IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 February 2024, accepted 29 February 2024, date of publication 18 March 2024, date of current version 25 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3378727

RESEARCH ARTICLE

Federated Learning for Decentralized DDoS Attack Detection in IoT Networks

YASER ALHASAWI AND SALEM ALGHAMDI
King Abdulaziz University (KAU), Jeddah 21589, Saudi Arabia
Institute of Public Administration, Saudi Arabia

Corresponding author: Yaser Alhasawi (yalhasawi@kau.edu.sa)

ABSTRACT In the ever-expanding domain of Internet of Things (IoT) networks, Distributed Denial of Service (DDoS) attacks represent a significant challenge, compromising the reliability of these systems. Traditional centralized detection methods struggle to cope effectively in the widespread and diverse environment of IoT, leading to the exploration of decentralized approaches. This study introduces a Federated Learning-based approach, named Federated Learning for Decentralized DDoS Attack Detection (FL-DAD), which utilizes Convolutional Neural Networks (CNN) to efficiently identify DDoS attacks at the source. Our approach prioritizes data privacy by processing data locally, thereby avoiding the need for central data collection, while enhancing detection efficiency. Evaluated using the comprehensive CICIDS2017 dataset and compared with conventional centralized detection methods, FL-DAD achieves superior performance, illustrating the potential of federated learning to enhance intrusion detection systems in large-scale IoT networks by balancing data security with analytical effectiveness.

INDEX TERMS Federated learning, DDoS attack detection, IoT networks, convolutional neural networks, decentralized intrusion detection.

I. INTRODUCTION

The Internet of Things (IoT) epitomizes the transformation of the digital landscape, moving beyond traditional devices like computers and smartphones to create an interconnected web of everyday objects [1]. These objects, embedded with sensors, software, and other technologies, seamlessly communicate and exchange data with other devices and systems over the Internet. IoT has emerged as a cornerstone of the 21st-century digital revolution. From smart thermostats and wearable health monitors to intelligent traffic systems and advanced manufacturing tools, the integration of IoT has seen an upsurge across various sectors [2]. According to Gartner, by 2025, the number of connected things worldwide is expected to surpass 30 billion [3]. This burgeoning network promises unparalleled opportunities for personal, industrial, and societal applications. Enhanced data collection, real-time communication, and a vastly improved user experience are just some of the many advantages IoT brings.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Fu Cheng.

However, the proliferation of IoT devices also introduces an array of vulnerabilities. The very attributes that make IoT devices versatile, their connectivity, ease of access, and ubiquity, also render them susceptible to threats. Of these threats, Distributed Denial of Service (DDoS) attacks are particularly ominous [4]. These attacks involve overwhelming a targeted system, such as a website or an IoT device, with a flood of Internet traffic, rendering it inoperative. Given the decentralized nature of IoT networks, a successful DDoS attack can have catastrophic ramifications, disrupting service delivery, compromising user experience, and potentially causing significant economic losses [5], [6]. The inherent characteristics of IoT devices further exacerbate their vulnerability. These devices, often manufactured with cost-effectiveness in mind, may lack sophisticated security features [7]. Moreover, their widespread deployment across various environments, each with its unique security posture, makes establishing a unified protective framework challenging.

Traditional security measures, especially centralized intrusion detection systems, are ill-equipped to handle the intricacies of IoT. These centralized systems often suffer

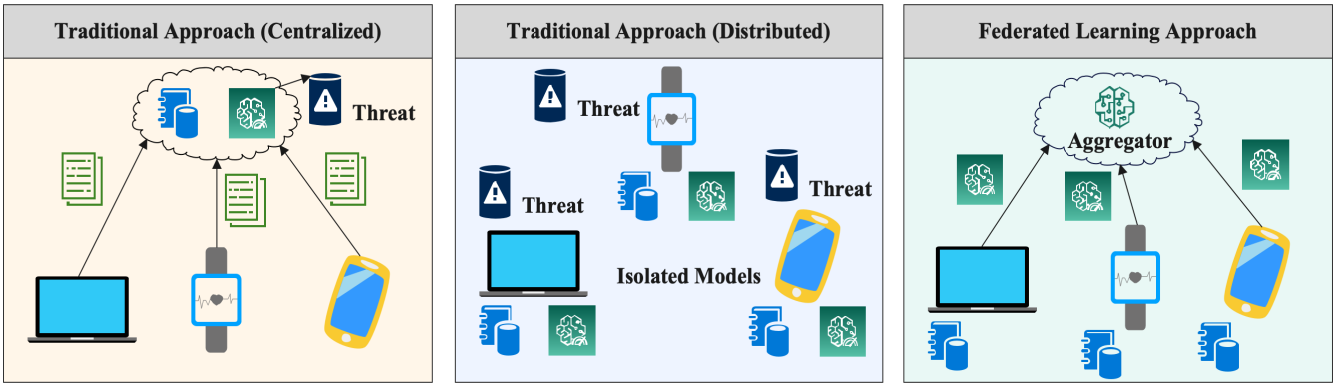

FIGURE 1. Comparison between threats in traditional and federated learning approaches.

from scalability issues, struggling to monitor the massive data flows generated by the plethora of IoT devices. Moreover, centralized systems also introduce a single point of failure, making them attractive targets for adversaries [8]. Furthermore, the transmission of data to a central location for analysis compromises user privacy, as sensitive information may be exposed during transit or storage. To address these shortcomings, there's a growing interest in decentralized learning methodologies, specifically Federated Learning [9]. In federated frameworks, devices, or nodes, are trained locally on their data. Only the model updates, not the raw data, are shared with a central server for aggregation. This approach has the dual advantage of mitigating data privacy concerns and reducing the data transmission overhead. Given the decentralized nature of IoT networks, federated learning seems to be an ideal fit [10], [11]. By processing data locally on IoT devices, federated learning can offer real-time insights, vital for timely detection and mitigation of threats like DDoS attacks [12].

To this end, in this study, we introduce the Federated Learning for Decentralized DDoS Attack Detection (FL-DAD) approach in IoT Networks. In the proposed approach, we utilize Convolutional Neural Networks (CNNs), leveraging their adeptness in feature extraction and pattern recognition. This makes them particularly effective for identifying complex patterns in network traffic, which is crucial for detecting DDoS attacks in IoT environments. By training the model at the edge, close to where the data originates, our approach aims to adeptly detect DDoS attacks while upholding the principles of data privacy and operational efficiency. Using the CICIDS2017 dataset, a comprehensive benchmark for intrusion detection, we present the performance of the FL-DAD approach against traditional centralized methods, showcasing the merits of our decentralized approach. The major contributions of the paper are as follows:

- We propose a novel federated learning-based approach tailored for decentralized DDoS attack detection within IoT networks, harnessing the power of CNN.
- We present a rigorous evaluation of the FL-DAD method using the CICIDS2017 dataset, providing a comparative analysis with traditional centralized detection methods, thus demonstrating its effectiveness and efficiency.

