SURFS: Sustainable IntrUsion Detection with HieraRchical Federated Spiking Neural Networks

Ons Aouedi, Kandaraj Piamrat

SURFS: Sustainable intrUsion detection with hieraRchical Federated Spiking neural networks

Ons Aouedi[+*] and Kandaraj Piamrat[*]
[*]*Nantes Université, École Centrale Nantes, CNRS, INRIA, LS2N, UMR 6004, F-44000 Nantes, France*
firstname.lastname@ls2n.fr
[+]*SnT, SIGCOM, University of Luxembourg, Luxembourg*
aouedions9@gmail.com

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices and the transition to distributed computing environments necessitate advanced intrusion detection systems (IDS) to safeguard the new paradigm known as Cloud-Edge-IoT (CEI) continuum. In this paper, we introduce a novel approach called `SURFS`, integrating Hierarchical Federated Learning (HFL) with Spiking Neural Networks (SNN) to propose a robust, sustainable, and energy-efficient IDS for this continuum. HFL, with its hierarchical learning strategy, keeps data where they are generated, thus preserving user privacy and reducing communication overhead through its combination of decentralized and centralized architecture. On the other hand, SNN, inspired by human neural mechanisms, offers significant computational efficiency. Our proposed IDS combines these strengths, facilitating localized and energy-efficient detection at the edge and IoT layers while enabling global model aggregation and updates at the cloud layer. Through extensive experiments using one of the most recent datasets (Edge-IIoTset), we demonstrate that our approach not only detects attacks with high accuracy but also substantially reduces energy consumption across the continuum. The SURFS model presents a slightly superior performance in classification accuracy, outstripping the FL+SNN and non-FL models by margins of 0.5% and 1.21%; however, with a much faster convergence time (3× and 17× respectively). In terms of sustainability, it achieves a remarkable reduction in communication overhead 99% lower than FL+SNN and 97% lower than non-FL. Additionally, it showcases significant improvements in computational cost, being 62% more efficient than FL+SNN and 94% more efficient than the non-FL model.**

***Index Terms*—Hierarchical federated learning, Spiking neural network, Intrusion detection system, Sustainable AI**

I. Introduction

According to recent statistics, by 2030 the number of connected Internet of Things (IoT) devices will surpass 500 million [1]. This tremendous expansion led to the realization of several applications and services such as smart cities. These IoT devices act in the background to collect the environment and user data. A recent report indicates that the data generated by IoT devices will reach 79.4 zettabytes (ZB) by 2025 [2]. Such data requires high computing resources for the treatment process with latency constraints in order to provide delay-sensitive services. Cloud computing can support IoT devices in solving computation tasks, but it cannot satisfy the delay-sensitive analysis applications that require fast analysis. To solve these issues, edge computing has been proposed and is considered "the new cloud". Migrating computing and storage to the edge of the network helps to reduce the congestion and latency that occur with the cloud and support IoT devices with the creation of the Cloud-Edge-IoT (CEI) continuum [3]. CEI improves users' computation experience and helps to make the IoT system highly scalable. Also, it adapts to distributed computing by avoiding the issues associated with a single point of failure. However, the migration of large-scale computing and storage services to the edge facilitates the interception and analysis of end user-sensitive data. Moreover, the distributed nature in the CEI introduces new security and privacy challenges [4].

In this context, some advances, such as Hierarchical Federated Learning (HFL) [5] and Intrusion Detection Systems (IDS) [6] can improve the confidentiality of the data and the security of the IoT devices. In particular, HFL is a combination of decentralized and centralized architecture [7]. It has been proposed to integrate several aggregations of local models taking place at the edge servers, which is then followed by sending the edge aggregated sub-models to the cloud for global aggregation. HFL helps reduce the impact of non-independent and identically distributed (non-IID) data on the model's performance. On the other hand, IDS is one of the requirements to monitor the communication system and to protect against malicious attacks [8]. It demands faster data processing, whereas sending user data to some central servers is time-consuming [6]. In fact, the existing literature on HFL for IDS uses traditional Artificial Neural Network (ANN) models to learn from the end-users' data [9]. However, using (ANN) with HFL for IDS consumes a significant amount of energy, further hindering the application of decentralized FL on energy-constrained IoT devices. To solve this issue, Spiking Neural Network (SNN) has been used as a new energy-efficient generation of neural networks [10]. In contrast to ANN, SNN replaces the multiplicative operations of inputs and weights with simple addition operations. This difference leads to a reduction in the power consumption of SNN-based models, offering more energy-efficient models as demonstrated in our previous work [11].

