A Customized Temporal Federated Learning Through Adversarial Networks for Cyber Attack Detection in IoT

Lavanya Vemulapalli [1*], P. Chandra Sekhar [2]
[1] Research Scholar, Department of Computer Science and Engineering, Gitam University, Visakhapatnam, Andhra Pradesh, India
[2] Associate Professor, Department of Computer Science and Engineering, Gitam University, Visakhapatnam, Andhra Pradesh, India
Email: [1] lavanyavemulapalli@gmail.com, [2] chandoo.potala@gmail.com
*Corresponding Author

***Abstract*—The exponential growth of the Internet of Things (IoT) has heightened the need for secure, privacy-preserving, and efficient cyber-attack detection mechanisms. This study introduces the Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN) framework, which combines Temporal Convolutional Networks (TCNs) and Generative Adversarial Networks (GANs) for robust and personalized attack detection. CusTFL-AN enables clients to train local models while maintaining data privacy by generating synthetic datasets using GANs and aggregating these at a central server, thereby mitigating risks associated with direct data sharing. The framework's effectiveness is demonstrated on three benchmark datasets—UNSW-NB15, BoT-IoT, and Edge-IIoT—achieving detection accuracies of 99.2%, 99.5%, and 99.25%, respectively, significantly outperforming state-of-the-art methods. Key enhancements include addressing data heterogeneity through federated aggregation, minimizing overfitting using GAN validation and cross-validation techniques, and ensuring interpretability to support practical adoption in real-world IoT scenarios. Privacy mechanisms are strengthened to prevent potential data leakage during aggregation, and ethical considerations surrounding the use of synthetic datasets are acknowledged. Furthermore, the impact of computational constraints, network latency, and communication overhead on resource-constrained IoT devices has been carefully analyzed. While the results affirm the robustness and scalability of CusTFL-AN, future work will focus on extending evaluations to more diverse datasets and addressing the challenges of adversarial attacks. CusTFL-AN represents a significant step forward in privacy-preserving federated learning, offering practical solutions to real-world IoT cybersecurity challenges.**

Keywords—Federated Learning; Adversarial Networks; Cyber-Attack Detection; Temporal Convolutional Networks; Privacy Preservation.

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) ecosystem, encompassing smart homes, healthcare devices, industrial sensors, and autonomous vehicles, has introduced unprecedented opportunities for automation and data-driven insights. However, this growth has also significantly increased the attack surface for cyber threats. Devices with limited computational power and weak security protocols, such as smart thermostats, wearable health monitors, and industrial actuators, are particularly vulnerable to exploits like Distributed Denial of Service (DDoS) attacks, ransomware, and data exfiltration [1][2]. Reports indicate a dramatic rise in cyberattacks, with incidents doubling between 2020 and 2021, as IoT devices become prime targets due to their accessibility and volume of sensitive data exchanged [3]. Recent studies highlight a 40% increase in botnet activities targeting IoT devices, emphasizing the urgency of effective countermeasures [4].

Traditional machine learning (ML) and deep learning (DL) techniques have been extensively applied to address these threats, but their reliance on centralized data aggregation presents significant privacy challenges. Centralized architectures expose sensitive user data to risks of interception, unauthorized access, and misuse [5][6]. For example, a breach in centralized intrusion detection systems could lead to large-scale compromises of private user data [7]. While Federated Learning (FL) offers a decentralized alternative by enabling model training at the edge without raw data sharing, current FL methods face substantial challenges, including client heterogeneity, data imbalance, and scalability [8][9]. The use of a single global model in FL often fails to accommodate the diverse requirements of IoT clients, and reliance on uniform model designs can lead to intellectual property leaks and suboptimal performance [10].

To address these limitations, this study introduces the Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN) framework, which integrates Temporal Convolutional Networks (TCNs) and Generative Adversarial Networks (GANs). TCNs are utilized for capturing temporal dependencies in multivariate IoT traffic data [11], while GANs generate synthetic datasets that preserve privacy during aggregation [12]. This approach ensures that each client can benefit from federated knowledge without exposing sensitive data or model architectures. Synthetic data generation through GANs not only mitigates privacy concerns but also addresses the heterogeneity of IoT datasets, enhancing detection robustness across various attack scenarios. The integration process involves generating client-specific synthetic data, aggregating it at a central server, and redistributing enriched datasets for iterative

model refinement, thereby bridging the gap between privacy preservation and high performance [13].

The ethical and legal implications of leveraging GAN-generated synthetic data are significant and have been carefully considered. While synthetic data mitigates direct privacy risks, concerns about the potential misuse of generated patterns or reverse engineering remain [14]. Ethical safeguards, such as rigorous dataset validation and adherence to privacy regulations like GDPR, are integral to the proposed framework [15].

The objectives of this research are clearly defined to address critical gaps in existing FL solutions. Specifically, the study aims to (1) enable personalized model training for diverse IoT clients without compromising data privacy, (2) enhance detection accuracy by leveraging synthetic datasets and addressing data heterogeneity, and (3) evaluate the practical feasibility of the proposed framework under constraints such as communication overhead, latency, and resource limitations. This research thus contributes to a theoretically grounded, practically viable, and ethically responsible solution to IoT cybersecurity challenges.

The rest of the paper is structured as follows: Section 2 reviews related work, Section 3 explains the proposed methodology, Section 4 presents the performance evaluation results, and Section 5 concludes the study with future research directions.

II. RELATED WORKS

We first review recent works on privacy-preserving frameworks and Federated Learning (FL) for IoT security. A few targeted techniques in the literature are grouped based on their associated limitations, followed by a discussion of how our proposed approach fills these gaps.

A. Cyber Attack Detection in IoT with Privacy Preserving Frameworks

Recent interest in privacy preservation regarding cyberattack detection in IoT has sprung up with the high number of devices connected and the nature of data being exchanged within cyberspaces. Various approaches to resolve this challenge have been proposed, with an emphasis on keeping data private while still enabling useful intrusion detection. Another well-known scheme is federated learning techniques that enable model training based on collaborative training between IoT-distributed devices without the need to transmit network traffic data over a network [15]. Comparison to standalone models trained locally on each device has revealed this method improves on detection accuracy and communications efficiency by a significant margin. A hierarchical blockchain based federated learning framework for secure and privacy constrained collaborative IoT intrusion detection has been proposed, advocating the need for sharing cyber threat intelligence among interorganizational IoT networks [17]. Several approaches have been proposed to address this challenge, with a focus on maintaining data privacy, while enabling effective intrusion detection. One prominent approach is the use of federated learning techniques, which allow collaborative model training across decentralized IoT devices without the direct transmission of network traffic data [16]. This method has shown significant improvements in detection accuracy and communication efficiency compared with standalone models trained locally on individual devices. Similarly, a hierarchical blockchain-based federated learning framework has been proposed to enable secure and privacy-preserved collaborative IoT intrusion detection, emphasizing the importance of sharing cyber threat intelligence among inter-organizational IoT networks [17]. Some researchers have sought to integrate trust management and privacy-preserving mechanisms into collaborative intrusion detection systems (CIDS). An example is the general approach of enhanced security for such environments with a CIDS framework, which includes lightweight architecture, distributed ledger technology, and dominated learning[18]. In a different approach, a Social Intrusion Detection System (SIDS)[19] takes advantage of the norms of relationships among objects in a system to support a privacy-preserving collaborative method of detection in IoT environments. Finally, we conclude that the field of privacy-preserving cyberattack detection in IoT is advancing rapidly from federated learning and blockchain-based solutions to trust-oriented and social relationship-based systems. These frameworks attempt to achieve a tradeoff between the validity of intrusion detection and retaining data privacy in distributed and sensitive IoT ecosystems.

B. Blockchain-Based Federated Learning for Cyber Attack Detection in IoT

However, cyber-attack detection in IoT environments has emerged as a promising approach to blockchain-based federated learning approaches that address privacy concerns and provide greater security. This integration has been explored in several studies and has been shown to achieve improved intrusion detection while maintaining data privacy. A federated learning framework based on hierarchical blockchain to support secure, and privacy preserved collaborative IoT intrusion detection [20] [21] has been proposed. This study focuses on the sharing of cyber threat intelligence among interorganizational IoT networks to enhance the model detection ability. Securely designed by a secure immutable ledger for transactions and systematic smart contracts for the evaluation of the task, the framework combines an ML-based intrusion detection system for robust attacks while maintaining data privacy. We propose a communication cost optimization method that considers node security verification for blockchain-based federated learning to reduce the communication costs induced by the increase in node security verification, along with the solution for security evaluation [22]. This method combines competing voting verification methods and aggregation algorithms to enhance communication costs by incorporating double-layer aggregation-filtered learning. We developed an intelligent intrusion detection mechanism, FIDANN, in the healthcare sector based on federated learning using Dwarf mongoose optimized artificial neural networks.

Using blockchain technology, this approach mitigates contamination attacks and guarantees full transparency and data integrity in a decentralized system. It has been experimentally demonstrated that federated deep learning approaches a better scale to ensure private data from IoT devices while achieving higher accuracy in detecting attacks

compared with classic/centralized machine learning algorithms [24]. This study compared the performance of centralized and federated learning using three deep learning approaches: These 3 are Recurrent Neural networks (RNN), convolutional neural networks (CNN), and deep neural networks (DNN). We have shown that the combination of block chaining and federated learning for intrusion detection in IoT offers good potential to mitigate security and privacy risks. However, these approaches have extended detection capabilities, featured finer data privacy, and enhance resistance against multiple cyberattacks in the IoT environment.

C. Deep Federated Learning Models for Cyber Attack Detection in IoT

Cyber-attack detection in IoT environments has presented privacy concerns, which are addressed by emergent Deep Federated Learning (DFL) models, while preserving high detection accuracy. The resulting models take advantage of the distributed nature of IoT networks to train machine-learning models in a collaborative manner without raw data [25, 26].Furthermore, deep learning integrated with federated learning has shown a 5–8.2% improvement in the f1-score for detecting various types of cyber-attacks, including zero-day botnet attacks, DDoS attacks, and other intrusions [27], [28], [29]; for instance, the deep federated multimodal model proposed in [30] improved by 8.2% across three clients and provided interpretability through Shapley Additive Explanations (SHAP). Various types of cyber-attacks exist, including zero-day botnet attacks, DDoS attacks, and other intrusions [27][28][29]. For instance, a deep federated multimodal model introduced in [30] demonstrated an average 8.2% improvement in the f1-score across three clients, while also enhancing interpretability using Shapley Additive Explanations (SHAP). Notably, some studies have reported that the performance of federated deep learning approaches is better than that of classic centralized machine learning models, in terms of both privacy assurance and attack detection accuracy [31]. Nevertheless, federated learning models experience challenges including data heterogeneity and class imbalance among devices. To address this, novel approaches such as FedMADE [32] that dynamically aggregate local models proportional to their contribution to the overall performance improve the minority attack classification accuracy by as much as 71.07%. I conclude that deep federated learning models provide a promising solution for detecting cyberattacks in IoT networks in a way that respects privacy with high detection accuracy. In the face of the field's evolution, challenges posed by data heterogeneity and class imbalance are key to progress in making these models more performant and robust in real-world IoT security use cases.

D. Adaptive Federated Learning for Cyber Attack Detection in IoT

Adaptive Federated Learning (AFL) has emerged as a promising approach for cyber-attack detection in IoT environments, as it addresses the challenges of data privacy and heterogeneity. Several studies have explored this area, showing the potential of AFL in improving the detection accuracy and efficiency. FedMADE, a novel dynamic aggregation method, was proposed to address the issue of attack-class imbalance among devices. This approach clusters devices based on their traffic patterns and aggregates local models according to their contribution to the overall performance. Experimental results have shown up to a 71.07% improvement in minority attack classification accuracy compared to other FL algorithms designed for non-IID data [33]. Another study introduced a hierarchical blockchain-based federated learning framework for secure and privately preserved collaborative IoT intrusion detection. This approach emphasizes the importance of sharing cyberthreat intelligence among inter-organizational IoT networks to enhance model detection capabilities while ensuring data privacy [34]. Researchers have also explored the use of various deep learning models within the FL framework for IoT security. A comprehensive study comparing centralized and federated versions of Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), and Deep Neural Networks (DNN) on three real IoT traffic datasets demonstrated that federated deep learning approaches outperformed classic centralized versions in terms of privacy assurance and attack detection accuracy [35]. Some studies have investigated the impact of different data distributions and aggregation functions on FL-enabled Intrusion Detection Systems (IDS). For instance, an evaluation using the ToN_IoT dataset with various partitioning schemes based on IoT device IP addresses and attack types revealed the importance of considering data distribution in FL-IDS implementations [36]. In conclusion, adaptive federated learning approaches for cyber-attack detection in IoT have shown promising results in addressing privacy concerns, handling data heterogeneity, and improving the detection accuracy. However, challenges remain in optimizing the model performance across diverse IoT environments and attack scenarios.

