computation offloading* khusus untuk perangkat IoT. Di sisi lain, pengembangan sistem FL dengan menggunakan *stacked autoencoder* diteliti pada penelitian [15]. Kemudian, penelitian [16] membuat sistem FL yang berbasis algoritma *greedy* untuk melakukan optimisasi penempatan layanan yang tepat pada *proactive caching*.

Dari semua sistem FL yang dibuat, semua penelitian di atas tidak mempertimbangkan adanya masalah pada privasi dan keamanan data ketika proses *training* dilakukan dan model lokal dikirimkan dari perangkat pengguna ke *cloud server*. Pada penelitian [17], sebuah teknik yang disebut dengan *differentially private stochastic gradient descent* dibuat untuk menambah kan beberapa gangguan pada parameter yang sudah di-*training* pada sistem FL. Kemudian, penelitian [18] mengembangkan sebuah pendekatan yang dapat mencapai perlindungan privasi yang lebih baik dengan mengacak partisipan yang berkontribusi dalam proses *training* dan menambahkan distribusi *Gaussian*. Pada penelitian [19], sebuah mekanisme kolaboratif untuk membuat banyak partisipan mempelajari model global tanpa mengunggah semua parameter dari model lokal mereka ke *cloud server* dirancang.

Penelitian-penelitian di atas hanya berfokus pada perlindungan privasi dari parameter model lokal yang dikirimkan ke *cloud server* pada proses *training* dari sistem FL. Namun, sejauh ini belum ada penelitian yang berfokus pada gabungan dari perlindungan data pribadi perangkat pengguna IoT yang digunakan untuk proses *training* dan

model lokal untuk proses agregasi model global. Oleh karena itu, penelitian ini dimaksudkan untuk meningkatkan perlindungan data pengguna perangkat IoT dengan melakukan enkripsi data dan juga enkripsi model lokal selama proses *training* pada sistem FL berbasis *logistic regression* sedang berlangsung. Hal ini cukup sulit dilakukan karena terdapat dua proses enkripsi yang harus diselesaikan selama proses *training* pada sistem FL berjalan sampai dengan selesai.

III. METODOLOGI

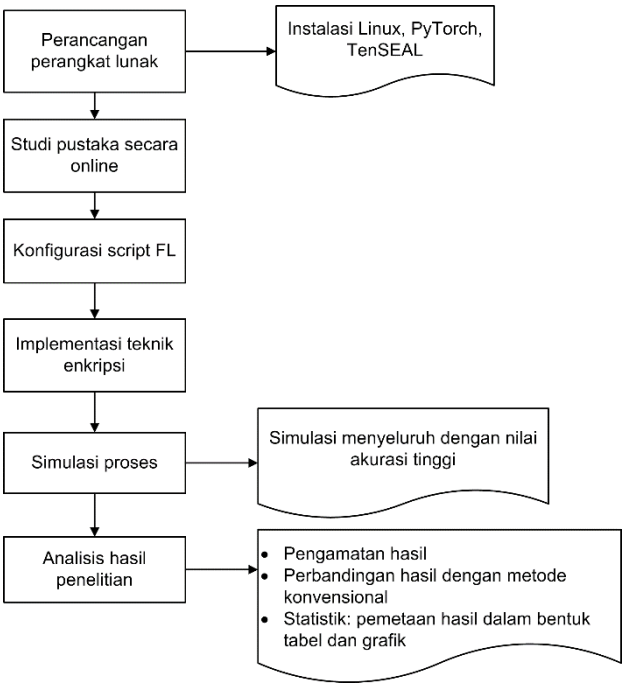
Pada penelitian ini, metode penelitian yang dilakukan berfokus pada perancangan pendekatan FL dengan tambahan metode enkripsi FHE. Berikut ini merupakan langkah-langkah proses penelitian yang dilakukan dengan diagram alir pada Gambar 1.