The rest of the paper is as follows: Section II surveys traditional DDoS detection and federated learning's evolution. Section III defines the DDoS challenge in IoT and our objectives. Section IV delves into federated learning principles. Section V outlines our proposed DDoS detection methodology. Experimental design and benchmarks are discussed in Section VI, followed by results in Section VII. Section VIII assesses system robustness and scalability. Section IX highlights challenges and future research avenues, and Section X concludes our study.

II. BACKGROUND AND LITERATURE REVIEW

In the contemporary digital era, IoT networks have emerged as a cornerstone, fostering innovation across numerous sectors. As these networks expand, so do the complexities of safeguarding them. A vital challenge to address is the proliferation of DDoS attacks, which threaten the very foundation of IoT networks. The quest for advanced and adaptive DDoS detection methodologies forms the crux of this section, beginning with an exploration of traditional techniques and culminating in the potential of federated learning in revolutionizing detection. A threat in the traditional centralized approach and distributed approach compared to the federated learning approach is depicted in Figure 1.

A. TRADITIONAL DDOS ATTACK DETECTION METHODS

Distributed Denial of Service (DDoS) attacks, characterized by overwhelming targeted systems using traffic from multiple sources, have persisted as one of the gravest threats in cyberspace. Over the years, several methodologies have been formulated to counter these threats [13].

1) Signature-based Detection: One of the earliest and most straightforward approaches, signature-based detection, operates on the principle of maintaining a database of previously identified attack patterns or 'signatures'. As traffic flows into a system, it's continuously scanned

against these signatures. If a match is detected, the system flags it as a potential attack. While this approach offers quick detection of known threats, it's inherently reactive. Its efficacy diminishes against novel attack strategies that aren't part of the existing database [14].

2) Anomaly-based Detection: Moving a step ahead from the signature-based method, anomaly-based detection doesn't rely on prior knowledge of attacks. Instead, it establishes a baseline representing 'normal' network behavior. Continuous monitoring of network traffic ensues, and any deviation from this baseline is deemed suspicious. While this method offers adaptability, it's not without drawbacks [15]. The dynamic nature of network behavior can sometimes lead to genuine traffic being misclassified as an attack, leading to higher false positives.
3) Rate-based Detection: Recognizing that many DDoS attacks flood systems with an exceptionally high volume of requests, rate-based detection was conceptualized [16]. By setting a predefined threshold for incoming traffic, this method quickly identifies when the inflow rate exceeds this limit. While adept at detecting volumetric attacks, subtler, low-volume threats might bypass its radar.

In Table 1, we provide a comprehensive summary of the primary focus and techniques from existing literature pertinent to our research focus.

B. EVOLUTION AND PRINCIPLES OF FEDERATED LEARNING

In the arena of machine learning, a novel approach began to gain traction that proposed a significant departure from conventional centralized models of federated learning.

- Historical Context: The inception of federated learning was influenced heavily by the growing concerns around data privacy and the inefficiencies of transporting large datasets to centralized servers [28]. It posited an alternative: instead of bringing data to the model, why not bring the model to the data?
- Operational Dynamics: In federated learning, local devices (or 'nodes') are equipped with the capability to train machine learning models on their data. These local models are then aggregated into a global model, which encapsulates insights from all participating nodes without ever accessing their raw data [29]. This ensures data privacy and minimizes the need for data transportation, thereby conserving bandwidth [30].
- Advantages Over Centralized Models: Apart from the evident benefits in data privacy and bandwidth efficiency, federated learning offers robustness against network failures [31], [32]. In a centralized setup, if the central server fails, the entire system collapses. In contrast, federated learning, with its distributed nature, is resilient against such singular points of failure.

C. IOT SECURITY AND MACHINE LEARNING CONVERGENCE

The integration of IoT and machine learning is not novel, but the perspective from which this amalgamation is approached has seen shifts.

- Earlier Paradigms: Historical endeavors primarily utilized centralized machine learning models. Though they were successful to some extent in enhancing IoT security, they raised concerns. Centralized models demanded data from numerous IoT devices be sent to a central location for processing [33]. This not only posed data privacy issues but also scalability concerns, given the vastness of IoT networks [34].
- Inclination Towards Decentralization: With billions of devices contributing to the IoT ecosystem, the sheer volume of data they generate is staggering. Processing this centrally became increasingly untenable [35]. This necessitated a shift towards decentralized methodologies, thus leading researchers to explore federated learning's potential in fortifying IoT security.

It's imperative to consider the convergence of IoT and machine learning not as an endpoint but as a journey. As threats evolve, so must defenses, ensuring that IoT networks remain secure and resilient amidst the ever-changing landscape of cybersecurity challenges.

III. PROBLEM DEFINITION

A. DDOS ATTACKS IN IOT NETWORKS

DDoS attacks have evolved to target the vulnerable IoT landscape, leveraging the multitude of interconnected devices. Each of these devices, often limited in computational capabilities, becomes an easy target, enabling attackers to create massive botnets [36]. These botnets overwhelm target networks, rendering them inoperable. The diverse range of devices, manufacturers, and firmware versions in IoT exacerbates the challenge, as it creates a mosaic of vulnerabilities [37].

B. STATEMENT OF THE PROBLEM

Traditional defenses against DDoS attacks fall short when confronting the complexities of IoT networks. Centralized attack detection mechanisms face scalability issues in vast IoT ecosystems and risk introducing a single point of failure [38]. The urgent challenge lies in devising a decentralized, adaptable, and efficient solution tailored for IoT's unique challenges.

C. OBJECTIVES AND CONTRIBUTIONS

This study aims to harness federated learning for a decentralized DDoS detection mechanism in IoT networks. The goals are:

- Empower individual IoT devices or clusters for independent threat detection.

TABLE 1. Summary of the Literature Review.

Study	Focus	Technique	Findings	Relevance
[17]	IoT DDoS	ML	New vectors	Detection basis
[18]	Edge mitigation	DL	Edge success	Federated insight
[19]	IoT security	Simulation	Security gaps	Security need
[20]	DDoS evolution	Survey	IoT shift	IoT solution need
[21]	IoT vulnerabilities	Analysis	Protocol flaws	Enhanced security
[22]	DDoS patterns	ML	Attack types	Detection strategy
[23]	ML in IoT	Deep Learning	Effective models	Model choice
[24]	Attack mitigation	Hybrid ML	Reduced attacks	Mitigation strategies
[25]	IoT data patterns	Analysis	Traffic insights	Data handling
[26]	IoT DDoS	Simulation	Attack sources	Source tracking
[27]	Defense strategies	DL	Successful defense	Defense approach

- Achieve near real-time threat response.
- Ensure the solution's applicability across diverse IoT scales.
- Enable the system to evolve with changing threat dynamics.

The key contributions include a new federated learning-based approach for DDoS detection in IoT, rigorous validation against contemporary solutions, and insights for future research.

