Integrating NWDAF and Federated Learning for Privacy-Preserving Intrusion Detection in B5G IoHT Networks

E. K. Cruz Ortega, Eduardo S. Porto, Daniel M. Batista,
Department of Computer Science, University of São Paulo (USP), Brazil
{evgeni.cruz,sandalo,batista}@ime.usp.br

***Abstract*—The combination of Federated Learning (FL) with the Network Data Analytics Function (NWDAF) opens up new possibilities for smart, secure, and privacy-friendly network analysis in Beyond 5G (B5G) settings. This paper introduces a framework that merges FL and NWDAF to support distributed intrusion detection in Internet of Healthcare Things (IoHT) networks. The proposed approach enhances network security by enabling various healthcare organizations to collaborate on training machine learning-based intrusion detection models without sharing sensitive patient information. For network simulation, we use the free5gc project and we use the Flower Python framework for federated learning orchestration.**

I. Introduction

The Internet of Health Things (IoHT), also referred to as the Internet of Medical Things (IoMT), connects medical devices, sensors, and healthcare systems to enable real-time analytics [Huang et al. 2023]. Smart hospitals are transforming healthcare into a data-driven environment, which is expected to continue growing globally over the next twenty years [Jovy-Klein et al. 2024]. However, these systems face major challenges related to scalability, privacy, and security. Federated Learning (FL) helps address privacy and security issues by allowing machine learning models to be trained locally within edge devices, keeping sensitive data within healthcare institutions [Vinitha and Salim 2025]. It can also help tackle scalability, allowing training to be delegated to multiple distributed devices. All of this, however, has to be implemented within a network architecture. Beyond 5G (B5G) network architectures have performance, scalability, and adaptability as core principles, which are well-suited to an FL environment in IoHT.

To support intelligent network operations, the 3rd Generation Partnership Project (3GPP) introduced the Network Data Analytics Function (NWDAF) to the 5G Core network functions in Release 15 [Guo et al. 2025]. The NWDAF provides real-time network analytics that can work with learning algorithms to support automation and detect anomalies. Combining FL with NWDAF offers a promising approach to create intelligent and privacy-focused healthcare systems in B5G networks that learn and analyze data in a distributed manner.

Specifically, the NWDAF can only subscribe to other network functions (NFs) and provide model inference to them. This means that its reach is only within the network level, and it never has direct access to user data. Thus, any prediction or analysis has to be done over network usage or information, making the NWDAF a great fit for privacy-sensitive situations. One such situation is intrusion detection, which can be done by analyzing network usage alone. Multiple NWDAFs can be deployed in the 5G Core, allowing each NF to have its own analysis mechanism. The data sets ECU-IoHT [Ahmed et al. 2021] and WUSTL-EHMS 2020 provide specific instances of intrusion data.

Despite recent advances, there is no published research integrating NWDAF, FL, and IoHT simultaneously, which would allow detection of intrusions in critical medical networks with low latency, preserving privacy and adaptability. This gap motivates our research, with the goal of producing a framework joining FL with NWDAF applied to IoHT, in particular for detecting cyberattack scenarios in real time. Integrating FL into 5G network architectures presents several challenges, including high communication overhead, model and data leakage, and interoperability between network analytics and machine learning modules [Guo et al. 2025].

Considering these points, we propose the development of a hybrid framework consisting of NWDAF and FL to detect intrusions in IoHT networks. The main elements of our proposal include:

- **Managed FL clients and servers**: local NWDAF instances distributed close to network functions in IoHT (e.g. hospital gateways, patient sensors) perform training, whose weights are then aggregated by a central, managing network function
- **Intrusion detection mechanism**: deep learning models (CNN, LSTM, Autoencoders) trained locally via FL. They can be trained with data generated via NWDAF and perform prediction via this same system, identifying suspicious traffic or attacks in real time.
- **Experimental validation**: we utilize the WUSTL-EHMS 2020 and ECU-IoHT [Ahmed et al. 2021] data sets, representative of attacks and realistic medical traffic. We expect to use the *free5gc* open-source project as the simulation environment for our experiments. Both data sets and the simulation environment will be explained in more detail in Section III.

