A Privacy-Preserving Federated Learning Framework for Robust Intrusion Detection in Decentralized Networks Using Packet Data

Quoc H. Nguyen*
University of South Florida
Tampa, Florida, USA
nguyenq29@usf.edu

Soumyadeep Hore*
University of South Florida
Tampa, Florida, USA
soumyadeep@usf.edu

Ankit Shah†
Indiana University
Bloomington, Indiana, USA
ankit@iu.edu

Trung Le
University of South Florida
Tampa, Florida, USA
tqle@usf.edu

Nathaniel D. Bastian
United States Military Academy
West Point, New York, USA
nathaniel.bastian@westpoint.edu

ABSTRACT

Network intrusion detection systems (NIDS) play a critical role in identifying potential threats within computer networks. Deep learning methods have taken center stage in developing state-of-the-art NIDS. However, the need for large, consolidated data sets to train these models poses challenges in decentralized environments with data privacy concerns. Additionally, NIDS predominantly rely on flow-level data, which can result in inconsistent feature sets across clients. To address these gaps, we propose a novel two-stage federated learning framework that enhances the accuracy, robustness, and privacy preservation of packet-based NIDS. Our methodology also addresses the issue of non-independent and identically distributed data across clients. The results from our experiments demonstrate the effectiveness of our approach, achieving an average F1 score of 0.97 across clients and adapting to novel attacks within four communication rounds.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**.

KEYWORDS

Federated learning, network intrusion detection system, packet-based NIDS, novel attack detection

ACM Reference Format:
Quoc H. Nguyen, Soumyadeep Hore, Ankit Shah, Trung Le, and Nathaniel D. Bastian. 2024. A Privacy-Preserving Federated Learning Framework for Robust Intrusion Detection in Decentralized Networks Using Packet Data. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (KDD).* ACM, New York, NY, USA, 5 pages. https://doi.org/XXXXXXX.XXXXXXX

*Both authors contributed equally to this research.
†Corresponding author.

KDD, August 25, 2024, Barcelona, Spain

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Network intrusion detection systems (NIDS) play a crucial role in cybersecurity by continuously monitoring network traffic to identify and respond to potential threats [13, 14]. The importance of NIDS has grown significantly with the increasing sophistication of cyber attacks and the expanding attack surface of modern networks. Deep learning (DL) methods, trained on large data sets, have emerged as powerful tools for NIDS [41]. DL-based NIDS can be developed using both supervised [3, 7] and unsupervised [17, 35] learning approaches. Supervised methods, which leverage labeled data, have shown superior performance in detecting known attacks compared to unsupervised techniques. However, consolidating data across distributed networks to train centralized DL models is challenging due to data privacy and security concerns [22, 28]. Overcoming these hurdles is crucial for safeguarding decentralized networks against evolving cyber threats.

Federated learning provides a compelling paradigm for collaboratively training models across clients without centralizing data [11, 26]. This approach is particularly crucial for NIDS due to the sensitivity of network data, regulatory compliance requirements, and the need to protect proprietary infrastructure information. By enabling DL-based NIDS to be trained on decentralized data while preserving privacy, federated learning can significantly enhance intrusion detection capabilities. Several studies have explored federated learning for NIDS [2, 5, 6, 12, 18, 28–30, 38]. NIDS typically utilize either flow-based or packet-based data. Flow-based features aggregate network traffic statistics, providing a high-level view of connections but potentially missing fine-grained details. In contrast, packet-based features are extracted from individual network packets, offering more granular information. Most federated NIDS work focuses on flow-based features [6, 12, 18, 29, 30], which can lead to inconsistent feature sets across clients due to variations in flow collection methods and definitions. Packet-based features, however, enable more granular, consistent data for federated NIDS [38], allowing for precise, timely detection of security incidents and effective content-based matching against known attacks [27]. Despite these advantages, existing packet-based federated NIDS studies [28, 38] have not addressed the challenge of non-independent and identically distributed (non-IID) data across clients, which can significantly degrade model performance [19, 23].

In this paper, we introduce a novel federated learning framework for packet-based NIDS that addresses key challenges in NIDS development:

- Decentralized training: Our approach enables training on decentralized data, preserving privacy and leveraging diverse data sets from multiple network environments.
- Packet-based analysis: We focus on packet-level data for more precise detection of subtle attack patterns, in contrast with flow-level data.
- Non-IID data handling: Our method addresses the challenge of non-IID data across clients, which is common in real-world networks.
- Adaptability to new threats: We propose a two-stage approach with initial training followed by fine-tuning for quick adaptation to novel attack patterns.