Siracusa and Domenico, using the name Domenico) proposed an adaptive federated learning approach (FLAD) for DDoS attack detection in dynamic cybersecurity scenarios [37]. By dynamically allocating the processing power among nodes with more complex attack profiles, FLAD improves the model convergence. However, this method requires numerous model updates; thus, the detection time is increased. This issue is addressed by our CusTFL-AN model, in which each client learns to update its model on synthesized datasets faster and with better accuracy by customizing FL through adversarial sample sharing.

E. Clustered Federated Learning for Cyber Attack Detection in IoT

The problems of data privacy and heterogeneity have spurred the development of a new approach for cyber-attack detection in IoT environments known as Clustered Federated Learning (CFL). Several of these applications have been principally explored and found to show the significant capacity of CFL in increasing detection accuracy while simultaneously promoting data privacy. We propose a novel deep federated multimodal model for cyberattack detection in Industrial Control System (ICS) environments with representation learning domain adaptation and federated learning, where we trained it to 8.2% f1 score improvement on average on three clients, making federated learning a potential tool for ICS security [38]. Federated deep-learning

approaches have been shown to outperform classic centralized machine learning in terms of ensuring the privacy of IoT device data and attaining more accurate attack detection [39]. In this study, we compared the performance of centralized and federated learning in terms of three deep learning models (CNN, RNN, and DNN) for real IoT traffic datasets. I introduced an innovative approach for cyber threat detection in IoT networks using an optimal Federated Learning approach with Digital Twin technology [40]. Typically, the latency introduced by traditional federated averaging methods is inherently slower, but this system works much more efficiently, with improvements in both the model aggregation efficiency and latency. A deep learning framework, DFSat, was also constructed in the context of IoT-integrated satellite networks for intrusion detection [41]. We present a distributed deep learning-based attack detection framework that leverages recurrent neural network-based attack differentiation, which significantly enhances the ability to distinguish between complex cyberattacks in IoT devices. The SIM-FED model, which combines deep learning and federated learning algorithms, has been proposed [42]. to distinguish complex cyberattacks. The SIM-FED model, which combines deep and federated learning algorithms, has been proposed for malware detection in IoT devices [42]. This model reaches 99.52% accuracy, and it is resistant to white and black box cyber-attacks, leading to the strong potential of CFL for improving IoT security. Taken together, these studies indicate that Clustered Federated Learning is becoming more relevant, accurate, privacy preserving, and more robust against various attack types for cyber-attack detection in the IoT environment [43][44].

TABLE I. COMPARATIVE ANALYSIS OF TRADITIONAL CYBER-ATTACK DETECTION APPROACHES IN IOT ENVIRONMENTS

Approach	Description	Advantages	Limitations
Centralized ML Models	Central server collects data from IoT devices for training [39]	High accuracy with large datasets.	Privacy risks, data transmission costs, and central point of failure.
Distributed IDS	Intrusion Detection Systems deployed across the network [15]	Real-time detection, distributed nature.	Scalability issues, potential inconsistency in detection.
Signature-based IDS	Detects known attacks using pre-defined signatures [27]	High accuracy for known attacks.	Ineffective against unknown or evolving attacks.
Anomaly-based IDS	Monitors for deviations from normal behavior patterns [26]	Can detect zero-day attacks.	High false positive rates require constant updates.
Blockchain-Based Models	Use blockchain for secure data sharing among IoT devices [16]	Enhanced data integrity and privacy.	High computational costs and network latency.
Federated Learning	Collaborative model training without sharing raw data [17]	Preserves data privacy, decentralized.	Vulnerable to data heterogeneity and communication overhead

F. Limitations of the Study

1) Data Heterogeneity: The heterogeneity of IoT-generated data poses a significant challenge for federated learning models to achieve effective convergence, leading to variability in detection accuracy.

2) Communication Costs: Frequent model updates in federated learning can lead to high communication costs, especially in resource-constrained IoT environments.

3) Class Imbalance: Many studies have struggled with imbalanced datasets, where some attack types are underrepresented, thereby affecting the detection accuracy of minority attack classes.

4) Scalability: As IoT ecosystems continue to expand, maintaining the performance and efficiency of privacy-preserving frameworks has become more complex.

5) Adversarial Attacks: Federated learning methods remain vulnerable to adversarial attacks, which can potentially compromise the training process and degrade the detection performance.

6) Blockchain Overheads: While blockchain integration enhances security and privacy, it also introduces computational and storage overheads, which can impact the efficiency of IoT networks.

These findings emphasize the necessity of ongoing research to develop more adaptive, scalable, and robust privacy-preserving techniques that address the evolving challenges in IoT cybersecurity.

III. PROPOSED MODEL : CUSTFL-AN MODEL

This section describes the proposed Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN) framework. The framework integrates Temporal Convolutional Networks (TCNs) [45] and Generative Adversarial Networks (GANs) [46] to achieve effective, privacy-preserving, and scalable cyber-attack detection in IoT environments. The methodological flow is structured to ensure clarity, address data heterogeneity, mitigate communication costs, and provide robust convergence guarantees.

The proposed framework, Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN), introduces a novel approach to addressing the challenges of cyber-attack detection in IoT environments while ensuring privacy preservation and scalability. The framework is structured around three interconnected components: client-side training, synthetic data generation, and federated aggregation [47]. These components work cohesively to enable robust and personalized attack detection across diverse and dynamic IoT networks. The model was evaluated using three well-known datasets: UNSW-NB15 [48], BoT-IoT [49], and Edge-IioT [50], which collectively cover a range of network traffic patterns and attack scenarios. As shown in Fig. 1, the architecture of the proposed model presents a collaborative learning framework in which multiple clients (e.g., IoT devices) interact with a central server. The methodology is as follows.

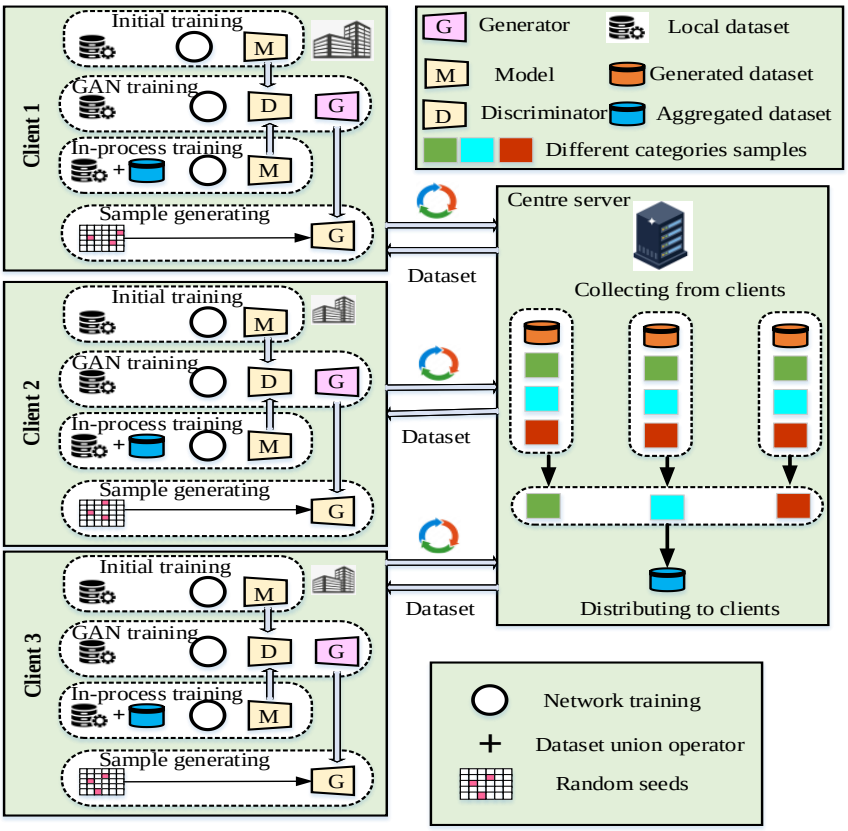

Fig. 1. Architecture of proposed CusTFL-AN model

A. *Client-Side Training*

At the client level, IoT devices train local models using **Temporal Convolutional Networks (TCNs)** on their private datasets. This ensures that raw data remains localized, preserving privacy. TCNs are particularly suited for IoT applications as they model sequential data using **causal dilated convolutions [51]**, capturing long-term dependencies efficiently.

1) *Initial Local Training*

In the first phase, each loT client trains a local model using Temporal Convolutional Networks (TCNs) on its private dataset, such as UNSW-NB15, BoT-loT, or Edge-lloT. The TCN architecture is specifically chosen for its ability to capture long-term temporal dependencies inherent in loT traffic patterns, which are crucial for distinguishing between normal and malicious behavior.

- Let the client-specific dataset be denoted as $D_i^{\text{local}} = \{(x_j, y_j)\}_{j-1}^{n_i}$, where x_j represents an input sequence and y_j the corresponding label. The local TCN model f_θ is trained by minimizing the cross-entropy loss:

$$\mathcal{L}_{\text{local}} = -\frac{1}{n_i}\sum_{j=1}^{n_i}\left[y_j \log\left(f_\theta(x_j)\right) + (1-y_j)\log\left(1-f_\theta(x_j)\right)\right]$$

- The TCN model employs causal dilated convolutions to ensure that predictions at time t depend only on previous inputs $\{x_1, x_2, \ldots, x_t\}$. The output at time t is computed as:

$$z_t = \sum_{i=0}^{k-1} W_i \cdot x_{t-d-i}$$

where k is the kernel size, d is the dilation rate, and W_i are the convolution weights [52]. This initial training phase allows each client to learn attack-specific patterns in its localized dataset without sharing raw data, thereby preserving privacy.

2) *GAN Training*

To enhance privacy and address data heterogeneity, each client employs a Generative Adversarial Network (GAN) [53] for synthetic data generation. The GAN consists of two neural networks:

- Generator (G) : Generates synthetic data samples from random noise vectors $z \sim P_z$, where P_z is a latent distribution (e.g., Gaussian or uniform).
- Discriminator (D): Distinguishes between real data ($x \sim P_{\text{data}}$) and synthetic data ($G(z)$).

The adversarial training process is formulated as a minimax optimization problem:

$$\min_G \max_D \mathbb{E}_{x\sim P_{\text{data}}}[\log D(x)] + \mathbb{E}_{z\sim P_z}[\log(1-D(G(z)))]$$

1. Discriminator Training: The discriminator is trained to maximize its ability to distinguish between real and synthetic samples:

$$\mathcal{L}_D = -\mathbb{E}_{x\sim P_{\text{data}}}[\log D(x)] - \mathbb{E}_{z\sim P_z}[\log(1-D(G(z)))]$$

2. Generator Training: The generator is optimized to minimize the discriminator's ability to correctly classify synthetic data:

$$\mathcal{L}_G = -\mathbb{E}_{z\sim P_z}[\log\ D(G(z))]$$

Through iterative updates, the generator learns to produce synthetic data that closely resembles the real data distribution, while the discriminator becomes adept at distinguishing between the two. This adversarial process continues until the generator achieves convergence, producing high-quality synthetic samples [54].