A. Perancangan perangkat lunak seperti melakukan instalasi Linux, PyTorch, dan *library* TenSEAL.
B. Studi literatur secara *online* yaitu dengan mengumpulkan literatur-literatur yang berkaitan dengan perangkat lunak seperti konfigurasi PyTorch, FL, dan metode enkripsi menggunakan FHE.
C. Konfigurasi *script* FL seperti penentuan dataset, data *pre-processing*, konfigurasi model, proses *training* dan *testing*, serta tampilan hasil.
D. Implementasi teknik enkripsi dengan menggunakan FHE dengan metode Cheon-Kim-Kim-Song (CKKS).
E. Simulasi proses melalui hasil integrasi antara FL dan FHE untuk mendapatkan hasil berupa nilai akurasi.
F. Perbandingan hasil penelitian dengan metode konvensional FL, sehingga diperoleh keunggulan dan kelemahan menggunakan hasil penelitian.

IV. HASIL DAN PEMBAHASAN

Untuk melakukan evaluasi terhadap rancang bangun FL dengan keamanan data melalui metode enkripsi FHE, dataset yang bersifat *random* dengan jumlah sampel dan fitur yang beraneka ragam dapat digunakan. Sebagai label, dua nilai klasifikasi biner dengan menggunakan pendekatan *logistic regression* yaitu 0 dan 1 diimplementasikan. Pada konfigurasi digunakan jumlah sampel sebanyak 1000, 5000, dan 10000 sampel dengan 2, 3, dan 5 fitur. Semua eksperimen dilakukan dengan menggunakan perangkat lunak PyTorch CPU 1.10.1 dan TenSEAL 0.3.12. Untuk mengaplikasikan pendekatan FL, diasumsikan 10 pengguna IoT di mana setiap pengguna memiliki jumlah sampel yang sama.

Selanjutnya perbandingan kinerja akurasi antara FL dengan FHE dan FL konvensional dapat dijelaskan sebagai berikut. Sesuai dengan ekspektasi seperti yang tampak pada Tabel 1-3, akurasi yang diperoleh dari pendekatan FL dengan tambahan enkripsi akan menghasilkan kinerja yang sedikit lebih rendah dibandingkan dengan FL konvensional. Hal ini dikarenakan dengan adanya penggunaan enkripsi FHE, maka akan sulit untuk menggunakan fungsi aktivasi *Sigmoid* secara langsung. Untuk mengatasi hal tersebut digunakan bentuk aproksimasi dari fungsi aktivasi *Sigmoid* dengan derajat *polynomial* yang lebih rendah untuk mengurangi banyaknya operasi perkalian pada proses *training*.



Gambar 1. Diagram alir metode penelitian FL dengan FHE

Tabel 1. Kinerja akurasi dengan 1000 sampel

Metode	2 fitur	3 fitur	5 fitur
FL	97.8%	99.2%	97.4%
FL + FHE	96.4%	97.8%	97%

Tabel 2. Kinerja akurasi dengan 5000 sampel

Metode	2 fitur	3 fitur	5 fitur
FL	99.8%	99.6%	99.5%
FL + FHE	96.4%	97%	97%

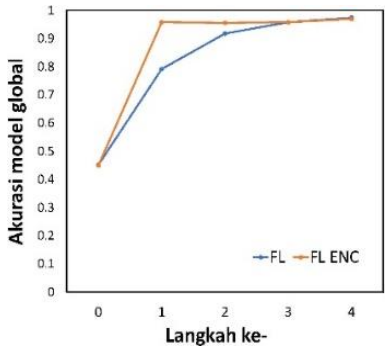
Tabel 3. Kinerja akurasi dengan 10000 sampel

Metode	2 fitur	3 fitur	5 fitur
FL	99.7%	99.8%	99.7%
FL + FHE	99.5%	95.5%	99.7%

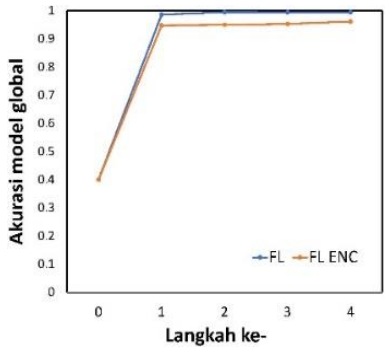
Secara umum dapat dilihat pada skenario 1000 sampel di Tabel 1 bahwa perbedaan akurasi antara FL konvensional dan FL dengan FHE adalah sampai dengan 1.43%. Namun, pada saat 5000 sampel digunakan di Tabel 2, ternyata perbedaan akurasi menjadi lebih besar yaitu sampai dengan 3.41%. Hal ini dikarenakan FL konvensional dapat melakukan *training* dengan baik sedangkan FL dengan FHE mengalami kendala dalam melakukan aproksimasi fungsi *Sigmoid*.

