2024 International Conference on Smart Applications, Communications and Networking (SmartNets) | 979-8-3503-8532-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/SMARTNETS61466.2024.10577653

Combating Malware Traffic in Emerging Networks: A Collaborative Learning Approach

Harshith Vaitla*[1], Gad Gad*[2], Zubair Md Fadlullah*[3], and Mostafa M. Fouda‡§[4]
*Department of Computer Science, Western University, London, ON, Canada.
‡Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID, USA.
§Center for Advanced Energy Studies (CAES), Idaho Falls, ID, USA.
Emails: [1]hvaitla@uwo.ca, [2]ggad@uwo.ca, [3]zfadlullah@ieee.org, [4]mfouda@ieee.org

***Abstract*—Identifying and mitigating malicious traffic poses a major challenge in the evolving field of network security. As threat profiles rapidly evolve, dynamic and adaptive methods are needed to match the swiftly changing attack patterns. This paper introduces a novel application of Federated Learning (FL) in the realm of malware traffic detection. As a distributed training framework, FL allows multiple network nodes to collaboratively learn a shared prediction model while keeping all the training data localized, thus ensuring data privacy and security. We present an effective malware identification and classification architecture utilizing Convolutional Neural Networks (CNN) within the FL framework distributed among network nodes. The paper details the design and implementation of this system, highlighting the integration of FL to harness the collective intelligence of diverse data sources without compromising data privacy. Our approach provides a scalable and efficient solution adaptable to diverse network environments. The results showcase the potential of FL in enhancing network security mechanisms, opening new avenues for combatting sophisticated cyber threats in an increasingly connected world.**

***Index Terms*—Federated Learning, Data Privacy, Malware Traffic Detection, Networked Systems**

I. Introduction

Advanced cyber security threats, in the form of Malware, are evolving rapidly presenting a critical concern in network security. Traditional malware detection and network monitoring methods are proving inadequate in the face of these advanced threats. These conventional approaches, predominantly centralized, often fail to scale effectively with different network environments [1], [2]. Additionally, The diverse and evolving nature of malware necessitates a more adaptive, robust, and responsive system for threat detection and mitigation.

Deep learning is a powerful traffic analysis tool that requires abundant and recent data to train up-to-date models [3]. Moving data from users' devices poses privacy risks to their data. We propose an approach that leverages the capabilities of Federated Learning (FL) to enhance malware traffic detection within network infrastructures [4]–[8]. Federated Learning, emerging as a potent paradigm in distributed machine learning, allows for the collaborative training of a shared prediction model across multiple network nodes [9]. This collaborative approach enables the leveraging of data from diverse sources, contributing to a more comprehensive and effective detection system [10]. More importantly, it does so while ensuring the privacy and security of users training data.

Our paper proposes a novel architecture based on Convolutional Neural Networks (CNN). By utilizing CNN, known for its proficiency in feature extraction and pattern recognition, in conjunction with FL's decentralized and collaborative nature, our system can adaptively learn from multiple data sources.

Our research highlights the significant improvements in detection rates and response times achieved by this FL-based system. Additionally, the paper delves into the system architecture, elucidating how the fusion of CNN and FL leads to a more resilient and dynamic malware detection mechanism.

In summary, the integration of Federated Learning into network security represents a transformative shift in approach. This method introduces more dynamic, efficient, and privacy-conscious strategies for malware detection. Our research not only highlights the real-world applicability of Federated Learning but also lays the groundwork for future advancements in this area in the face of ever-evolving cyber threats.

The structure of this paper is outlined as follows: Section II provides an overview of the pertinent research in this field. Section III delineates the research problem under consideration. Section IV introduces the proposed Federated learning-based malware detection model. In Section V, we assess the efficacy of our proposed method. Followed by Future work in Section VI. The paper concludes with Section VII, summarizing our findings and contributions.