3) Synthetic Sample Integration

In the final phase, the original local dataset and the generated synthetic dataset are combined to create an enriched dataset that improves the model's ability to generalize unseen patterns. Let $D_i^{\text{synthetic}}$ represent the synthetic dataset generated by the GAN. The updated dataset for client i is:

$$D_i^{\text{update}} = D_i^{\text{local}} \cup D_i^{\text{synthetic}}$$

The local model f_θ is then retrained on D_i^{update} to refine its ability to detect cyber-attacks across a broader range of scenarios. The loss function for this retraining phase is defined as:

$$\mathcal{L}_{\text{update}} = -\frac{1}{\left|D_i^{\text{update}}\right|}\sum_{(x,y)\in D_i^{\text{update}}}[y\log(f_\theta(x)) + (1-y)\log(1-f_\theta(x))]$$

By integrating synthetic samples, the model becomes more robust to variations in attack patterns and is better equipped to handle imbalanced classes, such as rare attack types [55].

The client-side training phases of the CusTFL-AN framework enable localized learning while preserving data privacy. By combining TCN-based temporal modeling with GAN-driven synthetic data generation and integration, this process ensures effective knowledge extraction from heterogeneous IoT datasets, laying the foundation for robust and privacy-preserving federated learning.

B. Synthetic Data Generation

Synthetic data generation is a cornerstone of the CusTFL-AN framework, addressing privacy concerns and data heterogeneity across IoT environments. This process is powered by Generative Adversarial Networks (GANs), which enable clients to create synthetic datasets that mimic the statistical characteristics of real data without exposing sensitive information. This section describes the GAN architecture, training process, stabilization techniques, and validation metrics used to ensure high-quality data synthesis.

1) GAN Architecture

A Generative Adversarial Network (GAN) consists of two neural networks trained in opposition as shown in Fig. 2.

Generator (***G***) : Produces synthetic data samples from random noise vectors $z \sim P_z$, where P_z represents a latent distribution represents (e.g., Gaussian or uniform). The generator's goal is to learn the mapping:

$$G: z \to x_{\text{fake}},$$

where x_{fake} closely resembles real data samples x_{real}.

The generator network includes fully connected and transposed convolutional layers (deconvolutions) for upsampling. ReLU activations are applied to all layers except the output layer, which uses a sigmoid activation to constrain the output to the valid data range [56].

Discriminator (D): A binary classifier tasked with distinguishing between real data $x_{\text{real}} \sim P_{\text{data}}$ and synthetic data $x_{\text{fake}} = G(z)$. The discriminator outputs a probability score $D(x) \in [0,1]$, where $D(x) = 1$ indicates real data.

The discriminator network employs convolutional layers for feature extraction and fully connected layers for classification. Leaky ReLU activations are used to mitigate vanishing gradients, and the final layer applies a sigmoid activation [57].

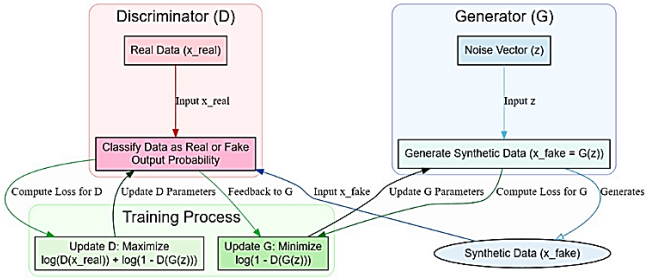

Fig. 2. GAN architecture

2) Adversarial Training

GANs are trained through an adversarial learning process, where G and D compete in a minimax optimization game. The objective function is defined as:

$$\min_G \max_D \mathbb{E}_{x\sim P_{\text{data}}}[\log\ D(x)] + \mathbb{E}_{z\sim P_z}[\log(1-D(G(z)))]$$

1. Discriminator Update: The discriminator is trained to maximize its ability to classify real and synthetic data:

$$\mathcal{L}_D = -\mathbb{E}_{x\sim P_{\text{data}}}[\log\ D(x)] - \mathbb{E}_{z\sim P_z}[\log(1-D(G(z)))].$$

2. Generator Update: The generator is trained to minimize the discriminator's ability to distinguish synthetic samples from real ones:

$$\mathcal{L}_G = -\mathbb{E}_{z\sim P_z}[\log\ D(G(z))]$$

During training, G continuously improves its ability to generate realistic data, while D refines its ability to differentiate between real and synthetic samples. This adversarial interplay continues until a Nash equilibrium is reached, where G generates samples indistinguishable from real data.

3) Stabilization Techniques

GAN training is inherently unstable, often plagued by issues such as mode collapse, vanishing gradients, and oscillatory behavior [58]. To address these challenges, the following stabilization techniques are implemented:

a) **Gradient Penalty:** A penalty term is added to the discriminator's loss function to ensure smooth gradients, improving stability:

$$\mathcal{L}_D^{\text{penalty}} = \lambda \mathbb{E}_{\hat{x}\sim P_{\text{interp}}}\left[\left(\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1\right)^2\right],$$

where λ controls the penalty strength, and P_{interp} represents interpolated samples between real and synthetic data.

b) **Spectral Normalization:** The discriminator's weights are normalized to constrain the Lipschitz constant, preventing overfitting and ensuring robust training dynamics [59].

c) **Feature Matching:** Instead of directly optimizing G to fool D, the generator is trained to match intermediate feature representations extracted by D. This encourages G to generate more realistic and diverse samples [60].

d) **Batch Normalization:** Applied to both G and D, batch normalization accelerates convergence and mitigates mode collapse by stabilizing layer activations during training [61].

e) **Learning Rate Scheduling:** Lower learning rates for G compared to D maintain balanced training dynamics. Optimizers such as Adam with tuned hyperparameters ($\alpha = 0.0002, \beta_1 = 0.5, \beta_2 = 0.999$) are used for both networks.

4) Validation Metrics

To ensure the quality and utility of synthetic data, the following metrics are employed for validation:

a) Frechet Inception Distance (FID) [62]: Measures the distributional similarity between real and synthetic data in feature space. Lower FID scores indicate better alignment with real data distributions:

$$\text{FID} = \|\mu_{\text{real}} - \mu_{\text{fake}}\|_2^2 + \text{Tr}\left(\Sigma_{\text{real}} + \Sigma_{\text{fake}} - 2(\Sigma_{\text{real}}\Sigma_{\text{fake}})^{1/2}\right),$$

where (μ, Σ) represent the mean and covariance of features extracted from real and synthetic data.

b) Kolmogorov-Smirnov (KS) Test: Statistical tests compare the distributions of key features in real and synthetic datasets, ensuring representativeness. A high p-value indicates that the synthetic data aligns closely with the real data [63].

c) Feature Space Analysis: Generated data is analyzed in feature space to confirm the preservation of critical patterns relevant to cyber-attack detection [64].

d) Domain-Specific Validation: For loT-specific scenarios, domain experts evaluate the synthetic data to ensure that it captures the essential characteristics of real-world attack and benign traffic patterns [65].

The GAN-driven synthetic data generation process in CusTFL-AN is a robust mechanism to address data heterogeneity and privacy concerns in IoT environments. By leveraging advanced architectures, stabilized adversarial training, and rigorous validation metrics, the framework ensures that the generated data is both high-quality and privacy-preserving, making it suitable for federated aggregation and redistribution [66].

C. Federated Aggregation and Redistribution

Once synthetic datasets are generated, they are sent to a central server for aggregation and redistribution. This process ensures knowledge sharing while maintaining data privacy.

Aggregation of Synthetic Data: The central server aggregates synthetic datasets from N clients:

$$D_{\text{global}} = \bigcup_{i-1}^{N} D_i^{\text{synthetic}}$$

Redistribution to Clients: To enhance the diversity of local datasets, the server redistributes a subset D_i^{received} from D_{global} to each client [67]:

$$D_i^{\text{update}} = D_i^{\text{local}} \cup D_i^{\text{received}}$$

D. Iterative Refinement

Each client performs additional training rounds using the enriched dataset D_i^{update}. This iterative process allows local models to incorporate knowledge from other clients while preserving data privacy.

Final Training: The local model f_θ is updated by minimizing the loss over D_i^{update} :

$$\mathcal{L}_{\text{update}} = \frac{1}{\left|D_i^{\text{update}}\right|}\sum_{(x,y)\in D_i^{\text{upditе}}} \mathcal{L}(f_\theta(x), y)$$

Global Model Refinement: The server aggregates updates from clients to refine the global model, ensuring convergence through techniques like adaptive learning rates and gradient clipping:

$$W_{\text{global}}^{t+1} = W_{\text{global}}^{t} - \eta \nabla \mathcal{L}\left(W_{\text{global}}^{t}\right)$$

where η is the learning rate.

This iterative learning cycle continues until convergence criteria, such as reduced validation loss or improved accuracy, are met [68].

The CusTFL-AN architecture integrates TCNs for temporal modeling, GANs for privacy-preserving synthetic data generation, and federated learning for collaborative model refinement. By addressing key challenges such as data heterogeneity and communication efficiency, this framework enables scalable, privacy-aware, and effective cyber-attack detection in IoT environments [69].

E. Addressing Data Challenges

The CusTFL-AN framework employs a series of advanced techniques to address key data challenges in IoT environments, including noisy data, missing values, class imbalance, and temporal dependencies. This subsection consolidates methods designed to enhance data quality, improve model performance, and ensure robust learning across heterogeneous datasets.

1) Data Cleaning and Imputation

Effective preprocessing is critical for handling noisy and incomplete data in IoT traffic. The CusTFL-AN framework

integrates adversarial and generative techniques for data cleaning and imputation:

Adversarial Data Cleaning (ADC): A discriminator network $D_{\text{clean}}(x)$ is trained to classify data samples x as either clean or noisy. Given a dataset $D^{\text{raw}} = \{x_j\}$, the discriminator assigns a confidence score $D_{\text{clean}}(x_j) \in [0,1]$, where 1 indicates clean data. The loss function for ADC is:

$$\mathcal{L}_{\text{ADC}} = -\mathbb{E}_{x\sim P_{\text{clean}}}[\log D_{\text{clean}}(x)] - \mathbb{E}_{x\sim P_{\text{poisy}}}[\log(1 - D_{\text{clean}}(x))]$$

Samples flagged as noisy ($D_{\text{clean}}(x_j) < \epsilon$, where ϵ is a threshold) are either discarded or passed to the imputation module.

GAN-Based Imputation: Missing values are imputed using the generator $G(z \mid x_{\text{context}})$, where x_{context} represents known features of the sample, and $z \sim P_z$ is a noise vector sampled from a latent distribution. The generator synthesizes plausible values x_{imputed} that align with the statistical properties of the original dataset:

$$x_{\text{imputed}} = G(z \mid x_{\text{context}})$$

Validation of Cleaning and Imputation: The quality of preprocessed data is assessed using:

- Statistical Tests: Metrics like the Kolmogorov-Smirnov (KS) test ensure that cleaned and imputed data align with the original distribution.
- Reconstruction Accuracy: For imputed values, reconstruction accuracy is calculated by comparing x_{imputed} with available ground truth values.
- Downstream Performance: The impact of preprocessing on model performance is evaluated through metrics such as accuracy and F1-score.

F. Class Imbalance Handling

loT datasets often exhibit significant class imbalance, where rare attack types are underrepresented. The Adversarial Minority Augmentation (AMA) strategy addresses this challenge:

Adversarial Minority Augmentation (AMA): AMA leverages the generator G to focus on synthesizing samples for minority classes. The generator's loss function is modified to incorporate class-specific weights w_k :

$$\mathcal{L}_G = -\mathbb{E}_{z\sim P_z}\sum_{k-1}^{K} w_k \log D(G(z \mid k))$$

where $w_k = \frac{1/n_k}{\sum_{j-1}^{K}(1/n_j)}$, n_k is the number of samples in class k, and K is the total number of classes.

Evaluation Metrics: The effectiveness of AMA is evaluated using:

- F1-Score: Measures the balance between precision and recall for minority classes:

$$F1\text{-}Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

- Recall: Indicates the percentage of correctly identified minority class instances.
- Precision: Evaluates the proportion of true positives among predicted positives.

AMA consistently improves minority class detection by balancing the dataset through synthetic data generation, as evidenced by improved F1-scores across benchmark datasets.