To the best of our knowledge, this is the first study to address non-IID data across clients for packet-based federated NIDS. Our experiments demonstrate the superior performance of this framework compared to other state-of-the-art methods under non-IID settings, as well as its faster adaptation to new attack patterns across all clients.

2 RELATED WORK

DNNs have shown great promise in enhancing NIDS accuracy by capturing complex patterns in network traffic [36]. DNNs can learn hierarchical features, detect subtle anomalies [41], adapt to new threats [20], and model non-linear relationships [36]. Both supervised [3, 7] and unsupervised [17, 35] DNN-based NIDS have been developed, with supervised methods demonstrating superior performance on known attacks when labeled data is available.

NIDS can be broadly categorized as flow-based or packet-based, depending on the granularity of the input data [4]. Flow-based systems analyze high-level patterns but may miss certain attack types [4]. Packet-based methods enable precise, timely detection and effective content-based matching [27]. However, most DNN-based NIDS rely on centralized data, which is problematic in decentralized environments with privacy concerns [22, 28].

Federated learning enables collaborative model training across decentralized data sets while preserving privacy [11, 26]. Clients train local models on their private data and share only model updates, not raw data [1, 11]. Federated averaging (FedAvg) [26] is a fundamental algorithm where local models are averaged to obtain a global model. Techniques like secure aggregation and differential privacy further enhance security [1, 11]. However, data heterogeneity across clients (non-IID data) can degrade federated model performance [19, 23]. FedProx [24] addresses this by adding a proximal term to the client objective to limit divergence from the global model. Other approaches include FedNova [37] and SCAFFOLD [21]. Despite its challenges, federated learning has been successfully applied in various domains, including healthcare [40] and IoT [39], highlighting its potential for NIDS [22, 32].

Several studies have explored federated learning for NIDS [2, 5, 6, 12, 18, 29, 30]. However, most focus on flow-based data [6, 12, 18, 29, 30], which can result in inconsistent features across clients [35]. In contrast, raw packet data provides a more uniform, granular basis for federated NIDS [10, 38]. Packet-based federated approaches have been explored by Nguyen et al. [28] and Willeke et al. [38], but they do not address the non-IID data challenge, which significantly impacts performance [19, 23]. Additionally, the resilience of federated NIDS to novel attacks like zero-day and adversarial evasion has not been thoroughly evaluated.

Our work addresses these gaps by proposing a packet-based federated NIDS framework designed to handle non-IID data using FedProx technique, adapt to novel attacks via fine-tuning, and demonstrate resilience against adversarial evasion attempts. By focusing on these key challenges, our methodological framework aims to provide a robust, privacy-preserving solution for decentralized NIDS.

3 METHODOLOGY

In this section, we describe our privacy preserving federated learning framework for packet-based NIDS. This methodological framework consists of two distinct stages, as shown in Figure 1 and described as follows:

Stage 1 - Federated DNN Pre-training: A global DNN model is collaboratively pre-trained across K clients on their local packet data. Each client k has a local data set D_k. In each round t, the clients train the model on their data, and the updates are aggregated to refine the global model. We handle non-IID data by adding a proximal term μ to the client objective, as in FedProx [24], which is given below:

$$\underset{w_k}{\text{minimize}}\ F_k(w_k) = L_k(w_k) + \frac{\mu}{2}\|w_k - w_G^t\|^2 \tag{1}$$

where w_k are the local model weights, w_G^t are the global model weights at round t, L_k is the local loss, and μ controls the proximity to the global model. This limits divergence and improves stability under non-IID data.

Stage 2 - Federated Novel Attack Fine-tuning:

When a client encounters new attack samples, the entire pre-trained global model w_G is fine-tuned using only this novel data. This process is distinct from periodic retraining, which uses the full data set. Fine-tuning is triggered by novel attack detection and involves updating the model on the new samples for a few epochs. The updated model weights are then shared, allowing all clients to rapidly adapt to the emerging threat. This approach enables quick incorporation of new attack signatures without a full retraining cycle, providing faster response to emerging threats while complementing regular periodic retraining for overall model maintenance.

3.1 Experimental Setup

Data Sets: We use packet capture (PCAP) files from the CIC-IDS2017 and CIC-IDS2018 data sets [33, 34]. These contain network traffic collected over several days, including various attack types. We extract packet-level features following the process in [10].

