Sustainable Cybersecurity in Future Networks via Distributed Learning Methods

Gökcan Cantali
Institute of Computer Science
Zürich University of Applied Sciences
CH-8401 Winterthur, Switzerland;
Communication Systems Group
University of Zürich
CH-8050 Zürich, Switzerland
Email: canl@zhaw.ch

Gürkan Gür
Institute of Computer Science
Zürich University of Applied Sciences
CH-8401 Winterthur, Switzerland
Email: gueu@zhaw.ch

Burkhard Stiller
Communication Systems Group
University of Zürich
CH-8050 Zürich, Switzerland
Email: stiller@ifi.uzh.ch

***Abstract*—With the development of 6G networks and their envisaged support of artificial intelligence (AI)-native services for an unprecedented number of users and apps, privacy is becoming an increasing concern. While there is a large body of research on the use of distributed learning techniques for privacy-aware AI development, particularly federated learning (FL), the simultaneous consideration of cybersecurity and sustainability perspectives in this area is understudied. As such, this Ph.D. thesis aims to analyze the use of distributed learning in future wireless networks through the lens of cybersecurity and sustainability, including the carbon footprint dimension, and to formulate a joint optimization problem to help application or infrastructure owners obtain optimal configurations tailored to their needs.**

***Index Terms*—distributed machine learning; cybersecurity; sustainability; 6G networks; federated learning; artificial intelligence**

I. Introduction

The development of next-generation wireless networks, such as 6G networks, is likely to exacerbate cybersecurity issues by enabling a "hyper-connected" environment [1]. Based on this rationale, many researchers are focusing on the security aspect of next-generation wireless networks, specifically targeting the 6G architecture [2]. As such, real-time threat or intrusion detection systems are demanded, preferably machine learning (ML)- or artificial intelligence (AI)-powered security solutions that rely on large amounts of data. To mitigate privacy concerns associated with such techniques, federated learning (FL) has emerged as a paradigm shift from traditional centralized learning to distributed learning methods [3], enabling collaborative training environments in which each party retains its sensitive data.

Another challenge in developing AI-based cybersecurity solutions, which entail FL-based applications, is sustainability, a fast-growing concern due to the recent advancements in the AI domain [4], including large language models (LLMs), generative AI, and agentic AI. While limiting the training duration or using smaller models via quantization or pruning [5] is a straightforward approach to tackle this problem, they lead to model degradation, which implies a decreased level of security for the cybersecurity domain. In that regard, the energy efficiency of FL is investigated in greater detail for future 6G networks [6], as well as the combination of split learning [7] or sequential learning [8] with FL for further improvement. In addition, measuring and reducing the carbon emissions of FL processes is another sustainability concern, which is understudied compared to the energy efficiency dimension [9]. Nevertheless, recent studies address this issue through smart client selection [10], work offloading [11], or renewable excess energy [12].

TABLE I
Recent study on the overlap of security, sustainability, distributed learning, and future networks

Prior study	Cyber-security	Sustainable computing	Distributed learning	Future networks
Shati *et al.* [13]	✓	✓	×	×
Sharmin *et al.* [14]	✓	✓	×	✓
Guo *et al.* [15]	×	✓	✓	✓
CAFE [10]	×	✓	✓	×
FedGuard-DC [16]	✓	×	✓	×
Maiga *et al.* [17]	✓	×	✓	✓

There is a growing body of research, individually, in each of the three concepts, namely, cybersecurity, sustainability, and distributed learning. Nevertheless, as shown in Table I, a joint outlook on these concepts through the lens of future networks is lacking, which could provide significant benefits for application or system owners intending to run their applications on critical future network infrastructures.

II. Problem Statement and Research Questions

As explained in the previous section, there is still a need to tackle the multi-faceted problem considering various dimensions: i) privacy-preservation of data owners, ii) the level of security of the system, and iii) the impact of the ML components on environmental sustainability. To the best of our knowledge, no study has yet come up with a formally structured solution for application or infrastructure owners in a future network setup to determine the optimal system configuration, considering the levels of security, sustainability, and privacy, that is tailored to their needs. This gap in the literature drives the motivation for this Ph.D. thesis research.