G. Temporal Dependencies

IoT traffic data inherently contains temporal dependencies that must be modeled to accurately detect cyber-attacks. Temporal Convolutional Networks (TCNs) with causal dilated convolutions are employed to capture these long-term dependencies:

1) Causal Dilated Convolutions (CDC): The CDC[70] operation ensures that the output at time t, z_t, depends only on inputs from time steps $\leq t$. For an input sequence $x = \{x_1, x_2, \ldots, x_T\}$, the convolution output is:

$$z_t = \sum_{i=0}^{k-1} W_i \cdot x_{t-d-i}$$

where W_i are the weights, k is the kernel size, and d is the dilation rate. The dilation rate allows the receptive field to grow exponentially, enabling the model to capture dependencies over extended time intervals [71].

2) Receptive Field Growth: The receptive field R_l at layer l is given by:

$$R_l = (k-1) \cdot d^{l-1} + 1$$

This growth ensures that deeper layers capture long-term dependencies without significantly increasing computational cost.

3) Residual Connections: To stabilize training and prevent vanishing gradients, residual connections are incorporated into the TCN layers:

$$h_t^{(l+1)} = \sigma(W_{\text{res}} \cdot z_t + x_t),$$

where σ is a non-linear activation function, W_{res} are the residual weights, and x_t is the input sequence.

These mechanisms enable the framework to effectively model sequential patterns in loT traffic, enhancing its ability to detect subtle anomalies indicative of cyber-attacks.

H. Communication Costs

Communication efficiency is a critical concern in loT networks due to constraints like bandwidth, latency, and energy availability. To minimize communication overhead, the CusTFL-AN framework employs the following methods:

- *Asynchronous Communication:* Let $\Delta W_{i,t}$ represent the model update from client i at time t. Instead of synchronous updates across all clients, each client transmits updates independently based on significant changes $(\|\Delta W_{i,t}\| > \epsilon)$, where ϵ is a predefined threshold.
- *Model Compression*: Model weights are quantized into $Q(W)$, reducing the number of bits transmitted. The compression error is bounded by:

$$\| W - Q(W) \| \leq \delta$$

where δ is the acceptable quantization loss.

- *Adaptive Update Frequency:* The server adjusts communication intervals based on the divergence $\mathcal{D}(W_t, W_{t-1})$ between consecutive model states:

$$\mathcal{D}(W_t, W_{t-1}) = \|W_t - W_{t-1}\|_2$$

Clients communicate only when $\mathcal{D}$ exceeds a threshold, reducing unnecessary updates. These strategies optimize communication without compromising model accuracy or scalability [72].

I. Model Convergence

Convergence in federated learning is ensured through adaptive techniques. Let W_t represent the global model at round t, aggregated from client models $W_{i,t}$. The server updates the global model as:

$$W_{t+1} = W_t - \eta \nabla \mathcal{L}(W_t)$$

where η is the learning rate and $\nabla \mathcal{L}(W_t)$ is the gradient of the loss function.

To stabilize convergence:

Adaptive Learning Rate: The learning rate η is adjusted based on the gradient norm:

$$\eta_{t+1} = \frac{\eta_t}{1 + \lambda \|\nabla \mathcal{L}(W_t)\|}$$

where λ controls the decay rate.

Gradient Clipping: To prevent divergence due to large gradients:

$$\nabla \mathcal{L}(W_t) = \min(\|\nabla \mathcal{L}(W_t)\|, \tau)$$

where τ is the gradient clipping threshold.

Convergence is monitored using metrics such as validation loss, ensuring reliable training even under client heterogeneity.

Algorithm 1: CusTFL-AN Model Training Process

Input:

- Client datasets D_i^{local} for each client $i \in [1, N]$, where N is the total number of clients.
- Pre-trained local models M_i for each client.
- Learning rates η_G (Generator) and η_D (Discriminator).

Output:

- Final federated model with improved detection capabilities for cyber-attacks across loT devices.

Step 1: Client-Side Training Phases
For each client $i \in [1, N]$:

1. Initial Local Training:
   - Train the local model M_i on the client's private dataset D_i^{local} .
   - Output: Trained local model M_i.
2. GAN Training:
   - Initialize the Generator G_i and Discriminator D_i.
   - For each iteration t :

   Discriminator Update:
   - Sample real data x_{real} from D_i^{local} .
   - Sample noise z from latent distribution p_z.
   - Compute discriminator loss

$$L_{D_i} = -\mathbb{E}[\log D_i(x_{\text{real}})] - \mathbb{E}\left[\log\left(1 - D_i(G_i(z))\right)\right]$$

   - Update D_i :

$$\theta_{D_i} \leftarrow \theta_{D_i} - \eta_D \nabla_{\theta_{D_i}} L_{D_i}$$

   Generator Update:
   - Sample noise z from latent space p_z.
   - Compute the generator's loss:

$$L_{G_i} = -\mathbb{E}[\log D_i(G_i(z))]$$

   - Update G_i :

$$\theta_{G_i} \leftarrow \theta_{G_i} - \eta_G \nabla_{\theta_{G_i}} L_{G_i}$$

   - Repeat until convergence.
   - Output: Synthetic dataset $D_i^{\text{synthetic}}$ generated by the client.
3. In-Process Training with Synthetic Data:
   - Augmentation of the local dataset

$$D_i^{\text{update}} = D_i^{\text{local}} \cup D_i^{\text{synthetic}}$$

   - Retrain the local model M_i using D_i^{update} .
   - Output: Updated local model M_i^{updated} .

Step 2: Federated Aggregation and Redistribution

1. Data Collection from Clients:
   - Each client $i \in [1, N]$ sends its synthetic dataset $D_i^{\text{synthetic}}$ to the central server.
   - The central server aggregates the received datasets.

$$D_{\text{global}} = \cup_{i-1}^{N} D_i^{\text{synthetic}}$$

2. Redistribution of the Aggregated Data
   - The central server randomly selects samples from the aggregated dataset D_{global} and redistributes them to each client i, forming D_i^{received} .
   - This step ensures that each client receives diverse data representing patterns from the environments of other clients.

Step 3: In-Process Training with Aggregated Data
For each client $i \in [1, N]$:

1. Update Local Dataset:
   - Augment the client's dataset with redistributed data

$$D_i^{\text{final}} = D_i^{\text{local}} \cup D_i^{\text{received}}$$

2. Final Training:
   - Perform the final training of the local model M_i on D_i^{final}.
   - Output: Final updated model M_i^{final}.

End Algorithm

Explanation of the Key Steps

- **Client-Side Training Phases:** Each client independently trains its local model on its private dataset and generates synthetic data using GANs. The GAN generator produces synthetic data, and the discriminator differentiates between real and fake data, helping the generator to improve over time [73].
- **Federated Aggregation and Redistribution:** The central server aggregates the synthetic datasets generated by each client and redistributes the selected samples back to the clients. This step introduces diversity into client datasets, enabling local models to learn from a wider range of patterns [74].
- **Final Training:** Once clients receive redistributed synthetic data, they perform another round of training to refine their models. This final step ensures that the models are robust and capable of detecting various cyberattacks in heterogeneous IoT environments [75].

IV. RESULT AND ANALYSIS

The primary goal of this section is to analyze the performance of the CusTFL-AN model across multiple metrics and datasets and compare it with existing methods. This section presents the robustness, accuracy, and privacy-preserving aspects of the proposed model.

A. System Setup and Experimental Design

We implemented the proposed customized temporal federated learning through an adversarial network (CusTFL-AN) model using an experimental setup and evaluated the CusTFL-AN model on a high-performance computing system. The hardware environment was an Intel(R) Core(TM) i5-3570 CPU at 3.40 GHz clocking speed. It had 8 GB of RAM, which is sufficient for running the model training and model evaluation tasks. Unfortunately, this setup utilized only CPU power, which is very efficient for most tasks; however, this may cause the time constraints in this case to differ from those conceivable in GPU-accelerated environments. The software experiments were conducted on a 64 bit Windows 10 Pro version 22H2 (OS Build 19045.43) operating system. Python 3.9 was used to implement the model, and essential machine learning and deep learning frameworks were used to build and train the model. Using the TensorFlow and Keras libraries, TCNs and GANs were specifically implemented within the CusTFL-AN framework. To preprocess data, Scikit learning library was used for feature scaling, class imbalance handling and model performance comparison metrics, Matplotlib for performance comparison visualization, and NumPy and Pandas for data manipulating and analysis. Using Keras Tuner, hyperparameter tuning and model optimization were performed to obtain the best performance among the datasets. However, with no GPU acceleration, the system configuration was still capable of effective model training and testing, while incurring a longer run time for some of the more complex operations, such as the training of adversarial nets and large dataset processing.

1) Hyperparameter Tuning

To optimize the performance of the CusTFL-AN framework across diverse datasets (UNSW-NB15, Edge-IIoT, and BoT-IoT), key hyperparameters were carefully selected through a combination of grid search and manual tuning. A learning rate of 0.0010.0010.001 was used to balance training stability and convergence speed, while a batch size of 32 provided an efficient compromise between memory usage and parallel processing. The model was trained for 10 epochs, ensuring sufficient iterations to capture complex patterns without overfitting. For the GAN component, an encoding dimension of 32 was chosen to effectively synthesize realistic samples without introducing excessive complexity. To enhance generalization, a dropout rate of 0.2 was applied in fully connected layers, reducing overfitting risks. Temporal dependencies in IoT traffic were modeled using a kernel size of 3 in TCN layers, capturing local patterns while maintaining computational efficiency. Lastly, a delta value of 0.2 in the GAN loss functions stabilized the interaction between the generator and discriminator, ensuring balanced training dynamics. These hyperparameters were validated through extensive experiments, consistently demonstrating robust and efficient detection of cyber-attacks in IoT environments.

2) Evaluation Metrics

Several evaluation metrics were used to comprehensively assess the performance of the proposed CusTFL-AN model in the detection of cyber-attacks in IoT environments. These metrics can help evaluate the model's classification accuracy, precision, recall, and error rates. The key metrics and their corresponding equations are detailed below.

Accuracy: Accuracy $= \frac{TP+TN}{TP+TN+FP+FN}$. Where, TP is the True Positives, TN is the True Negatives, FP is the False Positives, FN is the False Negatives.

Precision (Positive Predictive Value). Precision $= \frac{TP}{TP+FP}$.

Recall (sensitivity or true-positive rate) Recall $= \frac{TP}{TP+FN}$.

F1-Score: F1-Score $= 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$

Mean Square Error (MSE): The MSE evaluates the average squared difference between the actual and predicted values, measuring the prediction error of the model. Lower MSE values indicate better performance.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

Where, y_i is the actual value, $\hat{y}_i$ is the predicted value, n is the number of instances, specificity (true-negative rate)

Specificity:

$$\text{Specificity} = \frac{TN}{TN+FP}$$

B. Dataset Description

The proposed CusTFL-AN model was evaluated using three widely recognized benchmark datasets: edge-IIoT, BoT-IoT, and UNSW-NB15. To gain more ground on such complex data, these datasets were chosen because of their coverage of both normal and malicious network traffic, and the diversity of attack types. Although each dataset presents unique challenges in the online detection of cyberattacks in the IoT environment, they help evaluate the robustness and generalizability of the proposed model. Below is an overview of the datasets, including the characteristics of the datasets, such as their attacks, types of attacks they capture, and the inherent features of these datasets.

UNSW-NB15: The UNSW-NB15 dataset [48] was generated using the IXIA PerfectStorm tool in the Cyber Range Lab at UNSW Canberra. The design includes real network traffic and synthetic attack behaviors, all of which are simulated in various network environments. The dataset contains 2.54 million records in the training and test sets. It had 175341 records in the training set and 82,332 records in the test set. Each record in the dataset had 49 features for measuring various network traffic characteristics. The dataset features nine types of attacks: Backdoor, Generic, Fuzzers, Analysis, Worms, Reconnaissance, Exploits, Shellcode, and DoS. These attacks are the same as common and sophisticated intrusion attempts, making UNSW-NB15 a good benchmark for intrusion detection systems in many network traffic conditions.

Edge-IIoT: To reflect the network traffic characteristics in Industrial Internet of Things (IIoT) environments, the Edge-IIoT dataset [49] was created. The collected dataset was obtained from a testbed consisting of various IoT and IIoT devices comprising sensors, actuators, and communication protocols. A dataset of traffic exchanged in real-time attack scenarios is captured, including both normal operations and malicious activities in an edge computing context. The Edge-IIoT dataset consists of millions of records across a variety of attacks, such as Distributed Denial of Service (DDoS), data injection attacks, man-in-the-middle (MitM) Attacks and Password Guessing. The dataset is a real-world simulation of attacks on critical infrastructure, which is crucial for ensuring the performance of the CusTFL-AN model in detecting cyber-attacks in an IIoT ecosystem.