In this paper, we propose `SURFS` (Sustainable intrUsion detection with hieraRchical Federated Spiking neural networks), a novel IDS based on SNN within HFL for the CEI continuum. It aims to reduce energy and communication costs as well as to mitigate the impact of the non-IID data on the attack detection performance. To the best of our knowledge, this is

the first study that explores the classification and sustainability of the SNN-based HFL model for IDS. The contributions of this paper are summarized in the following.

- We propose a sustainable IDS (SURFS) based on hierarchical federated spiking neural networks for the CEI continuum. It takes advantage of HFL to mitigate the impact of the non-IID data and SNN to reduce the energy consumption of the model on IoT devices.
- We evaluate the sustainability of SURFS using a sustainable indicator (S), which illustrates the trade-off between energy consumption, communication costs, and classification accuracy.
- We use one of the most recent and open cyber-security datasets, called Edge-IIoTset (published in 2022) in order to investigate the performance of SURFS against classical FL with SNN (FL+SNN) and non-FL SNN-based models.

The rest of the paper is organized as follows. Section II provides related work and Section III presents our SURFS solution. Experimental settings and results are presented in Section IV. Finally, the conclusion is provided in Section V.

II. Related Work

Many solutions have been proposed for IDS using HFL. In this context, Sun *et al.* [12] proposed an HFL-based IDS to enhance the security of advanced metering infrastructure in smart grids, called HFed-IDS. The experiment results demonstrate that the HFed-IDS can improve the IDS in terms of detection accuracy and communication cost. In the same direction, Singh *et al.* [7] proposed a HFL-HLSTM intrusion detection model for the Internet of medical things (IoMT) application. The Preliminary results show also that attack detection using the proposed HFL-HLSTM is better than existing state-of-the-art models. Also, Saadat *et al.* [13] proved the superiority of HFL over classical FL in terms of training loss, attack detection, and speed of convergence. Moreover, Sarhan *et al.* [14] introduce a novel Hierarchical Blockchain-based FL HBFL framework for collaborative detection of IoT intrusions. The framework adopts a cloud fog–edge topology in which IoT endpoints and combiners are hosted on edge and fog perimeters, respectively. The outcome of the framework is a robust and securely designed HFL-based IDS to protect and preserve the integrity of IoT networks. However, all these proposed schemes were carried out using an outdated dataset (NSL-KDD dataset). In addition, to address the heterogeneity issues (i.e., non-IID data) that arise in FL settings, Saez *et al.* [15] proposed HFL for IDS in large-scale heterogeneous IoT networks. In particular, before the local models are aggregated in the initial FL round, the local partially trained models from all the clients are clustered in a fully unsupervised way based on similarities between model parameters. Once each client is assigned to a cluster center, the FL training process is started for each identified cluster of devices.

Discussion: It is important to note that the IDS has significantly shifted from simple models to more advanced DL models and then to FL/HFL. The focus has been primarily on classification performance such as accuracy (in centralized systems), communication efficiency, and privacy (in FL). However, no study focuses on the sustainability of the proposed scheme, as well as the combination power of SNN and HFL for IDS has not been proposed yet. Considering these factors, we propose in this paper a sustainable IDS based on SNN and HFL for the CEI continuum. This approach not only offers the advantages of efficient distributed learning with non-IID data but also ensures a reduction in communication costs and most importantly energy consumption, thus making it an efficient and promising solution.

III. Methodology

To achieve better learning efficiency and sustainable IDS, we propose SURFS, a sustainable IDS solution that combines the strengths of HFL and SNN-based for the CEI continuum.

A. SURFS

As illustrated in Figure 1, our proposition integrates SNN within HFL. In particular, SNN is inspired by the way biological neurons communicate through spikes. Unlike traditional ANN where information is conveyed through continuous values (often between 0 and 1), the information in SNN is conveyed through discrete events called spikes [10]. In particular, each neuron maintains a membrane potential (an accumulated value) that varies over time. This potential increases with incoming spikes from other neurons and naturally decays or leaks over time. When the neuron's membrane potential exceeds a certain threshold, it generates a spike and resets its potential. Then, the membrane potential gradually decays toward a resting value when the neuron is not firing due to a leak factor. This process is repeated for T timesteps. All this makes SNN a closer computational analogy to biological neural systems. Because SNN only activates (i.e., spike) when necessary, they are inherently energy-efficient solutions. Moreover, since only the spikes are communicated between neurons, this leads to sparse data transmission. Consequently, SNN can reduce the computation, bandwidth, and memory requirements, making it suitable for resource-constrained environments (i.e., IoT applications).