Non-IID Data Split: The data is partitioned into four non-IID clients using a label-based split (Table 1). Each client has a unique combination of attack types, representing different network environments, which are split into training, validation, and testing data sets. To illustrate the non-IID characteristic of these clients, pairwise hypothesis testing is conducted. The Kolmogorov-Smirnov test [9] is employed to evaluate whether two samples share identical underlying distributions, while the Mann-Whitney rank sum

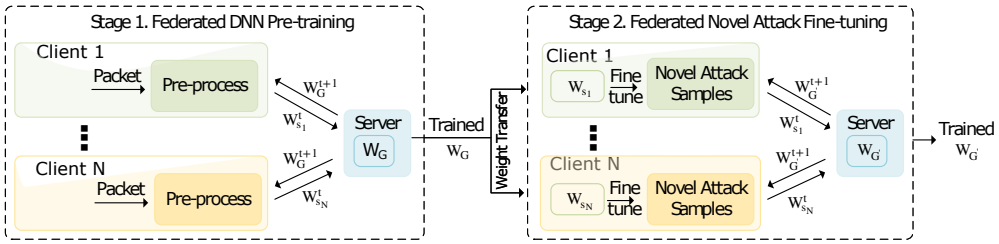

Figure 1: Schematic of the privacy preserving federated learning framework for packet-based NIDS.

Table 1: Non-IID data split across clients.

Silo	Packet Type	Data Set	# of Forward Packets		
			Train	Val	Test
Client 1	Port Scan, DoS, DDoS, and Benign	CIC-IDS2017	133906	15000	33476
Client 2	Brute Force, Infiltration, Web Attack, and Benign	CIC-IDS2017	110585	15000	30146
Client 3	DoS, Brute Force, and Benign	CIC-IDS2018	102947	15000	25736
Client 4	DDoS, Infiltration, Web Attack, and Benign	CIC-IDS2018	102324	15000	25581

test [25] is utilized to discern distribution disparities between independent samples. Our analysis reveals significant distinctions in the data distributions across all clients, thereby affirming the non-IID nature of our crafted partitions.

Hyperparameters: The DNN architecture and training parameters (Table 2) are selected based on literature [8, 29] and empirical tuning. The federated learning process uses five communication rounds with five local epochs per round. Techniques like L2 regularization, dropout, and early stopping are used to prevent overfitting.

Hyperparameter	Value
Regularization (μ)	0.005
Dropout rate	0.3
Architecture	[512, 256, 128, 64]
Activation function	ReLU
Learning rate (η)	0.01
Local epochs (E)	5

Table 2: Hyperparameters for the federated learning model.

Evaluation: We compare our approach against FedAvg [38], FedAdam [31], and a centralized DNN. Models are evaluated on held-out test data for each client. We report precision, recall, and F1 scores for the attack class.

Adaptation to New Attacks: To assess adaptation, we introduce a novel attack type (Botnet), which we held back from CIC-IDS2017 data set during training, to client 1 after pre-training. We evaluate the global model's performance before and after fine-tuning on this data.

Resilience to Adversarial Attacks: We generate adversarial evasion attacks using two toolchains: one that perturbs packets while preserving malicious functionality [16], and another that applies heuristic perturbations [15]. We evaluate our framework against these attacks before and after fine-tuning.

4 RESULTS AND DISCUSSION

In this section, we present the results of the conducted experiments. First, we compare the performance of our framework against other state-of-the-art federated learning approaches. This is followed by a demonstration of the quick adaptation of our two-stage framework to new attack patterns observed by one of the clients. We also show the resilience of our framework against adversarial attacks.

4.1 Attack Detection Performance

Our approach maintains high recall (≥ 0.95) for all clients, including clients 3 and 4 (where attack patterns are more complex and diverse), while FedAvg and FedAdam struggle with these clients (recall ≤ 0.68). This improvement is likely due to our use of the the proximal term in the objective function (see Equation 1), which helps handle non-IID data by limiting divergence between local and global models. In real-world NIDS implementations, higher recall means fewer missed attacks, which is crucial for maintaining network security. The significant recall improvement for clients 3 and 4 ($\geq$ 27 percentage points) suggests our approach could substantially reduce the number of undetected intrusions in diverse network environments, potentially preventing costly security breaches.