Through our approach, our main research goals are to:

i Achieve higher precision in intrusion detection than traditional centralized methods,
ii Reduce latency in responding to suspicious events in critical medical networks,
iii Preserve the privacy of clinical data, as sensitive information will not leave local devices,

iv Scale to complex IoHT scenarios with multiple connected devices,

This paper is organized as follows. In Section II, we review recent work connecting FL with NWDAF and FL with IoHT. In Section III, we present our methodology and experiments, with our results in Section IV. Finally, in Section V we conclude our findings.

II. Related Work

Our work has three main components: usage of NWDAF, an application of federated learning, and integration with IoHT networks. As we will present in this section, previous works have connected NWDAF with FL and FL with IoHT, but none have incorporated all three. Our approach innovates by bridging NWDAF and critical medical networks (IoHT), utilizing federated learning to ensure clinical data privacy and efficient intrusion detection, and validating with recent, realistic data sets to align our framework with practical scenarios.

A. Federated learning and NWDAF

Recent studies have shown notable progress in integrating NWDAF and FL technologies. [Guo et al. 2025] proposed a Hierarchical Networking and Privacy-Preserving Federated Learning (HiNP-FL) framework to reduce communication overhead and protect model privacy in 5G networks. [Hernández et al. 2025] extended NWDAF capabilities beyond the core network, introducing additional analytics functions such as RAN-DAF and UE-DAF for comprehensive multi-layer analytics. [Zhang et al. 2024] applied fair federated learning in multi-task NWDAF setups for 6G anomaly detection, achieving efficient model distribution and fairness across heterogeneous devices. However, none of these studies have open-source, reproducible experiments available.

[Rajabzadeh and Outtagarts 2023] present a distributed NWDAF architecture for B5G exploring three strategies of machine learning: centralized machine learning, decentralized federated learning, and their own proposal of centralized federated learning with additional security mechanisms. The system is implemented in an environment with four NWDAF instances, each running on separate virtual machines, responsible for analyzing metrics such as CPU usage and network function (NF) performance. Its main innovation is the usage of Local Differential Privacy (LDP) and a feedback weighting mechanism to enhance robustness and mitigate security threats. Experimental results show that the proposed framework achieved approximately 97.7% prediction accuracy and reduced inference latency from 21.4 s to around 4.8 s, outperforming both centralized ML (93.1%) and decentralized FL ($\approx$ 95.8%). While decentralized FL exhibited instability in model convergence among NWDAF instances, the centralized FL design maintained consistent performance and improved robustness. Nevertheless, this work focuses primarily on network load prediction rather than addressing medical or IoHT-specific cybersecurity scenarios.

Another approach for distributed NWDAF with federated learning is divided into two levels: leaf NWDAFs and root NWDAFs [Jeon et al. 2022]. The former are installed in local network functions, which train models with specific data (e.g. session duration), and the latter are localized in a central cloud, responsible for aggregating local models into a global model. The goal is to preserve data privacy and reduce resource usage, avoiding unnecessary uploads of sensitive information. The authors also illustrate examples of predicting user communication patterns combining different network functions: application functions (AFs), user plane functions (UPFs), session management functions (SMFs), and mobility management functions (AMFs). However, this paper is a conceptual proposal based on 3GPP standards, without practical implementations — including implementations based on medical environments or validation on IoHT data sets.

B. Federated learning and IoHT

In the context of IoHT and IoMT, [Islam et al. 2025] developed an Adaptive Federated Learning Framework (AFLF) incorporating hierarchical edge-fog-cloud architecture, differential privacy, and blockchain-based validation to enhance security and personalization. Similarly, [Amjath and Henna 2025] introduced a Differentially Private Federated Adversarial Learning (DP-FAT) model to mitigate poisoning and membership inference attacks in IoHT environments. Together, these works underscore the promise of combining FL with NWDAF to achieve scalable, secure, and privacy-preserving learning for healthcare and other mission-critical applications.