II. Related Work

The field of network security [11], particularly in the context of malware traffic detection, has witnessed significant advancements due to the interplay of machine learning techniques and network technologies. This section explores various studies that have contributed to this domain, with a focus on federated learning [10], [12], convolutional neural networks, and other related methodologies.

Sakib *et al.* [13] proposed a method for electrocardiogram (ECG) analytics focused on arrhythmia detection using an asynchronous weight updating federated learning approach. The study stands out for its application in a healthcare context, where privacy is paramount. By leveraging federated learning, the study demonstrated a method that maintains data privacy while ensuring accurate medical diagnostics [14], [15].

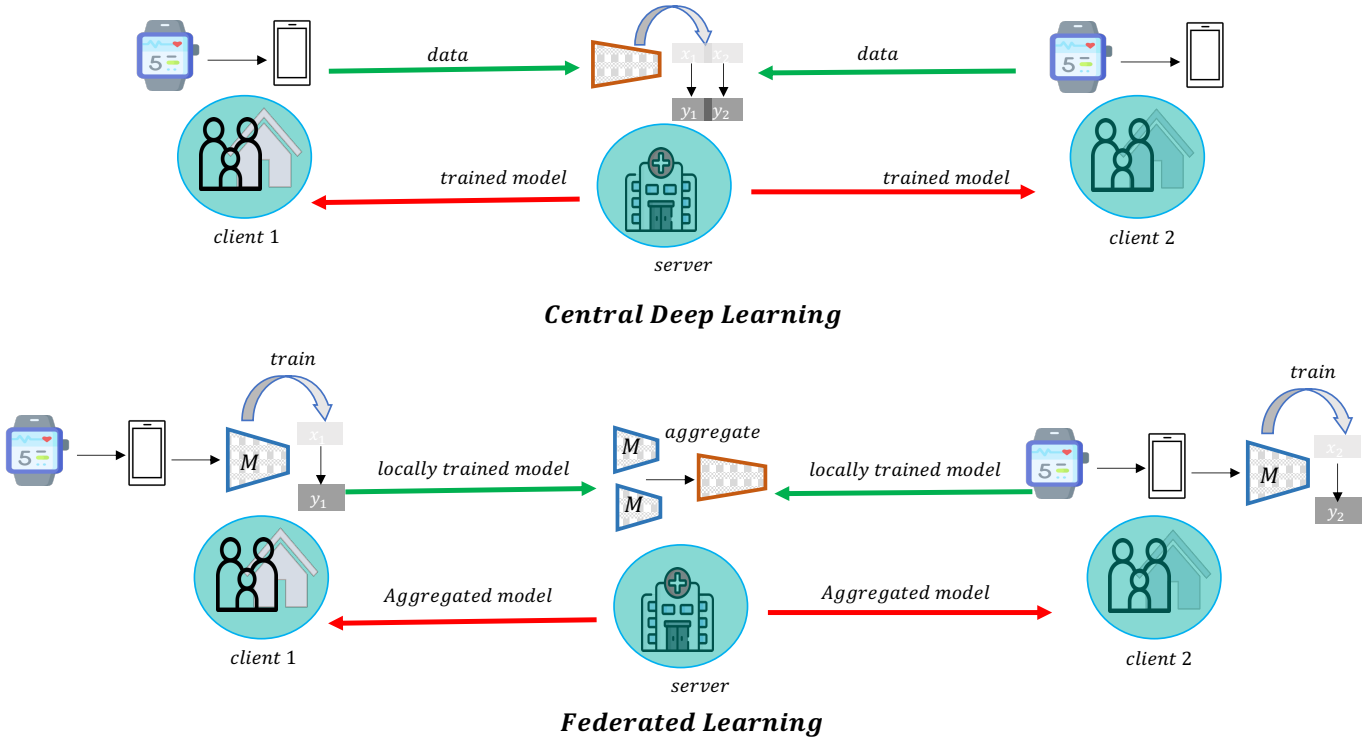

Fig. 1. Contrast between centralized learning and federated learning-based collaborative learning paradigms.