Sebagai bentuk solusi, penggunaan sampel yang lebih banyak yaitu 10000 sampel yang tambak pada Tabel 3 dapat memperbaiki perbedaan akurasi antara keduanya menjadi 0.22% saja khususnya untuk penggunaan 2 dan 5 fitur.

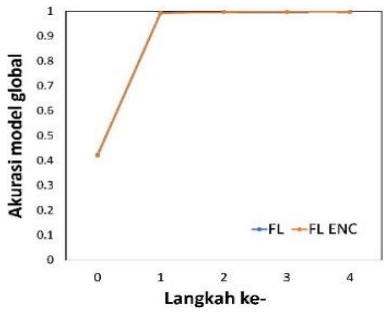
Untuk dapat melihat bagaimana proses *training* berjalan, hasil dalam bentuk grafik dengan jumlah 5 langkah dapat dilihat pada Gambar 2 dan 3 berikut ini. Untuk penggunaan jumlah sampel yang berbeda pada Gambar 2, semakin banyak sampel yang digunakan, maka perbedaan akurasi antara FL konvensional dan FL dengan FHE semakin kecil. Hal ini menunjukkan bahwa FL dengan tambahan keamanan data dapat digunakan untuk mengurangi adanya kebocoran data tanpa harus mengurangi nilai akurasi yang signifikan. Kemudian untuk penggunaan jumlah fitur yang berbeda pada Gambar 3, tidak dapat disimpulkan tren perbedaan nilai akurasi ketika fitur diperbanyak. Hal ini menunjukkan bahwa jumlah fitur yang semakin banyak tidak akan selalu menghasilkan nilai akurasi model yang lebih besar pada pendekatan FL dengan FHE.



(a) 1000 sampel

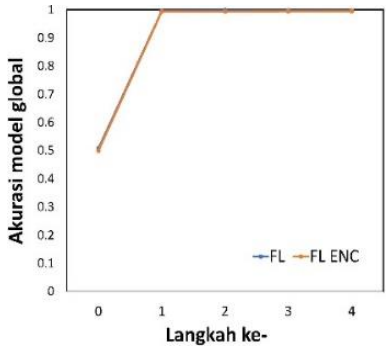


(b) 5000 sampel

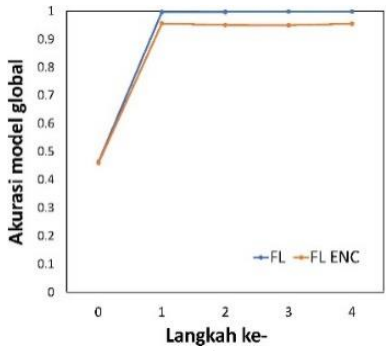


(c) 10000 sampel

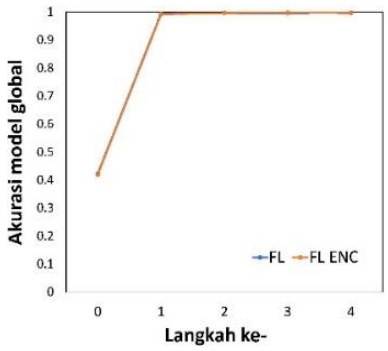
Gambar 2. Perbandingan akurasi dengan jumlah sampel yang berbeda (5 fitur)



(a) 2 fitur



(b) 3 fitur



(c) 5 fitur

Gambar 3. Perbandingan akurasi dengan jumlah fitur yang berbeda (10000 sampel)

V. SIMPULAN

Pada penelitian ini telah dibuat sebuah rancang bangun sistem FL dengan tambahan keamanan data yang dapat digunakan oleh pengguna perangkat IoT. Teknik enkripsi FHE dengan metode *training logistic regression* digunakan sebagai bentuk perlindungan privasi pengguna IoT dari *malicious attackers*. Dari penelitian ini dapat disimpulkan bahwa, pendekatan FL dengan FHE menghasilkan nilai kinerja akurasi yang sedikit lebih rendah dengan adanya aproksimasi fungsi aktivasi *Sigmoid*. Namun, penggunaan jumlah sampel yang lebih banyak dapat digunakan untuk mengurangi perbedaan kinerja akurasi. Oleh karena itu, pendekatan FL dengan FHE dapat digunakan untuk mengurangi adanya kebocoran data pada perangkat IoT tanpa harus mengurangi nilai akurasi model global yang signifikan.