The work in [Chaddad et al. 2024] provides a comprehensive survey on federated learning in healthcare, exploring clinical applications such as AI-assisted diagnostics, disease prediction, and the analysis of distributed medical images. The authors demonstrate how FL enables different health institutions to collaborate on model development without sharing sensitive data, thus preserving patient privacy. The study highlights key benefits like enhanced data security, inter-hospital collaboration, and diagnostic efficiency, while also discussing practical challenges such as data heterogeneity, large-scale communication problems, and the risks of adversarial attacks. However, while this work is directly relevant to the medical sector, it does not address the use of NWDAF or integration with 5G/6G infrastructures for traffic management and anomaly detection in IoHT environments. [Mosaiyebzadeh et al. 2023] proposed an FL-based Intrusion Detection SYstem (DNN-FL) designed for IoHT environments. Their model achieved 91.4% and 98.47% accuracy on the WUSTL-EHMS 2020 and ECU-IoHT data sets, respectively. This demonstrates that decentralized learning can maintain high detection performance while keeping patient data private.

C. NWDAF

While direct applications of NWDAF to IoHT are absent from the literature, the capability to support massive IoT is a key motivation for the function's existence.

To understand the core functionality of the NWDAF, it is useful to review its architectural evolution. The work in [Tiwari et al. 2025] provides a detailed overview of the NWDAF's development, from early 3GPP drafts to Releases 16 and 17. The paper describes how the NWDAF collects

data from multiple network functions, processes metrics, and generates both historical and predictive analytics. These analytics assist operators with tasks such as resource optimization, load balancing, predictive maintenance, and anomaly detection. Furthermore, the authors present real-world use cases and highlight new functions introduced in recent releases, including the Data Collection Coordination Function (DCCF) and the Analytics Data Repository Function (ADRF). While this provides a foundational understanding of the NWDAF's role, the paper does not explore its integration with federated learning or specific applications in IoHT, focusing instead on general 5G network analysis.

III. Methodology

Our methodology consists of two main parts: (1) an implementation of an NWDAF based on the work of [Oliveira et al. 2024], fully integrated and containerized with the *free5gc* simulator for the 5G Core architecture, and (2) the federated learning system orchestrated by the NWDAF. The code for the experiments is available at *https://github.com/edusporto/fl-nwdaf-ioht*.

A. NWDAF

Based on the *free5gc-compose* project, we adapted the NWDAF implementation developed by [Oliveira et al. 2024] and [Kim et al. 2022] to a containerized environment with Docker Compose. The NWDAF container is responsible for registering itself as a NF and starting an HTTP server that can be used to communicate with it both from other NFs and, for experimental purposes, from outside the internal network. This HTTP server can be used to start FL training rounds and run inference.

Four other services are added to this same Docker network: (i) a Flower *SuperLink*, which connects FL clients, (ii, iii) two clients representing other internal NWDAFs (but not actually implemented as NFs) which run the training over the relevant data sets, and (iv) a training manager, which is an HTTP server that starts a Flower *driver*. This driver is responsible for connecting to the SuperLink, requesting training rounds to start, and for aggregating the weights generated by each client. The central NWDAF HTTP server communicates with this FL HTTP server to decide when and how to initiate training or inference.

B. Federated Learning

The Flower framework version 1.22.0 was used to implement a distributed FL architecture for intrusion detection in Internet of Healthcare Things (IoHT) networks. The setup included a SuperLink which handled communication between all the elements. Two SuperNodes were responsible for subsets of client partitions, and a central ServerApp managed the training rounds and aggregated model parameters using the Federated Averaging strategy, FedAvg. Local training is performed on each client node using a model with either the ECU-IoHT or WUSTL-EHMS 2020 dataset, thereby enabling performance to be measured across heterogeneous sources of health data.

To strengthen data privacy and communication security, we added Differential Privacy (DP) techniques on the server-side. We used a controlled Gaussian noise measure to determine the added noise during model aggregation for the purpose of privacy protection. Additionally, Transport Layer Security was deployed on all links to ensure that data exchange between the server, the SuperLink, and the clients was encrypted and authenticated. The global model checkpoints were stored in the *npz* format, while the accuracy, loss, and F-1 score evaluation metrics were recorded after each communication round.

C. Data sets

Two publicly available IoHT datasets were utilized in the experiments:

1) **WUSTL-EHMS 2020**: A hospital monitoring dataset containing physiological metrics, sensor events, and medical annotations.
2) **ECU-IoHT Dataset**: A dataset simulating cyberattacks in IoHT environments, with labeled attack types such as Smurf Attack, DoS Attack, ARP Spoofing, and No Attack, used to train and evaluate intrusion detection models (IDS).