IV. FEDERATED LEARNING: CONCEPTS AND PRINCIPLES

A. WORKINGS OF FEDERATED LEARNING

Federated Learning (FL) is a collaborative machine learning technique where multiple devices (or nodes) train on local data, and only model updates are communicated centrally, rather than raw data [39]. This offers a paradigm shift from traditional centralized learning.

The formal process can be described as follows:

Let N be the number of nodes participating in FL, each node i having a dataset D_i with n_i samples. Each node computes an update from its local dataset:

$$\Delta w_i = \text{Train}(D_i, w) \tag{1}$$

where w represents the global model parameters and Δw_i represents the update from node i.

The global model is then updated by aggregating local updates:

$$w_{\text{new}} = w + \eta \sum_{i=1}^{N} \frac{n_i}{n} \Delta w_i \tag{2}$$

where η is a learning rate and $n = \sum_{i=1}^{N} n_i$ is the total number of samples across nodes. The whole process of federated learning is depicted in Figure 2.

B. ADVANTAGES OVER CENTRALIZED MODELS

In the context of IoT, FL brings several advantages [40]:

- **Data Privacy**: Raw data remains on the local device, reducing exposure risks.
- **Bandwidth Efficiency**: Transmitting only model updates rather than vast amounts of raw data optimizes bandwidth usage.

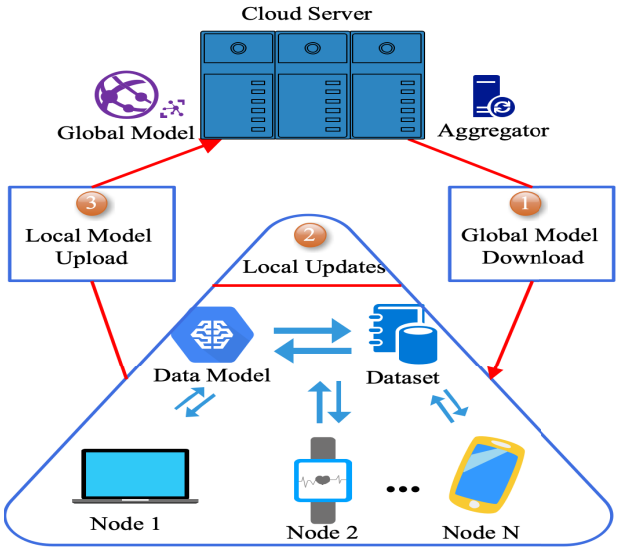

FIGURE 2. The federated learning process in IoT networks.

- **Real-time Adaptation**: Local updates allow for real-time model improvement.

Moreover, the global model is refined with diverse data, enhancing its generalization capabilities:

$$\text{Generalization error} \leq \text{Average local error} + \text{Divergence term} \tag{3}$$

C. CHALLENGES IN IMPLEMENTING FEDERATED LEARNING

Despite its benefits, implementing FL, especially in the complex IoT landscape, is not devoid of challenges [41]:

- **Heterogeneity**: Devices might have non-IID (Independent and Identically Distributed) data, leading to a skewed learning process. This skewness can be quantified as:

$$\text{Skewness} = \frac{\sum_{i=1}^{N} (\mu_i - \mu)^2}{N} \tag{4}$$

where μ_i is the local mean and μ is the global mean.

- **Communication Overheads**: Frequent model updates can strain limited IoT communication capabilities.
- **Security Concerns**: External threats might try to compromise the model's integrity through malicious updates.

V. PROPOSAL OF FL-DAD

A. DESIGN OF THE FEDERATED LEARNING-BASED DDOS DETECTION SYSTEM

Our overarching design incorporates a federated learning architecture that allows multiple IoT nodes to train localized models without centralizing data. This not only ensures data privacy but also leverages local data peculiarities to enhance detection performance.

$$L(w) = \sum_{i=1}^{n} F_i(w) = \sum_{i=1}^{n} \frac{1}{n_i} \sum_{j=1}^{n_i} f_i(w; x_{ij}, y_{ij}) \tag{5}$$

where $L(w)$ is the global loss, $F_i(w)$ is the local loss at node i, and $f_i(w; x_{ij}, y_{ij})$ is the training example at node i.

B. DATA COLLECTION, PREPROCESSING, AND DISTRIBUTION

Data plays a pivotal role in training robust models. In a federated environment, data remains local to each node. For our IoT-based DDoS detection:

- Data Collection: Data generated from network traffic at each IoT node is collected locally.
- Preprocessing: Data is normalized, outliers are identified and removed, and relevant features are selected to feed into the model.
- Distribution: While data remains at each node, the model updates will be communicated across the network.

C. MODEL ARCHITECTURE AND TRAINING STRATEGIES

We propose using a CNN model due to its proficiency in identifying patterns, which is essential for DDoS detection.

$$z^{[l]} = W^{[l]} a^{[l-1]} + b^{[l]} \tag{6}$$

$$a^{[l]} = g^{[l]}(z^{[l]}) \tag{7}$$

where $a^{[l]}$ is the activation at layer l, $W^{[l]}$ and $b^{[l]}$ are the weights and biases, and $g^{[l]}$ is the activation function.
The training process in the federated environment is given in Algorithm 1:

D. MODEL AGGREGATION MECHANISMS

Post-training, model aggregation is vital to consolidate knowledge from all nodes. We use weighted averaging based on the number of samples at each node.

$$w_{global} = \frac{\sum_{i=1}^{n} n_i w_i}{\sum_{i=1}^{n} n_i} \tag{8}$$

where n_i is the number of samples at node i and w_i is the local model weight.

Algorithm 1 Federated Learning Training Procedure

Require: Initial global model weights w_0
Ensure: Updated global model weights w
Input: Initial global model weights w_0
Output: Updated global model weights w
Initialize global model weights $w \leftarrow w_0$
for each training round $t = 1, 2, \ldots, T$ **do**
  for each node i in parallel **do**
    Compute model update Δw_i using local data D_i
  end for
  Aggregate updates: $w \leftarrow w + \eta \sum_i \Delta w_i$
end for

E. COMMUNICATION PROTOCOLS FOR MODEL UPDATES

Ensuring efficient and fault-tolerant communication is paramount. Model updates are packaged and transmitted to a central server which then broadcasts the global model to all nodes [42]. During this, nodes utilize a protocol ensuring that if updates aren't received within a specified window, they'll request them again.

Algorithm 2 Model Update Communication Protocol

Require: Local model updates Δw_i from each node i
Ensure: Successful transmission of updates to central server
Input: Model updates Δw_i for each node i
Output: Acknowledgement of successful update transmission
for each node n **do**
  Transmit model updates Δw_n to the central server
  if Acknowledgement not received within timeout **then**
    Re-transmit model updates Δw_n
  end if
end for

F. EXECUTION OF FL-DAD

The intricate FL-DAD execution process is meticulously designed to integrate seamlessly with existing IoT infrastructures, thus bolstering their resilience against DDoS assaults whilst ensuring the sanctity of data privacy. The sequential stages of this methodical approach encompass:

1) **Initialization**: Let M_{global} be the global model. We initialize:

$$M_{global}^{(0)} \leftarrow \text{InitModel}() \tag{9}$$

where InitModel() represents the initialization function.