Our proposition consists of three layers: *IoT*, *edge*, and *cloud*; matching with its integration into the CEI continuum. The IoT devices represent the lowest layer. The edge servers are located in the middle layer, which is used for sub-global aggregations of IoT device models. The cloud servers located at the top layer are used for global model aggregation. Similar to FL, HFL allows IoT devices to train a shared global model while the raw data are kept local. The learning process in the continuum includes the following key steps:

- *Distributed local training and updates*: Once the subset of the IoT devices that participate in the learning process is selected, the cloud server sends an initial SNN model to trigger the distributed training (*Global SNN model downloading*). Then, after several local epochs, each IoT device uploads its local SNN model updates to the corresponding edge servers for sub-global model aggregation (*Local model uploading*).

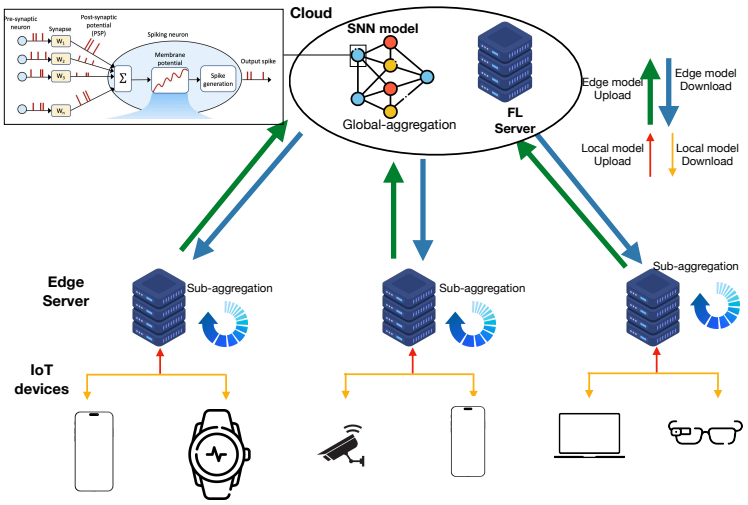

Fig. 1. Envisioned framework for sustainable HFL for IDS. In this framework, the IoT devices train the SNN model locally, the edge servers perform sub-aggregation, and the cloud performs the global aggregation.

- *Sub-global model aggregations and uploads*: Upon receiving all the updates from the IoT devices, the edge servers perform the sub-global SNN model aggregation and transfer it back (*Edge model downloading*) to their assigned IoT devices to update their local SNN models accordingly. Then, after a specific number of rounds, the edge servers send their sub-global models (*Edge model uploading*) to the cloud server.
- *Global model aggregation*: After receiving the sub-global models, a combined global model is created by averaging the parameters of the edge models. Finally, the global model parameters are transmitted along the hierarchy downwards to the IoT devices.
- *Iterated Training*: The HFL training is iterated until the desired performance is achieved.

B. Sustainability metrics

To evaluate the sustainability of our proposition, we use metrics proposed in [16]. These metrics consider both the classification performance and environmental impact as follows:

- *Error rate* (which is $1 - accuracy$) on unseen data.
- *Computational efficiency* in terms of energy consumed in units of Watt hours (Wh).
- *Communication efficiency*, which is quantified by the data size communicated between the cloud server and the edge servers (resp. IoT devices) in each communication round in kilobytes (kB) in the FL scenario. It is represented by the raw data size in the non-FL scenario.

Using the error rate serves as an evaluation metric for the classification performance of the proposed model while computational efficiency is associated with energy consumption and its corresponding environmental impact, and communication efficiency is connected to throughput and bandwidth needs. These considerations are vital when evaluating the sustainability of a solution.