Both datasets were preprocessed using custom scripts that performed normalization, client-based partitioning, and tensor conversion steps. Each client received a unique data partition, preserving non-IID characteristics inherent to federated environments.

D. Model architecture

Each client trained either a lightweight convolutional neural network (CNN) or a fully connected tabular model depending on the dataset's characteristics. The architecture was optimized for IoT-scale devices, consisting of two convolutional layers and two dense layers, ReLU activations, batch normalization, and cross-entropy loss. The Adam optimizer was used with a learning rate of 0.001. On the server side, a Federated Averaging (FedAvg) aggregation strategy was employed, optionally extended with Differential Privacy (DP) mechanisms to introduce Gaussian noise during model aggregation and ensure client data anonymity.

IV. Results

The FL setup operated for ten rounds of training to assess convergence, stability, and privacy. Using distributed updates with the help of the Flower framework, the global model is trained in a way that ensures raw data is never centralized.

Figure 1 shows the training accuracy across training rounds for the ECU-IoHT data set, fluctuating between 0.72 and 0.82 in the first iterations and stabilizing at approximately 0.75. The per-class recall is shown in Figure 2. Most types of attacks achieved a high recall rate, and a relatively lower recall rate was observed among smaller classes. Finally, Figure 3 shows the privacy accounting results for the server-side DP mechanism. The final privacy budget was $\epsilon = 12.30$; thus, a good compromise between privacy and model accuracy was achieved with $q = 1.0$, $\sigma = 1.0$, $\delta = 10^{-5}$.

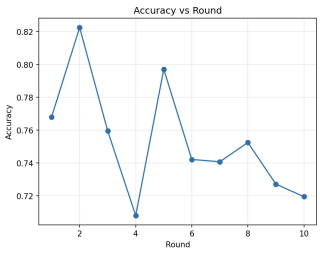

Figure 1: Accuracy between training rounds for the ECU-IoHT data set.

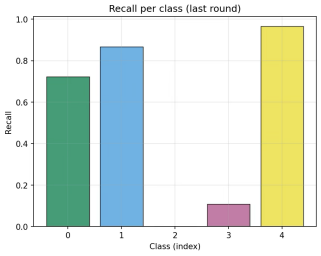

Figure 2: Training recall for the ECU-IoHT data set.

```
[Privacy Accounting] mode=server
  rounds = 5
  q      = 1.000000
  sigma  = 1.0
  delta  = 1e-05
  --> epsilon = 12.3017

[OK] Report saved to: runs/A_tls_dp/privacy.txt
```

Figure 3: Differential Privacy metrics for the ECU-IoHT data set.

Similar metrics are available in Figures 4 and 5. Training achieved a higher accuracy on this data set, reaching 0.93 by the fifth round. The model accurately identified the main class and achieved a recall of above 0.5 for the smaller class.

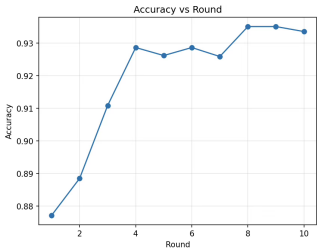

Figure 4: Accuracy between training rounds for the WUSTL data set.

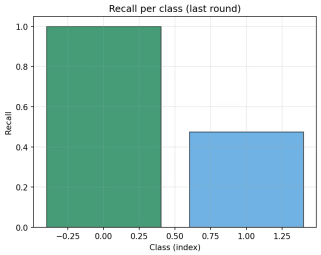

Figure 5: Training recall for the WUSTL data set.

V. Conclusion

This work proposed a framework to integrate federated learning (FL) with the Network Data Analytics Function (NWDAF) from the 5G Core to detect intrusions in IoHT environments connected by B5G networks. We performed experiments with real IoHT data sets for FL, and integrated the management of FL clients and servers through a custom implementation of an NWDAF within the *free5gc* simulator. We also validated our training metrics and incorporated Differential Privacy (DP) and TLS security in network communications to further improve data safety. The outcome is a secure and efficient framework capable of supporting distributed analytics without compromising data confidentiality. Possible future work includes (i) extending this integration with Explainable Artificial Intelligence (XAI) to improve model interpretability and trust, and (ii) the expansion of the simulated environment to include multiple registered NWDAFs and perform training with live-ingested data instead of pre-defined data sets.