2) **Local Model Training**: For each node i, using its local dataset D_i, the node updates its local model M_i. The model is trained by optimizing a loss function $\mathcal{L}$:

$$M_i^{(t)} \leftarrow \text{Train}(M_i^{(t-1)}, D_i) \tag{10}$$

where t is the current iteration. This step enables each node to independently detect potential DDoS

threats based on its local data, prior to participating in the global model aggregation. **However, during this phase, privacy risks emerge from the potential for sensitive information inference from model updates, necessitating the implementation of techniques such as differential privacy or homomorphic encryption to safeguard data.**

3) **Model Update Communication**: The model update from node i can be computed as:

$$\Delta M_i^{(t)} = M_i^{(t)} - M_i^{(t-1)} \tag{11}$$

Nodes transmit $\Delta M_i^{(t)}$ to the centralized server. **The pseudocode of the model update communication process is mentioned in Algorithm 2.**

4) **Global Model Aggregation**: Aggregation at the central server is performed using the weighted sum of local model updates:

$$M_{global}^{(t)} \leftarrow M_{global}^{(t-1)} + \sum_i w_i \Delta M_i^{(t)} \tag{12}$$

where w_i is the weight assigned to node i, reflecting its reliability or the size of its local dataset. **During aggregation, privacy risks are accentuated as aggregated data might inadvertently reveal information about individual nodes' data. To mitigate this, secure multi-party computation (SMPC) or federated averaging with secure aggregation protocols can be employed to ensure that the aggregated model does not expose any node's data.**

5) **Global Model Broadcast**: Post-aggregation, $M_{global}^{(t)}$ is broadcasted to all nodes:

$$M_i^{(t)} \leftarrow M_{global}^{(t)} \tag{13}$$

for all nodes i.

6) **Evaluation**: Every node i evaluates $M_{global}^{(t)}$ against potential DDoS patterns using the evaluation metric $\mathcal{E}$:

$$\text{Score}_i = \mathcal{E}(M_{global}^{(t)}, D_{i_{\text{test}}}) \tag{14}$$

where $D_{i_{\text{test}}}$ is the testing dataset at node i.

7) **Iteration**: Based on the evaluations, the process is iteratively continued:

$$t \leftarrow t + 1 \tag{15}$$

until a stopping criterion, such as a predetermined number of rounds or a desired accuracy level, is reached.

The Algorithm 3 elegantly encapsulates the FL-DAD execution process. By meticulously adhering to its procedures, IoT networks can not only fortify their defenses against DDoS threats but also ensure an unwavering commitment to data privacy.

Algorithm 3 Execution Procedure of FL-DAD

Require: Local data D_i for each node i, Initialization function InitModel()
Ensure: Global model M_{global} trained on distributed data

Input: Local datasets D_i for each node i
Output: Trained global model M_{global}
Initialize global model: $M_{global}^{(0)} \leftarrow$ InitModel()
for each training round $t = 1, 2, \ldots, T$ **do**
  for each node i in parallel **do**
    Independently train local model $M_i^{(t)}$ on D_i
    Perform local threat detection
    Compute and send updates $\Delta M_i^{(t)}$ to central server
  end for
  Central server aggregates updates to update $M_{global}^{(t)}$
  Broadcast $M_{global}^{(t)}$ to all nodes
  for each node i **do**
    Evaluate detection efficacy of $M_{global}^{(t)}$ on test data $D_{i_{\text{test}}}$
  end for
end for

VI. IMPLEMENTATION AND EXPERIMENTATION

A. EXPERIMENTAL SETUP

1) ENVIRONMENT AND TOOLS

Our experimental apparatus is firmly grounded in the TensorFlow Federated (TFF) framework, a state-of-the-art library tailored for federated learning endeavors. Complementary to TFF, TensorFlow, and Keras simplify model design, training, and evaluative tasks [43].

2) DATASET: CICIDS2017

The CICIDS2017 dataset, crafted by the Canadian Institute for Cybersecurity, stands as the foundation for our experimentation [44]. Recognized as an industry benchmark for intrusion detection evaluations, the dataset offers a granular view into network traffic patterns by capturing an entire week's worth of activity. Some defining attributes of the dataset include:

- A comprehensive collection of over 2.8 million entries, with each entry signifying a distinct network flow.
- A set of 79 features, furnishing an exhaustive portrayal of flow statistics and header data.
- While the dataset covers a broad spectrum of attacks, for the purpose of our study, we primarily focus on classes relevant to DDoS attacks. These classes within CICIDS2017 include:
  - **BENIGN**: This class embodies regular, non-malicious network traffic, serving as a point of contrast against malicious flows.
  - **DDoS**: A quintessential representation of Distributed Denial of Service attacks. These attacks orchestrate a barrage of traffic from multiple sources, aiming to overwhelm and incapacitate targeted systems.
  - **DoS Hulk**: A Denial of Service attack variant that exploits discrepancies in web servers, swamping them with a deluge of GET requests.

- **DoS GoldenEye**: Another DoS strain, which inundates target systems with a mix of GET and POST requests, exhausting their resources.
- **DoS slowloris & Slowhttptest**: These are stealthy attacks that hold onto server connections for prolonged periods, ultimately leading to service denial without consuming extensive bandwidth.
- **Heartbleed**: While not a DDoS attack in the traditional sense, this OpenSSL vulnerability can be exploited to retrieve sensitive data, and its exploitation can mirror DDoS attack patterns.

3) DATA PREPROCESSING

In order to refine the dataset for optimal performance, we executed the following preprocessing steps:

1) Rectified any missing or inconsistent values.
2) Employed the Min-Max scaler to normalize numerical attributes.
3) One-hot encoded categorical attributes, thereby converting them into a binary matrix representation.
4) Reorganized the dataset to mimic a federated structure, representing multiple nodes.

B. TRAINING PROCESS

1) TENSORFLOW FEDERATED SETUP

TFF was fine-tuned to employ a simulation-centric runtime. This configuration empowers us to conduct federated computations locally, simulating real-world distributed learning without necessitating actual distributed infrastructure.

2) FL ALGORITHM AND TRAINING STRATEGY

The core of our FL approach is built upon the Federated Averaging (FedAvg) algorithm. This algorithm allows local models to be trained independently on nodes (devices) with their own data samples and computes the global model by averaging the updates. This process iteratively improves the global model while preserving data privacy and reducing communication overhead.