979-8-3195-0167-7/26/$31.00 ©2026 IEEE

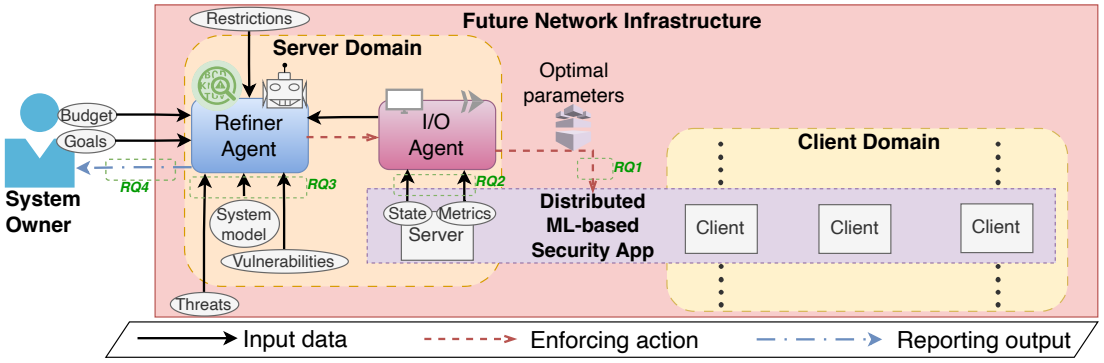


Fig. 1. The design of the proposed framework

During the development of this thesis, the following research questions are to be addressed:

- **RQ1**: What are the limitations of existing distributed learning-powered cyber-defense applications deployed on future network infrastructures, and how can sustainable computing methods be leveraged to configure the distributed learning schemes to overcome such limitations?
- **RQ2**: Can we accurately measure and report the provided level of security and resource usage of cybersecurity applications running on distributed ML techniques, using a quantifiable and robust set of metrics/KPIs that are applicable in multiple scenarios?
- **RQ3**: Which efficient techniques can be used to dynamically infer the constraints and properties of the operating environment/infrastructure, as well as constructing and solving an optimization problem between levels of security, privacy of parties, and sustainability of cyber-defense applications, and to what extent can this approach be automated, preferably using AI-based techniques?
- **RQ4**: How can we evaluate the proposed approach in a comprehensive manner that considers multiple use cases and various scenarios applicable for future network setups, to obtain fair and generalizable findings?

III. The Proposed Approach of the Ph.D. Thesis

As part of this thesis, this section presents the proposed design along with the adopted methodology.

A. Framework Design

The framework for tackling the cybersecurity and sustainability trade-off, in services powered by distributed learning techniques and operating on future network infrastructures, is expected to contain two major components: the *Refiner Agent* and the *I/O Agent*, as shown in Fig. 1.

1) The Refiner Agent: This component comprises the main intelligence of the proposed framework and will employ sophisticated AI/ML techniques. The current state and metrics/KPIs of the application, provided by the I/O Agent, can be combined with various environmental factors, including threats and restrictions, as well as specific goals and budgets of the system owner, to construct a joint optimization problem. Then, to solve the optimization problem, various techniques such as linear programming, mixed-integer programming, or reinforcement learning could be adopted.

The Refiner Agent addresses RQ3 via its interaction with the operational environment to infer properties of the infrastructure, system vulnerabilities, and possible threats from adversaries. Furthermore, by reporting results back to the user, it aids the evaluation process, thereby addressing RQ4 as well.

2) The I/O Agent: This component is responsible for investigating the current state and operational metrics by communicating with the application via communication protocols such as WebSockets or gRPC. In addition, the I/O Agent will interact with relevant APIs, such as Kubernetes, to enforce the configuration changes determined by the Refiner Agent into the application.

The I/O Agent tackles RQ2 via its monitoring of the distributed learning-based cybersecurity application state and measurement of relevant metrics/KPIs. Moreover, due to its role in enforcing the (Pareto) optimal configuration for the distributed learning scheme, it is also related to RQ1.