Therefore, the sustainability indicator (S) is computed using the following equation:

$$S = S^{tr} + S^{Inf} \tag{1}$$

where S^{tr} and S^{Inf} are the sustainability indicators for training and testing/inference, respectively. S^{tr} is defined as:

$$S^{tr} = (1 + E_{tr}) \times (1 + C_{tr}) \times (1 + D_{tr}) \tag{2}$$

where E_{tr} is the training error rate (which is $1 - accuracy$), C_{tr} represents the energy consumed by our model during the training in Wh, and D_{tr} is the data size communicated to the cloud server during the model training in terms of kB. In particular, to calculate the D_{tr}, we used the formulas proposed in [17]; hence, it is calculated as follows:

$$D_{tr} = P \times R_g \times (2 \times size(H)) \tag{3}$$

where P is the number of participants in each communication round, R_g represents the total number of global rounds, and $size(H)$ is the size of the model/data exchanged between the device/edge servers and cloud server in each communication round. Furthermore, as mentioned in the paper [16], a lower value of S^{tr} indicates better computational and communication efficiency relative to accuracy. An ideal model would have $E_{tr} = C_{tr} = D_{tr} = 0$ and $S^{tr} = 1$. Lastly, S^{Inf} is defined as:

$$S^{Inf} = (1 + E_{Inf}) \times (1 + C_{Inf}) \tag{4}$$

where E_{Inf} represents the inference error rate and C_{Inf} represents the energy consumed by our model during the inference. During the inference, we do not consider the communication cost as each client keeps its own model locally. Similar to S^{tr}, the ideal $S^{Inf} = 1$ and $C_{Inf} = E_{Inf} = 0$.

IV. Experiments and Performance Evaluation

In this section, we first describe the experimental parameters and the dataset. Then, we evaluate our proposed model in terms of classification performance, training time, energy, communication cost, and most importantly sustainability.

A. Experimental Setup

1) Implementation Details: In this study, we use `PyTorch` and `snnTorch` as libraries. All experiments are run on a Apple M1 Pro, and 32GB of RAM. The energy consumption per considered model is measured using `CodeCarbon`[1], a tool that monitors the energy consumed either in GPU or CPU during the training. The communication overhead is quantified by the data size to be transmitted between the cloud server and the edge servers (resp. IoT devices) in each communication round with our SNN-based HFL model (resp. classical FL). To evaluate the performance, we compare our proposed model with FL+SNN and non-FL in terms of accuracy, energy consumption, communication cost, and sustainability.

2) Dataset description: To evaluate the performance of the proposed model, we have chosen one of the most recent datasets, called *Edge-IIoTset*, published in 2022 [18]. This dataset contains 46 features and 15 classes, normal and 14 attacks, where the normal traffic represents 72.8% of the total samples used. In alignment with the paper of the dataset [18], we drop unnecessary flow features such as IP addresses, ports, timestamps, and payload information. Moreover, as this dataset consists of different features with values in different scales, the data are normalized so all their values are in the range of [0,1]. In addition, to evaluate the performance of our model, we split the dataset into two subsets: train (80%), validation (10%), and test (10%).

3) Implementation Settings: The experiments have been conducted over a fully connected SNN model with 3 layers, Adam as an optimizer, Softmax as a classification function, and learning rate = 0.0001. Also, we use 5 local epochs for model training, 10 rounds as sub-global rounds (between device and edge server), and 5 rounds as global rounds (R_g) in total. For a fair comparison, we use 5 local epochs and 10 global rounds with FL+SNN, whereas with non-FL we use 250 as training epochs. Moreover, in all simulations, we encode the data values into spike trains of length T using rate coding.

B. Experimental Evaluation

1) Classification performance: Table I shows the classification performance of our model against baseline schemes, which are the non-FL model and classical FL+SNN model with IID data in terms of accuracy and F1-score. Overall, our model `SURFS` achieves a higher accuracy and F1-score in comparison to FL+SNN. This enhanced performance is achieved with significantly fewer global communication rounds (5 global rounds). Furthermore, our model outperforms the non-FL model with only 0.5 active rates of 100 clients (meaning 10% of clients participate in each round). In addition, as shown in the table, our model not only improves the classification performance but also accelerates the convergence of the global model and in turn requires less training time than others (**3**× faster than FL+SNN and **17**× that of non-FL).

[1]https://github.com/mlco2/codecarbon

TABLE I
PERFORMANCE OF THE PROPOSED MODEL (SURFS) AGAINST THE CLASSICAL FL AND NON-FL MODEL WITH IID DATA.