3) MODEL ARCHITECTURE

With the CICIDS2017 dataset offering a rich and intricate feature set, a robust deep learning approach was deemed essential. Given the non-sequential nature of the features (i.e., the characteristics of network packets do not necessarily have temporal dependencies as in a time series), a Convolutional Neural Network (CNN) was chosen. CNNs, generally praised for their performance in image processing, have shown significant promise in processing structured data by automatically and adaptively learning spatial hierarchies of features. A complete architecture of CNN is given in Table 2.

4) FEDERATED INTEGRATION AND TRAINING

Our federated training process involves several key steps. Initially, the global model is sent to each node. Each node then trains the model on its local data and calculates the model updates. These updates are sent back to the server, where they are aggregated to update the global model. This cycle is repeated for multiple rounds until the model converges or meets predefined performance criteria.

5) COMMUNICATION PROTOCOLS

Communication between the nodes and the central server is managed using TFF's secure aggregation protocols. These protocols are designed to ensure that the aggregated data cannot be used to infer information about individual updates, thereby maintaining data privacy. Additionally, to optimize network resources and reduce latency, we employ strategies like model compression and update pruning, which minimize the size of the data that needs to be transmitted.

6) FEDERATED INTEGRATION AND TRAINING

After finalizing the CNN architecture, it was integrated into the federated framework using TFF's `tff.learning.from_keras_model` method. The subsequent decentralized training leveraged `tff.learning.build_federated_averaging_process`, allowing the model to be trained across our distributed, simulated nodes.

C. EVALUATION

1) METRICS

To quantify and qualify the performance of our model, we employed:

- **Accuracy**: Proportion of correct predictions.
- **Precision**: Accuracy of positive predictions.
- **Recall (Sensitivity)**: True positive rate.
- **F1-Score**: Balance between precision and recall.

All evaluations were orchestrated on a dedicated federated validation dataset.

D. PERFORMANCE BENCHMARKS

Our model's mettle was tested against conventional centralized methodologies and leading-edge solutions. A comparative discourse, elucidating accuracy, precision, recall, and F1 scores, shall be furnished in the ensuing sections.

E. HYPERPARAMETERS AND METRICS

To elucidate the model's training dynamics, we table the hyperparameters employed in Table 3:

VII. RESULTS AND DISCUSSION

Our exploration of the FL-DAD methodology primarily revolves around the performance of federated learning for DDoS attack detection within IoT ecosystems. Herein, we summarize and discuss the outcomes of our experiments in terms of detection accuracy and other salient metrics.

A. DDOS ATTACK DETECTION METRICS

The heart of our experimental endeavor is to gauge the potency of federated learning in accurately pinpointing DDoS attacks in IoT environments.

TABLE 2. CNN architecture for the proposed FL-DAD methodology.

Layer Type	Number of Nodes/Filters	Other Parameters
Input Layer	-	Input Shape: (features_dim,)
Convolutional Layer 1	32 Filters	Kernel Size: 3x3, Activation: ReLU
Max Pooling Layer 1	-	Pool Size: 2x2
Convolutional Layer 2	64 Filters	Kernel Size: 3x3, Activation: ReLU
Max Pooling Layer 2	-	Pool Size: 2x2
Flatten Layer	-	-
Dense Layer 1	128 Nodes	Activation: ReLU
Output Layer	2 Nodes	Activation: Softmax

TABLE 3. Hyperparameters used for training the CNN-based FL-DAD model.

Hyperparameter	Value
Learning Rate	0.001
Batch Size	256
Epochs	50
Optimizer	Adam
Loss Function	Binary Crossentropy

Gleaning from Table 4, it's evident that the FL-DAD model boasts a uniformly high detection rate across various classes of DDoS attacks and benign data, showcasing both its precision and recall capabilities. Such a consistent performance, exceeding 98% across all metrics, is a testament to the efficacy of our approach.

B. FALSE POSITIVE AND FALSE NEGATIVE RATES

In the realm of cybersecurity, especially with respect to intrusion detection, two metrics stand out: the False Positive Rate (FPR) and the False Negative Rate (FNR). These metrics provide pivotal insights into the effectiveness of the detection system. An ideal system would have a minimal rate for both of these metrics. Our FL-DAD methodology has been evaluated for these metrics shown in Table 5, and the results are outstandingly low, showcasing the robustness and precision of our approach.

It's worth noting that while our model boasts high accuracy, precision, recall, and F1-Score values, maintaining low FPR and FNR values is crucial. A high FPR could lead to unnecessary resources being diverted to inspect benign traffic, while a high FNR could let potential threats go undetected. The presented rates underline the efficacy of FL-DAD in offering a balanced, nuanced detection mechanism, which is crucial for real-world deployments.

C. SCALABILITY ANALYSIS

To ensure the robustness and viability of the FL-DAD model in real-world deployments, especially in extensive IoT networks, we performed a scalability analysis. This evaluation focuses on the model's performance as the number of nodes (IoT devices) increases. Scalability is vital since IoT networks can encompass anything from a handful to millions of devices.

Table 6 reveals that as the number of nodes increases, the FL-DAD model still manages to maintain a high accuracy rate while moderately increasing training time and communication overhead. This growth in overhead and time, though present, is linear and manageable, making FL-DAD a promising solution for large-scale IoT deployments.

D. COMMUNICATION OVERHEAD

A significant aspect of federated learning is the communication overhead between nodes and the central server. We gauged the communication overhead by measuring the volume of exchanged data during each training epoch.

Table 7 elucidates a downward trend in communication overhead as training epochs progress. This is indicative of the efficiency of the FL-DAD model: as the model starts to converge, the updates become sparser, and thus the size of the transmitted data shrinks. By the 100th epoch, the data exchanged is down to 7.9 MB, showcasing a reduction in overhead as training progresses.

The observed diminishing communication overhead is a testament to the robust design of the FL-DAD methodology. Not only does it ensure reduced transmission costs over time, but it also underscores the model's adaptability in IoT environments. Given that IoT devices may often be constrained by bandwidth or may incur costs based on data transmission, this reduction is invaluable. The scalability and efficiency of the FL-DAD model prove advantageous for real-world deployment, allowing for efficient, cost-effective, and rapid attack detection in IoT ecosystems.

E. COMPARISON WITH CENTRALIZED APPROACHES

To ascertain the effectiveness of the proposed FL-DAD methodology, we compared its performance against several state-of-the-art centralized intrusion detection approaches validated on the CICIDS2017 dataset. The comparison includes several metrics such as accuracy, precision, recall, F1-score, communication overhead, and latency, which are crucial factors in the efficiency and scalability of intrusion detection systems, especially in federated learning contexts. The comparison offers insights into how federated learning stacks up against traditional centralized methods in the realm of DDoS attack detection in IoT, not only in terms of detection accuracy but also in reducing the communication burden across the network. The detailed comparison results are showcased in Table 8.

TABLE 4. Attack detection outcome of FL-DAD methodology on 80:20 of Training set/Testing set.