B. Methodology

To develop and evaluate the proposed approach, an empirical and experimental methodology will be employed, using a variety of scenarios and applications within the scope of future networks and with a particular focus on 6G networks, preferably with varying environmental factors. For generalizable findings, multiple threat vectors, fluctuating network conditions, varying workloads, and diverse client resources should be used for evaluation, and several KPIs should be measured across overlapping areas of cybersecurity, privacy, and sustainability for both the proposed multi-dimensional approach and a set of state-of-the-art studies in these areas.

For the data collection phase, 5G testbeds will be used to generate synthetic data, as 6G deployment does not exist yet. Nevertheless, this decision is justified given the insight that 6G architecture will be heavily based on the modular 5G design, with a greater focus on containerized workloads, AI services, and AI-driven network management. Therefore, use cases will primarily focus on containerized network functions (CNFs) and, preferably, AI workloads, to more realistically represent future 6G applications. In that regard, some of the services

deployed on the testbed could be powered by LLM or an agentic AI paradigm.

In the experimentation phase, multiple baseline methods need to be established for proper benchmarking. One such baseline could be a fixed, hard-coded configuration based on the prioritized goal, while others will be selected from state-of-the-art studies. Each experiment with a specific set of parameters will be repeated a certain number of times to decrease bias and increase the generalizability of the findings.

IV. Initial Results and Prospective Work

During the early stage of this Ph.D. study, preliminary results have been obtained through a partial and joint implementation of both components. The implemented scheme, namely FedSynthesis [18], aims to reduce the carbon footprint of an FL process via heuristic-based carbon prediction methods (the Refiner Agent) and a carbon-aware client selection mechanism (the I/O Agent) for customizing the FL pipeline.

TABLE II
Carbon footprint improvement by FedSynthesis

CO_2 **estimation technique**	CO_2 $(10^{-5}kg)$	**Improvement**
Baseline FL	1.93	-
Simple Averaging	1.75	9.3%
Exponential Smoothing	1.84	4.7%
Linear Regression	1.79	7.2%

The developed solution is tested on a graph neural network-based anomaly detection system [19] running in the cloud. As shown in Table II, experiments reveal that the carbon footprint of the FL scheme can be reduced by 4%-10% across three different carbon emission estimation techniques, without having a major degradation on the final model performance.

While initial work shows promising results, the current work needs to be expanded to include metrics beyond the carbon footprint and should be tested under various threat models, which may require incorporating additional privacy-enhancing mechanisms such as differential privacy. The task segregation between the Refiner Agent and the I/O Agent should have clear boundaries, enabling the components to interact reliably.

In addition, the Refiner Agent should be further developed to formulate a valid optimization problem, perhaps using agentic AI or LLMs, while supporting accurate optimization methods, such as game theory, reinforcement learning, or linear/mixed-integer programming, to achieve customized goals based on the scenario and application requirements.

Finally, distributed learning protocols other than FL should also be investigated, such as split learning, where the compute-intensive task could be shared across entities with different resource capabilities. The proposed framework, in this case, should evaluate how the split should be configured to optimize the trade-off between security, sustainability, and privacy.

Acknowledgments

This work was supported partially by (a) the University of Zürich UZH, Switzerland and (b) the Horizon Europe Framework Program's project NATWORK, Grant Agreement No. 101139285 funded by the Swiss State Secretariat for Education, Research, and Innovation SERI, under Contract No. 22.00642.

References

[1] H. Lee *et al.*, "Towards 6G hyper-connectivity: Vision, challenges, and key enabling technologies," *Journal of Communications and Networks*, vol. 25, no. 3, pp. 344–354, 2023.

[2] P. Porambage *et al.*, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, vol. 54 of *Proceedings of Machine Learning Research*, pp. 1273–1282, PMLR, 20–22 Apr 2017.

[4] M.-K. Kim, T.-A. Yoo, and J.-B. Chung, "Toward sustainable AI: A scoping review of carbon footprint and environmental impacts across training and inference stages," *IEEE Access*, vol. 14, pp. 18881–18896, 2026.