The authors in [16] addressed the challenge of limited communication bandwidth in federated learning. The proposed solution introduces an innovative asynchronous learning strategy, differentiating between shallow and deep layers of neural networks for updating frequencies. This approach, paired with temporally weighted aggregation on the server, enhances both the accuracy and convergence of the central model. The study is particularly relevant for scenarios with restricted bandwidth, highlighting the adaptability of federated learning in diverse environments [17], [18].

Deploying Artificial Intelligence (AI) applications is challenging due to computation and communication resource constraints. The authors in [19] explored the application of federated learning in the context of edge computing and Internet of Things (IoT) systems. Their research focuses on developing an asynchronous weight-updating federated learning algorithm, with a specific application to face mask detection. This study is pioneering in its approach to integrating federated learning with IoT systems, emphasizing the potential of this technology in enhancing edge computing capabilities [20], [21].

In the domain of malware detection, Wang *et al.* presented an innovative approach to network security, [22] and introduced a method for malware traffic classification using a CNN model that processes raw traffic data as images. This technique, notable for its application of representation learning to network security, eliminates the need for hand-designed features and directly utilizes raw traffic data for classification. The approach not only demonstrates high accuracy in malware detection but also underscores the versatility of CNNs in handling diverse data types beyond traditional image processing.

These studies collectively lay the groundwork for our research, demonstrating the efficacy of federated learning and deep learning techniques in network security contexts. They also highlight the ongoing evolution of methodologies in tackling the challenges of privacy, communication efficiency, and computational constraints in distributed learning environments. As we build upon these foundations, our project aims to further explore the synergies between federated learning and CNNs for robust and efficient malware traffic detection in network systems.

III. Problem Description

The primary challenge lies in accurately detecting malware traffic in a decentralized manner while ensuring data privacy and minimizing the need for data transmission. Traditional centralized models require transferring vast amounts of potentially sensitive data to a central server for processing, which raises privacy concerns and increases vulnerability to data breaches. Moreover, centralized models may not efficiently adapt to the unique malware patterns and behaviors present in different network segments.

The federated learning approach addresses these challenges by enabling local model training on client nodes (representing different network segments), with each node processing its traffic data. This method ensures that the raw data remains within the client's domain, significantly enhancing data privacy and security. The challenge is to effectively synchronize and aggregate these local learnings to build a comprehensive,

robust model capable of detecting a wide array of malware traffic patterns. Figure 1 provides an overview illustration of the working principles of central learning and federated learning.

Another critical aspect of the problem is the inherent diversity in network traffic patterns across different segments of the network. Each client node encounters unique traffic, which may include varying types and behaviors of malware. This diversity presents both a challenge and an opportunity - a challenge in harmonizing these diverse learnings into a single coherent model, and an opportunity to develop a more versatile and comprehensive detection system.

Implementing federated learning in this context also involves overcoming algorithmic and architectural challenges. Designing a CNN architecture that can effectively process and learn from network traffic data, conceptualized as image-like data, requires careful consideration. Additionally, developing an efficient federated learning algorithm that can handle the training, aggregation, and updating of models across multiple clients is crucial. The algorithm must ensure that the learning process is not only effective in detecting malware but also efficient in terms of communication and computational resources.

The ultimate objective is to create a federated learning-based system that can detect malware traffic with high accuracy and efficiency while maintaining user privacy and minimizing network overhead. This system should be capable of adapting to evolving malware threats and scalable across various network sizes and configurations.

IV. Proposed Design and Architecture

A. System Architecture

The system's architecture is designed to implement federated learning for enhanced malware traffic detection in networks. It consists of multiple client nodes and a central server node. Each client node represents a different network segment, possessing its unique dataset of network traffic, which includes both benign and malware traffic. The central server coordinates the learning process across different clients without accessing their actual data, thereby preserving privacy and reducing data transmission costs.