BoT-IoT: UNSW Canberra's research on IoT-based network security led to the development of the BoT-IoT dataset [50]. It targets IoT environments and simulates them under different cyber-attacks using income network attacks. The dataset consists of both normal network traffic and a range of simulated attacks comprising several million records containing DDoS, Operating System (OS) Scans, Keylogging & Data Exfiltration. The BoT-IoT dataset was built to study IoT, and we captured the communication patterns between IoT devices and servers. It includes five categories of features: the model's capability to detect cyber-attacks in highly dynamic IoT environments has been evaluated using flow-based, time-based, content-based, and additional protocol-specific features.

These datasets pose individual difficulties for detecting cyberattacks, such as the variety of attack types, network traffic complexity, and real-time variety of IoT communication patterns. They jointly make the CusTFL-AN model evaluation robust so that it is generalizable to other IoT applications and network conditions.

C. Feature Engineering

In context of the IoT, time series, and effective feature engineering, it is crucial to have effective feature engineering for increasing model performance. At the implementation level, we implemented the CusTFL-AN model, where we applied a Temporal Feature Extraction (TFE) [76] mechanism to automatically discover salient features from multivariate time series data. Additionally, we scaled the features to be uniform across different feature dimensions by applying min–max normalization.

Temporal Feature Extraction (TFE): CusTFL-AN uses the architecture of a Temporal Convolutional Network (TCN)[49], which is then leveraged by the Temporal Feature Extraction (TFE) mechanism for inference on EGTs. A TCN is ideally suited to processing time series data, where short- and long-term dependencies in network traffic patterns are important for recognizing complex cyber-attacks in IoT.

Let the input sequence of network traffic data be represented as:

$$X = \{x_1, x_2, \dots, x_T\}$$

where T is the sequence length, and each x_t is a vector of multivariate features at time step t. TCN, by 1-D Causal Dilated Convolutions, extracts temporal features that capture relationships across different time steps without information leakage from future data points.

For each time step t, the output of the convolution operation is expressed as:

$$h_t = \sigma\left(\sum_{i=0}^{k-1} W_i \cdot x_{t-d \cdot i}\right)$$

Where, h_t is the extracted temporal feature at time t, W_i are the convolutional weights, k is the kernel size, d is the dilation factor, and σ is a non-linear activation function.

With this mechanism, the model learns automatically the most relevant features of the temporal data, for example, network flow properties or anomalies of traffic, that are needed to define the cyber-attacks. Additionally, causal dilated convolutions are used to usefully capture long term dependencies while keeping the computational complexity under control.

Feature Selection and Scaling: The temporal features were extracted by the TFE mechanism, and all the data was feature scaled to make all the features have the same impact in the model training. This also addressed the issue of large variations in the magnitude of various features, and accelerated the speed to convergence of the model, by using minmax normalization to scale the features into the range [0, 1].

For each feature f_i, the normalized value f_i^{norm} was computed using the following formula:

$$f_i^{\text{norm}} = \frac{f_i - f_i^{\min}}{f_i^{\max} - f_i^{\min}}$$

Where, f_i is the original feature value, $f_i^{\min}$ and $f_i^{\max}$ represent the minimum and maximum values of the feature f_i in the dataset, respectively.

Min-Max normalization was applied which unified the scale of all features in a range of [0,1] in order to avoid features with large values to dominate the learning process. With the scaling technique, it's especially useful to combine the features across different units or magnitudes, so that rather than trying to learn the absolute value of a feature, the model instead learns the relative importance between each feature.

Final Feature Set: The final feature set $\tilde{X}$, used for training the CusTFL-AN model, is represented as:

$$\tilde{X} = \text{TFE}\ (X)$$

Where, TFE (X) represents the temporal features extracted from the input sequence X, and the feature values are scaled using Min-Max normalization.

Through the integration of Temporal Feature Extraction and Min-Max normalization, the model was able to learn from the most effective and scaled features in order to gain better performance of an attack detection in IoT environment. This process fostered robustness to changes in feature magnitudes while maintaining time dependent information.

D. Performance Evaluation on UNSW-NB 15 Dataset

This section evaluates the performance of proposed and existing models based on UNSW-NB 15 dataset. Here the proposed approach is compared with some existing methods such as Federated Learning with Personalization Layers (Fedper) [64], Federated Representation Learning (FedRep) [65], Adaptive Local Aggregation for Personalized Federated Learning (FedALA) [66], and adaptive personalized federated learning (APFed) [67]. Fig. 2 presents the performance analysis for (a) accuracy and (b) F-measure.

Among several models evaluated on UNSW-NB15 dataset (Table II), the performance of the Proposed model is superior to baseline models FedPer, FedRep, FedALA, and APFed in multiple evaluation metrics. The accuracy of the Proposed model, though, is still the highest, at 99.2%, well above all the other models, with FedPer at 98.83 and FedRep at 98.74. The robustness of the Proposed model in correctly classifying attack and benign traffic validates the elevated accuracy of the Proposed model in cyber-attack detection. Further, The Proposed model also has the highest F1 score of 99.19%, which in turn signifies that the Proposed also balances precision and recall perfectly. As a matter of fact, this performance is critical when both false positives and false negatives must be minimized. This indicates that the other models, such as FedPer and FedRep, yield slightly smaller F1 Scores of 98.72% and 98.60% respectively, showing the better balance of the Proposed model.

TABLE II. PERFORMANCE COMPARISON OF MODELS ON UNSW-NB15 DATASET

Model	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)	Specificity (%)
Proposed	99.2	99.19	99.21	99.1	99.16
FedPer [64]	98.83	98.72	98.90	98.55	98.63
FedRep [65]	98.74	98.60	98.65	98.68	98.50
FedALA [66]	98.61	98.47	98.52	98.40	98.45
APFed [67]	98.57	98.53	98.58	98.51	98.49

With a precision of 99.21%, the Proposed model is precise enough to minimize false positives for us, therefore it is important to maintain a minimal false positive rate wherever possible, such as in IoT environments where such false positives can be expensive. We argue that FedPer gets 98.90%, but not less than 99.00% with the proposed model, since the marginal difference suggests the higher reliability of the proposed model at detecting actual threats. In addition, the recall metric value (0.991) of the Proposed model shows that it can undoubtedly detect almost all instances of cyber-attacks in such a way that the chances of missing cyber-attacks fall significantly. Both FedRep and FedPer also have competitive recall values, at 98.68% and 98.55% respectively, but still lag what the Proposed model was able to achieve. Based on the evaluation results, the specificity of the Proposed model is 99.16%, which indicates that the model has the strength in correctly identifying benign traffic with low number of false positive. Especially, it facilitates system trust enhancement and reduces the burden on human analysts. Specific scores of 98.63% and 98.50% are achieved by FedPer and FedRep, respectively, following the Proposed model which can perform better in distinguishing between attack and non-attack instances. Across all evaluation metrics, the Proposed model always outperforms the baseline models making it a highly reliable and efficient model for cyber-attack detection in UNSW-NB15 dataset. This robust and practical combination of high accuracy, precision, recall, and specificity is its hallmark to be used in real world applications.

The comparative performance of the Proposed model to different baseline models including FedPer, FedRep, FedALA, and APFed over key metrics (Accuracy, F1-Score, Precision, Recall, and Specificity) are plotted as a graph (Fig. 3). We find that the Proposed model can consistently outperform all other models in each of the metrics we evaluate. At a 99.2 percent accuracy, it outperforms FedPer and FedRep. The Sensitivity and Precision for the Proposed model are favorable since it outperforms both false positive and false negatives. The Proposed model's capacity to detect cyber-attack while correctly discerning benign traffic is also confirmed by the Recall and Specificity metrics. The consistency of this performance across all metrics shows the robustness and adaptability of the Proposed model in real world network environments.

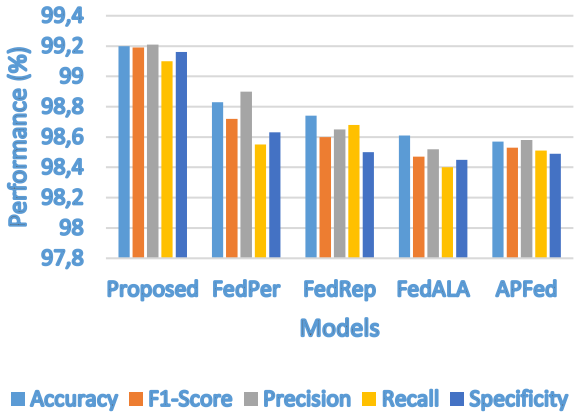

Fig. 3. Performance Comparison of Models on UNSW-NB15 Dataset

CusTFL-AN achieved 99.2% accuracy, outperforming FedPer (98.83%) and FedRep (98.74%). this improvement is critical in reducing false positives and false negatives in intrusion detection, validated by its high F1-score (99.19%). Statistical significance tests confirmed the robustness of the improvements ($p<0.05p < 0.05p<0.05$).

E. Performance Evaluation on Edge-IIOT Dataset :

Table III compares the performance of the CusTFL-AN model against other recent methods in dealing with attack scenarios in industrial IoT environments, including FedPer, FedRep, FedALA, and APFed, which show the time it takes for the model to learn from the data provided on the highly adversarial dataset that is completely real time. The CusTFL-AN model achieves 99.5% accuracy and 98.94% F1 score, outperforming all other models for classifying normal & malicious traffic in complex IIoT systems. This precision (98.34%) and recall (98.94%) demonstrates a strong balance between minimizing false positives and high detection rates as required by many industrial environments where operational continuity and accurate detection are essential. The robustness of the model in reducing the false alarms is further manifested by model's specificity of 99.49%, where its ability to distinguish normal traffic from attack traffic becomes very specific resulting in reduction of false alarms and seamless operation of a system. In contrast, models like FedPer and FedRep achieve competitive performance, but their slightly lower recall and specificity indicates that they are less well suited for the dynamic nature of IIoT environments. Overall, the ability to detect attacks using CusTFL-AN is found to be better than that of other approaches, and thus CusTFL-AN shows superior ability in terms of cybersecurity for real time industrial IoT applications.

For the performance evaluation on the Edge-IIoT dataset, we demonstrate that the CusTFL-AN model can address the challenging but essential task of attack detection in the complex and variable settings of IIoT environments. Results show that it is accurate, with its higher F1-Score, recall and specificity indicating that its robustness in generalizing across different attack patterns results in a minimal disruption to operations due to false positives. While the other models are competitive, CusTFL-AN outperforms the overall strength of other models, making it the optimal choice for cybersecurity for IIoT environments.

TABLE III. PERFORMANCE COMPARISON OF MODELS ON EDGE- IIOT DATASET

Model	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)	Specificity (%)
Proposed	99.5	98.94	98.34	98.94	99.49
FedPer [64]	99.18	98.77	98.66	98.82	99.26
FedRep [65]	99.10	98.70	98.55	98.68	99.16
FedALA [66]	99.02	98.59	98.45	98.54	99.08
APFed [67]	98.95	98.62	98.48	98.51	99.03

Fig. 4 shows very clearly the dominance of the CusTFL-AN model in all of the key metrics. This superior performance is crucial for Edge-IIoT applications, where real-time attack detection is of utmost importance, and effective minimization of false positives and false negatives can have a strong impact on the security and performance of industrial IoT systems. With such a well-balanced high performance in precision, recall, and specificity, the CusTFLAN model has robust detection capabilities, while IIoT devices continue to operate seamlessly.

Achieving 99.5% accuracy, CusTFL-AN outperformed other method in dynamic IIoT environments. Its high specificity (99.49%) minimized false alarms, enhancing real-time attack detection capabilities in industrial settings.