Metric	Non-FL	FL+SNN	**SURFS**
Accuracy (%)	92.19	92.90	**93.40**
F1-score (%)	92.02	91.79	**93.06**
Training time (s)	228,907	38,564	**13,137**

2) Impact of data distribution: To study the impact of non-IID data on the performance of our model, we vary the α parameter of the Dirichlet distribution [19], which controls the degree of non-IIDness in the data distribution among the devices. For example, if $\alpha \to \infty$, all clients have an IID data distribution, and if $\alpha \to 0$ each client holds samples from only one randomly chosen class. Figure 2 and Figure 3 show the performance of `SURFS` and classical FL in terms of accuracy and training time respectively. It can be seen that the data distribution/heterogeneity can impact the performance of both `SURFS` and the FL+SNN model. In particular, the skewed distribution of data makes the global model struggle to converge and to generalize well across all clients, leading to increasing the training time with reduced accuracy. However, our model `SURFS` performs better than classical FL especially when dealing with a higher degree of non-IID data. This is because HFL introduces a hierarchical structure where edge servers can perform intermediate aggregations. This local aggregation helps in capturing local data patterns better, contributing to improved global model performance and fast convergence.

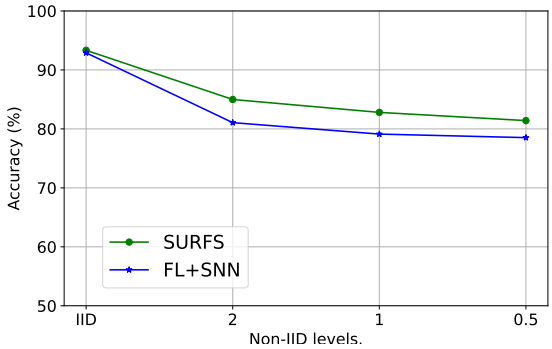

Fig. 2. Classification accuracy under IID data and different non-IID levels (α).

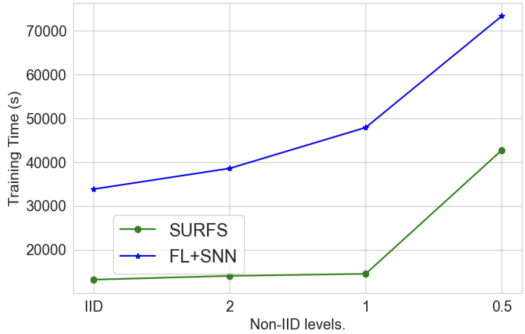

Fig. 3. Training time under IID data and different non-IID levels (α).

3) Communication and energy costs:

- **Communication overhead:**

To calculate the communication overhead of our SURFS and classical FL+SNN model, we used the equation 3. As can be seen in Figure 4 the size of the communication overhead is greatly decreased by **99%** and **97%** compared to non-FL and FL+SNN, respectively. The intermediate layer within HFL significantly improves the performance of SURFS as compared to FL+SNN since it speeds up the convergence and, as a result, lowers communication costs. Furthermore, the greater performance of SURFS in comparison to non-FL is due to the HFL/FL training process that sends only model parameters and not raw data samples to the central entity. This benefit will be significantly more important if the training data become larger. This is also attributed to several characteristics of SNN and how it learns from the data. Thus, SURFS not only optimizes bandwidth usage but also enhances data privacy and security, as sensitive information is not exposed during transmission. Thereby, SURFS paves the way towards robust and secure distributed learning, especially in environments constrained by limited communication resources.

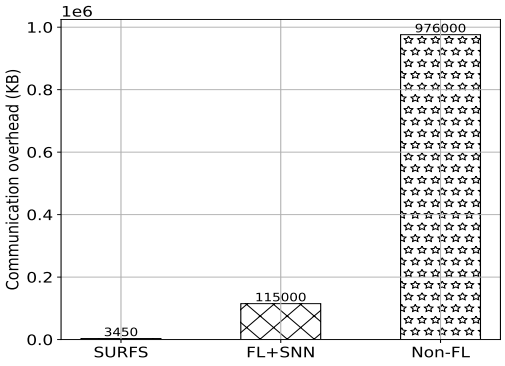

Fig. 4. communication overhead (Lower implies better).

- **Energy cost:**

Integrating SNNs into HFL can potentially lead to further reductions in energy consumption, particularly at the IoT device levels where computations are performed. The training and inference phases of machine learning need energy. In this subsection, we study the energy used during training because the inference time of our model inference is marginal. As shown in Figure 5, using the CodeCarbon library, we can quantify the energy consumption (in Wh) of our model against FL+SNN and non-FL models. We can notice that the data distribution impacts the energy consumption of the HFL/FL model training. This is intuitive as we will see later in Table II that the high data heterogeneity increases the training time. On the other hand, with IID and non-IID (with different values of α), SURFS consumes less energy. On the other hand, the overall energy consumption of non-FL is high due to the volume of computations required for training the model on large datasets.