B. Proposed Learning Model Architecture

The learning model is a Convolutional Neural Network (CNN), known for its effectiveness in handling image-based data. Considering the network traffic as image-like data, CNN can extract intricate patterns and features that distinguish between benign and malware traffic. The model architecture comprises several layers:

- Input Layer: Accepts pre-processed traffic data reshaped into a format suitable for convolutional operations.
- Convolutional Layers: These layers perform the convolution operation, extracting features from the input data. The use of multiple filters enables the model to learn various aspects of the traffic data.
- Pooling Layers: Follow the convolutional layers to reduce the dimensionality of the data, focusing on the most relevant features.
- Flattening Layer: Converts the 2D feature maps into a 1D feature vector, preparing the data for the fully connected layer.
- Fully Connected Layer: A dense layer that integrates signals from the feature extraction layers to make the final classification decision.
- Output Layer: Uses a softmax activation function for multi-class classification, providing the probability distribution over different traffic classes.

C. Proposed Algorithm

The federated learning algorithm involves training individual models on client nodes and aggregating their learned parameters on the server node. The process is as follows:

- Data Loading and Preprocessing: Each client node loads its local data, performing necessary preprocessing steps like normalization and reshaping.
- Model Initialization: Each client initializes a local CNN model with the architecture defined in part B.
- Local Training: Clients train their models on local datasets. The training process is privacy-preserving as data does not leave the client's premises.
- Parameter Aggregation: After training, clients send their model parameters to the central server. The server aggregates these parameters to update the global model. The aggregation function typically involves averaging the weights of the same layers from different client models.
- Global Model Update and Distribution: The updated global model is then sent back to the clients for further training or inference tasks.
- Federated Learning with Stratified K-Fold Validation: The federated learning process is enhanced with Stratified K-Fold cross-validation to improve model robustness and generalizability.
- Global Model Evaluation: The global model's performance is evaluated on a held-out test dataset to assess its accuracy in detecting malware traffic.

An overview of the Malware Traffic Detection Federated Learning algorithm is shown in algorithm 1.

V. Performance Evaluation

In this section, we evaluate the performance of our proposed method.

A. Dataset Preparation

For this research we have utilized a specialized dataset that is derived from preprocessed results from the work of [22]. This dataset is tailored to address the specific requirements of malware traffic detection in network environments, where the detection accuracy and the ability to handle diverse traffic patterns are crucial. The dataset is structured to support federated learning, ensuring that it caters to the nuances of

Algorithm 1 Federated Learning For Malware Traffic Detection

function SGD(Initial Model θ_k^{r-1}, Dataset D_k, Number of epochs E)
  Initialize model weights: $\theta_k^{r,0} \leftarrow \theta_k^{r-1}$
  for epoch $e = 1, 2, \ldots, E$ **do**
    for each batch (X_i, y_i) in D_k **do**
      Compute gradient: $\nabla_{\theta_k^{r,e}} \mathcal{L}(\theta_k^{r,e}, X_i, y_i)$ ▷ Loss gradient
      Update model weights: $\theta_k^{r,e+1} \leftarrow \theta_k^{r,e} - \eta \nabla_{\theta_k^{r,e}}$ ▷ SGD update
    end for
  end for
  return θ_k^r
end function
function MAIN
  Input: Local dataset : D_k, Initial global model weights: θ_0, Number of communication rounds: N_r, Number of epochs: E, Total number of participating clients: N_k, DP parameters ϵ and δ, Gradient Clipping norm S
  Output: Collaboratively trained global model θ^R
  Initialize model θ_0
  for round $r = 1, 2, \ldots, N_r$ **do**
    $K^r \leftarrow$ randomly select K participants
    for each participant $k \in K^r$ **do**:
      $\theta_k^r \leftarrow \text{SGD}(\theta_k^{r-1}, D_k, E)$ ▷ Clients train in parallel
    end for
    $\theta^{r+1} \leftarrow \sum_{k \in K^r} \theta_k^r$
  end for
  return θ^R
end function

distributed learning while maintaining the integrity and privacy of data.