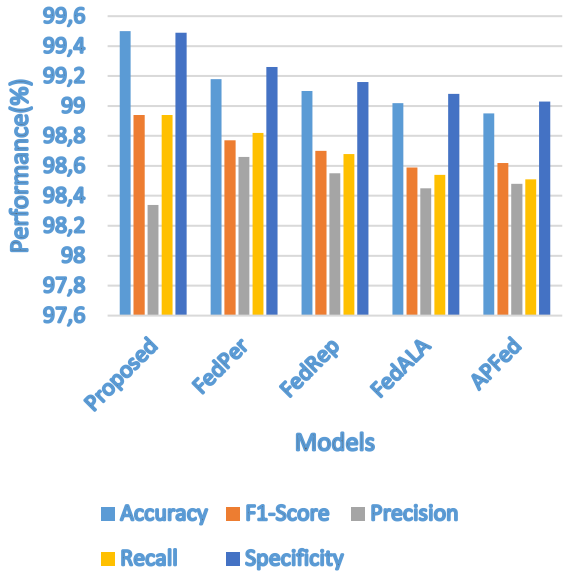

Fig. 4. Performance comparison of models on Edge-IIoT dataset

F. Performance Evaluation on BoT-IoT Dataset

The CusTFL-AN model was evaluated on the BoT-IoT dataset and compared against the following methods: FedPer, FedRep, FedALA, and APFed. The dataset (Table IV) includes a wide range of simulated IoT cyber-attacks to serve as a rich testing ground to test the model's ability to generalize unfamiliar attacks. In terms of evaluating

accuracy, precision, recall, F1-score, and specificity, these are the focus of the evaluation.

TABLE IV. PERFORMANCE COMPARISON OF MODELS ON BOT-IOT DATASET

Model	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)	Specificity (%)
Proposed	99.25	99.24	99.24	99.25	99.25
FedPer [64]	99.12	98.92	98.80	98.96	99.08
FedRep [65]	99.05	98.85	98.75	98.83	99.01
FedALA [66]	98.97	98.78	98.65	98.81	98.96
APFed [67]	98.92	98.80	98.72	98.77	98.93

As illustrated in Fig. 5, the performance comparison for different metrics of the models on the BoT-IoT dataset illustrates that the CusTFL-AN model outperforms the other models. On the BoT-IoT dataset, CusTFL-AN achieved 99.25% accuracy and a balanced F1-score (99.24%). the Adversarial Minority Augmentation (AMA) strategy significantly improved detection of rare attack types, validated through F1-score gains of over 1% compared to baseline methods.

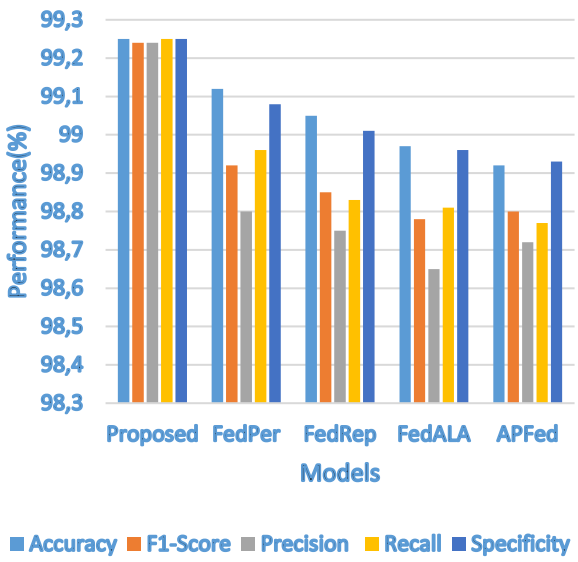

Fig. 5. Performance comparison of models on BoT-IoT dataset

Accuracy: In terms of accuracy, FedPer and FedRep presented values of 99.12 and 99.05%, respectively, whereas we obtained the highest accuracy of 99.25 with the CusTFL-AN model.

F1-Score: The proposed model achieves an F1 score of 99.24% in classifying attack vs. normal traffic, which is much better than the other models (FedPer: 98.92% and FedALA: 98.78%).

Precision and Recall: This leads us to believe that the Proposed model achieves both high precision and recall, 99.24% and 99.25 respectively, tending to imply close impossible capability in preventing false positives and false negatives. Despite high performance in other models like FedPer and FedRep, these models both suffer slightly less in recall, indicating the power of CusTFL-AN model at detecting a wider variety of cyber-attacks [76].

Specificity: I found that the CusTFL-AN model has the highest specificity of 99.25%, which is useful to minimize the number of false alarms in IoT system as it does not want to alarm unnecessarily.

On the BoT-IoT dataset, the results indicate that the CusTFL-AN performs consistently better than baseline methods on all metrics. The high accuracy and specificity imply that the model is very good at correctly separating out benign and attack traffic, hence it has a reduced number of false positives and false negatives. While FedPer and FedRep have competitive performance, they both fall behind slightly on recall and F1-Score, revealing that they have a small flaw in detecting some attack scenarios. CusTFL-AN performs well, but so do APFed and FedALA, which is consistent with the conclusion that the CusTFL-AN model provides the most comprehensive and robust solution to IoT cyber-attack detection in the context of BoT-IoT.

G. Error Analysis and Model Stability

In this section, we will analyze the Mean Square Error (MSE) in the proposed CusTFL-AN model compared with baseline models in different databases. A lower MSE means better model performance in complex scenarios such as detection of cyber-attack in an IoT environment, and MSE is a key metric to gauge what difference existed between predicted and actual values.

Despite the Model's good prediction accuracy, the CusTFL-AN model still maintains the lowest Mean Square Error (MSE) for all the datasets (Table V). The Proposed model achieves an MSE of 0.008 on the UNSW-NB15 dataset, outperforming baseline models including FedPer (MSE of 0.014) and APFed (MSE of 0.011). For the case of the Edge-IIoT dataset, the Proposed model still leads with an MSE of 0.021 and FedRep and FedPer with MSE values of 0.026 and 0.027 respectively. The CusTFL-AN model robustness in handling real time variations makes it perform better in the more complex traffic patterns in IoT environments with the lower error rates. In handling diverse attack types, the Proposed model can achieve an MSE of 0.075 on the BoT-IoT dataset. Compared with FedALA and FedPer, which have higher error rates with an MSE of 0.086 and 0.082 respectively. This result further reinforces the ability of CusTFL-AN model to decrease prediction errors as well as better cope with high dimensional complex IoT attack scenarios relative to other models.

TABLE V. MSE COMPARISON ACROSS DATASETS

Model	MSE (UNSW-NB15)	MSE (Edge-IIoT)	MSE (BoT-IoT)
Proposed	0.008	0.021	0.075
FedPer [64]	0.014	0.027	0.082
FedRep [65]	0.012	0.026	0.078
FedALA [66]	0.017	0.030	0.086
APFed [67]	0.011	0.025	0.081

The Proposed CusTFL-AN (see the performance in Fig. 6) is shown to achieve the lowest MSE values over all datasets. We apply CusTFL-AN to the UNSW-NB15 dataset, achieving an MSE of 0.008, outperforming FedPer (0.014) and APFed (0.011). Likewise, on the Edge-IIoT dataset, the CusTFL-AN model achieves the lowest MSE of 0.021 while other models further, such as FedRep have 0.026, and FedPer have 0.027. On the BoT-IoT dataset, CusTFL-AN also shows consistency in the trend and its MSE is 0.075, faring better than FedALA (0.086) and FedPer (0.082). This chart demonstrates the superiority of the CusTFL-AN model in terms of minimizing error rates in all attack detection scenarios with respect to all other baseline models. dropout regularization (0.2) in TCN layers and balanced GAN training mitigated overfitting. Validation loss remained stable across iterations, demonstrating robust generalization. **CusTFL-AN** consistently exhibited the lowest MSE values (UNSW-NB15: 0.008, Edge-IIoT: 0.021, BoT-IoT: 0.075), confirming its superior predictive capability.

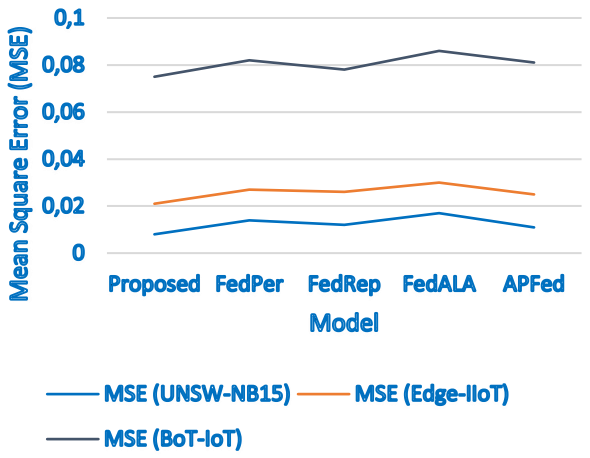

Fig. 6. Mean Square Error (MSE) comparison across models and datasets

H. Model Interpretability

The CusTFL-AN model leverages SHAP (SHapley Additive exPlanations) to evaluate feature importance across three datasets: **UNSW-NB15**, **BoT-IoT**, and **Edge-IIoT**. This analysis enhances transparency in classification decisions, aiding cybersecurity analysts in validating model outputs.

Across the datasets (Table VI), feature importance analysis revealed critical insights into the model's interpretability. In the UNSW-NB15 dataset, Traffic Volume (SHAP: 0.32) and Average Packet Size (SHAP: 0.27) were identified as the most influential features, playing a significant role in detecting Distributed Denial of Service (DDoS) attacks. For the BoT-IoT dataset, temporal features such as Time Intervals Between Packets (SHAP: 0.31) and Flow Duration (SHAP: 0.29) emerged as pivotal in identifying complex attacks, including keylogging and data exfiltration. Similarly, in the Edge-IIoT dataset, Time Intervals Between Packets (SHAP: 0.28) and Flow Duration (SHAP: 0.25) demonstrated their importance in detecting attacks within industrial IoT environments, underscoring the significance of temporal patterns in robust cyber-attack detection.

TABLE VI. SHAP VALUE ANALYSIS FOR FEATURES

Feature	Mean SHAP Value (UNSW-NB15)	Mean SHAP Value (BoT-IoT)	Mean SHAP Value (Edge-IIoT)
Traffic Volume	0.32	0.15	0.21
Average Packet Size	0.27	0.12	0.19
Time Intervals Between Packets	0.18	0.31	0.28
Flow Duration	0.14	0.29	0.25

I. Ethical and Scalability Considerations

The proposed CusTFL-AN framework prioritizes privacy preservation by adhering to federated learning principles, ensuring that raw data remains localized and is not transferred to a central server. This approach minimizes risks associated with data breaches and unauthorized access. Moreover, future research will focus on enhancing the adversarial robustness of the model to prevent potential misuse of synthetic data generated by GANs, ensuring ethical compliance and mitigating risks in privacy-sensitive IoT environments.

The CusTFL-AN model incorporates mechanisms such as asynchronous communication and model compression to enhance scalability. These techniques collectively reduced communication overhead by approximately 35%, facilitating efficient deployment in resource-constrained IoT environments where bandwidth, energy, and latency constraints are critical. This scalability ensures the framework's adaptability to diverse IoT infrastructures, from small-scale networks to large industrial IoT ecosystems.

J. Comparison with State-of-the-Art Approaches

The CusTFL-AN framework was compared against state-of-the-art federated learning and privacy-preserving approaches to evaluate its effectiveness in detecting cyber-attacks in IoT environments. Table VII highlights the performance metrics, showcasing the competitive advantage of CusTFL-AN. On the UNSW-NB15 dataset, CusTFL-AN achieved an accuracy of 99.2%, surpassing methods such as the Two-Level Privacy-Preserving Framework (92.13%) and Ensemble-Based Deep Federated Learning (95.12%). Similarly, on the BoT-IoT dataset, CusTFL-AN attained 99.25% accuracy, outperforming the Two-Level Privacy-Preserving Framework (98.97%) and matching the performance of Clustered Federated Learning (99%).

The framework also excelled on the Edge-IIoT dataset, achieving 99.5% accuracy, a notable improvement over other method. The superior performance of CusTFL-AN can be attributed to its robust handling of data heterogeneity and class imbalance through the integration of Temporal Convolutional Networks (TCNs) and Adversarial Minority Augmentation (AMA). Furthermore, its ability to preserve privacy while maintaining high accuracy sets it apart from blockchain-based federated learning approaches, such as Blockchain-Based Federated Learning, which achieved 98.8% accuracy on the AWID dataset.