Client	FedAvg			FedAdam			Our Approach		
	Prec	Rec	F1	Prec	Rec	F1	Prec	Rec	F1
1	1.00	0.97	0.98	0.99	0.99	0.99	1.00	0.99	0.99
2	1.00	0.96	0.98	0.99	0.99	0.99	1.00	0.99	0.99
3	1.00	0.68	0.80	0.99	0.65	0.78	1.00	0.95	0.96
4	1.00	0.67	0.80	1.00	0.64	0.78	1.00	0.96	0.94

Table 3: Attack detection performance comparison.

4.2 Adaptation to New Attacks

When client 1 encounters Botnet attacks after pre-training, the global model initially performs poorly (high loss). However, after fine-tuning on this new data and sharing the updates, all clients adapt to detect the novel attack within ~4 rounds, as shown in

Figure 2. This fast adaptation is crucial for responding to emerging threats in a timely manner.

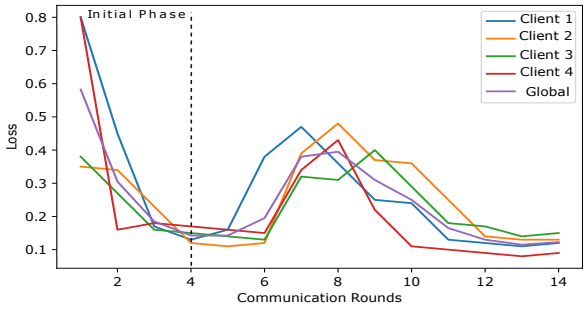

Figure 2: Adaptation to novel attack patterns.

4.3 Resilience to Adversarial Attacks

Finally, we test our trained global model against adversarial evasion attacks before and after fine-tuning. Before fine-tuning, the model struggles to detect these attacks, with an F1 score of 0.17. However, after fine-tuning on a subset of the adversarial samples, the model's resilience improves significantly, with the F1 score reaching 0.92. (see Figure 3). This experiment further demonstrates the importance of updating the model on new attack variants to maintain robustness.

5 CONCLUSION AND FUTURE WORK

This study proposes a novel federated learning framework for packet-based NIDS that addresses key challenges in decentralized environments. Our approach handles non-IID data across clients, achieves accurate attack detection, quickly adapts to novel attacks, and shows strong resilience against adversarial evasion attempts. By enabling collaborative learning while preserving data privacy, this framework enhances NIDS in distributed networks.

Our work assumes reliable client-server communication and the ability of clients to detect and share novel attack samples. Future research could explore automated novelty detection, integration of flow-based features, strategies for handling class imbalance, extension to resource-constrained edge devices, and additional privacy-preserving techniques like differential privacy and secure aggregation.

This study represents an important step towards effective, privacy-preserving, and adaptable NIDS in decentralized environments using packet-level data. As cyber threats evolve, such collaborative learning approaches will play a crucial role in safeguarding distributed networks.

ACKNOWLEDGMENTS

This work was supported in part by the U.S. Military Academy (USMA) under Cooperative Agreement No. W911NF-22-2-0045. The views and conclusions expressed in this paper are those of the authors and do not reflect the official policy or position of USMA, U.S. Army, U.S. Department of Defense, or U.S. Government.

REFERENCES

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 308–318.

[2] Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Mamoun Alazab, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, and Thippa Reddy Gadekallu. 2022. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications* 195 (2022), 346–361.

[3] Muhammad Ahmad, Qaiser Riaz, Muhammad Zeeshan, Hasan Tahir, Syed Ali Haider, and Muhammad Safeer Khan. 2021. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. *EURASIP Journal on Wireless Communications and Networking* 2021, 1 (2021), 1–23.

[4] Mohiuddin Ahmed, Abdun Naser Mahmood, and Jiankun Hu. 2016. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications* 60 (2016), 19–31.

[5] Ammar Alazab, Ansam Khraisat, Sarabjot Singh, and Tony Jan. 2023. Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. *Electronics* 12, 16 (2023), 3382.

[6] Ons Aouedi, Kandaraj Piamrat, Guillaume Muller, and Kamal Singh. 2022. FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 523–524.

[7] Manjula C Belavagi and Balachandra Muniyal. 2016. Performance evaluation of supervised machine learning algorithms for intrusion detection. *Procedia Computer Science* 89 (2016), 117–123.

[8] Aitor Belenguer, Jose A Pascual, and Javier Navaridas. 2023. GöwFed: A novel federated network intrusion detection system. *Journal of Network and Computer Applications* (2023), 103653.

[9] Vance W Berger and YanYan Zhou. 2014. Kolmogorov–smirnov test: Overview. *Wiley statsref: Statistics reference online* (2014).