The dataset comprises a comprehensive collection of network traffic data, categorized into benign and malicious traffic. It includes various types of malware traffic, encompassing a wide range of attack vectors and patterns. The benign traffic data encapsulates regular network activities, providing a contrasting background to identify anomalies effectively.

Before its inclusion in the dataset, the traffic data underwent extensive preprocessing. This process involved the conversion of raw network traffic into a format that is suitable for analysis by CNNs, a core component of our federated learning model. The preprocessing steps included:

- Continuous network traffic was segmented into discrete units based on predetermined criteria, ensuring uniformity in data representation.
- To preserve privacy and security, the dataset was anonymized, with sensitive information such as IP addresses and MAC addresses randomized.
- Key features from the network traffic data were extracted and normalized to create a consistent input format for the CNN.
- Each data unit was labeled as either benign or malicious, based on its characteristics and known patterns of network behavior

In the context of federated learning, the dataset serves as the foundational element for training local models on client nodes. Each node, representing a unique segment of the network, utilizes a portion of this dataset to train its model independently. The federated learning framework ensures that the learning process is decentralized and privacy-preserving, as the raw data remains within the client's domain.

B. Evaluation Methodology

The federated learning model for malware traffic detection underwent a thorough evaluation to assess its performance in comparison to a centralized learning model. The key focus of this evaluation was on the model's accuracy, scalability, and effectiveness in a distributed learning environment.

C. Experimental Setup

The dataset included both benign and malicious network traffic. It was appropriately segregated into training and testing sets, with the training set distributed among multiple clients for the federated learning process.

D. Model Configuration

- Configured as per the proposed architecture, with parameters adjusted for distributed learning.
- Established as a baseline for comparison, with standard centralized training methodology. Training Process:
- Implemented through multiple rounds involving local training on client nodes and subsequent aggregation of learned parameters.
- Employed to ensure a comprehensive evaluation across different data subsets.
- Varied number of clients involved in the training to replicate real-world distributed data environments.

E. Results and Analysis

- Evaluated using accuracy, precision, recall, and F1-score, the federated learning model displayed an accuracy of 84.07%, while the centralized model showed 89%.
- The federated learning model exhibited a notable increase in accuracy correlated with the rising number of participating client nodes as demonstrated in Fig. 2. This increment was systematically observed across various client configurations. Specifically, with an initial setup of 3 clients, the model achieved an accuracy of 74.02%. This accuracy improved to 77.06% when the number of clients was increased to 6. A further increase to 10 clients led to an accuracy of 79.67%, demonstrating a consistent upward trend. When the client count reached 13, the model's accuracy was further enhanced to 81.83%. The peak performance was observed at 15 clients, where the model achieved its highest accuracy of 84%. These results underline the effectiveness of federated learning in environments with a diverse range of client nodes,

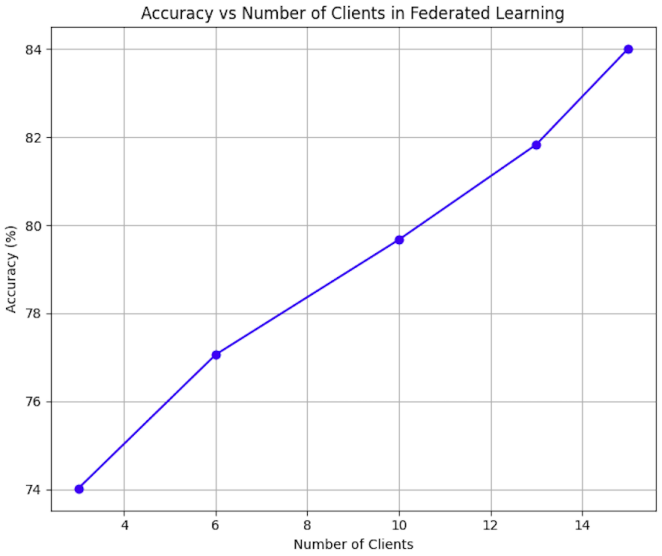

Fig. 2. Accuracy vs. number of clients in federated learning.