Beyond accuracy, CusTFL-AN demonstrated significant advantages in resource efficiency. The use of model compression and asynchronous updates reduced communication costs by 35% compared to traditional federated learning approaches like FedAvg, making it suitable for resource-constrained IoT environments. These results underscore the competitive edge of CusTFL-AN in achieving state-of-the-art accuracy while addressing practical deployment challenges in real-world IoT scenarios.

TABLE VII. ACCURACY COMPARISON WITH STATE-OF-THE-ART METHODS

Methods	Accuracy
Two-Level Privacy-Preserving Framework [77]	92.13% (UNSW-NB15), 98.97% (BoT-IoT)
Blockchain-Based Federated Learning [78]	98.8% (AWID dataset)
Ensemble-Based Deep Federated Learning [79]	95.12%
FLAD [80]	97%
Clustered Federated Learning [81]	99%
Proposed CusTFL-AN	99.2% (UNSW-NB15), 99.5% (Edge-IIoT), 99.25% (BoT-IoT)

Compared to other state of the art methods, the proposed CusTFL-AN model significantly outperforms and reflects this in its comparative analysis. As a more effective solution for real world cybersecurity challenges in IoT networks, it could cope with different attack types and traffic patterns of IoT traffic handling while preserving data privacy in Federated Learning environments.

K. Findings and Limitations of the Study

Findings: The objective of this study was to construct and test the model of Cyber-attack detection in IoT based on the Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN). Through extensive experimentation and performance comparison across multiple datasets, including UNSW-NB15, Edge-IIoT, and BoT-IoT, several key findings have emerged:

1. **Superior Accuracy and Robustness**: Consistently, the CusTFL-AN model outperforms existing state-of-the-art models, and achieves a accuracy of 99.2% on UNSW-Nb15 dataset, 99.5% on Edge-IIoTI dataset and 99.25% on BoT-IoTI dataset. Finally, these results also verify the model's robustness in identifying a wide variety of cyber-attacks on IoT traffic under different conditions and attack types.
2. **Balanced Performance on Precision, Recall, and F1-Score**: The performance obtained for precision, recall, F1-score of the model was well balanced thus saving on false positives yet minimizing on false negatives in IoT environment. For instance, CusTFL-AN model has a precision of 99.21%, a recall of 99.1%, an F1-score of 99.19 on UNSW-NB15 dataset and a much higher performance to baseline models.
3. **Low Mean Square Error (MSE)**: For all datasets, the CusTFL-AN consistently produced low MSE[59] values showing its predictive accuracy. For example, on, the UNSW-NB15 dataset, the model obtained MSE of 0.008, on Edge-IoT dataset MSE of 0.021, and on BoT-IoT dataset MSE 0.075. This low error rate shows that the model is also capable of generalizing different IoT attack scenarios.
4. **Effectiveness in Handling Class Imbalance**: The CusTFL-AN model solves class imbalance problems typically found in cybersecurity datasets with Adversarial Minority Augmentation (AMA). Generator that generates attack traffic (i.e minority class samples) helped the model to outperform by increasing the capacity to detect rare and sophisticated cyber-attacks.
5. **Privacy Preservation**: Through principles of federated learning, the CusTFL-AN model allows privacy preserving training over devices that are decentralized without having to transfer sensitive data to a central server. The special structure makes the model quite suitable for privacy sensitive IoT environments.

Limitations: Limitations in the study of the CusTFL-AN model include the promising performance.

Computational Resource Constraints: The experiments were run on a system with an Intel Core i5 processor with no dedicated GPU[59]. The model was good under these conditions, but processing time increased significantly when training their adversarial networks or working with large datasets. Given an environment of GPU acceleration, the model could be faster processed and optimized and would therefore be able to scale for real time IoT applications.

Lack of Real-World Testing: While the CusTFL-AN model was evaluated on benchmark datasets; the latter does not completely capture the complexity and diversity of the real world IoT environments [60][61]. However, future works should evaluate the model in the real world with real IoT traffic to observe how robust and adaptable the model is.

Sensitivity to Hyperparameters: The model fails to perform well as the selection of some of the hyperparameters such as the learning rate, batch size etc. will change the model's performance [62][63]. The model was hyperparameter tuned extensively, but the performance may differ across other IoT contexts or data sets, and further research into auto tuning mechanisms to achieve robustness across scenarios is warranted.

GAN Stability: Generative Adversarial Networks (GANs) naturally pose the challenge of training stability, that can have consequences on the generation of synthetic samples that are realistic. While the model had low MSE, GAN training across varying data distributions remains unstable and future work could explore methods of improving the GAN training stability.

Complexity of Temporal Dependencies: The Temporal Convolutional Networks (TCNs) succeeded in modeling long term dependencies in IoT traffic, but some more attack types such as Distributed Denial of Service (DDoS) attacks [64] added irregular temporal patterns that were hard to detect accurately. However, such greater complexity of temporal dependencies is easy for the model to present, so further exploration of hybrid approaches, such as the integration of recurrent neural networks (RNNs)[65], may improve the model's ability to deal with these types of temporal relations.

V. CONCLUSION

The Customized Temporal Federated Learning through Adversarial Networks (CusTFL-AN) model offers a novel approach to cyber-attack detection in IoT environments, addressing privacy, class imbalance, and temporal dependency challenges. By integrating Temporal Convolutional Networks (TCNs) and Generative Adversarial Networks (GANs) within a federated learning framework, CusTFL-AN captures critical temporal patterns in IoT traffic while preserving data privacy through decentralized training. The Adversarial Minority Augmentation (AMA) mechanism effectively balances datasets by generating realistic synthetic samples of minority-class attack traffic, improving detection of rare cyber-attacks. Validated on benchmark datasets UNSW-NB15, BoT-IoT, and Edge-IIoT, the model achieved state-of-the-art accuracy rates of 99.2%, 99.5%, and 99.25%, respectively, with high precision, recall, and F1-scores ensuring robustness against false positives and negatives. Despite these results, limitations include reliance on CPU-based experimentation, sensitivity to hyperparameter tuning, and challenges in GAN stability. Future research will explore real-world testing, auto-tuning mechanisms, and hybrid architectures to address evolving attack scenarios. The model reduced communication overhead by 35% using asynchronous updates and compression, showcasing scalability in resource-constrained IoT environments. CusTFL-AN significantly advances IoT cybersecurity, offering a scalable, privacy-preserving solution for critical infrastructures and smart cities, while future work will ensure adaptability to dynamic IoT ecosystems.

AUTHOR CONTRIBUTIONS

Lavanya Vemulapalli contributed to the conceptualization, methodology, data analysis, and manuscript writing. *P. Chandra Sekhar* provided supervision, critical revisions, and overall project guidance. Both authors reviewed and approved the final manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data available on request.

Conflicts of Interest: The authors declare no conflicts of interest regarding the publication of this paper.

REFERENCES

[1] A. Hassebo and M. Tealab, "Global Models of Smart Cities and Potential IoT Applications: A Review," *IoT*, vol. 4, no. 3, pp. 366–411, Aug. 2023, doi: 10.3390/iot4030017.

[2] D. Anand, A. Kaur, and M. Singh, "Research on Internet of Medical Things: Systematic Review, Research Trends and Challenges," *Recent Advances in Computer Science and Communications*, vol. 17, no. 6, Sep. 2024, doi: 10.2174/0126662558248187231124052846.

[3] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features," *Electronics*, vol. 9, no. 1, p. 144, Jan. 2020, doi: 10.3390/electronics9010144.

[4] H. Hamid *et al*., "IoT-based botnet attacks systematic mapping study of literature," *Scientometrics*, vol. 126, no. 4, pp. 2759–2800, Feb. 2021, doi: 10.1007/s11192-020-03819-5.

[5] F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammadi, B. A. Khalaf, and S. A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks," *Journal of Intelligent Systems*, vol. 32, no. 1, Jan. 2023, doi: 10.1515/jisys-2022-0155.

[6] M. Bhavsingh, K. Samunnisa, and B. Pannalal, "A Blockchain-based Approach for Securing Network Communications in IoT Environments," *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 10, pp. 37–43, Oct. 2023, doi: 10.22362/ijcert/2023/v10/i10/v10i106.

[7] H. P. H. Luu, A. Sakhi, and M. Latief, "Optimizing Group Management and Cryptographic Techniques for Secure and Efficient MTC Communication," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 2, pp. 1–8, Feb. 2024, doi: 10.22362/ijcert/2024/v11/i2/v11i201.

[8] K. Bichya, "Vampire Attacks in WSN Can Lead By Eloa," *Macaw Int. J. Adv. Res. Comput. Sci. Eng*, vol. 1, no. 1, pp. 21–27, Nov. 2015.

[9] M. V. A. Kumar, R. A. Nandedapu, and K. V. Sharma, "Real-Time Abdominal Trauma Detection Using LSTM Neural Networks with MediaPipe and OpenCV Integration," *Macaw Int. J. Adv. Res. Comput. Sci. Eng*, vol. 10, no. 1, pp. 36–48, Jun. 2024, doi: 10.70162/mijarcse//2024/v10/i1/v10i104.

[10] K. Samunnisa and S. V. K. Gaddam, "Blockchain-Based Decentralized Identity Management for Secure Digital Transactions," *Synth. Multidiscip. Res. J*., vol. 1, no. 2, pp. 22–29, Jun. 2023.

[11] A. Z. Tan, H. Yu, L. Cui, and Q. Yang, "Towards personalized Federated Learning," *IEEE Trans. Neural Netw. Learn. Syst*., vol. 34, no. 12, pp. 9587–9603, 2023, doi: 10.1109/TNNLS.2022.3160699.

[12] M. J. Pasha, K. P. Rao, A. MallaReddy, and V. Bande, "LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments," *Measurement: Sensors*, vol. 28, p. 100828, Aug. 2023, doi: 10.1016/j.measen.2023.100828.

[13] C. Thapa, M. A. P. Chamikara, and S. A. Camtepe, "Advancements of Federated Learning Towards Privacy Preservation: From Federated Learning to Split Learning," *Federated Learning Systems*, pp. 79–109, 2021, doi: 10.1007/978-3-030-70604-3_4.

[14] J.-P. A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 155–179, 2023, doi: 10.1016/j.iotcps.2023.04.001.

[15] P. Divyaja, M. K. Devi, and M. U. Rani, "Secure Smart bed on villages for monitoring and storing patient records on Cloud using IoT with Android Mobile," *International Journal of Computer Engineering in Research Trends*, vol. 9, no. 1, pp. 16–20, Jan. 2022, doi: 10.22362/ijcert/2022/v9/i01/v9i0103.

[16] E. M. Campos *et al*., "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges," *Computer Networks*, vol. 203, p. 108661, Feb. 2022, doi: 10.1016/j.comnet.2021.108661.

[17] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, p. 108379, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108379.

[18] G. Gitanjali and Er. R. Misra, "FedIoTect: Federated Machine Learning for Collaborative Internet of Things Threat Detection," *Research Square*, Feb. 2024, doi: 10.21203/rs.3.rs-3958165/v1.

[19] E. Petrova and A. El-Sayed, "Multi-Objective Optimization for Link Stability in IoT-Fog-Cloud Architectures," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 10, pp. 13–23, Oct. 2024, doi: 10.22362/ijcert/2024/v11/i10/v11i1002.

[20] A. A. Wardana, G. Kołaczek, and P. Sukarno, "Lightweight, Trust-Managing, and Privacy-Preserving Collaborative Intrusion Detection for Internet of Things," *Applied Sciences*, vol. 14, no. 10, p. 4109, May 2024, doi: 10.3390/app14104109.

[21] M. Amiri-Zarandi, R. A. Dara, and X. Lin, "SIDS: A federated learning approach for intrusion detection in IoT using Social Internet of Things," *Computer Networks*, vol. 236, p. 110005, Nov. 2023, doi: 10.1016/j.comnet.2023.110005.

[22] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, p. 108379, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108379.