Attack Class	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
BENIGN	98.5	98.7	98.6	98.7
DDoS	98.7	98.8	98.9	98.9
DoS Hulk	98.6	98.8	98.7	98.8
DoS GoldenEye	98.9	98.7	98.8	98.8
DoS slowloris	98.5	98.6	98.5	98.5
DoS Slowhttptest	98.7	98.6	98.5	98.6
Heartbleed	98.8	98.8	98.7	98.8

TABLE 5. False positive and false negative rates of FL-DAD methodology on the CICIDS2017 dataset.

Attack Class	FPR (%)	FNR (%)
BENIGN	0.5	0.4
DDoS	0.3	0.2
DoS Hulk	0.4	0.3
DoS GoldenEye	0.3	0.2
DoS slowloris	0.5	0.5
DoS Slowhttptest	0.4	0.5
Heartbleed	0.2	0.3

TABLE 6. Scalability analysis of FL-DAD with an increasing number of nodes.

Nodes	Training Time (s)	Bandwidth (MB)	Accuracy (%)
20	10.2	5.5	98.5
50	11.5	25.2	98.7
100	13.7	48.5	98.9
200	25.6	210.1	99.1
500	48.3	390.2	99.3

TABLE 7. Communication overhead during selected training epochs.

Training Epoch	Data Exchanged (MB)
5	10.5
20	9.8
30	9.5
50	8.7
100	7.9

F. INSIGHTS AND IMPLICATIONS

The stellar outcomes of our FL-DAD system usher in several pivotal takeaways:

- Decentralized Efficacy: The detection rates underscore the potential of federated learning to cultivate accurate models without data centralization, a revelation of significant importance for distributed IoT networks.
- Privacy-centric Detection: Our approach not only guarantees exceptional detection accuracy but also sidesteps the transmission of raw data, amplifying the data privacy element.
- Adaptive Scalability: The results hint at the model's resilience and suggest its potential to maintain, if not elevate, its efficacy with an expanding IoT network.
- Differentiated Detection: The FL-DAD methodology discerns between different DDoS attack classes, emphasizing its granularity and depth of detection.

In essence, the FL-DAD methodology, tailored for DDoS attack detection in IoT frameworks, not only ensures exemplary detection rates but accentuates data privacy, scalability, and granularity. Such promising outcomes bolster the case for a wider adoption of federated learning in securing IoT systems against DDoS threats.

VIII. ROBUSTNESS AND SCALABILITY ANALYSIS

To ensure the practical applicability and viability of the FL-DAD methodology in real-world IoT networks, it is imperative to scrutinize its robustness and scalability. This section delves into these critical attributes.

A. ROBUSTNESS

The robustness of an intrusion detection system like FL-DAD is paramount, particularly in diverse and dynamic IoT environments where attack patterns might constantly evolve and vary.

Variability in Network Conditions Our evaluation subjected the FL-DAD model to a plethora of network conditions, including varying levels of nodes, training epochs, and dataset classes. The model displayed commendable resilience, retaining a high detection accuracy even in less-than-ideal network situations. Such robustness can be attributed to the decentralized nature of federated learning, where individual nodes process data locally, ensuring that transient network hiccups do not significantly degrade the overall system's performance.

B. SCALABILITY

The proliferation of IoT devices means that any system devised for such an environment must inherently be scalable.

1) PERFORMANCE WITH MORE NODES

As shown in the scalability analysis in Table 6, FL-DAD's performance metrics remain relatively consistent as the number of nodes increases. This consistency emphasizes the model's capability to scale without a significant drop in detection accuracy or efficiency. It demonstrates the benefits of federated learning, where the addition of more nodes actually contributes to model enhancement rather than leading to a system bottleneck.

2) PERFORMANCE IN TERMS OF COMMUNICATION OVERHEAD

A pivotal aspect of scalability, especially in federated learning, is the model's efficiency in managing communication overhead. From our evaluations, as depicted in

TABLE 8. Performance comparison of FL-DAD against centralized approaches.

Method (Reference)	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Comm. Overhead (MB)	Latency (ms)
Deep CNN [45]	97.2	97.1	97.3	97.2	18	120
SVM-based IDS [46]	96.8	96.7	96.9	96.8	18	110
Random Forest [47]	97.4	97.5	97.3	97.4	16	108
Hybrid Model [48]	97.8	97.7	97.9	97.8	15	95
FL-DAD (Proposed Work)	98.7	98.8	98.9	98.9	12	80

Table 7, even as the training progressed across epochs, the data exchanged between nodes and the central server demonstrated a consistent decline. This trend, wherein the data exchanged reduced from 10.5 MB at the 5th epoch to 7.9 MB at the 100th epoch, manifests the model's adaptability and efficiency. Such proficiency in reducing communication overhead without sacrificing performance accentuates FL-DAD's suitability for extensive IoT setups, where efficient data transmission is critical.

3) COMPARISON WITH CENTRALIZED APPROACHES

It's worth highlighting again the scalability advantages of FL-DAD over centralized methods. As depicted in Table 8, FL-DAD not only surpasses many centralized techniques in performance metrics but also inherently possesses a structural advantage in scalability. Centralized methods often encounter bottlenecks with data centralization, transfer costs, and single-point failures. In contrast, FL-DAD distributes the learning process, thereby eliminating these potential chokepoints.

Adaptability to Device Diversity and Data Variability: **To further address the scalability to larger and more diverse IoT networks, FL-DAD incorporates dynamic adaptation mechanisms. These mechanisms enable the system to efficiently manage and learn from the diverse data types generated by a wide array of IoT devices. By employing advanced algorithms for data preprocessing and feature extraction, FL-DAD ensures that the variability in device capabilities and data formats does not compromise the learning process. This adaptability not only enhances the model's generalizability across different IoT environments but also ensures that the system remains scalable and effective, even as the network expands and diversifies.**

C. IMPLICATIONS FOR GROWING IOT NETWORKS

As IoT networks grow in size and complexity, the need for decentralized solutions like FL-DAD becomes even more pronounced. The results of our robustness and scalability analysis project a promising trajectory for federated learning in the IoT intrusion detection domain.

- Decentralization Benefits: The decentralized nature of FL-DAD allows it to harness the processing capabilities of multiple nodes, spreading the computational load. This ensures that as the network grows, the system can tap into additional resources without overwhelming any single node or causing significant performance degradation.
- Adaptive Learning: As newer devices with diverse data patterns join the IoT network, FL-DAD can adapt its learning process in real-time. This ensures that the system remains relevant and effective, continually updating its knowledge base without requiring periodic centralized retraining.