REFERENSI

[1] I. H. Sarker, M. M. Hoque, Md. K. Uddin, and T. Alsanoosy, "Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions," *Mob. Netw. Appl.*, vol. 26, no. 1, pp. 285–303, Feb. 2021, doi: 10.1007/s11036-020-01650-z.

[2] "Big Data and Business Analytics Market 2027," 2021. [Online]. Available: https://www.alliedmarketresearch.com/big-data-and-business-analytics-market

[3] C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2224–2287, 2019, doi: 10.1109/COMST.2019.2904897.

[4] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of Machine Learning in Wireless Networks: Key Techniques and Open Issues," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3072–3108, 2019, doi: 10.1109/COMST.2019.2924243.

[5] Q. Yang, Y. Liu, Y. Cheng, Y. Khang, T. Chen, and H. Yu, "Federated Learning: Synthesis Lectures on Artificial Intelligence and Machine Learning," *Learning*, vol. 13, no. 3, pp. 1–207, 2019.

[6] W. Y. B. Lim *et al.*, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 2031–2063, 2020, doi: 10.1109/COMST.2020.2986024.

[7] E. Zeydan *et al.*, "Big Data Caching for Networking: Moving from Cloud to Edge," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 36–42, Sep. 2016, doi: 10.1109/MCOM.2016.7565185.

[8] S. Zhang, L. Yao, A. Sun, and Y. Tay, "Deep Learning based Recommender System: A Survey and New Perspectives," *ACM Comput. Surv.*, vol. 52, no. 1, pp. 1–38, Jan. 2020, doi: 10.1145/3285029.

[9] W. Nie, V. C. S. Lee, D. Niyato, Y. Duan, K. Liu, and S. Nutanong, "A Quality-Oriented Data Collection Scheme in Vehicular Sensor Networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5570–5584, Jul. 2018, doi: 10.1109/TVT.2018.2818190.

[10] A. Mulyani and U. Y. Oktiawati, "Implementasi Arsitektur Serverless Internet of Things pada Monitoring Cold Chain," 2022.

[11] T. Nishio and R. Yonetani, "Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China: IEEE, May 2019, pp. 1–7. doi: 10.1109/ICC.2019.8761315.

[12] N. Yoshida, T. Nishio, M. Morikura, K. Yamamoto, and R. Yonetani, "Hybrid-FL for Wireless Networks: Cooperative Learning Mechanism Using Non-IID Data," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–7. doi: 10.1109/ICC40277.2020.9149323.

[13] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning," *IEEE Netw.*, vol. 33, no. 5, pp. 156–165, Sep. 2019, doi: 10.1109/MNET.2019.1800286.

[14] J. Ren, H. Wang, T. Hou, S. Zheng, and C. Tang, "Federated Learning-Based Computation Offloading Optimization in Edge Computing-Supported Internet of Things," *IEEE Access*, vol. 7, pp. 69194–69201, 2019, doi: 10.1109/ACCESS.2019.2919736.

[15] Z. Yu *et al.*, "Federated Learning Based Proactive Content Caching in Edge Computing," in *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates: IEEE, Dec. 2018, pp. 1–6. doi: 10.1109/GLOCOM.2018.8647616.

[16] Y. Qian, L. Hu, J. Chen, X. Guan, M. M. Hassan, and A. Alelaiwi, "Privacy-aware Service Placement for Mobile Edge Computing via Federated Learning," *Inf. Sci.*, vol. 505, pp. 562–570, Dec. 2019, doi: 10.1016/j.ins.2019.07.069.

[17] M. Abadi *et al.*, "Deep Learning with Differential Privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2016, pp. 308–318. doi: 10.1145/2976749.2978318.

[18] R. C. Geyer, T. Klein, and M. Nabi, "Differentially Private Federated Learning: A Client Level Perspective." arXiv, Mar. 01, 2018. Accessed: May 10, 2023. [Online]. Available: http://arxiv.org/abs/1712.07557

[19] R. Shokri and V. Shmatikov, "Privacy-Preserving Deep Learning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver Colorado USA: ACM, Oct. 2015, pp. 1310–1321. doi: 10.1145/2810103.2813687.