[10] David A Bierbrauer, Michael J De Lucia, Krishna Reddy, Paul Maxwell, and Nathaniel D Bastian. 2023. Transfer learning for raw network traffic detection. *Expert Systems with Applications* 211 (2023), 118641.

[11] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2017. Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 1175–1191.

[12] Jie Cui, Hu Sun, Hong Zhong, Jing Zhang, Lu Wei, Irina Bolodurina, and Debiao He. 2023. Collaborative Intrusion Detection System for SDVN: A Fairness Federated Deep Learning Approach. *IEEE Transactions on Parallel and Distributed Systems* (2023).

[13] Felix Erlacher and Falko Dressler. 2018. FIXIDS: A high-speed signature-based flow intrusion detection system. In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 1–8.

[14] Pedro Garcia-Teodoro, Jesus Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security* 28, 1-2 (2009), 18–28.

[15] Jalal Ghadermazi, Ankit Shah, and Nathaniel Bastian. 2023. Towards Real-time Network Intrusion Detection with Image-based Sequential Packets Representation. *TechRxiv preprint* (2023). https://doi.org/10.36227/techrxiv.23291588.v1

[16] Soumyadeep Hore, Jalal Ghadermazi, Diwas Paudel, Ankit Shah, Tapas K. Das, and Nathaniel D. Bastian. 2023. Deep PackGen: A Deep Reinforcement Learning Framework for Adversarial Network Packet Generation. arXiv:2305.11039 [cs.CR]

[17] Soumyadeep Hore, Quoc Nguyen, Yulun Xu, Ankit Shah, Nathaniel Bastian, and Trung Le. 2023. Empirical Evaluation of Autoencoder Models for Anomaly Detection in Packet-based NIDS. In *Proceedings of the 2023 6th IEEE Conference on Dependable and Secure Computing*. IEEE.

[18] Meryem Janati Idrissi, Hamza Alami, Abdelkader El Mahdaouy, Abdellah El Mekki, Soufiane Oualil, Zakaria Yartaoui, and Ismail Berrada. 2023. Fed-ANIDS: Federated learning for anomaly-based network intrusion detection systems. *Expert Systems with Applications* 234 (2023), 121000.

[19] Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. 2021. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning* 14, 1–2 (2021), 1–210.

[20] Min-Joo Kang and Je-Won Kang. 2016. Intrusion detection system using deep neural network for in-vehicle network security. *PloS one* 11, 6 (2016), e0155781.

[21] Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. 2020. Scaffold: Stochastic controlled averaging for federated learning. In *International conference on machine learning*. PMLR, 5132–5143.

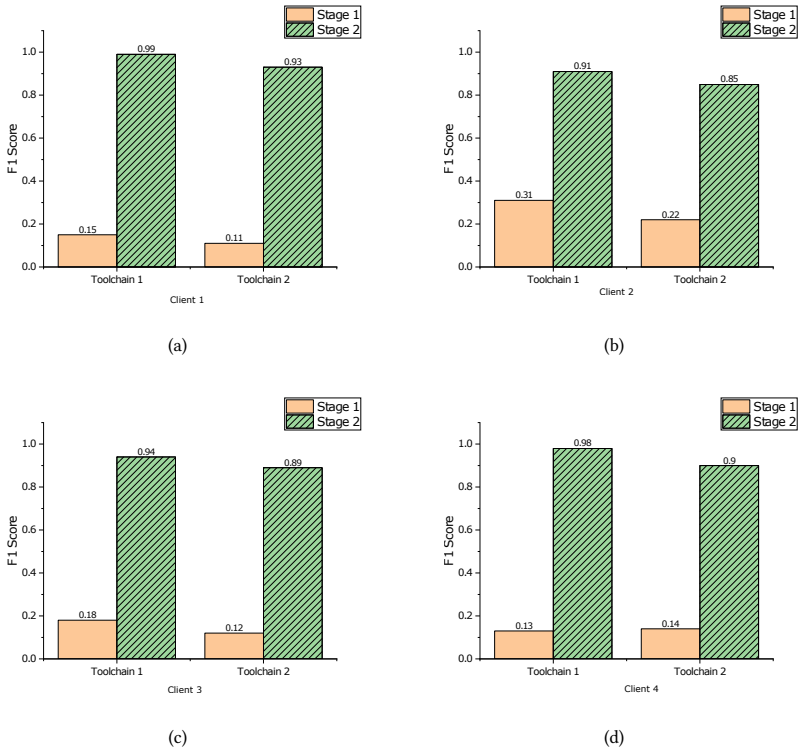

Figure 3: Before and after fine-tuning the model showing adaptation to novel botnet attacks.