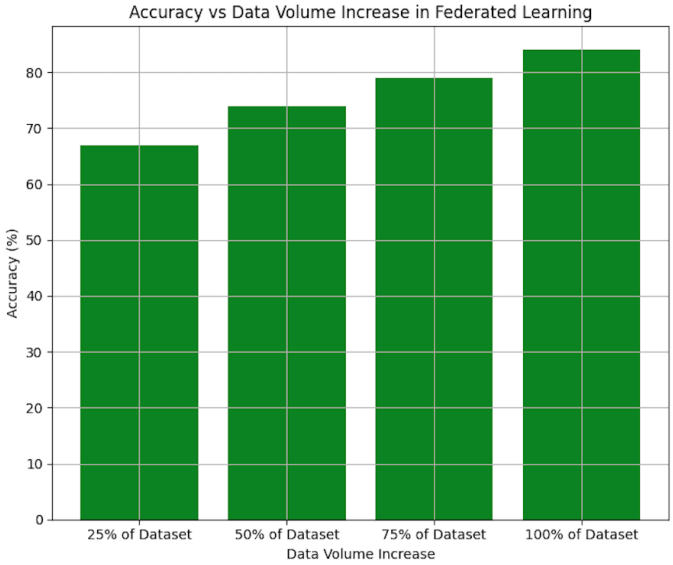

Fig. 3. Accuracy vs. data volume increase in federated learning.

highlighting its capability to leverage the collective data for more accurate predictions.

- Parallel to the client-based evaluation, the study also focused on understanding the impact of increasing data volumes on the model's accuracy as demonstrated in the results presented in Fig. 3. This aspect of the experiment revealed a direct positive correlation between the volume of data used for training and the accuracy of the malware detection model. With 25% of the dataset utilized, the model attained an accuracy of 67%. This accuracy figure rose to 74% when the data volume was increased to 50%. A further increase to 75% of the dataset saw an improvement in accuracy to 79.07%. Notably, the utilization of the complete dataset (100%) resulted in the model achieving its optimal accuracy of 84%. These findings decisively suggest that the federated learning model's ability to effectively detect malware traffic is enhanced significantly with larger datasets, thereby emphasizing the importance of comprehensive data in training robust network security models.
- Despite the centralized model showing higher accuracy in standard conditions, the federated learning model demonstrated superior performance in more complex scenarios involving larger data and more clients. This underscores the federated model's adaptability and efficiency in learning from diverse and distributed data sources.

F. Discussion

The results indicate that while the federated learning model has a slightly lower accuracy in standard settings compared to the centralized model, it excels in larger and more complex network environments. Its ability to effectively learn from distributed data sources and adapt to the increase in data volume and client numbers highlights its suitability for real-world applications in network security. The model's performance improvement in scalable scenarios is particularly promising for large-scale network systems facing diverse security threats.

VI. Future Work

Future work can explore extending this work to areas addressing optimization for Non-IID data, where data distributions from different clients are different, and developing integration frameworks to seamlessly integrate FL security solutions into real-world security applications.

The potential of federated learning in enhancing network security is immense, particularly in its ability to handle complex, large-scale data while preserving user privacy. The path forward involves refining the technology to address current limitations and exploring its integration into broader network security strategies.

VII. Conclusion

Malware detection applications face the challenge of continuously developing malicious software and malware. Federated Learning is a promising distributed training paradigm that protects the users' data privacy. In this work demonstrated the implementation of federated learning for malware traffic detection in network environments, showcasing a promising approach to enhancing network security. Federated learning, as compared to centralized models, shows substantial promise, particularly in scenarios characterized by large datasets and a multitude of clients. One of the key advantages of federated learning is its inherent capability to maintain data privacy, as it processes data locally at the client level without requiring data to be shared centrally. This enhances security and aligns with contemporary data privacy laws and regulations.