[5] P. Prakash *et al.*, "IoT device friendly and communication-efficient federated learning via joint model pruning and quantization," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13638–13650, 2022.

[6] K. Raja *et al.*, "An efficient 6G federated learning-enabled energy-efficient scheme for UAV deployment," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 2, pp. 2057–2066, 2025.

[7] X. Qiang, Z. Chang, C. Ye, T. Hämäläinen, and G. Min, "Split federated learning empowered vehicular edge intelligence: Concept, adaptive design, and future directions," *IEEE Wireless Communications*, vol. 32, no. 4, pp. 90–97, 2025.

[8] Y. Li and X. Lyu, "Convergence analysis of sequential federated learning on heterogeneous data," in *Proceedings of the 37th International Conference on Neural Information Processing Systems*, NIPS '23, (Red Hook, NY, USA), Curran Associates Inc., 2023.

[9] X. Qiu *et al.*, "A first look into the carbon footprint of federated learning," *J. Mach. Learn. Res.*, vol. 24, Jan. 2023.

[10] J. Bian, L. Wang, S. Ren, and J. Xu, "CAFE: Carbon-aware federated learning in geographically distributed data centers*," in *Proceedings of the 15th ACM Int. Conf. on Fut. and Sust. Energ. Sys.*, e-Energy '24, (New York, NY, USA), p. 347–360, ACM, 2024.

[11] H. R. Chi, D. Corujo, and R. L. Aguiar, "Carbon-aware full-decentralized multi-provider edge computing peer offloading," in *2024 IEEE 22nd Int. Conf. Ind. Inform. (INDIN)*, pp. 1–6, 2024.

[12] P. Wiesner, R. Khalili, D. Grinwald, P. Agrawal, L. Thamsen, and O. Kao, "FedZero: Leveraging renewable excess energy in federated learning," in *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, e-Energy '24, (New York, NY, USA), p. 373–385, ACM, 2024.

[13] I. A. K. Shati, M. F. S. Gernaz, A. I. O. Abdullah, and A. S. A. Sahab, "Enhancing cybersecurity and green communication in 5G networks: Challenges and sustainable solutions," in *2025 14th Int. Symposium on Image and Signal Processing and Analysis (ISPA)*, pp. 181–186, 2025.

[14] S. Sharmin, I. Ahmedy, and H. Ismail, "Enhancing 5G/6G network efficiency and security via artificial intelligent-driven real-time analytics and resource optimization," in *2025 IEEE Int. Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, pp. 13–16, 2025.

[15] C. Guo, F. Cui, C. Xu, M. Su, Z. Wang, and H. Li, "A hierarchical networking and privacy-preserving federated learning framework for 5G networks," *Journal of Communications and Information Networks*, vol. 10, no. 1, pp. 26–36, 2025.

[16] M. Kibria Saroare and M. Rubel Ahmed, "FedGuard-DC: Privacy-Preserving Federated Load Forecasting and Cyber-Attack Detection for Data-Center Loads in Transmission Systems," *arXiv e-prints*, p. arXiv:2608.19155, Aug. 2026.

[17] A.-A. Maiga, E. Ataro, and S. Githinji, "XGBoost and deep learning based-federated learning for DDoS attack detection in 5G core network VNFs," in *2024 6th International Conference on Computer Communication and the Internet (ICCCI)*, pp. 128–133, 2024.

[18] G. Cantali, G. Gür, and B. Stiller, "FedSynthesis: A flower-based framework for carbon-reduced federated learning," in *Proceedings of the 18th IEEE/ACM International Conference on Utility and Cloud Computing*, UCC '25, (New York, NY, USA), ACM, 2025.

[19] M. Osswald, T. Schönenberger, G. Cantali, W. Soussi, and G. Gür, "Anomaly detection in microservices architecture using graph neural networks," in *2025 33rd Euromicro Int. Conf. on Prll., Distr., and Network-Based Processing (PDP)*, (Torino, Italy), IEEE, 2025.