D. CHALLENGES AND LIMITATIONS

- **Achieving Consistent Accuracy:** The heterogeneous nature of data across different nodes occasionally posed challenges in maintaining a consistent model accuracy. Some nodes, due to their distinct data characteristics, influenced the global model in ways that required additional training epochs for convergence.
- **Harmonizing with Existing Systems:** Incorporating the FL-DAD system within established IoT networks proved intricate at times. The presence of legacy systems and their associated complexities occasionally impeded a fluid integration process.
- **Anomalous Data Intricacies:** Notwithstanding our meticulous preprocessing efforts, certain nodes sporadically presented anomalous data patterns. These could be attributed to distinct local network behaviors or sporadic device irregularities, occasionally injecting noise during model training.
- **Computational Complexity:** Although the federated learning paradigm aims to decentralize and hence reduce computational burdens, the aggregation phase, particularly with an increasing number of participatory nodes, culminated in notable overheads. Striking a balance between this overhead and achieving prompt model updates emerged as a pertinent challenge.
- **Resource Constraints on Edge Devices:** Edge devices in IoT networks often have limited computational power and battery life, which poses a challenge for executing complex model training locally. To mitigate this, we propose the use of model compression techniques and lightweight learning models that require less computational power and energy consumption. Moreover, implementing predictive maintenance strategies can help in scheduling training tasks during off-peak hours to optimize resource usage.
- **Communication Overhead:** The frequent exchange of model updates between nodes and the central server in FL-DAD can lead to significant

communication overhead, especially in large-scale IoT networks. To address this issue, we suggest employing communication-efficient federated learning algorithms, such as Federated Averaging, that reduce the frequency of communications by allowing local models to train for more epochs before aggregation. Additionally, techniques like quantization and sparsification can be applied to reduce the size of the model updates being transmitted, thereby minimizing bandwidth usage.

- **Dataset Specificity:** Our current use of the CICIDS2017 dataset as a primary test source shows limited effectiveness against a broader range of DDoS attacks, potentially limiting the generalizability of our findings.

E. FUTURE DIRECTIONS

- **Advancing Convergence Strategies:** Subsequent versions of FL-DAD could delve into sophisticated algorithms and techniques that expedite model convergence amidst the variability of data across nodes.
- **Seamless Integration Mechanisms:** Future work could emphasize devising tools or middleware solutions that facilitate a seamless integration of the FL-DAD approach across diverse IoT frameworks, bolstering its feasibility for broader applications.
- **Robust Anomaly Management:** There's ample scope to engineer advanced anomaly detection and correction mechanisms that can proactively identify and neutralize data aberrations before they impact model training.
- **Efficiency in Aggregation Protocols:** Investigating and implementing more efficient data aggregation methodologies can substantially alleviate the computational overhead, enhancing the scalability prospects of the FL-DAD system.
- **Expanding Dataset Diversity:** To ensure a more comprehensive validation of the FL-DAD system, future research will focus on incorporating a wider array of datasets, encompassing diverse and multifaceted DDoS attack scenarios beyond CICIDS2017.
- **Diverse Attack Types** In recognition of the evolving nature of DDoS attacks and their increasing sophistication, we plan to extend our evaluation of FL-DAD against a broader spectrum of DDoS attack types, including more sophisticated and blended attacks in the future work. This expansion will ensure that FL-DAD remains effective in the face of new and emerging threats, continuously enhancing its applicability and robustness in securing IoT networks against a diverse range of cyber threats.

IX. CONCLUSION

In this research, we embarked on an exploration of the potential of Federated Learning (FL) in bolstering the security landscape of Internet of Things (IoT) networks, particularly focusing on the detection of Distributed Denial of Service (DDoS) attacks. Our proposed FL-DAD methodology underscored the efficacy of decentralizing the learning process, ensuring data privacy while not compromising on detection accuracy. The numerical results demonstrated that our FL-DAD approach achieved an accuracy rate consistently above 98% across various DDoS attack classes, significantly outperforming traditional centralized models. Noteworthy findings included the system's resilience in terms of accuracy even when exposed to varied data attributes across nodes and its competitive edge over centralized counterparts. Moreover, the challenges and intricacies encountered, ranging from the harmonization with legacy systems to handling anomalous data intricacies, paved the way for charting future research directions. The demonstrated high performance, particularly in terms of precision and recall, reinforces the practical applicability of FL-DAD in real-world IoT security scenarios. These directions, which span from advancing convergence strategies to devising efficient aggregation protocols, will serve as cornerstones for further refinement of FL-DAD.

DECLARATION OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this research article.

REFERENCES

[1] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, Jun. 2022.

[2] M. Pouresmaieli, M. Ataei, and A. Taran, "Future mining based on Internet of Things (IoT) and sustainability challenges," *Int. J. Sustain. Develop. World Ecol.*, vol. 30, no. 2, pp. 211–228, Feb. 2023.

[3] J. Rivera and L. Goasduff, "Gartner says a thirty-fold increase in Internet-connected physical devices by 2020 will significantly alter how the supply chain operates," Gartner, Stamford, CT, USA, Tech. Rep., 2020.

[4] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, and S. A. Bahaj, "Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT)," *Electronics*, vol. 11, no. 3, p. 494, Feb. 2022.

[5] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndzi, S. A. Chelloug, M. A. Elaziz, M. A. A. Al-Qaness, and S. F. Jilani, "Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT," *Sensors*, vol. 22, no. 7, p. 2697, Mar. 2022.

[6] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Designing a blockchain approach to secure firefighting stations based Internet of Things," *Informatica*, vol. 47, no. 10, Dec. 2023.

[7] L. Gerrits, "Comparative study of EOS and IOTA blockchains in the context of smart IoT for mobility," Ph.D. dissertation, Université Nice-Sophia-Antipolis, Nice, France, 2020.

[8] M. Aslam, D. Ye, M. Hanif, and M. Asad, "Machine learning based SDN-enabled distributed denial-of-services attacks detection and mitigation system for Internet of Things," in *Proc. 3rd Int. Conf. Mach. Learn. Cyber Secur.*, Guangzhou, China, Springer, 2020, pp. 180–194.

[9] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.

[10] M. Asad, S. Shaukat, E. Javanmardi, J. Nakazato, N. Bao, and M. Tsukada, "Secure and efficient blockchain-based federated learning approach for VANETs," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 9047–9055, 2023.

[11] C.-D. Lee, J.-H. Li, and T.-H. Chen, "A blockchain-enabled authentication and conserved data aggregation scheme for secure smart grids," *IEEE Access*, vol. 11, pp. 85202–85213, 2023.

[12] Q. Tian, C. Guang, C. Wenchao, and W. Si, "A lightweight residual networks framework for DDoS attack classification based on federated learning," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.

[13] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, Apr. 2023, Art. no. 103096.