While centralized models have higher accuracy in certain scenarios, federated learning is inherently private and can adapt to different scenarios and environments. This adaptability, along with the inherent data privacy and security features,

positions federated learning as a significant advancement in the field of network security.

REFERENCES

[1] A. Gaurav, B. B. Gupta, and P. K. Panigrahi, "A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system," *Enterprise Information Systems*, vol. 17, no. 3, article no. 2023764, 2023.

[2] Z. M. Fadlullah and A. Benslimane, "Joint provisioning of QoS and security in IoD networks: Classical optimization meets AI," *IEEE Internet of Things Magazine*, vol. 4, no. 4, pp. 40–46, 2021.

[3] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[4] Z. M. Fadlullah and N. Kato, "On smart IoT remote sensing over integrated terrestrial-aerial-space networks: An asynchronous federated learning approach," *IEEE Network*, vol. 35, no. 5, pp. 129–135, 2021.

[5] G. Gad, Z. M. Fadlullah, K. Rabie, and M. M. Fouda, "Communication-efficient privacy-preserving federated learning via knowledge distillation for human activity recognition systems," in *ICC 2023 - IEEE International Conference on Communications*, pp. 1572–1578, 2023.

[6] G. Gad, A. Farrag, Z. M. Fadlullah, and M. M. Fouda, "Communication-efficient federated learning in drone-assisted IoT networks: Path planning and enhanced knowledge distillation techniques," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2023.

[7] G. Gad, Z. M. Fadlullah, M. M. Fouda, M. I. Ibrahem, and N. Nasser, "Joint knowledge distillation and local differential privacy for communication-efficient federated learning in heterogeneous systems," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, pp. 2051–2056, 2023.

[8] G. Gad, A. Farrag, A. Aboulfotouh, K. Bedda, Z. M. Fadlullah, and M. M. Fouda, "Joint self-organizing maps and knowledge-distillation-based communication-efficient federated learning for resource-constrained UAV-IoT systems," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15504–15522, 2024.

[9] A. H. Bondok, M. Mahmoud, M. M. Badr, M. M. Fouda, M. Abdallah, and M. Alsabaan, "Novel evasion attacks against adversarial training defense for smart grid federated learning," *IEEE Access*, vol. 11, pp. 112953–112972, 2023.

[10] F. Sattler, S. Wiedemann, K. R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-IID data," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 9, pp. 3400–3413, 2019.

[11] Z. M. Fadlullah, C. Wei, Z. Shi, and N. Kato, "GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1037–1050, 2017.

[12] M. Mohri, G. Sivek, and A. T. Suresh, "Agnostic federated learning," in *International Conference on Machine Learning*, pp. 4615–4625, 2019.

[13] S. Sakib, M. M. Fouda, Z. M. Fadlullah, K. Abualsaud, E. Yaacoub, and M. Guizani, "Asynchronous federated learning-based ecg analysis for arrhythmia detection," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2021.

[14] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of FedAvg on non-IID data," in *International Conference on Learning Representations*, 2019.

[15] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[16] Y. Chen, X. Sun, and Y. Jin, "Communication-efficient federated deep learning with asynchronous model update and temporally weighted aggregation," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 10, pp. 4229–4238, 2020.

[17] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[18] V. Smith, C. K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated multi-task learning," in *Advances in Neural Information Processing Systems*, pp. 4424–4434, 2017.

[19] Y. Gupta, Z. M. Fadlullah, and M. M. Fouda, "Toward asynchronously weight updating federated learning for AI-on-edge IoT systems," in *2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 2022.

[20] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial Intelligence and Statistics*, pp. 1273–1282, 2017.

[21] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *ArXiv Preprint, ArXiv:1610.05492*, 2016.

[22] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *2017 International Conference on Information Networking (ICOIN)*, pp. 712–717, 2017.