Moreover, the lack of hierarchical aggregation means that FL+SNN may require more iterations to converge compared to HFL+SNN, resulting in higher computational energy consumption. HFL+SNN emerges as the most energy-efficient due to the hierarchical structure of HFL that enables efficient aggregation of model updates at the edge servers and leads to faster convergence. In addition, SNN is known for its energy efficiency due to its event-driven nature, where neurons only activate and consume energy when necessary. This makes the computations more sparse and energy-efficient. Thus, we can conclude that SURFS is much better than FL+SNN and non-FL settings during the training phase and in turn has less CO_2 emission and environmental impact.

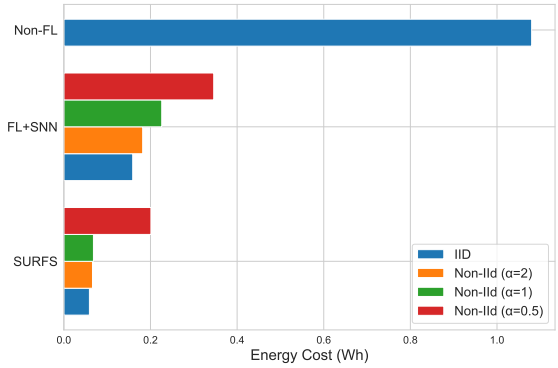

Fig. 5. Total energy consumed during the training (Lower implies better).

4) Sustainability Evaluation: In this section, we discuss an important factor that is expected to be used during the choice between non-FL, FL+SNN, and SURFS towards a sustainable solution. The sustainability (S) is measured here in terms of classification accuracy, along with computational and communication efficiencies throughout both the training and inference phases, as defined in equation 1. Table II presents a comprehensive summary of the pertinent parameters gathered for each model variant, under both IID and non-IID data scenarios, subsequently leading to the computation of S for each case (the lower S, the more sustainable).

From the results, it is evident that SURFS distinguishes itself as a sustainable and greener alternative. This advancement in sustainability can be primarily attributed to two major factors: its consistently high classification accuracy and significantly reduced communication energy costs. On the contrary, the non-FL paradigm emerges as the least sustainable model. The inherent inefficiencies of non-FL can be attributed to its larger dataset sizes and higher energy consumption. Along with its leak privacy preservation of the data users. This is further exacerbated by its inability to safeguard user data privacy, as the necessity to centralize data poses substantial privacy risks. FL+SNN shows improvement over non-FL with reduced error rates and communication overhead. However, it is still not as efficient as SURFS. On the other hand, with non-IID ($\alpha = 2$ and $\alpha = 1$) both FL+SNN and SURFS show increased error rates and decreased sustainability compared to the IID scenario. Moreover, when $\alpha = 0.5$, we can notice that FL+SNN faces significant challenges when a higher error rate and lower sustainability. Although SURFS is affected

TABLE II
STATISTICAL MEASURES OF THE ERROR RATE, COMPUTATIONAL CONSUMPTION, COMMUNICATION OVERHEAD AND MODELS SUSTAINABILITY.

Data distribution	**Model**	E_{tr}	E_{Inf}	C_{tr}	C_{Inf}	$size(H)$	S^{Inf}	$S^{tr}(\times 10^3)$	$S(\times 10^3)$
IID	Non-FLSNN	7.88	7.81	1.080	0.0001	976000	8.8	18027.128	18027.136
	FL+SNN	7.1	7.1	0.159	0.0001	115	8.1	1079.617	1079.625
	SURFS	**6.6**	**6.6**	**0.059**	**0.0001**		**7.6**	**26.382**	**26.389**
Non-IID (α = 2)	FL+SNN	18.98	18.94	0.1	0.0001	-	19.94	2715.905	2715.924
	SURFS	**15.02**	**15.01**	**0.066**	**0.0001**		**16.01**	**58.933**	**58.949**
Non-IID (α = 1)	FL+SNN	20.94	20.88	0.226	0.0001	-	21.88	3093.347	3093.369
	SURFS	**17.24**	**17.2**	**0.068**	**0.0001**		**18.28**	**67.226**	**67.244**
Non-IID (α = 0.5)	FL+SNN	21.5	21.48	0.346	0.0001	-	22.48	3482.805	3482.827
	SURFS	**18.54**	**18.59**	**0.201**	**0.0001**		**19.59**	**80.986**	**81.006**

by the extreme non-IID condition, it still maintains better performance and sustainability than FL+SNN. In summary, these results indicate that the non-FL solution is no longer efficient for IDS due to its high energy consumption and communication overhead in contrast to our SURFS scheme, which is environmentally sustainable. It is able to handle both IID and non-IID scenarios effectively, ensuring high intrusion detection accuracy while minimizing energy costs and upholding data privacy.