VI. Acknowledgements

The authors would like to thank the National Secretariat of Science, Technology, and Innovation of Panama (SENACYT) and the National Council for Scientific and Technological Development of Brazil (CNPq) for the financial support.

References

[Ahmed et al. 2021] Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L. F., and Haskell-Dowland, P. (2021). Ecu-ioht: A dataset for analyzing cyberattacks in internet of health things. *Ad Hoc Networks*, 122:102621.

[Amjath and Henna 2025] Amjath, M. and Henna, S. (2025). Differentially Private Federated Adversarial Learning for Robust Malware Detection in Internet of Health Things (IoHTs) . In *2025 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 492–497, Los Alamitos, CA, USA. IEEE Computer Society.

[Chaddad et al. 2024] Chaddad, A., Wu, Y., and Desrosiers, C. (2024). Federated learning for healthcare applications. *IEEE Internet of Things Journal*, 11(5):7339–7358.

[Guo et al. 2025] Guo, C., Cui, F., Xu, C., Su, M., Wang, Z., and Li, H. (2025). A hierarchical networking and privacy-preserving federated learning framework for 5g networks. *Journal of Communications and Information Networks*, 10:26–36.

[Hernández et al. 2025] Hernández, I., Mejías, D., Fernández, Z., and Herranz, V. (2025). Beyond nwdaf services for comprehensive 5g network analytics and orchestration. In *2025 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pages 1–8.

[Huang et al. 2023] Huang, C., Wang, J., Wang, S., and Zhang, Y. (2023). Internet of medical things: A systematic review. *Neurocomputing*, 557:126719.

[Islam et al. 2025] Islam, U., Ullah, H., Khan, N., Ahmad, I., and Saleem, K. (2025). Adaptive federated learning framework for privacy-preserving consumer-centric iomt: A novel secure data collaboration model. *IEEE Transactions on Consumer Electronics*, pages 1–1.

[Jeon et al. 2022] Jeon, Y., Jeong, H., Seo, S., Kim, T., Ko, H., and Pack, S. (2022). A Distributed NWDAF Architecture for Federated Learning in 5G. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–2. ISSN: 2158-4001.

[Jovy-Klein et al. 2024] Jovy-Klein, F., Stead, S., Salge, T. O., Sander, J., Diehl, A., and Antons, D. (2024). Forecasting the future of smart hospitals: findings from a real-time delphi study. *BMC Health Services Research*, 24:1421.

[Kim et al. 2022] Kim, T., Kim, J., Ko, H., Seo, S., Jcon, Y., Jeong, H., Lee, S., and Pack, S. (2022). An Implementation Study of Network Data Analytic Function in 5G. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–3. ISSN: 2158-4001.

[Mosaiyebzadeh et al. 2023] Mosaiyebzadeh, F., Pouriyeh, S., Parizi, R. M., Han, M., and Batista, D. M. (2023). Intrusion Detection System for IoHT Devices using Federated Learning. In *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6. ISSN: 2833-0587.

[Oliveira et al. 2024] Oliveira, L. A. d., Silva, R. O., Lima, P. C., Pereira, A. M. S., Valadares, J. A., Silva, E. F., and Dantas, M. A. R. (2024). Análise da Funcionalidade da NWDAF no Core 5G Sobre um Conjunto de Dados. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 798–811. SBC. ISSN: 2177-9384.

[Rajabzadeh and Outtagarts 2023] Rajabzadeh, P. and Outtagarts, A. (2023). Federated learning for distributed nwdaf architecture. In *2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pages 24–26.

[Tiwari et al. 2025] Tiwari, A., Das, S., Kumar, A., and Srivastava, S. (2025). Nwdaf in 5g: Architecture, use cases, and evolution across 3gpp releases. In *2025 National Conference on Communications (NCC)*, pages 1–6.

[Vinitha and Salim 2025] Vinitha, V. and Salim, A. (2025). Securing health: Privacy-preserving federated learning in iot healthcare. *IEEE International Conference on Advances in Computing, Communication, Embedded and Secure Systems*.

[Zhang et al. 2024] Zhang, C., Shan, G., and Roh, B.-h. (2024). Fair federated learning for multi-task 6g nwdaf network anomaly detection. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–12.