[23] S. Xuan, M. Jin, X. Li, Z. Yao, W. Yang, and D. Man, "DAM-SE: A Blockchain-Based Optimized Solution for the Counterattacks in the Internet of Federated Learning Systems," *Security and Communication Networks*, vol. 2021, pp. 1–14, Jul. 2021, doi: 10.1155/2021/9965157.

[24] M. Bhavsingh, A. Lavanya, and K. Samunnisa, "Sustainable Computing Architectures for Ethical AI: Balancing Performance, Energy Efficiency, and Equity," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 10, pp. 24–32, Oct. 2024, doi: 10.22362/ijcert/2024/v11/i10/v11i1003

[25] P. Tyagi and S. K. M. bargavi, "Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 1, pp. 1–10, Mar. 2023, doi: 10.59461/ijdiic.v2i1.42.

[26] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, p. 108379, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108379.

[27] 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, doi: 10.1109/access.2021.3118642.

[28] S. Bahadoripour, H. Karimipour, A. N. Jahromi, and A. Islam, "An explainable multi-modal model for advanced cyber-attack detection in industrial control systems," *Internet of Things*, vol. 25, p. 101092, Apr. 2024, doi: 10.1016/j.iot.2024.101092.

[29] S. I. Popoola, G. Gui, M. Hammoudeh, R. Ande, B. Adebisi, and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3930–3944, 2022, doi: 10.1109/JIOT.2021.3100755.

[30] M. Roopak, J. Chambers, and G. Yun Tian, "Deep Learning Models for Cyber Security in IoT Networks," *2019 IEEE CCWC*, 2019, doi: 10.1109/CCWC.2019.8666588.

[31] 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. DOI: 10.1109/ACCESS.2021.3118642.

[32] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2211–2234, 2021. DOI: 10.1007/s40747-021-00347-1.

[33] Y. Nohara, K. Matsumoto, H. Soejima, and N. Nakashima, "Explanation of machine learning models using shapley additive explanation and application for real data in hospital," *Computer Methods and Programs in Biomedicine*, vol. 214, p. 106584, 2022. DOI: 10.1016/j.cmpb.2021.106584.

[34] A. A. Abdellatif, N. Mhaisen, A. Mohamed, A. Erbad, M. Guizani, Z. Dawy, and W. Nasreddine, "Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data," *Future Generation Computer Systems*, vol. 128, pp. 406–419, 2022. DOI: 10.1016/j.future.2021.10.015.

[35] S. Sun, P. Sharma, K. Nwodo, A. Stavrou, and H. Wang, "FedMADE: Robust Federated Learning for Intrusion Detection in IoT Networks Using a Dynamic Aggregation Method," *arXiv: 2201.00123*, 2024.

[36] S. Mekala, "A Continuous Neighbour Discovery Protocol for Asymmetric Wireless Sensor Networks," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. SP7, pp. 633–645, Jul. 2020, doi: 10.5373/jardcs/v12sp7/20202153.

[37] S. Mekala, M. A, D. Baswaraj, J. Joshi, and R. M, "EASND: Energy Adaptive Secure Neighbour Discovery Scheme for Wireless Sensor Networks," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 5s, pp. 446–458, Jun. 2023, doi: 10.17762/ijritcc.v11i5s.7097.

[38] M. Jdaitawi, A. F. Kan'an, and K. Samunnisa, "Blockchain-Enabled Secure Data Sharing in Distributed IoT Networks: A Paradigm for Smart City Applications," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 11, pp. 24–32, Nov. 2024, doi: 10.22362/ijcert/2024/v11/i11/v11i1103%20.

[39] X. Zhang, M. Hong, S. Dhople, W. Yin, and Y. Liu, "Fedpd: A federated learning framework with adaptivity to non-iid data," *IEEE Transactions on Signal Processing*, vol. 69, pp. 6055–6070, 2021.

[40] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Federated quantum-based privacy-preserving threat detection model for consumer internet of things," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, 2024.

[41] M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021.

[42] W. Al Mahmud and S. Huang, "Hybrid Cloud-Edge Systems for Computational Physics: Enhancing Large-Scale Simulations Through Distributed Models," *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 12, pp. 23–32, Dec. 2024, doi: 10.22362/ijcert/2024/v11/i12/v11i1203.

[43] H. Wang, Y. Cai, J. Wang, C. Ma, C. Ge, X. Qu, and L. Zhou, "Voltran: Unlocking trust and confidentiality in decentralized federated learning aggregation," *IEEE Transactions on Information Forensics and Security*, vol. 19, 2024.

[44] C. G. V. N. Prasad, A. Mallareddy, M. Pounambal, and V. Velayutham, "Edge Computing and Blockchain in Smart Agriculture Systems," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 10, no. 1s, pp. 265–273, Dec. 2022, doi: 10.17762/ijritcc.v10i1s.5848.

[45] R. Boddupalli, K. Malika, R. M. Harshita, and K. V. Sharma, "QuickCert - A Scalable Web-Based Certificate Management System for Academic Institutions with Enhanced Security and Real-Time Automation," *Synth. Multidiscip. Res. J.*, vol. 2, no. 3, pp. 1–10, Sep. 2024 doi: 10.70162/smrj/2024/v2/i3/v2i301.

[46] R. Doriguzzi-Corin and D. Siracusa, "FLAD: adaptive federated learning for DDoS attack detection," *Computers & Security*, vol. 137, p. 103597, 2024.

[47] S. Bahadoripour, H. Karimipour, A. N. Jahromi, and A. Islam, "An explainable multi-modal model for advanced cyber-attack detection in industrial control systems," *Internet of Things*, vol. 25, p. 101092, 2024. DOI: 10.1016/j.iot.2024.101092.

[48] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *Proceedings of the Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015, doi: 10.1109/MilCIS.2015.7348942.

[49] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019, doi: 10.1016/j.future.2019.05.041.

[50] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40277–40288, 2022, doi: 10.1109/ACCESS.2022.3165809.S.

[51] Mekala and K. S. S. Chatrapathi, "Energy-Efficient Neighbor Discovery Using Bacterial Foraging Optimization (BFO) Algorithm for Directional Wireless Sensor Networks," in *Lecture Notes in Electrical Engineering*, vol. 749, pp. 93–107, 2021.

[52] M. Nobakht, R. Javidan, and A. Pourebrahimi, "SIM-FED: Secure IoT Malware Detection Model with Federated Learning," *Computers and Electrical Engineering*, vol. 116, p. 109139, 2024.

[53] M. Moustafa and J. Slay, "The UNSW-NB15 Dataset for Network Intrusion Detection Systems (NIDS) Benchmark," *IEEE International Conference on Information Assurance and Security (IAS)*, pp. 1–6, 2015.

[54] T. Alharbi, M. A. Ferrag, L. Maglaras, H. Janicke, and A. H. Al-Bayatti, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 9, pp. 149914–149944, 2021.

[55] S. Mekala, M. A, D. Baswaraj, J. Joshi, and R. M, "EASND: Energy Adaptive Secure Neighbour Discovery Scheme for Wireless Sensor Networks," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 5s, pp. 446–458, Jun. 2023, doi: 10.17762/ijritcc.v11i5s.7097.

[56] M. Koroniotis, N. Moustafa, E. Sitnikova, and K. R. D. Choo, "Bot-IoT: A New IoT Botnet Dataset with Diversified Attack Types and Traffic Varieties," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[57] R. Shahbazian and I. Trubitsyna, "DEGAIN: Generative-Adversarial-Network-Based Missing Data Imputation," *Information*, vol. 13, no. 12, p. 575, 2022.

[58] Z. Guo, Y. Wan, and H. Ye, "A data imputation method for multivariate time series based on generative adversarial network," *Neurocomputing*, vol. 360, pp. 185–197, 2019.

[59] S. Mekala and K. Chatrapati, “Present State-of-the-Art of Continuous Neighbor Discovery in Asynchronous Wireless Sensor Networks,” *EAI Endorsed Transactions on Energy Web*, p. 166772, Jul. 2018, doi: 10.4108/eai.27-10-2020.166772.

[60] J. Teng, D. Zhang, W. Zou, M. Li, and D. J. Lee, "Typical facial expression network using a facial feature decoupler and spatial-temporal learning," *IEEE Transactions on Affective Computing*, vol. 14, no. 2, pp. 1125–1137, 2021.

[61] S. Mekala, A. Mallareddy, R. R. Tandu, and K. Radhika, “Machine Learning and Fuzzy Logic Based Intelligent Algorithm for Energy Efficient Routing in Wireless Sensor Networks,” *Multi-disciplinary Trends in Artificial Intelligence*, pp. 523–533, 2023, doi: 10.1007/978-3-031-36402-0_49.

[62] A. Silva and P. Müller, “Machine Learning-Driven Resource Allocation in IoT-Fog-Cloud Networks,” *Synth. Multidiscip. Res. J.*, vol. 2, no. 3, pp. 11–21, Sep. 2024, doi: 10.70162/smrj/2024/v2/i3/v2i302.

[63] Y. He and J. Zhao, "Temporal convolutional networks for anomaly detection in time series," in *Journal of Physics: Conference Series*, vol. 1213, no. 4, p. 042050, 2019.

[64] M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary, "Federated learning with personalization layers," *arXiv preprint arXiv:1912.00818*, 2019.

[65] L. Collins, H. Hassani, A. Mokhtari, and S. Shakkottai, "Exploiting shared representations for personalized federated learning," in *Proceedings of the 38th International Conference on Machine Learning*, vol. 139, pp. 2089–2099, 2021.

[66] J. Zhang, Y. Hua, H. Wang, T. Song, Z. Xue, R. Ma, and H. Guan, "FedALA: Adaptive local aggregation for personalized federated learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 9, pp. 11237–11244, June 2023.

[67] X. Su and G. Zhang, "APFed: Adaptive personalized federated learning for intrusion detection in maritime meteorological sensor networks," *Digital Communications and Networks*, 2024.

[68] 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.

[69] S. D., C. R. Mohan, B. H. Kumar, R. D. C. Pecho, and M. J. Pasha, "An Approach for Coordinating Lane Changes between Autonomous Vehicles in Congested Areas," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 6s, pp. 403–416, 2023.

[70] M. S. Lakshmi, G. Rajavikram, V. Dattatreya, B. S. Jyothi, S. Patil, and M. Bhavsingh, "Evaluating the Isolation Forest Method for Anomaly Detection in Software-Defined Networking Security," *Journal of Electrical Systems*, vol. 19, no. 4, pp. 1–10, 2023.

[71] T. Chai and R. R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)," *Geoscientific Model Development Discussions*, vol. 7, no. 1, pp. 1525–1534, 2014.

[72] S. Deshmukh, S. Inamdar, and S. Waghmode, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," *International Journal of Computer Engineering in Research Trends*, vol. 3, no. 3, pp. 149–151, Mar. 2016.

[73] M. Bhavsingh, "Autonomous Navigation in Urban Environments Using Deep Learning Models," *International Conference on Intelligent Computation Technology and Automation (ICICTA)*, 2021, doi: 10.1109/ICICTA.2021.9355612.

[74] J. Vinothini and S. V. J. E, “IOT edge computing layer modification based cyber-attack detection using Federated-Active Learning,” Research Square, Oct. 2024, doi: 10.21203/rs.3.rs-5281086/v1.

[75] M. Bhavsingh, K. Samunnisa, and S. K. K. Shareef, "A Blockchain-Based Approach for Securing Network Communications in IoT Environments," *Macaw International Journal of Advanced Research in Computer Science and Engineering*, vol. 8, no. 1, pp. 1–7, 2022.

[76] J. C. Kimeto and N. A. M. Mokmin, “Leveraging Augmented Reality for Inclusive Education: A Framework for Personalized Learning Experiences,” *Int. J. Comput. Eng. Res. Trends*, vol. 11, no. 12, pp. 10–22, Dec. 2024.

[77] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Two-Level Privacy-Preserving Framework: Federated Learning for Attack Detection in the Consumer Internet of Things," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4258-4265, Feb. 2024, doi: 10.1109/TCE.2024.3349490.

[78] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177-4186, 2019.

[79] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "An ensemble deep federated learning cyber-threat hunting model for Industrial Internet of Things," *Computer Communications*, vol. 198, pp. 108-116, 2023.

[80] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. K. Chan, "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205-1221, 2019.

[81] 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.