V. CONCLUSION

This paper proposes a novel sustainable IDS with SNN-based HFL called SURFS. We have used a sustainability indicator for evaluating energy and communication costs with respect to accuracy, which enables fair comparisons across various classical FL and non-FL under IID and non-IID data. Experimental results using one of the most recent datasets have shown that SURFS is a robust solution for IDS, achieving superior performance, faster convergence (**3**$\times$ faster than FL+SNN and **17**$\times$ that of non-FL), low communication overhead (reduction by **99%** and **97%** compared to non-FL and FL+SNN, respectively), and substantial energy savings (62% more efficient than FL+SNN and 94% more efficient than the non-FL model). The preliminary results and the sustainability-centric approach of our work pave the way for future research and implementations, driving towards energy-efficient and environmentally conscious IDS solutions.

REFERENCES

[1] "Cisco edge-to-enterprise iot analytics for electric utilities solution overview, 2020." https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/big-data/solution-overview-c22-740248.html.

[2] "The growth in connected iot devices is expected to generate 79.4zb of data in 2025, according to a new idc forecast. accessed:," https://infohub.delltechnologies.com/.

[3] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, and C.-T. Lin, "Edge of things: The big picture on the integration of edge, iot and the cloud in a distributed computing environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2017.

[4] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964–988, 2021.

[5] L. Liu, J. Zhang, S. Song, and K. B. Letaief, "Client-edge-cloud hierarchical federated learning," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[6] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *arXiv preprint arXiv:2106.09527*, 2021.

[7] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in iomt," *IEEE journal of biomedical and health informatics*, vol. 27, no. 2, pp. 722–731, 2022.

[8] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, vol. 22, no. 1, pp. 949–961, 2019.

[9] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, 2021.

[10] J. L. Lobo, J. Del Ser, A. Bifet, and N. Kasabov, "Spiking neural networks and online learning: An overview and perspectives," *Neural Networks*, vol. 121, pp. 88–100, 2020.

[11] O. Aouedi, K. Piamrat, and M. Südholt, "Hfedsnn: Efficient hierarchical federated learning using spiking neural networks," in *21st ACM International Symposium on Mobility Management and Wireless Access (MobiWac 2023)*, 2023.

[12] X. Sun, Z. Tang, M. Du, C. Deng, W. Lin, J. Chen, Q. Qi, and H. Zheng, "A hierarchical federated learning-based intrusion detection system for 5g smart grids," *Electronics*, vol. 11, no. 16, p. 2627, 2022.

[13] H. Saadat, A. Aboumadi, A. Mohamed, A. Erbad, and M. Guizani, "Hierarchical federated learning for collaborative ids in iot applications," in *2021 10th Mediterranean Conference on Embedded Computing (MECO)*. IEEE, 2021, pp. 1–6.

[14] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "Hbfl: A hierarchical blockchain-based federated learning framework for collaborative iot intrusion detection," *Computers and Electrical Engineering*, vol. 103, p. 108379, 2022.

[15] X. Sáez-de Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous iot networks," *Computers & Security*, vol. 131, p. 103299, 2023.

[16] V. Perifanis, N. Pavlidis, S. F. Yilmaz, F. Wilhelmi, E. Guerra, M. Miozzo, P. S. Efraimidis, P. Dini, and R.-A. Koutsiamanis, "Towards energy-aware federated traffic prediction for cellular networks," *arXiv preprint arXiv:2309.10645*, 2023.

[17] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semi-supervised learning for attack detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2022.

[18] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," 2022.

[19] M. Yurochkin, M. Agarwal, S. Ghosh, K. Greenewald, N. Hoang, and Y. Khazaeni, "Bayesian nonparametric federated learning of neural networks," in *International conference on machine learning*. PMLR, 2019, pp. 7252–7261.