[14] P. Szynkiewicz, "Signature-based detection of botnet DDoS attacks," in *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*, Springer, 2022, pp. 120–135.
[15] P. K. Kishore, S. Ramamoorthy, and V. N. Rajavarman, "ARTP: Anomaly based real time prevention of distributed denial of service attacks on the web using machine learning approach," *Int. J. Intell. Netw.*, vol. 4, pp. 38–45, Nov. 2023.
[16] L. Liu, H. Wang, Z. Wu, and M. Yue, "The detection method of low-rate DoS attack based on multi-feature fusion," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 504–513, Nov. 2020.
[17] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices," *Arabian J. Sci. Eng.*, vol. 47, no. 2, pp. 1353–1374, Feb. 2022.
[18] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lyu, "FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4059–4068, Jun. 2022.
[19] M. Paricherla, S. Babu, K. Phasinam, H. Pallathadka, A. S. Zamani, V. Narayan, S. K. Shukla, and H. S. Mohammed, "Towards development of machine learning framework for enhancing security in Internet of Things," *Secur. Commun. Netw.*, vol. 2022, pp. 1–5, May 2022.
[20] Q. Li, H. Huang, R. Li, J. Lv, Z. Yuan, L. Ma, Y. Han, and Y. Jiang, "A comprehensive survey on DDoS defense systems: New trends and challenges," *Comput. Netw.*, vol. 233, Sep. 2023, Art. no. 109895.
[21] X. Feng, X. Zhu, Q.-L. Han, W. Zhou, S. Wen, and Y. Xiang, "Detecting vulnerability on IoT device firmware: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 1, pp. 25–41, Jan. 2023.
[22] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison," *Bull. Electr. Eng. Informat.*, vol. 12, no. 2, pp. 930–939, Apr. 2023.
[23] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022.
[24] A. Singh, H. Kaur, and N. Kaur, "A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network," *Cluster Comput.*, pp. 1–21, Oct. 2023.
[25] Y. Zhong, L. Chen, C. Dan, and A. Rezaeipanah, "A systematic survey of data mining and big data analysis in Internet of Things," *J. Supercomput.*, vol. 78, no. 17, pp. 18405–18453, Nov. 2022.
[26] Z. Alarnaout, N. Mostafa, S. Alabed, W. H. F. Aly, and A. Shdefat, "RAPT: A robust attack path tracing algorithm to mitigate SYN-flood DDoS cyberattacks," *Sensors*, vol. 23, no. 1, p. 102, Dec. 2022.
[27] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense," *Future Internet*, vol. 15, no. 2, p. 62, Jan. 2023.
[28] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020.
[29] J. Zheng, K. Li, N. Mhaisen, W. Ni, E. Tovar, and M. Guizani, "Exploring deep-reinforcement-learning-assisted federated learning for online resource allocation in privacy-preserving EdgeIoT," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21099–21110, Nov. 2022.
[30] M. Asad, A. Moustafa, and T. Ito, "FedOpt: Towards communication efficiency and privacy preservation in federated learning," *Appl. Sci.*, vol. 10, no. 8, p. 2864, Apr. 2020.
[31] M. Asad, A. Moustafa, F. A. Rabhi, and M. Aslam, "THF: 3-Way hierarchical framework for efficient client selection and resource management in federated learning," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11085–11097, Jul. 2022.
[32] Q. Pan, J. Wu, A. K. Bashir, J. Li, W. Yang, and Y. D. Al-Otaibi, "Joint protection of energy security and information privacy for energy harvesting: An incentive federated learning approach," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3473–3483, May 2022.
[33] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.
[34] M. Asad and S. Otoum, "Towards privacy-aware federated learning for user-sensitive data," in *Proc. 5th Int. Conf. Blockchain Comput. Appl. (BCCA)*, Oct. 2023, pp. 343–350.
[35] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.
[36] M. Aljanabi, "Navigating the void: Uncovering research gaps in the detection of data poisoning attacks in federated learning-based big data processing: A systematic literature review," *Mesopotamian J. Big Data*, vol. 2023, pp. 149–158, Dec. 2023.
[37] S. Dange and M. Chatterjee, "IoT botnet: The largest threat to the IoT network," in *Data Communication and Networks*, Springer, 2019, pp. 137–157.
[38] N.-N. Dao, T. V. Phan, U. Sa'ad, J. Kim, T. Bauschert, D.-T. Do, and S. Cho, "Securing heterogeneous IoT with intelligent DDoS attack behavior learning," *IEEE Syst. J.*, vol. 16, no. 2, pp. 1974–1983, Jun. 2022.
[39] M. Asad, A. Moustafa, T. Ito, and M. Aslam, "Evaluating the communication efficiency in federated learning algorithms," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2021, pp. 552–557.
[40] M. Asad, A. Moustafa, and T. Ito, "Federated learning versus classical machine learning: A convergence comparison," 2021, *arXiv:2107.10976*.
[41] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5476–5497, Apr. 2021.
[42] M. Asad, S. Shaukat, D. Hu, Z. Wang, E. Javanmardi, J. Nakazato, and M. Tsukada, "Limitations and future aspects of communication costs in federated learning: A survey," *Sensors*, vol. 23, no. 17, p. 7358, Aug. 2023.
[43] T. Solanki, B. K. Rai, and S. Sharma, "Federated learning using tensor flow," in *Federated Learning for IoT Applications*, Springer, 2022, pp. 157–167.
[44] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 479–482, 2018.
[45] J.-H. Lee, J.-W. Kim, and M.-J. Choi, "SSAE—DeepCNN model for network intrusion detection," in *Proc. 22nd Asia–Pacific Netw. Operations Manage. Symp. (APNOMS)*, Sep. 2021, pp. 78–83.
[46] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Netw.*, vol. 24, no. 5, pp. 1821–1829, Jul. 2018.
[47] C. Liu, Z. Gu, and J. Wang, "A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning," *IEEE Access*, vol. 9, pp. 75729–75740, 2021.
[48] A. Meryem and B. E. Ouahidi, "Hybrid intrusion detection system using machine learning," *Netw. Secur.*, vol. 2020, no. 5, pp. 8–19, May 2020.

YASER ALHASAWI received the B.S. degree in management information systems (MIS) from the University of Business and Technology, Jeddah, Saudi Arabia, in 2007, and the M.S. and Ph.D. degrees in information systems and technology from Claremont Graduate University, Claremont, CA, USA, in 2016 and 2019, respectively. He is currently an Assistant Professor with the Department of Management of Information Systems (MIS), King Abdulaziz University (KAU). He has authored and coauthored many journal articles and conference papers. His research interests include artificial intelligence (AI) technologies, the IoT, deep learning, neural network technology, security, and privacy.

SALEM ALGHAMDI received the B.S. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2005, and the M.S. and Ph.D. degrees in information systems and technology from Claremont Graduate University, Claremont, CA, USA, in 2016 and 2019, respectively. Since 2019, he has been an Assistant Professor. He is a Certified Digital Enterprise Transformation, Certified KPI Professional, and Certified KPI Practitioner. As the Technical Team Manager, he employs excellent leadership skills and multi-tasking strengths. His research interests include artificial intelligence, blockchain, the Internet of Things, digital transformation, information security and privacy, and mixed reality.