[22] Beibei Li, Yuhao Wu, Jiarui Song, Rongxing Lu, Tao Li, and Liang Zhao. 2020. DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. *IEEE Transactions on Industrial Informatics* 17, 8 (2020), 5615–5624.

[23] Qinbin Li, Zeyi Wen, Zhaomin Wu, Sixu Hu, Naibo Wang, Yuan Li, Xu Liu, and Bingsheng He. 2021. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering* (2021).

[24] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. 2020. Federated optimization in heterogeneous networks. *Proceedings of Machine learning and systems* 2 (2020), 429–450.

[25] Patrick E McKnight and Julius Najab. 2010. Mann-Whitney U Test. *The Corsini encyclopedia of psychology* (2010), 1–1.

[26] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. 2017. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*. PMLR, 1273–1282.

[27] Srinivas Mukkamala, Guadalupe Janoski, and Andrew Sung. 2002. Intrusion detection using neural networks and support vector machines. In *Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290)*, Vol. 2. IEEE, 1702–1707.

[28] Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Hossein Fereidooni, N Asokan, and Ahmad-Reza Sadeghi. 2019. DÏoT: A federated self-learning anomaly detection system for IoT. In *2019 IEEE 39th International conference on distributed computing systems (ICDCS)*. IEEE, 756–767.

[29] Sawsan Abdul Rahman, Hanine Tout, Chamseddine Talhi, and Azzam Mourad. 2020. Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE Network* 34, 6 (2020), 310–317.

[30] Md Mamunur Rashid, Shahriar Usman Khan, Fariha Eusufzai, Md Azharuddin Redwan, Saifur Rahman Sabuj, and Mahmoud Elsharief. 2023. A federated learning-based approach for improving intrusion detection in industrial internet of things networks. *Network* 3, 1 (2023), 158–179.

[31] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečnỳ, Sanjiv Kumar, and H Brendan McMahan. 2020. Adaptive federated optimization. *arXiv preprint arXiv:2003.00295* (2020).

[32] Pedro Ruzafa-Alcázar, Pablo Fernández-Saura, Enrique Mármol-Campos, Aurora González-Vidal, José L Hernández-Ramos, Jorge Bernal-Bernabe, and Antonio F Skarmeta. 2021. Intrusion detection based on privacy-preserving federated learning for the industrial IoT. *IEEE Transactions on Industrial Informatics* 19, 2 (2021), 1145–1154.

[33] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. 2019. A detailed analysis of the cicids2017 data set. In *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4*. Springer, 172–188.

[34] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp* 1 (2018), 108–116.

[35] Miel Verkerken, Laurens D'hooge, Tim Wauters, Bruno Volckaert, and Filip De Turck. 2022. Towards model generalization for intrusion detection: Unsupervised machine learning techniques. *Journal of Network and Systems Management* 30 (2022), 1–25.

[36] Bo Wang, Yang Su, Mingshu Zhang, and Junke Nie. 2020. A deep hierarchical network for packet-level malicious traffic detection. *IEEE Access* 8 (2020), 201728–201740.

[37] Jianyu Wang, Qinghua Liu, Hao Liang, Gauri Joshi, and H Vincent Poor. 2020. Tackling the objective inconsistency problem in heterogeneous federated optimization. *Advances in neural information processing systems* 33 (2020), 7611–7623.

[38] Mikal R Willeke, David A Bierbrauer, and Nathaniel D Bastian. 2023. Data-efficient, federated learning for raw network traffic detection. In *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V*, Vol. 12538. SPIE, 247–262.

[39] Kai Yang, Yuanming Shi, Yong Zhou, Zhanpeng Yang, Liqun Fu, and Wei Chen. 2020. Federated machine learning for intelligent IoT via reconfigurable intelligent surface. *IEEE network* 34, 5 (2020), 16–22.

[40] Binhang Yuan, Song Ge, and Wenhui Xing. 2020. A federated learning framework for healthcare iot devices. *arXiv preprint arXiv:2005.05083* (2020).

[41] Si-si Zhang, Jian-wei Liu, and Xin Zuo. 2021. Adaptive online incremental learning for evolving data streams. *Applied Soft Computing* 105 (2021), 107255.